По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, однако и в этом случае сомнения не оставят меня.

Ю. Спаффорд

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Е. И. Деза, Л. В. Котова

ВВЕДЕНИЕ В КРИПТОГРАФИЮ

Теоретико-числовые основы защиты информации

Около 150 разобранных примеров различного уровня сложности по всем основным разделам криптографии и соответствующим разделам прикладной теории чисел

URSS

14
Е. И. Деза
Л. В. Котова
ВВЕДЕНИЕ В КРИПТОГРАФИЮ
Теоретико-числовые основы защиты информации
URSS

Основы защиты информации • № 14

Е. И. Деза, Л. В. Котова

ВВЕДЕНИЕ В КРИПТОГРАФИЮ

Теоретико-числовые основы защиты информации

Издание стереотипное

URSS
МОСКВА

ББК 22.176 22.18 32.811 32.97

Редактор серии *М. А. Борисов*

Деза Елена Ивановна, Котова Лидия Владимировна

Введение в криптографию: Теоретико-числовые основы защиты информации. Учебное пособие. Изд. стереотип. — М.: ЛЕНАНД, 2022. — 376 с. (Основы защиты информации. № 14.)

Учебное пособие предназначено для изучения курсов «Методы и средства защиты информации», «Основы криптографии», других родственных дисциплин основных образовательных программ высшего образования, для изучения дисциплин по выбору, посвященных основам криптографии и прикладным вопросам теории чисел. Пособие включает в себя теоретические факты, упражнения и задачи различного уровня сложности по всем основным разделам криптографии и соответствующим разделам прикладной теории чисел. Помимо обширного списка упражнений и задач, в пособии представлены индивидуальные задания для проведения творческих и лабораторных работ, контрольные вопросы и типовые задания обязательного минимума по каждой теме.

Пособие составлено в соответствии с требованиями федеральных государственных образовательных стандартов высшего образования и примерных основных образовательных программ высшего образования. Книга написана на базе многолетнего опыта практической работы авторов, ее материал построен по модульному принципу: выбор изучаемых разделов, порядок знакомства с ними и глубина освоения соответствующих теоретических и практических вопросов зависят от направления подготовки и профиля, в рамках которых проводится обучение.

Пособие предназначено для преподавателей и студентов высших учебных заведений, прежде всего математических факультетов педвузов, учителей профильной школы, старшеклассников, интересующихся прикладными теоретико-числовыми проблемами, всех, кого привлекают история и современные тенденции развития криптографии. Материалы пособия могут быть полезны для организации индивидуальной учебно-исследовательской работы студентов в рамках подготовки курсовых работ, выпускных квалификационных работ бакалавра и магистерских диссертаций.

Рецензенты:

д-р физ.-мат. наук, проф. кафедры теоретической информатики и дискретной математики МПГУ *И. И. Баврин*;
д-р физ.-мат. наук, проф. кафедры математического анализа МГУ имени М. В. Ломоносова *В. Г. Чирский*

Печатается по решению ученого совета Московского педагогического государственного университета

Формат 60×90/16. Печ. л. 23,5. Доп. тираж. Зак. № АР-9586.

Отпечатано в ООО «ЛЕНАНД». 117312, Москва, проспект 60-летия Октября, 11А, стр. 11.

ISBN 978–5–9710–7833–3

978–5–9519–2849–8

32798 ID 282571

Содержание

Обозначения

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел;
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ — множество целых чисел.
- $\text{rest}(a, b)$ — остаток от деления целого числа a на натуральное число b: $a = bq + \text{rest}(a, b)$, где $q, \text{rest}(a, b) \in \mathbb{Z}$, и $0 \leqslant \text{rest}(a, b) < b$.
- $b|a$ — целое число b, отличное от нуля, делит целое число a, то есть $a = bc$, где $c \in \mathbb{Z}$.
- $(a_1, \ldots a_n)$ — *наибольший общий делитель* целых чисел $a_1, \ldots, a_n$, хотя бы одно из которых не равно нулю, то есть наибольшее целое число, делящее каждое из чисел $a_1, \ldots, a_n$.
- $[a_1, \ldots a_n]$ — *наименьшее общее кратное* целых чисел $a_1, \ldots, a_n$, каждое из которых не равно нулю, то есть наименьшее натуральное число, делящееся на каждое из чисел $a_1, \ldots, a_n$.
- $P = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ — множество *простых чисел*, то есть натуральных чисел, имеющих ровно два натуральных делителя; p, q, $p_1, \ldots, p_s, q_1, \ldots, q_t$ — простые числа; $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, где $p_1, p_2, \ldots, p_s$ — различные простые числа, и $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$ — *каноническое представление* натурального числа $n > 1$, то есть представление n в виде произведения натуральных степеней различных простых чисел.
- p_n — n-е простое число: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ и т. д.
- $p = a \cdot q + 1$ (где $p, q \in P$, и q велико) — *сильное простое число*, то есть достаточно большое простое число p, такое что $p - 1$ имеет большие простые делители, например q (причем $q - 1$ также имеет большие простые делители), и $p + 1$ имеет большие простые делители.
- $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ (где $p_1, p_2, \ldots, p_s$ — различные простые числа) — *бесквадратное число*.
- $S = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \ldots\}$ — множество *составных чисел*, то есть натуральных чисел, имеющих не менее трех натуральных делителей; $\mathbb{N} = P \cup S \cup \{1\}$.
- $n = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot \ldots \cdot p_s^{\alpha_{p_s}}$ (где $2, 3, \ldots, p_s$ — последовательные простые числа, $\alpha_2 \geqslant \alpha_3 \geqslant \ldots \geqslant \alpha_{p_s}$, и $\alpha_{p_s} = 1$ кроме $n = 4; 36$) — *сильно составное число*, то есть натуральное число, которое имеет больше делителей, чем любое предшествующее ему натуральное число.

- $B = \{p_1, p_2, \ldots, p_s\}$ — *база разложения*, то есть множество, состоящее из нескольких различных простых чисел; $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ (где $\alpha_i \geqslant 0$) — *B-гладкое число*, то есть натуральное число, все простые делители которого принадлежат базе B.
- $n = \overline{(a_{k-1}a_{k-2}\ldots a_1a_0)}_g$ (где $k \geqslant 0$, $0 \leqslant a_i < g$, и $a_{k-1} \neq 0$) — *запись* натурального числа n *в системе счисления с основанием* g, то есть представление $n = a_{k-1}g^{k-1} + a_{k-2}g^{k-2} + \ldots + a_1 \cdot g + a_0$; a_0, a_1, $\ldots$, a_{k-1} — *g-ичные цифры* числа n.
- $\lfloor x \rfloor$ — *целая часть* действительного числа x, то есть наибольшее целое число, не превосходящее x; $\lceil x \rceil$ — наименьшее целое число, большее или равное x.
- $\varphi(n)$ — *функция Эйлера*, дающая число натуральных чисел, не превосходящих n и взаимно простых с ним:

$$\varphi(n) = |\{x \in \mathbb{N} : x \leqslant n, (x, n) = 1\}| = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

- $\mu(n)$ — *функция Мебиуса*: $\mu(1) = 1$, $\mu(n) = (-1)^s$ для бесквадратного числа $n = p_1 \cdot \ldots \cdot p_s$, и $\mu(n) = 0$ в остальных случаях.
- $\operatorname{sign}(x)$ — *знак* действительного числа x: $\operatorname{sign}(x) = 1$ при $x > 0$, $\operatorname{sign}(x) = -1$ при $x < 0$, и $\operatorname{sign}(x) = 0$ при $x = 0$.
- $\pi(x) = \sum\limits_{p \leqslant x} 1$ — число простых чисел, не превосходящих действительное число x.
- $\sum\limits_{d|n} f(d)$ $\left(\prod\limits_{d|n} f(d)\right)$ — сумма (произведение) значений комплекснозначной функции $f(x)$, определенной для всех $x \in \mathbb{N}$, по всем натуральным делителям d натурального числа n.
- $f(n) = O(g(n))$ (где f, g — комплекснозначные функции натурального аргумента) — функция $f(n)$ есть *O-большое* от функции $g(n)$, то есть существует такая положительная действительная константа C и такое натуральное число n_0, что для любого $n \geqslant n_0$ имеет место неравенство $|f(n)| \leqslant C \cdot |h(n)|$.
- $a \equiv b \pmod{n}$ — целые числа a и b *сравнимы по модулю* n, $n \in \mathbb{N}$, то есть a и b имеют одинаковые остатки при делении на n, или, что то же, $n|(a - b)$.
- $a \not\equiv b \pmod{n}$ — целые числа a и b несравнимы по модулю n, $n \in \mathbb{N}$, то есть a и b имеют различные остатки при делении на n, или, что то же, $n \nmid (a - b)$.

- $\mathbf{a_n} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$ — *класс вычетов* (числа a) по модулю n, то есть множество всех целых чисел, сравнимых с числом a по модулю n.
- $a \bmod n$ — один из вычетов, принадлежащих классу вычетов $\mathbf{a_n}$; как правило, наименьший неотрицательный (наименьший по модулю, наименьший натуральный) вычет класса $\mathbf{a_n}$, то есть наименьшее неотрицательное (наименьшее по модулю, наименьшее натуральное) число, сравнимое с a по модулю n.
- $\left(\frac{a}{p}\right)$ — *символ Лежандра*: $\left(\frac{a}{p}\right) = 1$, если целое число a, взаимно простое с нечетным простым числом p, является квадратичным вычетом по модулю p (то есть сравнение $x^2 \equiv a \pmod{p}$ разрешимо), и $\left(\frac{a}{p}\right) = -1$, если целое число a, взаимно простое с нечетным простым числом p, является квадратичным невычетом по модулю p (то есть сравнение $x^2 \equiv a \pmod{p}$ неразрешимо); если $a|p$, то $\left(\frac{a}{p}\right) = 0$.
- $\left(\frac{a}{n}\right) = \prod\limits_{i=1}^{s} \left(\frac{a}{p_i}\right)^{\alpha_i}$ для нечетного $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ — *символ Якоби*.
- $P_n(a)$ — *показатель* целого числа a (взаимно простого с n) по модулю n, то есть наименьшее натуральное число γ, такое что $a^\gamma \equiv 1 \pmod{n}$; если $P_n(g) = \varphi(n)$, то g — *первообразный корень* по модулю n.
- $\mathrm{ind}_g a$ — *индекс* целого числа a по модулю n с основанием g, то есть наименьшее целое неотрицательное число β, такое что $a \equiv g^\beta \pmod{n}$. Здесь $n \in \{2, 4, p^\alpha, 2p^\alpha\}$ для нечетного простого p и натурального α, g — первообразный корень по модулю n, и a — целое число, взаимно простое с n.
- $[a_0, a_1, \ldots, a_n, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots \cfrac{1}{a_n + \ldots}}}$ — *цепная дробь*. Здесь a_0 — некоторое целое число, а все a_n, $n \in \mathbb{N}$ — натуральные числа, причем последнее, если оно существует, отлично от 1.
- $\delta_k = [a_0, a_1, \ldots, a_k] = \frac{P_k}{Q_k}$, $k = 0, 1, \ldots, n, \ldots,$ — *подходящие дроби* для цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$; a_k, $k = 0, 1, \ldots, n, \ldots,$ — *неполные частные* цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$; $\alpha_k = [a_k, a_{k+1}, \ldots,$

$a_n, \ldots]$, $k = 0, 1, \ldots, n, \ldots$, — *полные частные* цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$.

- $\log_a x$, $a, x \in \mathbb{R}$, $a > 0, a \neq 1$, $x > 0$, — *логарифм числа* x *по основанию* a, то есть такое число $y \in \mathbb{R}$, что $a^x = y$; $\log x = \ln x$ — *натуральный логарифм* $\log_e x$.
- $n! = 1 \cdot 2 \cdot \ldots \cdot n$ — *факториал* натурального числа n; $0! = 1$.
- $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$, $n, m \in \mathbb{N}$, $n \geqslant m$, — *число сочетаний* из n элементов по m элементов; числа $\binom{n}{m}$ являются коэффициентами разложения *бинома Ньютона*:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \\ + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{1}ab^{n-1} + \binom{n}{n}b^n.$$

- $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ — *числа Ферма*.
- $M_n = 2^n - 1$ $n = 1, 2, 3, \ldots$ — *числа Мерсенна*.
- $E = p_1 \cdot p_2 \cdot \ldots \cdot p_s - 1$ (где $p_i \in P$ и $p_i \neq p_j$ при $i \neq j$) — *евклидово число*.
- $u_1 = u_2 = 1$, $u_{n+2} = u_{n+1} + u_n$ — *числа Фибоначчи*.
- $\langle K, + \rangle$ — *полугруппа*: операция сложения $+$ ассоциативна; $\langle K, +, 0 \rangle$ — *коммутативная группа*: операция сложения $+$ ассоциативна и коммутативна, 0 — нейтральный элемент по сложению, для любого элемента $a \in K$ существует противоположный ему элемент $-a \in K$.
- $\mathbb{K} = \langle K, +, \cdot, 0 \rangle$ — *кольцо*: $\langle K, +, 0 \rangle$ — коммутативная группа, $\langle K \backslash \{0\}, \cdot \rangle$ — полугруппа, и операция умножения дистрибутивна относительно операции сложения.
- $\mathbb{Z} = \langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ — *кольцо целых чисел*.
- $\mathbb{Z}_n = \langle \mathbb{Z}_n, +, \cdot, 0, 1 \rangle$ — *кольцо классов вычетов по модулю* n.
- $M_k(\mathbb{K})$ — множество всех $k \times k$ матриц с элементами из кольца $\mathbb{K}$; $M_k^*(\mathbb{K})$ — множество всех обратимых $k \times k$ матриц с элементами из кольца $\mathbb{K}$.
- $\Delta = \Delta_A$ — *определитель* матрицы $A \in M_k^*(\mathbb{K})$.
- $\varphi_k(\mathbb{Z}_n)$ — число обратимых $k \times k$ матриц с элементами из $\mathbb{Z}_n$:

$$\varphi_k(\mathbb{Z}_n) = |M^*(\mathbb{Z}_n)| = N^{k^2} \cdot \prod_{p|n} \left(\left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{p^2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p^k}\right) \right).$$

- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \pmod{n}$ — матрицы $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in M_2(\mathbb{Z})$ *сравнимы по модулю* $n \in \mathbb{N}$, то есть $a \equiv a_1 \pmod{n}$, $b \equiv b_1 \pmod{n}$, $c \equiv c_1 \pmod{n}$, $d \equiv d_1 \pmod{n}$.
- $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} u \\ v \end{pmatrix} \pmod{n}$ — вектора $\begin{pmatrix} x \\ y \end{pmatrix}$ и $\begin{pmatrix} u \\ v \end{pmatrix}$ с целыми элементами *сравнимы по модулю* $n \in \mathbb{N}$, то есть $x \equiv u \pmod{n}$, и $y \equiv v \pmod{n}$.
- $\mathbb{F} = \langle F, +, \cdot, 0, 1\rangle$ — *поле*: $\langle F, +, 0\rangle$ — коммутативная группа, $\langle F\backslash\{0\}, \cdot, 1\rangle$ — коммутативная группа, и операция умножения дистрибутивна относительно операции сложения; $\mathbb{F}^* = \langle F^*, \cdot, 1\rangle$ (где $F^* = F\backslash\{0\}$) — *мультипликативная группа* поля $\mathbb{F}$).
- $\mathbb{F}_q = \langle F_q, +, \cdot, 0, 1\rangle$ — *конечное поле* из q элементов.
- $n * a$ (где $a \in F$, $n \in \mathbb{N}$) — *натуральное кратное* элемента a поля $\mathbb{F}$, то есть сумма n копий элемента $a \in F : n * a = \sum_{i=1}^{n} a$.
- $\operatorname{ord} a$ — *порядок* ненулевого элемента a конечного поля $\mathbb{F}_q$, то есть наименьшее натуральное число γ, такое что $a^\gamma = 1$; если $\operatorname{ord} a = q-1$, то a — *примитивный элемент* поля; если $q = p$, $p \in P$, то $\operatorname{ord} a = P_p(a)$.
- $\log_g a$ — *дискретный логарифм* ненулевого элемента a конечного поля $\mathbb{F}_q$ с основанием $g \in F_q^*$, то есть наименьшее целое неотрицательное число β, такое что $g^\beta = a$; если $q = p$, $p \in P$ и g — первообразный корень по модулю p, то $\log_g a = \operatorname{ind}_g a$.
- $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n, a_{n-1}, \ldots, a_0 \in F$, $a_n \neq 0$ — *многочлен степени* n над полем $\mathbb{F}$; $\deg f(x)$ — степень n многочлена $f(x)$.
- $\mathbb{F}[x] = \langle F[x], +, \cdot, 0, 1\rangle$ — *кольцо многочленов* над полем $\mathbb{F}$.
- $\operatorname{ord} f(x)$ — *порядок многочлена* $f \in F_p[x]$, то есть наименьшее натуральное число δ, такое что $f|(x^\delta - 1)$.
- $a_p(n)$ — число *неприводимых* над полем $\mathbb{F}_p$ многочленов степени n, то есть многочленов $f \in F_p[x]$, которые нельзя представить над $\mathbb{F}_p$ в виде произведения двух многочленов положительной степени:
$$a_p(n) = \frac{1}{n} \sum_{m|n} p^{\frac{n}{m}} \mu(m).$$
- $b_p(n)$ — число *примитивных* многочленов степени n над полем F_p, то есть многочленов $f \in F_p[x]$ степени n, для которых
$$\operatorname{ord}(f(x)) = p^n - 1 : b_p(n) = \frac{\varphi(p^n - 1)}{n}.$$

- $\delta = \{\delta_n\}_{n=0}^{\infty} = \{\delta_n\}_n$ — *псевдослучайная последовательность.*
- $S(\mathbb{F}_p) = \{\alpha = \{\alpha_n\}_n | n = 0, 1, 2, \ldots, \alpha_n \in F_p\}$ — множество всех последовательностей элементов поля $\mathbb{F}_p$; $\theta = \{0\}_n$ — *нулевая последовательность*, состоящая из одних нулей; $\varepsilon = \{1\}_n$ — *единичная последовательность*, состоящая из одних единиц.
- $T \bullet \alpha = T \bullet \{\alpha_n\}_n = \{\alpha_{n+1}\}_n$ — *сдвиг* последовательности $\alpha \in S(\mathbb{F}_p)$.
- $g^T \bullet \alpha = \beta$ — преобразование последовательности $\alpha \in S(\mathbb{F}_p)$ в последовательность $\beta \in S(\mathbb{F}_p)$ с помощью *полиномиального оператора* g^T, задаваемого многочленом $g(\lambda) = b_0 + b_1\lambda + b_2\lambda^2 + \ldots + b_k\lambda_k \in F_p[\lambda]$: для любого целого неотрицательного n $\beta_n = b_0 \cdot \alpha_n + b_1\alpha_{n+1} + b_2\alpha_{n+2} + \ldots + b_k\alpha_{n+k}$.
- $m_\delta(\lambda)$ — *минимальный многочлен* последовательности δ, то есть нормированный и наименьшей степени многочлен, *аннулирующий* $\delta \in S(\mathbb{F}_p)$: $m_\delta^T \bullet \delta = \theta$.
- $\{\delta_x\}_x$ — *линейная рекуррентная последовательность* над полем $\mathbb{F}_p$, являющаяся *решением линейного рекуррентного уравнения* $\delta_{x+n} = a_{n-1} \times \times \delta_{x+n-1} + a_{n-2} \cdot \delta_{x+n-2} + \ldots + a_0 \cdot \delta_x$, $(a_i \in F_p)$ *порядка* n над полем $\mathbb{F}_p$; $f(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - \ldots - a_0 \in F_p[\lambda]$ — *характеристический многочлен* этого уравнения; $S(f)$ — множество всех решений этого уравнения.
- $\operatorname{per}\delta$ — *примитивный период* линейной рекуррентной последовательности $\delta \in S(f)$, то есть наименьший натуральный период этой последовательности.
- $\smile$ — символ пробела в используемых открытых сообщениях и шифротекстах.

Введение

Учебное пособие составлено в соответствии с требованиями федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) и примерных основных образовательных программ высшего образования (ООП ВО) по направлениям подготовки 44.03.01 — Педагогическое образование (профили: Математика, Информатика), 44.03.05 — Педагогическое образование с двумя профилями подготовки (профили: Математика и Информатика, Математика и Экономика, Информатика и Математика, Информатика и Экономика), 01.03.01 — Математика (профиль: Преподавание математики и информатики), 09.03.02 — Информационные системы и технологии (профиль: Информационные технологии в образовании) и др.

Учебное особие подготовлено на основе лекций, в течение многих лет читавшихся авторами студентам математического факультета Московского государственного педагогического университета, и предназначено для изучения курсов «Методы и средства защиты информации», «Основы криптографии», других родственных дисциплин ООП ВО, для изучения дисциплин по выбору, посвященных основам криптографии и прикладным вопросам теории чисел. Материалы пособия могут быть полезны и для организации индивидуальной учебно-исследовательской работы студентов в рамках подготовки курсовых работ, выпускных квалификационных работ бакалавра и магистерских диссертаций.

Учебное пособие включает в себя теоретические факты, упражнения и задачи различного уровня сложности по всем основным разделам криптографии и соответствующим разделам прикладной теории чисел. Эти материалы представлены в первых восьми главах пособия: «Из истории криптографии», «Простейшие симметричные криптосистемы», «Шифрующие матрицы», «Система *RSA*. Дискретный логарифм», «Вычислительные алгоритмы и их трудоемкость», «Простые и псевдопростые числа», «Факторизация натуральных чисел», «Псевдослучайные последовательности над конечным полем». В девятой главе «Материалы для организации промежуточного и итогового контроля» содержатся контрольные вопросы для подготовки к зачету и экзамену, типовые задания обязательного минимума по криптографии и прикладным разделам теории чисел, индивидуальные задания для проведения творческих лабораторных работ к раз-

делу «Из истории криптографии», а также индивидуальные задания для проведения лабораторных работ к разделам «Система *RSA*. Дискретный логарифм», «Вычислительные алгоритмы и их трудоемкость», «Простые и псевдопростые числа», «Факторизация натуральных чисел», «Псевдослучайные последовательности над конечным полем». В десятой главе «Таблицы» собраны полезные для освоения курса справочные материалы, представленные в виде таблиц. Для облегчения навигации по теоретическим вопросам курса предназначен и предлагаемый в конце пособия «Словарь терминов».

Изложение каждого из выделенных содержательных разделов проведено в пособии по единой схеме: основные определения и иллюстрирующие их примеры; свойства рассматриваемых объектов и примеры решения связанных с ними задач; упражнения, решаемые по представленным в примерах образцам и предназначенные для первоначального усвоения предлагаемого теоретического и практического материала, задачи для самостоятельного решения, направленные на углубленное знакомство студентов с рассматриваемыми вопросами. Индивидуальные задания для проведения лабораторных работ, контрольные вопросы и типовые задания обязательного минимума по каждой теме можно найти в девятой главе пособия.

В конце каждой «содержательной» главы имеется список рекомендуемой для изучения темы литературы. В этом списке представлены все источники, которые были использованы авторами при разработке теоретических и практических материалов по соответствующему разделу курса; в частности, источники, в которых можно найти доказательства теоретических утверждений, представленных в данном пособии без доказательства. Кроме того, в список литературы включен ряд дополнительных источников, полезных и для углубленного изучения изложенных в разделе вопросов (в том числе для успешного выполнения соответствующих творческих и лабораторных работ), и для организации самостоятельной учебно-исследовательской работы студентов, заинтересовавшихся тематикой, в рамках написания курсовых работ, выпускных квалификационных работ бакалавра и магистерских диссертаций.

Пособие построено по модульному принципу: выбор изучаемых разделов, порядок знакомства с ними и глубина освоения соответствующих теоретических и практических вопросов зависят от направления подготовки и профиля, в рамках которых проводится обучение, а также от уровня предварительной подготовки обучающихся в предметной области «Математика и Информационные технологии». Для изучения курса студентам необходимы знание ряда классических вопросов элементарной теории чисел («Теория делимости», «Теория сравнений», «Решение сравнений вто-

рой степени; символы Лежандра и Якоби», «Показатели, первообразные корни и индексы», «Цепные дроби»), знакомство с основными алгебраическими структурами (прежде всего, с определением и классическими примерами кольца и поля), а также владение начальными навыками программирования.

Авторы выражают глубокое уважение памяти своих учителей и коллег А. А. Бухштаба, С. М. Воронина, Е. Б. Гладковой, Д. А. Митькина, В. И. Нечаева, Л. Л. Степановой, В. Л. Топунова: в ходе многолетнего творческого общения с ними была создана теоретическая концепция курса, посвященного криптографии, а их ставшие сегодня классическими публикации легли в основу практических разработок, на основе которых и было впоследствии написано данное пособие. Авторы благодарят за многолетнее плодотворное сотрудничество своих коллег Н. В. Александрову, Ю. Н. Баулину, Г. Г. Брайчева, А. В. Жмулеву, Т. К. Иконникову, Е. С. Крупицына, А. Ю. Нестеренко, В. Г. Чирского, А. Л. Юрченко, без помощи и поддержки которых было бы невозможно создание этой книги.

Глава 1

Из истории криптографии

1.1. Исторические шифры

Термин *криптография*, означающий *тайнопись* (от древне-греческих слов *κρυπτος* — *«скрытый»* и *γραφω* — *«пишу»*) был введен в XVII в. Д. Валлисом (John Wallis, 1616–1703) [128].

Изначально криптография изучала методы *шифрования информации* — обратимого преобразования *открытого* (исходного) *текста* на основе специального алгоритма — *шифра* — в *шифрованный текст*.

Шифр (от французского слова *chiffre* — *«цифра»* и арабского слова *sifr* — *«ноль»*) представляет собой систему преобразования текста, обладающую некоторым секретом (*ключом*) для обеспечения секретности передаваемой информации.

Не стоит путать шифр с *кодированием* — фиксированным преобразованием информации из одного вида в другой, которое используется, как правило, в целях, не связанных с защитой информации от несанкционированного доступа.

Известнейшие с древних времен шифры можно разделить на два основных класса. Это *шифры подстановки* и *шифры перестановки*. *Шифры подстановки* заменяют элементы исходного открытого текста — символы некоторого алфавита, зашифрованным текстом — символами другого алфавита, в соответствии с некоторым правилом; элементами текста могут быть отдельные символы, пары или тройки букв, комбинирование этих случаев и т. д. *Шифры перестановки* сохраняют все символы исходного сообщения, меняя лишь порядок их следования. Другими словами, при использовании подстановочных шифров элементы исходного текста не меняют свою последовательность, но изменяются сами, в то время как при использовании перестановочных шифров элементы исходного текста остаются неизменными, но переставляются в ином, отличном от исходного, порядке.

1.1.1. Простейшие подстановочные шифры (шифры простой замены)

Самыми простыми шифрами подстановки являются *шифры простой замены*, они используют однозначную замену элементов алфавита символами другого алфавита или же символами исходного алфавита по некоторому правилу. К наиболее известным шифрам простой замены принадлежат *диск Энея*, *шифр Цезаря*, *квадрат Полибия*.

Диск Энея — криптографический инструмент для защиты информации, придуманный Энеем Тактиком (Aeneas Tacticus, IV в. до н. э.). Устройство представляло собой диск диаметром 13–15 см и толщиной 1–2 см с проделанными в нем отверстиями, количество которых равнялось числу букв в алфавите. Каждому отверстию ставилась в соответствие конкретная буква. В центре диска находилась катушка с намотанной на нее ниткой.

Механизм шифрования был очень прост. Для того чтобы зашифровать послание, необходимо было поочередно протягивать свободный конец нити через отверстия, обозначающие буквы исходного сообщения. В итоге сам диск с продетой в его отверстия нитью и являлся зашифрованным посланием.

Получатель сообщения последовательно вытягивал нить из каждого отверстия, тем самым получая последовательность букв. Эта последовательность являлась обратной по отношению к исходному сообщению, то есть получатель читал сообщение «наоборот». У данного вида защиты информации был один существенный недостаток: зашифрованное сообщение было доступно к прочтению любому, кто смог завладеть диском. Так как сообщение передавали обычные гонцы, а не воины, Эней предусмотрел возможность быстрого уничтожения передаваемой информации. Для этого было достаточно вытянуть всю нить за один из ее концов, либо сломать диск, просто наступив на него. Обычно он ломался в местах шифрующих отверстий, как следствие продетая в них нить спутывалась и прочесть сообщение было невозможно [57].

Созданный Энеем диск можно считать родоначальником инструментов криптографии. Сходным криптографическим инструментом, в основе действия которого лежит посимвольное шифрование, стала игральная кость. В ней проделывалось 24 отверстия, по шесть на каждой грани (использовалось четыре грани кости из шести). Каждому отверстию ставилась в соответствие определенная буква алфавита. Буквы шли по порядку. Что бы знать, какое отверстие определяет какую букву, запоминалось начало, то есть буква «альфа». Принцип шифрования был полностью аналогичен схеме использования диска Энея: нитка продевалась в отверстия, соответствующие буквам исходного сообщения, в порядке следования его букв. В итоге вокруг кости образовывался клубок ниток. Получателю было необходимо поочередно вытягивать нить из отверстий и выписывать при этом получавшиеся символы.

Квадрат Полибия (*шахматная доска Полибия*) — одна из древнейших систем кодирования, предложенная греческим историком и полководцем Полибием (Polybius, III в. до н. э.) [85].

Хотя изначально квадрат создавался для кодирования на базе греческого алфавита, с его помощью можно успешно шифровать тексты, записанные на любом языке.

Для этого, работая с тем или иным алфавитом, необходимо составить таблицу шифрования с некоторым количеством пронумерованных строк и столбцов, параметры которой зависят от количества букв в используемом алфавите (как правило, нужное число строк и столбцов задается двумя натуральными числами, произведение которых близко к количеству букв заданного алфавита). Таблица заполняется буквами алфавита — по одной в каждую клетку (при нехватке клеток можно вписать в одну из них две буквы, редко употребляющиеся или схожие по употреблению).

Так, современный английский алфавит содержит 26 букв, поэтому таблица шифрования может состоять из 5 строк и 5 столбцов ($25 = 5 \times 5$ — натуральное число, близкое к числу 26). Поскольку одной ячейки в этом случае не хватает, буквы *I* и *J* помещаются в одну ячейку, то есть буква *J* отождествляется с буквой *I*. Таким образом, таблица принимает следующий вид.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Для русского алфавита построим квадрат, содержащий 6 строк и 6 столбцов ($36 = 6 \cdot 6$ — натуральное число, близкое к числу 33). После его заполнения получим следующую таблицу.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я			

Впрочем, возможны и другие варианты составления таблицы шифрования для русского алфавита. Например, объединение букв Е и Ё, И и Й, Ъ и Ь позволяет использовать таблицу, состоящую из пяти строк и шести столбцов. Попробуйте построить ее самостоятельно. Можно использовать и квадрат 5×5, исключив из рассмотрения буквы Ъ и Ё и поместив в одну клетку буквы Е-Э, И-Й, Ж-З, Р-С, Ф-Х, Ш-Щ.

В результате построения таблицы шифрования каждой букве заданного алфавита соответствует пара чисел. Заменяя в процессе шифрования каждый символ открытого текста соответствующей ему числовой парой, мы получим шифротекст, представляющий собой некоторую последовательность таких пар. Для расшифровки текста достаточно по каждой паре чисел восстановить букву, стоящую на пересечении соответствующих строки и столбца.

Пример 1.1.1 Зашифруем известное послание Цезаря «Veni, vidi, vici», в переводе на русский означающее «Пришел, увидел, победил». Шифруя оригинальное сообщение «VENI VIDI VICI», получим, пользуясь таблицей шифрования английского алфавита, набор «(5, 1)(1, 5)(3, 3)(2, 4) (5,1)(2, 4)(1, 4)(2, 4) (5, 1) (2, 4)(1, 3)(2, 4)». Для расшифровки полученного шифротекста восстановим первую букву V, найдя ее на пересечении пятой строки и первого столбца, вторую букву Е — найдя ее на пересечении первой строки и пятого столбца, и т. д. Шифруя русский перевод «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ», пользуясь таблицей шифрования русского алфавита, получим набор «(3, 5)(3, 6)(2, 4)(5, 2)(2,1)(3, 1)(4, 3)(1, 3)(2, 4)(1, 5)(1, 6)(3, 1) (3, 5)(3, 4)(1, 2)(1, 6)(1,5)(2, 4)(3, 1)». Для расшифровки полученного шифротекста восстановим первую букву П, найдя ее на пересечении третьей строки и пятого столбца, вторую букву Р, найдя ее на пересечении третьей строки и шестого столбца, и т. д. □

Шифр Атбаш был изобретен древними иудеями для иврита и использовался на протяжении многих столетий (около 500 г. до н. э. – около 1300 г. н. э.).

Суть шифра очень проста: шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю и т. д. В частности, первая буква иврита «алеф» заменяется на последнюю «тав», а вторая буква «бет» переходит в предпоследнюю «шин». Это и дало название шифру: на иврите слово «атбаш» составлено из букв «алеф», «тав», «бет» и «шин». Другими словами, для алфавита длины N шифр Атбаш состоит в замене символа, имеющего i-ый номер в алфавите, на символ, имеющий в этом же алфавите номер $j = N - i + 1$.

Для английского алфавита таблица шифрования выглядит следующим образом.

Исходный алфавит	A	B	C	D	E	F	G	H	I	J	K	L	M
Алфавит замены	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Исходный алфавит	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Алфавит замены	M	L	K	J	I	H	G	F	E	D	C	B	A

Для русского алфавита шифр Атбаш будет выглядеть следующим образом.

Исходный алфавит	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Алфавит замены	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х
Исходный алфавит	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Алфавит замены	Ф	У	Т	С	Р	П	О	Н	М	Л	К
Исходный алфавит	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Алфавит замены	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	А

Для расшифровки заданного шифротекста достаточно воспользоваться обратным преобразованием: символ шифротекста, имеющий j-ый номер в алфавите, заменяется на символ, имеющий в этом же алфавите номер $i = N - j + 1$. Другими словами, для получения исходного открытого текста достаточно еще раз применить шифр Атбащ — теперь для имеющегося шифрованного сообщения.

Пример 1.1.2 Зашифруем с помощью шифра Атбаш фразу «Обучая, ты учишься сам». Выписав открытый текст в виде «ОБУЧАЯ ТЫ УЧИШЬСЯ САМ», проведем замену каждого символа в соответствии с представленной выше таблицей шифрования и получим шифрованное сообщение «РЮЛЗЯА МД ЛЗЦЖГНЯ НЯТ». Для его дешифровки еще раз воспользуемся заданным криптографическим алгоритмом: нетрудно убедиться, что повторное шифрование текста «РЮЛИЯА МД ЛЗЦЖГНЯ НЯТ» приводит к сообщению «ОБУЧАЯ ТЫ УЧИШЬСЯ САМ». □

Шифр Цезаря (*шифр сдвига*, *код Цезаря*, *сдвиг Цезаря*) — один из самых простых и наиболее широко известных методов шифрования. Шифр назван в честь римского императора Гая Юлия Цезаря (Gaius Iulius Caesar, 100–44 до н. э.), использовавшего его для защиты военных сообщений.

Он представляет собой шифр простой замены, в котором каждый символ открытого текста заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в том же алфавите. Сам Цезарь использовал шифр со сдвигом 3: при таком шифровании буква A переходит в букву D, буква B — в букву E, ..., буква X — в букву A, буква Y — в букву B, и, наконец, буква Z — в букву C.

Для английского алфавита таблица шифрования выглядит в случае шифра Цезаря со сдвигом 3 следующим образом.

Исходный алфавит	A	B	C	D	E	F	G	H	I	J	K	L	M
Алфавит замены	D	E	F	G	H	I	J	K	L	M	N	O	P
Исходный алфавит	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Алфавит замены	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Для русского алфавита шифр Цезаря со сдвигом 3 принимает вид.

Исходный алфавит	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Алфавит замены	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
Исходный алфавит	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Алфавит замены	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Исходный алфавит	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Алфавит замены	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Внучатый племянник Цезаря Октавиан Август (Octavianus Augustus, 63 до н. э. — 14 н. э.) также использовал этот шифр, но со сдвигом вправо на один символ.

Говоря математическим языком, шифр Цезаря со сдвигом k для алфавита длины N состоит в замене символа, имеющего i-ый номер в алфавите, на символ, имеющий в этом же алфавите номер $j \equiv i + k \pmod{N}$. Для расшифровки шифротекста достаточно применить к нему обратное преобразование, заключающееся в замене символа, имеющего j-ый номер в алфавите, на символ, имеющий в этом же алфавите номер $i \equiv j - k \pmod{N}$.

Пример 1.1.3 При использовании шифра Цезаря со сдвигом 3 уже рассмотренное нами послание «VENI VIDI VICI» выглядит в зашифрованном виде так: «YHQL YLGL YLFL». Русскому открытому тексту «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ» соответствует в этом случае шифрованное сообщение

«ТУЛЫЗО ЦЕЛЖЗО ТСДЗЖЛО». Для расшифровки полученных шифротекстов достаточно произвести циклический сдвиг каждого из их элементов на 3 символа влево в соответствующем алфавите. Как использовать для этого уже имеющиеся в нашем распоряжении таблицы? □

Существует множество других интересных «исторических» и «литературных» примеров шифров простой замены.

Так, *тарабарская грамота* (криптографический алгоритм, в котором согласные буквы взаимозаменяются по схеме Б ↔ Щ, В ↔ Ш, Г ↔ Ч, Д ↔ Ц, Ж ↔ Х, З ↔ Ф, К ↔ Т, Л ↔ С, М ↔ Р, Н ↔ П, а гласные остаются без изменения) представляет собой первое применение тайнописи в России и ведет свою историю с XIII в. К XVII в. относится тайнопись *уголки* — пример алфавита, специально придуманного для передачи секретных сообщений: обычные буквы заменяются здесь квадратами или полученными из них удалением ребер «скобами» и «уголками» — обычными или содержащими от одной до трех внутренних точек.

Наиболее известные упоминания шифров простой замены в классической литературе — рассказы «Пляшущие человечки» Артура Конан Дойла и «Золотой жук» Эдгара Алана По — на конкретных примерах демонстрируют основной недостаток этих криптографических систем: возможность несанкционированного раскрытия шифра на основе анализа шифротекста с использованием таблицы частот встречаемости букв того или иного алфавита.

1.1.2. Полиалфавитные подстановочные шифры

Для затруднения частотного анализа вместо шифров простой замены (называемых также *моноалфавитными*, поскольку каждый символ открытого текста переходит в некоторый, фиксированный при данном ключе, символ того же алфавита) с XV в. стали использовать более сложные подстановочные шифры, в том числе *однозвучные*, в целом похожие на моноалфавитные за исключением того, что символам открытого текста с большей частотой ставится в соответствие несколько возможных символов-заменителей, что «сглаживает» частоту употребления символов в шифротексте; *полиграммные*, заменяющие не один символ открытого текста, а два, три или целую группу, и *полиалфавитные*, состоящие в циклическом применении нескольких моноалфавитных шифров к определенному числу букв шифруемого текста.

Первое точное документированное описание полиалфавитного шифра было дано итальянским ученым Леоном Баттиста Альберти (Leone Battista Alberti, 1404–1472) в 1467 г. Для переключения между алфавитами Альберти использовал шифровальный диск, имеющий сегодня название *диск Альберти*.

Следующей попыткой построения полиалфавитного шифра является *шифр Тритемиуса* — система шифрования, разработанная Иоганном Тритемием (Iohannes Trithemius, 1462–1516) — автором первой печатной книги по криптографии «Полиграфия»

Шифр Тритемиуса представляет собой усовершенствованный шифр Цезаря. По алгоритму шифрования каждый символ сообщения смещается на символ, отстающий от данного на некоторый шаг. Здесь шаг смещения является переменным, то есть зависящим от каких-либо дополнительных факторов.

Простейший способ задания закона смещения — использование некоторого ключевого слова. Для шифрования в алфавите длины N ключевое слово подписывают, с нужным числом повторений, под текстом исходного сообщения; номер очередной буквы шифруемого сообщения складывают с номером соответствующей буквы ключа по модулю N; заменяя числа полученной последовательности соответствующими буквами, получают искомый шифротекст. Шифр Цезаря получается при таком подходе, если в качестве ключа выбрано слово, состоящее из одной буквы. Так, выбор однобуквенного слова «В» приводит к классическому шифру Цезаря со сдвигом 3.

Говоря математическим языком, символ, стоящий на i-ой позиции открытого сообщения, заменяется при осуществлении данного алгоритма по закону $l_i \equiv m_i + k_i \pmod N$, где m_i — числовой эквивалент i-го символа открытого сообщения, k_i — числовой эквивалент i-го символа ключа, получающегося последовательным повторением заданного ключевого слова, и l_i — числовой эквивалент i-го символа шифротекста. Для дешифрования достаточно провести обратную операцию: $m_i \equiv l_i - k_i \pmod N$, то есть для расшифровки шифротекста из номера очередной буквы зашифрованного сообщения вычитают номер соответствующей буквы ключа, осуществляя эту операцию по модулю N.

Пример 1.1.4 Попробуем использовать шифр Тритемиуса для шифровки сообщения «ОПЕРАЦИЯ НАЧИНАЕТСЯ», используя ключевое слово «МОСКВА». В качестве числовых эквивалентов букв русского алфавита возьмем числа от 0 до 32. Осуществим описанную выше схему шифрования: выпишем ключевое слово под текстом исходного сообщения, повторив его нужное число раз (в нашем случае ровно три раза); выписав числовые эквиваленты букв исходного сообщения и букв ключа, сложим соответствующие значения; заменим полученные числа их остатками при делении на 33 (в нашем случае пришлось заменить только одно число, 47); заменим числа получившейся последовательности соответству-

ющими буквами и получим искомый шифротекст. Оформим результаты работы алгоритма в виде таблицы.

О	П	Е	Р	А	Ц	И	Я	Н	А	Ч	И	Н	А	Е	Т	С	Я
15	16	5	17	0	23	9	32	14	0	24	9	14	0	5	19	18	32
М	О	С	К	В	А	М	О	С	К	В	А	М	О	С	К	В	А
13	15	18	11	2	0	13	15	18	11	2	0	13	15	18	11	2	0
28	31	23	28	2	23	22	47	32	11	26	9	27	15	23	30	20	32
Ы	Ю	Ц	Ы	В	Ц	Х	Н	Я	К	Щ	И	Ъ	О	Ц	Э	У	Я

Таким образом, искомое шифрованное сообщение имеет вид «ЫЮЦЫВЦХНЯКЩИЬОЦЭУЯ». Для его расшифровки достаточно использовать тот же алгоритм, заменив сложение числовых эквивалентов символов открытого текста и символов ключевого слова по модулю 33 соответствующим вычитанием. Проведите эту операцию самостоятельно. □

Таблица Виженера — еще один метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Шифр Виженера изобретался многократно. Впервые этот метод описал итальянский ученый Джован Баттиста Беллазо (Giovan Battista Bellaso, 1505 – вторая половина XVI в.) в 1553 г., однако с XIX в. этот криптографический алгоритм носит имя Блеза де Виженера (Blaise de Vigenère, 1523–1596), французского дипломата, криптографа и алхимика.

Для шифрования по таблице Виженера необходимо прежде всего построить соответствующую таблицу (см. главу 10, табл. 10.3, 10.4), которая устроена следующим образом: в первой строке выписан весь алфавит; в каждой следующей строке осуществлен циклический сдвиг на одну букву; в итоге получен квадрат, число строк и столбцов которого совпадает с количеством символов в заданном алфавите. Чтобы зашифровать то или иное сообщение, выберем ключевое слово и выпишем его с нужным чис лом повторений под шифруемым сообщением. Для замены того или иного символа открытого текста рассмотрим столбец таблицы, начинающийся с этого символа, и строку таблицы, начинающуюся с соответствующего символа ключевого слова; используем для замены символ, стоящий на пересечении выделенных столбца и строки. Таким образом, замена по таблице Виженера является простой заменой с циклическим изменением алфавита, то есть мы получаем полиалфавитную подстановку, число используемых алфавитов которой определяется числом букв в ключевом слове.

Шифр Виженера легко выражается математически. Если заменить буквы на их номера в алфавите длины N, то операции шифрования и дешифрования будут операциями сложения и вычитания по модулю N: символ, стоящий на i-ой позиции открытого сообщения, заменяется при осуществлении данного алгоритма по закону $l_i \equiv m_i + k_i \pmod N$, где m_i — числовой эквивалент i-го символа открытого сообщения, k_i — числовой эквивалент i-го символа ключа, получающегося последовательным повторением заданного ключевого слова, и l_i — числовой эквивалент i-го символа шифротекста. (Для дешифрования достаточно провести обратную операцию: $m_i \equiv l_i - k_i \pmod N$.)

Формально, если f_i — описанная выше подстановка, то ключ системы Виженера длины k можно интерпретировать как последовательность $(f_0, f_1, \ldots, f_{k-1})$ таких подстановок и утверждать, что функция Виженера преобразует открытый текст, выраженный последовательностью символов $\{x_0, x_1, \ldots, x_{n-1}\}$ в шифротекст $\{y_0, y_1, \ldots, y_{n-1}\}$ согласно правилу

$$\{y_0, y_1, \ldots, y_{n-1}\} = \{f_0(x_0), f_1(x_1), \ldots, f_{n-1}(x_{n-1})\}, \quad \text{где } f_i = f_{i \bmod k}.$$

Пример 1.1.5 Зашифруем с помощью таблицы Виженера сообщение «ПРОСТЕЙШИЕ КРИПТОСИСТЕМЫ», используя ключевое слово «КНИГА».

Проведем подготовительную работу, выделив из полной таблицы Виженера для русского алфавита (31 буква, без Ё и Ъ) первую строку и добавив к ней те строки, первые символы которых соответствуют буквам ключа шифрования, разместив их в порядке следования этих букв в ключе. Полученная рабочая матрица для ключа «КНИГА» имеет следующий вид.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я

□

Для шифрования сообщения «ПРОСТЕЙШИЕ КРИПТОСИСТЕМЫ» выпишем его в строку и под ним запишем ключевое слово «КНИГА», циклически повторяя его нужное число раз. Полученный результат представлен в таблице.

П	Р	О	С	Т	Е	Й	Ш	И	Е	К	Р	И	П	Т	О	С	И	С	Т	Е	М	Ы
К	Н	И	Г	А	К	Н	И	Г	А	К	Н	И	Г	А	К	Н	И	Г	А	К	Н	И

Осуществим непосредственное шифрование: взяв первую букву шифруемого текста П и соответствующую ей букву ключа К, выберем в рабочей таблице по букве шифруемого текста П столбец, а по букве ключа К — строку. Буква на пересечении «П»-столбца и «К»-строки является искомым символом шифротекста. В нашем случае буква П исходного сообщения преобразуется в букву Щ шифротекста. Продолжая работу алгоритма, находим искомый шифротекст «ЩЮЦФТПЦБЛЕ ФЮРТТШЯРФТПЩГ». Для расшифровки данного сообщения достаточно, зная ключевое слово «КНИГА», проделать обратное преобразование: так, взяв букву ключа К, найдем в соответствующей строке рабочей таблицы первую букву шифротекста Ъ и выделим отвечающий ей столбец; символ П, лежащий на пересечении этого столбца с первой строкой рабочей таблицы, является искомым символом открытого текста.

Полиалфавитным шифром, который можно рассматривать как дальнейшее усовершенствование шифра Цезаря, является появившийся в XVIII в. *шифр по книге*, а основанный на той же идее *шифровальный блокнот* представляет собой пример нераскрываемого шифра [78].

1.1.3. Простейшие шифры перестановки

Древнейшим шифром перестановки считается *Скитала* (*шифр Древней Спарты*).

Скитала (от греческого $\sigma\kappa\upsilon\tau\alpha\lambda\eta$- *«жезл»*) представляла собой прибор, состоящий из цилиндра и узкой полоски пергамента или папируса, обматывавшейся вокруг него по спирали, на которой писалось сообщение. Античные греки, в частности спартанцы, использовали этот шифр для связи во время военных кампаний.

Обратимся к описанию ее работы, данному Плутархом (Plutarchus, около 50 – около 120) [84].

Отправляя к месту службы начальника флота или сухопутного войска, эфоры берут две круглые палки совершенно одинаковой длины и толщины. Одну они оставляют себе, другую передают отъезжающему. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую, вроде ремня, полосу папируса, наматывают ее на свою скиталу, не оставляя на ней ни одного промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, они пишут на нем то, что нужно, а написав, снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, но разбросаны в беспорядке, прочитать написанное он может, только взяв свою скиталу и намотав на нее вырезанную полосу, располагая ее извивы в прежнем порядке,

чтобы, водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение. Полоса папируса называется, как и деревянная палка, «скиталой», подобно тому как измеряемый предмет называется по мере.

Считают, что первым придумал способ расшифровать сообщение, закодированное с помощью скиталы, Аристотель (Aristotle, 384–322 до н. э.). Метод состоит в том, что, не зная точного диаметра скиталы, можно использовать конус, имеющий переменный диаметр, и перемещать пергамент с сообщением по его длине до тех пор, пока текст не начнет читаться — таким образом находится искомый диаметр скиталы.

Шифрующие таблицы, которые появились в эпоху Возрождения, в сущности задают правила перестановки букв в сообщении. Простейшим табличным шифром перестановки является *простая перестановка*, где ключом служит размер таблицы.

Пример 1.1.6 Сообщение «ПРОСТЕЙШИЕ КРИПТОСИСТЕМЫ» (учтем пробел, так как иначе количество знаков — простое число), внесенное в таблицу, содержащую 4 строки и пять столбцов, по столбцам, будет выглядеть следующим образом.

П	Т	И	Р	О	Т
Р	Е	Е	И	С	Е
О	Й		П	И	М
С	Ш	К	Т	С	Ы

Выписав элементы построенной таблицы по строкам, мы получим зашифрованное сообщение «ПТИРОТРЕЕИСЕОЙ ПИМСШКТСЫ». Для его расшифрования достаточно проделать обратное преобразование: внеся символы шифротекста в таблицу 4×5 по строкам, прочитаем исходное сообщение по столбцам. □

Для успешного пользования шифром получатель и отправитель шифротекста должны заранее оговорить ключ — размер таблицы, а также уточнить «маршруты» ее заполнения символами открытого текста и дальнейшего считывания символов шифрованного сообщения. В случае нестандартных маршрутов, усложняющих алгоритм, соответствующие табличные шифры называются *маршрутной транспозицией*.

Для дальнейшего усложнения данного метода шифрования можно использовать ключевое слово: при составлении шифротекста столбцы

заполненной символами открытого сообщения таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Обычно такой табличный шифр называется *постолбцовой транспозицией* [78].

Пример 1.1.7 Используем для шифрования сообщения «ПРОСТЕЙШИЕ КРИПТОСИСТЕМЫ» постолбцовую транспозицию. Возьмем в качестве ключа слово «ЛАСТИК». Заполнив таблицу 4 × 5 символами открытого текста по столбцам, запишем ключевое слово над построенной таблицей и пронумеруем его буквы.

Л	А	С	Т	И	К
4	1	5	6	2	3
П	Т	И	Р	О	Т
Р	Е	Е	И	С	Е
О	Й		П	И	М
С	Ш	К	Т	С	Ы

Переставим столбцы полученной таблицы так, чтобы буквы ключевого слова расположились в порядке их следования в алфавите.

А	И	К	Л	С	Т
1	2	3	4	5	6
Т	О	Т	П	И	Р
Е	С	Е	Р	Е	И
Й	И	М	О		П
Ш	С	Ы	С	К	Т

Выписав элементы последней таблицы по строкам, придем к зашифрованному сообщению «ТОТПИРЕСЕРЕИЙИМО ПШСЫСКТ». Схема дешифрования полученного шифротекста очевидна. □

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием *двойная перестановка*. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки.

Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

В 1550 г. итальянский ученый Джероламо Кардано (Girolamo Cardano, 1501–1576) предложил простую решетку для шифрования сообщений. *Решетка Кардано* представляет собой прямоугольную (возможно, квадратную) таблицу-карточку, часть ячеек которой вырезана таким образом, чтобы они не накладывались друг на друга при размещении решетки в возможных четырех позициях — лицом вверх, лицом вниз, вертикально и в перевернутом положении.

Механизм использования решетки предельно прост. Пользователь помещает ее на лист бумаги и пишет сообщение в прямоугольных отверстиях, размещая в каждом из них отдельный символ, слог или целое слово. (Возможность использования решетки в четырех положениях вчетверо увеличивает число допустимых размещений сетки.) Затем решетка убирается и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью сообщения, замаскированного под обычное послание, не похожее на шифрованное. Такое замаскированное сообщение может служить примером использования *стеганографии* — науки о скрытой передаче информации путем сохранения в тайне самого факта передачи.

При использовании решетки Кардано как криптографического инструмента ситуация меняется: сообщение, получаемое размещением в отверстиях решетки отдельных символов (как правило, букв или цифр) при использовании всех четырех ее допустимых положений, представляет собой шифротекст, выполненный в форме прямоугольной таблицы.

В каждом из описанных случаев для восстановления исходного сообщения получатель должен иметь такую же решетку.

Пример 1.1.8 Используем решетку Кардано для шифровки сообщения «*Что знают двое — знают все*». При шифровании не будем учитывать пробелы, чтобы не указывать на начало и конец слов, и откажемся от знаков препинания. Таким образом, исходное сообщение «ЧТОЗНАЮТДВОЕЗНАЮТВСЕ» содержит 20 букв.

Подберем для него решетку подходящего размера, учитывая, что любая шифровальная решетка должна содержать четное число строк и столбцов, поскольку при ее построении необходимо использовать симметрию относительно вертикальной и горизонтальной осей.

В нашем случае можно использовать таблицу размера 2×10. Для получения из нее шифровальной решетки необходимо сделать 5 отверстий так, чтобы при переходе в любое из допустимых положений эти отверстия не накладывались друг на друга.

Разобьем таблицу на четыре части, переходящие друг в друга при смене допустимых положений, получив таблицы размера 1×5. Пронумеруем элементы одной из частей (например, верхней левой), числами 1, 2, 3, 4, 5. Посмотрим, какие позиции может занимать каждая из пронумерованных клеток при переходе в одно из допустимых положений. Так, клетка 1 будет переходить в клетки $1a$, $1b$, $1c$; аналогичные преобразования имеют место и для клеток 2, 3, 4, 5. Результаты нашего исследования представлены в таблице.

1	2	3	4	5	5a	4a	3a	2a	1a
1b	2b	3b	4b	5b	5c	4c	3c	2c	1c

Для получения шифровальной решетки мы можем взять любую комбинацию клеток без повторяющихся номеров. Например, можно проделать отверстия в клетках 1, $2a$, $3b$, $4c$, 5.

X				X				X	
		X				X			

Итак, решетка Кардано построена. Перейдем к шифрованию нашего сообщения. После заполнения отверстий решетки, находящейся в исходном положении, первыми пятью буквами открытого текста получим следующую картину.

Ч				Т				О	
		З				Н			

Заполнение отверстий решетки, находящейся во втором положении (после отражения относительно вертикальной оси симметрии) даст нам такое расположение символов.

	А				Ю				Т
			Д				В		

Третье положение (после отражения решетки относительно горизонтальной оси симметрии) приведет к следующей ситуации.

			О				Е		
	З				Н				А

Наконец, в четвертом положении (после отражения решетки относительно вертикальной оси симметрии) мы придем к такой картине.

		Ю				Т			
В				С				Е	

В результате проведенных операций мы получим следующий результат.

Ч	А	Ю	О	Т	Ю	Т	Е	О	Т
В	З	З	Д	С	Н	Н	В	Е	А

□

Замечание. *Для шифрования нашего сообщения можно было использовать и решетку* 6×4. *Если при шифровании сообщения остались свободные клетки, в них обычно вписываются буквы в алфавитном порядке*: *А*, *Б*, *В*, *Г и т. д.*

Магические квадраты — квадратные $k\times k$ таблицы со вписанными в их клетки последовательными натуральными числами от 1 до k^2, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число — в свое время широко применялись для вписывания шифруемого текста по приведенной в них нумерации. При последующем выписывании содержимого таблицы по строкам получалась шифровка перестановкой букв.

На первый взгляд кажется, что этот метод перестановочного шифрования совсем неэффективен, поскольку магических квадратов очень мало. Тем не менее это не так: число магических квадратов очень быстро возрастает с увеличением их размеров. Так, существует лишь один магический квадрат размера 3×3. Магических квадратов размера 4×4 насчитывается уже 880, а число магических квадратов размера 5×5 около 250 000. Таким образом, магические квадраты больших размеров были хорошей основой для надежной системы шифрования «докомпьютерной эры», поскольку ручной перебор всех вариантов ключа для этого шифра был немыслим.

Пример 1.1.9 Используем для шифрования сообщения «*Д. Бонд в Москве*» *квадрат Дюрера* — знаменитый магический квадрат размера 4×4, изображенный на гравюре Альбрехта Дюрера (Albrecht Dürer, 1471–1528) «Меланхолия I» и считающийся самым ранним в европейском искусстве.

16	3	2	13
5	10	11	8
9	6	7	12
4	**15**	**14**	1

Два средних числа в нижнем ряду указывают дату создания гравюры — 1514 г.

Последовательно вписывая символы сообщения «ДБОНДВМОСКВЕ» в клетки квадрата с номерами 1, 2, 3, ..., 12 и заполняя оставшиеся клетки буквами А, Б, В, Г, мы получим следующую таблицу.

Г	О	Б	А
Д	К	В	О
С	В	М	Е
Н	В	Б	Д

Выписывая теперь содержимое таблицы по строкам, перейдем к шифротексту «ГОБАДКВОСВМЕНВБД». Для его расшифровки нужно восстановить последнюю таблицу и, проставив номера клеток в соответствии со структурой квадрата Дюрера, получить оригинальное сообщение, выписывая символы в порядке возрастания присвоенных им номеров. □

Упражнения

(1) Зашифруйте с помощью квадрата Полибия следующие латинские фразы:

a) «Ab aqua silente cav» («Остерегайся тихой воды»);

b) «Abeunt studia in mores» («Занятия накладывают отпечаток на характер»);

c) «Actum ne agas» («С чем покончено, к тому не возвращайся»);

d) «Alter ego» («Второе Я»);

e) «Alma mater» («Мать-кормилица»);

f) «Amicus verus — rara avis» («Верный друг — редкая птица»);

g) «Amor vincit omnia» («Любовь побеждает все»);

h) «Bis dat, qui cito dat» («Вдвойне дает, кто дает скоро»);

i) «Caesarem decet stantem mori» («Цезарю подобает умереть стоя»);

j) «Carmina morte carent» («Стихи лишены смерти»).

Проверьте результат, произведя расшифровку полученных шифротекстов.

(2) Зашифруйте с помощью квадрата Полибия размера 6 × 6 русские переводы латинских фраз, использованных в предыдущем упражнении; постройте и используйте для этой цели квадрат 5 × 5, исключив из рассмотрения буквы Ъ и Ё и поместив в одну клетку буквы Е-Э, И-Й, Ж-З, Р-С, Ф-Х, Ш-Щ; постройте и используйте для этой цели таблицу, состоящую из пяти строк и шести столбцов, полученную объединением букв Е и Ё, И и Й, Ъ и Ь. Проверьте результат, произведя расшифровку полученных шифротекстов.

③ Аналогом квадрата Полибия является *тюремная азбука*, позволявшая перестукиваться заключенным разных камер. Составьте шифрующую таблицу 6×5 символов русского алфавита без букв Ё, Й и Ъ, в которой каждой букве соответствует пара чисел — номер соответствующих строки и столбца. Зашифруйте сообщение «МЫ ГОТОВИМ ПОБЕГ».

④ Зашифруйте представленные выше латинские фразы шифром Атбаш. Зашифруйте этим же шифром их русские переводы. Проверьте результат, произведя расшифровку полученных шифротекстов.

⑤ Зашифруйте представленные выше латинские фразы шифром Цезаря со сдвигом 3. Зашифруйте этим же шифром их русские переводы. Проверьте результат, произведя расшифровку полученных шифротекстов.

⑥ Составьте для шифра Августа шифрующие таблицы для латинского и русского алфавитов. Зашифруйте представленные выше латинские фразы шифром Августа. Зашифруйте этим же шифром их русские переводы. Проверьте результат, произведя расшифровку полученных шифротекстов.

⑦ Зашифруйте представленные выше латинские фразы шифром Цезаря со сдвигом $2k$, где k — ваш номер в списке группы. Зашифруйте этим же шифром их русские переводы. Проверьте результат, произведя расшифровку полученных шифротекстов.

⑧ Пользуясь тарабарской грамотой (согласные переходят друг в друга по схеме Б ↔ Щ, В ↔ Ш, Г ↔ Ч, Д ↔ Ц, Ж ↔ Х, З ↔ Ф, К ↔ Т, Л ↔ С, М ↔ Р, Н ↔ П; гласные остаются на месте), зашифруйте сообщение «ЧИСЛА КРАСИВЫ». Проверьте результат, произведя расшифровку полученного шифротекста.

⑨ Используя шифр Тритемиуса и ключевое слово «ОБРАЗОВАНИЕ», зашифруйте фразу «НАУКА СРЕДНЕВЕКОВЬЯ» и любую придуманную вами фразу. Проверьте результаты, осуществив расшифровку полученных шифротекстов.

⑩ Используя шифр Тритемиуса и ключевое слово «НАУКА», зашифруйте фразу «ДЕТИ КАПИТАНА ГРАНТА» и любую придуманную вами фразу. Проверьте результат, осуществив расшифровку полученного шифротекста.

⑪ Используя таблицу Виженера и ключевое слово «ЦВЕТОК», зашифруйте фразу «КОНЕЙ НА ПЕРЕПРАВЕ НЕ МЕНЯЮТ» и любую придуманную вами фразу. Проверьте результат, осуществив расшифровку полученного шифротекста.

⑫ Используя таблицу Виженера и ключевое слово «ШКОЛА», зашифруйте фразу «ПЕРВЫЙ РАЗ В ПЕРВЫЙ КЛАСС» и любую придуманную вами фразу. Проверьте результат, осуществив расшифровку полученного шифротекста.

⑬ Зашифруйте фразу «КОСИНУС НУЛЯ РАВЕН ЕДИНИЦЕ» с помощью постолбцовой транспозиции, используя таблицу подходящего размера и ключ «ПАРИЖ». Приведите несколько других примеров использования постолбцовой транспозиции. Проверьте результаты, расшифровав полученные шифротексты.

⑭ Приведите, если это возможно, примеры решетки Кардано размера 6×4, 6×6; 6×9; 6×8; 5×5. Для каждой из построенных решеток придумайте сообщение, которое удобно зашифровать с ее помощью; осуществите шифрование; проверьте результат, расшифровав полученные шифротексты.

⑮ Зашифруйте сообщение, используя решетку Кардано:

a) «КРИПТОГРАФИЯ — НАУКА О ШИФРАХ»;

b) «СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»;

c) «ПРИКЛАДНЫЕ ВОПРОСЫ МАТЕМАТИКИ».

d) «ШИФР ЦЕЗАРЯ НЕСЛОЖЕН».

⑯ Для шифрования текста шифром *поворотная решетка* изготовьте трафарет — бумажный квадрат размером 4×4 клеток. Вырезанные клетки выберите так, чтобы при наложении трафарета на лист бумаги того же размера четырьмя возможными способами — при повороте квадрата на 90 градусов относительно его центра симметрии — каждая клетка листа «открывалась» ровно один раз. Первые 4 буквы текста сообщения впишите в прорези трафарета (по одной в каждую), потом поверните трафарет на 90 градусов и впишите следующие 4 буквы. Повторите процедуру. Зашифруйте с помощью построенной решетки сообщение «ЯВКА ПРОВАЛЕНА. ЖАН.» Придумайте и зашифруйте с помощью имеющегося трафарета три других сообщения.

⑰ Изготовьте трафарет для поворотной решетки размером 6×6 клеток, должным образом вырезав из бумажного квадрата 9 клеток; зашифруйте с помощью полученного трафарета три подходящих сообщения.

⑱ Для использования шифра *прямоугольная решетка* изготовьте из бумажного прямоугольника трафарет размером 6×10 клеток. Вырезанные клетки выберете так, чтобы при наложении трафарета на лист бумаги того же размера четырьмя возможными способами каждая клетка листа «открывалась» ровно один раз. Зашифруйте с помощью построенной решетки по образцу примера 1.1.8 сообщение «ТЕОРЕМА ПИФАГОРА — ВАЖНЕЙШЕЕ УТВЕРЖДЕНИЕ ЕВКЛИДОВОЙ ГЕОМЕТРИИ». Придумайте и зашифруйте с помощью имеющегося трафарета три других сообщения.

⑲ Изготовьте трафарет для прямоугольной решетки размером 8 × 12 клеток, должным образом вырезав из бумажного прямоугольника 24 клетки; зашифруйте с помощью полученного трафарета три подходящих сообщения.

⑳ Клетки квадрата 4×4 пронумеровали так, что клетка в правом нижнем углу получила номер 1, а все остальные получили разные номера от 2 до 16 таким образом, что суммы номеров клеток каждой строки, каждого столбца, а также каждой из двух диагоналей квадрата оказались одинаковы. Убедитесь в том, что приведенные ниже квадраты 4 × 4 с единицей в правом нижнем углу являются магическими.

a)

4	10	7	13
5	15	2	12
9	3	14	8
16	6	11	1

c)

12	2	5	15
7	13	10	4
9	3	8	14
6	16	11	1

b)

10	5	11	8
6	9	7	12
3	4	14	13
15	16	2	1

d)

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Зашифруйте с помощью каждого из указанных квадратов сообщение «ДВА САПОГА — ПАРА». Проверьте результат, расшифровав полученные шифротексты.

㉑ Зашифруйте свое имя, фамилию и отчество, используя один из шифров подстановки и один из шифров перестановки.

Задачи

1 Осуществите шифрование сообщения «ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ», пользуясь шифром, описанным в рассказе А. Конан Дойла «Пляшущие человечки». Зашифруйте этим шифром придуманную вами фразу. В случае нехватки информации достройте имеющуюся таблицу подстановки.

2 Осуществите шифрование сообщения «НЕ СТРЕЛЯЙТЕ В БЕЛЫХ ЛЕБЕДЕЙ», пользуясь шифром, описанным в рассказе Э. По «Золотой жук». Зашифруйте этим шифром придуманную вами фразу. В случае нехватки информации достройте имеющуюся таблицу подстановки.

3 Осуществите шифрование сообщения «ВСТРЕЧА ОТМЕНЯЕТСЯ», пользуясь шифром, описанным в романе Ж. Верна «Дети капитана Гранта». Зашифруйте этим шифром придуманную вами фразу. В случае нехватки информации достройте имеющуюся таблицу подстановки.

4 Для шифрования по квадрату Полибия договоримся заменять каждую букву открытого текста буквой, расположенной непосредственно под ней в том же столбце квадрата; нижнюю букву столбца заменяем верхней из того же столбца. Зашифруйте с помощью этого метода сообщение «НЕЛЬЗЯ ОБЪЯТЬ НЕОБЪЯТНОГО», используя один из вариантов квадрата Полибия для русского алфавита.

5 Зашифруйте с помощью метода, описанного в предыдущей задаче, сообщение «SOMETEXT», пользуясь квадратом Полибия для английского алфавита. Проверьте полученные результаты.

6 Еще один вариант шифрования с помощью квадрата Полибия состоит в следующем: шифротекст, полученный заменой букв сообщения на двузначные числа, соответствующие их порядковому номеру в алфавите, выписывается в строку без разбиения на пары, полученная последовательность цифр сдвигается циклически влево на один шаг (или любое другое нечетное количество шагов), вновь разбивается в группы по два и по таблице заменяется на окончательный шифротекст. Зашифруйте с помощью этого метода сообщение «НЕЛЬЗЯ ОБЪЯТЬ НЕОБЪЯТНОГО». Придумайте и зашифруйте еще две русские фразы. Проверьте полученные результаты.

7 Зашифруйте с помощью метода, описанного в предыдущей задаче, сообщение «SOMETEXT». Придумайте и зашифруйте еще две английские фразы. Проверьте полученные результаты.

8 При использовании квадрата Полибия возможно использование ключевого слова. Именно, сначала в квадрат вписывается ключевое слово, а затем в оставшиеся клетки в алфавитном порядке выписываются буквы алфавита, отсутствующие в ключе. Приведите пример шифрования одной русской и одной английской фразы с помощью описанного метода.

9 *Шифр Плейфера* использует построенную с помощью ключевого слова (см. предыдущую задачу) матрицу Полибия (квадрат 5×5 для английского алфавита, таблицу 4×8 для русского алфавита). Для того чтобы зашифровать сообщение, необходимо разбить его на *биграммы* (группы

из двух символов). Если два символа биграммы совпали (или если остался один символ), добавим после первого символа X (или любую другую фиксированную букву соответствующего алфавита). Для шифрования биграммы нужно отыскать ее в ключевой таблице. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. (Другими словами, отражаем полученный прямоугольник относительно вертикальной оси симметрии. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. (Другими словами, мы сдвигаем биграмму на одну позицию вправо по строке.) Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. (Другими словами, мы сдвигаем биграмму на одну позицию вниз по столбцу.) Придумайте и зашифруйте с помощью шифра Плейфера одно сообщение на русском и одно — на английском языке. Проверьте результат, расшифровав сообщение. Что делать с «лишней» буквой X? [128]

10 Для работы с *парным шифром* используют фразу, содержащую 15 различных букв русского алфавита, и под каждой из этих букв записывают не вошедшие в выбранную фразу буквы в алфавитном порядке (считаем, что буквы Е и Ё, И и Й, Ь и Ъ отождествлены). Например, при выборе фразы «НЕ СЛЫШНЫ В САДУ ДАЖЕ ШОРОХИ» мы получим следующую шифрующую таблицу.

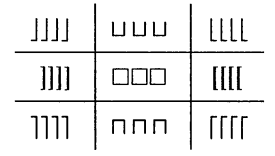
Н	Е	С	Л	Ы	Ш	Н	Ы	В	С	А	Д	У	Д	А	Ж	Е	Ш	О	Р	О	Х	И
В	Г	З	К	М	П			Т		Ф	Ц	Ч			Щ			Ь	Э		Ю	Я

Осуществите шифрование сообщения «МАТЕМАТИКА — ЦАРИЦА НАУК», пользуясь полученной таблицей подстановки. Используйте для шифрования этого же сообщения таблицу подстановки, полученную по придуманной вами фразе. Проверьте результаты, осуществив расшифровку полученных шифротекстов.

11 Для использования шифра *уголки* разбейте 33-буквенный русский алфавит следующим образом.

АБВГ	ДЕЁ	ЖЗИЙ
КЛМН	ОПР	СТУФ
ХЦЧШ	ЩЪЫ	ЬЭЮЯ

Тогда буквам будут соответствовать уголки, повторяющие контуры ячейки, куда попала буква.



Поскольку каждой группе букв соответствует только один символ, проставьте в его копиях 0, 1, 2 или 3 точки: теперь каждой букве соответствует свой код. Зашифруйте сообщение «А ЗОРИ ЗДЕСЬ ТИХИЕ» с помощью полученной таблицы подстановки. Проверьте результат, осуществив расшифровку полученного шифротекста.

12 Алгоритм использования *шифра Бофора*, подразумевающий наличие таблицы Виженера, выглядит так: составить сообщение и выбрать ключ, длина которого совпадает с длиной сообщения; взять n-ый символ открытого текста m_n; найти столбец j, первый символ которого равен m_n; найти строку i, символ которой, расположенный на пересечении с j-ым столбцом, равен n-му символу ключа k_n; добавить к шифротексту символ первого столбца i-ой строки. Зашифруйте с помощью шифра Бофора сообщение «ПРОСТЫХ ЧИСЕЛ БЕСКОНЕЧНО МНОГО». Сравните алгоритм шифра Бофора со схемой шифрования по таблице Виженера.

13 *Однозвучный* (*омофонический*) *шифр* — шифр подстановки, при котором каждый символ открытого текста заменяется на один из нескольких символов алфавита шифрования, причем количество заменяющих символов для одной буквы пропорционально частотности этой буквы. Пользуясь таблицами частотности букв русского языка (см. главу 10), приведите пример такого шифра и зашифруйте с его помощью два сообщения. Осуществите расшифровку полученных шифротекстов. Однозначен ли оказался результат расшифровки?

14 Зашифруйте сообщение «ПОНЕДЕЛЬНИК НАЧИНАЕТСЯ В СУББОТУ» шифром Тритемиуса, используя ключ 3-5-9-2-4. Зашифруйте то же сообщение, если n-ый символ ключевого слова вычисляется по формуле $k_n = 15n - 3$; по формуле $k_n = 3n^2 + 8n + 1$. При каких значениях параметров A, B и C формулы $k_n = An + B$ и $k_n = An^2 + Bn + C$ генерируют нетривиальные ключи?

15 Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Э	Ю	Я	
16	17	18	19	20	21	22	23	24	25	26	27	28	29	

Для шифрования полученного числового сообщения используется шифрующий отрезок последовательности $A_1, A_2, \ldots$ подходящей длины, начинающийся с A_{100}. При шифровании каждое число числового сообщения складывается с соответствующим числом шифрующего отрезка, затем вычисляется остаток от деления полученной суммы на 30, который по данной таблице заменяется буквой. Зашифруйте сообщение «КРИПТОГРАФИЯ», если шифрующий отрезок взят из последовательности, у которой $A_1 = A_2 = 1$ и $A_{k+2} = A_k + A_{k+1}$ для любого натурального k. Восстановите сообщение «КЕНЗЭРЕ», если шифрующий отрезок взят из последовательности с $A_1 = 3$ и $A_{k+1} = A_k + 3(k^2 + k + 1)$ для любого натурального k.

16 Определите количество возможных решеток Кардано размера 6×4; 6×6; 8×8; $n \times n$.

17 Для шифрования текста шифром *поворотная решетка* использовали трафарет размером 6×6 клеток. Для повышения сложности шифра процедуру повторили, последовательно шифруя получающиеся шифротексты некоторое количество раз, и вдруг обнаружили, что снова получился текст сообщения. После скольких повторов это произошло в первый раз?

18 Определите число ключей шифра Тритемиуса, если в качестве ключа используется набор из 10 различных цифр.

19 Клетки квадрата 4×4 пронумеровали так, что клетка в правом нижнем углу получила номер 1, а все остальные получили разные номера от 2 до 16 таким образом, что суммы номеров клеток каждой строки, каждого столбца, а также каждой из двух диагоналей квадрата оказались одинаковы. Докажите, что сумма чисел в каждом столбце, строке и диагонали этого магического квадрата составляет 34.

1.2. Криптоанализ классических шифров

Криптоанализ — наука о методах несанкционированного вскрытия зашифрованной информации без знания ключей. (Термин был введен в 1920 г.)

Попытку раскрытия конкретного шифра с применением методов криптоанализа называют *криптографической атакой* на этот шифр. Криптографическая атака, в ходе которой раскрыть шифр удалось, называется *взломом* или *вскрытием*.

Криптостойкостью шифра называется его стойкость к взлому. Она обычно определяется количеством всех возможных ключей шифра и временными затратами на перебор всех вариантов.

1.2.1. Криптоанализ шифров перестановки

Для шифров перестановки количество возможных вариантов оценивается как $n!$, где n — количество символов в сообщении. Однако во многих случаях существуют достаточно простые способы взлома перестановочных шифров. Для скитады такой способ, изобретенный Аристотелем, был описан выше. Шифры, основанные на использовании решеток, довольно просто вскрываются, если известны размеры соответствующей таблицы.

Пример 1.2.10 Рассмотрим один из случаев вскрытия решетки, размеры которой оказались известны. Зная эту информацию, мы можем предположить, что текст исходного сообщения был записан в таблицу обычным образом, по строкам, а затем столбцы этой таблицы были некоторым образом переставлены.

Т	Ф	З	Е	А	О	Р	Н	И	Т	Т	С	Я	Ш	Э	В	А	Ы	В	Е
К	Ь	П	С	Я	И	Н	А	Л	Т	Т	А	Н	А	Р	Р	Е	Е	О	В
С	С	Б	В	Л	Е	Т	О	И	А	Н	Е	М	Л	К	К	О	И	Н	О
О	Щ	Е	Н	И	С	Е	Н	Б	О	О	П	Р	О	Г	О	Ж	М	О	Ч
Ь	Ж	З	П	Е	Т	Е	Н	А	С	Р	А	В	Д	Е	А	Я	Н	И	Л
Р	Т	В	Т	О	Е	А	Н	С	П	О	Л	Б	Е	А	И	С	К	Ц	О
Б	Ц				А	Ы		И	Т				Л	В					

Записав шифротекст в виде таблицы размера 7 × 20, обратим внимание на то, что столбцы сообщения имеют разную высоту. Естественно предположить, что это произошло из-за неполного заполнения последней строки. Выделим имеющиеся 8 столбцов высоты семь в отдельную группу и попытаемся расположить их так, чтобы в каждой строке таблицы получился читаемый текст. Подбор проще сделать по последней строке — там угадывается слово «ТАБЛИЦЫ».

Подбирая продолжения по четвертой («СООБЩЕ» → «СООБЩЕНИЕ») и шестой («ПЕРЕСТА» → «ПЕРЕСТАНОВКИ») строкам среди оставшихся столбцов, находим исходное состояние таблицы.

Э	Т	О	Т	Ш	И	Ф	Р	Н	А	З	Ы	В	А	Е	Т	С	Я	В	Е
Р	Т	И	К	А	Л	Ь	Н	А	Я	П	Е	Р	Е	С	Т	А	Н	О	В
К	А	Е	С	Л	И	С	Т	О	Л	Б	И	К	О	В	Н	Е	М	Н	О
Г	О	С	О	О	Б	Щ	Е	Н	И	Е	М	О	Ж	Н	О	П	Р	О	Ч
Е	С	Т	Ь	Д	А	Ж	Е	Н	Е	З	Н	А	Я	П	Р	А	В	И	Л
А	П	Е	Р	Е	С	Т	А	Н	О	В	К	И	С	Т	О	Л	Б	Ц	О
Б	Т	А	Б	Л	И	Ц	Ы												

Таким образом, исходное сообщение имело вид «ЭТОТ ШИФР НАЗЫВАЕТСЯ ВЕРТИКАЛЬНАЯ ПЕРЕСТАНОВКА ЕСЛИ СТОЛБИКОВ НЕМНОГО СООБЩЕНИЕ МОЖНО ПРОЧЕСТЬ ДАЖЕ НЕ ЗНАЯ ПРАВИЛА ПЕРЕСТАНОВКИ СТОЛБЦОВ ТАБЛИЦЫ». □

Замечание. *При использовании шифров-перестановок пробелы и знаки препинания обычно опускаются. Важным является также не оставлять в таблицах и решетках пустые клетки. Если число символов сообщения меньше размерности приготовленных решеток, то после сообщения можно записать по порядку буквы используемого алфавита. Это позволяет получателю понять, что сообщение окончено и затрудняет взлом.*

1.2.2. Криптоанализ шифров простой замены

Для вскрытия шифров простой замены применяют *частотный анализ* — один из методов криптоанализа, основывающийся на предположении о том, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка.

Метод частотного анализа известен с IX в. Его родоначальником считают арабского философа и математика Аль Кинди (Abu Yūsuf Ya'qūb ibn 'Isḥāq aṣ-Ṣabbāḥ al-Kindī, около 801 – около 873), который составил сочинение «О дешифровке криптографических сообщений». Раздел, посвященный шифрам замены, включающий в себя описание способа их

вскрытия, основанного на частотном анализе встречаемых в шифре символов, включен в арабскую энциклопедию XV в. Наиболее известным случаем применения частотного анализа в реальной жизни является дешифровка египетских иероглифов Ж.-Ф. Шампольоном в 1822 г.

Для вскрытия шифра Цезаря по элементу шифротекста надо просто вычислить величину сдвига и выполнить обратный сдвиг: данный вид шифрования очень прост, но, к сожалению, не является надежным. Так, в русском языке наиболее часто встречается буква О (11 %). Поэтому разумно предположить, что наиболее часто встречающаяся буква в шифротексте на русском языке будет результатом шифрования буквы О, и найти величину используемого в шифре сдвига простым вычитанием друг из друга соответствующих числовых эквивалентов букв. Впрочем, даже если в нашем распоряжении имеется лишь небольшое послание, не дающее нам определить чаще всего встречающуюся букву, то для величины сдвига k имеется всего 33 возможности, и можно просто попробовать их все. Лишь одному значению k будет соответствовать осмысленное сообщение, такое k и будет ключом шифрования.

Пример 1.2.11 Для вскрытия шифротекста «ЗДЙЧ ОТФТЕД РТПТОТ», полученного с помощью шифра Цезаря со сдвигом k, достаточно заметить, что чаще других в шифротексте встречается буква Т. Это означает, что сдвиг k преобразует наиболее часто встречающуюся букву русского алфавита О $= 15$ в Т$= 19$, то есть $k = 4$. Чтобы дешифровать сообщение «ЗДЙЧОТФТЕДРТПТОТ», остается вычесть 4 (mod 33) из числовых эквивалентов букв послания, получив исходное сообщение «ДАЕТ КОРОВА МОЛОКО». □

Для повышения стойкости шифра Цезаря используют ключевое слово для смещения и изменения порядка символов в алфавите подстановки. Ключевое слово (буквы которого не должны повторяться) записывается под буквами алфавита, начиная с буквы, числовым эквивалентом которой является некоторое число k. Буквы алфавита подстановки, не вошедшие в ключевое слово, записываются после него циклически в алфавитном порядке.

Так, для русского алфавита таблица шифрования в случае шифра Цезаря с ключевым словом «ЧИСЛО» и сдвигом $k = 5$ выглядит следующим образом.

Исходный алфавит	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
Алфавит замены	Ы	Ь	Э	Ю	Я	Ч	И	С	Л	О	А	Б	В	Г	Д	Е	Ё
Исходный алфавит	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
Алфавит замены	Ж	З	Й	К	М	Н	П	Р	Т	У	Ф	Х	Ц	Ш	Щ	Ъ	

Несомненным достоинством системы Цезаря с ключевым словом является то, что количество возможных ключей практически неисчерпаемо. Это делает частотный анализ затруднительным, но все же возможным, поэтому надежность этого метода тоже не очень высока.

Квадрат Полибия тоже кажется на первый взгляд очень нестойким. Однако для его реальной оценки следует учитывать два фактора: возможность заполнить квадрат Полибия буквами произвольно, а не только строго по алфавиту, и возможность периодически заменять используемые для шифрования квадраты. Тогда анализ предыдущих сообщений ничего не дает, так как к моменту раскрытия шифра он может быть заменен.

Буквы могут вписываться в таблицу в произвольном порядке — заполнение таблицы в этом случае и является ключом. Максимальное количество ключей для шифра на таблице английского алфавита равно 25!. В данном случае мы имеем дело с комбинацией шифров замены и перестановки.

В принципе, для любых одноалфавитных шифров процесс частотного анализа для достаточно больших текстов не представляет особой трудности. Об этом свидетельствуют и множество примеров из классической литературы (рассказы «Пляшущие человечки» А. Конан Дойла и «Золотой жук» Э. По, роман «Дети капитана Гранта» Ж. Верна и др.), в которых приведено подробное описание соответствующих алгоритмов.

Пример 1.2.12 Попробуем расшифровать представленную ниже криптограмму, полученную простой заменой букв русского алфавита на числа 1–32 (буквы Е и Ё не различаются).

12 2 24 5 3 21 6 29 28 2 20 18 20 21 5 10 27 17 2 11 2 16
19 2 27 5 8 29 12 31 22 2 16, 19 2 19 5 17 29 8 29 6 29 16:
8 2 19 19 29 10 19 29 14 19 29 29 19 10 2 24 2 11 2 16
10 14 18 21 17 2 20 2 28 29 16 21 29 28 6 29 16

Один из вариантов решения состоит из следующих этапов.

- Анализируя двухбуквенные сочетания цифр, приходим на основании изучения второй строки к выводу, что 19 = Н (из соединений «19, 2» и «19, 5»).
- На основании анализа третьей строки получим, что 29 = О (из «29,Н,10»), а 10 = А или 10 = И.
- Аналогичным образом заключаем, что 14 = Щ (из «но 14 но»).
- Далее, дешифруем 8 = Д, 2 = Е, 10 = И (из «денно и нощно»).

- Осуществив выделенные замены, получим следующий текст.
  12 е 24 5 3 21 6 о 28 е 20 18 20 21 5 и 27 17 е 11 е 16
  н е 27 5 д о 12 31 22 е 16, н е н 5 17 о д о 6 о 16:
  д е н н о и н о щ н о о н и е 24 е 11 е 16
  и щ 18 21 17 е 20 е 28 о 16 21 о 28 6 о 16
  Продолжим анализ.
- Из второй строки следует, что 5 = А и 27 = З.
- Кроме того, 17 = В, 6 = П, 16 = Й (последнее слово второй строки — «водопой»).
- Теперь мы получаем такой текст:
  12 е 24 а 3 21 п о 28 е 20 18 20 21 а и з в е 11 е й
  н е з а д о 12 31 22 е й, н е н а в о д о п о й:
  д е н н о и н о щ н о о н и е 24 е 11 е й
  и щ 18 21 в е 20 е 28 о й 21 о 28 п о й.
- Нетрудно видеть, что 21 = Т, 18 = У, 28 = Л, 20 = С (из последней строки «ищут веселой толпой»).
- Аналогично, 11 = Р (из «з в е 11 е й» первой строки).
- Итак, текст принимает такой вид:
  12 е 24 а 3 т п о л е с у с т а и з в е р е й
  н е з а д о 12 31 22 е й, н е н а в о д о п о й:
  д е н н о и н о щ н о о н и е 24 е р е й
  и щ у т в е с е л о й т о л п о й.
  Теперь мы можем закончить нашу работу.
- 24 = Г (из «егерей»).
- 12 = Б, 3 = Ю (из «бегают»).
- 31 = Ы, 22 = Ч (из «добычей»).

Таким образом, мы получили следующее четверостишие В. С. Высоцкого.

«Бегают по лесу стаи зверей
Не за добычей, не на водопой:
Денно и нощно они егерей
Ищут веселой толпой.» □

1.2.3. Криптоанализ полиалфавитных криптосистем

Для затруднения частотного анализа подстановочных шифров используют разные методы, заменяя монобуквенные системы шифрования однозвучными, полиграммными или полиалфавтиными, комбинируя различные виды шифрования и т. д.

Наиболее известными полиалфавитными шифрами являются шифр Тритемиуса и таблица Виженера. Преимущество этих методов шифрования состоит в том, что статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Стойкость такой криптосистемы определяется произведением стойкости прямой замены на число используемых алфавитов, т. е. число букв в ключе. Одним из недостатков шифрования является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Пример 1.2.13 Используя шифр Тритемиуса для русского алфавита размерности 30 (без Й, Ё и Ъ), была получена шифрограмма «РБЬНПТСИТСРРЕЗОХ». Попробуем прочитать исходное сообщение, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б, В.

Для этого каждую букву шифрованного сообщения расшифруем в трех вариантах, предполагая последовательно, что соответствующая буква шифрующей последовательности есть буква А, Б или В.

шифрованное сообщение	Р	Б	Ь	Н	П	Т	С	И	Т	С	Р	Р	Е	З	О	Х
вариант 1	П	А	Щ	М	О	С	Р	З	С	Р	П	П	Д	Ж	Н	Ф
вариант 2	О	Я	Ш	Л	Н	Р	П	Ж	Р	П	О	О	Г	Е	М	У
вариант 3	Н	Ю	Ч	К	М	П	О	Е	П	О	Н	Н	В	Д	Л	Т

Выбирая из каждой колонки полученной таблицы ровно по одной букве, находим осмысленное сообщение «НАШКОРРЕСПОНДЕНТ», которое и является искомым. □

Замечание. *Из полученной таблицы можно было найти и такое исходное сообщение, как «НАШ МОРОЗ ПОПОВ ЕМУ», которое представляется не менее осмысленным, чем приведенное выше. А если предположить, что при передаче шифрованного сообщения произошло одно искажение — скажем, в качестве* 11*-й буквы была принята не буква Р, а буква П, — то, наряду с правильным вариантом, можно получить и такой: «НАШ МОРОЗ ПОМОГ ЕМУ». При этом число различных вариантов исходного сообщения, полученных по нашей схеме, без ограничений на осмысленность равно* 3^{16} *или* 43 046 721, *т. е. более* 40 *миллионов!*

Несмотря на недостатки практической реализации, полиалфавитные шифры оказались достаточно криптостойкими для своего времени. Например, шифр Виженера не могли взломать на протяжении 400 лет. Однако, в 1863 г. Фридрих Вильгельм Касиски (Friedrich Wilhelm Kasiski, 1805–1881), немецкий шифровальщик и археолог, опубликовал свой труд «Тайнопись и искусство дешифрования», в котором описал свое крупное открытие в криптоанализе: алгоритм, известный сегодня как *тест Касиски*.

Этот алгоритм позволил взламывать полиалфавитные шифры, в частности, шифр Виженера. Открытие Касиски уступает по важности только работе Аль-Кинди, который открыл метод частотного анализа.

Метод Касиски позволяет криптоаналитику найти длину ключевого слова, используемого в полиалфавитном шифре. Как только длина ключевого слова обнаружена, криптоаналитик выстраивает зашифрованный текст в n колонках, где n — длина ключевого слова. Тогда каждую колонку можно рассматривать как зашифрованный моноалфавитным шифром текст, который можно подвергнуть частотному анализу.

Идея метода Касиски основана на том, что ключи являются периодическими, а в естественном языке существуют часто встречающиеся буквосочетания: биграммы и триграммы. Это наводит на мысль, что повторяющиеся наборы символов в шифротексте — повторения популярных биграмм и триграмм исходного текста. Криптоаналитик ищет в зашифрованном тексте повторные сегменты по крайней мере из трех символов. Если найдено два таких сегмента и расстояние между ними равно d, то криптоаналитик предполагает, что $n|d$, где n — длина ключа. Если удается найти несколько повторных сегментов с расстояниями $d_1, d_2, \ldots, d_m$ между ними, то будет выполняться соотношение $n|(d_1, d_2, \ldots, d_m)$, т. е. наибольший общий делитель всех найденных таким образом расстояний будет кратен предполагаемой длине ключевого слова.

Сложность метода Касиски состоит в необходимости поиска повторяющихся сегментов. Это практически невозможно сделать вручную, однако не составляет особой сложности на компьютере. Тем не менее метод требует вмешательства человека, так как некоторые совпадения могут оказаться случайными, что приведет к тому, что наибольший общий делитель всех расстояний будет равен 1. Криптоаналитик должен выяснить, какие длины являются подходящими и, в конечном итоге, проверить правильность подобранного периода, исходя из осмысленности расшифрованного текста [128].

Пример 1.2.14 Попробуем применить метод Касиски к зашифрованному с помощью некоторого полиалфавитного шифра периода k сообщению, представленному ниже.

«СЪСШ ЩГЖИСЮБЩЫРО ФЧ РЛЫОУУПЦЛЫ ЦЙУБЭЫФСЮДЯ ЛКЧААЮЦЩДХИЯ Б ХЙЕУЖ ШЩ ЧЙХК ЯПУЩА УОРЧЙ ЧЬЩ ЬЙЬЩУЙЙЧ Е ПЛЖЮС ЧАХОИ ЩЦ ЛЩДФСНБЮСЛ Щ ЙККЦЖЦЛЩ ЭЙСНШТ ЩЧЫОВХЮДИ ЗЗН ЛЪЯД ЛЕЖОН ЕЮЧЪЛМСРТЖЦЬВЖ ЛГСЗЙЬЧШ НФЧЗ ЧЮАЮЕ ЛЖЙКУАХЙНАИЕЬВ ЙЦЛ ККФЩУЮИЙЧ З ЬЦСЙВГЫХ СОЗЖЪНШШО ЛЪЯД ЦСЗНКЕШЛГЫХ ЦЩЗШО ЦСПЛЛТП С ЧАХЙВЩ ЮЙЦСЗХФС КЗСАХЦЩ СЙФФЗШО ЛЪЯД РЛЬНГЫХЪЖ ДПХЛЕЗ НФЧГХЛ ШЙ ШУЩ ЮООЕЛХЧУЛУ ЩКЯЙЛЩНКЫЭА ЕЧРЮЗЫГЧЖФЖ ЩЦ ЧРШЙЛЩМ ДЛВОЖЫРО КЙЯЛЫОЖЧЖФПШЙЪНХ ХЙЕЩЖ СЪСШ СЬЛРНГ ШПРТЗПЗН ЧЕЧУЦЖЪЕЩУС РЫСОНШЙ ЩЩТЖЛТЕЗ СЪСПХЛ СПРЬЛЕСЧШЙЪНХЩ ЪЙУЖЫЬЛ ЯЧВАЕЧИ ЩРЩТ ОЕФЖЫХЪЖ ДХЩЦЩЦХОВХЮДФ ЩРЩТ Щ ЗМУВ ЫЩГЕПЫЛЖПЯЛЩ Е ШУБЭЫЛЯЖ ЛШДФСНБЮСЖ ШПБВЩ КЛЩА УОРЧЙ С ЛЪЯД Р ЮЯЙЭЩИЙЯЩ ЭЧНЛЯДФ ДЙРЧБЩЫРО ЫФЖ НЖЫФМ ЕРУЛКФТЕЗ У ЬЩУ ЧНШЙЪЖЧКИ ЧЩЫЙЕЧЗАФДЭСФ ЮЙНЭЩСЦТА З СЪСШ РГФПЛТ З ЙЪЬЛЕО ЛР ИОСЩХ АФЧЭЧ ЩЮЯОЧАИОЬШЙО ЦСЙМУБУХЬЛЖ ЪЩНЖЩСБЮСФ НЗНГЯХСЮАКУЛА ЬЙЧБМС Л ГЖФФШПШУБЕФФШЮЧФ ЛЪЬЮАЮСФ НИИ ДЛЯЧЫЛ ЙЩЪБЮСОЛЕЙЬШЙТ СЩЬЦЛ НЖЫФМ Е НФЧКУЩЕ КЙЧК ЮОЩФЦЧЧЩУЧ УБЬЦЩЛЪЩГЖЗО ЛЪЯ ЫГЯ ЭЙЕ ЧЙФПЯЙ ШУЩ ОЫЛР АЪВЛЕСЖР ЪЬЧАХ ЧААКШФЦЖЦГ НЖЫЖЕ ЕЧОЕЙПЬЛКЫП ЩЮЫФСЖЪЬЛТ С РЛЫОУУПЫФТГЦЩМ ЫОЖЧЖФПШЙЪНЩ УЦЩЪЙЧАСПРЛА ХСЦЛЕ ЛЛНЙЛ ЗЛЯХ ЛЪЯ ЦФЩЬКФУЮЧ ЕБЭ ЦФЩЬКФУЮЧ ЯШЙМЩЛЪЩГЖЗО СЩЬЦЛ ЯЙЫЩСАЗ ЩШЗ ЧНСППГЫХ УГЯ ЮОЛЖЪОСШЙ ХЬЛРЧЩФЯЙОЩЖ ЦФДУЧНСД ЦГ ЗЮОЫШЩЗ РРЙПФДХЕ ЛЪЯ ЧЧШЙМЩ ЧЗШГ ЕЙНФТЗ.»

Поиск повторяющихся сегментов текста из трех букв дает такие результаты.

- Группа «СЪС» встречается в позициях 1, 373, 417, 613. Соответствующие расстояния равны

$$d_1 = 373 - 1 = 372 = 4 \cdot 3 \cdot 31,$$
$$d_2 = 417 - 373 = 44 = 4 \cdot 11,$$
$$d_3 = 613 - 417 = 196 = 4 \cdot 49.$$

Поскольку $(d_1, d_2, d_3) = 4$, то предполагаем, что период k вскрываемого полиалфавитного шифра делит 4.

- Группа «ЩГЖ» встречается в позициях 5, 781, 941. Соответствующие расстояния равны

$$d_1 = 781 - 5 = 776 = 8 \cdot 97,$$

$$d_2 = 941 - 781 = 160 = 32 \cdot 5.$$

Поскольку $(d_1, d_2) = 8$, можно предположить, что период шифра делит 8. Это не противоречит выводу для предыдущей группы.

- Группа «ЫРО» встречается в позициях 13, 349, 557. Соответствующие расстояния равны

$$d_1 = 349 - 13 = 336 = 16 \cdot 3 \cdot 7,$$

$$d_2 = 557 - 349 = 208 = 16 \cdot 13.$$

Следовательно, $(d_1, d_2) = 16$, что позволяет предполагать, что период шифра делит 16. Это тоже не противоречит предыдущим результатам.

Таким образом, на основе проведенного теста Касиски можно сделать правдоподобное предположение: период вскрываемого полиалфавитного шифра равен 4.

Теперь, подвергая текст частотному анализу, нетрудно получить ключевое слово «ЙГБП» и прочитать исходное сообщение:

«Игры различаются по содержанию характерным особенностям а также по тому какое место они занимают в жизни детей их воспитании и обучении Каждый отдельный вид игры имеет многочисленные варианты Дети очень изобретательны Они усложняют и упрощают известные игры придумывают новые правила и детали Например сюжетно-ролевые игры создаются самими детьми но при некотором руководстве воспитателя Их основой является самодеятельность Такие игры иногда называют творческими сюжетно-ролевыми играми Разновидностью сюжетно-ролевой игры являются строительные игры и игры драматизации В практике воспитания нашли свое место и игры с правилами которые создаются для детей взрослыми К ним относятся дидактические подвижные и игры забавы В основе их лежит четко определенное программное содержание дидактические задачи и целенаправленное обучение. Для хорошо организованной жизни детей в детском саду необходимо разнообразие игр так как только при этих условиях будет обеспечена детям возможность интересной и содержательной деятельности Многообразие типов видов форм игр неизбежно как неизбежно многообразие жизни которую они отражают как неизбежно многообразие несмотря на внешнюю схожесть игр одного типа модели». □

Метод Касиски окажется бесполезным, если при работе полиалфавитного шифра будет использовано ключевое слово бесконечной длины. Реализацией данной идеи является *шифр Вернама* (*одноразовый шифровальный блокнот*) — единственная система шифрования, для которой доказана абсолютная криптографическая стойкость.

Шифр назван в честь американского инженера по телекоммуникациям Гильберта Вернама (Gilbert Sandford Vernam, 1890–1960), который в 1917 г. построил телеграфный аппарат, выполнявший соответствующую операцию шифрования автоматически — надо было только подать на него ленту с ключом. Ключ, по мысли Вернама, должен был представлять собой случайную последовательность букв. В 1945 г. американский ученый и инжинер Клод Шеннон (Claude Elwood Shannon, 1916–2001) доказал абсолютную стойкость шифра Вернама: перехват шифротекста не дает никакой информации о сообщении и, с точки зрения криптографии, невозможно придумать более безопасную криптографическую систему.

Недостатком шифра Вернама является отсутствие подтверждения подлинности и целостности сообщения. Шифр Вернама чувствителен к любому нарушению процедуры шифрования. Кроме того, под рукой всегда необходимо иметь достаточное количество ключей, которые могут понадобиться в дальнейшем для шифрования больших объемов открытого текста. Проблемой является защищенная передача последовательности и сохранение ее в тайне. На практике можно один раз физически передать носитель информации с длинным истинно случайным ключом, а потом по мере необходимости пересылать сообщения. На этом основана идея шифроблокнотов: шифровальщик по дипломатической почте или при личной встрече снабжается блокнотом, каждая страница которого содержит ключи. Такой же блокнот есть и у принимающей стороны. Использованные страницы уничтожают [78].

Наконец, для работы шифра Вернама необходима истинно случайная последовательность, а, по определению, последовательность, полученная с использованием любого алгоритма, является не истинно случайной, а псевдослучайной (см. главу 8).

В настоящее время шифрование Вернама используется достаточно редко. Это связано с тем, что современные методы криптографии развиты достаточно хорошо для того, чтобы удовлетворять потребностям пользователей. Однако с развитием технологий и с увеличением доступных компьютерных мощностей растет и вероятность успешной атаки. Современные носители данных могут хранить огромное количество случайных ключей, а современные генераторы случайных чисел позволяют производить случайные ключи достаточного для использования в шифре Вернама качества. Все это повышает актуальность использования современных модификаций этого криптографического метода.

Упражнения

1. Сообщение было зашифровано с помощью шифра простой перестановки столбцов. Найдите исходное сообщение, если известно число

строк m и число столбцов n использованной для шифрования таблицы:

a) «ДНТНВОСЕАГЕШРОНАПЕЬР», $m = 4, n = 5$;

b) «ДЛТЕОЕВВШДЕЯЕНЛИЬЕМВП», $m = 3, n = 7$;

c) «ВЙГШАОСОИУАЕДНЯТШАМСПАМСИСТАЙЧИРЛАТ», $m=5$, $n=7$.

(2) Сообщение было зашифровано с помощью шифра *постолбцовая транспозиция*. Пробелы в сообщении были опущены, а знаки препинания заменены на условные комбинации: точка — «ТЧК», запятая — «ЗПТ». Прочтите исходное сообщение, если после шифрования оно выглядело так, как показано в таблице.

Я	Н	Л	В	К	Р	А	Д	О	Е	Т	Е	Р	Г	О	М	И	З	Я	Е
Й	Л	Т	А	Л	Ф	Ы	И	П	Е	У	И	О	О	Г	Е	Д	Б	О	Р
Ч	Р	Д	Ч	И	Е	С	М	О	Н	Д	К	Х	И	Н	Т	И	К	Е	О
Н	У	Л	А	Е	Р	Е	Б	Ы	Ы	Е	Е	З	И	О	Н	Н	Ы	Ч	Д
Ы	Т	Д	О	Е	М	П	П	Т	Щ	В	А	Н	И	П	Т	Я	З	С	Л
И	К	С	И	—	Т	Ч	Н	О	—	—	Е	—	Л	У	Л	-	Т	-	Ж

(3) Сообщение было зашифровано с помощью решетки Кардано. Прочтите исходное сообщение, если после шифрования оно приняло нижеследующий вид.

Р	П	Т	Е	Ш	А	В	Е	С	Л
О	Я	Т	А	Л	—	Ь	З	Т	-
-	У	К	Т	-	Я	А	Ь	—	С
Н	П	—	Ь	Е	У	-	Ш	Л	С
Т	И	Ь	З	Ы	Я	Е	М	—	О
-	Е	Ф	—	—	Р	О	—	С	М

(4) При шифровании текста на русском языке каждую букву заменяют парой цифр, опуская пробелы и знаки препинания. При этóм разные буквы текста заменяются разными парами цифр, а одинаковые — одинаковыми. Найдите все возможные расположения слова «РАБОТА» в исходном тексте по шифрованному тексту.

15 17 16 72 17 15 70 73 97 90 17 72 38 39 74 76 17 34 79 78 17 70 76 74 72 74 73 74 76 70 70 17 76 74 96 74 37 39 75 17 70 39 74 79 39 37 71 74 98 35 94 90 98 17 94 96 74 98 74 76 17

⑤ Шифрование сообщения состоит в замене букв известного текста на русском языке на пары цифр в соответствии с некоторой таблицей, в которой разным буквам алфавита соответствуют разные пары цифр. В каком случае будет легче восстановить текст: если известно, что первое слово второй строки — «ПРАКТИКА»; если известно, что первое слово пятой строки — «СЕМИНАР»?

⑥ Для шифрования открытого текста каждую букву заменяют парой цифр, при этом разные буквы текста заменяются разными парами цифр, а одинаковые — одинаковыми. Даны два зашифрованных текста.

a) 79 15 38 98 95 91 34 95 73 77 96 15 78 95 73 98 1596 15 72 98 96 77 72 15 34 77 96 75 90 76 95 38 98 15 70 33 90 96 79 90 96 77 98 95 90 38 77 70 70 90 98 74 15 96 98 96 77 72 15 34 77 96 75 73 77 96 15 98 74 15 79 96 90 79 15 96 98 94 90 76 98 74 15 95 96 96 15 73 79 15 33 98 95 32 15 90 93 38 15 96 73 94 90 91 96 91 73 15 98 74 95 73 33 72 96 90 34 95 73 73 91 36 71 15 33 98 98 90 77 38 15 38 72 91 73 15 96 70 95 33 15 38 33 15;

b) 71 75 74 39 74 73 74 72 30 73 74 78 33 79 98 94 78 36 79 97 72 29 78 74 96 74 92 30 38 79 70 72 94 78 79 22 92 92 79 98 37 70 92 74 94 77 74 93 31 78 74 70 39 79 71 75 94 98 70 39 97 92 72 22 23 39 78 94 70 74 76 78 94 78 78 30 77 39 94 74 75 94 39 79 38 94 70 73 79 77 79 78 39 94 75 94 70 73 75 74 76 94 39 74 96 74 76 78 74 96 79 94 39 79 71 30 27 39 79 32 71 75 74 39 74 73 74 72 74 92 71 75 94 98 35 22 92 72 22 23 39.

Известно, что один из них соответствует сообщению на русском языке, а другой — на английском (пробелы и знаки препинания опущены). Определите, какой шифрованный текст соответствует сообщению на русском языке.

⑦ Зная, что сообщение зашифровано с помощью шифра Цезаря, найдите величину k примененного сдвига и расшифруйте сообщение:

a) «ФОЫИЫШОЩОФОЬЦДОШЬСАД»;

b) «ТИМСЖУТПЙСЙЖТМС»;

c) «БШЬАШЭЕЖВЧДЗЫШЭУЬАШЭЕЖВДЗФЯШЭ».

⑧ Перехвачена криптограмма, которая была получена при использовании шифра Тритемиуса для русского алфавита размерности 30 (без Й, Ё и Ъ). Попробуйте прочитать исходное сообщение, если шифротекст имеет вид «ФФЧСЙИФНЧЧИНЩЩЩЧФРСИШД» и известны буквы, формирующие ключ: Ж, З, И.

⑨ Используя частотный анализ букв русского языка, вскройте сообщение (стихотворение Р. Киплинга), если известно, что различным буквам соответствуют различные двузначные числа. Знаки препинания сохранены для удобства вскрытия.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35

⑩ Криптограмма получена при использовании шифра простой замены букв 32-буквеного русского алфавита (буквы Е и Ё идентифицированы). Используя метод частотного анализа, прочтите четверостишия:

a) «Гыюь Фюббшн эй яюэовл,
Пфзшэюь юришь эй шчьйфшвл:
Г эйщ юбюрйээо бвпвл —
С Фюббшн ьюцэю вюылъю сйфшвл.»

b) «Йхпм кмлся цйег тердсйц
Сй уйыдпяхг, сй хйфимхя!
Ж ийся чсасмг хрмфмхя:
Ийся жйхйпяг, жйфя, сдхцдсйц.»

c) «Щм умэс яи сс щс нарф,
Щм умэс ьщм ючмрць ямц юыфя;
Аяэь риефя а щсх щм пэарф,
Лэць ыиеся щм лшцмв чмщэя.»

d) «Исжжу спзы обе збслпк ойгпк,
Й пу ойгэ й еп ойгэ
Дпойу гжужс рсйцпумйгэк
Ипмпуэж ржсжмйгэ.»

⑪ Задан некоторый текст, зашифрованный шифром Виженера. Определите ключевое слово и прочитайте текст:

Влцдутжбюцхъяррмшбрхцэооэцгбрьцмйфктъъюьмшэсяцпунуящэйтаьэдкцибрьцгбрпачкъуцпъбьсэгкцъгуущарцеэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйояфывбнэнфуюгбрьсшьжэтбзечюъюръегофкбьчябашвеэуъъюаднчжчужцеэвлрнчулбюпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуфбюацмнубсюкйтаьэдйюнооэгюожбгкбрънцэпотчмеодзцвбцшщвщепчдчдръюьскасэгъппэгюкдойрсрэвоопчщшоказръббнэугнялекьсрбеуыэбдэулбюасшоуэтъшкрсдугэфлбубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуэзьрадзьжчюрмфцхраююанчечюъыхьъцомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъьрьцъцпоилуфэдцойэдятррачкубуфнйтаьэдкцкрннцюабугюуубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэъуяфшечцюйрщвяхвмкршрпгюопэуцчйтаьэдкцибрьцыяжтюрбуэтэбдуящэубъибрювъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэулькнъщбжяцэьредъьвювлрнуяфуоухфекьгцччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбудэндадъярьеюэлэтчоубъцэфэвлнеэгфдсэвэекбсчоукгаутэыпуббцчкпэгючсаъбэнэфъркацхеваетуфяепьрювържадфежбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжыкгсцбрясшчйотъъжрсщчл.

Задачи

1 Известно, что каждому из трех шифрованных текстов «ЙМЫВОТСЬЛКЪГВЦАЯЯ»,«УКМАПОЧСРКЩВЗАХ»,«ШМФЭОГЧСЙЪКФЬВЫЕАКК» соответствовало исходное сообщение «МОСКВА». Расшифруйте три текста

«ПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ»,

«ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП»,

«РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК»

при условии, что двум из них соответствует одно и тоже сообщение.

2 Расшифруйте фразу, зашифрованную постолбцовой транспозицией, если символ ⌣ используется как знак пробела:

a) «⌣ОНКА⌣БНЫЕЦВЛЕ⌣К⌣ТГОАНЕИР»;

b) «НЗМАЕЕАА⌣Г⌣НОТВОССОТЬЯАЛС»;

c) «РППОЕААДТВЛ⌣ЕБЬЛНЫЕ⌣ПА⌣ВР»;

d) «ОПЗДЕП⌣ИХРДОТ⌣И⌣ВРИТЧ⌣САА»;

e) «ВКЫОСИРЙУ⌣ОЬВНЕ⌣СОАПНИОТС».

3 Расшифруйте фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки), если символ ⌣ используется как знак пробела:

a) «⌣ЙЕСТОВО⌣НИИНЛАЕТИЖДСОПВ⌣»;

b) «НДИАЕОЫЛПНЕ⌣ ⌣НВЕАНГТ⌣ИЗЛА»;

c) «П⌣БИРДЛЬНЕВ⌣ОП⌣ОПЗДЕВЫГЕА»;

d) «МДООИТЕЬ⌣СМТ⌣НАДТЕСУБЕХНО»;

e) «АИНАЛЖНОЛЕШФ⌣ЗИ⌣УАРОЬСНЕ⌣».

4 Шифр *Bid*, имеющий простое правило шифрования, использует в качестве ключа квадратную таблицу, в которую в некотором порядке записаны буквы английского алфавита (буквы I и J отождествлены).

C	O	D	E	A
B	F	G	H	I
K	L	M	N	P
Q	R	S	T	U
V	W	X	Y	Z

Результатом шифрования фразы «SIXTY EIGHT MILES» на приведенном ключе является фраза «RYXXT OFTXT LKSWS». Зашифруйте на том же ключе фразу «ENTER OTHER LEVEL».

5 Получателю было отправлено три письма. В первом письме содержался листочек с квадратной таблицей (a).

a)

Э	А	П	Я	Т	З
Р	О	Е	Т	Ы	О
В	Ш	В	О	Ш	Е
А	Р	И	Т	Е	Ф
Р	К	О	Т	Т	С
А	Н	Я	Н		А

b)

0	X	X	X	0	X
X	0	X	0	X	X
X	X	X	X	0	X
X	X	0	X	X	0
0	X	X	X	X	X
X	X	X	0	X	X

В третьем — листочек с таблицей (b). Второе письмо, содержащее пояснения по использованию этих таблиц, потерялось. Помогите получателю прочитать зашифрованное сообщение.

6 Для зашифровывания текста шифром *поворотная решетка* из бумажного квадрата размером 8 × 8 клеток изготовили трафарет. Первые 16 букв текста сообщения вписали в прорези трафарета (по одной в каждую), потом трафарет повернули на 90 градусов и вписали следующие 16 букв и т. д. Для повышения сложности шифра процедуру шифрования провели дважды. Найдите текст исходного сообщения по шифрованному тексту.

a)

В	Р	И	Е	А	Ь	И	Л
Р	Е	Е	Ы	П	Ы	П	А
О	С	Н	Л	Х	А	Л	Н
Ы	Н	Ф	И	О	О	П	Т
Е	Р	Г	Ь	Р	Д	Г	Ц
Р	Е	Ф	Й	И	К	П	Н
О	А	И	Т	И	С	Ж	Д
Н	О	Л	И	Х	Р	Е	И

c)

А	И	Н	С	З	Е	Н	Ц
О	А	Ш	О	Н	Ф	Ю	З
Е	Л	И	К	И	Н	И	Е
Х	Ь	И	Н	И	Т	Д	Н
Ж	Д	У	О	Е	Н	М	Б
А	И	Ь	О	И	Й	Ф	Е
Ю	Ц	А	О	Й	В	А	Р
Н	Р	А	Э	Р	Л	Л	А

b)

А	Т	Е	И	Л	Я	О	Т
Л	С	Ь	Л	Р	Е	С	А
У	Ю	Р	А	Й	Е	Б	Х
Я	Х	И	С	О	Ш	В	Г
И	В	И	С	К	Л	В	О
Я	И	Ч	И	И	С	М	А
В	З	Б	Ы	С	И	Р	К
Т	С	Р	Г	Д	Р	Ы	Д

d)

Ь	Л	А	В	Е	О	Ж	Н
А	К	Й	Ы	О	О	З	И
Л	Е	Р	Т	З	О	Т	Ы
Ы	Ь	П	С	О	О	М	Ж
Т	З	Л	Ь	О	Е	Е	И
Р	Н	Д	Д	И	Е	Т	Л
Ю	Е	М	Ь	Е	В	С	Б
В	П	А	С	Х	К	Т	Д

e)

И	Ь	М	Н	О	Ж	А	Е
И	В	В	А	Т	Р	Х	К
О	С	Д	Д	Ж	Н	Е	Н
У	С	С	В	Д	М	И	Р
Ж	О	О	Д	В	Е	Т	И
П	Ы	Т	Я	Т	З	О	С
У	О	П	Ж	Т	Н	С	Ч
Е	Е	О	О	К	Я	Я	О

f)

Е	Л	Ь	В	З	Е	И	М
Ы	А	Ф	Н	А	С	К	Е
К	С	Т	А	Т	С	Ч	Л
Ы	С	Ь	Я	Е	Т	У	Д
Н	Р	И	Ч	Ю	Н	С	Е
Е	А	О	Б	П	О	Ш	Ы
Н	Т	Е	А	Е	Р	Е	А
А	Я	О	О	И	Л	Т	Т

7 Для использования шифра *прямоугольная решетка* был изготовлен трафарет размером 6 × 10 клеток. При наложении трафарета на лист бумаги того же размера вписали первые 15 букв текста сообщения в прорези трафарета (по одной в каждую), потом трафарет повернули на 180 градусов и вписали следующие 15 букв, после чего трафарет перевернули «наизнанку» и т.д. Результат шифрования выглядит так.

Е	Е	И	С	А	Т	Ш	С	Я	И
К	О	Р	Т	Л	М	О	Р	Г	Е
Б	К	Б	Р	А	И	Н	И	У	А
О	Ч	К	И	С	Т	У	П	Т	Р
Ы		Е	О	О		С	Р	Л	Ь
Н	З	У	Ы	Ю		К			И

Какой текст был зашифрован?

8 Шифрование фразы на русском языке проходит в два этапа. На первом этапе каждая буква текста заменяется на следующую в алфавитном порядке (последняя заменяется на первую), используется алфавит без Ъ и Ё. На втором этапе применяется шифр простой замены с неизвестным ключом (его применение заключается в замене каждой буквы шифруемого текста буквой того же алфавита, при этом разные буквы заменяются разными буквами). После шифрования фразы был получен следующий шифротекст (пробелы разделяют слова):

a) «ГНПНВТ НРЗКЗС ЗГТШЗИ»;

b) «АЯРЙДСАНК ЗВПЯ ЛЗККЗНМНБ»;

c) «ЛКЬФПЭЛШХ ТНЫК ЦТХХТШЧШМ»;

d) «ОШЫШНЮ ШЬТХТЭ ТОЮДТУ».

По данному шифротексту восстановите открытое сообщение, если известно, что результат шифрования любого открытого сообщения не зависит от порядка выполнения его этапов.

9 Расшифруйте текст, если известно, что каждой букве алфавита соответствует двузначное число.

- 39 25 20 34 82 63 66 46 35 20 25 82 86 39 51 74 35 51 66 20 44 37 25 27 51 35 44 20 90 37 51 25 25 51 63 91 20 11 37 46 48 25 20 37 61 51 14 82 82 66 82 35 29 82 91 25 51 74 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37 37 44 82 31 11 37 82 51 46 25 51 34 82 25 37 82 86 37 25 27 51 35 44 20 90 37 51 25 25 48 44 46 82 78 25 51 14 51 18 37 59 44 51 74 82 35 20 90 37 59 44 66 90 82 25 25 48 44 37 61 10 44 20 18 20 44 37 86 61 20 25 86 51 39 66 86 51 44 10 66 82 86 46 51 35 10 37 66 51 46 51 39 51 63 66 39 59 91 37 56 46 51 86 20 66 20 82 46 66 59 24 35 10 18 37 78 51 35 18 20 25 37 91 20 90 37 63 46 51 66 51 18 14 20 66 25 51 35 82 91 10 14 29 46 20 46 20 44 35 20 91 14 37 56 25 48 78 37 66 66 14 82 24 51 39 20 25 37 63 35 10 86 51 39 51 24 37 46 82 14 37 44 25 51 18 37 78 37 91 25 37 78 91 25 20 31 46 51 61 51 66 25 51 39 25 48 78 39 37 24 20 78 10 18 35 51 91 25 51 25 82 10 24 82 14 59 31 46 24 51 14 42 25 51 18 51 39 25 37 44 20 25 37 59 24 20 25 25 48 44 39 51 74 35 51 66 20 44 66 56 37 46 20 59 56 46 51 51 61 82 66 74 82 56 82 25 37 82 37 25 27 51 35 44 20 90 37 51 25 25 51 63 61 82 91 51 74 20 66 25 51 66 46 37 25 82 37 44 82 82 46 66 44 48 66 14 20 82 66 14 37 51 46 66 10 46 66 46 39 10 82 46 39 37 24 37 44 20 59 10 18 35 51 91 20
- 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53 59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27 50 25 91 32 59 77 95 29 50 25 99 59 25 99 74 29 53 25 59 17 99 25 91 23 49 71 25 17 99 60 49 25 34 32 25 71 95 27 82 27 32 32 25 29 50 17 25 15 77 99 32 59 77 62 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 25 99 95 29 45 49 74 29 62 95 27 63 34 27 71 17 27 12 25 50 27 17 62 27 95 27 50 25 91 32 29 35 95 29 50 25 99 29 17 29 82 49 83 62 25 17 27 50 27 62 95 25 34 59 74 99 25 71 50 27 53 25 62 29 17 32 25 17 99 49 17 71 35 53 29 32 29 17 32 29 15 49 23 49 27 82 32 29 34 27 63 32 25 95 29 50 25 99 29 77 10 27 12 25 25 50 25 95 59 34 25 71 29 32 49 35 49 95 27 53 27 95 71 49 95 25 71 29 32 49 27 82 74 95 49 99 49 23 32 89 83 74 25 99 74 29 53 59 50 15 25 74 25 71 62 49 99 29 32 49 35 49 53 29 62 25 82 49 32 29 77 10 49 83 59 17 99 95 25 91 17 99 71 34 15 35 62 25 17 15 27 34 32 49 83 25 62 99 49 82 29 15 60 32 25 62 95 49 82 27 32 27 32 49 27 34 49 17 74 25 71 89 83 82 29 17 17 49 71 25 71 12 25 95 35 23 27 91 53 29 82 27 32 89 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 89 34 25 17 99 49 12 29 27 99 17 35 25 62 99 49 82 49 53 29 67 49 27 91 62 95 25 12 95 29 82 82 32 25 12 25 25 50 27 17 62 27 23 27 32 49 35

10 Используя частотный анализ букв русского языка, вскройте сообщение, если известно, что различным буквам соответствуют различные двузначные числа. Знаки препинания и некоторые пробелы сохранены для удобства вскрытия.

56 27 54 54 27 56 51 32 82 16 63 49 27 63 11 30 73 35 23 54 89 70 27 63 27 49 32 70 35 16 97 82 1 6 67 73 27 51 30 56 32 63 70 29 63 27 49 32 73 29 54 73 27 48 29 13 29 82 56 82 27 95 54 27 35 27 18 51 29, 97 56 27 70 29 63 30 51 51 35 15 63 89 48 16. 16 63 15 11 51 30 82 29 49 65 27 54 32 63 30 49 29 61 27 63 32 48 30 — 27 56 51 35 15 56 30 23 32 27 11 70 27 35 27 18 32 56 29 63 89 82 30 23, 27 82 30 51 30 51 11 15 73 35 29 54 70 27 49 65 32 38 30 63 30 73 35 32 23 56 82 16 67 70 49 56 35 29 97 16. 82 27 49 51 27 13 51 29 54 30 27 82 27 73 16 49 56 32 63 70 29 63 27 49 32 73 29 54 82 15 95 16 73 27 35 32 70 15 56 30 38 32 63 32 92-73 27 54 11 30 61 30 18 82 32 51 30 49 63 27 18 29 82 82 16 67 61 30 92 29 56 16. 27 82 49 16 82 16 63 61 30 92 29 56 16 73 27 54 13 15 24 51 16 32 70 92 27 24 29 63 73 27 49 56 16 73 29 82 89 51 30 13.

11 Шифрование сообщений состоит в замене букв исходного текста в соответствии с некоторой (известной только отправителю и получателю) таблицей, в первой строке которой выписаны все буквы используемого алфавита в естественном (алфавитном) порядке, а во второй — все буквы того же алфавита в произвольном порядке. Перед шифрованием из текста сообщения удалили все пробелы и знаки препинания. Восстановите исходное сообщение по имеющемуся зашифрованному тексту (для удобства чтения его разбили на группы по пять букв).

ЙЛЙСЭ ВНЛЦЩ ТНАРТ ЦСКЕЛ ХИЦЭК ЦЫЦИП МОНКЕ
ЖКГЁК ЗКДЁК ТЦЩЯР КСАНИ ЦЩТЮЗ НКРЛС ФМТКС
АНШАЁ ЁКЁАЗ КЁИЖЛ ЮЁЛУА ЖКТЁК СЛЁЭА ОККВА
ХЛЁИЮ КВАТЗ АУИЦЩ СЛЖОЛ НЛЁЦИ НКСЛЁ ЁМЯЕЛ
ХИЦМИ ДИЖКГ ЁКТРА ДЛЦЩТ ЛЖКТЦ КЮЦАТ ЩЁЭБК
ТКЕЁЛ ЁЁЭБС ЭВКНС КСЦКН КЖТДМ УЛАСЛ ЖЁАКВ
КБЦИТ ЩВАЕЕ ЁЛЁИБ ЁЛМУЁ ЭПКТЁ КСЙНИ ЗЦКОН
КЛЦИИ

12 Для шифрования сообщения используют неизвестную последовательность целых чисел. Каждую букву сообщения заменяют ее порядковым номером в алфавите: А — на 1, ..., Я — на 33, затем прибавляют к полученному номеру очередной член последовательности и, наконец, выписывают остаток от деления этой суммы на 33. При реализации указанного алгоритма получилось вот такое шифрованное сообщение: 22 24 23 27 2 3 3 9 18 25 1 18 18 8 12 32 6 32 23.

Если бы при шифровании того же самого сообщения вместо сложения с членами заданной последовательности мы производили вычитание, то был бы получен такой результат:

14 11 15 7 1 9 7 3 8 20 29 2 27 16 14 32 11 13 32.

Найдите исходное сообщение.

13 При шифровании исходного сообщения каждую его букву заменили одной либо двумя цифрами, причем одинаковые буквы всегда заменяли одной и той же цифрой или парой цифр. Полученную последовательность разбили на группы по пять цифр для удобства записи. Найдите исходное сообщение по данному шифрованному тексту.

40745 21618 52412 92008 62528 72621 41386
44415 44214 34922 41612 21322 43150 85412
14341 64725 40212 11328 68541 93552 38321
40222 18141 52854 02144 40540 21417 28213
02298 72625 54347 32243 15047 52540 52940
74440 53645 53417 12241 92872 84787 02223
52347 28147 53417 44223 05415 02120 28545
21621 24221 22022 74822 46651 74040 54347
35523 83214 22829 22292 34728 12202 24422
32103 41544 02287 96214 02286 28622 45415
20674 65122 28222 92951 74022 21672 90224
44085 49305 34550 54932 24315 05140 21473
05264 08621 26408 24667

14 При зашифровывании исходного сообщения каждый его символ (букву или пробел) заменяли одной либо двумя цифрами, причем одинаковые символы всегда заменяли одинаково. Для удобства записи полученную последовательность сгруппировали по пять цифр. Найдите исходное сообщение по данному шифрованному тексту.

14939 21803 25872 18125 86808 62163 49258 62581 21432
42921 29325 43204 08781 32545 81127 81208 56212 57270
32508 74986 21478 04349 32547 49874 92128 25866 43246
21472 98325 81443 64725 74947 47293 80254 46125 45246
72749 24802 16202 84781 23812 54381 47214 94321 49254
26125 27149 80347 81832 54524 81276 24438 02580 25446
12545 24672 74924 80216 20284 78123 81258 14436 47492
54349 43818 32520 80448 12580 47268 12434 95806 83252
78685 25476 81442 28178 03498 52572 08525 45818 62920
43802 54180 26248 12749 47478 12381 25868 18144 42647
80852 58047 26812 43495 80852 58144 42678 18621 04547

15 Шифротекст

А М И М О П Р А С Т Е Т И Р А С И С П Д
И С А Ф Е И И Б О Е Т К Ж Р Г Л Е О Л О
И Ш И С А Н Н С Й С А О О Л Т Л Е Я Т У
И Ц В Ы И П И Я Д П И Щ П Ь П С Е Ю Я Я

получен из исходного сообщения перестановкой его букв. Текст

У Щ Ф М Ш П Д Р Е Ц Ч Е Ш Ю Ш Ч Д А К Е
Ч М Д В К Ш Б Е Е Ч Д Ф Э П Й Щ Г Ш Ф Щ
Ц Е Ю Щ Ф П М Е Ч П М Е Р Щ М Е О Ф Ч Щ
Х Е Ш Р Т Г Д И Ф Р С Я Ы Л К Д Ф Ф Е Е

получен из того же исходного сообщения однозначной заменой каждой буквы на другую. Восстановите исходное сообщение.

16 Для проверки телетайпа, печатающего буквами русского алфавита «АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ», передан набор из 9 слов, содержащий все 33 буквы алфавита. В результате неисправности телетайпа на приемном конце получены слова «ГЪЙ АЭЕ БПРК ЕЖЩЮ НМЬЧ СЫЛЗ ШДУ ЦХОТ ЯФВИ». Восстановите исходный текст, если известно, что характер неисправности таков, что каждая буква заменяется буквой, отстоящей от нее в указанном алфавите не дальше, чем на две буквы (например, буква Б может перейти в одну из букв А, Б, В, Г).

17 В результате перестановки букв сообщения получена криптограмма «БТИПЧЬЛОЯЧЫЬТОТПУНТНОНЗЛЖАЧОЬОТУНИУХНИППОЛОЬЧОЕЛОЛС». Прочтите исходное сообщение, если известно, что оно было разбито на отрезки одинаковой длины r, в каждом из которых буквы были переставлены по следующему правилу: буква отрезка, имеющая порядковый номер x ($x = 1,2,\ldots,r$), в соответствующем отрезке криптограммы имеет порядковый номер $f(x) = REST(ax + b, r)$, где a и b — некоторые натуральные числа, а величина $REST(ax + b, r)$ равна остатку от деления суммы $ax + b$ на r, если этот остаток не равен нулю, и r, если остаток равен нулю.

18 *Одноразовый блокнот* — ключ шифра Вернама, обладающий тремя критически важными свойствами: генерироваться с помощью случайных чисел (то есть иметь случайное равномерное распределение: $P_k(k) = \frac{1}{2^N}$, где k — ключ, а N — количество бинарных символов в ключе); совпадать по размеру с заданным открытым текстом; применяться только один раз. Какие из рассмотренных нами шифров наиболее близки шифру Вернама? Как нужно модифицировать использование тех или иных изученных шифров, чтобы приблизить их свойства к свойству шифра Вернама? В чем преимущества и недостатки практического использования одноразового блокнота в шифровании?

1.3. Задачи криптографических олимпиад

Примеры решения задач

Пример 1.3.15 Формулировка некоторого геометрического утверждения была вписана в клетки таблицы 10×10 построчно слева направо, начиная с верхней левой клетки. Знак переноса на следующую строку не ставился, но между соседними словами одной строки помещалась пустая клетка. Решили переставлять буквы в отдельных столбцах, сдвигая их все на одну позицию вверх и перенося самую верхнюю букву вниз (при этом пустую клетку также считая буквой). Иногда меняли местами сразу все строки, симметричные относительно средней линии, а именно 1-ю с 10-й, 2-ю с 9-й и т.д., после чего снова брались за передвижение букв в столбцах. В результате таблица приняла представленный на рисунке вид. Прочитайте исходное геометрическое утверждение.

А	Л	П	Н	В	И		В	Т	Р
Е	О	С	Н	Л	Я		О	Л	Т
П		Я	Л	Ы	Е	О	Ы	Т	У
Е	О	А	О	Щ	Д	Р	Р	А	Е
Н	Р	У	И		О	Н	С	Т	В
П	К	И	М	Е	Ь		Р		
Е	В	О	Ю	Т	Х	Х	Н	А	С
Д	С	Е	Х	И	И	Е	О	Я	
О	К	Ь	Т	Ы	П	Ь	П	Е	Н
С	Ж	С	С	Е	Л		О	О	О

Решение Будем решать эту задачу перебором, вырезав из бумаги три полосы, соответствующие первым трем строкам таблицы. Используем попытки «увидеть» в зашифрованном тексте какое-либо слово, имеющее отношение к геометрической тематике, например, «*прямая*», «*точка*» и т.п., учитывая естественное соображение: круг слов, используемых в геометрических текстах, существенно ограничен. Сузим набор операций сдвига букв в столбцах и отражения столбца относительно средней линии: сдвинуть столбец на одну позицию вверх и затем отразить — это все равно, что столбец сначала отразить, а затем сдвинуть вверх на девять позиций, поэтому можно считать, что сначала мы передвигали буквы в столбцах, а затем, может быть, один раз отразили таблицу относительно средней линии.

Рассмотрим букву «Я» в предпоследнем столбце. Перед ней могут стоять буквы «О», «П», «Н», «Р», «С», «Ы», «В». Сочетание «ОЯ» встречается в математических текстах в слове «*постоянная*», но необходимой буквы «Т» в седьмом столбце нет. Сочетание «РЯ» может быть частью слова «*прямая*», но в седьмом столбце нет «Р». Сочетания «*касающихся*», «*пересекающихся*» представляются наиболее вероятным, и присутствие буквы «Щ» в пятом столбце тому подтверждение. После того как столбцы с пятого по девятый выстроены так, чтоб прочитывалось «ЩИХСЯ», получение ответа становится совсем простым делом.

П	О	С	Л	Е	Д	О	В	А	Т
Е	Л	Ь	Н	Ы	Е		О	Т	Р
А	Ж	Е	Н	И	Я		П	Л	О
С	К	О	С	Т	И		О	Т	Н
О	С	И	Т	Е	Л	Ь	Н	О	
Д	В	У	Х		П	Е	Р	Е	С
Е	К	А	Ю	Щ	И	Х	С	Я	
П	Р	Я	М	Ы	Х		Р	А	В
Н	О	С	И	Л	Ь	Н	Ы		Е
Е		П	О	В	О	Р	О	Т	У

□

Пример 1.3.16 Для шифровании текста $v_1, v_2, \ldots, v_k$ на русском языке каждую его букву v_i заменили числом t_i согласно таблице.

v_i	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
t_i	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
v_i	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	
t_i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

К каждому числу t_i последовательности $t_1, t_2, \ldots, t_k$ прибавили число a_i последовательности $a_1, a_2, \ldots, a_k$, заданной соотношениями $a_1 = 1$, $a_{n+1} = 3a_n + 4$ при $n > 0$. Затем остаток от деления каждой суммы $t_i + a_i$ на 33 вновь заменили буквой по той же таблице. При переписывании зашифрованного текста несколько букв были пропущены. В результате получилось вот что: «РЧЖЬЭТСЪЙЛЖЪЯОШКС». Найдите исходный текст.

Решение Заменяя каждый член последовательности $a_1 = 1$, $a_{n+1} = 3a_n + 4$ остатком от его деления на 33, получим последовательность 1, 7, 25, 13, 10, 1, 7, 25, 13, 10, ... Так как каждый член этой последовательности остатков однозначно находится из предыдущего, заключаем, что ее период равен пяти.

Будем вычитать из чисел, соответствующих буквам зашифрованного текста, числа этой периодической последовательности, а результаты заменять буквами согласно данной в условии задачи таблице.

Р	Ч	Ж	Ь	Э	Т	С	Ъ	Й	Л	...
17	24	7	29	30	19	18	27	10	12	...
1	7	25	13	10	1	7	25	13	10	...
16	17	15	16	20	18	11	2	30	2	...
П	Р	О	П	У	С	К	В	Э	В	...

После слова «ПРОПУСК» идет нечитаемый текст. Значит, или непосредственно после этого слова, или после буквы «В» пропущены буквы. (Перебор различных вариантов тривиален и поэтому здесь не приводится.) Сдвигая нашу периодическую последовательность относительно зашифрованного текста, находим такой вариант.

17	24	7	29	30	19	18		27	10	12	7	27	32	15	25	11	18
Р	Ч	Ж	Ь	Э	Т	С		Ъ	Й	Л	Ж	Ъ	Я	О	Ш	К	С
1	7	25	13	10	12	7	25	13	10	1	7	25	13	10	1	7	25
16	17	15	16	20	18	11		14	0	11	0	2	19	5	24	4	26
П	Р	О	П	У	С	К		Н	А	К	А	В	Т	Е	Ч	Д	Щ

Естественно предположить, что на месте пропущенного знака в исходном тексте находилась буква «З». Действуя далее аналогично, восстанавливаем весь текст

17	24	7	29	30	19	18		27	10	12	7	27	32	15		25	11	18
Р	Ч	Ж	Ь	Э	Т	С		Ъ	Й	Л	Ж	Ъ	Я	О		Ш	К	С
1	7	25	13	10	12	7	25	13	10	1	7	25	13	10	1	7	25	13
16	17	15	16	20	18	11		14	0	11	0	2	19	5		18	19	5
П	Р	О	П	У	С	К		Н	А	К	А	В	Т	Е		С	Т	Е

ПРОПУСК ЗНАКА В ТЕКСТЕ □

Пример 1.3.17 Каждую букву исходного сообщения заменили ее двузначным порядковым номером в русском алфавите согласно таблице.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

Полученную числовую последовательность разбили на трехзначные цифровые группы без пересечений и пропусков. Каждое из полученных трехзначных чисел умножили на 77 и оставили только три последние цифры произведения. В результате получилась последовательность «317564404970017677550547850355». Восстановите исходное сообщение.

Решение Для нахождения последней буквы исходного сообщения необходимо решить сравнение $77n \equiv 355 \pmod{1000}$: здесь n пока неизвестное трехзначное число.

Пусть $n = 100a + 10b + c$, где a, b, c — цифры его десятичной записи. Тогда $77(100a + 10b + c) \equiv 355 \pmod{1000} \Leftrightarrow 7000a + 700b + 70c + 700a + 70b + 7c \equiv 355 \pmod{1000} \Leftrightarrow 700(a+b) + 70(b+c) + 7c \equiv 355 \pmod{1000}$.

Значит, $c = 5$. Далее, $700(a+b) + 70b + 30 \equiv 0 \pmod{1000}$. Отсюда $b = 1$. Тогда $700a + 800 \equiv 0 \pmod{1000}$. Значит, $a = 6$, и поэтому $n = 615$.

Сравнение $77n \equiv 355 \pmod{1000}$ могло быть решено иначе. Умножив обе части его на 13, получим $1001n \equiv 13 \cdot 355 \pmod{1000}$. Ясно, что последние три цифры числа, стоящего в левой части равенства, совпадают с тремя последними цифрами самого числа n. Вычислив $13 \cdot 355 = 4615$, найдем $n = 615$.

Теперь аналогично решаем сравнение, в правой части которого стоят другие трехзначные цифровые группы шифрсообщения (850, 547, 550 и т. д.).

Искомая цифровая последовательность имеет вид «121332252610221-801150111050615», что позволяет получить исходное сообщение «КЛЮЧ-ШИФРАНАЙДЕН». □

Пример 1.3.18 Для доступа к управлению параметрами своего счета клиенту банка необходимо связаться по телефону с банком и набрать семизначный пароль. После первой же неправильно набранной цифры пароля банк прерывает телефонное соединение. Как надо действовать, чтобы за наименьшее число попыток подобрать пароль?

Решение Цифры пароля будем подбирать последовательно. Свяжемся с банком и наберем цифру 0. Если связь не оборвалась, то первая цифра пароля — ноль. Если связь прервана, то первая цифра отлична от 0 и, связываясь заново с банком, пробуем набрать 1, и т.д. Не позднее чем через девять звонков мы будем точно знать, какая цифра стоит на первом месте в пароле, и сможем перейти к подбору второй цифры. Общее число звонков, которое понадобится для выяснения пароля, не превосходит $7 \cdot 9 = 63$. Еще один звонок может понадобиться для получения доступа после полного выяснения пароля. □

Замечание. *Если бы решение о доступе или отказе принималось только после ввода всего пароля, то система защиты была бы гораздо надежнее — последовательный подбор был бы невозможен, и потенциально пришлось бы перебирать все* $10^7 = 10000000$ *вариантов пароля.*

Пример 1.3.19 Центральный замок автомобиля открывается и закрывается с помощью брелка. При получении сигнала брелка замок открывается (если был закрыт) или закрывается (если был открыт). В брелке и замке имеются счетчики (назовем их *СБ* и *СЗ*), на которых изначально было выставлено одно и то же число. Пусть N — текущее значение *СБ*. При нажатии на кнопку брелка *СБ* меняет значение на $N + 1$, старое же значение N в зашифрованном виде передается замку. Микрокомпьютер замка расшифровывает полученный сигнал и находит число, переданное брелком. Если это число равно или превосходит значение *СЗ*, то замок срабатывает, а *СЗ* принимает значение $N + 1$. Если это число оказывается меньше или при расшифровании обнаруживается ошибка, то замок остается в прежнем состоянии. Злоумышленник способен запоминать сигналы брелка; поставив помеху, искажать сигналы брелка (при этом сам злоумышленник получает сигнал без искажений); посылать замку ранее запомненные сигналы. Как злоумышленнику открыть замок, если алгоритмы шифрования и дешифрования ему неизвестны?

Решение Приведенный в задаче протокол работы брелка и замка был изобретен в ЮАР и практически без изменения использовался во многих известных противоугонных системах. Достаточно продолжительное время уязвимость этого протокола не была замечена. Перейдем собственно к решению, пояснив предварительно одно из условий задачи: если $СБ = k$ и $СЗ = m$, где $k \geqslant m$, то при нажатии на кнопку брелка и срабатывании замка счетчик замка принимает значение не $m + 1$, а $k + 1$. Это сделано для того, чтобы один и тот же сигнал брелка не мог быть использован дважды.

Запишем теперь по пунктам действия злоумышленника.

- Пусть замок открыт. Владелец хочет запереть машину и уйти. Пусть $СБ = k$ и $СЗ = m$, где $k \geqslant m$. Владелец нажимает кнопку брелка. Злоумышленник запоминает посланный сигнал k и ставит помеху. В результате получаем, что $СБ = k+1$ и по-прежнему $СЗ = m$, т.е. замок не закрылся.
- Заметив, что машина не заперта, владелец повторно нажимает кнопку брелка. Злоумышленник снова запоминает сигнал $k+1$ брелка и опять ставит помеху. В этот момент $СБ = k + 2$, а замок так и остается открытым, т. е. $СЗ = m$.
- Выполнив действия предыдущего пункта, злоумышленник немедленно посылает замку ранее запомненный сигнал k. Замок закрывается, и $СЗ = k + 1$. Владелец уходит, полагая, что машину запер он сам.
- Злоумышленник посылает замку ранее запомненный сигнал $k + 1$, и замок открывается. □

Задачи

1 Можно ли создать проводную телефонную сеть связи, состоящую из 993 абонентов, каждый из которых был бы связан ровно с 99 другими?

2 Кодовая комбинация сейфа устанавливается на внутренней стороне дверцы с помощью трех дисков. Каждый из них может быть установлен в одно из 20 положений, пронумерованных числами от 0 до 19, поворотом по часовой стрелке. В начальный момент диски установлены в положение (0, 0, 0). За положение с номером 19 диск не поворачивается. При повороте каждого диска на одно положение раздается щелчок. Сравните число возможных ходовых комбинаций, при установке которых раздается 33, 32, 25 щелчков.

3 Два криптографа выясняют, чей шифр содержит больше ключей. Первый говорит, что ключ его шифра состоит из 50 упорядоченных символов, каждый из которых принимает 7 значений. Второй говорит, что ключ его шифра состоит всего из 43 упорядоченных символов, зато каждый из них принимает 10 значений. Чей шифр содержит больше ключей?

4 В первую строку таблицы размером 3×10 вписали 10 различных букв 30-буквенного русского алфавита (Е и Ё, И и Й, Ь и Ъ отождествлены). Затем все оставшиеся буквы в естественном порядке (построчно сверху вниз, слева направо) вписали в свободные клетки таблицы. Алгоритм шифрования по заданной таблице следующий: из номеров

столбцов таблицы с буквами открытого сообщения составим натуральное число и умножим его на 9. Первую, вторую, третью и т.д. цифры полученного числа будем рассматривать как последовательные номера столбцов таблицы, в которых находятся первая, вторая, третья и т.д. буквы шифротекста. Последовательные номера строк таблицы, в которых находятся буквы шифротекста, определяются набором соответствующих номеров строк с буквами исходного слова, к которому слева приписывается 1, если число цифр произведения больше числа букв исходного слова. Можно ли слово «АСТРАХАНЬ» зашифровать с помощью такой таблицы в слово «БУТЕРБРОД»?

5 Исходное сообщение, состоящее из букв русского алфавита и знака ⌣ пробела между словами, преобразуется в цифровое сообщение заменой каждого его символа парой цифр согласно следующей таблице.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	⌣	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	

Для шифрования используется отрезок последовательности $A_1 = 3$, $A_{k+1} = A_k + 3(k^2 + k + 1)$ для любого натурального k, начинающийся с некоторого фиксированного члена A_m. При шифровании каждая цифра сообщения складывается с соответствующей цифрой отрезка и заменяется последней цифрой полученной суммы. Восстановите сообщение «233986721645816067061731558 8».

6 Преобразование цифрового текста заключается в том, что каждая его цифра заменяется остатком от деления значения многочлена $f(x) = a(x^3 + 4x^2 + 4x + b)$ на число 10, где a и b — фиксированные натуральные числа. Выясните, при каких значениях a и b указанное преобразование допускает однозначное дешифрование.

7 Пусть x_1 и x_2 — корни трехчлена $x^2 + 3x + 1$. Для шифрования открытого текста, записанного в 31-буквенном русском алфавите (не используются буквы Ё и Ъ), к порядковому номеру каждой его буквы прибавим значение многочлена $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$, вычисленное либо при $x = x_1$, либо при $x = x_2$, а затем заменим полученное число соответствующей ему буквой. Зашифруйте этим методом сообщение «НАС УТРО ВСТРЕЧАЕТ ПРОХЛАДОЙ». Расшифруйте сообщение «ДЮСРНПЗПР».

8 Цифры $0, 1, \ldots, 9$ разбиты на несколько непересекающихся групп. Из цифр каждой группы составлены всевозможные числа, для записи каждого из которых все цифры группы используются ровно один раз (учитываются и записи, начинающиеся с нуля). Все полученные числа расположены в порядке возрастания, и k-му числу поставлена в соответствие k-я буква алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ При реализации данного алгоритма оказалось, что каждой букве соответствует число и каждому числу соответствует некоторая буква. Шифрование сообщения осуществляется заменой каждой буквы соответствующим ей числом. Если ненулевое число начинается с нуля, то при шифровании этот нуль не выписывается. Восстановите сообщение «873146507381» и укажите таблицу замены букв числами.

9 Дана криптограмма.

ФН	×	Ы	=	ФАФ
+		×		-
ЕЕ	+	Е	=	НЗ
=		=		=
ИША	+	МР	=	ИМН

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют разные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите исходный текст.

10 В нашем распоряжении имеется два сейфа. Первый содержит 100 переключателей по два положения каждый, второй — 8 переключателей по 100 положений каждый. Сейф открывается только при полном совпадении. Какой сейф надежнее и почему?

11 Клетки магического квадрата размера 4×4 с единицей в правом нижнем углу заполнили буквами некоторого сообщения так, что его первая буква попала в клетку с номером 1, вторая — в клетку с номером 2 и т. д. В результате построчного выписывания букв заполненного квадрата (слева направо и сверху вниз) получилась последовательность букв «ЫРЕУСТЕ ВЬТАБЕВКП». Зная, что существует ровно четыре таких магических квадрата, расшифруйте данное шифрованное сообщение.

12 Клетку таблицы размера 8×8 назовем «хорошей», если все остальные клетки таблицы можно замостить прямоугольниками 3×1.

Укажите все «хорошие» клетки таблицы.

Сообщение, записанное в 33-буквенном русском алфавите, числовыми аналогами символов которого являются числа 0–32, зашифровано шифром Тритемиуса по правилу, определяемому некоторым ключевым словом. Во все клетки таблицы, за исключением «хороших», построчно вписаны буквы шифрованного текста, а в «хорошие» клетки — буквы ключевого слова. Найдите ключевое слово и восстановите исходное сообщение по приведенной таблице.

Щ	Е	Д	Е	Ю	У	Я	Б
Б	В	Ш	А	Р	Ш	Д	Н
П	Ь	Р	Щ	Е	У	В	Ё
Ъ	Й	Л	Ё	И	Ж	Щ	Е
Д	Е	Ю	У	В	К	Ч	Ч
С	Б	С	Г	Е	Ь	Р	Е
Ш	В	Й	Е	С	В	Ь	О
З	Ю	Ь	Ь	А	Ь	З	Ь

13 В банке работают девять директоров, причем они не очень-то доверяют друг другу. Главный сейф банка открывается в том и только том случае, когда все его замки открыты. Для каждого замка можно изготовить необходимое число копий ключа. Какое наименьшее число замков должно быть у сейфа и как надо распределить ключи между директорами, чтобы сейф мог быть открыт, только если вместе соберутся не менее 5 директоров?

14 Один из девяти директоров банка (см. предыдущую задачу) был избран председателем, в связи с чем потребовалось внести изменения в конструкцию сейфа: нужно, чтобы сейф могли открыть не только любые пять собравшихся вместе директоров, но и любой директор вместе с председателем. При этом группа из менее чем пяти директоров, среди которых нет председателя, либо председатель в одиночку не должны иметь возможность открыть сейф. Какое наименьшее число замков надо установить на двери сейфа и каким образом раздать ключи директорам для реализации указанных правил доступа к содержимому сейфа?

15 Числа, расположенные в клетках таблицы, указывают, сколько соседних по горизонтали, вертикали и диагонали клеток (включая ту, в которой находится само число) должны быть окрашены. Восстановите картину, которой соответствуют эти числа.

	5		2		0		0	1		2		1
		5		3			3			5		
3		4							6			4
			5	3		3				5		
				2		3	3	3	2			1
2		2								0		
	0		3		5				3			0
						3				1		
	1	3										
0				9			7		8		2	
		6			6							
	3									6		0
0			6			5						

16 В центральном компьютере сети пейджинговой связи имеется вирус. Он преобразует сообщения так, что все буквы передаются без искажений, а каждая цифра несколько раз шифруется, причем количество шифрований равно абонентскому номеру получателя сообщения. Кроме того, раз в день таблица шифрования меняется на другую. Как выбрать абонентский номер так, чтобы не зависеть от действий вируса? Найдите все такие номера.

17 Чтобы не забыть секретную комбинацию цифр, открывающую сейф, зашифруем ее и запишем результат в ежедневник. Для шифрования выпишем цифры в таблицу, после чего несколько раз наугад переставим столбцы этой таблицы, запомнив при этом способ перестановки. Переставим столбцы тем же способом еще раз и запишем окончательный результат. Полученная таблица выглядит так.

4	5	6	2	2	0
2	9	0	1	9	9

Во сколько раз знание таблицы из ежедневника упростит вскрытие сейфа?

18 Перед шифрованием сообщения каждую его букву заменили двумя цифрами в соответствии с ее порядковым номером в алфавите, под полученной строкой цифр выписали еще одну строку, в которой встречаются только цифры 1 и 2, а затем сложили цифры в каждом столбце и записали остатки этих сумм при делении на 10. При реализации указанного алгоритма получилась цифровая последовательность «29173018132839332553371832». Найдите исходное сообщение.

19 В первую строку таблицы размером 3×10 вписали 10 различных букв 30-буквенного русского алфавита (Е и Ё, И и Й, Ь и Ъ отождествлены). Затем все оставшиеся буквы в естественном порядке (построчно сверху вниз, слева направо) вписали в свободные клетки таблицы. Алгоритм шифрования по заданной таблице следующий: из номеров столбцов таблицы с буквами открытого сообщения составим натуральное число и умножим его на 9. Первую, вторую, третью и т. д. цифры полученного числа будем рассматривать как последовательные номера столбцов таблицы, в которых находятся первая, вторая, третья и т. д. буквы шифротекста. Последовательные номера строк таблицы, в которых находятся буквы шифротекста, определяются набором соответствующих номеров строк с буквами исходного слова, к которому слева приписывается 1, если число цифр произведения больше числа букв исходного слова. Постройте шифрующую таблицу указанного вида и зашифруйте с помощью указанного криптографического алгоритма слово «РУСЬ»; сообщение «МАТЕМАТИКА ЦАРИЦА НАУК».

20 При установке кодового замка каждой из 26 английских букв, расположенных на его клавиатуре, сопоставляется произвольное натуральное число, известное лишь обладателю замка. Условие сопоставления разным буквам разных чисел не обязательно. После набора произвольной комбинации попарно различных букв происходит суммирование числовых значений, соответствующих набранным буквам. Замок открывается, если сумма делится на 26. Докажите, что для любых числовых значений букв существует комбинация, открывающая замок.

21 Для изображения Моны Лизы в квадратной таблице размера 15×15 каждую ее клетку покрасили белой или черной краской. Назовем подряд идущие клетки одного цвета строки или столбца таблицы полосой, а число клеток в полосе — ее длиной. Восстановите изображение по известным длинам полос черного цвета в каждой строке и в каждом столбце (следующих соответственно сверху вниз и слева направо).

Информация по строкам: 9; 11; 1, 1; 2, 3, 3, 2; 2, 2; 2, 1, 1, 1, 2; 2, 1, 2; 2, 2; 1, 5, 1; 2, 3, 2; 2, 2; 7; 1, 1; 6, 6; 1, 4, 1, 4, 1.

Информация по столбцам: 1; 5, 1; 9, 2; 2, 2, 2; 2, 1, 2, 2; 2, 1, 1, 1, 1, 2; 2, 1, 2, 3; 2, 2, 2, 1, 1; 2, 1, 2, 3; 2, 1, 1, 1, 1, 2; 2, 1, 2, 2; 2, 2, 2; 9, 2; 5, 1; 1.

22 Знаменитый математик Леонард Эйлер в 1759 г. нашел замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно по одному разу. Прочтите текст, вписанный в клетки шахматной доски по такому маршруту, если начало текста расположено в клетке A4.

Д	Л	Р	И	Л	П	Н	Б
У	К	А	О	Т	У	С	Т
О	О	О	А	Н	О	И	Р
Т	Б	Г	К	Т	Т	У	К
К	О	Е	О	Р	А	В	О
К	Д	Г	П	В	Л	Е	Т
Т	А	Н	Р	М	А	Г	О
Е	А	О	В	И	Д	У	Л

23 Пользователи сети связи для обеспечения секретности сообщений выбирают (независимо друг от друга) пары преобразований $(E; D)$, одно из которых, E (открытый ключ), публикуют в справочнике, а второе, D (личный ключ), держат в секрете. Известно, что значения $E(m)$ и $D(n)$ легко вычислить для любых сообщений m и n, причем из равенства $E(m) = n$ следует, что $D(n) = m$. В то же время нахождение m по $E(m)$ является сложной задачей, которую невозможно решить (любыми средствами) за реальное время, если неизвестно D. Если пользователь A хочет послать пользователю B сообщение m, он берет из справочника открытый ключ EB пользователя B, вычисляет $n = EB(m)$ и посылает n к B. Получив n, B вычисляет $DB(n) = m$. Злоумышленник, перехвативший n, не сможет вычислить m. Это гарантирует секретность информации. Вкладчик предложил банкиру способ передачи секретных сообщений с уведомлением о получении: A передает B сообщение $(A; EB(m))$; B, получив сообщение, вычисляет m и направляет A уведомление $(B; EA(m))$. Банкир возразил вкладчику, что этот способ не обеспечивает секретности информации от любого пользователя, который может перехватывать сообщения и как угодно их изменять. Дополнительно потребовав, чтобы для каждого преобразования E было сложно подобрать пару $(m; n)$, для которой $E(m) = E(n)$, банкир предложил вкладчику свой способ: A передает B сообщение $EB(A; m)$; B, получив сообщение, находит m и направляет A уведомление $EA(B; m)$. Объясните, почему способ банкира лучше способа вкладчика.

Литература к главе 1

При подготовке текста главы 1 были использованы следующие источники [3], [6–12], [18], [24], [25], [27], [30], [35], [39–42], [44–47], [53–55], [57], [62], [78–81], [83–85], [87], [89], [96], [119], [128].

Глава 2

Простейшие симметричные криптосистемы

Рассмотрев исторические аспекты развития криптографии, в этой главе мы переходим к систематическому изложению математических основ теории защиты информации.

Как и ранее, будем называть предназначенное для пересылки сообщение *открытым текстом*, а замаскированное сообщение — *шифротекстом*, процесс преобразования открытого текста в шифротекст — *шифрованием*, а обратную процедуру — *дешифрованием*.

Открытый текст и шифротекст записываются в некоторых алфавитах; обычно, но не всегда, эти алфавиты совпадают. Открытый и шифрованный тексты разбиваются на *элементы*. Элементами могут служить как отдельная буква, так и пара (*биграмма*), и тройка (*триграмма*) букв или даже блок из, например, 64 букв.

Шифрующее преобразование является функцией, которая преобразует элемент открытого текста в элемент шифротекста. Другими словами, это отображение f из множества X всех возможных элементов открытого текста в множество Y всех возможных элементов шифротекста:

$$f : X \to Y.$$

Дешифрующее преобразование действует в обратном направлении, восстанавливая открытый текст по шифротексту. Это функция f^{-1}, обратная к функции f:

$$f^{-1} : Y \to X.$$

Описанный способ шифрования называется *симметричной криптосистемой*, поскольку для шифрования и расшифровывания применяется один и тот же криптографический ключ (точнее, ключ шифрования может быть рассчитан по ключу дешифрирования, и наоборот).

2.1. Аффинные криптосистемы

К числу простейших симметричных криптосистем принадлежат *аффинные криптосистемы*, основанные на использовании так называемых *аффинных преобразований*.

Пусть $x \in X$ — элемент открытого текста, a и b — некоторые целые числа, по модулю не превосходящие N — мощность используемого алфавита. Тогда отображение $f : X \to Y$, осуществляемое по закону

$$f(x) \equiv ax + b \pmod{N},$$

называется *аффинным преобразованием с ключами a и b* [53].

Важными частными случаями аффинного преобразования являются *линейное преобразование*

$$f(x) \equiv ax \pmod{N},$$

соответствующее случаю $b = 0$, и *сдвиг*

$$f(x) \equiv x + b \pmod{N},$$

соответствующий случаю $a = 1$. Нетрудно видеть, что сдвиг является ничем иным, как математическим выражением шифра Цезаря.

Пример 2.1.1 Зашифруем сообщение «КРИПТОГРАФИЯ», записанное в 33-буквенном русском алфавите, используя аффинное отображение с ключами шифрования $a = 7, b = 4$.

Первая буква слова К имеет в алфавите порядковый номер 11 (нумерация букв начинается с нуля). Выполним преобразование

$$7 \cdot 11 + 4 = 81 \equiv 15 \pmod{33}$$

и убедимся, что 15-я буква в алфавите — это О. Таким образом, буква К переходит в ходе преобразования в букву О.

Аналогичным образом получим, что

Р $(7 \cdot 17 + 4 = 123 \equiv 24 \pmod{33})$ перейдет в Ч;

И $(7 \cdot 9 + 4 = 67 \equiv 1 \pmod{33})$ перейдет в Б;

П $(7 \cdot 16 + 4 = 116 \equiv 17 \pmod{33})$ перейдет в Р;

Т $(7 \cdot 19 + 4 = 137 \equiv 5 \pmod{33})$ перейдет в Е;

О $(7 \cdot 15 + 4 = 109 \equiv 10 \pmod{33})$ перейдет в Й;

Г $(7 \cdot 3 + 4 = 25 \equiv 25 \pmod{33})$ перейдет в Ш;

А $(7 \cdot 0 + 4 = 4 \equiv 4 \pmod{33})$ перейдет в Д;

Ф $(7 \cdot 21 + 4 = 151 \equiv 19 \pmod{33})$ перейдет в Т;

Я $(7 \cdot 32 + 4 = 228 \equiv 30 \pmod{33})$ перейдет в Э.

Другими словами, заменяя символы слова «КРИПТОГРАФИЯ» их числовыми эквивалентами, мы получим последовательность «11 17 9 16 19 15 3 17 0 21 9 32», переходящую в ходе аффинного преобразования в последовательность «15 24 1 17 5 10 25 24 4 19 1 30» числовых эквивалентов шифротекста «ОЧБРЕЙШЧДТБЭ».

Аффинные криптосистемы относятся к симметричным криптосистемам, т. е. обладают обратным преобразованием. Для того чтобы найти такое преобразование, надо выразить $y = f(x)$ через x:

$$y \equiv ax + b \pmod N,\ y - b \equiv ax \pmod N,\ x \equiv a^{-1}(y - b) \pmod N.$$

Для поиска a^{-1} необходимо решить сравнение $at \equiv 1 \pmod N$, которое имеет ровно одно решение в случае $(a, N) = 1$.

Этот результат следует из *теоремы о линейных сравнениях* [36], которая утверждает, что *линейное сравнение* $ax \equiv b \pmod n$ *имеет ровно одно решение, если* $(a, n) = 1$, *ровно* d *решений, если* $(a, n) = d$, $d|b$, *и не имеет решений в остальных случаях.*

Таким образом, мы получаем *условие существования дешифрующего (обратного аффинного) преобразования: если* $(a, N) = 1$, *то обратное аффинное отображение существует и имеет вид*

$$x \equiv a' \cdot f(x) + b' \pmod N, \text{ где } a' = a^{-1},\ b' = -a^{-1} \cdot b. \qquad \square$$

Пример 2.1.2 Найдем обратное преобразование для аффинного отображения

$$y \equiv 4x + 3 \pmod 7.$$

Сначала найдем $a' = a^{-1}$ из сравнения $4t \equiv 1 \pmod 7$. Поскольку $(4, 7) = 1$, то сравнение имеет единственное решение по модулю 7. Рассмотрим несколько способов его нахождения.

1. Последовательно перебирая числа 0, 1, 2, ..., 6, являющиеся представителями всех классов вычетов по модулю 7, мы получим, что $4 \cdot 2 = 8 \equiv 1 \pmod 7$, то есть решением сравнения $4t \equiv 1 \pmod 7$ является класс вычетов $t \equiv 2 \pmod 7$.
2. Последовательно добавляя к правой части первоначального сравнения модуль 7, мы получим сравнения $4t \equiv 1 \pmod 7$, $4t \equiv 8 \pmod 7$. Получив в правой части число, делящееся на 4, сократим обе части сравнения на 4 и получим $t \equiv 2 \pmod 7$.
3. *Теорема Эйлера* [36] утверждает, что *для любого натурального числа* n *и любого целого* a, *взаимно простого с* n, *имеет место сравнение* $a^{\varphi(n)} \equiv 1 \pmod n$, *где* $\varphi(n)$ *— функция Эйлера.* Таким образом, для взаимно простого с модулем элемента a имеет место соотношение

$$a^{-1} \equiv a^{\varphi(n)-1} \pmod n.$$

Домножая обе части сравнения $4t \equiv 1 \pmod 7$ на $4^{\varphi(7)-1} = 4^5$, мы получаем, что $t \equiv 4^5 \pmod 7$. Поскольку

$$4^5 \equiv (-3)^5 \equiv 9 \cdot (-27) \equiv 2 \cdot 1 \equiv 2 \pmod 7, \text{ то } t \equiv 2 \pmod 7.$$

Таким образом, мы убедились, что в условиях нашей задачи

$$a^{-1} \equiv 2 \pmod 7.$$

Вычислив $b' \equiv -a^{-1} \cdot b \equiv -2 \cdot 3 \equiv -6 \equiv 1 \pmod 7$, мы получим обратное аффинное преобразование

$$x \equiv 2y + 1 \pmod 7.$$

Возвращаясь к аффинному преобразованию $y \equiv 7x + 4 \pmod{33}$, нетрудно убедиться, что $7^{-1} \equiv 19 \pmod{33}$, и следовательно обратное аффинное преобразование имеет вид $x \equiv 19y + 23 \pmod{33}$. Пользуясь этим результатом, совсем несложно расшифровать полученный нами ранее шифротекст «ОЧБРЕЙШЧДТБЭ»: последовательно применяя к числовым эквивалентам букв О, Ч, ..., Э преобразование $x \equiv 19y + 23 \pmod{33}$, мы получим числовые эквиваленты букв К, Р, ..., Я исходного сообщения «КРИПТОГРАФИЯ». □

Достоинством аффинной системы является удобное управление ключами — ключи шифрования и расшифрования представляются в компактной форме в виде пары чисел (a, b). По сравнению с простейшей системой шифрования Цезаря количество возможных ключей аффинной системы значительно больше, и алфавитный порядок слов при шифровании не сохраняется. Недостатком этой системы является то, что частотным анализом, перебором или просто догадкой можно установить соответствие между буквами алфавита и найти ключ шифрования.

Для того чтобы вычислить количество аффинных шифров над алфавитом длины N, нужно найти все возможные ключи (a, b). Поскольку a должно быть числом, взаимно простым с N, то существует ровно $\varphi(N)$ возможных значений a. Каждому значению a могут соответствовать N дополнительных сдвигов, задаваемых величиной b, т. е. всего существует $\varphi(N) \cdot N$ возможных ключей. Поскольку случай $(a, b) = (1, 0)$ дает тождественное преобразование, то мы можем утверждать, что *число аффинных шифрующих преобразований над алфавитом длины N равно* $\varphi(N) \cdot N - 1$.

Здесь $\varphi(n)$ — *функция Эйлера*, вычисляющая для данного натурального числа n количество натуральных чисел, не превосходящих n и взаимно простых с n:

$$\varphi(n) = |\{x \in \mathbb{N} : x \leqslant n, (x, n) = 1\}|.$$

Хорошо известно, что функция Эйлера мультипликативна [20]. Для ее вычисления можно воспользоваться формулой

$$\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_s - 1),$$

где $p_1, p_2, \ldots, p_s$ — различные простые числа, и $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$.

Пример 2.1.3 В случае шифрования на русском языке существует 659 различных аффинных шифров, учитывая 32 тривиальных шифра Цезаря. Действительно, так как $\varphi(33) = \varphi(3 \cdot 11) = (3-1)(11-1) = 20$, то общее число аффинных шифров равно

$$\varphi(33) \cdot 33 - 1 = 20 \cdot 33 - 1 = 659. \qquad \square$$

Элемент x открытого текста называется *неподвижным* при данном шифрующем преобразовании, если $f(x) = x$. В этом случае $x \equiv ax + b \pmod N$, то есть для неподвижного элемента шифрующего преобразования имеет место сравнение

$$x \cdot (a-1) \equiv -b \pmod N.$$

Пример 2.1.4 Найдем неподвижные элементы преобразований

$$y \equiv 13x + 6 \pmod{15} \quad \text{и} \quad y \equiv 79x + 171 \pmod{273}.$$

Начнем с первого преобразования. Если x — его неподвижный элемент, то $x \equiv 13x + 6 \pmod{15}$, откуда следует, что $12x \equiv -6 \pmod{15}$.

В этом случае $(12, 15) = 3$, $3|(-6)$, и мы можем воспользоваться соответствующим утверждением теоремы о линейных сравнениях [36]: *если* $(a, n) = d$, $d|b$, *то сравнение* $ax \equiv b \pmod n$ *имеет ровно* d *решений*; *разделив все три части сравнения на число* d, *мы получим новое сравнение первой степени* $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{n}{d}\right)$, *которое имеет единственное решение* $x \equiv \alpha \left(\mathrm{mod}\, \frac{n}{d}\right)$ *по модулю* $\frac{n}{d}$; *записывая класс вычетов* $x \equiv \alpha \left(\mathrm{mod}\, \frac{n}{d}\right)$ *по модулю* $\frac{n}{d}$ *в виде* d *классов вычетов по модулю* n, *мы получим все* d *решений* $x \equiv \alpha + k \cdot \frac{n}{d} \pmod n$, $k = 0, 1, 2, \ldots, d-1$, *первоначального сравнения.*

Реализуя этот алгоритм, поделим все три части сравнения $12x \equiv -6 \pmod{15}$ на 3. Получим сравнение $4x \equiv -2 \pmod 5$, или, что то же, сравнение $-x \equiv -2 \pmod 5$, откуда $x \equiv 2 \pmod 5$. Из одного решения по модулю 5 получим 3 решения по модулю 15: $x \equiv 2 \pmod{15}$, $x \equiv 2 + 5 \equiv 7 \pmod{15}$, $x \equiv 2 + 10 \equiv 12 \pmod{15}$.

Таким образом, неподвижными символами при аффинном преобразовании $y \equiv 13x + 6 \pmod{15}$ будут три элемента: 2, 7, 12.

Для нахождения неподвижных элементов второго преобразования выпишем сравнение $x \equiv 79x + 171 \pmod{273}$, из которого следует, что $78x \equiv -171 \pmod{273}$, или, что то же, $78x \equiv 102 \pmod{273}$. В этом случае $(78, 273) = 39$, и $39 \nmid 102$. Пользуясь теоремой о линейных сравнениях, которая утверждает, что *если* $(a, n) = d$, $d \nmid b$, *то сравнение*

$ax \equiv b \pmod{n}$ *не имеет решений* [36], убеждаемся в том, что сравнение $78x \equiv 102 \pmod{273}$ неразрешимо, и следовательно аффинное преобразование $y \equiv 79x + 171 \pmod{273}$ не имеет неподвижных элементов. □

С помощью аффинных преобразований можно зашифровывать и биграммы. Для этого текст разбивается на отдельные двухбуквенные сегменты. Если открытый текст состоит из нечетного числа букв, то чтобы получить целое число биграмм, к концу текста добавляют еще одну букву, выбрав ее так, чтобы не исказить смысл передаваемого сообщения.

Каждой биграмме приписывается ее числовой эквивалент x. Для этого используется формула

$$x = tN + l,$$

где t — числовой эквивалент первой буквы биграммы, l — числовой эквивалент второй буквы биграммы, а N — число букв в используемом алфавите.

Следующий шаг — выбор шифрующего преобразования

$$y \equiv ax + b \pmod{N^2}.$$

Здесь, так же как и в случае простого аффинного преобразования, число a не должно иметь общих множителей с N (что означает и отсутствие общих множителей с N^2).

Пример 2.1.5 Для шифрования сообщения «ДАМА» используем русский алфавит, состоящий из 33 букв, которым соответствуют числовые эквиваленты 0–32, и биграммное шифрующее преобразование

$$y \equiv 157x + 35 \pmod{1089}.$$

Биграмма «ДА» имеет числовой эквивалент $4 \cdot 33 + 0 = 132$, и ей соответствует биграмма шифротекста $157 \cdot 132 + 35 \equiv 68 \pmod{1089}$, то есть «ВВ». (Биграмма «ВВ» получается из ее числового эквивалента 68 его делением с остатком на 33: $68 = 2 \cdot 33 + 2$; первая буква биграммы соответствует неполному частному, вторая — остатку.) Заметим, что биграмма преобразуется как единое целое, так что если мы зашифруем биграмму «АД», состоящую из тех же самых букв, но записанных в другом порядке, то получим совсем другой результат: числовой эквивалент данной биграммы будет равняться $0 \cdot 33 + 4 = 4$, а ее образ $157 \cdot 4 + 35 \equiv 663 = 20 \cdot 33 + 3 \pmod{1089}$ при афинном преобразовании будет соответствовать биграмме «УГ». Аналогичным образом переведем биграмму «МА» в биграмму «ТФ». Таким образом, окончательный результат принимает вид «ВВТФ».

Аналогично можно работать с триграммами, 4-граммами и т. д. Преимуществами такой работы будет увеличение мощности алфавита: при работе с k-граммами мощность используемого алфавита будет равна N^k.

□

Упражнения

(1) Зашифруйте сообщение «HELP ME», используя 27-буквенный алфавит A = 0, ..., Z = 25, пробел = 26 и аффинное шифрующее преобразование с ключом (a, b), если

a) $a = 13$, $b = 9$; d) $a = 19$, $b = 5$; g) $a = 5$, $b = 12$;
b) $a = 2$, $b = 8$; e) $a = 7$, $b = 12$; h) $a = 7$, $b = 1$.
c) $a = 11$, $b = 0$; f) $a = 17$, $b = 2$;

(2) Зашифруйте сообщение «09.05.1945», используя 11-буквенный алфавит 0, 1, 2, ..., 9, . = 10 и аффинное шифрующее преобразование с ключом (a, b), если

a) $a = 7$, $b = 2$; d) $a = 5$, $b = 0$; g) $a = 8$, $b = 1$;
b) $a = 3$, $b = 2$; e) $a = 1$, $b = 4$; h) $a = 1$, $b = 6$.
c) $a = 9$, $b = 1$; f) $a = 3$, $b = 0$;

(3) Зашифруйте сообщение «АФФИННЫЕ КРИПТОСИСТМЫ», используя 34-буквенный алфавит А = 0, ..., Я = 32, пробел = 33 и аффинное шифрующее преобразование с ключом (a, b), если

a) $a = 13$, $b = 10$; d) $a = 19$, $b = 5$; g) $a = 5$, $b = 12$;
b) $a = 3$, $b = 8$; e) $a = 7$, $b = 12$; h) $a = 7$, $b = 1$.
c) $a = 11$, $b = 0$; f) $a = 15$, $b = 2$;

(4) Найдите обратное аффинное преобразование f^{-1} для преобразования $f(x) \equiv ax + b \pmod N$, если

a) $N = 30$, $a = 7$, $b = 12$; d) $N = 33$, $a = 1$, $b = 17$;
b) $N = 30$, $a = 17$, $b = 2$; e) $N = 27$, $a = 7$, $b = 1$;
c) $N = 33$, $a = 5$, $b = 12$; f) $N = 27$, $a = 1$, $b = 20$.

(5) С помощью аффинного преобразования $f(x) \equiv ax+b \pmod N$ зашифруйте придуманную вами фразу, записанную в соответствующем алфавите:

a) $N = 10$, $a = 3$, $b = 6$; d) $N = 11$, $a = 1$, $b = 9$;
b) $N = 11$, $a = 10$, $b = 2$; e) $N = 12$, $a = 5$, $b = 0$;
c) $N = 10$, $a = 1$, $b = 5$; f) $N = 13$, $a = 7$, $b = 1$.

Найдите обратное аффинное преобразование f^{-1} и проведите дешифрование полученного шифротекста.

(6) Сколько существует различных преобразований сдвига для N-буквенного алфавита, если

a) $N = 26$; b) $N = 30$; c) $N = 40$; d) $N = 50$.

⑦ Сколько существует различных линейных шифрующих преобразований для N-буквенного алфавита, если

a) $N = 27$; b) $N = 33$; c) $N = 44$; d) $N = 30$.

⑧ Сколько существует различных аффинных шифрующих преобразований для N-буквенного алфавита, если

a) $N = 30$; b) $N = 33$; c) $N = 44$; d) $N = 27$.

Сколько существует различных преобразований сдвига для N-буквенного алфавита? Сколько существует различных линейных преобразований для N-буквенного алфавита?

⑨ Сколько неподвижных символов получится при аффинном отображении $f(x) \equiv ax + b \pmod N$, если

a) $N = 30$, $a = 7$, $b = 12$;
b) $N = 30$, $a = 17$, $b = 2$;
c) $N = 33$, $a = 5$, $b = 12$;
d) $N = 33$, $a = 1$, $b = 18$;
e) $N = 27$, $a = 1$, $b = 23$;
f) $N = 27$, $a = 7$, $b = 1$.

Найдите эти символы, используя построенные вами алфавиты соответствующей длины.

⑩ Зашифруйте сообщение «HELP HIM», используя 27-буквенный алфавит A = 0, ..., Z = 25, пробел = 26 и биграммное шифрующее преобразование $f(x) \equiv ax + b \pmod{N^2}$, если

a) $a = 13$, $b = 9$; d) $a = 19$, $b = 5$; g) $a = 5$, $b = 12$;
b) $a = 2$, $b = 8$; e) $a = 7$, $b = 12$; h) $a = 7$, $b = 1$.
c) $a = 11$, $b = 0$; f) $a = 17$, $b = 2$;

⑪ Зашифруйте сообщение «АФФИННЫЕ КРИПТОСИСТЕМЫ», используя 34-буквенный алфавит А = 0, ..., Я = 32, пробел = 33 и биграммное шифрующее преобразование $f(x) \equiv ax + b \pmod{N^2}$, если

a) $a = 13$, $b = 10$; d) $a = 19$, $b = 5$; g) $a = 5$, $b = 12$;
b) $a = 3$, $b = 8$; e) $a = 7$, $b = 12$; h) $a = 7$, $b = 1$.
c) $a = 11$, $b = 0$; f) $a = 15$, $b = 2$;

⑫ Зашифруйте сообщение "07.07.2015", используя 11-буквенный алфавит 0, 1, 2, ..., 9, . = 10 и биграммное шифрующее преобразование $f(x) \equiv ax + b \pmod{N^2}$, если

a) $a = 3$, $b = 6$; d) $a = 7$, $b = 1$; g) $a = 8$, $b = 0$;
b) $a = 10$, $b = 2$; e) $a = 1$, $b = 6$; h) $a = 4$, $b = 9$.
c) $a = 5$, $b = 0$; f) $a = 1$, $b = 2$;

Зашифруйте тем же методом дату вашего рождения.

⑬ Зашифруйте номер машины "FDKL 07–28", состоящий из четырех английских букв и двух пар цифр, используя алфавит 0, 1, 2, ..., 9, - = 10, A = 11, B = 12, ..., Z = 36 и биграммное шифрующее преобразование $f(x) \equiv ax + b \pmod{N^2}$, если

a) $a = 7$, $b = 5$; d) $a = 17$, $b = 1$; g) $a = 1$, $b = 28$;
b) $a = 11$, $b = 2$; e) $a = 1$, $b = 20$; h) $a = 27$, $b = 1$.
c) $a = 5$, $b = 0$; f) $a = 10$, $b = 0$;

Решите задачу, если для формирования номера используются ровно N первых букв английского алфавита, $N = 10, 15, 20$.

⑭ Зашифруйте придуманную вами фразу, записанную в разработанном вами алфавите длины N, используя биграммное шифрующее преобразование $f(x) \equiv ax + b \pmod{N^2}$, если

a) $N = 30$, $a = 13$, $b = 10$; e) $N = 34$, $a = 7$, $b = 12$;
b) $N = 31$, $a = 3$, $b = 8$; f) $N = 26$, $a = 15$, $b = 2$;
c) $N = 32$, $a = 11$, $b = 0$; g) $N = 27$, $a = 5$, $b = 12$;
d) $N = 33$, $a = 19$, $b = 5$; h) $N = 44$, $a = 7$, $b = 1$.

⑮ Найдите преобразование f^{-1}, обратное биграммному шифрующему преобразованию $f(x) \equiv ax + b \pmod{N^2}$, если

a) $N = 30$, $a = 13$, $b = 10$; e) $N = 34$, $a = 7$, $b = 12$;
b) $N = 31$, $a = 3$, $b = 8$; f) $N = 26$, $a = 15$, $b = 2$;
c) $N = 32$, $a = 11$, $b = 0$; g) $N = 27$, $a = 5$, $b = 12$;
d) $N = 33$, $a = 19$, $b = 5$; h) $N = 44$, $a = 7$, $b = 1$.

Пользуясь полученным результатом, расшифруйте шифротексты, получившиеся при выполнении упражнения 14.

⑯ Сколько существует различных биграммных шифрующих преобразований для N-буквенного алфавита, если

a) $N = 27$; b) $N = 34$; c) $N = 44$; d) $N = 31$.

Сколько существует различных биграммных преобразований сдвига для N-буквенного алфавита? Сколько существует различных линейных биграммных преобразований для N-буквенного алфавита?

⑰ Сколько неподвижных символов получится при биграммном отображении $f(x) \equiv ax + b \pmod{N^2}$, если

a) $N = 30$, $a = 7$, $b = 12$; d) $N = 33$, $a = 5$, $b = 12$;
b) $N = 30$, $a = 17$, $b = 2$; e) $N = 27$, $a = 1$, $b = 28$;
c) $N = 33$, $a = 1$, $b = 15$; f) $N = 27$, $a = 7$, $b = 1$.

Задачи

1 Докажите, что для для множества шифрующих аффинных преобразований над одним и тем же алфавитом выполняются следующие утверждения:

a) композиция двух шифрующих аффинных преобразований является шифрующим аффинным преобразованием;

b) композиция двух шифрующих преобразований сдвига является преобразованием сдвига;

c) композиция двух шифрующих линейных преобразований является шифрующим линейным преобразованием.

При каких условиях композиция становится тождественным преобразованием?

2 Докажите, что композиция двух биграммных аффинных преобразований над одним и тем же алфавитом является биграммным аффинным преобразованием над тем же алфавитом. При каких условиях композиция становится тождественным преобразованием?

3 Докажите, что в случае линейного аффинного отображения для любых $x_1, x_2 \in X$ выполняется соотношение $f(x_1 + x_2) = f(x_1) + f(x_2)$.

4 При каких целых a преобразование $f(x) \equiv ax + b \pmod N$ обладает обратным преобразованием, если

a) $N = 30$; c) $N = 27$; e) $N = 26$;
b) $N = 44$; d) $N = 33$; f) $N = 29$?

5 Для каких натуральных a отображение $f : x \to y$ можно использовать в качестве аффинного преобразования, если

a) $y \equiv (a^2 + 1)x - a^2 \pmod{a^3 + 2a}$;
b) $y \equiv (a^2 + 2a)x - 1 \pmod{a^2 + 3a + 1}$?

6 Укажите число сдвигов, число линейных преобразований и общее число аффинных преобразований над N-буквенным алфавитом, если

a) $N{=}\varphi(10)!$; b) $N{=}\varphi(27)!$; c) $N{=}\varphi(30)!$; d) $N{=}\varphi(32)!$.

7 Если это возможно, приведите примеры алфавитов, для которых существует ровно T шифрующих аффинных преобразований; ровно L шифрующих линейных аффинных преобразований:

a) $T = 929$, $L = 29$; d) $T = 311$, $L = 11$; g) $T = 30$, $L = 9$;
b) $T = 479$, $L = 15$; e) $T = 242$, $L = 8$; h) $T = 47$, $L = 3$.
c) $T = 659$, $L = 19$; f) $T = 39$, $L = 3$;

Сколько преобразований сдвига существует в каждом из этих случаев?

8 Если это возможно, приведите пример N-буквенного алфавита, число шифрующих аффинных преобразований которого равно S:

a) $S = \dfrac{N^2}{2} - 1$; d) $S = \dfrac{4N^2}{5} - 1$; g) $S = \dfrac{8N^2}{15} - 1$;

b) $S = \dfrac{6N^2}{7} - 1$; e) $S = \dfrac{N^2}{3} - 1$; h) $S = \dfrac{2N^2}{3} - 1$.

c) $S = \dfrac{2N^2}{5} - 1$; f) $S = N^2 - N - 1$;

9 Найдите число неподвижных точек для шифрующего преобразования $y \equiv ax + b \pmod N$, если

a) $a = 19$, $b = 4$, $N = 729$; e) $a = 45$, $b = 115$, $N = 1936$;

b) $a = 28$, $b = 0$, $N = 729$; f) $a = 23$, $b = 8$, $N = 1936$;

c) $a = 32$, $b = 14$, $N = 729$; g) $a = 31$, $b = 2$, $N = 1936$;

d) $a = 1$, $b = 13$, $N = 729$; h) $a = 13$, $b = 0$, $N = 1936$.

10 Докажите, что любое линейное шифрующее преобразование N-буквенного алфавита обладает по крайней мере одной неподвижной буквой.

11 Докажите, что любое линейное шифрующее преобразование N-буквенного алфавита с четным N обладает по крайней мере двумя неподвижными буквами.

12 Докажите, что для простого числа N аффинное шифрующее преобразование N-буквенного алфавита, не являющееся сдвигом, обладает ровно одной неподвижной буквой.

13 Приведите пример аффинного преобразования, не имеющего неподвижных букв. Сколько таких преобразований существует для $N = 10, 15, 26, 27, 33, 34$?

14 Для $N = 10, 15, 26, 27, 33, 34$ выпишите все аффинные преобразования, не содержащие неподвижных букв. Дайте характеристику остальных аффинных преобразований над N-буквенным алфавитом.

15 Укажите преобразование, имеющее ровно k неподвижных букв:

a) $k = 0$; b) $k = 1$; c) $k = 2$; d) $k = 5$.

16 Может ли аффинное отображение $f(x) \equiv ax + b \pmod N$ иметь k неподвижных букв, если

a) $N = 30$, $k = 0$; c) $N = 33$, $k = 4$;

b) $N = 30$, $k = 2$; d) $N = 27$, $k = 4$?

Приведите примеры. Что можно сказать при тех же условиях о биграммном отображении $f(x) \equiv ax + b \pmod{N^2}$?

17 Приведите пример двух аффинных преобразований для 33-буквенного алфавита, каждое из которых имеет неподвижные буквы, а их комбинация не имеет неподвижных букв.

18 Приведите пример двух аффинных преобразований для 33-буквенного алфавита, каждое из которых не имеет неподвижных букв, а их комбинация имеет неподвижные буквы.

2.2. Криптоанализ аффинных криптосистем

Криптоанализ — наука о методах вскрытия зашифрованной информации. В большинстве случаев под криптоанализом понимается выяснение ключа шифрования.

Попытку раскрытия конкретного шифра с применением методов криптоанализа называют *криптографической атакой* на этот шифр. Криптографическая атака, в ходе которой раскрыть шифр удалось, называется *взломом* или *вскрытием*.

Для вскрытия криптосистемы нужна информация двух видов: во-первых, информация о природе (структуре) криптосистемы (используемый алфавит, его мощность, тип шифрующего преобразования и т. д.); во-вторых, информация о конкретном выборе сменных параметров — ключей.

В современной криптографии при оценке надежности шифрования принято предполагать, что противник знает об используемой системе шифрования все, кроме применяемых ключей, то есть секретность любого криптографического алгоритма должна быть сосредоточена именно в ключе, а не в особенностях самого алгоритма. В этом состоит *принцип Керкгоффса* — правило разработки криптографических систем, согласно которому в засекреченном виде держится только определенный набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Впервые данный принцип сформулировал в XIX в. голландский криптограф Огюст Керкгоффс (Auguste Kerckhoffs, 1835–1903). К. Шеннон сформулировал этот принцип (вероятно, независимо от Керкгоффса) следующим образом: «Враг знает систему».

Криптостойкостью шифра называется его стойкость к взлому. В ситуации, когда криптоанализ сводится к выяснению ключа, криптостойкость шифра определяется количеством всех возможных ключей шифра и временными затратами на перебор всех вариантов.

В случае аффинных криптосистем криптоанализ заключается в поиске двух параметров-ключей (a, b). Как правило, для решения этой задачи используются методы частотного анализа.

Замечание. *Поскольку число $\varphi(N) \cdot N - 1$ ключей аффинной криптосистемы над N-буквенным алфавитом относительно невелико, то все варианты возможных ключей могут быть найдены современными компьютерами обычным перебором. Поэтому сегодня аффинные шифры не являются криптостойкими. На практике они успешно использовались несколько веков назад. В наши дни их применение ограничивается большей частью иллюстрациями основных криптологических положений.*

Пример 2.2.6 Рассмотрим отрезок «УТЙТИТКЫКЦКЯЬТ» длинного шифротекста, в котором чаще всего встречаются буквы «Т» и «К». Разумно предположить, что ими зашифрованы две наиболее часто встречающиеся буквы русского алфавита «О» и «Е». Заменяя буквы их числовыми эквивалентами в 33-буквенном русском алфавите и подставляя последние в формулу дешифрования, получаем:

$$\begin{cases} 19a' + b' \equiv 15 \pmod{33}, \\ 11a' + b' \equiv 5 \pmod{33}. \end{cases}$$

Решив данную систему сравнений, получаем значения $a' = 26$ и $b' = 16$. Таким образом, сообщение может быть дешифровано применением формулы $x \equiv 26y + 16 \pmod{33}$. Непосредственная проверка показывает, что исходное сообщение имело вид «ЗОЛОТОЕ СЕМЕЧКО». □

Аналогичным методом можно вскрыть и сообщение, построенное с использованием биграмм. В этом случае увеличится лишь объем вычислений.

Пример 2.2.7 Перехвачено сообщение противника, частотный анализ которого показал, что биграммы «ШЙ» и «МВ» встречаются чаще остальных. Зная, что для шифрования использовался русский 33-буквенный алфавит и что наиболее часто встречающиеся в русском языке сочетания двух букв — это «СТ» и «НО», попытаемся дешифровать это сообщение, начинающееся с символов «ЖВПЬКС».

Чтобы дешифровать шифротекст «ЖВПЬКС» по правилу

$$x \equiv a'y + b' \pmod{33^2},$$

нужно знать ключи дешифрования a' и b'. Чтобы их найти, понадобятся числовые эквиваленты известных нам биграмм. Алгоритм их вычисления представлен в таблице.

ШЙ	$25 \cdot 33 + 10 = 835$	СТ	$18 \cdot 33 + 19 = 613$
МВ	$13 \cdot 33 + 2 = 431$	НО	$14 \cdot 33 + 15 = 477$

Подставляя полученные значения в сравнение $x \equiv a'y + b' \pmod{33^2}$, приходим к системе сравнений

$$\begin{cases} 835a' + b' \equiv 613 \pmod{1089}, \\ 431a' + b' \equiv 477 \pmod{1089}. \end{cases}$$

Исключив b', взяв разность этих сравнений, получим соотношение $404a' \equiv 136 \pmod{1089}$, что дает единственное решение $a' \equiv 809 \pmod{1089}$. Следовательно, $b' \equiv 477 - 431 \cdot 809 \equiv 278 \pmod{1089}$. Формула дешифрования получена:

$$x \equiv 809y + 278 \pmod{1089}.$$

Разобьем известный нам шифротекст на биграммы «ЖВ», «ПЬ» и «КС». Их числовые эквиваленты равны 233, 557 и 381, соответственно. Подставив их в формулу дешифрования, найдем числовые эквиваленты биграмм исходного сообщения:

$$x_{\text{ЖВ}} \equiv 809 \cdot 233 + 278 \equiv 378 \pmod{1089},$$
$$x_{\text{ПЬ}} \equiv 809 \cdot 557 + 278 \equiv 45 \pmod{1089},$$
$$x_{\text{КС}} \equiv 809 \cdot 381 + 278 \equiv 320 \pmod{1089}.$$

Получив соответствующие числовым эквивалентам биграммы ($378 = 11 \cdot 33 + 15$, и пара 11, 15 даст биграмму «КО»; $45 = 1 \cdot 33 + 12$, и пара 1, 12 даст биграмму «БЛ»; $320 = 9 \cdot 33 + 27$, и пара 9, 27 даст биграмму «ИЦ») и соединив их в единое слово, получим окончательный результат: исходное сообщение начиналось с символов «КОБЛИЦ». □

В некоторых случаях двух сравнений для однозначного нахождения параметров (a, b) аффинной криптосистемы бывает недостаточно, и приходится прибегать к дополнительным исследованиям.

Пример 2.2.8 Перехвачено сообщение «OFJDFOHFXOL», полученное применением аффинного преобразования букв 27-буквенного алфавита A = 0, ..., Z = 25, пробел = 26. Известно, что первым символом исходного сообщения является «I», за ним следует пробел. Попытаемся расшифровать полученный шифротекст. Для этого найдем ключи дешифрующего отображения из системы сравнений

$$\begin{cases} 14a' + b' \equiv 8 \pmod{27}, \\ 26a' + b' \equiv 5 \pmod{27}. \end{cases}$$

Вычтя из первого сравнения второе, получим сравнение $a' \equiv -18 \pmod{27}$, или, что то же, сравнение $9a' \equiv 9 \pmod{27}$, откуда следует, что $a' \equiv 1 \pmod{3}$. Переходя к модулю 27, получим для a' девять возможностей: $a' \equiv 1 + k \cdot 3 \pmod{27}$, $k = 0, 1, 2, \ldots, 8$. По фиксированному a' однозначно определим соответствующее значение b': $b' \equiv 8 - 14a' \pmod{27}$.

Таким образом, получим 9 возможных наборов (a', b'): $(1, 21)$, $(4, 6)$, $(7, 18)$, $(10, 3)$, $(13, 15)$, $(16, 0)$, $(19, 12)$, $(22, 24)$, $(25, 9)$. Ничего не остается, как просто перепробовать все эти 9 вариантов. Получаем следующие варианты открытого текста: «I DY IB RIF», «I PS IH RIX», «I AM IN RIO», «I MG IT RIF», «I YA IZ RIX», «I JV IE RIO», «I VP IK RIF», «I GJ IQ RIX», «I SD JW RIO».

Осмысленный текст дает только третий вариант: «I AM IN RIO». Это сообщение соответствует дешифрующему преобразованию

$$x \equiv 7y + 18 \pmod{27}. \qquad \square$$

Замечание. *Хотя биграммные аффинные криптосистемы, преобразования в которых осуществляются по модулю N^2, лучше аналогичных однобуквенных систем, использующих модуль N, они тоже имеют свои недостатки. Так, нетрудно заметить, что вторая буква биграммы шифротекста зависит только от второй буквы биграммы открытого текста: действительно, она определяется значением $y \equiv ax + b \pmod{N^2}$ по модулю N, которое зависит только от x по модулю N, т. е. только от второй буквы биграммы открытого текста. Поэтому помимо частотного анализа биграмм, важную информацию можно также получить от частотного анализа четных букв шифротекста. Подобное замечание справедливо и для аффинных преобразований k-буквенных блоков по модулю N^k.*

Упражнения

1. Определите ключи шифрования в примере 2.2.8 и ответьте «STAY THERE».
2. Известно, что перехваченное сообщение «FQOCUDEM» было зашифровано с использованием сдвига 26-буквенного алфавита. Анализируя длинные отрезки шифротекста, полученного тем же способом, выяснили, что чаще всего в шифротексте встречается символ «U». Зная, что «E» — наиболее часто встречающаяся буква английского алфавита, найдите величину сдвига и прочтите сообщение.
3. Используя частотный анализ, вскройте сообщение, зашифрованное преобразованием сдвига символов 31-буквенного русского алфавита (Е и Ё отождествлены, символ Ъ не используется):

   «Ф чпцю т щэтбк чп хпэтэ

   т этны чпуопэ — хтге мташые впычжу

   чк оыпмш ьцпыэт чклптэ

   т цвтэый щышве юрп эхпэмшычжу».

④ Известно, что при шифровании использовалось аффинное шифрующее преобразование букв 26-буквенного английского алфавита с ключами (7,12). Вскройте сообщение «NMYSOZGK».

⑤ Известно, что при шифровании была использована аффинная криптосистема над 26-буквенным английским алфавитом. При анализе шифротекста оказалось, что чаще всего в нем встречаются символ «K» и, затем, символ «D». Зная, что «E» и «T» — наиболее часто встречающиеся буквы английского алфавита, найдите дешифрующее преобразование.

⑥ При анализе перехваченных шифротекстов, составленных над расширенным 47-символьным русским алфавитом 0, 1, ..., 9, А = 10,..., Я = = 42, пробел = 43, . = 44, , = 45, ! = 46, была получена следующая система сравнений:

$$\begin{cases} 17x + 25y \equiv 3 \pmod{47}, \\ 10x + 31y \equiv 14 \pmod{47}. \end{cases}$$

Решите систему. Найдите ключ дешифрования (x, y). Восстановите по нему ключ шифрования и отправьте противнику сообщение «ПИСЬМО ПОЛУЧЕНО, ВСЕ ИДЕТ ПО ПЛАНУ!».

⑦ Используя метод аффинного шифрования (вручную или с использованием компьютера) над 34-буквенным русским алфавитом (добавьте символ пробела) с ключом (a, b), зашифруйте отрывок выбранной вами книги, содержащий не менее M символов (знаками препинания пренебречь):

a) $a = 3$, $b = 0$, $M = 200$;
b) $a = 15$, $b = 25$, $M = 100$;
c) $a = 11$, $b = 12$, $M = 150$;
d) $a = 19$, $b = 28$, $M = 100$;
e) $a = 1$, $b = 13$, $M = 250$;
f) $a = 5$, $b = 5$, $M = 150$.

⑧ В длинном отрезке шифротекста, полученного применением аффинного отображения букв 26-буквенного английского алфавита, чаще всех встречаются буквы «Y» и «V» (в указанном порядке). Предполагая, что эти элементы шифротекста получены шифрованием букв «E» и «T» соответственно, прочитайте сообщение «QAOOYQQEVHEQV».

⑨ Известно, что перехваченное сообщение «УУШНУУЬЛУ» было зашифровано с использованием биграммного сдвига 33-буквенного русского алфавита. Анализируя длинные отрезки шифротекста, полученного тем же способом, выяснили, что чаще всего в шифротексте встречаются биграммы «УЁ». Зная, что «СТ» наиболее часто используемая биграмма алфавита, найдите величину сдвига и прочтите сообщение.

⑩ Известно, что при шифровании была использована аффинная биграммная криптосистема над 26-буквенным английским алфавитом. При анализе шифротекста оказалось, что чаще всего в нем встречаются элемент «KS» и, затем, элемент «RE». Зная, что «TH» и «HE» английского языка, найдите дешифрующее преобразование.

⑪ Используя метод биграммного аффинного шифрования (вручную или с использованием компьютера) над 34-буквенным русским алфавитом (добавьте символ пробела) с ключом (a, b), зашифруйте отрывок выбранной вами книги, содержащий не менее M символов:

a) $a = 15$, $b = 5$, $M = 50$;
b) $a = 115$, $b = 0$, $M = 30$;
c) $a = 1$, $b = 75$, $M = 60$;
d) $a = 3$, $b = 2$, $M = 50$.

Задачи

1 Известно, что при шифровании использовалось аффинное шифрующее преобразование букв 37-буквенного алфавита 0, 1, 2, ..., 9, A = 10, ..., Z = 35, пробел = 36. Перехвачено сообщение «OH7F86BB46R3627O-266BB9» (O — буква). Известно, что открытый текст заканчивается подписью «007» (ноль-ноль-семь). Вскройте сообщение. Найдите способ шифрования и отправьте ответ «VERY SAD».

2 При шифровании было использовано аффинное шифрующее преобразование букв 41-буквенного алфавита А = 0, Б = 1, ..., Я =32, пробел = 33, . = 34, , = 35, - = 36, : = 37, ; = 38, ! = 39, ? = 40. Перехвачено сообщение «ЬХЗЭБЗКОХЖУ.АЩНЛК,Щ,Щ».Известно, что открытый текст заканчивается подписью «МАМА». Прочитайте сообщение. Определите ключ шифрования и ответьте «ПРИЕДУ ЗАВТРА».

3 Перехвачено сообщение «ОЗЯЗЙФ;БХП!ЕЬ;ЙПЖБНПН». Известно, что использовалось аффинное шифрующее преобразование букв 41-буквенного алфавита, содержащего символы А = 0, Б = 1, ..., Я = 32, пробел = 33, . = 34, , = 35, - = 36, : = 37, ; = 38, ! = 39, ? = 40. Известно, что открытый текст заканчивается подписью «БОБ». Прочитайте сообщение. Определите ключ шифрования и ответьте «ВЫПОЛНЯЙТЕ».

4 При шифровании использовалось аффинное шифрующее преобразование букв 41-буквенного алфавита, содержащего символы А = 0, Б = 1, ..., Я = 32, пробел = 33, . = 34, , = 35, - = 36, : = 37, ; = 38, ! = 39, ? = 40. Перехвачено сообщение «ЯК?ТЦШЕ;КГЖЁСТЖ». Известно,что первым символом является «Я», а за ним следует пробел. Прочтите сообщение. Определите ключ шифрования и ответьте «СООБЩИТЕ ВРЕМЯ».

5 Перехвачено сообщение «ПЙБУЛХП!ЙФ!БОЗЯЗЙФ;Ж». Известно, что применялось аффинное шифрующее преобразование букв 41-буквенного алфавита, содержащего символы А = 0, Б = 1, ..., Я = 32, пробел = 33, . = 34, , = 35, - = 36, : = 37, ; = 38, ! = 39, ? = 40. Известно, что первым словом является «ОН», а за ним следует пробел. Прочитайте сообщение. Определите ключ шифрования и ответьте «ПОЛУЧИТЕ НОВОЕ».

6 В отрезке шифротекста 28-буквенного английского алфавита А = 0, ..., Z = 25, пробел = 26, ? = 27 чаще всего встречаются символы В, ?. Зная, что наиболее часто встречающимися символами английского алфавита являются пробел, «Е», «Т», найдите шифрующее отображение. Достаточно было бы двух предположений о переходах букв?

7 Перехвачено шифрованное сообщение «PWULPZTQAWHF», полученное применением аффинного отображения биграмм 26-буквенного английского алфавита. Статистический анализ предшествующих шифротекстов показал, что чаще всего в них встречаются биграммы «IX» и «TQ» (в указанном порядке). Известно, что наиболее часто встречающимися биграммами английского текста являются «TH» и «HE» (в указанном порядке). Найдите ключи дешифрования и прочтите сообщение. Найдите ключи шифрования и отправьте сообщение «GOODWORK».

8 Перехвачено шифрованное сообщение «NDXBHO», полученное применением аффинного отображения биграмм 27-буквенного английского алфавита А = 0, ..., Z = 25, пробел (⌣) = 26. Статистический анализ предшествующих шифротекстов показал, что чаще всего в них встречаются биграммы «ZA», «IA» и «IW» (в указанном порядке). Известно, что наиболее часто встречающимися биграммами английского текста являются «⌣E», «S⌣» и «⌣T» (в указанном порядке). Найдите ключ дешифрования и прочтите сообщение. Найдите ключ шифрования и отправьте сообщение «ALLISOK».

9 При анализе перехваченных шифротекстов были получены следующие системы сравнений:

a) $\begin{cases} 3x+4y-29 \equiv 0 \pmod{143}, \\ 2x-9y+84 \equiv 0 \pmod{143}; \end{cases}$ c) $\begin{cases} 9x+20y \equiv 0 \pmod{29}, \\ 16x-13y \equiv 0 \pmod{29}; \end{cases}$

b) $\begin{cases} x+4y-1 \equiv 0 \pmod{9}, \\ 5x-8y-2 \equiv 0 \pmod{9}; \end{cases}$ d) $\begin{cases} 3x+4y-29 \equiv 0 \pmod{143}, \\ 2x-5y+84 \equiv 0 \pmod{143}; \end{cases}$

e) $\begin{cases} x + 4y - 1 \equiv 0 \pmod 9, \\ 5x - 8y - 1 \equiv 0 \pmod 9; \end{cases}$ f) $\begin{cases} 9x + 20y - 10 \equiv 0 \pmod{29}, \\ 16x - 13y - 21 \equiv 0 \pmod{29}. \end{cases}$

В каждом из случаев найдите ключ (x, y) дешифрования. Восстановите по нему ключи шифрования.

10 Выясните, при каких целых a из имеющейся системы сравнений можно найти ключ дешифрования (x, a):

a) $\begin{cases} 8x \equiv 20 \pmod{36}, \\ 75x + 30a \equiv 0 \pmod{36}; \end{cases}$ c) $\begin{cases} 9x \equiv 15 \pmod{30}, \\ 8x + 12a \equiv 0 \pmod{30}; \end{cases}$

b) $\begin{cases} 9x \equiv 12 \pmod{24}, \\ 50x + 70a \equiv 0 \pmod{24}; \end{cases}$ d) $\begin{cases} 18x \equiv 90 \pmod{60}, \\ 46x - 5a \equiv 0 \pmod{60}. \end{cases}$

Решите систему при найденных значениях параметра a, найдите ключ дешифрования (x, a), восстановите по нему ключ шифрования.

11 Перехвачено шифрованное сообщение «ОНПИЕФБЧЖОЛЖ», полученное применением аффинного отображения биграмм 31-буквенного русского алфавита (Е и Ё не различимы, символ Ъ не используется). Полагая известным, что биграммы «ОВ» и «СТ» (в указанном порядке) переходят соответственно в биграммы «РЦ» и «ЭК» (в указанном порядке), найдите ключи шифрования и вскройте сообщение.

12 Перехвачено шифрованное сообщение «DXM⌣SCE⌣DCCUVGX», полученное применением аффинного отображения биграмм 30-буквенного английского алфавита A = 0, ..., Z = 25, пробел (⌣) = 26, ? = 27, ! = 28, . = 29. Статистический анализ предшествующих шифротекстов показал, что чаще всего в них встречаются биграммы «M⌣», «U⌣» и «IH» (в указанном порядке). Известно, что наиболее часто встречающимися биграммами английского текста являются «⌣ E», «S⌣» и «⌣T» (в указанном порядке). Найдите ключ дешифрования и прочтите сообщение. Найдите ключ шифрования и отправьте сообщение «YES OF COURSE».

13 С помощью аффинного преобразования $f(x) \equiv 7x + 11 \pmod{N^3}$ зашифруйте:

a) триграмму «АБВ», записанную в 33-буквенном русском алфавите;

b) триграмму «ABC», записанную в 26-буквенном английском алфавите;

c) триграмму «204», записанную в алфавите 0, 1, 2, ..., 9.

В каждом из случаев зашифруйте придуманное вами сообщение, записанное в соответствующем алфавите. Найдите обратное аффинное преобразование f^{-1} и проведите дешифрование полученных шифротекстов. Имеет ли аффинное преобразование $f(x) \equiv 7x + 11 \pmod{N^3}$ неподвижные точки?

14 Проведите исследование аффинного триграммного преобразования $f(x) \equiv ax + b \pmod{N^3}$ на наличие неподвижных точек, если

a) $N = 10$, $a = 3$, $b = 6$;
b) $N = 11$, $a = 10$, $b = 2$;
c) $N = 12$, $a = 5$, $b = 0$;
d) $N = 13$, $a = 7$, $b = 1$.

Литература к главу 2

При подготовке текста главы 2 были использованы следующие источники [2], [4], [5], [7], [20], [21], [26], [32], [34], [36], [43], [53], [55], [70], [72], [80], [127].

Глава 3

Шифрующие матрицы

3.1. Алгебра матриц и аффинные матричные криптосистемы

Биграммы, на которые разбиваются криптографические сообщения, представляют собой пары символов, и, следовательно, их числовыми аналогами могут служить двумерные векторы: биграмме «XY», состоящий из символов некоторого N-буквенного алфавита, естественно поставить в соответствие вектор $\begin{pmatrix} x \\ y \end{pmatrix}$, в котором целое число x представляет собой числовой эквивалент первого символа «X» биграммы «XY», а число y — числовой эквивалент второго символа «Y» биграммы.

В этой связи естественно задавать шифрующее преобразование, переводящее биграммы открытого текста в биграммы шифротекста, с помощью квадратных 2×2 матриц, элементами которых являются целые числа.

Именно, для заданной матрицы $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ с целыми элементами a, b, c, d и заданного вектора $B = \begin{pmatrix} u \\ v \end{pmatrix}$ с целыми координатами u, v рассмотрим преобразование f множества двумерных векторов с целыми координатами в себя, осуществляемое по закону

$$f(X) \equiv A \cdot X + B \,(\mathrm{mod}\ N),$$

где знак сравнения векторов означает их покоординатную сравнимость:

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} u \\ v \end{pmatrix} (\mathrm{mod}\ N), \quad \text{если} \quad x \equiv u \,(\mathrm{mod}\ N) \quad \text{и} \quad y \equiv v \,(\mathrm{mod}\ N).$$

Такое преобразование называется *аффинным матричным отображением* [53].

Поскольку умножение 2×2 матрицы $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ и двумерного вектора $X = \begin{pmatrix} x \\ y \end{pmatrix}$ осуществляется по закону

$$A \cdot X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix},$$

то наше аффинное матричное преобразование можно записать в виде

$$\begin{pmatrix} z \\ t \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} \pmod{N},$$

или, что то же, в виде системы сравнений

$$\begin{cases} z \equiv ax + by + u \pmod{N}, \\ t \equiv cx + dy + v \pmod{N}. \end{cases}$$

Если $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, то есть вектор констант B равен нулевому вектору, то шифрующее отображение f принимает вид

$$f(X) \equiv A \cdot X \pmod{N}$$

и называется *линейным матричным отображением*; если

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

то есть шифрующая матрица A равна единичной матрице E, то шифрующее отображение f принимает вид

$$f(X) \equiv X + B \pmod{N}$$

и называется *матричным сдвигом*.

Поскольку все целые числа, участвующие в построении шифрующего матричного отображения, как и операции над ними, рассматриваются по модулю N, то естественно считать, что координаты используемых двумерных векторов и элементы рассматриваемых 2×2 матриц принадлежат кольцу классов вычетов $\mathbb{Z}_N$ по модулю N.

В этом случае общая схема матричного шифрования принимает вид

$$\begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix},$$

где $a, b, c, d, u, v \in \mathbb{Z}_N$, или, что то же, вид

$$f(X) = A \cdot X + B,$$

где знак равенства понимается как сравнимость элементов по модулю N.

Пример 3.1.1 Пользуясь 33-буквенном русским алфавитом, зашифруем сообщение «ДА» с помощью матрицы $A = \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix}$. Для этого найдем числовой эквивалент биграммы «ДА» — вектор $X = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$ и вычислим произведение $A \cdot X$. Поскольку

$$A \cdot X = \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 8 \\ 16 \end{pmatrix},$$

то числовым эквивалентом шифротекста $Z = f(X)$ является вектор $\begin{pmatrix} 8 \\ 16 \end{pmatrix}$, откуда следует, что сообщение «ДА» переходит в шифротекст «ЗП». □

Чтобы зашифровать с помощью аффинного матричного преобразования некоторое сообщение, его следует разбить на биграммы и построить последовательность $X_1X_2X_3 \ldots X_k$, состоящую из k числовых эквивалентов $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, ..., $X_k = \begin{pmatrix} x_k \\ y_k \end{pmatrix}$ биграмм открытого текста. Эту последовательность можно рассматривать как $2 \times k$ матрицу X, состоящую из k векторов-столбцов, которые представляют биграммы открытого текста.

Произведение 2×2 матрицы A на $2 \times k$ матрицу X существует и имеет вид

$$A \cdot X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x_1 & \ldots & x_k \\ y_1 & \ldots & y_k \end{pmatrix} = \begin{pmatrix} ax_1 + by_1 & \ldots & ax_k + by_k \\ cx_1 + dy_1 & \ldots & cx_k + dy_k \end{pmatrix}.$$

Другими словами, при умножении матрица A применяется поочередно к каждому столбцу X_i матрицы X, давая при этом соответствующий

столбец произведения. Поскольку для числового эквивалента X_i i-ой биграммы открытого текста преобразование $A \cdot X_i$ дает числовой эквивалент Z_i i-ой биграммы шифротекста, то столбцы матрицы $A \cdot X$ представляют собой последовательность $Z_1 Z_2 \ldots Z_k$ биграмм шифротекста.

Таким образом, для шифровки сообщения достаточно умножить 2×2 матрицу A на $2 \times k$ матрицу X и, получив при этом $2 \times k$ матрицу $Z = A \cdot X$, состоящую из числовых эквивалентов шифрованных биграмм-векторов, перейти с ее помощью к шифрованному сообщению.

Пример 3.1.2 Зашифруем открытый текст «КРИПТОГРАФИЯ», записанный в 33-буквенном русском алфавите, используя шифрующую матрицу $A = \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix}$. Для этого представим сообщение «КРИПТОГРАФИЯ» в виде последовательности биграмм «КР», «ИП», «ТО», «ГР», «АФ», «ИЯ». Заменяя каждую биграмму ее числовым эквивалентом, получим последовательность $\begin{pmatrix} 11 \\ 17 \end{pmatrix}, \begin{pmatrix} 9 \\ 16 \end{pmatrix}, \begin{pmatrix} 19 \\ 15 \end{pmatrix}, \begin{pmatrix} 3 \\ 17 \end{pmatrix}, \begin{pmatrix} 0 \\ 21 \end{pmatrix}, \begin{pmatrix} 9 \\ 32 \end{pmatrix}$, состоящую из шести двумерных векторов. Объединим полученные вектора в 2×6 матрицу $X = \begin{pmatrix} 11 & 9 & 19 & 3 & 0 & 9 \\ 17 & 16 & 15 & 17 & 21 & 32 \end{pmatrix}$ и рассмотрим произведение матриц A и X:

$$A \cdot X \equiv \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix} \cdot \begin{pmatrix} 11 & 9 & 19 & 3 & 0 & 9 \\ 17 & 16 & 15 & 17 & 21 & 32 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 73 & 66 & 83 & 57 & 63 & 114 \\ 180 & 164 & 196 & 148 & 168 & 612 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 7 & 0 & 17 & 24 & 30 & 15 \\ 15 & 32 & 31 & 16 & 3 & 18 \end{pmatrix} \pmod{33}.$$

Рассматривая столбцы матрицы $A \cdot X = \begin{pmatrix} 7 & 0 & 17 & 24 & 30 & 15 \\ 15 & 32 & 31 & 16 & 3 & 18 \end{pmatrix}$ как двумерные векторы Z_i, являющиеся числовыми эквивалентами биграмм шифротекста, получим, что зашифрованное сообщение имеет вид «ЖОАЯРЮЧПЭГОР». □

Для дешифрования сообщения нужно получить отображение, позволяющее выражать элемент открытого текста X как функцию от элемента шифротекста Z, другими словами, найти для аффинного матричного преобразования $f(X) = Z$ обратное ему преобразование $f^{-1}(Z) = X$. Обратное преобразование, выражающее биграмму открытого текста через биграмму шифротекста, может быть получено следующим образом:

$$A \cdot X + B = Z,\ A \cdot X = Z - B,\ X = A^{-1} \cdot Z - A^{-1} \cdot B,$$

где A^{-1} — матрица, обратная матрице A, и все операции, как и ранее, рассматриваются над кольцом классов вычетов $\mathbb{Z}_N$.

Это преобразование также будет аффинным матричным отображением. Для удобства запишем его в виде

$$X = A'Z + B',\ \text{где}\ A' = A^{-1},\ B' = -A^{-1}B.$$

Для однозначности дешифрования требуется обратимость матрицы A. Нетрудно убедиться в том, что матрица $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ с элементами $a, b, c, d \in \mathbb{Z}_N$ имеет обратную тогда и только тогда, когда ее определитель $\Delta = ad - bc$ взаимно прост с N [53]. В этом случае обратная матрица имеет вид

$$A^{-1} = \Delta^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Пример 3.1.3 Найдем матрицу, обратную матрице $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in \mathbb{Z}_{26}$.

Вычислим определитель матрицы A, выполняя операции в кольце $\mathbb{Z}_{26}$, то есть заменяя, в случае необходимости, встречающиеся в вычислениях целые числа на числа, сравнимые с ними по модулю 26: $\Delta = 2 \cdot 8 - 3 \cdot 7 = -5 = 21$. Так как $(21, 26) = 1$, то определитель обратим в $\mathbb{Z}_{26}$: $21^{-1} = 5$, поскольку в $\mathbb{Z}_{26}$ $21 \cdot 5 = 105 = 1$. (Для нахождения элемента, обратного элементу a в кольце $\mathbb{Z}_N$, нужно решить сравнение $ax \equiv 1 \pmod{N}$. В случае взаимной простоты элемента a и модуля N такое решение существует и единственно [36]). Таким образом,

$$A^{-1} = 21^{-1} \cdot \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = 5 \cdot \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} =$$

$$= \begin{pmatrix} 5 \cdot 8 & 5 \cdot (-3) \\ 5 \cdot (-7) & 5 \cdot 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}.$$

Осуществим проверку полученного результата:

$$A \cdot A^{-1} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 105 & 130 \\ 104 & 131 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E. \quad \square$$

Таким образом, для заданной матрицы $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}_N$, и заданного вектора $B = \begin{pmatrix} u \\ v \end{pmatrix}$ $u, v \in \mathbb{Z}_N$, преобразование $X = A'Z + B'$, переводящее вектор $Z = \begin{pmatrix} z \\ t \end{pmatrix}$ в вектор $X = \begin{pmatrix} x \\ y \end{pmatrix}$, принимает вид

$$\begin{pmatrix} x \\ y \end{pmatrix} = \Delta^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} z \\ t \end{pmatrix} - \Delta^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} u \\ v \end{pmatrix}.$$

Переходя к сравнениям, получим соотношение

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \Delta^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} z \\ t \end{pmatrix} - \Delta^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} u \\ v \end{pmatrix} \pmod N.$$

Оно может быть записано и в виде системы сравнений:

$$\begin{cases} x \equiv \Delta^{-1}(dz - bt) - \Delta^{-1}(du - bv) \pmod N, \\ y \equiv \Delta^{-1}(-cz + at) - \Delta^{-1}(-cu + av) \pmod N. \end{cases}$$

Пример 3.1.4 Дешифруем сообщение «ЗП», полученное в 33-буквенном русском алфавите при использовании матрицы $A = \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix} \in M_2(\mathbb{Z}_{33})$.

Для этого вычислим $\Delta = 4$, убедимся, что $(4, 33) = 1$, найдем величину $\Delta^{-1} = 25$ из сравнения $\Delta \cdot \Delta^{-1} \equiv 1 \pmod{33}$ и вычислим матрицу A^{-1}, обратную матрице A:

$$A^{-1} \equiv 4^{-1} \cdot \begin{pmatrix} 8 & -3 \\ -4 & 2 \end{pmatrix} \equiv 25 \cdot \begin{pmatrix} 8 & -3 \\ -4 & 2 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 25 \cdot 8 & -25 \cdot 3 \\ -25 \cdot 4 & 25 \cdot 2 \end{pmatrix} \equiv \begin{pmatrix} 200 & -75 \\ -100 & 50 \end{pmatrix} \equiv \begin{pmatrix} 2 & -9 \\ -1 & 17 \end{pmatrix} \pmod{33}.$$

После этого найдем числовой эквивалент $Z = \begin{pmatrix} 8 \\ 16 \end{pmatrix}$ биграммы «ЗП» и вычислим числовой эквивалент X соответствующей биграммы открытого текста:

$$X \equiv A^{-1} \cdot Z \equiv \begin{pmatrix} 2 & -9 \\ -1 & 17 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 16 \end{pmatrix} \equiv \begin{pmatrix} -128 \\ 264 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 0 \end{pmatrix} \pmod{33}.$$

Получив вектор $X = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$, перейдем к исходному сообщению «ДА». □

На практике мы можем столкнуться при дешифровке сообщений с различными «нештатными» ситуациями, поскольку при использовании необратимой матрицы описанный выше алгоритм дает сбои и требуются специальные методы для его корректировки. Рассмотрим различные случаи, которые могут произойти при дешифровании.

Пример 3.1.5

1. Используя 33-буквенный русский алфавит и шифрующее отображение $f(X) = A \cdot X$ с матрицей $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, была получена биграмма «ББ» шифротекста. Найдем соответствующую ей биграмму открытого текста.

Для этого заметим, что биграмма «ББ» имеет числовой эквивалент $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Таким образом, для нахождения числового эквивалента соответствующей биграммы открытого текста необходимо решить сравнение

$$\begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{33}.$$

Поскольку $\Delta = 1 \cdot 4 - 2 \cdot 3 = 4 - 6 = -2$ и $(-2, 33) = 1$, то данное сравнение разрешимо и имеет ровно одно решение — биграмму по модулю 33. Найдем его двумя способами.

Первый способ. В матричной форме сравнение имеет вид

$$Y \equiv A \cdot X \pmod{33}.$$

Перейдем к сравнению $X \equiv A^{-1} \cdot Y \pmod{33}$ и найдем

$$A^{-1} = \Delta^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Прежде всего найдем Δ^{-1}. Поскольку $\Delta \cdot \Delta^{-1} \equiv 1 \pmod{33}$, то есть $-2 \cdot \Delta^{-1} \equiv 1 \pmod{33}$, то $\Delta^{-1} = 16$. Тогда

$$A^{-1} = 16 \cdot \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 16 \cdot 4 & 16 \cdot (-2) \\ 16 \cdot (-3) & 16 \cdot 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 64 & -32 \\ -48 & 16 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -15 & 16 \end{pmatrix}.$$

Отсюда следует, что

$$X \equiv \begin{pmatrix} -2 & 1 \\ -15 & 16 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} -2+1 \\ -15+16 \end{pmatrix} \equiv \begin{pmatrix} 32 \\ 1 \end{pmatrix} \pmod{33}.$$

Таким образом, числовой эквивалент биграммы открытого текста $X = \begin{pmatrix} 32 \\ 1 \end{pmatrix}$, а сама биграмма имеет вид «ЯБ».

Второй способ. Запишем наше преобразование в виде системы сравнений:

$$\begin{cases} x + 2y \equiv 1 \pmod{33} \\ 3x + 4y \equiv 1 \pmod{33}. \end{cases}$$

Домножим левую и правую части первого сравнения на 2 и вычтем из второго сравнения первое. Получим $x \equiv -1 \pmod{33}$, откуда следует, что $y \equiv 1 \pmod{33}$. Поскольку $x \equiv -1 \equiv 32 \pmod{33}$, то получаем окончательный ответ $X = \begin{pmatrix} 32 \\ 1 \end{pmatrix}$, дающий, как и в предыдущем случае, биграмму «ЯБ».

2. Если при шифровании по той или иной причине была использована «плохая» шифрующая матрица A, ситуация может осложниться. Рассмотрим, например, задачу дешифрования биграммы «АД», полученной при использовании 33-буквенного русского алфавита и шифрующего отображения $f(X) = A \cdot X$ с матрицей $A = \begin{pmatrix} 1 & 5 \\ 2 & 1 \end{pmatrix}$.

Попробуем, как и ранее, найти биграмму из сравнения

$$\begin{pmatrix} 1 & 5 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 5 \end{pmatrix} \pmod{33}.$$

Поскольку $\Delta = 1 \cdot 1 - 2 \cdot 5 = 1 - 10 = -9$, и $(-9, 33) \neq 1$, то для матрицы $\begin{pmatrix} 1 & 5 \\ 2 & 1 \end{pmatrix}$ обратной матрицы не существует, и решить сравнение первым способом не представляется возможным.

Что даст второй способ? Запишем сравнение в виде системы сравнений:

$$\begin{cases} x + 5y \equiv 1 \pmod{33}, \\ 2x + y \equiv 5 \pmod{33}. \end{cases}$$

Проведя несложные преобразования, получим сравнение $-9y \equiv 3 \pmod{33}$. Поскольку $(-9, 33) = 3$, то данное сравнение имеет три решения: $y \equiv 7, 18, 29 \pmod{33}$. Находя соответствующие $x \equiv 1 - 5y \pmod{33}$, получим следующие возможности:

$$\begin{cases} y \equiv 7,\ 18,\ 29 \pmod{33}, \\ x \equiv 32,\ 10,\ 21 \pmod{33}. \end{cases}$$

Это дает нам три вектора $\begin{pmatrix} 32 \\ 7 \end{pmatrix}$, $\begin{pmatrix} 10 \\ 18 \end{pmatrix}$, $\begin{pmatrix} 21 \\ 29 \end{pmatrix}$, и, следовательно, три возможных варианта «ЯЖ», «ЙС», «ФЬ» расшифровки имеющегося в нашем распоряжении шифротекста.

3. Если же при использовании 33-буквенного русского алфавита и того же шифрующего отображения $f(X) = A \cdot X$ с матрицей $A = \begin{pmatrix} 1 & 5 \\ 2 & 1 \end{pmatrix}$ была получена биграмма «БД», то попытка ее дешифровки будет выглядеть следующим образом.

Как и ранее, попытка найти биграмму из сравнения

$$\begin{pmatrix} 1 & 5 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 4 \end{pmatrix} \pmod{33}$$

заставит нас убедиться в том, что обратной матрицы не существует и решить задачу первым способом не представляется возможным. При решении задачи вторым способом, записав сравнение в виде системы сравнений

$$\begin{cases} x + 5y \equiv 1 \pmod{33}, \\ 2x + y \equiv 4 \pmod{33}, \end{cases}$$

получим, после несложных преобразований, сравнение $-9y \equiv 2 \pmod{33}$. Поскольку $(-9, 33) = 3$, и $3 \nmid 2$, то данное сравнение решений не имеет, и дешифровать имеющуюся в нашем распоряжении биграмму не представляется возможным. Видимо, в ходе шифрования произошел какой-то сбой. □

Чтобы с помощью аффинных матричных преобразований дешифровать некоторое шифрованное сообщение, его следует разбить на биграммы и построить последовательность $Z_1 Z_2 Z_3 \ldots Z_m$, состоящую из m числовых эквивалентов $Z_1 = \begin{pmatrix} z_1 \\ t_1 \end{pmatrix}, \ldots, Z_m = \begin{pmatrix} z_m \\ t_m \end{pmatrix}$ биграмм шифротекста. Эту последовательность можно рассматривать как $2 \times m$ матрицу Z, состоящую из m векторов-столбцов, которые представляют биграммы шифротекста.

Таким образом, для дешифровки сообщения достаточно умножить 2×2 матрицу A^{-1} на $2 \times m$ матрицу Z и, получив при этом $2 \times m$ матрицу $X = A^{-1} \cdot Z$, состоящую из числовых эквивалентов биграмм-векторов открытого текста, перейти с ее помощью к исходному сообщению.

Пример 3.1.6 Дешифруем сообщение «БЯЕБФХ», полученное при использовании 33-буквенного русского алфавита и шифрующего преобразования $Z = A \cdot X$ с матрицей $A = \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix}$. Для этого представим шифрованное сообщение «БЯЕБФХ» в виде последовательности трех векторов $\begin{pmatrix} 1 \\ 32 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \begin{pmatrix} 21 \\ 22 \end{pmatrix}$. Составим из них 2×3 матрицу $Z = \begin{pmatrix} 1 & 5 & 21 \\ 32 & 1 & 22 \end{pmatrix}$ и осуществим нужное преобразование:

$$X \equiv A^{-1} \cdot Z \equiv \begin{pmatrix} 2 & 24 \\ 32 & 17 \end{pmatrix} \cdot \begin{pmatrix} 1 & 5 & 21 \\ 32 & 1 & 22 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 770 & 34 & 570 \\ 576 & 177 & 1046 \end{pmatrix} \equiv \begin{pmatrix} 11 & 1 & 9 \\ 15 & 12 & 23 \end{pmatrix} \pmod{33}.$$

Рассматривая вектора-столбцы $\begin{pmatrix} 11 \\ 15 \end{pmatrix}, \begin{pmatrix} 1 \\ 12 \end{pmatrix}, \begin{pmatrix} 9 \\ 23 \end{pmatrix}$ полученной матрицы как числовые эквиваленты биграмм открытого текста, без труда получим исходное сообщение «КОБЛИЦ». □

Упражнения

① Используя 33-буквенный алфавит и матрицу $A = \begin{pmatrix} 2 & 3 \\ 5 & 8 \end{pmatrix}$, зашифруйте слова «ЗАДАЧА»; «ПРИМЕР».

② В 26-буквенном алфавите, используя матрицу $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$, зашифруйте фразу «NOANSWER»; дешифруйте фразу «FWMDIQ».

③ В 26-буквенном алфавите, используя матрицу $A = \begin{pmatrix} 1 & 3 \\ 3 & 8 \end{pmatrix}$ и вектор констант $B = \begin{pmatrix} 13 \\ 2 \end{pmatrix}$, зашифруйте следующие латинские фразы:

a) «Alter ego» («Второе Я»);

b) «Caesarem decet stantem mori» («Цезарю подобает умереть стоя»);

c) «Carmina morte carent» («Стихи лишены смерти»).

Проверьте результат, произведя расшифровку полученных шифротекстов.

④ В 27-буквенном алфавите, используя матрицу $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ и вектор констант $B = \begin{pmatrix} 13 \\ 2 \end{pmatrix}$, зашифруйте следующие латинские фразы:

a) «Ab aqua silente cave» («Остерегайся тихой воды»);

b) «Abeunt studia in mores» («Занятия накладывают отпечаток на характер»);

c) «Alma mater» («Мать-кормилица»);

d) «Bis dat, qui cito dat» («Вдвойне дает, кто дает скоро»).

Проверьте результат, произведя расшифровку полученных шифротекстов.

⑤ Зашифруйте в 33-буквенном алфавите, используя матрицу $A = \begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix}$ и вектор констант $B = \begin{pmatrix} 1 \\ 7 \end{pmatrix}$, русские переводы латинских фраз, использованных в предыдущих упражнениях. Проверьте результат, произведя расшифровку полученных шифротекстов.

⑥ Для шифрующего преобразования $f(X) \equiv A \cdot X \pmod{N}$ постройте обратное шифрующее преобразование, если

a) $N = 29$ и $A = \begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix}$;

b) $N = 26$ и $A = \begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix}$;

c) $N = 41$ и $A = \begin{pmatrix} 40 & 0 \\ 0 & 21 \end{pmatrix}$;

d) $N = 25$ и $A = \begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix}$;

e) $N = 16$ и $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$;

f) $N = 29$ и $A = \begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix}$.

Выбрав подходящий алфавит, зашифруйте и расшифруйте в каждом из случаев сообщение, числовой эквивалент которого имеет вид « 11 10 12 8 12 15 14 10 10 13». Зашифруйте и расшифруйте собственную фразу, записанную в соответствующем алфавите.

⑦ Найдите биграмму $\begin{pmatrix} x \\ y \end{pmatrix}$ открытого текста из сравнения:

a) $\begin{pmatrix} 1 & 4 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{9}$;

b) $\begin{pmatrix} 1 & 4 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{9}$;

c) $\begin{pmatrix} 1 & 4 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{9}$;

d) $\begin{pmatrix} 1 & 4 \\ 5 & 7 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{9}$;

e) $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{26}$;

f) $\begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{26}$;

g) $\begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{26}$;

h) $\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 11 \end{pmatrix} \pmod{26}$.

В каждом из случаев, выбрав подходящий алфавит, расшифруйте сообщение «ABCDEFG». Зашифруйте и расшифруйте придуманное вами сообщение.

(8) Пользуясь 30-буквенным русским алфавитом (И и Й, Е и Ё, Ь и Ъ отождествлены), дешифруйте биграмму $f(X)$, которая была получена с помощью аффинного матричного преобразования $f(X) \equiv A \cdot X + B \pmod{30}$, если

a) $A = \begin{pmatrix} 2 & 4 \\ 5 & 8 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$, $f(X) =$ «МА»;

b) $A = \begin{pmatrix} 1 & 3 \\ 6 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 7 \\ 1 \end{pmatrix}$, $f(X) =$ «ПЫ»;

c) $A = \begin{pmatrix} 10 & 3 \\ 5 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 13 \\ 0 \end{pmatrix}$, $f(X) =$ «ЛИ»;

d) $A = \begin{pmatrix} 1 & 4 \\ 5 & 8 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $f(X) =$ «РТ»;

e) $A = \begin{pmatrix} 4 & 2 \\ 19 & 10 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$, $f(X) =$ «МУ»;

f) $A = \begin{pmatrix} 9 & 2 \\ 12 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 3 \\ 3 \end{pmatrix}$, $f(X) =$ «КО»;

g) $A = \begin{pmatrix} 7 & 2 \\ 15 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 11 \\ 2 \end{pmatrix}$, $f(X) =$ «ЗЫ».

Получили ли вы дешифровку; однозначную дешифровку? Почему? В каждом из случаев придумайте пример сообщения, допускающего однозначную расшифровку; сообщения, которое не может быть расшифровано в указанных условиях.

Задачи

1 Докажите, что для множества аффинных матричных преобразований над одним и тем же алфавитом выполняются следующие утверждения:

a) композиция матричных сдвигов является матричным сдвигом;

b) композиция линейных матричных преобразований является линейным матричным преобразованием;

c) композиция аффинных матричных преобразований является аффинным матричным преобразованием.

2 Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_N)$ и $\Delta = ad - bc$ — определитель этой матрицы. Докажите, что следующие утверждения эквивалентны:

a) $(\Delta, N) = 1$;

b) Матрица A имеет обратную;

c) Если хотя бы один из элементов $x, y \in \mathbb{Z}_N$ отличен от нуля, то

$$A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

d) Матрица A задает взаимно-однозначное отображение множества $\mathbb{Z}_N \times \mathbb{Z}_N$ на себя.

3 Найдите биграмму $\begin{pmatrix} x \\ y \end{pmatrix}$ открытого текста из сравнения:

a) $\begin{pmatrix} 9 & 20 \\ 16 & 13 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{29}$;

b) $\begin{pmatrix} 17 & 11 \\ 13 & 10 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{29}$;

c) $\begin{pmatrix} 17 & 11 \\ 13 & 10 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{29}$;

d) $\begin{pmatrix} 9 & 20 \\ 16 & 13 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 21 \end{pmatrix} \pmod{29}$;

e) $\begin{pmatrix} 9 & 20 \\ 16 & 13 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{29}$;

f) $\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 8 \end{pmatrix} \pmod{25}$;

g) $\begin{pmatrix} 480 & 971 \\ 297 & 398 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 416 \\ 319 \end{pmatrix} \pmod{1111}$;

h) $\begin{pmatrix} 480 & 971 \\ 297 & 398 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 109 \\ 906 \end{pmatrix} \pmod{1111}$;

i) $\begin{pmatrix} 480 & 971 \\ 297 & 398 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{1111}$;

j) $\begin{pmatrix} 480 & 971 \\ 298 & 398 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{1111}$;

k) $\begin{pmatrix} 480 & 971 \\ 298 & 398 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 648 \\ 1004 \end{pmatrix} \pmod{1111}$;

l) $\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 7 \end{pmatrix} \pmod{25}$.

4 Числа Фибоначчи определяются правилами $u_1 = u_2 = 1$, $u_{n+1} = u_n + u_{n-1}$ при $n > 1$. Докажите, что в матричной форме это правило может быть записано в виде

$$\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

Используя определение чисел Фибоначчи в матричной форме, докажите, что u_n четно тогда и только тогда, когда n делится на 3; докажите, что u_n делится на a тогда и только тогда, когда n делится на b, если $a = 2$, $b = 3$; $a = 3$, $b = 4$; $a = 5, b = 5$; $a = 7$, $b = 8$; $a = 8$, $b = 6$; $a = 11$, $b = 10$.

5 Постройте первые двадцать чисел Фибоначчи. Постройте матрицы $\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}$ для $n = 1, 2, ..., 19$, пользуясь уже известными значениями чисел Фибоначчи. Осуществите построение указанных матриц последовательным умножением уже имеющейся матрицы на матрицу

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Какой способ удобнее? Можно ли использовать полученные матрицы для построения аффинных матричных отображений? Можно ли использовать для этой цели матрицу $\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}$ при произвольном задании параметра n? Почему?

6 Осуществите шифрование биграммы «ОХ», записанной в 33-буквенном русском алфавите, с помощью аффинного матричного отображения $f(X) = \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} \cdot X$, где n — ваш номер в списке группы, а u_n — n-е число Фибоначчи.

7 Пусть $N, M \in \mathbb{N}$, и $(N, M) = 1$. Убедитесь в том, что любую матрицу $A \in M_2(\mathbb{Z}_N)$ можно вложить в множество $M_2(\mathbb{Z}_M)$ простым приведением элементов по модулю M. Приведите примеры таких вложений.

8 Пусть $N = mn$, где $(m, n) = 1$. Пусть $A_m \in M_2(\mathbb{Z}_m)$ — матрица, полученная путем приведения элементов матрицы A по модулю m, и $A_n \in M_2(\mathbb{Z}_n)$ — матрица, полученная путем приведения элементов матрицы A по модулю n.

a) Докажите, что отображение, сопоставляющее матрице A пару (A_m, A_n), является взаимно-однозначным соответствием между множеством $M_2(\mathbb{Z}_N)$ и декартовым произведением $M_2(\mathbb{Z}_m) \times M_2(\mathbb{Z}_n)$ множеств $M_2(\mathbb{Z}_m)$ и $M_2(\mathbb{Z}_n)$. Приведите примеры.

b) Докажите, что это отображение задает взаимно-однозначное соответствие между множеством $M_2^*(\mathbb{Z}_N)$ обратимых 2×2 матриц с элементами из $\mathbb{Z}_N$ и декартовым произведением $M_2^*(\mathbb{Z}_m) \times M_2^*(\mathbb{Z}_n)$ множества $M_2^*(\mathbb{Z}_m)$ обратимых 2×2 матриц с элементами из $\mathbb{Z}_m$ на множество $M_2^*(\mathbb{Z}_n)$ обратимых 2×2 матриц с элементами из $\mathbb{Z}_n$. Приведите примеры.

9 Найдите число элементов множества $M_2(\mathbb{Z}_p)$, где p — простое число. Подсчитайте число решений в $\mathbb{Z}_p$ уравнения $ad - bc = 0$. Докажите, что число $\varphi_2(p) = |M_2^*(\mathbb{Z}_p)|$ обратимых элементов множества $M_2(\mathbb{Z}_p)$ можно получить, используя формулу $\varphi_2(p) = p(p^2 - 1)(p - 1)$.

10 Найдите число элементов множества $M_2(\mathbb{Z}_{p^\alpha})$, где $p \in P$, $\alpha \in \mathbb{N}$. Докажите, что число $\varphi_2(p^\alpha) = |M_2^*(\mathbb{Z}_{p^\alpha})|$ обратимых элементов множества $M_2(\mathbb{Z}_{p^\alpha})$ можно получить, используя формулу

$$\varphi_2(p^\alpha) = p^{4\alpha-3}(p^2 - 1)(p - 1).$$

11 Найдите число элементов множества $M_2(\mathbb{Z}_N)$, где $N \in \mathbb{N}$. Используя задачи 8 и 10, докажите, что число $\varphi_2(N) = |M_2^*(\mathbb{Z}_N)|$ обратимых 2×2 матриц с элементами из $\mathbb{Z}_N$ можно получить, используя формулу

$$\varphi_2(N) = N^4 \prod_{p|N} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right).$$

12 Докажите, что число $\varphi_k(N) = |M_k(\mathbb{Z}_N)|$ обратимых $k \times k$ матриц с элементами из $\mathbb{Z}_N$ может быть вычислено по формуле

$$\varphi_k(N) = N^{k^2} \prod_{p|N} \left(\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) \dots \left(1 - \frac{1}{p^k}\right)\right).$$

13 Сколько существует шифрующих 2×2 матриц при $N = 26, 29, 30$?

14 Зашифруйте триграмму X с помощью аффинного триграммного матричного преобразования $f(X) \equiv A \cdot X + B \pmod{N}$, если

a) $N = 29$, $A = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 4 & 3 \\ 1 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, $X =$ «WAU»;

b) $N = 26$, $A = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 4 & 3 \\ 0 & 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $X =$ «YES»;

c) $N = 30$, $A = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $X =$ «ГАВ»;

d) $N = 33$, $A = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 4 & 3 \\ 2 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $X =$ «МЯУ».

Найдите обратное аффинное триграммное матричное отображение. Выбрав подходящий алфавит, зашифруйте и расшифруйте в каждом из случаев сообщение, числовой эквивалент которого имеет вид «11 10 12 12 15 14 10 10 13». Зашифруйте и расшифруйте собственную фразу, записанную в соответствующем алфавите.

15 Сколько имеется аффинных матричных шифрующих преобразований для триграмм 26-буквенного алфавита?

16 Дайте определение неподвижной точки аффинного матричного отображения. Найдите число неподвижных точек аффинного матричного отображения $f(X) = A \cdot X + B$ над N-буквенным алфавитом, если

a) $N = 10$, $A = \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$;

b) $N = 10$, $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$;

c) $N = 10$, $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$;

d) $N = 10$, $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$;

e) $N = 10$, $A = \begin{pmatrix} 3 & 3 & 4 \\ 0 & 0 & 3 \\ 1 & 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 4 \\ 8 \\ 0 \end{pmatrix}$.

3.2. Криптоанализ аффинных матричных криптосистем

Приступая к обсуждению вопросов криптоанализа матричных аффинных шифров, будем полагать что, согласно принципу Керкгоффса, природа вскрываемого шифра известна: именно, мы знаем, что наш противник использует матричный аффинный метод шифрования в N-буквенном алфавите.

Начнем обсуждение с методов вскрытия матричной линейной системы шифрования $Z = A \cdot X$ в N-буквенном алфавите. Для вскрытия данной шифросистемы достаточно найти шифрующую матрицу A.

С помощью частотного анализа или дополнительной информации (в сообщении может использоваться подпись, адрес и т.д.), у нас может появиться возможность найти две пары биграмм открытого и шифрованного текстов: $Z_1 = A \cdot X_1$ и $Z_2 = A \cdot X_2$. В этом случае, для того чтобы определить матрицы A и A^{-1}, мы можем объединить два столбца X_1 и X_1

в 2×2 матрицу X и таким же образом поступить со столбцами шифротекста, получив 2×2 матрицу Z. Таким образом, мы получим матричное уравнение $Z = A \cdot X$, в котором матрицы Z и X нам известны. Можно с легкостью решить это уравнение относительно неизвестной нам матрицы A, домножив обе части уравнения на X^{-1}:

$$Z \cdot X^{-1} = A \cdot X \cdot X^{-1} = A.$$

Аналогично, из матричного уравнения $X = A^{-1}Z$ находим матрицу A^{-1}:

$$X \cdot Z^{-1} = A^{-1} \cdot Z \cdot Z^{-1} = A^{-1}.$$

Таким образом, при наличии двух матриц X и Z, соответствующих двум имеющимся в нашем распоряжении парам биграмм открытого текста и шифротекста, мы можем получить шифрующую матрицу A и дешифрующую матрицу A^{-1}, пользуясь простым правилом:

$$A = Z \cdot X^{-1},\ A^{-1} = X \cdot Z^{-1}.$$

Пример 3.2.7 Нам известно, что противник использовал для шифрования сообщения 2×2 матрицу с элементами из 34-буквенного алфавита А = 0, ..., Я = 32, пробел = 33. Попробуем дешифровать перехваченное сообщение «ЩЛДОРЪАЖФЛРБСЕЦЯ», если оказались известны последние четыре буквы открытого текста:«ЕЖНО».

Известных нам букв как раз хватит, чтобы построить две пары биграмм: прообразами биграмм «СЕ» и «ЦЯ» шифротекста в открытом тексте являются биграммы «ЕЖ» и «НО», соответственно.

Выпишем числовые эквиваленты всех четырех биграмм и построим матрицы X и Z: нетрудно убедиться в том, что

$$X = \begin{pmatrix} 5 & 14 \\ 7 & 15 \end{pmatrix}, \quad Z = \begin{pmatrix} 18 & 23 \\ 5 & 32 \end{pmatrix}.$$

Для дешифрования имеющегося шифротекста нам понадобится матрица A^{-1}, получить которую можно по формуле $A^{-1} = X \cdot Z^{-1}$:

$$A^{-1} \equiv \begin{pmatrix} 5 & 14 \\ 7 & 15 \end{pmatrix} \cdot \begin{pmatrix} 18 & 23 \\ 5 & 32 \end{pmatrix}^{-1} \equiv$$

$$\equiv \begin{pmatrix} 5 & 14 \\ 7 & 15 \end{pmatrix} \cdot \begin{pmatrix} 16 & 31 \\ 23 & 26 \end{pmatrix} \equiv \begin{pmatrix} 28 & 9 \\ 15 & 29 \end{pmatrix} \pmod{34}.$$

Теперь, построив матрицу

$$Z' = \begin{pmatrix} 26 & 4 & 17 & 0 & 21 & 17 & 18 & 23 \\ 12 & 15 & 27 & 7 & 12 & 1 & 5 & 32 \end{pmatrix},$$

составленную из числовых эквивалентов биграмм имеющегося в нашем распоряжении шифротекста «ЩЛДОРЪАЖФЛРБСЕЦЯ», и реализовав операцию $A^{-1} \cdot Z'$, найдем матрицу X', составленную из числовых эквивалентов биграмм оригинального сообщения, уже известным нам способом:

$$X' \equiv A^{-1} \cdot Z' \equiv \begin{pmatrix} 28 & 9 \\ 15 & 29 \end{pmatrix} \cdot \begin{pmatrix} 26 & 4 & 17 & 0 & 21 & 17 & 18 & 23 \\ 12 & 15 & 27 & 7 & 12 & 1 & 5 & 32 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 20 & 9 & 5 & 29 & 16 & 9 & 5 & 14 \\ 24 & 19 & 18 & 33 & 17 & 12 & 7 & 15 \end{pmatrix} (\mathrm{mod}\ 34).$$

В итоге получаем сообщение «УЧИТЕСЬ ПРИЛЕЖНО». □

Существенным условием решения задачи предыдущего примера явился факт обратимости матрицы Z. Что же делать, если нам не повезет?

В этом случае можно отыскать еще одну пару биграмм открытого и шифрованного текстов. Тогда есть вероятность того, что составленная из других пар биграмм матрица будет обратимой. Если у нас нет такой возможности, то мы не можем определить матрицу A^{-1} точно. Однако имеющейся у нас информации, как правило, должно хватить, чтобы значительно сократить число возможных вариантов для дешифрующей матрицы.

Пример 3.2.8 Перехвачено сообщение противника «СЗЪАУЗКО» и известно, что он использует для шифрования матрицу A с элементами из 34-буквенного алфавита с такими же числовыми эквивалентами, как и в предыдущем примере. Попробуем найти матрицу дешифрования A^{-1} и прочитать оригинальное сообщение, если известно, что первые буквы открытого текста «ВЫПО».

Для этого, как и ранее, запишем символы открытого текста «ВЫПО» и шифротекста «СЗЪА» в виде 2×2 матриц

$$X = \begin{pmatrix} 2 & 16 \\ 28 & 15 \end{pmatrix}, \quad Z = \begin{pmatrix} 18 & 27 \\ 8 & 0 \end{pmatrix}.$$

Однако мы сразу сталкиваемся с трудностями, поскольку построенная матрица Z не является обратимой: ее определитель $\Delta_Z = -216$,

и $(-216, 34) = 2$. (Убедитесь самостоятельно, что матрица X также не является обратимой). Мы можем продолжить следующим образом. Обозначим символом $\overline{A}$ матрицу, полученную из матрицы A приведением всех ее элементов по модулю 17. Тот же самый смысл будут иметь символы $\overline{X}$ и $\overline{Z}$. В этом случае получаем, что

$$\overline{X} = \begin{pmatrix} 2 & 16 \\ 11 & 15 \end{pmatrix}, \overline{Z} = \begin{pmatrix} 1 & 10 \\ 8 & 0 \end{pmatrix}.$$

Рассматривая эти матрицы как элементы множества $M_2(\mathbb{Z}_{17})$, найдем $\overline{Z}^{-1}$, что возможно, поскольку при данных условиях $(\Delta_{\overline{Z}}, 17) = 1$. В нашем случае $\overline{Z}^{-1} = \begin{pmatrix} 0 & 15 \\ 12 & 7 \end{pmatrix}$. Теперь из равенства $\overline{A}^{-1} = \overline{X} \cdot \overline{Z}^{-1}$ мы можем найти матрицу $\overline{A}^{-1}$:

$$\overline{A}^{-1} = \overline{X} \cdot \overline{Z}^{-1} = \begin{pmatrix} 2 & 16 \\ 11 & 15 \end{pmatrix} \cdot \begin{pmatrix} 0 & 15 \\ 12 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 10 & 15 \end{pmatrix}.$$

Таким образом, элементы матрицы A^{-1}, которые являются элементами кольца классов вычетов по модулю 34, по модулю 17 должны приводиться к элементам матрицы $\begin{pmatrix} 5 & 6 \\ 10 & 15 \end{pmatrix}$. Точнее,

$$A^{-1} = \begin{pmatrix} 5 & 6 \\ 10 & 15 \end{pmatrix} + 17 \cdot A_1,$$

где A_1 представляет собой некоторую 2×2 матрицу, составленную только из нулей и единиц. Поэтому из всех $\varphi_2(34) = 157248$ возможных вариантов дешифрующей матрицы у нас остается только $2^4 = 16$ возможных вариантов.

Мы можем еще больше сократить количество возможных вариантов, учитывая то, что матрица A^{-1} должна быть обратима, а следовательно, ее определитель должен быть числом, взаимно простым с 34, в частности, обязан быть числом нечетным.

Тогда для A^{-1} останется всего 6 возможных вариантов:

$$\begin{pmatrix} 5 & 6 \\ 27 & 15 \end{pmatrix}, \begin{pmatrix} 5 & 6 \\ 10 & 15 \end{pmatrix}, \begin{pmatrix} 5 & 23 \\ 10 & 15 \end{pmatrix}, \begin{pmatrix} 5 & 23 \\ 27 & 32 \end{pmatrix}, \begin{pmatrix} 22 & 23 \\ 27 & 15 \end{pmatrix}, \begin{pmatrix} 22 & 23 \\ 27 & 32 \end{pmatrix}.$$

Подставляя возможные варианты матрицы A^{-1} в уравнение $A^{-1} \cdot Z = X$, или, что то же, в уравнение

$$A^{-1} \cdot \begin{pmatrix} 18 & 27 \\ 8 & 0 \end{pmatrix} = \begin{pmatrix} 13 & 19 \\ 0 & 26 \end{pmatrix},$$

мы исключим все возможности, кроме окончательного решения: $A^{-1} = \begin{pmatrix} 22 & 23 \\ 27 & 15 \end{pmatrix}$. (Заметим, что этому случаю отвечает вспомогательная матрица $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$). Дешифруя сообщение «СЗЪАУЗКО» с помощью полученной матрицы, мы придем к соотношению

$$\begin{pmatrix} 22 & 23 \\ 27 & 15 \end{pmatrix} \cdot \begin{pmatrix} 18 & 27 & 20 & 11 \\ 8 & 0 & 8 & 15 \end{pmatrix} = \begin{pmatrix} 2 & 16 & 12 & 9 \\ 28 & 15 & 14 & 12 \end{pmatrix},$$

что соответствует тексту «ВЫПОЛНИЛ». □

Если для шифрования было использовано аффинное матричное шифрующее преобразование $Z = A \cdot X + B$ биграмм-векторов из N-буквенного алфавита, то обратное ему преобразование имеет вид $X = A'Z + B'$, где $A' = A^{-1}$ и $B' = -A^{-1}B$. В этом случае для нахождения ключа шифрования — матрицы A и вектора констант B — нам необходимо знать, по крайней мере, три пары биграмм:

$$X_1 = A'Z_1 + B',\ X_2 = A'Z_2 + B',\ X_3 = A'Z_3 + B'.$$

Для нахождения матрицы A' и вектора B' мы можем осуществить следующую операцию: вычтем последнее уравнение из первых двух и образуем 2×2 матрицу X из столбцов $X_1 - X_3$ и $X_2 - X_3$, а матрицу Z такой же размерности — из столбцов $Z_1 - Z_3$ и $Z_2 - Z_3$. В итоге мы получим матричное уравнение $X = A'Z$, которое, при условии, что матрица Z обратима, будет разрешимо относительно A':

$$A' = XZ^{-1}.$$

Наконец, определив $A^{-1} = A'$, найдем B', используя любое из приведенных выше уравнений: например,

$$B' = X_1 - A'Z_1.$$

Пример 3.2.9 Найдем ключ дешифрования, если нам известны числовые эквиваленты трех пар биграмм, построенных над 33-буквенным русском алфавитом:

$$\begin{pmatrix}13\\0\end{pmatrix}=A'\begin{pmatrix}3\\30\end{pmatrix}+B',\ \begin{pmatrix}19\\5\end{pmatrix}=A'\begin{pmatrix}20\\26\end{pmatrix}+B',\ \begin{pmatrix}11\\0\end{pmatrix}=A'\begin{pmatrix}32\\22\end{pmatrix}+B'.$$

Составим 2×2 матрицу X из столбцов X_1-X_3 и X_2-X_3, и матрицу Z такой же размерности — из столбцов Z_1-Z_3 и Z_2-Z_3:

$$X=\begin{pmatrix}2&8\\0&5\end{pmatrix},\ Z=\begin{pmatrix}-29&-12\\8&4\end{pmatrix}=\begin{pmatrix}4&21\\8&4\end{pmatrix}.$$

Убедимся, что определитель Δ_Z матрицы Z взаимно прост с числом 33: $\Delta_Z=16-168=-152=13$ и $(13,33)=1$. Следовательно, матрица Z обратима, и уравнение $X=A'Z$ имеет единственное решение $A'=XZ^{-1}$:

$$A'=\begin{pmatrix}2&8\\0&5\end{pmatrix}\cdot\begin{pmatrix}4&21\\8&4\end{pmatrix}^{-1}=$$

$$=\begin{pmatrix}2&8\\0&5\end{pmatrix}\cdot\begin{pmatrix}13&6\\32&13\end{pmatrix}=\begin{pmatrix}282&116\\160&65\end{pmatrix}=\begin{pmatrix}18&17\\28&32\end{pmatrix}.$$

Таким образом, матрица $A^{-1}=A'$ найдена. Осталось найти вектор констант:

$$B'=\begin{pmatrix}13\\0\end{pmatrix}-\begin{pmatrix}18&17\\28&32\end{pmatrix}\cdot\begin{pmatrix}3\\30\end{pmatrix}=$$

$$=\begin{pmatrix}13\\0\end{pmatrix}-\begin{pmatrix}564\\1044\end{pmatrix}=\begin{pmatrix}-551\\-1044\end{pmatrix}=\begin{pmatrix}10\\12\end{pmatrix}.$$ □

Замечание. *Подобные шифрующие преобразования можно использовать и для векторов длины k, соответственно рассматривая шифрующие матрицы размера $k\times k$, к которым предъявляться те же требования обратимости. При этом вычисление обратной матрицы превратится в значительно более трудоемкий процесс.*

Упражнения

(1) Вы анализируете матричное линейное шифрующее преобразование букв 33-буквенного алфавита А = 0, ..., Я = 32. Перехвачено сообщение «ЗПДЗЧО». Вам известно, что при данном шифровании биграммы

«ИВ» и «ЕТ» переходят соответственно в биграммы «РЧ» и «ОБ». Вскройте сообщение, определите шифрующую матрицу и отправьте ответное сообщение «РЕШЕНА».

(2) Известно, что противник использует шифрующую матрицу A с элементами из 26-буквенного алфавита. Перехвачено сообщение «WKNCCHSSBT». Известно, что первое слово открытого текста — «GIVE». Найдите матрицу дешифрования A^{-1} и прочитайте оригинальное сообщение.

(3) Перехвачено сообщение «ZRIXXYVBMNPO». Известно, что при шифровании использовалось матричное линейное отображение 26-буквенного алфавита A = 0, ..., Z = 25, пробел = 26. Вскройте сообщение и найдите шифрующую матрицу, если вам известно, что при данном шифровании биграммы «E⌣» и «S⌣» переходят соответственно в биграммы «PK» и «RZ».

(4) Известно, что для шифрования сообщения использовалось аффинное матричное преобразование $Z = A \cdot X + B$ над 33-буквенным русским алфавитом (без Ъ, но с пробелом). Определите параметры A' и B' дешифрующего сообщения $X = A' \cdot Z + B'$ и дешифруйте перехваченный шифротекст «ФФЛЭГЦ», если есть основания предполагать, что при шифровании биграммы «МА», «АВ», «ТР» переходят в биграммы «ПД», «ГЗ», «ХЕ», соответственно. Найдите параметры A и B исходного аффинного матричного преобразования и отправьте противнику сообщение «ВСЕ ГОТОВО».

(5) Определите, если это возможно, дешифрующую матрицу A^{-1}, если имеется две пары биграмм открытого и шифрованного текстов в N-буквенном алфавите, которые позволяют записать соотношение $Z \equiv A \cdot X \pmod{N}$, где

a) $N = 34$, $X = \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}$, $Z = \begin{pmatrix} 17 & 2 \\ 5 & 21 \end{pmatrix}$;

b) $N = 34$, $X = \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}$, $Z = \begin{pmatrix} 21 & 28 \\ 2 & 11 \end{pmatrix}$;

c) $N = 21$, $X = \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}$, $Z = \begin{pmatrix} 21 & 28 \\ 2 & 11 \end{pmatrix}$;

d) $N = 21$, $X = \begin{pmatrix} 2 & 3 \\ 2 & 6 \end{pmatrix}$, $Z = \begin{pmatrix} 21 & 28 \\ 2 & 11 \end{pmatrix}$.

⑥ Известно, что для шифрования сообщения использовалось аффинное матричное преобразование $Z = A \cdot X + B$ над 33-буквенным русским алфавитом (без Ъ, но с пробелом). Постарайтесь вскрыть сообщение L, определив параметры A' и B' дешифрующего сообщения $X = A' \cdot Z + B'$, если есть основания предполагать, что при шифровании биграммы X_1, X_2 и X_3 переходят в биграммы Z_1, Z_2, и Z_3:

a) L =«МЮТЯИХАП», X_1 = «СП», X_2 = «ТР», X_3 = «АВ», Z_1 = «СН», Z_2 = «ТЯ», Z_3 = «АБ»;

b) L =«ХТМЫДФ», X_1 = «МА», X_2 = «АВ», X_3 = «ТР», Z_1 = «РВ», Z_2 = «ДЁ», Z_3 = «ЦГ»;

c) L =«ПДХЕЛЭГЦ», X_1 = «СП», X_2 = «ТР», X_3 = «АВ», Z_1 = «ФФ», Z_2 = «ХЕ», Z_3 = «ГЗ»;

⑦ Известно, что для шифрования сообщения использовалось аффинное матричное преобразование $Z = A \cdot X + B$ над N-буквенным алфавитом. Определите параметры A' и B' дешифрующего сообщения $X = A' \cdot Z + B'$, если есть основания предполагать, что при шифровании биграммы X_1, X_2 и X_3 переходят в биграммы Z_1, Z_2, и Z_3:

a) $N = 33$, X_1 = «ДА», X_2 = «НО», X_3 = «ОТ», Z_1 = «ТИ», Z_2 = «СМ», Z_3 = «КЫ»;

b) $N = 34$, X_1 = «НЕ», X_2 = «ИЗ», X_3 = «О‿», Z_1 = «ЬБ», Z_2 = «ЮЪ», Z_3 = «ЧФ»;

c) $N = 26$, X_1 = «AN», X_2 = «OF», X_3 = «IN», Z_1 = «GS», Z_2 = «BV», Z_3 = «LK»;

d) $N = 27$, X_1 = «TO», X_2 = «IT», X_3 = «IS», Z_1 = «JK», Z_2 = «WE», Z_3 = «AJ».

Найдя ключ (A, B) используемой противником криптосистемы, отправьте ему сообщение «ОК».

Задачи

1 Вы анализируете матричное линейное шифрующее преобразование букв 33-буквенного алфавита А = 0, ..., Я = 32. Перехвачено сообщение «СРРЧОБ». Вам известно, что при данном шифровании биграммы «ДА» и «РЕ» переходят соответственно в биграммы «ДЗ» и «ДП». Вскройте сообщение, определите шифрующую матрицу и отправьте ответное сообщение «ГОТОВО».

2 Вы анализируете матричное линейное шифрующее преобразование букв 33-буквенного алфавита А = 0, ..., Я = 32. Перехвачено сообщение «ДПЛЯНЫ». Вам известно, что при данном шифровании биграммы

«ЕТ» и «ДА» переходят соответственно в биграммы «ОБ» и «ДЗ». Вскройте сообщение, определите шифрующую матрицу и отправьте ответное сообщение «ВОПРОС».

3 Вы анализируете матричное линейное шифрующее преобразование букв 33-буквенного алфавита А = 0, ..., Я = 32. Перехвачено сообщение «ЖВЯЁМЩ». Вам известно, что при данном шифровании биграммы «ЕТ» и «НА» переходят соответственно в биграммы «ОБ» и «НЫ». Вскройте сообщение, определите шифрующую матрицу и отправьте ответное сообщение «ЗАДАЧА».

4 Вы анализируете матричное линейное шифрующее преобразование букв 33-буквенного алфавита А = 0, ..., Я = 32. Перехвачено сообщение «ЭСМРЬП». Вам известно, что при данном шифровании биграммы «ШЕ» и «ДИ» переходят соответственно в биграммы «ЛЯ» и «ЖВ». Вскройте сообщение, определите шифрующую матрицу и отправьте ответное сообщение «РАБОТА».

5 Перехвачено сообщение «GFPYJP⌣X?UYXSTLADPLW». Известно, что при шифровании использовалось матричное линейное отображение 29-буквенного алфавита A = 0, ..., Z = 25, пробел = 26, ? = 27, ! = 28. Предполагается, что сообщение заканчивается словом «KARLA». Вскройте сообщение и найдите шифрующую матрицу.

6 Перехвачено сообщение «SONAFQCHMWPTVEVY». Известно, что при шифровании использовалось матричное линейное отображение 26-буквенного алфавита A = 0, ..., Z = 25. Вскройте сообщение и найдите шифрующую матрицу, если вам известно, что при данном шифровании биграммы «TH» и «HE» переходят соответственно в биграммы «KH» и «XW».

7 Перехвачено сообщение «!IWGVIEX!ZRADRYD». шифровании использовалось матричное линейное отображение 29-буквенного алфавита A = 0, ..., Z = 25, пробел = 26, ? = 27, ! = 28. Предполагается, что сообщение заканчивается подписью «MARIA». Вскройте сообщение и найдите шифрующую матрицу.

8 Перехвачено сообщение «KVW?⌣TA!KJB?FVR⌣». (Пробелы после ? и «R» входят в сообщение.) Известно, что использовано линейное шифрующее преобразование в 30-буквенном алфавите A = 0, ..., Z = 25, пробел = 26, . = 27, , = 28, ? = 29. Известно также, что последние шесть букв открытого текста — подпись «KARLA.». Найдите дешифрующую матрицу A^{-1} и прочитайте открытый текст.

9 Докажите, что если биграммы-векторы шифруются по формуле $Z \equiv A \cdot X \pmod{N}$ необратимой матрицей A, то любой шифротекст может быть дешифрован по крайней мере в два различных открытых текста.

10 Для затруднения задачи вскрытия криптосистемы сначала зашифруем биграммы в 26-буквенном алфавите, используя матрицу $\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix}$, а затем проведем ту же операцию в 29-буквенном алфавите с помощью матрицы $\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$. В этих условиях:

a) зашифруйте сообщение «SEND»; c) зашифруйте сообщение «PLAN»;

b) дешифруйте сообщение «ZMOY»; d) дешифруйте сообщение «ECDK».

11 Определите шифрующую 2×2 матрицу A с элементами из $\mathbb{Z}_{30}$, если имеется две пары биграмм открытого и шифрованного текстов в 30-буквенном алфавите, которые позволяют записать соотношение

$$A \cdot X \equiv Z \pmod{30}, \quad \text{где } X = \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}, \; Z = \begin{pmatrix} 17 & 8 \\ 8 & 29 \end{pmatrix}.$$

a) Убедитесь, что задачу невозможно решить стандартным методом;

b) Используя приведение по модулю 10, запишите матрицу A в виде $A \equiv A_0 + 10A_1 \pmod{30}$, где A_1 — неизвестная матрица по модулю 3 (с 0, 1 и 2 в качестве элементов), и A_0 — матрица, получаемая в результате вычислений по модулю 10. Выберите A_0 так, чтобы все ее элементы лежали между 0 и 29 и делились на 3.

c) Используя приведение по модулю 3, найдите второй столбец матрицы A_1.

d) Сколько существует вариантов для исходной матрицы A? Перечислите их.

12 Перехвачено сообщение «S⌣GNLKD?KOZQLLIOMKUL.VY». Известно, что при шифровании использовалось матричное линейное отображение 30-буквенного алфавита A = 0, ..., Z = 25, пробел = 26, . = 27, , = 28, ? = 29. Предполагается, что сообщение заканчивается подписью «KARLA.». Вскройте сообщение и найдите шифрующую матрицу.

13 Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — шифрующая матрица линейного преобразования биграмм N-буквенного алфавита, то есть обратимая 2×2 матрица с элементами из $\mathbb{Z}_N$.

a) Дайте определение неподвижной биграммы, соответствующей матрице A (предполагается, что матрица A не является единичной).

b) Покажите, что биграмма «АА» $= \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ всегда неподвижна.

c) Какой должна быть шифрующая матрица $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ для того, чтобы «АА» была единственной неподвижной биграммой?

d) Пусть N — простое число и известно, что, кроме биграммы «АА», существует по крайней мере еще одна неподвижная биграмма. Докажите, что в этом случае имеется ровно N неподвижных биграмм.

14 Известно, что для шифрования перехваченного сообщения использовалось линейное матричное преобразование $Z = A \cdot X$ над 33-буквенным русским алфавитом. Определите параметр A' дешифрующего отображения $X = A' \cdot Z$, если при частотном анализе перехваченного шифротекста выяснилось, что наиболее часто в нем встречаются биграммы «ЬТ» и «БЮ» (в указанном порядке). Определите ключ A исходной криптосистемы и отправьте противнику сообщение «ВСЕИДЕТПОПЛАНУ».

15 Известно, что для шифрования перехваченного сообщения использовалось аффинное матричное преобразование $Z = A \cdot X + B$ над 26-буквенным английским алфавитом. Определите параметры A' и B' дешифрующего сообщения $X = A' \cdot Z + B'$, если при частотном анализе сообщения выяснилось, что наиболее часто в нем встречаются биграммы «GH», «KL», «MF» (в указанном порядке). Определите ключ (A, B) исходной криптосистемы и отправьте противнику сообщение «ALLRIGHT».

16 Перехвачено сообщение «WUXHURWZNQR XVUEXU!JHALGQGJ», которое зашифровано аффинным преобразованием векторов $\begin{pmatrix} x \\ y \end{pmatrix}$ в 841-буквенном алфавите. Здесь числовыми эквивалентами биграмм

являются числа $x = 29x_1 + x_2$, где x_1 — эквивалент первой, и x_2 — эквивалент второй букв биграммы. Таким образом, каждый блок из четырех букв дает столбец $\begin{pmatrix} x \\ y \end{pmatrix}$: две первые буквы дают целое x, а две другие — целое y. Известно также, что последние 12 букв приведенного выше шифротекста отвечают подписи «HEADQUARTERS».

a) Найдите дешифрующее преобразование и прочитайте исходное сообщение.

b) Найдите шифрующее преобразование и постройте шифрованное сообщение от имени штаба следующего содержания: слова «CANCEL LAST ORDER!» после двух пробелов сопровождаются подписью «HEADQUARTERS».

17 Сколько аффинных шифрующих преобразований существует над 841-элементным алфавитом биграмм?

18 Перехвачено сообщение «FBRTLWUGAJQINZTHHXTEPHBNXSW», зашифрованное линейным шифрующим преобразованием триграмм 26-буквенного алфавита A = 0, ..., Z = 25. Известно, что последние три триграммы — это подпись отправителя «JAMESBOND». Найдите дешифрующую матрицу и прочитайте сообщение.

Литература к главе 3

При подготовке текста главы 3 были использованы следующие источники [13], [19], [21], [31], [36], [53], [59], [60], [55], [66], [74], [75], [80], [89], [91].

Глава 4

Система RSA. Дискретный логарифм

Рассмотрев в первой главе историю криптографии, которая, в сущности, является историей развития методов симметричного шифрования, и изучив во второй и третьей главах основы функционирования простейших симметричных криптосистем, мы переходим к обзору истории и основ асимметричного шифрования, или, что то же, криптосистем с открытым ключом. Хотя эта область криптографической науки и практики еще очень молода — с момента появления работ, содержащих базовые идеи использования в шифровании открытого ключа, не прошло и полувека — в настоящее время криптографические системы с открытым ключом находят широкое практическое применение и как самостоятельное средство для защиты передаваемой и хранимой информации, и как средство распределения ключей, и как средство аутентификации пользователей.

4.1. Система *RSA* и ее модификации

В 1976 г. была опубликована работа молодых американских математиков Уитфилда Диффи (Bailey Whitfield Diffie, род. 1944) и Мартина Э. Хилльмана (Martin E. Hellman, род. 1945) «Новые направления в криптографии», которая не только существенно изменила криптографию, но и привела к появлению новых теоретических разработок в математике.

Центральное понятие, введенное в этой статье — *односторонняя функция* $F : X \to Y$, обладающая двумя свойствами:

1. по известному x довольно просто найти значение $F(x)$;
2. инвертирование функции F, то есть нахождение x из известного $F(x)$, невозможно за разумный срок.

Впрочем, сама односторонняя функция бесполезна в применении: ею можно зашифровать сообщение, но нельзя его расшифровать. Поэтому криптография с открытым ключом использует понятие *односторонней функции с секретом* (*функции с ловушкой*) — отображения $F_k : X \to Y$, зависящего от *ключа* k и обладающего тремя свойствами:

1. для любого k существует «быстрый» алгоритм вычисления значения $F_k(x)$ по известному x;
2. при неизвестном k не существует «быстрого» алгоритма инвертирования $F_k(x)$, то есть вычисления x по известному $F_k(x)$;
3. при известном k существует «быстрый» алгоритм инвертирования $F_k(x)$.

Криптографические системы, использующие односторонние функции, принято называть *ассиметричными*. Как правило, в основу известных асимметричных криптосистем положена одна из сложных математических проблем, которая позволяет строить те или иные односторонние функции с секретом.

Применение функций с секретом в криптографии позволяет организовывать обмен шифрованными сообщениями с использованием только открытых каналов связи; включать в задачу вскрытия шифра трудную математическую задачу и тем самым повышать обоснованность стойкости шифра; решать новые криптографические задачи, отличные от шифрования (цифровая электронная подпись и др.) [22] .

В 1977 г. учеными Рональдом Линном Ривестом (Ronald Linn Rivest, род. 1947), Ади Шамиром (Adi Shamir, род. 1952) и Леонардом Адлеманом (Leonard Adleman, род. 1945) из Массачусетского технологического института был разработан алгоритм шифрования, основанный на особенностях теоретико-числовой проблемы разложения на множители натуральных чисел. Система была названа по первым буквам их фамилий (*RSA*: Rivest, Shamir, Adleman). Авторы схемы зашифровали с помощью разработанного ими алгоритма английскую фразу *«The Magic Words are Squeamish Ossifrage»* (*«Волшебные слова — брезгливый ягнятник»*). Она была записана стандартным образом (A=01, B=02, ..., Z=26, пробел =00) в виде числа x и зашифрована по схеме

$$x \to x^e \pmod{m}.$$

Числа

$$m = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$$

и $e = 9007$ были опубликованы вместе с шифротекстом.

9686 9613 7546 2206
1477 1409 2225 4355
8829 0575 9991 1245
7431 9874 6951 2093
0816 2982 2514 5708
3569 3147 6622 8839
8962 8013 3919 9055
1829 9451 5781 5154

Причем дополнительно сообщалось, что $m = pq$, где p и q — простые числа, записываемые соответственно 64 и 65 десятичными знаками. Первому, кто дешифрует соответствующее сообщение, была обещана награда в 100 долларов США.

История завершилась только спустя 17 лет, в 1994 г., когда команда, возглавляемая Дереком Аткинсом, Майклом Граффом, Арьеном Ленстрой и Полом Лейландом, нашла числа

$$p = 3490529510847650949147849619903898133417764638493387843990820577,$$

$$q = 3276913299326670954996198819083446141317764296799294253979828853 3$$

и расшифровала запись. Это заняло 220 дней и потребовало использования примерно 1600 компьютеров и участия около 600 добровольцев, соединенных через сеть Интернет. Полученные за разложение 100 долларов США были пожертвованы Фонду свободного программного обеспечения [24], [128].

Существуют несколько модификаций этой системы, однако все они основываются на нескольких хорошо известных фактах теории чисел.

Именно, *теорема Эйлера* (см., например, [20]) утверждает, что *для любого натурального числа n и любого целого a, взаимно простого с n, имеет место сравнение $a^{\varphi(n)} \equiv 1 \pmod n$, где $\varphi(n)$ — функция Эйлера.*

Очевидно, что $\varphi(p) = p-1$ для простого числа p. Таким образом, *малая теорема Ферма*, утверждающая, что *для любого простого числа p и любого целого a, взаимно простого с n, имеет место сравнение $a^{p-1} \equiv 1 \pmod p$*, является частным случаем теоремы Эйлера.

Из теоремы Эйлера немедленно следует основополагающее для наших рассуждений соотношение: *если $\alpha \equiv \beta \pmod{\varphi(n)}$, то для целого числа a, взаимно простого с n, $a^\alpha \equiv a^\beta \pmod n$*. Действительно, из условия следует, что $\alpha-\beta \equiv 0 \pmod{\varphi(n)}$, или, что то же, $\alpha-\beta = \varphi(n)\cdot k$, $k \in \mathbb{Z}$. Тогда, пользуясь теоремой Эйлера, получаем, что $a^{\alpha-\beta} \equiv a^{\varphi(n)\cdot k} \equiv (a^{\varphi(n)})^k \equiv 1 \pmod n$, и, следовательно, $a^\alpha \equiv a^\beta \pmod n$. Верно ли обратное утверждение?

Рассмотрим несколько наиболее известных модификаций системы *RSA* [78], [91].

4.1.1. Криптосистема без передачи ключей

Рассмотрим двух абонентов A и B, планирующих вести секретную переписку.

Первым шагом работы является выбор большого простого числа p, которое будет известно обоим абонентам. Как правило, при этом $p-1 = p_1 \cdot \ldots \cdot p_s$, где p_i — различные простые множители (то есть число p — *евклидово*), обычно небольшие.

Зафиксировав простое число p, каждый из абонентов A и B выбирает первый ключ (натуральные числа a и b, соответственно), удовлетворяющий условиям:

A: $a \in \mathbb{N}$, $(a, p-1) = 1$, $0 < a < p-1$;

B: $b \in \mathbb{N}$, $(b, p-1) = 1$, $0 < b < p-1$.

Затем абоненты находят вторые ключи (натуральные числа α и β, соответственно), из условий:

A: $\alpha \in \mathbb{N}$, $a \cdot \alpha \equiv 1 \pmod{p-1}$, $0 < \alpha < p-1$;

B: $\beta \in \mathbb{N}$, $b \cdot \beta \equiv 1 \pmod{p-1}$, $0 < \beta < p-1$.

Поскольку $(a, p-1) = (b, p-1) = 1$, то оба сравнения имеют ровно по одному решению, то есть такие натуральные числа α и β обязательно найдутся, причем будут определены единственным образом.

Итак, в конце предварительного этапа работы каждый из абонентов знает используемое большое простое число p и имеет в своем распоряжении два ключа, как представлено в нижеследующей таблице.

Абонент	Модуль n	$\varphi(n)$	Первый ключ	Второй ключ
A	p	$p-1$	a	
B	p	$p-1$	b	β

Схема работы алгоритма заключается в следующем.

1. Абонент A составляет сообщение для абонента B и представляет его в виде числа m, $0 < m < p$ (если кодирование сообщения привело к числу, равному или большему p, то разобьем его на две или несколько частей). Затем абонент A шифрует сообщение m ключом a:

$$m_1 \equiv m^a \pmod{p}, \quad 0 < m_1 < p;$$

полученное сообщение m_1 абонент A отправляет абоненту B.

2. Абонент B шифрует сообщение m_1 ключом b:

$$m_2 \equiv m_1^b \pmod{p}, \quad 0 < m_2 < p;$$

полученное сообщение m_2 абонент B отправляет абоненту A.

3. Абонент A шифрует сообщение m_2 ключом α:

$$m_3 \equiv m_2^\alpha \pmod{p}, \quad 0 < m_3 < p;$$

полученное сообщение m_3 абонент A отправляет абоненту B.

4. Абонент B расшифровывает сообщение m_3 ключом β:

$$m_4 \equiv m_3^{\beta} \pmod{p}, \quad 0 < m_4 < p.$$

В этом случае $m_4 = m$, и абонент B получает возможность прочитать исходное сообщение от абонента A, переведя число m в буквенную форму.

Доказательство корректности описанного выше алгоритма совсем несложно. Использованные при работе соотношения позволяют утверждать, что

$$m_4 \equiv m_3^{\beta} \equiv m_2^{\alpha\beta} \equiv m_1^{b\alpha\beta} \equiv m^{ab\alpha\beta} \pmod{p}.$$

При этом выбор ключей алгоритма таков, что

$$ab\alpha\beta \equiv (a\alpha)(b\beta) \equiv 1 \cdot 1 \equiv 1 \pmod{p-1}.$$

Таким образом, $m^{ab\alpha\beta} \equiv m^1 \equiv m \pmod{p}$. Поскольку числа m_4 и m удовлетворяют условиям $0 < m_4 < p$, $0 < m < p$, то $m_4 = m$; в ходе работы абонент B действительно получит числовой эквивалент исходного сообщения от абонента A.

Замечание. *Мы ничего не сказали о взаимной простоте числа m и модуля p. На самом деле, при реализации алгоритма этот вопрос непринципиален: во-первых, число m всегда можно откорректировать так, чтобы условие $(m, p) = 1$ имело место. Во-вторых, если $(m, p) \neq 1$, то $p \mid m$, то есть $m \equiv 0 \pmod{p}$. В этом случае используемое нами свойство $\alpha \equiv \beta \pmod{p-1} \Rightarrow m^{\alpha} \equiv m^{\beta} \pmod{p}$ очевидным образом выполнено. Впрочем, все преобразования алгоритма становятся в этом случае тривиальными.*

Пример 4.1.1 Выберем $p = 31$. Тогда $p - 1 = 30 = 2 \cdot 3 \cdot 5$ — евклидово число.

Выберем в качестве первых ключей абонентов A и B натуральные числа $a = 7$ и $b = 17$, соответственно. Найдем вторые ключи абонентов A и B — натуральные числа α и β — из сравнений $7 \cdot \alpha \equiv 1 \pmod{30}$ и $17 \cdot \beta \equiv 1 \pmod{30}$. Решив каждое из сравнений и учитывая ограничения $0 < \alpha < p$, $0 < \beta < p$, убеждаемся, что $\alpha = 13$ и $\beta = 23$. Предварительный этап работы завершен.

Составим сообщение для передачи нашему корреспонденту и получим его числовой эквивалент — натуральное число m. Предположим, что в нашем случае $m = 11$. Осуществим описанный выше алгоритм шифрования:

1. $m_1 \equiv 11^a \equiv 11^7 \equiv 11^5 \cdot 11^2 \equiv 6 \cdot (-3) \equiv -18 \equiv 13 \pmod{31}$;
2. $m_2 \equiv 13^b \equiv 13^{17} \equiv (13^3)^5 \cdot 14 \equiv (-4)^5 \cdot 14 \equiv (-64) \cdot 16 \cdot 14 \equiv (-2) \cdot 16 \cdot 14 \equiv$ $\equiv (-14) \equiv 19 \pmod{31}$;

3. $m_3 \equiv 19^{\alpha} \equiv 19^{13} \equiv (19^2)^6 \cdot (-14) \equiv 10^6 \cdot (-14) \equiv 2 \cdot (-14) \equiv -28 \equiv$ $\equiv 3 \pmod{31}$;
4. $m_4 \equiv 3^{\beta} \equiv 3^{23} \equiv (3^5)^4 \cdot 27 \equiv (-5)^4 \cdot (-4) \equiv 5 \cdot (-4) \equiv -20 \equiv 11 \pmod{31}$.

Таким образом, наш корреспондент получил числовой эквивалент m исходного текста. Переведя его в буквенную форму, он без труда прочтет наше сообщение. □

Замечание 1. Не следует забывать, что приведенные в тексте примеры являются лишь простейшими иллюстрациями работы описываемых алгоритмов. Для практических целей используются большие простые числа, имеющее не менее ста десятичных знаков.

Замечание 2. Недостатком криптосистемы без передачи ключей является тот факт, что сообщение «гоняется» туда-обратно несколько раз, что увеличивает возможность создания помех, искажения и потери сообщения.

4.1.2. Криптосистема с открытым ключом

Эта криптосистема имеет и другое название — *система с адресной книгой*, — поскольку каждый абонент, пользующийся ей, имеет свой адрес.

Для его построения каждый из абонентов — предположим, что это абонент A, — выбирает два простых числа p_1 и p_2 (на практике — очень больших) и находит их произведение $r_A = p_1 \cdot p_2$. Вычислив $\varphi(r_A) = (p_1 - 1) \cdot (p_2 - 1)$, абонент A выбирает свой открытый ключ a из условий $a \in \mathbb{N}$, $(a, \varphi(r_A)) = 1$, $0 < a < \varphi(r_A)$. Секретный ключ α определяется теперь однозначно из условий $\alpha \in \mathbb{N}$, $a \cdot \alpha \equiv 1 \pmod{\varphi(r_A)}$, $0 < \alpha < \varphi(r_A)$. Аналогичные действия выполняет любой другой абонент, скажем, абонент B.

Таким образом, на предварительном этапе работы абоненты A и B обладают следующей информацией:

A: $p_1, p_2 \in P$ большие; $r_A = p_1 \cdot p_2$; $\varphi(r_A) = (p_1 - 1) \cdot (p_2 - 1)$.
Открытый ключ: $a \in \mathbb{N}$, $(a, \varphi(r_A)) = 1$, $0 < a < \varphi(r_A)$.
Секретный ключ: $\alpha \in \mathbb{N}$, $a \cdot \alpha \equiv 1 \pmod{\varphi(r_A)}$, $0 < \alpha < \varphi(r_A)$.

B: $q_1, q_2 \in P$ большие, $r_B = q_1 \cdot q_2$; $\varphi(r_B) = (q_1 - 1) \cdot (q_2 - 1)$.
Открытый ключ: $b \in \mathbb{N}$, $(b, \varphi(r_B)) = 1$, $0 < b < \varphi(r_B)$.
Секретный ключ: $\beta \in \mathbb{N}$, $b \cdot \beta \equiv 1 \pmod{\varphi(r_B)}$, $0 < \beta < \varphi(r_B)$.

В открытый доступ абонент A (как и любой другой абонент системы) предоставляет используемый им модуль $r_A = p_1 q_1$ и открытый ключ a. Сами простые числа p_1 и q_1 (а, следовательно, и $\varphi(r_A) = (p_1 - 1) \cdot (p_2 - 1)$), и ключ b абонент A держит в секрете.

По результатам имеющейся открытой информации составляется телефонная книга.

Абонент	Модуль	Открытый ключ
A	r_A	a
B	r_B	b

Она содержит доступную всем желающим часть полной информации о системе, представленной в следующей таблице.

Абонент	Модуль n	Откр. ключ	Простые числа p, q	$\varphi(n)$	Секр. ключ
A	r_A	a	p_1, q_2	$(p_1-1)(q_1-1)$	α
B	r_B	b	p_2, q_2	$(p_1-1)(p_2-1)$	β

Схема работы алгоритма заключается в следующем.

1. Абонент A составляет сообщение для абонента B и кодирует его в виде числа m, $0 < m < r_B$. Затем абонент A шифрует сообщение m открытым ключом b абонента B:

$$m_1 \equiv m^b \pmod{r_B}, \quad 0 < m_1 < r_B;$$

полученное сообщение m_1 абонент A отправляет абоненту B.

2. Абонент B расшифровывает сообщение m_1 своим секретным ключом β:

$$m_2 \equiv m_1^{\beta} \pmod{r_B}, \quad 0 < m_1 < r_B.$$

В этом случае $m_2 = m$, и абонент B получает возможность прочитать исходное сообщение от абонента A, переведя число m в буквенную форму.

Доказательство корректности работы описанного выше алгоритма также не представляет особого труда. Поскольку

$$m_2 \equiv m_1^{\beta} \equiv m^{b\cdot\beta} \pmod{r_B},$$

а ключи абонента B были выбраны так, что $b\beta \equiv 1 \pmod{\varphi(r_B)}$, то $m_2 \equiv m^1 \pmod{r_B}$, и, поскольку имеют место ограничения $0 < m_2 < r_B$, $0 < m < r_B$, мы получаем, что $m_2 = m$; в ходе работы абонент B действительно получит числовой эквивалент m исходного сообщения от абонента A.

Замечание. *В принципе m может быть таково, что $(m, pq) \neq 1$. В этом случае, оставив в стороне тривиальную ситуацию, получим две «симметричные» возможности: $p|m$ и $q \nmid m$ или $q|m$ и $p \nmid m$. Рассмотрим первую из них: поскольку $p|m$, то $m \equiv 0 \pmod{p}$, и, следовательно, $m^\alpha \equiv 0 \pmod{p}$, $m^\beta \equiv 0 \pmod{p}$, то есть $m^\alpha \equiv m^\beta \equiv 0 \pmod{p}$; поскольку $q \nmid m$, то $(m, q) = 1$, и, следовательно, из сравнения $\alpha \equiv \beta \pmod{q-1}$ вытекает, что $m^\alpha \equiv m^\beta \pmod{q}$. Таким образом, мы получаем, что $m^\alpha \equiv m^\beta \pmod{pq}$.*

Пример 4.1.2 Рассмотрим передачу сообщения от абонента A абоненту B в системе с открытым ключом, параметры которой заданы в нижеследующей таблице.

Абонент	Простые числа p, q	Модуль n	$\varphi(n)$	Откр. ключ	Секр. ключ
A	$p_1 = 19$, $p_2 = 29$	$r_A = 551$	$\varphi(r_A) = 504$	$a = 5$	$\alpha = 101$
B	$q_1 = 5$, $q_2 = 11$	$r_B = 55$	$\varphi(r_B) = 40$	$b = 3$	$\beta = 27$

Предположим, что числовой эквивалент пересылаемого сообщения получен и имеет вид $m = 6$. Осуществим описанный выше алгоритм шифрования:

1. $m_1 \equiv m^3 \equiv 6^a \equiv 6^3 \equiv 6^2 \cdot 6 \equiv (-19) \cdot 6 \equiv -60 - 54 \equiv -5 + 1 \equiv \equiv -4 \equiv 51 \pmod{55}$;
2. $m_2 \equiv 51^{27} \equiv (-4)^{27} \equiv -(2^2)^{27} \equiv -(2^{27})^2 \equiv -((2^6)^4 \cdot 2^3)^2 \equiv -(64^4 \cdot 8)^2 \equiv \equiv -9^8 \cdot 64 \equiv -26^4 \cdot 9 \equiv -13^4 \cdot 2^4 \cdot 9 \equiv -256 \cdot 9 \equiv 19 \cdot 9 \equiv 90 + 81 \equiv 35 + 26 \equiv \equiv 61 \equiv 6 \pmod{55}$.

Таким образом, наш корреспондент получил числовой эквивалент m исходного текста. Переведя его в буквенную форму, он без труда прочтет исходное сообщение. □

Замечание. *При работе криптосистемы с открытым ключом абонент A никак не пользуется своими ключами. Следовательно, недостатком этой системы является тот факт, что неизвестно, от кого пришло сообщение, то есть существует возможность его подмены.*

4.1.3. Электронная подпись

При описании данного алгоритма будем считать, что в его работе принимают участие банкир B и несколько вкладчиков $W, W_1, W_2, \ldots W_n$.

Подготовительный этап работы совпадает с аналогичным этапом для системы с открытым ключом. Именно, банкир B выбирает два простых числа p_1 и p_2; находит их произведение $R = p_1 \cdot p_2$; вычисляет

$\varphi(R) = (p_1 - 1) \cdot (p_2 - 1)$; выбирает свой открытый ключ S из условий $S \in \mathbb{N}$, $(S, \varphi(R)) = 1$, $0 < S < \varphi(R)$; находит свой секретный ключ T из условий $T \in \mathbb{N}$, $S \cdot T \equiv 1 \pmod{\varphi(R)}$, $0 < \alpha < \varphi(R)$. Аналогичные действия выполняет каждый из вкладчиков $W, W_1, W_2, \ldots W_n$.

Таким образом, на предварительном этапе разрабатывается информация о системе, представленная в следующей таблице.

Абонент	Простые числа p, q	Модуль n	Откр. ключ	Секр. ключ
B	p_1, p_2	$R = p_1 \cdot p_2$	S	T
W	q_1, q_2	$r = q_1 \cdot q_2$	s	t
W_1	q_1^1, q_2^1	$r_1 = q_1^1 \cdot q_2^1$	s_1	t_1
W_2	q_1^2, q_2^2	$r_2 = q_1^2 \cdot q_2^2$	s_2	t_2
...				

Схема работы алгоритма заключается в следующем.

1. Пусть m, $0 < m < r$, — числовой эквивалент сообщения, составленного вкладчиком W для банкира B. (Убедимся, что, кроме того, выполняется и ограничение $0 < r < R$.) Вкладчик W шифрует сообщение m своим секретным ключом t:

$$SW: \ m_1 \equiv m^t \pmod{r}, \ 0 < m_1 < r;$$

полученный результат m_1 он шифрует открытым ключом банкира S:

$$OB: \ m_2 \equiv m_1^S \pmod{R}, \ 0 < m_2 < R;$$

полученное сообщение m_2 вкладчик W отправляет банкиру B.

2. Банкир B преобразует сообщение m_2 своим секретным ключом T:

$$SB: \ m_3 \equiv m_2^T \pmod{R}, \ 0 < m_3 < R,$$

а затем расшифровывает полученный результат m_3 открытым ключом вкладчика W:

$$OW: \ m_4 \equiv m_3^s \pmod{r}, \ 0 < m_4 < r.$$

В этом случае $m_4 = m$, и банкир B получает возможность прочитать исходное сообщение от вкладчика W, переведя число m в буквенную форму.

Доказательство корректности данного алгоритма несколько сложнее предыдущих, но тоже не требует больших усилий. Сначала убедимся, что при реализации алгоритма $m_3 = m_1$. Действительно,

$$m_3 \equiv m_2^T \equiv m_1^{ST} \equiv m_1 \pmod{R},$$

и, поскольку $0 < m_1 < r < R$, $0 < m_3 < R$, то $m_3 = m_1$. Теперь нетрудно проверить, что $m_4 \equiv m_3^s \equiv m_1^s \equiv m^{st} \equiv m \pmod{r}$, и, поскольку $0 < m_1 < r$, $0 < m_4 < r$, то $m_4 = m$.

Замечание. *При доказательстве корректности работы алгоритма мы существенно использовали ограничение $r < R$. При данном ограничении схема работы алгоритма выглядела так: SW, OB, SB, OW. Если же $R < r$, то порядок действий будет иным: OB, SW, OW, SB. (Последовательность работы выбирается так, чтобы сравнения по большему модулю были «внутри».) Докажите корректность работы модифицированного алгоритма самостоятельно.*

Пример 4.1.3 Рассмотрим систему с параметрами, заданными в таблице.

Абонент	Простые числа p, q	Модуль	Открытый ключ	Секретный ключ
B	5, 11	$R = 55$	$OB = 3$	$SB = 27$
W	13, 7	$r = 91$	$OW = 5$	$SW = 29$
...				

Пусть числовой эквивалент сообщения, составленного вкладчиком W, имеет вид $m = 6$. Убедившись, что $0 < m < r$ и заметив, что $0 < R < r$, осуществим применимый в данных условиях алгоритм шифрования.

1. Вкладчик W шифрует сообщение m по меньшему модулю, то есть модулю банкира, следовательно, использует открытый ключ OB банкира:

$$OB: \ m_1 \equiv 6^3 \equiv 216 \equiv 51 \pmod{55}, \ 0 < m_1 < 55;$$

полученный результат $m_1 = 51$ вкладчик W шифрует своим секретным ключом SW:

$$SW: \ m_2 \equiv 51^{29} \equiv 25 \pmod{91}, \ 0 < m_2 < 91;$$

результат m_2 он отправляет банкиру B.

2. Банкир B, отмечая, что его модуль меньше модуля вкладчика, начинает работу по большему модулю (модулю вкладчика) и, следовательно, действует его открытым ключом OW:

$$OW: \ m_3 \equiv 25^5 \equiv 51 \pmod{91}, \ 0 < m_3 < 91;$$

затем он расшифровывает полученный результат m_3 своим секретным ключом SB:

$$SB: \ m_4 \equiv 51^{27} \equiv 6 \pmod{55}, \ 0 < m_4 < 55.$$

Как и ожидалось, $m_4 = m$, то есть банкир получил числовой эквивалент $m = 6$ сообщения вкладчика W. При этом было получено и подтверждение того факта, что сообщение отправлено именно вкладчиком W.

Если же при тех же исходных данных вкладчик W, передавая сообщение $m = 7$, начнет свои действия с работы своим секретным ключом t, то будет получена следующая картина:

$$SW: \ m_1 \equiv 7^{29} \equiv 63 \pmod{r},$$

что больше, чем модуль банкира $R = 55$. Таким образом, при последующем шифровании открытым ключом банкира по модулю 55 сообщение исказится, поскольку будет использоваться величина $m_1 \equiv 63 \equiv 8 \pmod{55}$. □

Упражнения

(1) Найдите k различных пар (a, α) ключей для работы системы «без передачи ключей» по модулю p:

a) $k = 2$, $p = 103$;
b) $k = 3$, $p = 87$;
c) $k = 4$, $p = 61$;
d) $k = 3$, $p = 97$;
e) $k = 4$, $p = 73$;
f) $k = 2$, $p = 113$;
g) $k = 3$, $p = 89$;
h) $k = 4$, $p = 67$.

(2) Найдите k различных пар (a, α) ключей для работы системы «с открытым ключом», использующей модуль $p_1 \cdot p_2$:

a) $k = 2$, $p_1 = 103$, $p_2 = 31$;
b) $k = 3$, $p_1 = 113$, $p_2 = 29$;
c) $k = 4$, $p_1 = 97$, $p_2 = 37$;
d) $k = 2$, $p_1 = 101$, $p_2 = 89$;
e) $k = 3$, $p_1 = 73$, $p_2 = 23$;
f) $k = 4$, $p_1 = 127$, $p_2 = 19$;
g) $k = 2$, $p_1 = 89$, $p_2 = 79$;
h) $k = 3$, $p_1 = 47$, $p_2 = 89$;

(3) Для работы в системе «без передачи ключей» по модулю p найдите ключ α, если известен ключ a:

a) $p = 31$, $a = 7$;
b) $p = 71$, $a = 17$;
c) $p = 137$, $a = 5$;
d) $p = 61$, $a = 11$;
e) $p = 101$, $a = 7$;
f) $p = 113$, $a = 3$.

(4) Для работы системы «с открытым ключом», использующей модуль $p_1 \cdot p_2$, найдите ключ a, если известен ключ α:

a) $p_1 = 13$, $p_2 = 11$, $\alpha = 77$;
b) $p_1 = 17$, $p_2 = 29$, $\alpha = 55$;
c) $p_1 = 37$, $p_2 = 5$, $\alpha = 65$;
d) $p_1 = 101$, $p_2 = 3$, $\alpha = 91$;
e) $p_1 = 73$, $p_2 = 5$, $\alpha = 105$;
f) $p_1 = 31$, $p_2 = 13$, $\alpha = 133$;
g) $p_1 = 29$, $p_2 = 11$, $\alpha = 57$;
h) $p_1 = 41$, $p_2 = 5$, $\alpha = 21$.

⑤ Найдите наименьшее неотрицательное число x, такое что:

a) $x \equiv 177^{1000} \pmod{10}$;
b) $x \equiv 3^{49} \pmod{15}$;
c) $x \equiv 2^{6000} \pmod{24}$;
d) $x \equiv 714^{3043} \pmod{52}$;
e) $x \equiv 714^{3034} \pmod{58}$;
f) $x \equiv 315^{487} \pmod{85}$;
g) $x \equiv 2^{1000} \pmod{100}$;
h) $x \equiv 15^{1000} \pmod{189}$;
i) $x \equiv 21^{1000} \pmod{297}$;
j) $x \equiv 21^{1073} \pmod{693}$.

⑥ Зашифруйте сообщение m, получив шифротекст x как наименьшее целое неотрицательное число, такое что $x \equiv m^{\alpha} \pmod{n}$:

a) $m = 14,\ n = 15, \alpha = 11$;
b) $m = 18,\ n = 21, \alpha = 11$;
c) $m = 3,\ n = 22, \alpha = 13$;
d) $m = 30,\ n = 33, \alpha = 9$;
e) $m = 28,\ n = 35, \alpha = 15$;
f) $m = 31,\ n = 37, \alpha = 12$;
g) $m = 16,\ n = 39, \alpha = 35$;
h) $m = 4,\ n = 41, \alpha = 37$.

⑦ Подготовьте к работе систему «без передачи ключей» по модулю 19: выберите пару ключей (a, α) для абонента A и пару ключей (b, β) для абонента B. Осуществите отправку сообщения m абоненту B, если

a) $m = 10$;
b) $m = 11$;
c) $m = 12$;
d) $m = 13$;
e) $m = 14$;
f) $m = 15$;
g) $m = 16$;
h) $m = 17$.

⑧ Подготовив к работе систему «без передачи ключей» по модулю p, осуществите отправку сообщения m абоненту B, если

a) $p = 23,\ m = 17$;
b) $p = 29,\ m = 8$;
c) $p = 31,\ m = 13$;
d) $p = 37,\ m = 30$;
e) $p = 41,\ m = 10$;
f) $p = 43,\ m = 12$;
g) $p = 47,\ m = 11$;
h) $p = 53,\ m = 48$;
i) $p = 59,\ m = 22$.

⑨ Используя систему «без передачи ключей» осуществите передачу слова «ДА», записанного в 33-буквенном русском алфавите А=00, Б=01, ..., Я=32, для чего подберите наименьший подходящий модуль.

⑩ Подготовьте к работе систему «с открытым ключом» на базе модулей 91 и 77: рассмотрев модуль $91 = 7 \cdot 13$, вычислите $\varphi(91)$ и подберите пару ключей (a, α) для абонента A; рассмотрев модуль $77 = 7 \cdot 11$, вычислите $\varphi(77)$ и подберите пару ключей (b, β) для абонента B. Осуществите отправку сообщения m абоненту B, если

a) $m = 10$;
b) $m = 11$;
c) $m = 12$;
d) $m = 13$;
e) $m = 14$;
f) $m = 15$;
g) $m = 16$;
h) $m = 17$.

(11) Подготовив к работе систему «с открытым ключом» на базе модулей $r_A = p_1 \cdot p_2$ и $r_B = q_1 \cdot q_2$, осуществите отправку сообщения m абоненту B, если

a) $p_1 = 7, p_2 = 23,$ $q_1 = 5, q_2 = 11, m = 40;$

b) $p_1 = 11, p_2 = 17,$ $q_1 = 3, q_2 = 7, m = 19;$

c) $p_1 = 13, p_2 = 19,$ $q_1 = 5, q_2 = 17, m = 32;$

d) $p_1 = 7, p_2 = 19,$ $q_1 = 11, q_2 = 19, m = 84;$

e) $p_1 = 11, p_2 = 23,$ $q_1 = 3, q_2 = 29, m = 20;$

f) $p_1 = 5, p_2 = 29,$ $q_1 = 7, q_2 = 11, m = 60;$

g) $p_1 = 5, p_2 = 31,$ $q_1 = 11, q_2 = 13, m = 120;$

h) $p_1 = 11, p_2 = 13,$ $q_1 = 5, q_2 = 19, m = 65.$

(12) Используя систему «с открытым ключом» зашифруйте слово «ШИФР», для чего подберите наименьший подходящий модуль.

(13) Подготовьте к работе систему «электронная подпись» на базе модулей $221 = 13 \cdot 17$ и $201 = 19 \cdot 11$: вычислив $\varphi(55)$, подберите пару ключей (S, T) для банкира B; вычислив $\varphi(51)$, подберите пару ключей (s, t) для вкладчика W. Осуществите отправку сообщения m, составленного вкладчиком W, банкиру B, если

a) $m = 11;$ c) $m = 123;$ e) $m = 41;$ g) $m = 16;$

b) $m = 101;$ d) $m = 13;$ f) $m = 51;$ h) $m = 17.$

Что изменится в схеме работы, если то же сообщение было отправлено банкиром B вкладчику W? Осуществите передачу сообщения m в этом случае.

Задачи

1 Пусть n — натуральное число, большее единицы, и a — целое число, такое что $(a, n) = 1$. Докажите следующие утверждения:

a) $a^{\varphi(n)} \equiv 1 \pmod{n}$ (*теорема Эйлера*);

b) если $\alpha \equiv \beta \pmod{\varphi(n)}$, то $a^\alpha \equiv a^\beta \pmod{n}$;

c) если $P_n(a)$ — *показатель числа a по модулю n* (то есть наименьшее натуральное число γ, такое что $a^\gamma \equiv 1 \pmod{n}$), то $P_n(a) | \varphi(n)$;

d) $a^\alpha \equiv a^\beta \pmod{n}$ тогда и только тогда, когда $\alpha \equiv \beta \pmod{P_n(a)}$.

2 Используя систему «без передачи ключей» осуществите передачу сообщения «KEY», для чего подберите подходящий модуль и ключи. Проведите шифрование в обе стороны.

3 В системе «без передачи ключей» на базе модуля p укажите количество возможных пар шифрующих ключей (с учетом порядка):

a) $p = 31$; c) $p = 41$; e) $p = 43$; g) $p = 61$;
b) $p = 37$; d) $p = 47$; f) $p = 59$; h) $p = 67$.

4 Найдите такой модуль для системы «без передачи ключей», чтобы в качестве ключей можно было использовать числа 3, 5, 7, 9, 11, 13, 15, 17, 19, 21.

5 Найдите все пары совпадающих ключей при использовании системы «без передачи ключей» по модулю 31.

6 Приведите пример модуля, по которому существуют ровно 3 пары совпадающих ключей при использовании системы «без передачи ключей».

7 Приведите пример модуля, по которому нет пар совпадающих ключей при использовании системы «без передачи ключей».

8 В системе «с открытым ключом», использующей модуль 259, укажите количество возможных пар шифрующих ключей, соответствующих этому модулю (с учетом порядка).

9 Укажите количество возможных пар шифрующих ключей по каждому из модулей в системе «с открытым ключом» на базе модулей $r_A = p_1 \cdot p_2$ и $r_B = q_1 q_2$:

a) $p_1 = 7, p_2 = 23$, $q_1 = 5, q_2 = 11$;
b) $p_1 = 11, p_2 = 17$, $q_1 = 3, q_2 = 7$;
c) $p_1 = 13, p_2 = 19$, $q_1 = 5, q_2 = 17$;
d) $p_1 = 7, p_2 = 19$, $q_1 = 11, q_2 = 19$;
e) $p_1 = 11, p_2 = 23$, $q_1 = 3, q_2 = 29$;
f) $p_1 = 5, p_2 = 29$, $q_1 = 7, q_2 = 11$;
g) $p_1 = 5, p_2 = 31$, $q_1 = 11, q_2 = 13$;
h) $p_1 = 11, p_2 = 13$, $q_1 = 5, q_2 = 19$.

В каждом из случаев подсчитайте общее число вариантов использования системы.

10 Найдите такой модуль для системы «с открытым ключом», чтобы в качестве ключей можно было использовать числа 3, 5, 7, 9, 11, 13,15.

11 Сравните количества различных пар ключей для модулей 69 и 65.

12 Почему число 2047 будет неудачным выбором для модуля в системе «с открытым ключом»? Приведите примеры подобных «неудачных» модулей.

13 Среди модулей 1541, 1081, 493 выберите наиболее удачный для системы «с открытым ключом». Обоснуйте свой выбор.

14 Докажите, что если в системе «с открытым ключом» модуль равен 35, то секретные и открытые ключи будут совпадать. Можно ли привести пример еще одного такого модуля?

15 Найдите все пары совпадающих ключей при использовании системы «с открытым ключом» по модулю 91, 109, 137, 143, 187, 209.

16 Докажите, что в качестве ключей любой из систем могут выступать только нечетные числа.

17 Докажите, что в системе «с открытым ключом» всегда найдутся «неподвижные» сообщения — сообщения, переводимые ключами шифрования в себя.

18 Докажите, что в системе «с открытым ключом» всегда найдутся ключи, переводящие все сообщения в себя. Приведите соответствующие примеры, используя модуль r:

a) $r = 33$; b) $r = 55$; c) $r = 77$; d) $r = 65$; e) $r = 91$; f) $r = 221$.

19 Если в системе «с открытым ключом» в качестве модуля рассматривать произведение трех простых чисел, то какие преимущества появятся у системы и какие недостатки?

20 Подготовив к работе систему «электронная подпись» на базе модуля банкира $R = p_1 \cdot p_2$ и модуля вкладчика $r = q_1 \cdot q_2$, осуществите отправку сообщения m банкиру B, если

a) $p_1 = 7, p_2 = 23,$ $q_1 = 5, q_2 = 11, m = 40;$

b) $p_1 = 11, p_2 = 17,$ $q_1 = 3, q_2 = 7, m = 19;$

c) $p_1 = 13, p_2 = 19,$ $q_1 = 5, q_2 = 17, m = 32;$

d) $p_1 = 7, p_2 = 19,$ $q_1 = 11, q_2 = 19, m = 84;$

e) $p_1 = 11, p_2 = 23,$ $q_1 = 3, q_2 = 29, m = 20;$

f) $p_1 = 5, p_2 = 29,$ $q_1 = 7, q_2 = 11, m = 60;$

g) $p_1 = 5, p_2 = 31,$ $q_1 = 11, q_2 = 13, m = 120;$

h) $p_1 = 11, p_2 = 13,$ $q_1 = 5, q_2 = 19, m = 65.$

Что изменится в схеме работы, если то же сообщение было отправлено банкиром B вкладчику W? Осуществите передачу сообщения m в этом случае.

21 Приведите пример неоднозначного дешифрования в системе «электронная подпись» при использовании неправильного порядка взятия ключей.

22 Приведите пример неоднозначного шифрования в системе «электронная подпись» при использовании числа, превышающего один из модулей.

4.2. Дискретный логарифм

На первый взгляд, нет ничего проще, чем вскрыть систему *RSA*: для этого достаточно найти метод обнаружения секретного ключа противника. А для этого «всего лишь» требуется, зная произведение двух простых чисел q_1 и q_2 (модуль, используемый противником) вычислить величину $\varphi(q_1q_2) = (q_1 - 1)(q_2 - 1)$ и, используя известное натуральное b (открытый ключ), найти натуральное число β, удовлетворяющее условиям $b \cdot \beta \equiv 1 \pmod{\varphi(p_1p_2)}$, $0 < \beta < \varphi(p_1p_2)$. Однако для решения данной задачи нам придется найти простые числа, образующие модуль, для чего потребуется разложить его на множители. При достаточно больших простых числах q_1 и q_2 эта операция крайне трудоемка и требует для своего осуществления слишком много времени.

Поиск других путей вскрытия сообщения, зашифрованного системой *RSA*, а также решение вопросов согласования ключей, приводит нас к задаче *дискретного логарифмирования*.

Если n — натуральное число, и a, b — целые числа, взаимно простые с n, то *дискретным логарифмом числа b с основанием a по модулю n* называют целое неотрицательное число x, такое что

$$a^x \equiv b \pmod{n}.$$

В этом случае пишут, что

$$x = \log_a b \text{ или, короче, } x = \log b.$$

Задачу нахождения числа $x = \log_a b$ при известном модуле n и заданных целых числах a, b и называют задачей дискретного логарифмирования.

Для обсуждения известных на сегодняшний день методов дискретного логарифмирования нам понадобится ряд хорошо известных фактов из курса теории чисел [36], [20], [75].

4.2.1. Показатели, первообразные корни и индексы

Прежде всего, рассмотрим понятие показателя целого числа по заданному модулю и перечислим необходимые для нас свойства показателей.

Для данного натурального числа n и данного целого числа a, взаимно простого с n, *показателем $P_n(a)$ числа a по модулю n* называют наименьшее натуральное число γ, такое что $a^\gamma \equiv 1 \pmod{n}$.

Свойства показателей

1. Если $a \equiv b \pmod{n}$, то $P_n(a) = P_n(b)$.
2. $a^\delta \equiv 1 \pmod{n}$ тогда и только тогда, когда $P_n(a) | \delta$.

3. $P_n(a)|\varphi(n)$; в частности, $1 \leqslant P_n(a) \leqslant \varphi(n)$.
4. $a^\delta \equiv a^\eta \pmod n$ тогда и только тогда, когда $\delta \equiv \eta \pmod{P_n(a)}$.
5. Числа $a^0, a^1, a^2, \ldots a^{P_n(a)-1}$ принадлежат различным классам вычетов по модулю n и образуют циклическую мультипликативную группу порядка $P_n(a)$.
6. Число натуральных чисел, не превосходящих n, показатель которых равен k, равно 0 или $\varphi(k)$; в частности, число классов вычетов по простому модулю p, показатель которых равен k, $k|p-1$, равно $\varphi(k)$.
7. $P_{p_1^{\alpha_1}\ldots p_s^{\alpha_s}}(a) = [P_{p_1^{\alpha_1}}(a), \ldots P_{p_s^{\alpha_s}}(a)]$.
8. $P_n(a^k) = \dfrac{P_n(a)}{(k, P_n(a))}$.

Целое число g называют *первообразным корнем по модулю* n, если $P_n(g) = \varphi(n)$. Другими словами, первообразным корнем является число, обладающее максимальным возможным показателем по модулю n. Этот факт определяет существенную роль первообразных корней в построении теории дискретного логарифмирования.

Свойства первообразных корней

1. Первообразные корни существуют только по модулю $2, 4, p^\alpha$ и $2p^\alpha$, где $p \in P\backslash\{2\}$, $\alpha \in \mathbb{N}$.
2. Для первообразного корня g по модулю n числа $g^0, g^1, g^2, \ldots g^{\varphi(n)-1}$ принадлежат различным классам вычетов по модулю n (пробегая при этом все классы вычетов, взаимно простые с n) и образуют циклическую мультипликативную группу порядка $\varphi(n)$.

Если g является первообразным корнем по модулю n, то для любого целого числа a, взаимно простого с n, имеет место сравнение $a \equiv g^\beta \pmod n$, где $\beta \in \{0, 1, \ldots \varphi(n) - 1\}$. Число β называют *индексом числа a с основанием g по модулю n*. В этом случае пишут, что

$$\beta = \operatorname{ind}_g a, \text{ или, короче, } \beta = \operatorname{ind} a.$$

Очевидно, что в терминах, введенных выше, число β является дискретным логарифмом числа a с основанием g по модулю n, и мы можем использовать обозначение $\beta = \log_g a$, или, короче, $\beta = \log a$. Поскольку в основе дискретного логарифмирования лежат теоретико-числовые вопросы исследования индексов, мы, как правило, будем пользоваться теоретико-числовой терминологией.

Таким образом, под задачей дискретного логарифмирования $a^x \equiv b \pmod n$ мы прежде всего понимаем, при заданном модуле n, целом числе b, взаимно простом с n, и целом a, являющимся первообразным

корнем по модулю n, задачу нахождения индекса x числа b по модулю n с основанием a. Эта задача всегда имеет решение, которое, при условии $x \in \{0, 1, 2, \ldots \varphi(n)\}$, является единственным.

Поскольку первообразные корни существуют только по модулям $n \in \in \{2, 4, p^\alpha, 2p^\alpha\}$, где $p \in P\backslash\{2\}$, и $\alpha \in \mathbb{N}$, то и классическая теория индексов применима только к модулям n из указанного списка. В частности, мы всегда можем говорить об индексах по простому модулю p.

Однако в случае вычисления дискретного логарифма мы, исходя из практических соображений, вынуждены рассматривать в качестве его основания a не только первообразные корни по модулю n, но и любой вычет, взаимно простой с n. В случае основания a, не равного первообразному корню по модулю n, понятие индекса можно ввести аналогичным образом: для натурального n и целых чисел a, b, взаимно простых с n, *индексом* $\mathrm{ind}_a b$ *числа* b *с основанием* a *по модулю* n называют целое неотрицательное число x, такое что $a^x \equiv b \pmod n$. Однако если основание a не является первообразным корнем, его целые неотрицательные степени a^i образуют циклическую группу порядка $P_n(a) < \varphi(n)$, и индексы с основанием a будут определены не для всех вычетов, взаимно простых с модулем n. Другими словами, задача дискретного логарифмирования в этом случае может не иметь решений.

В каждом из указанных случаев мы можем пользоваться для вычисления дискретного логарифма известными свойствами индексов, учитывая, что, в случае первообразного корня, $P_n(a) = \varphi(n)$ и, в случае простого числа, $\varphi(p) = p - 1$.

Свойства индексов

1. $\mathrm{ind}\ \ 1 \equiv 0 \pmod{P_n(a)}$.
2. Если $a \equiv b \pmod n$, то $\mathrm{ind}\, a \equiv \mathrm{ind}\, b \pmod{P_n(a)}$.
3. $\mathrm{ind}\, ab \equiv \mathrm{ind}\, a + \mathrm{ind}\, b \pmod{P_n(a)}$.
4. $\mathrm{ind}\, a^k \equiv k\ \mathrm{ind}\, a \pmod{P_n(a)}$ для любого целого неотрицательного числа k.
5. $P_n(a) = \dfrac{\varphi(n)}{(\mathrm{ind}\, a, \varphi(n))}$.

4.2.2. Метод перебора

Метод перебора является простейшим методом нахождения дискретного логарифма: для нахождения $x = \mathrm{ind}_a b$ достаточно рассмотреть по модулю n все степени $a^0, a^1, a^2, \ldots a^{\varphi(n)-1}$ [20], [36], [78].

Пример 4.2.4 Решим сравнение $2^x \equiv 9 \pmod{11}$, то есть найдем $x = \operatorname{ind}_2 9$ — индекс (дискретный логарифм) числа 9 с основанием 2 по модулю 11.

Рассмотрим вычет 2. Он является первообразным корнем по модулю 11. Действительно, $(2, 11) = 1$, и, рассматривая возможные значения 1, 2, 5, 10 показателей по модулю 11, мы убеждаемся в том, что $2^{10} \equiv 1 \pmod{11}$, но $2^5 \not\equiv 1 \pmod{11}$, $2^2 \not\equiv 1 \pmod{11}$, и $2^1 \not\equiv 1 \pmod{11}$. Отсюда следует, что числа 2^0, 2^1, 2^2, ..., 2^9 образуют приведенную систему вычетов по модулю 11. Именно, $2^0 \equiv 1 \pmod{11}$, $2^1 \equiv 2 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^4 \equiv 5 \pmod{11}$, $2^5 \equiv 10 \pmod{11}$, $2^6 \equiv 9 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$, $2^8 \equiv 3 \pmod{11}$, $2^9 \equiv 6 \pmod{11}$. Таким образом, $\operatorname{ind}_2 1 = 0$, $\operatorname{ind}_2 2 = 1$, $\operatorname{ind}_2 3 = 8$, $\operatorname{ind}_2 4 = 2$, $\operatorname{ind}_2 5 = 4$, $\operatorname{ind}_2 6 = 9$, $\operatorname{ind}_2 7 = 7$, $\operatorname{ind}_2 8 = 3$, $\operatorname{ind}_2 9 = 6$, $\operatorname{ind}_2 10 = 5$, и мы можем построить таблицу индексов по модулю 11, используя первообразный корень 2.

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 a$	0	1	8	2	4	9	7	3	6	5

Из таблицы следует, что $x = \operatorname{ind}_2 9 = 6$. Наша задача полностью решена.

Более того, мы окончательно решили вопрос нахождения дискретных логарифмов по модулю 11: чтобы найти тот или иной дискретный логарифм по модулю 11, достаточно воспользоваться нашей таблицей.

Так, для нахождения $y = \operatorname{ind}_2 4$ мы, пользуясь таблицей, просто выпишем значение $x = 4$.

А что делать, если требуется найти $\operatorname{ind}_6 4$?

Прежде всего, используя полученную таблицу, убедимся, что 6 является первообразным корнем по модулю 11: поскольку $P_p(a) = \dfrac{p-1}{(\operatorname{ind} a, p-1)}$, то число a является первообразным корнем по модулю p, то есть обладает свойством $P_p(a) = p - 1$, тогда и только тогда, когда $(\operatorname{ind} a, p-1) = 1$. Таким образом, индексами первообразных корней по модулю 11 будут числа, индексы которых взаимно просты с 10, то есть числа 1, 3, 5 и 7. Следовательно, первообразными корнями по модулю 11 являются числа 2, 6, 7 и 8 (точнее, все числа, принадлежащие классам вычетов $\mathbf{2}_{11}$, $\mathbf{6}_{11}$, $\mathbf{7}_{11}$ и $\mathbf{8}_{11}$).

Перейдем к нахождению индекса числа 4 с основанием 6 по модулю 11. Из определения следует, что $\operatorname{ind}_6 4 = \beta_1$, где $4 \equiv 6^{\beta_1} \pmod{11}$. Пользуясь свойствами индексов, мы получим сравнение $\beta_1 \cdot \operatorname{ind}_2 6 \equiv \operatorname{ind}_2 4 \pmod{10}$, и, консультируясь с таблицей, перейдем к сравнению $9\beta_1 \equiv 2 \pmod{10}$. Отсюда следует, что $\beta_1 \equiv 8 \pmod{10}$, то есть $\beta_1 = 8$. Таким образом, $\operatorname{ind}_6 4 = 8$.

Впрочем, на практике вопрос решения задачи дискретного логарифмирования $a^x \equiv b \pmod p$ далеко не всегда ограничивается случаем первообразного корня a. Что делать, если требуется найти, например, $\operatorname{ind}_5 4$, то есть решить задачу $5^x \equiv 4 \pmod{11}$? Вновь воспользуемся свойствами индексов и перейдем к сравнению $x \cdot \operatorname{ind} 5 \equiv \operatorname{ind} 4 \pmod{10}$. Консультируясь с таблицей, получим сравнение $4x \equiv 2 \pmod{10}$. Сократив все три части полученного сравнения на 2, придем к сравнению $2x \equiv 1 \pmod 5$, или, что то же, к сравнению $2x \equiv 6 \pmod 5$. Следовательно, $x \equiv 3 \pmod 5$. Наименьшее целое неотрицательное число, удовлетворяющее этому сравнению, равно 3. Таким образом, $\operatorname{ind}_5 4 = 3$.

С другой стороны, если требуется найти, например, $\operatorname{ind}_{10} 4$, то есть решить задачу $10^x \equiv 4 \pmod{11}$, то аналогичные преобразования приведут нас к сравнению $x \cdot \operatorname{ind} 10 \equiv \operatorname{ind} 4 \pmod{10}$. Консультируясь с таблицей, перейдем к сравнению $5x \equiv 2 \pmod{10}$. Поскольку $(5, 10) = 5$ и $5 \nmid 2$, то данное сравнение решений не имеет, и наша задача неразрешима. □

Мы убедились, что для малых простых чисел p задача дискретного логарифмирования полностью решается составлением соответствующей таблицы индексов. Однако с ростом модуля построение таблиц индексов становится все более трудоемкой и с какого-то момента невыполнимой на практике задачей. В этой ситуации на помощь приходят более «экономные» методы отыскания дискретного логарифма.

4.2.3. Метод согласования

Метод согласования, предложенный в 1962 г. Александром Осиповичем Гельфондом (1906–1968), является одним из первых методов такого рода. Он реализует алгоритм решения сравнения $a^x \equiv b \pmod p$, где $p \in P\backslash\{2\}$, и $(a, p) = (b, p) = 1$. Позже данный алгоритм был независимо описан Даниэлем Шенксом (Daniel Shanks, 1917–1996) и получил название *метода больших и малых шагов* (*baby steps and gigant steps*) [22], [74], [68], [78], [90] .

В основе метода лежит следующий хорошо известный теоретико-числовой факт: *пусть* $p \in P\backslash\{2\}$ *и* $h = \lfloor\sqrt{p}\rfloor$; *тогда для любого целого числа* x, $0 \leqslant x < p$, *найдутся такие целые числа* l, t, *что* $x = hl - t$, *и* $0 < l \leqslant h$, $0 \leqslant t < h$. (Для его доказательства достаточно рассмотреть $l = \left\lfloor \dfrac{x}{h} \right\rfloor$, и $t = hl - x$.)

В этих условиях для нахождения числа x из сравнения $b \equiv a^x \pmod p$ воспользуемся полученным разложением: $b \equiv a^x \equiv (a^h)^l \cdot a^{-t} \pmod p$, или $b \cdot a^t \equiv (a^h)^l \pmod p$. Это означает, что искомые значения l, t могут быть найдены перебором величин $b \cdot a^t$ и $(a^h)^l$ в указанных границах, а после этого будет определена и величина x.

Другими словами, *алгоритм метода согласования* заключается в следующем.

1. Для всех возможных значений $t = 0, \ldots, h-1$ вычислим вычеты $ba^t \pmod p$.
2. Вычисляя вычеты $(a^h)^l \pmod p$ последовательно для $l = 1, 2, \ldots, h$, будем сравнивать полученные значения со значениями первой последовательности.
3. Как только будет найдено совпадение элемента из второго множества с некоторым элементом первого множества, мы определим неизвестные l, t и вычислим $x = hl - t$.

Пример 4.2.5 Найдем x, удовлетворяющее сравнению $2^x \equiv 9 \pmod{23}$, пользуясь методом согласования. В нашем случае $p = 23$, $a = 2$, и $b = 9$. Найдем $h = \lfloor \sqrt{p} \rfloor = 4$ и составим таблицу возможных значений величины $ba^t \pmod p$, $t = 0, 1, 2, 3$.

t	0	1	2	3
ba^t	9	18	13	3

Теперь составим таблицу возможных значений величины $(a^h)^l \ mod\ p$, $l = 1, 2, 3, 4$.

l	1	2	3	4
$(a^h)^l$	16	3	2	9

Легко заметить, что в обеих таблицах содержится одно и тоже значение 3 — последующие значения величины $(a^h)^l \mod p$ второй таблицы можно было не вычислять.

Таким образом, выполнено сравнение $9 \cdot 2^3 \equiv 3 \equiv (2^4)^2 \pmod{23}$, откуда следует, что $l = 2, t = 3$, и мы можем найти x по формуле $x = 4 \cdot 2 - 3 = 5$. Проверка показывает, что мы не ошиблись: $2^5 \equiv 9 \pmod{23}$. □

Замечание. *Внимательно изучив построенные нами таблицы, мы найдем еще одно общее значение, число* 9. *В этом случае* $l = 4, t = 4$, *и* $x = 4 \cdot 4 - 0 = 16$. *Никакой ошибки нет. Дело в том, что* $P_{23}(2) = 11$, *и полученные индексы* 5 *и* 16 *сравнимы по модулю* 11. *Если бы мы заранее вычислили показатель* $P_{23}(2) = 11$, *то могли бы быть уверены в том, что наш перебор в любом случае остановится на третьем шаге, так как* $3 \cdot h = 12 > 11$.

4.2.4. Метод Сильвестра—Полига—Хеллмана

Метод Сильвестра—Полига—Хеллмана нахождения дискретного логарифма x из сравнения $a^x \equiv b \pmod p$ был предложен в 1965 г. Василием Ильичем Нечаевым (1920–1999). Это метод позволяет в случае составного показателя $P_p(a)$ свести задачу вычисления дискретного логарифма к нескольким таким подзадачам [22], [74], [73], [76], [78].

Именно, при $P_p(a) = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ решение задачи поиска целого неотрицательного числа x, удовлетворяющего сравнению

$$a^x \equiv b \pmod p, \quad 0 \leqslant x < P_p(a),$$

можно свести к решению системы сравнений

$$\begin{cases} x \equiv x_1 \pmod{p_1^{\alpha_1}}, \\ \ldots \\ x \equiv x_k \pmod{p_k^{\alpha_k}}. \end{cases}$$

После этого искомое x нетрудно восстановить, пользуясь китайской теоремой об остатках.

В этом случае исходная задача дискретного логарифмирования по модулю p с основанием a, $P_p(a) = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, сводится к нескольким другим задачам дискретного логарифмирования по модулю p с основаниями, имеющими показатели $p_1^{\alpha_1}$, ... $p_k^{\alpha_k}$.

Рассмотрим *схему работы алгоритма* более подробно. Начнем работу со случая, когда показатель числа a по модулю p равен степени некоторого простого числа. Этот частный случай общего алгоритма принято называть *методом Полига—Хеллмана* [22], [74], [73].

Пусть $a^x \equiv b \pmod p$, и $P_p(a) = q^\alpha$, где $q \in P$, $\alpha \in \mathbb{N}$. Для нахождения решения указанного сравнения достаточно рассмотреть $0 < x < q^\alpha$. В этом случае неизвестное значение x можно записать в виде

$$x = x_0 + x_1 \cdot q + \ldots + x_{\alpha-1} \cdot q^{\alpha-1},$$

где $0 \leqslant x_i < q$ для всех $i = 0, 1, \ldots \alpha - 1$.

Пусть $AF \equiv a^{q^{\alpha-1}} \pmod p$. Тогда, используя соотношение $A^q \equiv 1 \pmod p$ и разложение $x = x_0 + x_1 \cdot q + \ldots + x_{\alpha-1} \cdot q^{\alpha-1}$, получим сравнение

$$A^x \equiv A^{x_0} A^{x_1 \cdot q} \ldots A^{x_{\alpha-1} \cdot q^{\alpha-1}} \equiv A^{x_0} (A^q)^{x_1} \ldots (A^{q^{\alpha-1}})^{x_{\alpha-1}} \equiv A^{x_0} \pmod p.$$

С другой стороны,

$$A^x \equiv (a^{q^{\alpha-1}})^x \equiv (a^x)^{q^{\alpha-1}} \equiv b^{q^{\alpha-1}} \pmod p.$$

Введя обозначение $b^{q^{\alpha-1}} \equiv b_0 \pmod p$, получим, что

$$A^{x_0} \equiv b_0 \pmod p.$$

Определим последовательность

$$a_i \equiv a^{q^{\alpha-i-1}} \pmod p,\ i = 0, 1, \ldots, \alpha - 1.$$

В этом случае $a_0 \equiv A \pmod p$, и

$$a_i^x \equiv a_i^{x_0} a_i^{x_1 \cdot q} a_i^{x_{n-1} \cdot q^{\alpha-1}} \equiv a_i^{x_0} a_{i-1}^{x_1} \ldots a_0^{x_i} \pmod p.$$

С другой стороны, определяя b_i из сравнения

$$b_i \equiv b^{q^{\alpha-i-1}} \pmod p,$$

убедимся, что

$$a_i^x \equiv (a^{q^{\alpha-i-1}})^x \equiv (a^x)^{q^{\alpha-i-1}} \equiv b^{q^{\alpha-i-1}} \equiv b_i \pmod p.$$

Таким образом,

$$A^{x_i} \equiv a_0^{x_i} \equiv a_i^x a_i^{-x_0} a_{i-1}^{-x_1} \ldots a_1^{-x_{i-1}} \equiv b_i a_i^{-x_0} a_{i-1}^{-x_1} \ldots a_1^{-x_{i-1}} \pmod p,$$

и мы получаем сравнение

$$A^{x_i} \equiv B_i \pmod p, \quad \text{где } B_i = b_i a_i^{-x_0} a_{i-1}^{-x_1} \ldots a_1^{-x_{i-1}}.$$

Последовательно решая каждое из этих сравнений, получим числа x_0, x_1, ..., $x_{\alpha-1}$ и, следовательно, искомое $x = x_0 + x_1 q + \ldots + x_{\alpha-1} q^{\alpha-1}$.

Пример 4.2.6 Попробуем применить метод Полига—Хеллмана к нахождению дискретного логарифма x из сравнения $7^x \equiv 9 \pmod{37}$. В этом случае $p = 37$, $a = 7$, и $b = 9$. Непосредственная проверка показывает, что $P_{37}(7) = 9 = 3^2$.

Следуя вышеизложенному алгоритму, представим число x виде $x = x_0 + x_1 \cdot 3$.

Определим элементы последовательностей $\{a_i\}$, $\{b_i\}$:

$a_1 \equiv 7^{3^0} \equiv 7^1 \equiv 7 \pmod{37}$;

$a_0 \equiv 7^{3^1} \equiv 10 \pmod{37}$;

$b_1 \equiv 9^{3^0} \equiv 9 \pmod{37}$;

$b_0 \equiv 9^{3^1} \equiv 9^3 \equiv 26 \pmod{37}$.

Для нахождения чисел x_0 и x_1 нам нужно решить следующие сравнения:

$$\begin{cases} A^{x_0} \equiv b_0 \pmod p, \\ A^{x_1} \equiv b_1 \cdot a_1^{-x_0} \pmod p, \end{cases}$$

или, учитывая, что $A = a_0$ и используя полученные выше численные данные, сравнения

$$\begin{cases} 10^{x_0} \equiv 26 \pmod{37}, \\ 10^{x_1} \equiv 9 \cdot (7^{-1})^{x_0} \pmod{37}. \end{cases}$$

Отмечая, что $A^1 = 10$, $A^2 \equiv 100 \equiv 26 \pmod{37}$, $A^3 \equiv 1000 \equiv 1 \pmod{37}$, то есть $A^{3t+1} \equiv 10 \pmod{37}$, $A^{3t+2} = 100 \equiv 26 \pmod{37}$, и $A^{3m} = 1000 \equiv \equiv 1 \pmod{37}$, из первого сравнения находим $x_0 = 2$.

Для решения второго сравнения найдем величину 7^{-1} в кольце классов вычетов по модулю 37. Для этого рассмотрим сравнение $7y \equiv 1 \pmod{37}$ (методы решения таких сравнений рассматривались ранее). Нетрудно убедиться, что $y \equiv 16 \pmod{37}$, то есть $7^{-1} \equiv 16 \pmod{37}$. Таким образом,

$$10^{x_1} \equiv 9 \cdot (7^{-1})^2 \equiv 9 \cdot 16^2 \equiv 10 \pmod{37}.$$

Следовательно, $x_1 = 1$, и $x = x_0 + x_1 \cdot 3 = 2 + 1 \cdot 3 = 5$. Осуществляя проверку полученного результата, непосредственным вычислением убеждаемся, что, действительно, $7^5 \equiv 9 \pmod{37}$. □

В общем случае $P_p(a) = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ для нахождения дискретного логарифма x из сравнения $a^x \equiv b \pmod{p}$ нужно решить систему сравнений

$$\begin{cases} x \equiv x_1 \pmod{p_1^{\alpha_1}}, \\ \ldots \\ x \equiv x_k \pmod{p_k^{\alpha_k}}, \end{cases}$$

где $0 \leqslant x_i < p_i^{\alpha_i}$, $a^{\mu_i x_i} \equiv b^{\mu_i} \pmod{p}$, $\mu_i = \dfrac{P_p(a)}{p_i^{\alpha_i}}$, $i = 1, \ldots, k$. Это становится очевидным после простейших рассуждений:
если $a^{\mu_i x_i} \equiv b^{\mu_i} \pmod{p}$, то

$$a^x \equiv b \pmod{p} \Leftrightarrow a^{\mu_i x} \equiv b^{\mu_i} \pmod{p} \Leftrightarrow a^{\mu_i x} \equiv a^{\mu_i x_i} \pmod{p} \Leftrightarrow$$

$$\Leftrightarrow \mu_i x \equiv \mu_i x_i \pmod{P_p(a)} \Leftrightarrow x \equiv x_i \pmod{p_i^{\alpha_i}}.$$

Замечая, что $P_p(a^{\mu_i}) = \dfrac{P_p(a)}{(\mu_i, P_p(a))} = \dfrac{P_p(a)}{\mu_i} = p_i^{\alpha_i}$, мы можем утверждать, что осуществлен переход к другим задачам дискретного логарифмирования: нахождению дискретных логарифмов чисел $B_i = b^{\mu_i}$ по модулю p с основаниями a^{μ_i}, показатели которых по модулю p представляют собой степени простых чисел, входящих в каноническое разложение числа $p-1$.

Решая каждую из полученных задач одним из методов, рассмотренных ранее, мы найдем значения чисел x_i и, используя китайскую теорему об остатках, искомое число x.

Пример 4.2.7 Воспользуемся этим методом для нахождения дискретного логарифма x из сравнения $5^x \equiv 8 \pmod{23}$. В нашем случае $p = 23$, $a = 5$, и $b = 8$. Кроме того, нетрудно показать, что $P_{23}(5) = 22 = 2 \cdot 11$. Для решения поставленной задачи методом Сильвестра—Полига—Хеллмана найдем величины $\mu_1 = \dfrac{22}{2} = 11$, $\mu_2 = \dfrac{22}{11} = 2$ и составим систему сравнений

$$\begin{cases} x \equiv x_1 \pmod 2, \\ x \equiv x_2 \pmod{11}, \end{cases}$$

где x_1 и x_2 могут быть найдены из условий

$$\begin{cases} (5^{\mu_1})^{x_1} \equiv 8^{\mu_1} \pmod{23}, \\ (5^{\mu_2})^{x_2} \equiv 8^{\mu_2} \pmod{23}. \end{cases}$$

Подставляя в последнюю систему значения $\mu_1 = 11$ и $\mu_2 = 2$, получаем, что

$$\begin{cases} (5^{11})^{x_1} \equiv 8^{11} \pmod{23}, \\ (5^2)^{x_2} \equiv 8^2 \pmod{23}, \end{cases} \text{ откуда следует, что } \begin{cases} (-1)^{x_1} \equiv 1 \pmod{23}, \\ 2^{x_2} \equiv 64 \pmod{23}. \end{cases}$$

Оба сравнения имеют очевидные решения $x \equiv 0 \pmod 2$ и $x \equiv 6 \pmod{11}$, соответственно. Переходя к системе

$$\begin{cases} x \equiv 0 \pmod 2, \\ x \equiv 6 \pmod{11}, \end{cases}$$

убеждаемся, что $x \equiv 6 \pmod{22}$ удовлетворяет обоим сравнениям системы, и получаем ответ: $x = 6$. Выполняя проверку, докажем, что наш результат верен. Действительно, $5^6 \equiv 8 \pmod{23}$. □

Рассмотрим еще один, более презентативный пример нахождения дискретного логарифма в случае, когда показатель основания является составным числом.

Пример 4.2.8 Воспользуемся методом Сильвестра—Полига—Хеллмана для того, чтобы найти x из сравнения $3^x \equiv 4 \pmod{37}$. В нашем случае $p = 37$, $a = 3$, и $b = 4$. Кроме того, нетрудно показать, что $P_{37}(3) = 18 = 3^2 \cdot 2$. В этом случае x можно найти из системы сравнений

$$\begin{cases} x \equiv x_1 \pmod 2, \\ x \equiv x_2 \pmod 9, \end{cases}$$

где x_1 и x_2 получены из условий

$$\begin{cases} (3^{\mu_1})^{x_1} \equiv 4^{\mu_1} \pmod{37}, \\ (3^{\mu_2})^{x_2} \equiv 4^{\mu_2} \pmod{37}, \end{cases}$$

а μ_1 и μ_2 имеют следующий вид: $\mu_1 = \dfrac{18}{2} = 9$, $\mu_2 = \dfrac{18}{9} = 2$. Подставляя значения μ_1 и μ_2 в последнюю систему сравнений, получаем, что

$$\begin{cases} (3^9)^{x_1} \equiv 4^9 \pmod{23} \\ (3^2)^{x_2} \equiv 4^2 \pmod{23}, \end{cases} \text{ откуда следует, что } \begin{cases} (-1)^{x_1} \equiv -1 \pmod{37} \\ 9^{x_2} \equiv 16 \pmod{37}. \end{cases}$$

Действительно, $3^9 \equiv (3^4)^2 \cdot 3 \equiv 7^2 \cdot 3 = -1 \pmod{37}$, в то время как $4^9 \equiv (4^3)^3(-10)^3 \equiv (-11) \cdot (-10) \equiv 110 \equiv -1 \pmod{37}$.

Из первого сравнения следует, что $x_1 = 1$; для решения второго можно воспользоваться алгоритмом согласования или алгоритмом Полига—Хелмана. В результате получим $x_2 = 7$. Таким образом, получаем систему

$$\begin{cases} x_1 \equiv 1 \pmod 2 \\ x_2 \equiv 7 \pmod 9), \end{cases}$$

решая которую стандартным методом, найдем $x \equiv 7 \pmod{18}$. Таким образом, $x = 7$. Проверка показывает, что полученный результат верен: $3^7 \equiv 4 \pmod{37}$. □

4.2.5. Алгоритм исчисления порядка

На современном этапе развития криптографии наибольшую популярность имеют вероятностные алгоритмы вычисления дискретного логарифма (о характеристиках и особенностях вероятностных теоретико-числовых алгоритмов мы поговорим более подробно в главе 5) [22], [68], [74], [90].

Алгоритм исчисления порядка (*index-calculus algorithm*, *алгоритм Адлемана*, *алгоритм базы разложения*) относится к вероятностным методам вычисления дискретного логарифма. Основные идеи этого метода были известны в теории чисел еще с 20-х гг. XX в., однако только в 1979 г. Л. Адлеман, один из создателей системы *RSA*, указал на этот алгоритм как на средство решения уравнения $a^x = b \pmod p$ и исследовал его трудоемкость. В настоящее время алгоритм исчисления порядка (базы разложения) и его улучшенные варианты дают наиболее быстрый способ вычисления дискретных логарифмов из сравнений типа $a^x = b \pmod p$.

Для реализации алгоритма зафиксируем некоторое натуральное число t и сформируем *множество базовых множителей* (*факторную базу*) $S = \{p_1, p_2, \ldots p_t\}$, состоящее из первых t простых чисел.

Задавая последовательно значения $k = 1, 2, 3, \ldots$, находим $t + \varepsilon$ (ε — небольшое целое число) чисел вида $a^k \mod p$, которые можно представить в виде произведения простых из факторной базы. Поиск осуществляется непосредственным делением на числа, принадлежащие S.

Каждое из найденных чисел записывается через произведение базовых множителей:

$$a^k \equiv \prod_{i=1}^{t} p_i^{\alpha_i} \pmod p, \quad \alpha_i \geqslant 0.$$

Для каждого значения k получаем свой набор чисел α_i. Прологарифмировав (проиндексировав) обе части сравнения, получим:

$$k \equiv \sum_{i=1}^{t} \alpha_i \log_a p_i \pmod{P_p(a)}.$$

(На практике чаще всего используют в качестве a первообразный корень по модулю p; в этом случае $P_p(a) = p - 1$.)

Другими словами, мы получаем систему из $t + \varepsilon$ уравнений вида $k = \sum_{i=1}^{t} \alpha_i \log_a p_i$ с t неизвестными $\log_a p_i$, $i = 1, 2, \ldots t$. Число уравнений на ε больше числа неизвестных, что повышает вероятность получения решения системы в случае, если некоторые из уравнений окажутся линейно зависимыми.

Решая систему методами линейной алгебры по модулю $p - 1$, в результате получаем значения логарифмов чисел из множества S: $\log_a p_1$, $\log_a p_2$, ..., $\log_a p_t$.

Случайным образом выбирая r, находим число вида $b \cdot a^r$, разложимое по факторной базе:

$$b \cdot a^r \equiv \prod_{i=1}^{t} p_i^{\beta_i} \pmod p, \quad \beta_i \geqslant 0.$$

Логарифмируя последнее равенство, получаем:

$$x = \log_a b \equiv \left(\sum_{i=1}^{t} \beta_i \log_a p_i \right) - r \pmod{p-1}.$$

Пример 4.2.9 Найдем x из сравнения $10^x \equiv 37 \pmod{47}$, воспользовавшись алгоритмом исчисления порядка. В нашем случае $n = 47$, $a = 10$, и $b = 37$.

Пусть $t = 3$. Тогда множество базовых множителей имеет вид $S = \{2, 3, 5\}$. Выберем $\varepsilon = 1$ и будем строить систему из четырех уравнений.

Обозначим логарифмы чисел из S символами u_1, u_2, u_3: $u_1 = \log_{10} 2$, $u_2 = \log_{10} 3$, $u_3 = \log_{10} 5$.

Найдем четыре числа вида a^k, разложимых по базе:

$10^1 \equiv 10 = 2 \cdot 5 \pmod{47}$;

$10^2 \equiv 6 = 2 \cdot 3 \pmod{47}$;

$10^3 \equiv 13 \pmod{47}$ – не подходит;

$10^4 \equiv 36 = 2 \cdot 2 \cdot 3 \cdot 3 \pmod{47}$;

$10^5 \equiv 31 \pmod{47}$ – не подходит;

$10^6 \equiv 28 = 2 \cdot 2 \cdot 7 \pmod{47}$ – не подходит;

$10^7 \equiv 45 = 3 \cdot 3 \cdot 5 \pmod{47}$.

Найденные четыре числа 10, 6, 36 и 45 соответствуют степеням 1, 2, 4 и 7. Используя этот факт, получим систему сравнений

$$\begin{cases} 1 \equiv u_1 + u_3 \pmod{46}, \\ 2 \equiv u_1 + u_2 \pmod{46}, \\ 4 \equiv 2u_1 + 2u_2 \pmod{46}, \\ 7 \equiv 2u_2 + u_3 \pmod{46}. \end{cases}$$

Видим, что второе и третье сравнения линейно зависимы, так что найденное дополнительное четвертое число не оказалось лишним. Избавимся от одного сравнения и решим полученную систему:

$$\begin{cases} 1 \equiv u_1 + u_3 \pmod{46}, \\ 2 \equiv u_1 + u_2 \pmod{46}, \\ 7 \equiv 2u_2 + u_3 \pmod{46}; \end{cases} \Leftrightarrow \begin{cases} 1 - u_1 \equiv u_3 \pmod{46}, \\ 2 - u_1 \equiv u_2 \pmod{46}, \\ 7 \equiv 5 - 3u_1 \pmod{46}; \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 1 - u_1 \equiv u_3 \pmod{46}, \\ 2 - u_1 \equiv u_2 \pmod{46}, \\ 3u_1 \equiv -2 \pmod{46}; \end{cases} \Leftrightarrow \begin{cases} u_1 \equiv 30 \pmod{46}, \\ u_2 \equiv 2 - (-16) \equiv 18 \pmod{46}, \\ u_3 \equiv 1 - (-16) \equiv 17 \pmod{46}. \end{cases}$$

Найдем нужное r перебором величин $b \cdot a^r$, $r = 1, 2, \ldots$:

$37 \cdot 10 \equiv 370 \equiv 41 \pmod{47}$ – не подходит;

$37 \cdot 10^2 \equiv 37 \cdot 6 \equiv 34 \pmod{47}$ – не подходит;

$37 \cdot 10^3 \equiv 37 \cdot 13 \equiv 11 \pmod{47}$ – не подходит;

$37 \cdot 10^4 \equiv 37 \cdot 36 \equiv 16 \equiv 2 \cdot 2 \cdot 2 \cdot 2 \pmod{47}$ – подходит.

Логарифмируя последнее сравнение и используя найденное ранее значение $\log_{10} 2 = u_1 = 30$, получаем, что

$$\log_{10} 37 \equiv 4 \log_{10} 2 - 4 \equiv 4 \cdot 30 - 4 \equiv 24 \pmod{46}.$$

Осуществляя непосредственную проверку, убедимся, что результат верен: $10^{24} = 37 \pmod{47}$. □

Замечание. *Мы находили t последовательным перебором, и получили его только на четвертом шаге. Вероятностный выбор t мог бы дать результат быстрее. Например,* $37 \cdot 10^6 \equiv 37 \cdot 36 \cdot 6 \equiv 2 \pmod{47}$, *откуда немедленно следует, что* $\log_{10} 37 \equiv \log_{10} 2 - 6 \equiv 30 - 6 \equiv 24 \pmod{46}$. *Далее,* $37 \cdot 10^7 \equiv 2 \cdot 10 \equiv 20 \equiv 2^2 \cdot 5 \pmod{47}$, *и* $\log_{10} 37 \equiv \log_{10} 2 - 6 \equiv 30 - 6 \equiv$ $\equiv 24 \pmod{46}$. *При дальнейшем умножении на* 10, *мы будем получать произведения* 2 *и* 5; *все они годятся для «построения» окончательного результата.*

Упражнения

(1) Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{p}$ методом перебора:

a) $p = 5$, $a = 3$, $b = 2$;
b) $p = 7$, $a = 5$, $b = 4$;
c) $p = 11$, $a = 8$, $b = 3$;
d) $p = 13$, $a = 7$, $b = 8$;
e) $p = 17$, $a = 12$, $b = 3$;
f) $p = 19$, $a = 13$, $b = 14$;
g) $p = 23$, $a = 17$, $b = 9$;
h) $p = 29$, $a = 2$, $b = 16$.

В каждом из случаев составьте таблицу индексов по модулю p; определите все первообразные корни по модулю p; выпишите индексы числа b по модулю p, используя в качестве оснований каждый из найденных первообразных корней; решите задачу дискретного логарифмирования $(a + 1)^x \equiv b \pmod{p}$.

(2) Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{p}$, пользуясь таблицей индексов по модулю p:

a) $p = 31$, $a = 3$, $b = 2$;
b) $p = 37$, $a = 2$, $b = 4$;
c) $p = 41$, $a = 6$, $b = 3$;
d) $p = 43$, $a = 3$, $b = 8$;
e) $p = 47$, $a = 5$, $b = 3$;
f) $p = 53$, $a = 2$, $b = 14$;
g) $p = 59$, $a = 2$, $b = 9$;
h) $p = 61$, $a = 2$, $b = 16$.

В каждом из случаев определите все первообразные корни по модулю p; выпишите индексы числа b по модулю p, используя в качестве оснований каждый из найденных первообразных корней; решите задачу дискретного логарифмирования $(a + 1)^x \equiv b \pmod{p}$.

③ Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{p}$ методом согласования:

a) $p = 31, a = 4, b = 2$;
b) $p = 37, a = 10, b = 4$;
c) $p = 41, a = 8, b = 3$;
d) $p = 43, a = 7, b = 8$;
e) $p = 47, a = 9, b = 3$;
f) $p = 53, a = 10, b = 14$;
g) $p = 59, a = 3, b = 9$;
h) $p = 61, a = 13, b = 16$.

④ Решите задачу дискретного логарифмирования методом согласования:

a) $2^x \equiv 21 \pmod{29}$,
b) $5^x \equiv 12 \pmod{37}$,
c) $7^x \equiv 25 \pmod{31}$,
d) $3^x \equiv 11 \pmod{43}$,
e) $6^x \equiv 21 \pmod{41}$;
f) $2^x \equiv 13 \pmod{29}$.

Проверьте результаты, пользуясь таблицами индексов.

⑤ Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{p}$ методом Полига-Хеллмана:

a) $p = 17, a = 13, b = 16$;
b) $p = 17, a = 14, b = 4$;
c) $p = 17, a = 9, b = 8$;
d) $p = 19, a = 5, b = 16$;
e) $p = 13, a = 5, b = 8$;
f) $p = 29, a = 12, b = 17$.

⑥ Решите задачу дискретного логарифмирования методом Сильвестра—Полига—Хеллмана:

a) $2^x \equiv 21 \pmod{29}$,
b) $5^x \equiv 12 \pmod{37}$,
c) $7^x \equiv 25 \pmod{31}$,
d) $3^x \equiv 11 \pmod{43}$,
e) $6^x \equiv 21 \pmod{41}$;
f) $2^x \equiv 13 \pmod{29}$.

Сравните результаты с результатами решения упражнения 4. Какой метод эффективнее? Почему?

⑦ Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{p}$ методом исчисления порядка:

a) $p = 31, a = 4, b = 2$;
b) $p = 37, a = 10, b = 4$;
c) $p = 41, a = 8, b = 3$;
d) $p = 43, a = 7, b = 8$;
e) $p = 47, a = 9, b = 3$;
f) $p = 53, a = 10, b = 14$;
g) $p = 59, a = 3, b = 9$;
h) $p = 61, a = 13, b = 16$.

Сравните результаты с результатами упражнений 3. Какой метод эффективнее? Почему?

Задачи

[1] Пользуясь таблицей индексов, решите задачу дискретного логарифмирования $a^x \equiv 2 \pmod{p}$ для $p \in \{11, 13, 17, 19, 23, 29\}$ и $a \in \in \{3, 4, 5, 6, 7, 8, 9, 10\}$. Всегда ли задача разрешима? При каких a

задача не имеет решений? Для фиксированного простого числа p, $p > 3$, укажите хотя бы одно основание a, для которого задача $a^x \equiv 2 \pmod{p}$ заведомо неразрешима.

2 Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{n}$ перебором:

a) $N = 15$, $a = 2$, $b = 8$;
b) $N = 15$, $a = 2$, $b = 7$;
c) $N = 21$, $a = 2$, $b = 11$;
d) $N = 21$, $a = 2$, $b = 13$;
e) $N = 33$, $a = 2$, $b = 23$;
f) $N = 33$, $a = 2$, $b = 25$;
g) $N = 35$, $a = 2$, $b = 29$;
h) $N = 35$, $a = 2$, $b = 11$.

Всегда ли задача имеет решение? Почему?

3 Используя таблицу индексов по модулю p, где $p \in \{37, 47, 61, 67, 89\}$, укажите

a) первообразный корень, по которому построена таблица;
b) все первообразные корни по модулю p;
c) все классы $\mathbf{x_p}$, такие что $P_p(x) = \dfrac{p-1}{2}$.
d) индекс числа $p - 5$ по модулю p;
e) все возможные индексы числа $p - 4$ по модулю p.

4 Пусть p_n — n-е простое число, где

$$n = N - 5\left\lfloor \frac{N}{5} \right\rfloor + 5, \quad N \in \{1, 2, 3, \ldots, 25\}.$$

Пользуясь таблицей индексов по модулю p_n, укажите:

a) все первообразные корни по модулю p_n, принадлежащие промежутку $[100, 120]$;
b) все классы $\mathbf{x_{p_n}}$, такие что $P_{p_n}(x) = \dfrac{p_n - 1}{2}$;
c) все числа a, такие что $P_{p_n}(a) = 2$, $a \in [-15, -2]$.
d) все числа a, такие что $\operatorname{ind}_a(p-3) = p - 2$;
e) все числа a, такие что $\operatorname{ind}_a(p-3) = 2$.

5 Найдите все индексы числа a по модулю p, если $a \in \{6, 7, 8, 9\}$, а $p \in \{17, 19, 23, 29\}$.

6 Какие значения могут принимать показатели целого числа a по модулю n, если $n = N - 5\left\lfloor \dfrac{N}{5} \right\rfloor + 5$, $N \in \{1, 2, 3, \ldots 25\}$?

7 Сколько классов вычетов по модулю 17 имеют показатель:

a) 2; b) 3; c) 4; d) 8; e) 16?

8 Скольким классам вычетов по модулю 17 принадлежат натуральные степени числа 7?

9 Сколько классов первообразных корней существует по модулю:

a) 81; b) 98; c) 242; d) 338; e) 1250?

10 Решите задачу дискретного логарифмирования $a^x \equiv b \pmod p$ методом Полига—Хеллмана:

a) $p = 37, a = 6, b = 8$;
b) $p = 37, a = 7, b = 9$;
c) $p = 53, a = 30, b = 23$;
d) $p = 61, a = 7, b = 54$.

11 Решите задачу дискретного логарифмирования $a^x \equiv b \pmod p$ методом Сильвестра—Полига—Хеллмана:

a) $p = 31, a = 4, b = 2$;
b) $p = 37, a = 10, b = 4$;
c) $p = 41, a = 8, b = 3$;
d) $p = 43, a = 7, b = 8$;
e) $p = 47, a = 9, b = 3$;
f) $p = 53, a = 10, b = 14$;
g) $p = 59, a = 3, b = 9$;
h) $p = 61, a = 13, b = 16$.

Сравните результаты с результатами упражнений 3. Какой метод эффективнее? Почему?

12 Решите задачу дискретного логарифмирования $7^x \equiv 167 \pmod{587}$ методом согласования, если известно, что $P_{587}(7) = 293$.

13 Решите задачу дискретного логарифмирования $21^x \equiv 175 \pmod{251}$ методом исчисления порядка.

14 Решите задачу дискретного логарифмирования $7^x \equiv 151 \pmod{547}$ методом исчисления порядка.

15 Решите задачу дискретного логарифмирования $3^x \equiv 148 \pmod{181}$ методом:

a) согласования; b) Сильвестра—Полига—Хеллмана.

Сравните результаты вычислений. Какой метод производительнее? Целесообразно ли решать эту задачу методом перебора? Почему? Можем ли мы решить эту задачу, пользуясь таблицами индексов? Почему?

16 Решите задачу дискретного логарифмирования $21^x \equiv 175 \pmod{251}$ методом

a) согласования; b) Сильвестра—Полига—Хеллмана.

17 Решите задачу дискретного логарифмирования методом исчисления порядка:

a) $2^x \equiv 24 \pmod{53}$; d) $6^x \equiv 45 \pmod{61}$; g) $7^x \equiv 41 \pmod{67}$;
b) $5^x \equiv 24 \pmod{53}$; e) $2^x \equiv 41 \pmod{67}$; h) $11^x \equiv 41 \pmod{71}$.
c) $5^x \equiv 13 \pmod{97}$; f) $7^x \equiv 41 \pmod{71}$;

18 Решите задачу дискретного логарифмирования методом исчисления порядка:

a) $3^x \equiv 250 \pmod{1307}$, $r = 653$; c) $6^x \equiv 401 \pmod{2063}$, $r = 1031$;
b) $2^x \equiv 174 \pmod{1009}$, $r = 504$; d) $22^x \equiv 651 \pmod{2819}$, $r = 1409$.

Литература к главе 4

При подготовке текста главы 4 были использованы следующие источники [5], [6], [13], [16], [19], [20], [22], [24], [29], [36], [40], [53], [55], [58], [61], [63], [65], [68], [71], [73–76], [78], [80] [83], [88] [90], [91], [94], [95], [105], [110], [119], [128].

Глава 5

Вычислительные алгоритмы и их трудоемкость

Алгоритм (уст. *алгоритм*) — набор инструкций, описывающих порядок действий исполнителя для достижения результата решения задачи за конечное число действий.

Понятие алгоритма принадлежит к первоначальным, базисным понятиям математической науки. Вычислительные процессы алгоритмического характера (арифметические действия над целыми числами, нахождение наибольшего общего делителя двух чисел и т. д.) известны человечеству с глубокой древности.

Само слово «алгоритм» происходит от имени хорезмского ученого Абу Абдуллах Мухаммеда ибн Муса аль-Хорезми (Abū 'Abdallāh Muḥammad ibn Mūsā al-Khwārizmī, около 783 – около 850). Около 825 г. он написал сочинение, в котором впервые дал описание придуманной в Индии позиционной десятичной системы счисления. В первой половине XII века книга аль-Хорезми в латинском переводе проникла в Европу. Латинизированное имя среднеазиатского ученого было вынесено в заглавие книги «Algoritmi de numero Indorum», и сегодня считается, что слово «алгоритм» попало в европейские языки именно благодаря этому сочинению.

Однако вопрос о его смысле длительное время вызывал нешуточные споры. В явном виде понятие алгоритма сформировалось лишь в начале XX века, а современное формальное определение алгоритма было дано в 30–50-е гг. XX в. в работах Алана Мэтисона Тьюринга (Alan Mathison Turing, 1912–1954), Эмиля Леона Поста (Post Emil Leon, 1897–1954), Алонзо Черча (Alonzo Church, 1903–1995), Норберта Винера (Norbert Wiener, 1894–1964), Андрея Андреевича Маркова (1903–1979).

5.1. Трудоемкость арифметических действий

Существенной частью арифметики является изучение методов реализации арифметических действий, в том числе на основе различных устройств. Потребность в вычислениях возникла у человека в глубокой

древности. Искусство счета складывалось и развивалось в течение многих веков. Необходимость быстрых и точных вычислений привела к созданию простейших счетных устройств: абака, суаньпаня, юпаны и др. Следующим шагом было создание Уильямом Отредом (William Oughtred, 1575–1660) в 1622 г. логарифмической линейки. Первые вычислительные машины, которые позволяли механизировать четыре арифметических действия, были сконструированы в XVII в.: «арифметическая машина» Вильгельма Шиккарда (Wilhelm Schickard, 1592–1635) была построена в 1623 г.; машина Блеза Паскаля (Blaise Pascal, 1623–1662) была разработана им в 1642 г. для выполнения финансовых расчетов. Попытки усовершенствовать арифмометр продолжались весь XVIII в.; в XIX в. арифмометры получили широкое распространение. В XX в. на смену арифмометрам пришли электронные вычислительные машины. В их основе лежат алгоритмы, которые используют наименьшее число элементарных операций для выполнения арифметических действий.

5.1.1. Системы счисления

Классические арифметические алгоритмы построены на использовании позиционных систем счисления. При обработке чисел на ЭВМ они могут рассматриваются в различных системах счисления, однако проводимые при этом арифметические операции мало отличаются по трудоемкости [98], [36].

Разложение натурального числа n по основанию g, где $g \in \mathbb{N}, g > 1$, представляет собой запись числа n в виде

$$n = a_{k-1} \cdot g^{k-1} + a_{k-2} \cdot g^{k-2} + \ldots + a_1 \cdot g + a_0,$$

где k — целое неотрицательное число, а целые a_i (цифры g-ичной системы счисления) удовлетворяют неравенствам $0 \leqslant a_i < g$.

Если в приведенном выше разложении старшая цифра $a_{k-1} \neq 0$, то пишут, что

$$n = \overline{(a_{k-1}a_{k-2}\ldots a_1a_0)}_g$$

и говорят, что *натуральное число n записано в системе счисления с основанием g*. В случае десятичной системы счисления ($g = 10$) и двоичной системы счисления ($g = 2$), а также в тех случаях, когда основание системы счисления ясно из контекста, горизонтальная черта над набором цифр и индекс g обычно опускаются. Так, например,

$$\overline{(110111)}_2 = 110111_2 = 110111 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1.$$

Число $n = \overline{(a_{k-1}a_{k-2}\ldots a_1a_0)}_g$ называют *k-разрядным g-ичным числом*. Очевидно, что любое натуральное число n, удовлетворяющее неравенствам $g^{k-1} \leqslant n < g^k - 1$ является k-разрядным по основанию g.

При этом если $g^{k-1} \leqslant n < g^k$, то $k - 1 \leqslant \log_g n < k$, откуда следует, что $k - 1 = \lfloor \log_g n \rfloor$. Таким образом, *число k разрядов g-ичной записи натурального числа n* может быть получено по формуле

$$k = \lfloor \log_g n \rfloor + 1 = \left\lfloor \frac{\log n}{\log g} \right\rfloor + 1.$$

(Здесь и далее символ $\log n$ понимается как натуральный логарифм $\log_e n$).

Любое натуральное число n может быть единственным образом записано в системе счисления с основанием g, $g > 1$. Такое представление можно получить последовательным делением на g с остатком числа n и получающихся при этом неполных частных: если

$n = g \cdot q_0 + r_0,\ q_0, r_0 \in \mathbb{N}, 0 \leqslant r_0 < g,$
$q_0 = g \cdot q_1 + r_1,\ q_1, r_1 \in \mathbb{N}, 0 \leqslant r_1 < g,$
.....
$g_{s-3} = g \cdot q_{s-2} + r_{s-2},\ q_{s-2}, r_{s-2} \in \mathbb{N}, 0 \leqslant r_{s-2} < g,$
$g_{s-2} = g \cdot 0 + r_{s-1},\ r_{s-1} \in \mathbb{N}, 0 \leqslant r_{s-1} < g,$
то $n = r_{s-1}g^{s-1} + r_{s-2}g^{s-2} + \ldots + r_1 g + r_0$, или, что то же,
$n = \overline{(r_{s-1}r_{s-2}\ldots r_1r_0)}_g$.

Пример 5.1.1 Для записи числа 235 в троичной системе счисления осуществим описанный выше алгоритм: $235 = 3 \cdot 78 + 1$; $78 = 3 \cdot 26 + 0$; $26 = 3 \cdot 8 + 2$; $8 = 3 \cdot 2 + 2$; $2 = 3 \cdot 0 + 2$. Следовательно, $235 = 22201_3$.

Заметим, что для определения количества k знаков в троичной записи числа 235 находить искомое разложение вовсе необязательно: $k = \lfloor \log_3 235 \rfloor + 1 = 4 + 1 = 5$.

Для перевода числа 22201_3 из троичной системы счисления, например, в восьмеричную, можно сначала получить его десятичную запись по формуле $22201_3 = 2 \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3 + 1 = 235_{10}$, а затем воспользоваться алгоритмом перехода от десятичного числа к восьмеричному: $235 = 8 \cdot 29 + 3$; $29 = 8 \cdot 3 + 5$; $3 = 8 \cdot 0 + 3$; следовательно, $235_{10} = 353_8$, и $22201_3 = 353_8$. □

Впрочем, для перевода числа из одной системы счисления в другую совсем не обязательно пользоваться «промежуточной» десятичной системой. Перевод g-ичного числа $X_g = \overline{(x_{s-1}\ldots x_1x_0)}_g$ в t-ичное число $Y_t = \overline{(y_{k-1}\ldots y_1y_0)}_t$ можно осуществить, либо выполняя операции формулы $x^{s-1}g^{s-1} + \ldots + x_1 g + x_0$ в системе счисления с основанием t, либо

реализуя описанный выше алгоритм последовательного деления на t в системе счисления с основанием g. Первый способ более рационален при $t > g$ (почему?); второй — при $t < g$. Для лучшего запоминания удобно сформулировать описанное правило в следующем виде: *для перевода числа из одной системы счисления в другую нужно произвести либо умножение на «старое» основание в «новой» системе счисления, либо деление на «новое» основание в «старой» системе счисления.*

Перевод чисел из одной системы счисления в другую существенно упрощается, если одно основание представляет собой степень другого. В случае $g = t^k$, $k \in \mathbb{N}$, для перевода $X_g \to Y_t$ достаточно каждую цифру числа X_g представить в виде t-ичного числа, записанного k-знаками; для перевода $Y_t \to X_g$ достаточно разбить t-ичную запись числа Y_t на группы по k символов в каждой группе, начиная разбиение «справа», а затем представить каждое из полученных t-ичных чисел в виде цифр g-ичного числа X_g.

Пример 5.1.2 Для перевода числа 22201_3 в восьмеричную систему счисления воспользуемся «правилом умножения», осуществляя операции в восьмеричной системе счисления:

$$22201_3 = 2 \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + 1 = 2_8 \cdot 3_8^4 + 2_8 \cdot 3_8^3 + 2_8 \cdot 3_8^2 + 1_8.$$

Поскольку $3_8 \cdot 3_8 = 11_8$, $11_8 \cdot 11_8 = 121_8$; $11_8 \cdot 3_8 = 33_8$, то

$$n = 2_8 \cdot 121_8 + 2_8 \cdot 33_8 + 2_8 \cdot 11_8 + 1_8 = 242_8 + 66_8 + 22_8 + 1_8 = 353_8.$$

Для обратного перевода числа 353_8 в троичную систему счисления воспользуемся «правилом деления», осуществляя операции описанного выше алгоритма в троичной системе счисления: $353_8 = 3_8 \cdot 96_8 + 1_8$, $96_8 = 3_8 \cdot 32_8 + 0_8$; $32_8 = 3_8 \cdot 10_8 + 2_8$; $10_8 = 3_8 \cdot 2_8 + 2_8$; $2_8 = 3_8 \cdot 0_8 + 2_8$, следовательно, $353_8 = 22201_3$.

Для перевода числа $n = 10122201021_3$ в девятиричную систему счисления заметим, что $9 = 3^2$. Разобьем все цифры числа n справа налево на группы по 2 цифры в каждой группе: $n = 1|01|22|20|10|21_3$. Каждую группу запишем в виде цифры в девятиричной системе счисления: $1_3 = 1_9$; $01_3 = 1_9$; $22_3 = 2 \cdot 3 + 2 = 8_9$; $20_3 = 2 \cdot 3 = 6_9$; $10_3 = 1 \cdot 3 + 0 = 3_9$; $21_3 = 2 \cdot 3 + 1 = 7_9$. Заменяя имеющиеся блоки на соответствующие им девятиричные цифры, получим окончательный результат: $n = 118637_9$.

Для перевода числа $n = 7420_8$ в двоичную систему счисления заметим, что $8 = 2^3$, и запишем каждую цифру восьмеричного числа n в двоичной системе счисления, каждый раз используя три двоичных цифры: $7 = 1 \cdot 2^4 + 1 \cdot 2 + 1 = 111_2$; $4 = 1 \cdot 2^2 + 0 \cdot 2 + 0 = 100_2$; $2 = 1 \cdot 2 + 0 = 10_2 = 010_2$; $0 = 000_2$. Заменяя каждую восьмеричную цифру полученным для нее представлением, найдем двоичную запись числа n: $n = 111100010000_2$. □

5.1.2. Символ «О»-большое

Для обсуждения вопросов сложности выполнения арифметических действий, в частности, для краткой записи временных оценок сложности, мы будем использовать хорошо известный в математике символ $O(\,)$ — «*О-большое*»[24], [53], [74], [50].

Для функций $f(n)$ и $h(n)$ положительного целочисленного аргумента n, принимающих комплексные значения, будем говорить, что $f(n) = O(h(n))$ (или просто $f = O(h)$), если существует такая положительная действительная константа C и такое натуральное число n_0, что для любого $n \geqslant n_0$ имеет место неравенство $|f(n)| \leqslant C \cdot |h(n)|$.

Аналогичное обозначение можно использовать и для функций от нескольких переменных: если $f(n_1, n_2, \ldots n_s)$ и $h(n_1, n_2, \ldots n_s)$ — две функции от s положительных целочисленных переменных, принимающие комплексные значения, то будем говорить, что функция

$$f(n_1, n_2, \ldots n_s) = O(h(n_1, n_2, \ldots n_s)),$$

если существует такая положительная действительная константа C и такое натуральное число n_0, что для любого набора $(n_1, \ldots n_s)$, такого что $\max\{n_1, \ldots n_s\} \geqslant n_0$, имеет место неравенство

$$|f(n_1, \ldots n_s)| \leqslant C \cdot |h(n_1, \ldots n_s)|.$$

Пример 5.1.3 Нетрудно убедиться в том, что $2n^2 + n - 3 = O(n^2)$. Действительно, при любом натуральном n левая часть меньше $3n^2$: $2n^2+n-3 \leqslant 2n^2 + n^2 = 3n^2$. Поскольку $3n^2 < 3n^3$ при любом натуральном n, то можно утверждать, что $2n^2+n-3 = O(n^3)$, однако эта оценка оказывается слишком грубой. С другой стороны, $2n^2 + n - 3 \neq O(n)$, поскольку для любой положительной действительной константы C левая часть, начиная с некоторого n (например, начиная с $n = \max\{3, \lfloor C \rfloor\}$) будет больше $C \cdot n$.

Другой пример: функция $\sin(n_1^2 + n_2^2) = O(1)$, однако $\sin(n_1^2 + n_2^2) \neq O\left(\dfrac{1}{n_1 + n_2}\right)$. Хотя $\sin(n_1^2 + n_2^2) = O(n_1 + n_2)$, эта оценка является слишком грубой и на практике не используется. □

Приведенные примеры показывают, что равенство $f(n) = O(h(n))$ следует понимать скорее как неравенство, а символ O-большое — как некоторую мультипликативную константу; так, соотношение $f(n) = O(n^d)$ показывает, что функция f растет приблизительно как d-я степень аргумента; запись $f(n) = O(1)$ означает, что функция f ограничена некоторой константой; если $f(n)$ — многочлен степени d с положительным старшим коэффициентом, то $f(n) = O(n^d)$.

Если $f(n)$ обозначает число k разрядов записи натурального числа n в системе счисления с основанием g, то, как следует из полученной выше формулы для k, $f(n) = O(\log n)$. Заметим, что это соотношение имеет место для произвольного фиксированного основания g. С другой стороны, если основание g не фиксировано, а может расти, то число k разрядов записи натурального числа n в системе счисления с основанием g является функцией $f(n, g)$ двух переменных, и, пользуясь той же формулой для k, можно утверждать, что $f(n, g) = O\left(\dfrac{\log n}{\log g}\right)$.

5.1.3. Анализ трудоемкости арифметических действий

При обсуждении вопросов трудоемкости арифметических операций мы будем, как правило, говорить о записи чисел в двоичной системе счисления. Это связано с тем, что числами, записанными в двоичной системе счисления или системах счисления с основаниями, равными степенями двойки, оперируют современные ЭВМ; эти же системы счисления используются в криптографии.

Время, которое компьютер расходует на решение задачи, пропорционально выполненному при этом числу двоичных операций. Константа пропорциональности — число наносекунд, расходуемых на одну двоичную операцию, — зависит от технических особенностей компьютера.

Поэтому, когда мы говорим об оценке времени $Time(z)$, затрачиваемого на работу по решению задачи z, речь идет об оценке числа двоичных операций, необходимых для ее выполнения.

При таком подходе мы пренебрегаем временем, расходуемым на второстепенные действия, к которым относятся, например, запись информации, логические шаги, отличные от двоичных операций, умножение и деление на степень основания системы (соответствует всего лишь перезаписи (смещению) числа) и т. д. [53].

Сложение

Начнем обсуждение трудоемкости арифметической операции сложения с рассмотрения примера.

Пример 5.1.4 Найдем сумму $1111 + 101000$ двух двоичных чисел. Для этого выполним обычные операции сложения «в столбик», пользуясь тем, что в двоичной системе счисления $0 + 0 = 0$, $0 + 1 = 1$, и $1 + 1 = 10$:

$$\begin{array}{r} \ 1111 \\ +\ 101000 \\ \hline 110111 \end{array}$$

Непосредственный подсчет числа двоичных операций, необходимых для решения задачи, позволяет утверждать, что сложение двух k-разрядных двоичных чисел (то есть натуральных чисел, двоичная запись каждого из которых имеет длину в k *бит*; «*бит*» — сокращение выражения «*binarydigit*»), требует k двоичных операций, а в случае сложения k-разрядного и l-разрядного двоичных чисел число двоичных операций не превосходит $\max\{k, l\}$. Таким образом, мы получили следующую оценку:

$$Time(\text{сложение } k\text{-разрядного и } l\text{-разрядного чисел } m, n) = O(\max\{k, l\}).$$

Другими словами, *число двоичных операций, необходимых для сложения двух натуральных чисел, большее из которых равно* n, *есть* $O(\log n)$:

$$Time(n + m) = O(\max\{\log n, \log m\}) = O(\log n),\ n \geqslant m. \qquad \square$$

Умножение

Процесс умножения также рассмотрим на примере произведения двух двоичных чисел.

Пример 5.1.5 Осуществим умножение $11101 \cdot 1101$. Проводя операции умножения «в столбик» и учитывая, что в двоичной системе счисления $0 \cdot 0 = 0 \cdot 1 = 0$, $1 \cdot 1 = 1$, получим:

$$\begin{array}{r} 11101 \\ \times\quad 1101 \\ \hline 11101 \\ 11101 \\ 11101 \\ \hline 101111001 \end{array} \qquad \square$$

Внимательно посмотрев на результат, заметим, что процесс умножения в двоичной системе счисления становится предельно простым: каждая «промежуточная» строка вычислений представляет собой копию числа 11101, сдвинутую влево на то или иное расстояние (т. е. копию, дополненную нулями справа). Другими словами, операция умножения может быть представлена с помощью операций сдвига и суммирования. Таким образом, при умножении

$$\begin{array}{r} a_{k-1} \ldots a_0 \\ \times\quad b_{l-1} \ldots b_0 \\ \hline a_{k-1} \ldots a_0 \\ \ldots \\ a_{k-1} \ldots\ a_0 \\ \hline c_{i+k} \quad \ldots \quad c_0 \end{array}$$

k-разрядного двоичного числа $n = \overline{(a_{k-1} \dots a_0)}_2$ на l-разрядное двоичное число $m = \overline{(b_{l-1} \dots b_0)}_2$, $k \geqslant l$, мы получаем не более l «промежуточных» строк (каждый нулевой бит числа m уменьшает это количество на единицу), каждая из которых представляет собой сдвиг влево копии числа n. Если имеется $l' \leqslant l$ строк, то задача умножения сводится к $l' - 1$ сложению, по k двоичных операций каждое, что дает в общей сложности не более $(l' - 1)k$ двоичных операций. Так как $l' - 1 < l' \leqslant l$, то мы получаем следующую оценку:

$$Time(\text{умножение } k\text{-разрядного и } l\text{-разрядного чисел } m, n) = O(kl).$$

Другими словами, *число двоичных операций, необходимых для умножения двух натуральных чисел, большее из которых равно* n, *есть* $O(\log^2 n)$:

$$Time(n \cdot m) = O(\log n \log m) = O(\log^2 n),\ n \geqslant m.$$

Вычитание

Нетрудно убедиться, что арифметическая операция вычитания имеет ту же временную сложность, что и сложение. Проиллюстрируем этот факт на примере разности двух двоичных чисел.

Пример 5.1.6 Найдем разность $11101 - 1010$. Выполняя обычные операции вычитания «в столбик», получим:

$$\begin{array}{r} 11101 \\ -\ 1010 \\ \hline 10011 \end{array}$$ □

Непосредственный подсчет числа двоичных операций, необходимых для решения задачи, позволяет убедиться в том, что вычитание из k-разрядного двоичного числа l-разрядного двоичного числа m, $k > l$, требует не более k двоичных операций, и мы получаем следующую оценку:

$$Time(\text{вычитание из } k\text{-разрядного числа } n\ l\text{-разрядного числа } m) = O(\max\{k, l\}).$$

Другими словами, *число двоичных операций, необходимых для нахождения разности двух натуральных чисел, большее из которых равно* n, *есть* $O(\log n)$:

$$Time(n - m) = O(\max\{\log n, \log m\}) = O(\log n),\ n \geqslant m.$$

Деление

Аналогичная ситуация имеет место и при выполнении арифметической операции деления: нахождение частного двух натуральных чисел обладает той же оценкой временной сложности, что и операция умножения. Для того чтобы убедиться в этом, рассмотрим пример деления двух двоичных чисел.

Пример 5.1.7 Разделим, например, число 1101111 на 11. Непосредственная проверка показывает, что обычное деление в столбик

```
1 1 0 1 1 1 1 | 1 1
1 1           | 1 0 0 1 0 1
  0 0 1 1
    1 1
    0 0 1 1
    0 0 1 1
          0
```

приведет нас к результату $110111 \div 11 = 100101$, а анализ проводимых при этом операций позволяет заметить, что в двоичной системе счисления деление производится вычитанием делителя со сдвигом вправо, если остаток больше нуля. Другими словами, операция деления может быть представлена с помощью операций сравнения, сдвига и суммирования.□

Таким образом,

$$Time(\text{деление } k\text{-разрядного числа } n \text{ на } l\text{-разрядное число } m) = O(kl).$$

Другими словами, *число двоичных операций, необходимых для деления двух натуральных чисел, большее из которых равно* n, *есть* $O(\log^2 n)$:

$$Time(n \div m) = O(\log n \log m) = O(\log^2 n),\ n \geqslant m.$$

Итак, можно утверждать, что временные затраты на сложение (вычитание) и умножение (деление) двух k-разрядных чисел оцениваются как $O(k)$ и $O(k^2)$, соответственно. Можно ли улучшить эти оценки?

За последние десятилетия было предпринято много усилий по повышению скорости умножения k-разрядных двоичных чисел при больших k.

Так, легко доказать, что *умножение двух* $2n$*-значных чисел можно свести к четырем умножениям* n*-значных чисел*. Действительно, рассмотрев $2n$-значное g-ичное число $C_{2n} = \overline{(c_{2n-1}c_{2n-2}\ldots c_1c_0)}_g$, запишем его в следующем виде:

$$\begin{aligned} C_{2n} &= c_{2n-1}\cdot g^{2n-1} + \ldots + c_1\cdot g + c_0 = \\ &= g^n\cdot(c_{2n-1}\cdot g^{n-1} + \ldots + c_{n+1}\cdot g + c_n) + (c_{n-1}\cdot g^{n-1} + \ldots + c_1\cdot g + c_0) = \\ &= g^n\cdot A_n + B_n, \end{aligned}$$

где $A_n = \overline{(c_{2n-1}c_{2n-2}\ldots c_{n+1}c_n)}_g$, $B_n = \overline{(c_{n-1}c_{n-2}\ldots c_1c_0)}_g$. Аналогично поступим с $2n$-значным g-ичным числом $D_{2n} = \overline{(d_{2n-1}d_{2n-2}\ldots d_1d_0)}_g$:

$$D_{2n} = g^n\cdot E_n + F_n,$$

где $E_n = \overline{(d_{2n-1}d_{2n-1}\ldots d_{n+1}d_n)}_g$, $F_n = \overline{(d_{n-1}d_{n-2}\ldots d_1d_0)}_g$.

Найдем произведение $C_{2n} \cdot D_{2n}$:

$$C_{2n} \cdot D_{2n} = (g^n \cdot A_n + B_n) \cdot (g^n \cdot E_n + F_n) =$$
$$= g^{2n} \cdot A_n \cdot E_n + g^n \cdot (A_n \cdot F_n + B_n \cdot E_n) + B_n \cdot F_n.$$

Таким образом, мы получили четыре умножения n-значных чисел:

$$A_n \cdot E_n;\ A_n \cdot F_n;\ B_n \cdot E_n;\ B_n \cdot F_n.$$

(Остальные действия по сравнению с умножениями имеют пренебрежимо малые затраты времени.)

Однако такой подход в целом не улучшает ситуацию, поскольку порядок временных затрат остается неизменным:

$$Time(\text{умножение двух } 2n\text{-значных чисел}) = O((2n)^2) = O(4n^2) = O(n^2),$$

$$Time(\text{четырех умножение } n\text{-значных чисел}) = 4O(n^2) = O(n^2).$$

В 1962 г. Анатолий Алексеевич Карацуба (1937–2008) показал [51], что *умножение двух $2n$-значных чисел можно свести к трем умножениям n-значных чисел*:

$$C_{2n} \cdot D_{2n} = (g^n \cdot A_n + B_n) \cdot (g^n \cdot E_n + F_n) =$$
$$= (g^{2n} + g^n) \cdot A_n \cdot E_n + g^n \cdot (A_n - B_n) \cdot (F_n - E_n) + (g^n + 1) B_n \cdot F_n.$$

Time(трех умножений)$= 3\,O(n^2)$. Для больших n это дает значимую экономию времени, требующегося на выполнение операции.

Пример 5.1.8 Рассмотрим процесс умножения четырехзначных чисел 1234 и 5078. Проводя обычное умножение «в столбик», получим:

$$\begin{array}{r} 1234 \\ \times\ 5078 \\ \hline 9872 \\ 8638 \\ 6170 \\ \hline 6266252 \end{array}$$

Представляя числа 1234 и 5078 в виде $1234 = 100 \cdot 12 + 34$ и $5078 = 100 \cdot 50 + 78$, соответственно, осуществим умножение по схеме

$$1234 \cdot 5078 = (100 \cdot 12 + 34)(100 \cdot 50 + 78) =$$
$$= 10^4 \cdot (12 \cdot 50) + 10^2 (12 \cdot 78 + 34 \cdot 50) + 34 \cdot 78.$$

Найдя четыре произведения $12 \cdot 50 = 600$; $12 \cdot 78 = 936$; $34 \cdot 50 = 1700$; $34 \cdot 78 = 2652$ двузначных чисел, завершим вычисления:

$$1234 \cdot 5078 = 10^4 \cdot 600 + 10^2 (936 + 1700) + 2652 =$$
$$= 6000000 + 263600 + 2652 = 6266252.$$

Наконец, используя те же представления чисел 1234 и 5078 в виде $1234 = 100 \cdot 12 + 34$ и $5078 = 100 \cdot 50 + 78$, соответственно, осуществим умножение по схеме А. А. Карацубы:

$$1234 \cdot 5078 = (10^4 + 10^2) \cdot (12 \cdot 50) + 10^2 \cdot ((12-34) \cdot (78-50)) + (10^2 + 1)(34 \cdot 78).$$

Найдя три произведения $12 \cdot 50 = 600$; $(12-34) \cdot (78-50) = -22 \cdot 28 = 616$; $34 \cdot 78 = 2652$ двузначных чисел, завершим вычисления:

$$1234 \cdot 5078 = 10100 \cdot 600 - 100 \cdot 616 + 101 \cdot 2652 =$$
$$= 6060000 - 61600 + 267852 = 6266252. \qquad \square$$

Существуют еще более быстрые алгоритмы осуществления операции умножения. Так, используя *алгоритм Шенхаге-Штрассена*, основанный на так называемым *быстром преобразовании Фурье*, можно выполнить умножение двух целых чисел длины k бит каждое, выполнив $O(k \log k \log \log k)$ двоичных операций. Это лучше, чем $O(k^2)$, и даже лучше, чем $O(k^{1+\epsilon})$ при любом сколь угодно малом $\epsilon > 0$.

Возведение в степень

Чтобы вычислить степень m^n, $m, n \in \mathbb{N}$, обычным способом, нам предстоит выполнить $n-1$ умножение чисел, разрядность которых будет расти. Это, конечно, потребует очень больших временных затрат.

Однако для возведения в степень, как и для умножения, существуют способы повысить скорость вычислений, основанные на уменьшении количества производимых в ходе решения задачи умножений. Рассмотрим один из них.

Воспользуемся для показателя степени двоичной записью, т.е. представим число n в виде

$$n = e_0 + e_1 \cdot 2 + e_2 \cdot 2^2 + \ldots + e_{k-1} \cdot 2^{k-1},$$

где $e_i \in \{0, 1\}$, и $e_{k-1} = 1$. Таким образом, число n содержит k двоичных разрядов. Тогда

$$m^n = m^{e_0 + e_1 \cdot 2 + e_2 \cdot 2^2 + \ldots + e_{k-1} \cdot 2^{k-1}} = m^{e_0} \cdot m^{e_1 \cdot 2} \cdot \ldots \cdot m^{e_{k-1} \cdot 2^{k-1}} =$$
$$= m^{e_0} \cdot (m^2)^{e_1} \cdot \ldots \cdot (m^{2^{k-1}})^{e_{k-1}}.$$

Следовательно, операцию возведения натурального числа m в натуральную степень n можно провести по следующей схеме: сначала вычислить числа

$$m^2, m^{2^2} = (m^2)^2, \ldots, m^{2^{k-1}} = (m^{2^{k-2}})^2,$$

то есть произвести $k-1$ возведение в квадрат, а затем перемножить те из них, которым соответствует $e_i = 1$, выполнив не более чем $k-1$ умножение.

При таком подходе для возведения числа m в степень n будет выполнено не более чем $2(k-1)$ умножение. Таким образом, *для возведения числа m в степень n требуется $O(\log n)$ умножений*:

$$\text{Число умножений (возведение числа } m \text{ в степень } n) = O(\log n).$$

Пример 5.1.9 Для вычисления степени 5^{29} найдем двоичную запись числа 29:

$$29 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 = 11101_2.$$

Начиная с числа 5, осуществим операцию последовательного возведения в квадрат:

$$5^2 = 25, 5^{2^2} = (5^2)^2 = 25^2 = 625, 5^{2^3} = (5^{2^2})^2 = 625^2 = 390625,$$

$$5^{2^4} = (5^{2^3})^2 = 390625^2 = 152587890625.$$

В ходе этой операции мы выполнили четыре умножения. Наконец, перемножим числа 5, 625, 390625, 152587890625, соответствующие ненулевым цифрам в двоичной записи числа 29, что потребует трех умножений: $5 \cdot 625 \cdot 390625 \cdot 152587890625$. Таким образом,

$$5^{29} = 5 \cdot 625 \cdot 390625 \cdot 152587890625 =$$

$$= 1,93715\ldots15625 \cdot 10^{20} = 193715\ldots15625. \quad \square$$

5.1.4. Классификация алгоритмов по их трудоемкости

Конечно, может существовать несколько алгоритмов, решающих одну и ту же задачу. В этой ситуации возникает вопрос сравнения алгоритмов: при одних условиях мы можем воспользоваться алгоритмом, который проще в реализации, при других — выбрать более быстрый алгоритм, наконец, предпочесть некий компромисс между простотой и быстродействием.

Для того чтобы сделать правильный выбор, необходимо познакомиться с различными подходами к классификации алгоритмов [29], [74], [53].

Классифицируя по скорости реализации, выделяют *полиномиальные*, *экспоненциальные* и *субэкспоненциальные* по времени алгоритмы. Принадлежность к тому или иному классу определяется поведением *функции f сложности алгоритма*. Примером такой функции служит рассмотренная выше функция $Time(n, m)$, определяющая расход времени на осуществление той или иной арифметической операции над натуральными числами n и m.

Пусть $f(n_1, \ldots n_s)$ — функция, задающая сложность алгоритма, оперирующего с целыми числами $n_1, \ldots n_s$.

Алгоритм, обладающий функцией сложности $f(n_1, \ldots n_s)$, называется *полиномиальным*, если

$$f(n_1, \ldots, n_s) = O(\log^{d_1} n_1 \cdot \ldots \cdot \log^{d_s} n_s)$$

при целых неотрицательных $d_1, \ldots d_s$.

Алгоритм, обладающий функцией сложности $f(n_1, \ldots n_s)$, называется *экспоненциальным*, если

$$f(n_1, \ldots, n_s) = O(n_1^{z_1} \cdot \ldots \cdot n_s^{z_s})$$

при целых неотрицательных $z_1, \ldots z_s$, хотя бы одно из которых отлично он нуля.

Алгоритм, обладающий функцией сложности $f(n_1, \ldots n_s)$, называется *субэкспоненциальным*, если

$$O(\log^{d_1} n_1 \cdot \ldots \cdot \log^{d_s} n_s) < f(n_1, \ldots n_s) < O(n_1^{z_1} \cdot \ldots \cdot n_s^{z_s})$$

при целых неотрицательных $d_1, \ldots d_s$ и целых неотрицательных $z_1, \ldots z_s$, хотя бы одно из которых отлично от нуля.

Для того чтобы лучше понять используемую здесь терминологию, рассмотрим алгоритм для проведения вычислений, оперирующий натуральными числами $n_1, n_2, \ldots n_s$ и обладающий функцией сложности $f(n_1, \ldots n_s)$, оценивающей число двоичных операций при работе этого алгоритма. Если числа $n_1, n_2, \ldots n_s$ состоят из $k_1, k_2, \ldots, k_s$ бит, соответственно, то функцию f можно рассматривать как функцию g от $k_1, \ldots k_s$, и проводить классификацию алгоритмов в зависимости от поведения функции g. Поскольку $k_i = O(\log n_i)$, $i = 1, 2, \ldots s$, то, например, полиномиальным по времени будет алгоритм, для которого существуют такие целые неотрицательные числа $d_1, d_2, \ldots, d_s$, что число двоичных операций при работе этого алгоритма равно $O(k_1^{d_1} k_2^{d_2} \ldots k_s^{d_s})$. Как изменится определение экспоненциального алгоритма при таком переходе? Как изменится определение субэкспоненциального алгоритма?

Пример 5.1.10 Пользуясь этой классификацией, мы убеждаемся в том, что все рассмотренные выше алгоритмы арифметических операций являются полиномиальными: для натуральных чисел n и m длины k и l бит, соответственно, сложность сложения и вычитания при $k \geqslant l$ равна $O(k) = O(\log n)$; сложность умножения и деления при $k \geqslant l$ равна $O(k^2) = O(\log^2 n)$. □

Замечание. *В теории алгоритмов полиномиальные алгоритмы относят к классу P (от англ. polynomial). Поскольку для таких алгоритмов время их работы не превосходит многочлена от размера входных данных, а, значит, не слишком сильно зависит от этого размера, то алгоритмы, принадлежащие классу P, считаются быстрыми.*

Рассмотрим еще один способ классификации алгоритмов, который понадобится нам несколько позже. Он базируется на подразделении алгоритмов на *детерминированные* и *вероятностные*.

Алгоритм называется *детерминированным*, если после фиксированного числа шагов (операций над элементами конечного множества) результат его работы всегда является решением поставленной задачи. (Слово «всегда» в приведенном определении является существенно важным.)

Алгоритм называется *вероятностным*, если выполняется одно из следующих утверждений: результат работы алгоритма является решением поставленной задачи с некоторой вероятностью; алгоритм оканчивает свою работу с некоторой вероятностью; оценка числа шагов алгоритма является случайной величиной.

Собственно, один и тот же алгоритм может рассматриваться и как детерминированный, и как вероятностный, в зависимости от нашего толкования этого термина либо от попытки минимизировать его сложность.

Для детерминированного алгоритма оценка сложности вычисляется однозначно, в то время как для вероятностного алгоритма оценка сложности вычисляется при некоторых предположениях, которые могут существенно влиять на получаемые результаты. Так, например, оценки сложности вычислительных алгоритмов часто опираются на какие-либо недоказанные, но правдоподобные гипотезы, обычно относящиеся к аналитической теории чисел (гипотеза Римана, расширенная гипотеза Римана и др.).

Для некоторых задач эффективные алгоритмы вообще неизвестны. Иногда в таких случаях все же можно предположить последовательность действий, которая, «если повезет», быстро приводит к требуемому результату. Обычно работа этих алгоритмов зависит от одного или нескольких параметров. В худшем случае они работают достаточно долго, но удачный выбор параметров определяет быстрое завершение работы. Такие алгоритмы, если множество «хороших» значений параметра велико, на практике работают достаточно эффективно, хотя и не имеют хороших оценок сложности.

Упражнения

(1) Запишите первые десять натуральных чисел в системах счисления с основанием g, равным 2; 3; 4; 5. Проведите ту же работу для чисел 100, 101, ..., 109; для чисел 9990, 9991, ..., 9999.

(2) Выразите число 106 в системах счисления с основанием 2; 7; 26; 33. Подсчитайте число понадобившихся для этого арифметических операций.

(3) Запишите число 22010 в системе счисления с основанием g, если $g = 5$; $g = 6$; $g = 8$; $g = 11$; $g = 12$; $g = 14$; $g = 16$; $g = 60$. Подсчитайте число понадобившихся для этого арифметических операций.

(4) Используя десятичную систему счисления, переведите число n в систему с основанием g, если

a) $n = 101_2$, $g = 3$; c) $n = 2121_4$, $g = 8$; e) $n = 1000_5$, $g = 8$;
b) $n = 777_8$, $g = 12$; d) $n = 2320_4$, $g = 16$; f) $n = 11111_3$, $g = 9$.

Осуществите перевод более рациональным способом. Подсчитайте число понадобившихся в каждом из случаев арифметических операций. Сравните результаты.

(5) Переведите число n в систему с основанием g через десятичную систему счисления, если

a) $n = 100_3$, $g = 2$; c) $n = 1220_4$, $g = 2$; e) $n = 77_8$, $g = 3$;
b) $n = 1A1_{12}$, $g = 8$; d) $n = A01_{12}$, $g = 7$; f) $n = 543_8$, $g = 7$.

Осуществите перевод более рациональным способом. Подсчитайте число понадобившихся в каждом из случаев арифметических операций. Сравните результаты.

(6) Используя десятичную систему счисления, переведите число n в систему с основанием g, если

a) $n = 101110111111_2$, $g = 16$;
b) $n = 333323333_4$, $g = 16$;
c) $n = 2121_3$, $g = 9$;
d) $n = 1212121212_5$, $g = 25$;
e) $n = 1212121212100013$, $g = 27$;
f) $n = 10000211111312121_4$, $g = 64$.

Осуществите перевод более рациональным способом. Подсчитайте число понадобившихся в каждом из случаев арифметических операций. Сравните результаты.

(7) Переведите число n в систему с основанием g через десятичную систему счисления, если

a) $n = 100_8$, $g = 2$;
b) $n = 1A1_{16}$, $g = 4$;
c) $n = 33333355_9$, $g = 3$;
d) $n = 121212120_4$, $g = 2$;
e) $n = AD1_{25}$, $g = 5$;
f) $n = AAAAAABBBBB_{27}$, $g = 3$;
g) $n = CCCCCAAAAA00000_{16}$, $g = 2$.

Осуществите перевод более рациональным способом. Подсчитайте число понадобившихся в каждом из случаев арифметических операций. Сравните результаты.

(8) Найдите количество знаков в g-ичной записи числа n, если

a) $n = 4561, g = 3$; d) $n = 155, g = 12$; g) $n = 1000, g = 2$;
b) $n = 181, g = 11$; e) $n = 276, g = 5$; h) $n = 1940, g = 4$.
c) $n = 38446, g = 8$; f) $n = 1453, g = 13$;

Проверьте результат, найдя соответствующую g-ичную запись.

(9) Осуществите сложение и вычитание g-ичных чисел a и b:

a) $a = 54561_7$, $b = 481_7$; e) $a = B11B12_{12}$, $b = AABB12_{12}$;
b) $a = 332540_6$, $b = 53401_6$; f) $a = 2210102_3$, $b = 222200_3$;
c) $a = 756101_8$, $b = 1304_8$; g) $a = 32014_5$, $b = 4400_5$;
d) $a = 33333_9$, $b = 7777_9$; h) $a = ABC121110_{13}$, $b = 112121110_{13}$.

В каждом из случаев подсчитайте количество выполненных арифметических операций.

(10) Осуществите сложение и вычитание двоичных чисел a и b:

a) $a = 10110111111_2, b = 11011001_2$;
b) $a = 111111111_2, b = 1110111_2$;
c) $a = 1010101_2, b = 111110_2$;
d) $a = 110011001100_2, b = 11110011100_2$;
e) $a = 11111001111100_2, b = 11000111100011_2$;
f) $a = 10101010101010101010_2, b = 111111100001111111_2$.

В каждом из случаев подсчитайте количество выполненных бинарных операций.

(11) Осуществите умножение g-ичных чисел a и b:

a) $a = 4561_7$, $b = 55481_7$; e) $a = A11B12_{12}$, $b = AABB1212_{12}$;
b) $a = 2540_6$, $b = 53401_6$; f) $a = 10102_3$, $b = 22220011_3$;
c) $a = 756101_8$, $b = 1304_8$; g) $a = 32014_5$, $b = 4444400_5$;
d) $a = 33333_9$, $b = 77777_9$; h) $a = ABC121110_{13}$, $b = 101112121110_{13}$.

Осуществите деление полученного числа на b. В каждом из случаев подсчитайте количество выполненных арифметических операций.

(12) Осуществите умножение двоичных чисел a и b:

a) $a = 110111111_2$, $b = 1000011001_2$;
b) $a = 111111111_2$, $b = 111000111_2$;
c) $a = 1010101_2$, $b = 111110000_2$;
d) $a = 110011001100_2$, $b = 11110011100_2$;
e) $a = 1111100111_2$, $b = 1100011_2$;
f) $a = 10101010101010101010_2$, $b = 111001_2$

Осуществите деление полученного числа на a. В каждом из случаев подсчитайте количество выполненных бинарных операций.

(13) Выполните действия в восьмеричной системе счисления:

a) $(125_8 \cdot 27_8 - 1016015_8 \div 3751_8) \cdot 342_8 + 10477_8$;

b) $2744_8 + 1016015_8 \div 205_8 + 134_8 \cdot 257_8$;

c) $2035_8 + 233654_8 \div 155_8 \cdot (2112200_8 - 637_8 \cdot 134_8) + 467_8$;

d) $233654_8 \div 507_8 \cdot (2221100_8 - 376_8 \cdot 245_8) \cdot 764_8$.

(14) Вычислите:

a) $141_7 \cdot 41_7 + 25110_7 \div 625_7 - 1522_7 \cdot 32_7$;

b) $(7501_9 + 417_9 \cdot 783_9) \cdot (28753_9 - 22067_9 \div 144_9)$;

c) $438_{11} \cdot 57_{11} - (51A3406_{11} \div A539_{11} - 3A6_{11}) + 9979_{11}$;

d) $(6024_7 + 265502_7 \div 251_7) \cdot 437 - 345_7 \cdot 24_7$;

e) $(2606_7 \cdot 423_7 - 30232666_7 \cdot 343224_7 + 255443_7) \cdot 1265_7$;

f) $(855A20_{12} \div 26_{12} - 11_{12} \cdot A_{12}) \cdot 2A3_{12} + 44901_{12}$.

(15) Выполните действия:

a) $(235_6 + 423_6) \cdot 10_6$;

b) $4433220_9 \cdot 2233444_9 + 100_9$;

c) $(1235A_{12} + 4B42_{12}) \div 2_{12}$;

d) $3202_4 \cdot (11133_4 - 3212_4)$;

e) $ABCD_{14} \cdot (51C1_{14} - AD6_{14})$;

f) $1024_6 \cdot 550_6 + 444_6 \cdot (153_6 - 54_6)$.

(16) Выполните умножение двух $2n$-значных чисел тремя способами:

a) $6654 \cdot 7652$;

b) $3897 \cdot 2308$;

c) $665348 \cdot 276512$;

d) $273897 \cdot 802308$;

e) $66534228 \cdot 78276512$;

f) $109273897 \cdot 21802308$.

(17) Осуществите возведение числа m в степень n двумя способами:

a) $m = 2, n = 10$;

b) $m = 2, n = 20$;

c) $m = 2, n = 30$;

d) $m = 3, n = 13$;

e) $m = 3, n = 14$;

f) $m = 3, n = 15$;

g) $m = 5, n = 12$;

h) $m = 5, n = 13$;

i) $m = 5, n = 14$.

В каждом из случаев подсчитайте количество выполненных арифметических операций. Сравните полученные результаты.

(18) Докажите, что

a) $n^5 - n^3 + 5n = O(n^5)$;

b) $n^{100} + n^{10} + 1 = O(n^{100})$;

c) $\dfrac{1}{n^4 - n^2 + 5} = O(n^{-4})$;

d) $2\log^3 n - 17 = O(\log^3 n)$;

e) $\sin 6n \cdot \log n = O(\log n)$;

f) $\cos(nm) = O(1)$.

(19) Приведите примеры функций, представляющих собой $O(h(n))$, если

a) $h(n) = n^{10}$; b) $h = n^2$; c) $h(n) \equiv 1$; d) $h(n) = n^{-1}$.

(20) Самый простой способ найти нетривиальный множитель натурального числа n — перебрать все натуральные числа до n. Оцените количество делений и максимальное количество битовых операций для выполнения этой задачи.

Задачи

[1] Для обозначения цифр системы счисления с основанием $g = 26$ используются буквы английского алфавита A=0, ..., Z=25. Разделите HAPPY_{26} на SAD_{26}.

[2] Для обозначения цифр системы счисления с основанием $g = 33$ используются буквы русского алфавита А=0, ..., Я=32. Сложите УДАЧА_{33} и УСПЕХ_{33}.

[3] Запишите число $\pi = 3,1415926\ldots$ в двоичной системе счисления, оставив 15 цифр после запятой; в 26-ричной системе счисления, оставив 3 цифры после запятой.

[4] Запишите число $e = 2,7182818\ldots$ в двоичной системе счисления, оставив 15 цифр после запятой; в 26-ричной системе счисления, оставив 3 цифры после запятой.

[5] Докажите свойства символа «O-большое»:

a) $f(n) = O(f(n))$;

b) $O(-f(n)) = O(f(n))$;

c) $O(Cf(n)) = O(f(n))$, если C — константа;

d) $O(f(n)) + O(g(n)) = O(f(n) + g(n))$;

e) $O(f(n)) \cdot O(g(n)) = O(f(n) \cdot g(n))$;

f) если $g(n) = O(f(n))$, и $h(n) = O(g(n))$, то $h(n) = O(f(n))$.

[6] Докажите, что для любого сколь угодно малого положительного числа ϵ имеет место оценка $\log n = O(n^\epsilon)$, т.е. при больших n логарифмическая функция $\log n$ «меньше» любой степенной функции n^ϵ при любом сколь угодно малом показателе степени ϵ. Докажите, что, более того, при любом фиксированном сколь угодно большом положительном числе α имеет место оценка $\log^\alpha n = O(n^\epsilon)$.

[7] Оцените время, требующееся для перевода двоичного числа, состоящего из k бит, в десятичную систему счисления.

[8] Оцените время, требующиеся для перевода числа двоичного числа, состоящего из k бит, в систему счисления по основанию g, которое может быть очень большим.

9 Опишите алгоритмы перевода натурального числа из двоичной системы в шестнадцатиричную и обратно; объясните, почему эти алгоритмы требуют много меньше времени, чем алгоритмы перевода чисел из двоичной системы в пятнадцатиричную?

10 Используя обозначение «*О-большое*», оцените в терминах простой функции от n число двоичных операций при вычислении в двоичной системе счисления произведения $3 \cdot n$; $m \cdot n$, $m < n$; $n \cdot n$; $M \cdot n$, $M < n < 2M$.

11 Найдите верхнюю границу для числа двоичных операций, необходимых для вычисления *факториала* $n! = 1 \cdot 2 \cdot \ldots \cdot n$, $n \in \mathbb{N}$.

12 Найдите верхнюю границу для числа двоичных операций, необходимых для вычисления *биномиального коэффициента* $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$, $n, k \in \mathbb{N}, n \geqslant k$.

13 Определите верхнюю границу для числа двоичных операций, необходимых для умножения многочлена степени не выше n_1 на многочлен степени не выше n_2, считая, что коэффициенты многочленов — положительные целые числа, не превосходящие m.

14 Пусть $\pi(n) = \sum\limits_{p \leqslant n} 1$ — функция, вычисляющая количество простых чисел, не превосходящих n. Согласно теореме о распределении простых чисел, $\lim\limits_{n \to \infty} \dfrac{\pi(n)}{\frac{n}{\log n}} = 1$. В этом случае пишут, что $\pi(n) \sim \dfrac{n}{\log n}$, и говорят, что *функция* $\pi(n)$ *имеет асимптотику* $\dfrac{n}{\log n}$. Используя этот факт, выполните следующие действия:

a) оцените число двоичных разрядов в произведении всех простых чисел, меньших n;

b) найдите границу для числа двоичных операций при любом из умножений, которые производятся при вычислении этого произведения;

c) оцените число двоичных операций, требующихся для вычисления произведения всех простых чисел, меньших n.

15 Оцените число двоичных операций, необходимых для проверки простоты числа при помощи последовательного деления на все простые числа, не превосходящие $\sqrt{n}$, полагая, что имеется список таких простых чисел.

16 Оцените время, необходимое для ответа на вопрос, имеет ли число n простой делитель, не превосходящий число m, полагая, что имеется список таких простых чисел.

17 Докажите, что для нахождения нетривиального множителя натурального числа n достаточно перебрать все натуральные числа до $\sqrt{n}$. Оцените количество делений и максимальное количество битовых операций для выполнения этой задачи.

18 Оцените число двоичных операций, необходимых для проверки простоты нечетного числа n при помощи последовательного деления на все нечетные числа, не превосходящие $\sqrt{n}$.

19 Приведите пример полиномиального алгоритма; алгоритма, не являющегося полиномиальным.

20 Функцию $f(n)$ сложности алгоритма называют константой, если $f(n) = O(1)$. Приведите примеры таких функций. Приведите примеры алгоритмов, функция сложности которых является константой.

21 Функцию $f(n)$ сложности алгоритма называют сложностью тотального перебора, если $f(n) = O(n)$. Приведите примеры таких функций. Приведите примеры алгоритмов, функция сложности которых является сложностью тотального перебора.

5.2. Простейшие арифметические алгоритмы и их трудоемкость

Изучив особенности простейших алгоритмов, осуществляющих выполнение арифметических операций, мы перейдем к рассмотрению других хорошо известных арифметических алгоритмов, которые, с одной стороны, опираются на уже знакомые нам методы сложения, вычитания, умножения и деления натуральных чисел, и, с другой стороны, часто используются в качестве подзадач при решении более сложных вычислительных проблем.

5.2.1. Алгоритм Евклида

Наиболее известный алгоритм такого рода, осуществляющий нахождение наибольшего общего делителя двух натуральных чисел, был создан древнегреческим математиком Евклидом (Euclid, около 325 г. до н.э. – до 265 года до н.э.). Первое описание алгоритма было дано в «Началах» Евклида (около 300 г. до н.э.), что делает его одним из старейших численных алгоритмов, используемых в наше время.

В самом простом случае алгоритм Евклида, оперирующий с парой натуральных чисел, формирует новую пару, которая состоит из меньшего числа и разницы между большим и меньшим числом. Процесс повторяется, пока числа не станут равными. Найденное число и есть наибольший общий делитель исходной пары.

Для детального исследования алгоритма Евклида и его приложений нам придется использовать ряд классических свойств делимости целых чисел [20], [33], [36], [98].

Наибольшим общим делителем $(a_1, \ldots, a_n)$ целых чисел $a_1, \ldots a_n$, хотя бы одно из которых не равно нулю, называется наибольшее целое число, делящее каждое из чисел $a_1, \ldots a_n$. Например, $(4, -6) = 2$, так как множество общих делителей чисел 4 и -6 имеет вид $\{-2, -1, 1, 2\}$, и его наибольший элемент равен 2.

Свойства наибольшего общего делителя

1. $(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}, p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$, где $\alpha_i, \beta_i \geqslant 0$, $\gamma_i = \min\{\alpha_i, \beta_i\}$.
2. Каждый общий делитель чисел a и b делит (a, b).
3. Если $(a, b) = d$, то существуют целые числа x и y, такие что $ax + by = d$.
4. Если $a|bc$, и $(a, b) = d$, то $\dfrac{a}{d}|c$.
5. $(ma, mb) = m(a, b)$ для любого $m \in \mathbb{N}$.
6. Если $m|a$ и $m|b$, где $m \in \mathbb{N}$, то $\left(\dfrac{a}{m}, \dfrac{b}{m}\right) = \dfrac{(a, b)}{m}$.
7. Если $a \in \mathbb{Z}$, $b \in \mathbb{N}$, и $b|a$, то $(a, b) = b$.
8. Если целые числа a, b, c, k связаны соотношением $a = bk + c$, то $(a, b) = (b, c)$.
9. $(a + mb, b) = (a, b)$ для любого $m \in \mathbb{Z}$.

Из первого свойства следует, что наибольший общий делитель двух натуральных чисел можно найти, раскладывая имеющиеся числа по степеням простых. Однако в большинстве случаев удобнее использовать для этой процедуры *алгоритм Евклида*, осуществляющий определение наибольшего общего делителя двух натуральных чисел путем последовательного применения теоремы о делении с остатком.

Именно, *для любого целого a и любого натурального b, не делящего a, наибольший общий делитель чисел a и b равен последнему ненулевому остатку r_s следующего алгоритма*:

$$
\begin{aligned}
&a = bq_1 + r_1, \quad 0 < r_1 < b,\\
&b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{s-2} = r_{s-1} q_s + r_s, \quad 0 < r_s < r_{s-1},\\
&r_{s-1} = r_s q_s + 0,
\end{aligned}
$$

где $q_i, r_i \in \mathbb{Z}$, $i = 1, 2, \ldots s$.

Другими словами, *наибольший общий делитель чисел* a *и* b ($a \in \mathbb{Z}, b \in \mathbb{N}$, $b \nmid a$) *равен последнему ненулевому остатку алгоритма Евклида, записанного для этих чисел.*

Действительно, пользуясь перечисленными выше свойствами, мы можем утверждать, что

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_{s-2}, r_{s-1}) = (r_{s-1}, r_s),$$

в то время как $(r_{s-1}, r_s) = r_s$. При этом наличие хотя бы одного ненулевого остатка обеспечивается условием $b \nmid a$, в то время как существование последнего ненулевого остатка (то есть конечное число шагов алгоритма) следует из того факта, что числа $r_1, r_2, \ldots, r_s$ образуют строго убывающую последовательность $b > r_1 > r_2 > \ldots > r_s > 0$ натуральных чисел, которая заведомо конечна. (См., например, [20], [98]).

Пример 5.2.11 Найдем наибольший общий делитель натуральных чисел 88 и 52.

Во-первых, пользуясь определением, мы можем выписать множество $\{1, 2, 4, 8, 11, 22, 44, 88\}$ натуральных делителей числа 88, множество $\{1, 2, 4, 13, 26, 52\}$ натуральных делителей числа 52, построить множество $\{1, 2, 4\}$ общих натуральных делителей чисел 88 и 52 и определить его наибольший элемент 4. Таким образом, $(88, 52) = 4$.

С другой стороны, раскладывая числа 88 и 52 по степеням простых, мы получим, что $88 = 2^3 \cdot 11$, $52 = 2^2 \cdot 13$, и, пользуясь формулой

$$(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}, p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s,\beta_s\}},$$

найдем наибольший общий делитель чисел 88 и 52:

$$(88, 52) = (2^3 \cdot 11^1 \cdot 13^0, 2^2 \cdot 11^0 \cdot 13^1) = 2^2 \cdot 11^0 \cdot 13^0 = 4.$$

Наконец, воспользовавшись для нахождения наибольшего общего делителя чисел 88 и 52 алгоритмом Евклида, получим:

$$88 = 52 \cdot 1 + 36,$$
$$52 = 36 \cdot 1 + 16,$$
$$36 = 16 \cdot 2 + 4,$$
$$16 = 4 \cdot 4 + 0,$$

и, следовательно, $(88, 52) = 4$. □

Замечание. *Этот алгоритм может быть использован на любом множестве, где возможно деление с остатком. Такие множества включают в себя кольца многочленов над полем, кольцо целых чисел Гаусса, наконец, Евклидовы области.*

Рассмотрим формальную *схему реализации алгоритма Евклида.*

Алгоритм I.

Дано: целые числа a и b. Найти: $d = (a, b)$.

Шаг 1. $r_0 = a$, $r_1 = b$, $i = 1$.

Шаг 2. Найдем r_{i+1}: $r_{i-1} = r_i q + r_{i+1}$.

2.1. Если $r_{i+1} = 0$ то $d = r_i$.

2.2. Если $r_{i+1} \neq 0$, то проведем операции $(r_{i-1}, r_i) \to (r_i, r_{i+1})$, $i \to i + 1$ и вернемся к шагу 2. ▷

Протокол работы алгоритма для чисел $a = 88$, $b = 52$ представлен в нижеследующей таблице.

i	0	1	2	3	4	5
r_i	88	52	36	16	**4**	0

Перейдем к оценке трудоемкости алгоритма Евклида, используемого для нахождения наибольшего общего делителя чисел n и m, где $n > m$. Для этого подсчитаем, сколько раз при выполнении алгоритма производится деление. Это нетрудно сделать, убедившись, что получающиеся в ходе работы остатки убывают довольно быстро: именно, $r_{i+2} < \dfrac{r_i}{2}$.

Действительно, в случае $r_{i+1} \leqslant \dfrac{r_i}{2}$ мы сразу получаем оценку $r_{i+2} < r_{i+1} < \dfrac{r_i}{2}$; если же $r_{i+1} > \dfrac{r_i}{2}$, то следующее деление имеет вид $r_i = 1 \cdot r_{i+1} + r_{i+2}$, и, следовательно, $r_{i+2} = r_i - r_{i+1} < \dfrac{r_i}{2}$.

Так как за каждые два шага алгоритма остаток уменьшается по крайней мере вдвое и при этом не может стать меньше 1, то в ходе работы производится не более $2\lfloor \log_2 n \rfloor$ делений. Эта величина оценивается как $O(\log n)$. Кроме того, каждое деление производится над числами, не превышающими n, и, следовательно, в ходе его выполнения осуществляется $O(\log^2 n)$ двоичных операций. Таким образом, общее время работы алгоритма Евклида составляет $O(\log n) \cdot O(\log^2 n) = O(\log^3 n)$. Мы доказали, что *число двоичных операций, необходимых для нахождения с помощью алгоритма Евклида наибольшего общего делителя двух натуральных чисел n и m, большее из которых равно n, есть* $O(\log^3 n)$:

$$Time(\text{нахождение}(n, m) \text{ по алгоритму Евклида}) = O(\log^3 n),\ n > m.$$

Замечание. *Более тщательный подсчет числа двоичных операций алгоритма, учитывающий уменьшение чисел, участвующих в делении, позволяет улучшить оценку времени работы алгоритма Евклида до* $O(\log^2 n)$.

5.2.2. Расширенный алгоритм Евклида

Хорошо известно, что для любых натуральных чисел a и b существуют такие целые числа u и v, что $(a, b) = ua+bv$. Другими словами, *наибольший общий делитель двух чисел можно представить в виде целочисленной линейной комбинации этих чисел.*

Такое разложение нетрудно найти, используя алгоритм Евклида для нахождения (a, b): проходя последовательность равенств алгоритма снизу вверх и каждый раз выражая (a, b) через все более ранние остатки, мы в конце концов получаем выражение (a, b) через исходные числа a и b [98], [36].

Пример 5.2.12 Найдем представление наибольшего общего делителя $(88, 52)$ чисел 88 и 52 в виде их целочисленной линейной комбинации. Для этого, воспользовавшись полученными ранее при реализации алгоритма Евклида равенствами $88 = 52 \cdot 1 + 36$; $52 = 36 \cdot 1 + 16$; $36 = 16 \cdot 2 + 4$; $16 = 4 \cdot 4 + 0$, выразим из них $(88, 52) = 4$ по следующей схеме:

$$4 = 36 - 16 \cdot 2 = 36 - (52 - 36) \cdot 2 = 3 \cdot 36 - 2 \cdot 52 =$$
$$= 3(88 - 52) - 2 \cdot 52 + 3 \cdot 88 - 5 \cdot 52.$$

Таким образом, $4 = 3 \cdot 8 + (-5) \cdot 52$. □

Разложения такого рода бывают крайне полезны при решении различных вычислительных задач. Поэтому на практике часто требуется использовать алгоритм, который, одновременно с нахождением наибольшего общего делителя (a, b) двух натуральных чисел a и b, находит и целые u, v, для которых $(a, b) = ua + vb$. Такой алгоритм называется *расширенным алгоритмом Евклида.*

Рассмотрим формальную *схему реализации расширенного алгоритма Евклида.*

Алгоритм II.

Дано: целые числа a и b. Найти: $d = (a, b)$ и целые x, y: $d = xa + yb$.

Шаг 1. Зададим $r_0 = a$, $r_1 = b$, $x_0 = 1, y_0 = 0$, $x_1 = 0, y_1 = 1$, $i = 1$.

Шаг 2. Вычислим r_{i+1}, x_{i+1}, y_{i+1}: $r_{i+1} = r_{i-1} - q_i r_i$, $x_{i+1} = x_{i-1} - q_i x_i$, $y_{i+1} = y_{i-1} - q_i y_i$.

2.1. Если $r_{i+1} = 0$, то $d = r_i$, $x = x_i$, $y = y_i$.

2.2. Если $r_{i+1} \neq 0$, то осуществим операции $(r_{i-1}, r_i) \to (r_i, r_{i+1})$, $(x_{i-1}, x_i) \to (x_i, x_{i+1})$, $(y_{i-1}, y_i) \to (y_i, y_{i+1})$, $i \to i + 1$, и вернемся к шагу 2. ▷

Протокол работы алгоритма для $a = 88$, $b = 52$ представлен в нижеследующей таблице.

i	r_{i-1}	r_i	r_{i+1}	q_i	x_{i-1}	x_i	x_{i+1}	y_{i-1}	y_i	y_{i+1}	d
1	88	52	36	1	1	0	$1-1\cdot 0=1$	0	1	$0-1\cdot 1=-1$	
2	52	36	16	1	0	1	$0-1\cdot 1=-1$	1	-1	$1-1\cdot(-1)=2$	
3	36	16	4	2	1	-1	$1-2\cdot(-1)=3$	-1	2	$-1-2\cdot 2=-5$	
4	16	**4**	**0**	4	-1	**3**	$-1-4\cdot 3=-13$	2	**-5**	$2-4\cdot(-5)=22$	**4**

Для оценки трудоемкости выражения наибольшего общего делителя (n, m) натуральных чисел n и m, $n > m$, в виде их целочисленной линейной комбинации достаточно заметить, что в ходе вычислений используются все равенства соответствующего алгоритма Евклида, число которых, как было доказано выше, есть $O(\log n)$, то есть выполняется $O(\log n)$ шагов. На каждом шаге необходимо произвести одно умножение и одно сложение или вычитание, что для чисел, не превосходящих n, осуществляется за время $O(\log^2 n)$. Таким образом, число операций для решении нашей задачи снова получилось равным $O(\log^3 n)$, и мы доказали, что *число двоичных операций, необходимых для нахождения с помощью алгоритма Евклида разложения наибольшего общего делителя двух натуральных чисел n и m, большее из которых равно n, в виде их целочисленной линейной комбинации, есть* $O(\log^3 n)$.

$$Time\ (\text{нахождение разложения } (n, m) = un + vm \text{ с целыми } u, v) = \\ = O(\log^3 n), n > m.$$

В частности, полученная оценка временной трудоемкости позволяет утверждать, что *для взаимно простых целых чисел n и m, $n > m$, представление единицы в виде целочисленной линейной комбинации этих чисел можно найти за полиномиальное время*, именно, за $O(\log^3 n)$ двоичных операций.

5.2.3. Бинарный алгоритм Евклида

При вычислениях в двоичной системе счисления можно эффективно использовать четность и нечетность используемых чисел в силу того, что в двоичной системе умножение и деление на 2 представляют собой просто перезапись числа (сдвиг), то есть операцию с пренебрежимо малой затратой времени.

В этих условиях является полезным применение *бинарного алгоритма Евклида* — разновидности классического алгоритма, осуществляющей двоичные вычисления и существенно использующей четность (нечетность) получающихся в процессе этих вычислений натуральных чисел.

Для знакомства со схемой работы данного алгоритма нам понадобится ряд свойств наибольшего общего делителя, полезных с точки зрения четности и нечетности используемых чисел. Назовем их «*бинарными*»[68].

«Бинарные» свойства НОД

1. Если $a = 2a_1$, $b = 2b_1$, то $(a, b) = 2(a_1, b_1)$.
2. Если $a = 2a_1 + 1$, $b = 2b_1$, то $(a, b) = (a, b_1)$.
3. Если $a = 2a_1 + 1$, $b = 2b_1 + 1$, то $(a, b) = (a - b, b)$.
4. Если $a = b$, то $(a, b) = a$.

Идея работы бинарного алгоритма Евклида очень проста: избавившись от «лишних» двоек в числах a и b, то есть сведя задачу к нахождению наибольшего общего делителя двух натуральных чисел, по крайней мере одно из которых нечетно, решим последнюю задачу «базовым» методом Евклида: получая на каждом шаге некоторую пару натуральных чисел, формируем новую пару, которая состоит из меньшего числа и разницы между большим и меньшим числом; повторяем процесс до тех пор, пока числа не станут равными. Найденное число и есть наибольший общий делитель исходной «нечетной» пары, а (a, b) находится теперь умножением полученного результата на нужную степень двойки.

Пример 5.2.13 Рассмотрим процесс нахождения наибольшего общего делителя чисел 88 и 52 с помощью бинарного алгоритма Евклида. Прежде всего, разделив каждое из чисел на 2, перейдем к числам $\frac{88}{2} = 44$, $\frac{52}{2} = 26$. Поскольку оба полученных числа являются четными, проделаем эту операцию еще раз: $\frac{44}{2} = 22$, $\frac{26}{2} = 13$. Дальше делить на 2 оба числа нельзя, но деление на 2 четного числа 22 допустимо и упростит вычисления. Поэтому от пары (22, 13) перейдем к паре (11, 13) и начнем процесс последовательных вычитаний. В ходе этой работы будут получены следующие пары:

$$(13 - 11 = 2, 11), (2, 11 - 2 = 9), (2, 9 - 2 = 7),$$
$$(2, 7 - 2 = 5), (2, 5 - 2 = 3), (2, 3 - 2 = 1), (2 - 1 = 1, 1).$$

Таким образом, мы получили, что $(22, 13) = (11, 13) = 1$. Следовательно,

$$(88, 52) = 2^2 \cdot (22, 13) = 4 \cdot 1 = 4.$$

Впрочем, можно продолжать делить на два четное число получающихся в ходе работы «четно-нечетных пар»; тогда последовательность пар, начиная с $(11, 13)$, будет выглядеть так:

$$(11, 13), (11, 13 - 11 = 2), (11, 1), (11 - 1 = 10, 1),$$
$$(5, 1), (5 - 1 = 4, 1), (2, 1), (1, 1).$$

На окончательный результат это, конечно, никак повлиять не может. Заметим, что вычисления можно было остановить при получении пары $(11, 1)$, поскольку, очевидным образом, $(11, 1) = 1$. □

Перейдем к рассмотрению формальной *схемы бинарного алгоритма Евклида.*

Алгоритм III.

Дано: натуральные числа a, b, $a \geqslant b$. Найти: $d = (a, b)$.

Шаг 1. Зададим a, b, $g = 1$.

Шаг 2. Пока a, b — четные, будем осуществлять операции $a = \frac{a}{2}$, $b = \frac{b}{2}$, $g = 2g$. В противном случае перейдем к шагу 3.

Шаг 3. Зададим $u = a$, $b = v$.

Шаг 4. Пока $u \neq 0$, будем переходить к 4.1, в противном случае — к шагу 5.

4.1. Пока u — четное, будем осуществлять операцию $u \to \frac{u}{2}$; иначе перейдем к 4.2.

4.2. Пока v — четное, будем осуществлять операцию $v = \frac{v}{2}$; иначе перейдем к 4.3.

4.3. Если $u \geqslant v$, то осуществим операцию $u = u - v$, если $v > u$, то осуществим операцию $v = v - u$ и перейдем к шагу 4.

Шаг 5. Возьмем $d = gv$. ▷

Протокол работы алгоритма для уже знакомых нам чисел 88 и 52 представлен в нижеследующей таблице.

a	b	g	u	v	d
88	52	1			
44	26	2			
22	13	**4**	22	13	

a	b	g	u	v	d
			11	13	
			11	13-11=2	
			11	1	
			11-1=10	1	
			5	1	
			5-1=4	1	
			2	1	
			1	1	
			0	**1**	**4**

Мы видим, что при реализации бинарного алгоритма нам фактически не приходится выполнять «затратных» вычислений: используются только деления на 2, которые можно не учитывать при работе с двоичными числами, и вычитания, которые на порядок «быстрее» делений.

Сравним работу классического и бинарного алгоритмов Евклида на примере нахождения наибольшего общего делителя чисел 123 и 321. Проводимые в ходе реализации каждого из алгоритмов вычисления и время, затраченное компьютером на решение задачи, представлены в нижеследующей таблице (см. [68, с. 290]).

Алгоритм Евклида: $a = 321,\ b = 123$	Бинарный алгоритм Евклида: $a = 321,\ b = 123$
	$a = 321, b = 123, u = 321, v = 123$
$321 = 123 \cdot 2 + 75$	$u = 321 - 123 = 198,\ v = 123,$
$123 = 75 \cdot 1 + 48$	$u = 99,\ v = 123$
$75 = 48 \cdot 1 + 27$	$u = 99,\ v = 123 - 99 = 24,$
$48 = 27 \cdot 1 + 21$	$u = 99,\ v = 12$
$27 = 21 \cdot 1 + 6$	$u = 99,\ v = 6,$
$21 = 6 \cdot 3 + 3$	$u = 99,\ v = 3,$
$6 = 3 \cdot 2 + 0$	$u = 99 - 3 = 96,\ v = 3,$
$d = 3$	$u = 48,\ v = 3,$
$d = 3$	$u = 24,\ v = 3,$
	$u = 12,\ v = 3,$
	$u = 6,\ v = 3,$
	$u = 3,\ v = 3,$
	$u = 3 - 3 = 0,\ v = 3.$
4, 34 *с*	2, 25 *с*

5.2.4. Расширенный бинарный алгоритм

Для бинарного алгоритма также существует его расширенная версия, позволяющая находить одновременно и наибольший общий делитель (a, b) натуральных чисел a и b, и его линейное представление с помощью a и b.

Рассмотрим формальную *схему работы расширенного бинарного* алгоритма.

Алгоритм IV.

Дано: натуральные числа a, b, $a \geqslant b$. Найти: $d = (a, b)$ и целые x, y: $d = ax + by$.

Шаг 1. Зададим $g = 1$.

Шаг 2. Пока a, b — четные, выполним операции $a = a/2$, $b = b/2$, $g = 2g$, и перейдем к шагу 2; иначе перейдем к шагу 3.

Шаг 3. Зададим $u = a$, $v = b$, $A = 1$, $B = 0$, $C = 0$, $D = 1$ и перейдем к шагу 4.

Шаг 4. Пока $u \neq 0$, перейдем к 4.1; иначе перейдем к шагу 5.

4.1. Пока u — четное, перейдем к 4.1.1; иначе перейдем к 4.2.

4.1.1. выполним операцию $u = u/2$ и перейдем к 4.1.2;

4.1.2. если A и B — четные, то выполним операции $A = A/2$, $B = B/2$; в противном случае выполним операции $A = \dfrac{A + b}{2}$, $B = \dfrac{B - a}{2}$; перейдем к 4.1.

4.2. Пока v четное, перейдем к 4.2.1; иначе перейдем к 4.3.

4.2.1. выполним операцию $v = v/2$ и перейдем к 4.2.2;

4.2.2. если C и D — четные, то выполним операции $C = C/2$, $B = B/2$; в противном случае выполним операции $C = \dfrac{C + b}{2}$, $B = \dfrac{B - a}{2}$; перейдем к 4.3.

4.3. Если $u \geqslant v$, то выполним операции $u = u - v$, $A = A - C$, $B = B - D$, если $v > 0$, то выполним операции $v = v - u$, $C = C - A$, $D = D - B$ и перейдем к шагу 4; иначе перейдем к шагу 5.

Шаг 5. Зададим $d = gv$, $x = C$, $y = D$. ▷

Протокол работы расширенного бинарного алгоритма для $a = 88$ и $b = 52$ представлен в нижеследующей таблице.

a	b	g	u	v	A	B	C	D	d	x	y
88	52	1									
44	26	2									
22	13	**4**	22	13	1	0	0	1			
			11		7	−11					
				2			−7	12			
				1			3	-5			
			10		4	−6					
			5		2	−3					
			4		−1	2					
			2		6	−10					
			1	1	3	−5					
			0	**1**	3	-5			**4**	**3**	**−5**

Хотя теоретически быстродействие бинарных алгоритмов выше быстродейсвия классических алгоритмов, на практике бинарные алгоритмы работают быстрее обычных далеко не всегда. Вы сможете убедиться в этом и найти оптимальные условия применения того или иного алгоритма в процессе выполнения лабораторных работ.

5.2.5. Решение неопределенных уравнений первой степени

Решение неопределенных уравнений $ax + by = c$ первой степени с двумя неизвестными — пример теоретико-числовой задачи, в которой с успехом используется алгоритм Евклида.

Теория уравнений вида $ax + by = c$ очень проста: нетрудно проверить, что *уравнение* $ax + by = c$ *с целыми коэффициентами* a, b *и* c *разрешимо в целых числах если и только если* $(a, b)|c$; *в этом случае мы имеем бесконечно много решений вида*

$$x = x_0 \pm \frac{b}{(a, b)}t, \quad y = y_0 \mp \frac{a}{(a, b)}t,$$

где t *— произвольное целое число, а пара* (x_0, y_0) *— некоторое частное решение уравнения* $ax + by = c$. (Подробное доказательство этого факта можно найти, например, в [98]).

Таким образом, нахождение всех целых решений уравнения $ax + by = c$ (если они существуют) сводится к поиску его частного решения (x_0, y_0).

Пример 5.2.14 Решим уравнение

$$88x + 52y = 12.$$

Поскольку $(88, 52) = 4$ (мы убедились в этом ранее), и $4|12$, то уравнение $88x + 52y = 12$ разрешимо.

Для поиска его частного решения воспользуемся полученным ранее линейным представлением наибольшего общего делителя $(88, 52)$ чисел 88 и 52: $88 \cdot 3 + 52 \cdot (-5) = 4$. Чтобы получить в правой части число 12, умножим обе части уравнения на 3: $88 \cdot (3 \cdot 3) + 52 \cdot (-5 \cdot 3) = 12$. Теперь хорошо видно, что пара $(9, -15)$ является частным решением уравнения, и, следовательно, все его решения могут быть записаны в виде

$$x = 9 \pm \frac{52}{4}t, \quad y = -15 \mp \frac{88}{4}t,$$

где t — произвольное целое число. Другими словами, множество решений неопределенного уравнения $88x + 52y = 12$ полностью описывается парами $(9 + 13t, -15 - 22t)$, $t \in \mathbb{Z}$. □

Рассматривая пример, мы убедились в том, что алгоритм решения неопределенного уравнения $ax + by = c$ сводится к использованию расширенного алгоритма Евклида. Однако существуют и другие алгоритмы решения таких уравнений. Рассмотрим один из них, называемый *матричным*.

Алгоритм V.

Дано: неопределенное уравнение $ax + by = 1$ с целыми a и b. Найти: вектор $\begin{pmatrix} u \\ v \end{pmatrix}$ с целыми взаимно простыми a, b, такими что $au + bv = 1$.

Шаг 1. Зададим числа a, b и матрицу $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и перейдем к шагу 2.

Шаг 2. Вычислим остаток r от деления числа a на b: $a = bq + r$, $0 \leqslant r < b$, и перейдем к шагу 3.

Шаг 3. Если $r = 0$, возьмем в качестве вектора $\begin{pmatrix} u \\ v \end{pmatrix}$ второй столбец матрицы E; иначе перейдем к шагу 4.

Шаг 4. Осуществим операции

$$E \to E \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}, \quad (a, b) \to (b, r)$$

и перейдем к шагу 1. ▷

Если обозначить через E_k матрицу, возникающую в процессе работы алгоритма перед шагом 2 после k делений с остатком (шаг 1), то нетрудно убедиться, что на этом этапе алгоритма выполняется векторное равенство $(a, b) \cdot E_k = (r_{k-1}, r_k)$, где $r_0 = a$, $r_1 = b$ и $r_i = r_{i-1}q_i + r_i$, $0 < r_i < r_{i-1}$ — последовательные остатки алгоритма Евклида, примененного к числам a и b. Его легко доказать индукцией по k. Поскольку числа a и b взаимно просты, то последний ненулевой остаток равен 1. Это доказывает, что алгоритм действительно дает решение уравнения $ax + by = 1$. Количество выполняемых делений с остатком в точности соответствует количеству делений в алгоритме Евклида.

Пример 5.2.15 Решим указанным способом уравнение $88x + 52y = 12$. Прежде всего, разделив обе части уравнения на 4, перейдем к уравнению $22x + 13y = 3$. Заменим его на уравнение $22x + 13y = 1$ и применим к последнему уравнению описанный выше алгоритм.

I этап. Зададим числа $a = 88$, $b = 52$ и матрицу $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

II этап. Найдем остаток r от деления a на b: $22 = 13 \cdot 1 + 9$. Поскольку $r \neq 0$ (и $q = 1$), то заменим матрицу E матрицей

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}.$$

Заменим пару $(a, b) = (88, 52)$ парой $(b, r) = (52, 9)$.

III этап. Найдем остаток r от деления a на b: $13 = 9 \cdot 1 + 4$. Поскольку $r \neq 0$ (и $q = 1$), то заменим матрицу E матрицей

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

Заменим пару $(a, b) = (13, 9)$ парой $(b, r) = (9, 4)$.

IV этап. Найдем остаток r от деления a на b: $9 = 4 \cdot 2 + 1$. Поскольку $r \neq 0$ (и $q = 2$), то заменим матрицу E матрицей

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix}.$$

Заменим пару $(a, b) = (9, 4)$ парой $(b, r) = (4, 1)$.

V этап. Найдем остаток r от деления a на b: $4 = 1 \cdot 4 + 0$. Поскольку $r = 0$, возьмем в качестве вектора $\begin{pmatrix} u \\ v \end{pmatrix}$ второй столбец матрицы E:

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 3 \\ -5 \end{pmatrix}.$$

Таким образом, мы нашли пару $(3, -5)$ являющуюся решением уравнения $22x + 13y = 1$.

Домножая обе части равенства $22 \cdot 3 + 13 \cdot (-5) = 1$ на 3, убедимся, что пара $(9, -15)$ является решением уравнения $22x + 13y = 3$ и, следовательно, исходного уравнения $88x + 52y = 12$. Найти все решения нашего уравнения теперь не составит никакого труда. □

Легко видеть, что решение уравнения $ax + by = c$ равносильно решению сравнения первой степени $ax \equiv c \pmod{b}$: из определения отношения сравнимости следует, что $au + bv = c \Leftrightarrow au \equiv c \pmod{b}$.

Таким образом, обсуждение вопросов, связанных с алгоритмом Евклида, приводит нас к решению значимой для нашего курса задачи, связанной с исследованием сравнений или, что то же, изучением колец классов вычетов по тому или иному модулю. Алгоритм возведения в степень в кольце классов вычетов по модулю n, к обсуждению которого мы переходим, является еще одним примером такого рода [24], [29], [68], [78].

5.2.6. Алгоритм возведения в степень по модулю n

В первом разделе этой главы мы уже обсуждали алгоритм возведения натурального числа m в натуральную степень n. Несколько изменим условия задачи, договорившись рассматривать ее в кольце классов вычетов по модулю n, то есть будем искать вычет числа a^d, $a, d \in \mathbb{N}$, по модулю n.

На предварительном этапе работы запишем показатель d в двоичной системе счисления:

$$d = d_r + d_{r-1}2 + d_{r-2}2^2 + \ldots + d_1 2^{r-1} + d_0 2^r,$$

где $d_i \in \{0, 1\}, d_0 = 1$. (Заметим, что для удобства вычислений мы используем «встречную» нумерацию индексов).

Теперь, чтобы найти $a^d \bmod n$, достаточно построить последовательность чисел $a_0 = a$, $a_i \equiv a_{i-1}^2 \cdot a^{d_i} \pmod{n}$, $i = 1, 2, \ldots r$, и убедиться в том, что a_r — искомый вычет $a^d \pmod{n}$.

Действительно, поскольку $a_0 = a$, то

$$a_1 = a_0^2 \cdot a^{d_1} = a^{2+d_1} \pmod n,$$

$$a_2 = a_1^2 \cdot a^{d_2} = a^{2(2+d_1)+d_2} = a^{d_2+2d_1+2^2} \pmod n,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_i = a_{i-1}^2 \cdot a^{d_i} = a^{d_i+\ldots+d_0 2^i} \pmod n,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_r = a_{r-1}^2 \cdot a^{d_r} = a^{d_r+d_{r-1}2+d_{r-2}2^2+\ldots+d_1 2^{r-1}+d_0 2^r} \equiv a^d \pmod n,$$

то есть $a_r \equiv a^d \pmod n$.

Пример 5.2.16 Вычислим $7^{29} \bmod 31$. Прежде всего, запишем число 29 в системе счисления с основанием 2: $29 = 2^4 + 2^3 + 2^2 + 1 = 11101_2$. Таким образом, мы определили числа d_0, d_1, d_2, d_3 и d_4; их значения указаны в нижеследующей таблице.

d_0	d_1	d_2	d_3	d_4
1	1	1	0	1

Взяв $a_0 = 7$, вычислим a_i для $i = 1, 2, 3, 4$, параллельно проводя подсчет числа используемых при вычислениях арифметических операций:

$a_1 = 7^2 \cdot 7^{d_1} = 7^2 \cdot 7^1 = 49 \cdot 7 \equiv 18 \cdot 7 \equiv 2 \pmod{31}$ – 2 умножения;

$a_2 = 2^2 \cdot 7^{d_2} = 4 \cdot 7^1 \equiv 28 \pmod{31}$ – 2 умножения;

$a_3 = 28^2 \cdot 7^{d_3} = (-3)^2 \cdot 7^0 = 9 \pmod{31}$ – 1 умножение;

$a_4 = 9^2 \cdot 7^{d_4} = 81 \cdot 7^1 \equiv 19 \cdot 7 \equiv 9 \pmod{31}$ – 2 умножения;

таким образом, за 4 шага и 7 умножений мы получили окончательный результат: $7^{29} \equiv 9 \pmod{31}$. □

Рассмотрим формальную *схему алгоритма возведения в степень по модулю* n.

Алгоритм VI.

Дано: натуральное число n; натуральные числа a, d: $a, d \leqslant n$. Найти: натуральное число x: $x \equiv a^d \pmod n$.

Шаг 1. Зададим $a_0 = a$, $i = 1$ и перейдем к шагу 2.

Шаг 2. Если $i < r$, то вычислим $a_i \equiv a_0 \cdot a^{d_i} \pmod n$, где d_i — соответствующая цифра в двоичной записи числа d, осуществим операцию $i \to i + 1$ и перейдем к шагу 2; иначе перейдем к шагу 3.

Шаг 3. Зададим $x = a_i$. ▷

Протокол возведения в степень по модулю n для чисел $a = 7$, $d = 29$ и $n = 31$ представлен в нижеследующей таблице.

i	0	1	2	3	4
d_i	1	1	1	0	1
a_i	7	2	28	9	9

Оценка трудоемкости алгоритма возведения в степень по модулю n не составляет труда: в ходе алгоритма реализуется r шагов, где r — количество знаков в двоичной записи числа d. Поскольку $d < n$, то $r = O(\log n)$. Каждый шаг использует не более двух умножений, и, поскольку $a < n$, то каждое умножение требует не более $O(\log^2 n)$ двоичных операций. Таким образом, общее число двоичных операций при возвышении в степень есть $O(2 \log n \cdot \log^2 n) = O(\log^3 n)$, и мы доказали, что *число двоичных операций, необходимых для возведения натурального числа a в натуральную степень d по модулю n есть* $O(\log^3 n)$:

$$Time\begin{pmatrix}\text{возведение натурального числа } a \\ \text{в натуральную степень } d \text{ по модулю } n\end{pmatrix} = O(\log^3 n).$$

Приведенные выше алгоритмы относятся к разряду полиномиальных алгоритмов, поскольку сложность каждого из них оценивается сверху степенным образом в зависимости от длины записи входящих чисел. Если наибольшее из чисел, подаваемых на вход алгоритма, не превосходит n, то сложность алгоритмов этого типа оценивается сверху величиной $O(\log^c n)$, где c — некоторая положительная константа.

На самом деле полиномиальные алгоритмы в теории чисел — большая редкость. Большинство хорошо известных нам теоретико-числовых процедур полиномиальными алгоритмами не являются. Рассмотрим, например, вычисление факториала $n!$ натурального числа n и найдем верхнюю границу для числа двоичных операций, необходимых для этого.

Для вычисления $n!$ поступим стандартным образом: сначала умножим 2 на 3, затем результат умножим на 4, новый результат умножим на 5 и т. д., пока не получим $n!$. В этом случае на $(j-1)$-м шаге $(j = 2, 3, \ldots n-1)$ производится умножение $j!$ на $j+1$. Поэтому алгоритм состоит из $n-2$ шагов, каждый из которых реализует умножение частичного произведения $j!$ на очередное натуральное число. Частичные произведения быстро станут очень большими. В качестве оценки для числа разрядов частичного произведения в наихудшем случае возьмем число разрядов последнего произведения, т. е. числа $n!$. При определении числа двоичных разрядов в произведении будем использовать очевидную оценку:

это число не превосходит суммы числа разрядов сомножителей, в частности, произведение n натуральных k-разрядных чисел имеет не более $n \cdot k$ разрядов. Таким образом, если n — двоичное k-разрядное число, то $n!$ имеет самое большее $n \cdot k$ разрядов. Подведем итоги: в каждом из $n-2$ умножений, необходимых при вычислении $n!$, мы умножаем не более чем k-разрядное целое число $j+1$ на не более чем nk-разрядное число $j!$. Это требует не более $n \cdot k^2$ двоичных операций; так как алгоритм осуществляет $n-2$ таких умножений, то общее число двоичных операций при вычислении $n!$ ограничено сверху величиной $(n-2) \cdot n \cdot k^2$, или, что то же, величиной $O((n \log n)^2)$. Мы доказали, что *число двоичных операций, необходимых для вычисления факториала* $n!$ *натурального числа* n, *есть* $O(n^2 \log^2) n$:

$$Time(\text{вычисление } n!) = O(n^2 \log^2 n).$$

Таким образом, уже достаточно простой в реализации и часто используемый на практике алгоритм вычисления факториала натурального числа является экспоненциальным.

Упражнения

(1) Найдите (a, b), используя определение, разложение чисел на множители и алгоритм Евклида; сравните трудоемкость этих способов:

a) $a = 14$, $b = 98$;
b) $a = 112$, $b = 124$;
c) $a = 343$, $b = 258$;
d) $a = 204$, $b = 527$;
e) $a = 351$, $b = 312$;
f) $a = 781$, $b = 1408$;
g) $a = 1029$, $b = 483$;
h) $a = 1581$, $b = 1851$;
i) $a = 1728$, $b = 1536$;
j) $a = 1319$, $b = 1391$;
k) $a = 4303$, $b = 2873$;
l) $a = 4087$, $b = 3953$.

(2) Пользуясь алгоритмом Евклида, найдите наибольший общий делитель d чисел a и b и укажите два целых числа x_0, y_0, таких что $d = a \cdot x_0 + b \cdot y_0$; подсчитайте количество выполненных при решении каждой задачи операций:

a) $a = 137$, $b = -31$;
b) $a = 103$, $b = 189$;
c) $a = 41$, $b = 47$;
d) $a = 213$, $b = -321$;
e) $a = -56$, $b = 44$;
f) $a = 162$, $b = 99$.

(3) Пользуясь алгоритмом Евклида, найдите хотя бы одно целое решение уравнения

a) $26x + 91y = 11$;
b) $33x + 51y = 21$;
c) $73x + 85y = 7$;
d) $44x + 187y = 22$;
e) $311x - 28y = 2$;
f) $253x - 449y = 3$.

④ Пользуясь алгоритмом Евклида и бинарным алгоритмом Евклида, найдите:

a) (1234, 5678); d) (2747, 3149); g) (−1256, −8844);
b) (−765, −432); e) (1219, 1357); h) (7711, 1122).
c) (111, 3333); f) (−667, 580);

⑤ Найдите (n, m), используя каноническое разложение чисел n и m, алгоритм Евклида и бинарный алгоритм Евклида, и сравните использованные алгоритмы по трудоемкости:

a) $n = 12345$, $m = 24690$; d) $n = 12345$, $m = 13991$;
b) $n = 12345$, $m = 54321$; e) $n = 12345$, $m = 18030$;
c) $n = 12345$, $m = 12541$; f) $n = 12345$, $m = 28805$.

⑥ Используя расширенный алгоритм Евклида и расширенный бинарный алгоритм Евклида, найдите представление наибольшего общего делителя (n, m) чисел n и m в виде целочисленной линейной комбинации n и m; сравните процедуры по их трудоемкости:

a) $n = 12345$, $m = 24690$; d) $n = 12345$, $m = 13991$;
b) $n = 12345$, $m = 54321$; e) $n = 12345$, $m = 18030$;
c) $n = 12345$, $m = 12541$; f) $n = 12345$, $m = 28805$.

⑦ Решите неопределенное уравнение $ax + by = c$ с помощью расширенного алгоритма Евклида, бинарного расширенного алгоритма и «матричного» алгоритма:

a) $a = 24$, $b = 65$, $c = 11$; d) $a = 36$, $b = 81$, $c =; 27$
b) $a = 34$, $b = 85$, $c = 51$; e) $n = 37$, $b = 41$, $c = 43$;
c) $a = 35$, $m = 98$, $c = 14$; f) $n = 40$, $b = 42$, $c = 46$.

⑧ Вычислите степень a^d по модулю n классическим способом и с помощью алгоритма возведения в степень; сравните трудоемкость двух методов:

a) $n = 67$, $a = 246$, $d = 90$; d) $n = 78$, $a = 13$, $d = 100$;
b) $n = 45$, $a = 5$, $d = 43$; e) $n = 67$, $a = 246$, $d = 90$;
c) $n = 234$, $a = 45$, $d = 41$; f) $n = 67$, $a = 246$, $d = 90$.

⑨ Вычислите $n!$ для $n = 3, 4, 5, 6, 7, 8$. Оцените число выполненных операций.

Задачи

1 Докажите перечисленные выше свойства наибольшего общего делителя.

2 Докажите *критерий взаимной простоты*: целые числа a и b являются взаимно простыми тогда и только тогда, когда существуют целые числа x и y, такие что $ax + by = 1$.

3 Докажите, что наибольший общий делитель (a, b) делит наименьшее общее кратное $[a, b]$.

4 Докажите, что $(a, b) \cdot [a, b] = ab$, если a и b — натуральные числа.

5 Пусть $u_1 = 1, u_2 = 1$ и $u_{k+2} = u_k + u_{k-1}$ — *числа Фибоначчи*. Найдите (u_{n+10}, u_n) при $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. Подсчитайте число выполненных операций. Убедитесь, что $(u_n, u_m) = u_{(n,m)}$. Докажите это соотношение.

6 Докажите *теорему Ламе*: для натуральных чисел a и b, $a > b$, число делений алгоритма Евклида, используемого для нахождения (a, b), не превосходит $5k$, где k — число цифр в десятичной записи числа b.

7 При любом натуральном n найдите наибольший общий делитель чисел:

a) $n^2 + 1$ и $n^3 + 2n^2 + 2n + 1$;

b) $n^3 + 3n^2 + 6n + 2$ и $n^2 + 3n + 5$;

c) $n^4 + 2n^3 + 2n^2 + 3n + 1$ и $n^3 + 2n^2 + 2n + 2$.

8 При любом натуральном n найдите наибольший общий делитель чисел:

a) 4 и $2n + 1$;

b) 3 и $3n + 2$;

c) 25 и $5n + 4$;

d) 10 и $n^6 - n^2 + 1$.

9 Сократите дробь:

a) $\dfrac{6n + 4}{22n + 15}$; b) $\dfrac{16n + 60}{11n + 41}$; c) $\dfrac{6n + 5}{3n + 2}$; d) $\dfrac{21n + 4}{14n + 3}$.

10 Зная, что $(a, b) = 1$, вычислите:

a) $(3b + 5a, b + 2a)$; c) $(5b + 3a, 3b + 2a)$; e) $(9b + 6a, b + a)$;

b) $(3b + 5a, 2b + 3a)$; d) $(7b + 6a, 4b + 3a)$; f) $(9b + 6a, 4b + 3a)$.

11 Докажите, что для любого натурального n уравнение $ax + by = n$ разрешимо в натуральных числах:

a) $a = 7$, $b = 10$;

b) $a = 101$, $b = 89$;

c) $a = 127$, $b = -49$;

d) $a = n^2 + 1$, $b = n^3 + n^2 - 1$;

e) $a = 2n^2 - 4$, $b = n^4 - n^2 + 1$;

f) $a = n + 1$, $b = 7n + 8$.

12 Решите неопределенные уравнения первой степени, используя расширенные алгоритмы Евклида (обычный и бинарный), а также матричный алгоритм; сравните их трудоемкость:

a) $180x + 264y = 2304$;
b) $425x - 238y = 4012$;
c) $140x + 290y = 2380$;
d) $140x - 190y = 2460$;
e) $324x + 336y = 3444$;
f) $225x + 285y = 2385$;
g) $361x - 475y = 5358$;
h) $143x + 299y = 2574$;
i) $275x - 121y = 2959$.

13 Применяя алгоритм Евклида для многочленов, вычислите $(f(x), g(x))$:

a) $f(x) = x^5 + 3x^4 + 3x^3 + 2x^2$, $g(x) = x^4 + 2x^3 + 2x^2 + x$;
b) $f(x) = x^5 + x^3 + 2x^2 + 5$, $g(x) = x^3 + 2x^2 + 2$;
c) $f(x) = x^4 + x^3 + x^2 + x$, $g(x) = x^2 + x + 1$;
d) $f(x) = 2x^4 + 4x^2 + 9$, $g(x) = x^3 + x^2 + 2$.

14 Найдите наименьший неотрицательный вычет x:

a) $x \equiv 38^{30} \cdot 20^{23} \cdot 17^{31} \pmod{215}$;
b) $x \equiv 38^{30} \cdot 2^{22} \cdot 18^{31} \pmod{215}$.

Литература к главе 5

При подготовке текста главы 5 были использованы следующие источники [13], [20], [22], [24], [29], [33], [34], [36], [38], [50], [51], [53], [55], [68], [74], [78], [88], [98], [104], [108].

Глава 6

Простые и псевдопростые числа

6.1. Простые числа. Критерии простоты

Натуральное число p называется *простым*, если оно имеет ровно два натуральных делителя: 1 и p.

Множество простых чисел обозначают символом P. Таким образом, $P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\}$.

Натуральное число n называется *составным*, если оно имеет более двух натуральных делителей. Множество составных чисел обозначают символом S. Таким образом, $S = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \ldots\}$.

Пример 6.1.1 Так, натуральное число 12345 — составное, поскольку делится на 5, и, следовательно, обладает по крайней мере тремя натуральными делителями 1, 5 и 12345. С другой стороны, непосредственным перебором можно убедиться в том, что число 127 не делится ни на одно натуральное число, кроме 1 и 127, то есть является простым. □

Поскольку каждое натуральное число делится на 1 и само на себя, то любое натуральное число либо простое, либо составное, либо равно 1 (число 1 обладает ровно одним натуральным делителем; оно не является ни простым, ни составным). Следовательно, $\mathbb{N} = P \cup S \cup \{1\}$.

Простые числа играют исключительно важную роль в математике. Так, нетрудно убедиться в том, что *любое натуральное число* n, *большее* 1, *имеет простой делитель*. (Для доказательства этого факта достаточно рассмотреть наименьший натуральный делитель n, отличный от 1; см., например, [98]). Более того, *фундаментальная теорема арифметики* утверждает что *любое натуральное число*, *большее* 1, *можно*, *причем единственным образом* (*с точностью до порядка сомножителей*), *представить в виде произведения простых чисел*.

Таким образом, любое натуральное число n, большее единицы, единственным образом представимо в виде произведения натуральных степеней различных простых чисел $p_1, \ldots p_s$: $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Такое разложение называется *каноническим представлением* n.

Для получения канонического разложения можно найти все простые делители числа n непосредственным перебором, однако значительно удобнее воспользоваться *алгоритмом последовательного деления*, который основывается на следующем утверждении: *если n является составным числом, то оно имеет простой делитель $p \leqslant \sqrt{n}$.*

Доказательство этого факта несложно. Действительно, составное n обладает нетривиальным натуральным делителем $a \notin \{1, n\}$, то есть представимо в виде $n = a \cdot b$, $1 < a \leqslant b < n$. При этом $a \leqslant \sqrt{n}$, так как в противном случае мы получаем противоречие: поскольку $a > \sqrt{n}$ и $b \geqslant a$, то $b > \sqrt{n}$, откуда следует, что $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, то есть $n > n$. Поскольку a — натуральное число, большее единицы, то оно обладает простым делителем p. При этом, с одной стороны, делитель p числа a является делителем n, и, с другой стороны, $p \leqslant a \leqslant \sqrt{n}$. Таким образом, мы нашли для составного числа n его простой делитель p, удовлетворяющий условию $p \leqslant \sqrt{n}$.

Пример 6.1.2 Воспользуемся алгоритмом последовательного деления для разложения на простые множители числа 495.

Для этого проверим делимость данного числа на простые числа, не превосходящие $\sqrt{495}$: 2, 3, 5, 7, 11, 13, 17 и 19. Легко видеть, что число 495 не делится на 2, но делится на 3: $495 = 3 \cdot 165$. Далее, число 165 делится на 3: $165 = 3 \cdot 55$. В свою очередь, число 55 делится на 5: $55 = 5 \cdot 11$. Таким образом, мы получили разложение числа 495 на простые множители: $495 = 3^2 \cdot 5 \cdot 11$. □

Поскольку простые числа образуют мультипликативный базис множества натуральных чисел, возникает потребность исследования всего многообразия их свойств [98], [36], [48], [43], [92], [93], [123].

Например, для решения прикладных задач бывает очень удобным использовать специфику представления простых чисел по тем или иным составным модулям.

Пример 6.1.3 Докажем, что *любое простое число либо равно* 2, *либо равно* 3, *либо имеет вид* $6k + 1$, $k \in \mathbb{N}$, *либо имеет вид* $6q - 1$, $q \in \mathbb{N}$. Для этого воспользуемся теоремой о делении с остатком. Деля простое число p с остатком на 6, получим равенство $p = 6k + r$, $0 \leqslant r < 6$. Таким образом, $r \in \{0, 1, 2, 3, 4, 5\}$.

Если $r = 0$, то $p = 6k$, и, следовательно, p делится на 2 и на 3, что дает противоречие с определением простого числа. Аналогичная ситуация возникает и при $r = 4$. Если $r = 2$, то $p = 6k + 2$, и, следовательно, p делится на 2. Это возможно только в случае $p = 2$. Аналогичная ситуация возникает и при $r = 3$.

Остаются случаи $r = 1$, то есть $p = 6k+1$ (здесь k — число натуральное в силу того, что $p > 1$), и $r = 5$, то есть $p = 6k + 5$ или, что то же, $p = 6(k + 1) - 1$ (здесь $k + 1$ — число натуральное в силу того, что $p > 1$).

Таким образом, мы доказали, что любое простое число p либо 2, либо 3, либо представимо в виде $6q \pm 1$, $q \in \mathbb{N}$. □

Этот факт часто используется при решении различных арифметических и теоретико-числовых задач.

Пример 6.1.4 Найдем все $p \in P$, для которых $p + 10, p + 14 \in P$.

Как было показано в ходе решения предыдущей задачи, любое простое число либо равно 2, либо равно 3, либо имеет вид $6k + 1$, $k \in \mathbb{N}$, либо имеет вид $6q - 1$, $q \in \mathbb{N}$. Если $p = 2$, то $p + 10 = 12$, то есть $p + 10 \notin P$. Если $p = 3$, то $p + 10 = 13$, и $p + 14 = 17$, то есть $p + 10, p + 14 \in P$. Если $p = 6k + 1, k \in \mathbb{Z}$, то $p + 14 = 6k + 15$, или, что то же, $p + 14 = 6(k + 2) + 3$, то есть $p + 14$ делится на 3 и не равно 3, а, следовательно, является составным числом: $p + 14 \notin P$. Наконец, если $p = 6q - 1, q \in \mathbb{Z}$, то $p + 10 = 6q + 9$, или, что то же, $p + 10 = 6(k + 1) + 3$, то есть $p + 10$ делится на 3 и не равно 3, а, следовательно, является составным числом: $p + 10 \notin P$. Таким образом, числа $p, p + 10$ и $p + 14$ являются простыми одновременно только при $p = 3$. □

Около двух тысяч лет назад Евклид доказал, что *множество простых чисел бесконечно.*

Рассмотрим доказательство Евклида. Предположим, что множество P простых чисел конечно, и $p_1, \ldots p_k$ — все простые числа. Пусть $E = p_1 \cdot \ldots \cdot p_k + 1$, и пусть p — простое число, делящее E. Тогда p не может совпадать ни с одним из чисел $p_1, \ldots p_k$, иначе p должно делить разность $E - p_1 \cdot \ldots \cdot p_k = 1$, что невозможно. Таким образом, p — простое число, не попавшее в список, то есть числа $p_1, \ldots p_k$ не могут давать всех простых чисел.

Идея, лежащая в основе доказательства Евклида, часто применяется при исследовании вопросов конечности или бесконечности тех или иных числовых множеств, а числа вида $p_1 \cdot \ldots \cdot p_k + 1$, где $p_1 = 2, p_2 = 3, \ldots$ — последовательные простые числа, называются *евклидовыми.*

Пример 6.1.5 Используя идеи Евклида, докажем, что существует бесконечно много простых чисел вида $6k - 1$, $k \in \mathbb{N}$.

Предположим, что множество простых чисел вида $6k - 1$ конечно, и что $P_{6k-1} = \{p_1, p_2, \ldots p_k\}$ — все простые числа указанного вида. Построим натуральное число $E = 6p_1 \cdot p_2 \cdot \ldots \cdot p_k - 1$. Оно обладает простым делителем p, которое не может быть равно ни 2, ни 3 и, следовательно, должно иметь вид $6q \pm 1$. Однако любое произведение простых вида $6q + 1$

само имеет вид $6q + 1$. Следовательно, наше число обладает простым делителем p вида $6k - 1$. Легко видеть, что число p не может совпадать ни с одним из чисел $p_1, p_2, \ldots p_k$, так как иначе p делит $6p_1 \cdot p_2 \cdot \ldots \cdot p_k$, и, как следствие, должно делить разность $E - 6p_1 \cdot p_2 \cdot \ldots \cdot p_k = 1$, что невозможно. Таким образом, p — простое число вида $6k - 1$, не попавшее в вышеприведенный список, то есть множество простых чисел вида $6k - 1$ не может исчерпываться числами $p_1, p_2, \ldots p_k$. □

В контексте вопросов, обсуждаемых в пособии, наиболее важными для нас являются вопросы получения новых простых чисел, отвечающих потребностям практических (в частности, криптографических) задач, в первую очередь — алгоритмы проверки натуральных чисел на простоту.

Простейший метод нахождения всех простых чисел на данном интервале был предложен греческим математиком Эратосфеном. Он называется *решетом Эратосфена* и состоит в следующем. Рассмотрим последовательность 2, 3, 4, 5, ... натуральных чисел, больших единицы. Так как 2 является первым простым числом p_1, вычеркнем из нашей последовательности все числа, большие p_1 и делящиеся на p_1, то есть, начиная с 2, каждое второе число таблицы — заведомо составное. Первое из оставшихся чисел 3 — второе простое число p_2. Вычеркнем все числа, большие p_2 и делящиеся на p_2, то есть, начиная с 3, каждое третье число таблицы. Первое из оставшихся чисел 5 — третье простое число p_3 и т. д. Следуя указанной схеме, мы получаем $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ..., $p_{1000} = 7917$, ..., $p_{6000000} = 104395301$, ... Здесь символ p_n обозначает n-е простое число.

Пример 6.1.6 Для нахождения всех простых чисел на отрезке $[10, 200]$, выпишем все простые, не превосходящие $\lfloor\sqrt{200}\rfloor = 14$: 2, 3, 5, 7, 11, 13. Вычеркнем из таблицы

11 12 13 14 15 16 17 18 19 20

...

101 102 103 104 105 106 107 108 109 110

...

191 192 193 194 195 196 197 198 199 200

каждое второе число, начиная с первого делящегося на 2 числа 12; каждое третье число, начиная с первого делящегося на 3 числа 12; каждое пятое число, начиная с первого делящегося на 5 числа 15; каждое седьмое число, начиная с первого делящегося на 7 числа 21; каждое одиннадцатое число, начиная с 11, оставляя невычеркнутым само (простое) число 11; каждое тринадцатое число, начиная с 13, оставляя невычеркнутым само (простое)

число 13. Нетрудно видеть, что каждое вычеркнутое число было составным, а оставшиеся после проведения этой процедуры невычеркнутыми числа 11, 13, 17, ..., 197, 199 — простые. □

Алгоритм решета Эратосфена прост и понятен, однако крайне трудоемок даже при относительно небольших границах исследуемого промежутка и часто «избыточен»: при решении большинства задач требуется лишь определить, является ли данное натуральное число простым.

Для ответа на этот вопрос часто бывает легче доказать, что исследуемое число — составное. Иногда для этого достаточно использовать известные признаки делимости, в других случаях может помочь замеченное исследователем разложение имеющегося числа на нетривиальные множители.

Пример 6.1.7 Проверим на простоту числа 111111111111 и $32^n+1, n \in \mathbb{N}$.

Исследуя *репьюинт* 111111111111, заметим, что сумма его цифр делится на 3 и, следовательно, число $111111111111 \in S$.

Докажем, что для любого натурального n число $32^n + 1$ также является составным. Поскольку для любых целых чисел a и b и для любого нечетного натурального числа n имеет место тождество

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1}),$$

то $32^n + 1 = (2^n)^5 + 1 = (2^n + 1) \cdot (2^{4n} - 2^{3n} + 2^{2n} - 2^n + 1)$, или, что то же, $32^n + 1 = (2^n + 1)L$, где $L \in \mathbb{N}$. Следовательно, число $32^n + 1$ делится на 2^n+1 для любого натурального n. При этом натуральное число 2^n+1 является нетривиальным делителем большего единицы натурального числа $32^n + 1$, поскольку $2^n + 1 \neq 1$ и $2^n + 1 \neq 32^n + 1$. Таким образом, для любого натурального n число $32^n + 1$ является составным.

Классический тест *последовательного деления* основывается на уже рассмотренном нами утверждении о наличии или отсутствии у числа n простого делителя, меньшего $\sqrt{n}$: *натуральное число n, большее 1, является простым числом тогда и только тогда, когда у него нет простых делителей, не превосходящих $\sqrt{n}$.* □

Пример 6.1.8 Проверим на простоту число 101. Для этого проверим делимость данного числа на простые числа, не превосходящие $\sqrt{101}$: 2, 3, 5 и 7. Легко видеть, что число 101 не делится ни на одно из указанных простых чисел, то есть само является простым. □

Этот тест повсеместно применяется для проверки простоты небольших натуральных чисел, однако с ростом n объем необходимых для его проведения операций очень быстро возрастает.

Конечно, в теории чисел можно найти много других критериев простоты, которые имеют несомненную теоретическую и занимательную ценность.

Так, хорошо известным критерием простоты данного натурального числа является теорема Вильсона: *натуральное число p является простым тогда и только тогда, когда* $(p-1)! \equiv -1 \pmod{p}$ [37].

К сожалению, на практике теорема Вильсона не может быть использована как тест простоты, так как вычисление $(n-1)!$ при больших n — очень долгий процесс.

Еще одним красивым, но бесполезным на практике критерием простоты является следующее утверждение: *натуральное число p является простым тогда и только тогда, когда*

$$\sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor - \left\lfloor \frac{n-1}{m} \right\rfloor = 2.$$

Значительно более полезен с практической точки зрения следующий критерий простоты: *нечетное натуральное число p является простым тогда и только тогда, когда p представимо в виде разности квадратов двух натуральных чисел единственным образом.* Родственные ему тесты простоты, основанные на теории квадратичных форм, хорошо известны в теории чисел.

Еще один представляющий практический интерес критерий простоты связан с теорией показателей: *натуральное число n является простым тогда и только тогда, когда для некоторого $1 < a < n$ имеет место сравнение* $a^{n-1} \equiv 1 \pmod{n}$, *причем* $a^{\gamma} \not\equiv 1 \pmod{n}$ *для всех натуральных* $\gamma | (n-1)$. В вычислительной теории чисел этот тест называется *тестом Люка—Лемера*; для его практического использования необходимо знать все простые делители числа $n-1$. Мы вернемся к обсуждению подобных вопросов несколько позже.

Упражнения

(1) Разложите на простые множители числа:

a) 5472; c) 8250; e) 14125; g) 25750;
b) 6624; d) 8775; f) 19392; h) 34800.

(2) Докажите, что $61! + 1$ имеет простой делитель $p > 66$.

(3) Докажите, что если простое число p является делителем числа $100! + 101$, то $p \geqslant 103$.

(4) Докажите, что если p — нечетное простое число, то оно имеет вид $4k-1$ или $4k+1$, $k \in \mathbb{N}$.

(5) Докажите, что всякое простое число p, не равное 2 и 5, представимо в виде $10k \pm 1$ или $10k \pm 3$, $k \in \mathbb{N}$.

⑥ На какую цифру не может оканчиваться простое число в десятичной системе счисления?

⑦ Докажите, что всякое простое число, большее трех, представимо в виде $12k \pm 1$, $k \in \mathbb{N}$ или $12t \pm 5$, $t \in \mathbb{N}$.

⑧ Найдите все тройки $p, p+2, p+4$ последовательных нечетных простых чисел.

⑨ Существуют ли четверки $p, p+2, p+4, p+6$ последовательных нечетных простых чисел?

⑩ Найдите все $p \in P$, для которых $p + 5, p + 11 \in P$.

⑪ Найдите все $p \in P$, для которых $p^4 + 15 \in P$.

⑫ Найдите все простые p, для которых $7p^2 + 8$ — простое число.

⑬ Для каких простых p число $p + 4$ является квадратом целого числа?

⑭ Найдите все простые числа p, для которых $2p + 1$ является кубом целого числа.

⑮ Докажите, что если p и $2p - 1$ — простые числа, большие трех, то $p - 1$ делится на 6.

⑯ Найдите все числа p, для которых каждое из шести чисел p, $p + 2$, $p + 6$, $p + 8$, $p + 12$, $p + 14$ является простым.

⑰ Докажите, что любое натуральное число вида $4k - 1$, $k \in \mathbb{Z}$, имеет простой делитель того же вида. Верно ли аналогичное утверждение для целых чисел вида $4k + 1$, $k \in \mathbb{Z}$?

⑱ Докажите, что любое натуральное число вида $6k - 1$, $k \in \mathbb{Z}$, имеет простой делитель того же вида. Верно ли аналогичное утверждение для натуральных чисел вида $6k + 1$, $k \in \mathbb{Z}$?

⑲ Докажите, что существует бесконечно много простых чисел вида $4k - 1$, $k \in \mathbb{N}$.

⑳ Докажите, что для данного $n \geqslant 3$ между n и $n!$ существует по крайней мере одно простое число; докажите бесконечность множества простых, пользуясь этим соображением.

㉑ Составьте таблицу простых чисел p:

a) $100 \leqslant p \leqslant 200$;
b) $400 \leqslant p \leqslant 500$;
c) $400 \leqslant p \leqslant 500$;
d) $450 \leqslant p \leqslant 600$.

㉒ Найдите все натуральные n, для которых $8^n - 1$ — простое число.

㉓ Докажите, что сумма квадратов трех простых чисел, больших трех, есть число составное.

(24) Докажите, что сумма квадратов двух нечетных простых чисел есть число составное.

(25) Докажите, что сумма квадратов четырех нечетных простых чисел есть число составное.

(26) Может ли быть простым числом сумма трех последовательных целых чисел; сумма четырех последовательных целых чисел; сумма пяти последовательных целых чисел; сумма шести последовательных целых чисел; сумма семи последовательных целых чисел?

(27) Может ли сумма k последовательных нечетных чисел быть простым числом?

(28) При каких натуральных n число $n^4 + 4$ является простым числом?

(29) Найдите все натуральные n, для которых:

a) $3^n - 1 \in P$; b) $6^n - 1 \in P$; c) $12^n - 1 \in P$; d) $18^n - 1 \in P$.

(30) При каких натуральных n число $n^4 + n^2 + 1$ является простым?

(31) При каких натуральных n число $n^4 + 64$ является составным?

(32) Найдите все натуральные a и n, для которых $n^4 + 4a^4$ — составное число.

(33) Найдите все натуральные n, для которых $2^{2n} - 1$ — простое число.

(34) Проверьте число n на простоту, пользуясь алгоритмом последовательного деления:

a) $n = 89$; b) $n = 97$; c) $n = 131$; d) $n = 149$.

(35) Пользуясь критерием Вильсона, протестируйте на простоту первые двадцать натуральных чисел. Оцените число выполненных операций. Сравните трудоемкость критерия Вильсона с другими известными вам методами проверки простоты.

Задачи

[1] Если числа p и $p + 2$ являются одновременно простыми, то пара $\langle p, p + 2\rangle$ называется парой *простых-близнецов*. Укажите все пары $\langle p, p + 2\rangle$ простых-близнецов, для которых:

a) $p \leqslant 100$; c) $100 \leqslant p \leqslant 150$;

b) $100 \leqslant p \leqslant 150$; d) $200 \leqslant p \leqslant 250$.

[2] Какой остаток от деления на 12 дает сумма двух простых-близнецов, если меньшее из них больше 3?

3 Пусть $\langle p, q\rangle$ — пара простых-близнецов. Докажите, что либо $6|(q-1)$, либо $\langle p, q\rangle = \langle 3, 5\rangle$.

4 Найдите все пары простых-близнецов, в которых одно из чисел есть *число Мерсенна* $M_n = 2^n - 1$, $n \in \mathbb{N}$, а второе — *число Ферма* $F_n = 2^{2^n} + 1$, $n \in \mathbb{N} \cup \{0\}$.

5 Докажите, что $p_n \leqslant 2^{2^{n-1}}$ для любого натурального n, где p_n — **n-е** простое число.

6 Докажите, что $p_n \leqslant 2^{2^{n-2}}$ для $n > 1$.

7 Докажите, что разложение натурального числа n в произведение простых чисел содержит не более $\log_2 n$ множителей.

8 Пусть n — нечетное натуральное число. Докажите, что в разложении n на простые множители не более $\log_3 n$ множителей.

9 Докажите, что $p_n \leqslant 2^n$, где p_n — n-е простое число.

10 Докажите, что для любого натурального n число $(n+1)! + 2$ является составным.

11 Докажите, что в натуральном ряду существуют сколь угодно длинные промежутки, не содержащие простых чисел.

12 Докажите *теорему Вильсона*: *натуральное число p является простым тогда и только тогда, когда*

$$(p-1)! \equiv -1 \pmod{p}.$$

13 Докажите *теорему Лейбница*: *натуральное число p является простым тогда и только тогда, когда*

$$(p-2)! \equiv 1 \pmod{p}.$$

14 Докажите обобщение теоремы Вильсона, полученное Гауссом:

$$\prod_{1 \leqslant a < m, gcd(a,m)=1} a \equiv -1 \pmod{m}$$

для $m = 4, p^\alpha, 2p^\alpha$, *и*

$$\prod_{1 \leqslant a < m, gcd(a,m)=1} a \equiv 1 \pmod{m}$$

в остальных случаях, где p — нечетное простое число.

15 Докажите, что натуральное число $n \equiv 1 \pmod 4$ является простым тогда и только тогда, когда n может быть представлено в виде суммы квадратов двух натуральных чисел x, y единственным образом, причем это представление является *собственным*: $(x, y) = 1$.

16 Докажите, что $n \in P$ тогда и только тогда, когда

$$\sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor - \left\lfloor \frac{n-1}{m} \right\rfloor = 2.$$

17 Протестируйте на простоту первые тридцать натуральных чисел, пользуясь следующим критерием: *натуральное число p является простым тогда и только тогда, когда* $\sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor - \left\lfloor \frac{n-1}{m} \right\rfloor = 2$. Проведите анализ трудоемкости использованного алгоритма.

18 Убедитесь, что каждое нечетное натуральное число n, $1 < n < 30$, представимо в виде разности квадратов натуральных чисел. Для каждого нечетного натурального числа n, $1 < n < 30$, найдите все такие представления. Убедитесь, что каждое составное число, меньшее 30, обладает по крайней мере двумя такими представлениями. Что можно сказать о простых числах, меньших 30? Используйте для тестирования на простоту чисел 31, 33, 35, 37, 39 следующий критерий простоты: нечетное натуральное число p является простым тогда и только тогда, когда p представимо в виде разности квадратов двух натуральных чисел единственным образом.

19 Используйте для тестирования на простоту первых 30 натуральных чисел критерий Люка—Лемера: натуральное число n является простым тогда и только тогда, когда для некоторого $1 < a < n$ имеет место сравнение $a^{n-1} \equiv 1 \pmod{n}$, причем $a^{\gamma} \not\equiv 1 \pmod{n}$ для всех натуральных $\gamma | (n-1)$. Можно ли вместо тестирования всех натуральных делителей числа $n-1$ ограничиться тестированием лишь простых делителей числа $n-1$?

6.2. Вероятностные тесты простоты. Псевдопростые числа

Современные тесты простоты гораздо эффективнее рассмотренных в первом разделе методов решета Эратосфена и последовательного деления. Они разбиваются на две категории: точные и вероятностные. В первом случае мы имеем стопроцентную гарантию того, что прошедшее тест число является простым. Во втором случае существует небольшая, но не равная нулю вероятность того, что прошедшее тест число все-таки является составным [22], [29], [49], [53], [68] и др.

6.2.1. Тест Ферма

Тест Ферма является простейшим вероятностным тестом простоты. Он основан на использовании *малой теоремы Ферма* [36]: *если p — простое число и a — целое число, взаимно простое с p, то* $a^{p-1} \equiv 1 \pmod{p}$.

Таким образом, если мы хотим выяснить, является ли данное натуральное число n простым, мы случайным образом выбираем число a из промежутка $[2, n-1]$, и используем малую теорему Ферма. Если сравнение не имеет места для данного a, то n является составным. Если сравнение имеет место для нескольких значений a, мы говорим, что, с большой долей вероятности, n является простым.

Алгоритм теста Ферма.

Вход: Нечетное целое число $n \geqslant 5$.

Выход: «Число n составное» или «Число n, вероятно, простое».

Шаг 1. Выбрать случайное число a, $2 < a < n-2$.

Шаг 2. Вычислить $r \equiv a^{n-1} \pmod{n}$.

При $r = 1$ результат: «Число n, вероятно, простое».

В противном случае результат: «Число n составное». ▷

Сложность теста Ферма равна $O(\log^3 n)$ при умножении «в столбик» и $O(\log^2 n \log\log n)$ при умножении алгоритмом Шенхаге—Штрассена (алгоритм умножения больших целых чисел, основной идеей которого является быстрое преобразование Фурье).

Пример 6.2.9 Используя тест Ферма, проверим на простоту числа 31, 77, 127 и 143. Выбрав, например, число 2, убедимся в том, что

$$2^{30} \equiv (2^5)^6 \equiv 1 \pmod{31}, \text{ и } 2^{126} \equiv (2^7)^{18} \equiv 1 \pmod{127}.$$

Делаем вывод: числа 31 и 127, вероятно, простые. Далее,

$$2^{76} \equiv (2^6)^{12} \cdot 2^4 \equiv (-13)^{12} \cdot 16 \not\equiv 1 \pmod{77}, \text{ и } 2^{142} \not\equiv 1 \pmod{143}.$$

Следовательно, числа 77 и 143 — составные. □

К сожалению, всегда имеется вероятность того, что благополучно прошедшее тест Ферма число все-таки составное. Такие числа называются *псевдопростыми* (*псевдопростыми Ферма*). Точнее, составное число n называется *псевдопростым Ферма по основанию* a, если a и n взаимно просты, и $a^{n-1} \equiv 1 \pmod{n}$ [53], [68].

Пример 6.2.10 Убедимся, что число 25 является псевдопростым по основанию 7. Действительно, поскольку

$$7^2 \equiv -1 \pmod{25}, \text{ то } 7^{24} \equiv (7^2)^{12} \equiv (-1)^{12} \equiv 1 \pmod{25},$$

то есть при $a = 7$ для $n = 25$ выполняется соотношение $a^{n-1} \equiv 1 \pmod{n}$.

Непосредственная проверка показывает, что число $527 = 17 \cdot 31$ является псевдопростым по основаниям 1, 154, 373, 526, поскольку

$$1^{526} \equiv 154^{526} \equiv 373^{526} \equiv 1 \pmod{527}.$$

Аналогично можно показать, что число $629 = 17 \cdot 37$ является псевдопростым по основаниям 1, 38, 149, 154, 186, 191, 290, 302, 327, 339, 438, 443, 475, 480, 591, 628.

Псевдопростыми по основанию 7, кроме числа 25, являются числа

$325 = 5^2 \cdot 13$, $2352 = 13 \cdot 181$,
$561 = 3 \cdot 11 \cdot 17$, $2465 = 5 \cdot 17 \cdot 29$,
$703 = 19 \cdot 37$, $3277 = 29 \cdot 113$,
$817 = 19 \cdot 43$, $4525 = 562 \cdot 1814$,
$1105 = 5 \cdot 13 \cdot 17$, $4825 = 5^2 \cdot 193$,
$1825 = 5^2 \cdot 73$, $6697 = 37 \cdot 181$,
$2101 = 11 \cdot 191$, $8321 = 53 \cdot 157$. □

Свойства псевдопростых чисел

1. Нечетное составное число n является псевдопростым по основанию a тогда и только тогда, когда $n - 1$ делится на показатель $P_n(a)$ числа a по модулю n.
2. Если нечетное составное число n является псевдопростым по основаниям a и b, то n является псевдопростым и по основаниям $ab \pmod{n}$, $ab^{-1} \pmod{n}$, $a^{-1}b \pmod{n}$.
3. Если нечетное составное число n не является псевдопростым хотя бы по одному основанию a, то n является псевдопростым не более чем по $\dfrac{\varphi(n)}{2}$ основаниям, где $\varphi(n)$ — функция Эйлера.

Рассмотрим простейшие случаи «малых» оснований.

Очевидно, что любое нечетное составное число n является псевдопростым по основанию 1. Это основание является «тривиальным» и обычно не рассматривается.

Числа Пуле — это псевдопростые по основанию 2. Наименьшее число Пуле равно 341. Оно составное, так как представимо в виде $11 \cdot 31$, но удовлетворяет условиям малой теоремы Ферма: $2^{340} \equiv 1 \pmod{341}$. Числа Пуле образуют последовательность 341, 561, 645, 1105, 1387, ...

Оказывается, эта последовательность бесконечна. Дело в том, что если n — число Пуле, то $2^n - 1$ также является числом Пуле. Действительно, пусть $2^{n-1} \equiv 1 \pmod{n}$, то есть $2^{n-1} - 1 = kn$ для некоторого целого числа k. Тогда

$$2^{2^n-2} \equiv 2^{2(2^{n-1}-1)} \equiv 2^{2kn} \equiv (2^n)^{2k} \equiv 1^{2k} \equiv 1 \ \big(\mathrm{mod}(2^n - 1)\big).$$

Таким образом, мы доказали, что *существует бесконечно много чисел Пуле.*

Наименьшее псевдопростое по основанию 3 равно 91. Последовательность псевдопростых по основанию 3 начинается с элементов 91, 121, 286, 671, 703, ...

Начальные элементы последовательностей псевдопростых Ферма по малым основаниям представлены в таблице [126].

Основание a	Псевдопростые Ферма по основанию a
2	341, 561, 645, 1105, 1387, ...
3	91, 121, 286, 671, 703, ...
4	15, 85, 91, 341, 435, ...
5	4, 124, 217, 561, 781, ...
6	35, 185, 217, 301, 481, ...
7	6, 25, 325, 561, 703, ...
8	9, 21, 45, 63, 65, ...

На первый взгляд кажется, что наличие псевдопростых не является большой проблемой: мы получим информацию о том, что число n составное, просто сменив используемое основание.

Однако проблема заключается в том, что существуют натуральные числа n, которые являются псевдопростыми для всех допустимых (то есть взаимно простых с n) значений a. Такие числа называются *числами Кармайкла*. Первое и наименьшее такое число, 561, было найдено в 1910 г. Робертом Кармайклом (Robert Daniel Carmichael, 1879–1967). Следующие числа Кармайкла:

$1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$, ...
$1729 = 7 \cdot 13 \cdot 19$, $6601 = 7 \cdot 23 \cdot 41$,
$2465 = 5 \cdot 17 \cdot 29$, $8911 = 7 \cdot 19 \cdot 67$,

Основой изучения чисел Кармайкла является *критерий Корсельста* (1899): *натуральное число n является числом Кармайкла тогда и только тогда, когда n бесквадратно, и, для любого простого делителя p числа n, $p-1$ делит $n-1$* [112].

Пример 6.2.11 Пользуясь критерием, убедимся, что 561 является числом Кармайкла. Действительно, $561 = 3 \cdot 11 \cdot 17$ бесквадратно, и $2|560$, $10|560$, $16|560$.

Аналогично, $1729 = 7 \cdot 13 \cdot 19$ бесквадратно, и $6|1728$, $12|1728$, $18|1728$; $1105 = 5 \cdot 13 \cdot 17$ бесквадратно, и $4|1104$, $12|1104$, $16|1104$. □

Каждое из рассмотренных в примере чисел Кармайкла было составлено ровно из трех простых чисел. Закономерность ли это? Оказывается, да. Соответствующее утверждение является следствием теоремы Корсельста: *любое число Кармайкла является произведением не менее трех простых чисел.*

Более того, нетрудно показать, что *число* $(6k+1)(12k+1)(18k+1)$ *является числом Кармайкла, если все три указанных множителя являются простыми.* (Черник, 1939).

Действительно, рассмотрим простые числа вида

$$p_1 = 6k+1, \quad p_2 = 12k+1, \quad p_3 = 18k+1$$

и докажем, что число $n = p_1p_2p_3$ является числом Кармайкла. Согласно малой теореме Ферма, для любого числа a, взаимно простого с p_1, выполняется сравнение $a^{6k} \equiv 1 \pmod{p_1}$. Аналогично, $a^{12k} \equiv 1 \pmod{p_2}$, $a^{18k} \equiv 1 \pmod{p_3}$. Число $36k$ является наименьшим общим кратным чисел $6k$, $12k$, $18k$, и, по китайской теореме об остатках, $a^{36k} \equiv 1 \pmod{n}$ для всех чисел a, взаимно простых с n. Но

$$n - 1 = 1296k^2 + 396k + 36k = 36k \cdot (36k^2 + 11k + 1),$$

то есть $a^{n-1} \equiv 1 \pmod{n}$ для всех чисел a, взаимно простых с n.

Пример 6.2.12 При $k = 1$ получаем $p_1 = 7, p_2 = 13, p_3 = 19$, и, следовательно, число Кармайкла $1729 = 3 \cdot 13 \cdot 19$. При $k = 2$ число $p_2 = 25$ — составное; при $k = 3$ число $p_3 = 55$ — составное; при $k = 4$ число $p_1 = 25$ — составное; при $k = 5$ число $p_3 = 91$ — составное; при $k = 6$ получаем $p_1 = 37, p_2 = 73, p_3 = 109$, и, следовательно, число Кармайкла $294409 = 37 \cdot 73 \cdot 109$. □

Для генерации чисел Кармайкла общего вида можно воспользоваться *алгоритмом Эрдеша* (1956): возьмем *сильно составное число* m (натуральное число, которое имеет больше делителей, чем любое предшествующее ему натуральное число); составим множество S простых чисел p, для

которых $(m, p) = 1$ и m делится на $p - 1$; из множества S выберем такие числа $p_1, p_2, \ldots p_r$, $r \geqslant 3$, для которых $p_1 p_2 \ldots p_r \equiv 1 \pmod m$. Тогда $n = p_1 p_2 \ldots p_r$ — число Кармайкла.

Пример 6.2.13 Пусть $m = 120 = 2^3 \cdot 3 \cdot 5$. Составляем множество $S = \{7, 11, 13, 31, 41, 61\}$. (Чем больше множество S, тем больше чисел Кармайкла нам, возможно, удастся построить.) Перебирая возможные произведения элементов множества S, получаем числа Кармайкла:

$$41041 = 7 \cdot 11 \cdot 13 \cdot 41 \equiv 1 \pmod{120},$$
$$172081 = 7 \cdot 13 \cdot 31 \cdot 61 \equiv 1 \pmod{120},$$
$$852841 = 11 \cdot 31 \cdot 41 \cdot 61 \equiv 1 \pmod{120}$$ □

В 1994 г. было доказано [112], что *существует бесконечно много чисел Кармайкла.* Именно, для достаточно большого n существует приблизительно $n^{2/7}$ чисел Кармайкла между 1 и n. Однако при движении вправо по числовой оси числа Кармайкла становятся очень редки. Например, существует 1401644 чисел Кармайкла между 1 и 10^{18} (приблизительно одно на 700 миллионов чисел).

6.2.2. Тест Соловея—Штрассена

Тест Соловея—Штрассена — еще один вероятностный тест для определения простоты данного натурального числа.

По *критерию Эйлера* [20], [36], для любого нечетного простого p и любого $a \in [1, p-1]$ имеет место сравнение

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p,$$

где $\left(\frac{a}{p}\right)$ — *символ Лежандра. Символ Якоби* $\left(\frac{a}{n}\right)$, определяемый как

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

для $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, является обобщением символа Лежандра, обладает аналогичными свойствами и может быть вычислен для любого нечетного n [20], [36], [75], [95]. При использовании приведенных ниже свойств символ Якоби может быть вычислен за время $O(\log^2 n)$.

Свойства символа Якоби

1. Если $a \equiv b \pmod n$, то $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
3. $\left(\frac{a^2}{n}\right) = 1$; в частности, $\left(\frac{1}{n}\right) = 1$.
4. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, то есть $\left(\frac{-1}{n}\right) = 1$, если $n \equiv 1 \pmod 4$, и $\left(\frac{-1}{n}\right) = -1$, если $n \equiv -1 \pmod 4$.
5. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, то есть $\left(\frac{2}{n}\right) = 1$, если $n \equiv \pm 1 \pmod 8$, и $\left(\frac{2}{n}\right) = -1$, $n \equiv \pm 3 \pmod 8$.
6. Для различных нечетных натуральных чисел n и m имеет место равенство $\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}\left(\frac{n}{m}\right)$ (*квадратичный закон взаимности*).

Пример 6.2.14 Вычислим символ Якоби $\left(\frac{23}{63}\right)$:

$$\left(\frac{23}{63}\right) = (-1)^{\frac{23-1}{2}\cdot\frac{63-1}{2}}\left(\frac{63}{23}\right) = -\left(\frac{-6}{23}\right) = -\left(\frac{-1}{23}\right)\left(\frac{2}{23}\right)\left(\frac{3}{23}\right) =$$

$$= -(-1)^{\frac{23-1}{2}}(-1)^{\frac{23^2-1}{8}}(-1)^{\frac{23-1}{2}\cdot\frac{3-1}{2}}\left(\frac{23}{3}\right) =$$

$$= (-1)^4 \cdot \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1. \qquad \square$$

Если мы хотим проверить простоту числа n, мы можем произвольным образом выбрать несколько значений a и убедиться, что сравнение $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$ выполнено. В этом случае мы говорим что, вероятно, число n — простое. Если же для некоторого a сравнение нарушается, то мы можем утверждать, что n — составное число.

Алгоритм теста Соловея—Штрассена.

Вход: Нечетное целое число $n \geqslant 5$.

Выход: «Число n составное» или «Число n, вероятно, простое».

Шаг 1. Выбрать случайное число a, $2 < a < n - 2$.

Шаг 2. Вычислить $r = a^{\frac{n-1}{2}} \pmod n$.

При $r \neq 1$ **и** $r \neq n - 1$ **результат:** «Число n составное».

Шаг 3. Вычислить символ Якоби $s = \left(\frac{a}{n}\right)$.

При $r \equiv s \pmod n$ **результат:** «Число n, вероятно, простое».

В противном случае результат: «Число n составное». ▷

Сложность теста Соловея—Штрассена определяется сложностью вычисления символа Якоби и равна $O(\log^3 n)$.

Пример 6.2.15 Проверим числа 63 и 149 на простоту, пользуясь тестом Соловея—Штрассена.

Для проверки на простоту числа 63 выберем случайное число a, $2 < a < 61$, например, возьмем число $a = 4$. Вычислим $r \equiv 4^{\frac{63-1}{2}} \pmod{63}$. Поскольку $4^3 \equiv 1 \pmod{63}$, то $4^{\frac{63-1}{2}} \equiv 4^{31} \equiv (4^3)^{10} \cdot 4 \equiv 4 \pmod{63}$, то есть $r \neq \pm 1$, и мы доказали, что число 63 — составное.

Для проверки на простоту числа 149 выберем случайное число a, $2 < a < 147$, например, возьмем число $a = 23$. Вычислим $r \equiv 23^{\frac{149-1}{2}} \pmod{149}$. Поскольку непосредственная проверка приводит к результату $23^{74} \equiv -1 \pmod{149}$, то $r = -1$. Теперь вычисляем символ Якоби так, как это было сделано в предыдущем примере и получим, что $s = \left(\frac{23}{63}\right) = -1$. Таким образом, сравнение $r \equiv s \pmod n$ имеет место. Мы заканчиваем работу. Наш результат: «Число 149, вероятно, простое». □

Подобно тесту Ферма, при некотором a мы можем получить положительный ответ (о простоте) для составного числа n. Такое число — натуральное число n, для которого сравнение $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$ выполнено, но n является составным, называется *эйлеровым псевдопростым*.

Пример 6.2.16 Число 91 является эйлеровым псевдопростым, так как оно составное, но $\left(\frac{10}{91}\right) = -1$ и $10^{45} \equiv -1 \pmod{91}$, то есть сравнение $\left(\frac{a}{n}\right) \equiv a^{\frac{91-1}{2}} \pmod{91}$ выполнено для $a = 10$. □

Замечание. *Если n является псевдопростым Эйлера по основанию a, то оно является и псевдопростым Ферма по основанию a. Так, число* 91 *— псевдопростое Эйлера по основанию* 10, *является и псевдопростым Ферма по основанию* 10: $10^{90} \equiv (-1)^2 \equiv 1 \pmod{91}$. *Обратное утверждение неверно. Так, число* 91 *является псевдопростым Ферма по основанию* 3, *поскольку* $3^{90} \equiv 1 \pmod{91}$, *однако оно не является псевдопростым Эйлера по основанию* 3: $3^{45} \equiv 27 \not\equiv \pm 1 \pmod{91}$.

В отличие от теста Ферма, для каждого n по меньшей мере половина всех $a \in [1, p-1]$ являются «свидетелями» Эйлера, то есть не существует оснований, которые, подобных числам Кармайкла в тесте Ферма, являются «лгунами» для всех ситуаций. Тест объявляет составное n как вероятностно-простое с вероятностью не более 2^{-k}, где k — число различных использованных нами оснований a. Более того, перебрав более половины возможных оснований, мы получим стопроцентную гарантию правильного ответа.

Начальные элементы последовательностей псевдопростых Эйлера по основаниям 2 и 3 представлены в таблице [126].

Основание a	Псевдопростые Эйлера по основанию a
2	561, 1105, 1729, 1905, 2047, ...
3	121, 703, 1729, 1891, 2821, ...

6.2.3. Тест Миллера—Рабина

Тест Миллера—Рабина является на сегодняшний день вероятностным тестом, который чаще всего используется для проверки чисел на простоту.

Он основан на следующем свойстве простых чисел ([20], [36]): *если для нечетного простого p число $p-1$ записано в виде $p-1=2^k d$, где k — целое неотрицательное число, а d — нечетное число, то для любого целого a, взаимно простого с p, имеет место либо сравнение $a^d \equiv 1 \pmod p$, либо сравнение $a^{2^r d} \equiv -1 \pmod p$ для некоторого $r \in [0, k-1]$.*

Действительно, поскольку $a^{p-1} \equiv 1 \pmod p$, то $a^{2^k d} - 1 \equiv 0 \pmod p$, откуда $(a^{2^{k-1} d} - 1)(a^{2^{k-1} d} + 1) \equiv 0 \pmod p$, то есть $a^{2^{k-1} d} \equiv -1 \pmod p$ или $a^{2^{k-1} d} \equiv 1 \pmod p$. В первом случае мы получаем необходимое сравнение с $r = k-1$. Во втором случае, проведя аналогичные рассуждения, получим либо сравнение $a^{2^{k-2} d} \equiv -1 \pmod p$, дающее необходимое соотношение с $r = k-2$, либо сравнение $a^{2^{k-2} d} \equiv 1 \pmod p$, позволяющее дальнейшее разложение. Поскольку

$$\begin{aligned} a^{p-1} - 1 = a^{2^s r} - 1 &= (a^{2^{s-1} r} - 1)(a^{2^{s-1} r} + 1) = \\ &= (a^{2^{s-2} r} - 1)(a^{2^{s-2} r} + 1)(a^{2^{s-1} r} + 1) = \ldots = \\ &= (a^r - 1)(a^r + 1)(a^{2r} + 1) \ldots (a^{2^{s-2} r} + 1)(a^{2^{s-1} r} + 1), \end{aligned}$$

то в последнем произведении хотя бы одна из скобок обязательно делится на p, то есть либо $a^r \equiv 1 \pmod n$, либо среди чисел $a^r, a^{2r}, \ldots a^{2^{r-1}}$ найдется число, сравнимое с -1 по модулю n.

Тест Миллера—Рабина использует указанные соотношения: для данного нечетного n, записав число $n-1$ в виде $n-1 = 2^k d$, мы произвольным образом выбираем натуральное a, $2 < a < n-2$ и проверяем сравнение $a^d \equiv 1 \pmod{n}$. Если оно выполнено, то мы предполагаем, что число n — простое. В противном случае мы проверяем выполнимость одного из сравнений $a^{2^r d} \equiv -1 \pmod{n}$ для $r \in [0, n-1]$. Если такое сравнение найдено, то мы предполагаем, что число n — простое. Если нет, то можем быть уверены, что n — составное.

Алгоритм теста Миллера—Рабина.

Вход: Нечетное целое число $n \geqslant 5$.

Выход: «Число n составное» или «Число n, вероятно, простое».

Шаг 1. Представить $n-1$ в виде $n-1 = 2^s r$, где число r нечетное.

Шаг 2. Выбрать случайное число a, $2 < a < n-2$.

Шаг 3. Вычислить $y \equiv a^r \pmod{n}$.

Шаг 4. При $y \neq 1$ и $y \neq n-1$ выполнить:

4.1. Положить $j = 1$.

4.2. Если $j \neq s-1$ и $y \neq n-1$, то

4.2.1. Положить $y \equiv y^2 \pmod{n}$.

При $y = 1$ **результат:** «Число n составное».

4.2.2. Положить $j = j+1$.

При $y \neq n-1$ **результат:** «Число n составное».

Шаг 5. **Результат:** «Число n, вероятно, простое». ▷

Сложность алгоритма Миллера—Рабина равна $O(\log^3 n)$.

Пример 6.2.17 Проверим числа 81, 149 на простоту с помощью теста Миллера—Рабина.

Для числа 81 рассмотрим число $81-1 = 80$ и представим его в виде $80 = 2^4 \cdot 5$; таким образом, $d = 5$ и $r = 4$. Выберем $a = 4$ и проверим истинность сравнения $5^d \equiv 1 \pmod{81}$. Поскольку

$$4^d \equiv 4^5 \equiv 64^2 \cdot 4 \equiv (-17)^2 \cdot 4 \equiv 26 \cdot 4 \equiv 104 \equiv 23 \not\equiv 1 \pmod{81},$$

то продолжим работу. Возведя сравнение $4^5 \equiv 23 \pmod{81}$ в квадрат, мы убедимся, что

$$4^{2\cdot 5} \equiv 43 \not\equiv -1 \pmod{81}; \quad 4^{2^2\cdot 5} \equiv -14 \not\equiv -1 \pmod{81};$$

$$4^{2^3\cdot 5} \equiv 34 \not\equiv -1 \pmod{81}; \quad 4^{2^4\cdot 5} \equiv 22 \not\equiv -1 \pmod{81}.$$

Таким образом, мы убедились что число 81 — составное.

Для числа 149 рассмотрим число $149-1=148$ и представим его в виде $148=2^2\cdot 37$; таким образом, $d=2$ и $r=37$. Выберем $a=3$ и проверим истинность сравнения $3^d\equiv 1 \pmod{149}$. Поскольку

$$3^{37}\equiv (3^5)^7\cdot 3^2\equiv (-55)^7\cdot 9\equiv -45^3\cdot 48\equiv -88\cdot 45\cdot 48\equiv -86\cdot 44\not\equiv 1 \pmod{149},$$

то продолжим работу. Последовательно возведя сравнение $3^{37}\equiv 44 \pmod{149}$ в квадрат, мы убедимся, что $3^{2\cdot 37}\equiv 446\equiv -1 \pmod{149}$. Таким образом, мы можем остановиться и объявить результат: «Число 149, вероятно, простое». □

Итак, если для данного нечетного n с $n-1=2^k d$ мы можем указать такое целое a из промежутка $[3, n-3]$, что $a^d\not\equiv 1 \pmod n$, и $a^{2^r d}\not\equiv -1 \pmod n$ для всех $r\in[0, n-1]$, то a свидетельствует о том, что n — составное и называется «сильным свидетелем». Иначе — то есть в случае выполнения обоих условий для составного n — a называется «сильным лгуном», а n объявляется *сильным псевдопростым* по основанию a.

Пример 6.2.18 Нетрудно показать, что наименьшими сильными псевдопростыми числами являются: для $a=2$ — число $2047=23\cdot 89$, для $a=3$ — число $121=11\cdot 11$, для $a=5$ — число $781=11\cdot 71$, для $a=7$ — число $25=5\cdot 5$. Убедимся в этом, например, для случая $a=3$, $n=121$. Поскольку $n-1=120=2^5\cdot 5$, то $r=5$, $d=5$ и мы начнем с проверки справедливости сравнения $3^5\equiv 1 \pmod{121}$. Поскольку $3^5\equiv 243\equiv 1 \pmod{121}$, то, согласно алгоритму, мы остановимся и объявим заведомо неверный результат: «Число 121, вероятно, простое».

Начальные элементы последовательностей сильных простых по малым основаниям представлены в таблице [126].

Основание a	Сильные псевдопростые по основанию a
2	2047, 3277, 4033, 4681, 8321, ...
3	121, 703, 1891, 3281, 8401, ...
4	341, 1387, 2047, 3277, 4033, ...
5	781, 1541, 5461, 5611, 7813, ...
6	217, 481, 1111, 1261, 2701, ...
7	25, 325, 703, 2101, 2353, ...
8	9, 65, 481, 511, 1417, ...
9	91, 121, 671, 703, 1541, ...

□

В случае теста Миллера—Рабина для каждого нечетного составного n имеется много свидетелей: по меньшей мере $\frac{3}{4}$ от всех допустимых a. Поскольку мы не знаем простого способа нахождения таких a, то тест используется как вероятностный: выбирая a случайным образом k раз, мы получим высокую вероятность правильного ответа, так как тест объявит составное n простым с вероятностью не более 4^{-k}.

Замечание. *Если n является сильно псевдопростым по основанию a, то оно является псевдопростым Эйлера по основанию a. Более того, если $n \equiv 3 \pmod 4$, то оно будет сильно псевдопростым по основанию a в том и только в том случае, когда оно является псевдопростым Эйлера по основанию a.*

Упражнения

(1) Используйте тест Ферма для проверки на простоту числа n:

a) $n = 127$; d) $n = 133$; g) $n = 53$; j) $n = 89$;
b) $n = 129$; e) $n = 47$; h) $n = 57$; k) $n = 35$;
c) $n = 131$; f) $n = 49$; i) $n = 87$; l) $n = 37$.

(2) Докажите, что 15 — псевдопростое число Ферма по основанию 4. Найдите все основания a, для которых 15 — псевдопростое число Ферма.

(3) Является ли число 21 псевдопростым числом Ферма по основаниям 2, 4, 8? Найдите все основания a, для которых 21 — псевдопростое число Ферма.

(4) Проверьте, является ли число 91 псевдопростым Ферма по основаниям 2, 3, 4, 5. Найдите по крайней мере 10 таких оснований. Докажите, что 91 — наименьшее псевдопростое число по основанию 3. Докажите, что существует 36 оснований (то есть половина всех возможных оснований), для которых 91 — псевдопростое число.

(5) Докажите, что 1729 является псевдопростым Ферма по основаниям 2, 3 и 5. Что можно сказать об основаниях 4 и 6? Назовите еще 10 оснований, по которым число 1729 является псевдопростым Ферма. Убедитесь, что 1729 является числом Кармайкла.

(6) Найдите наименьшее псевдопростое число Ферма по основанию a:

a) $a = 4$; b) $a = 5$; c) $a = 6$; d) $a = 7$; e) $a = 8$.

(7) Для каждого из чисел $5, 91, 703$ найдите все основания, по которым эти числа являются псевдопростыми Ферма.

(8) Проверьте, что числа 561, 645, 1105, 1387 являются числами Пуле.

(9) Докажите, что существует бесконечно много псевдопростых по основаниям 2, 3 и 5.

(10) Используя критерий Корсельста, проверьте, что числа 1105, 1729, 2465, 2821, 6601 являются числами Кармайкла.

(11) Найдите все числа Кармайкла вида $3pq$, p и q — простые.

(12) Найдите все числа Кармайкла вида $5pq$, p и q — простые.

(13) Докажите, что 561 — наименьшее число Кармайкла.

(14) Покажите, что числа $2821 = 7 \cdot 13 \cdot 31$, $29341 = 13 \cdot 37 \cdot 61$, $172081 = 7 \cdot 13 \cdot 31 \cdot 61$, $278545 = 5 \cdot 17 \cdot 29 \cdot 113$ являются числами Кармайкла.

(15) Убедитесь, что последовательность сильно составных чисел начинается с элементов 1, 2, 4, 6, 12, 24, 36, 48, 60, 120. Используйте тест Эрдеша для нахождения чисел Кармайкла, выбирая сильно составное число m из множества $\{180, 240, 360, 720, 840, 1260, 1680\}$.

(16) Вычислите символ Якоби:

a) $\left(\frac{129}{337}\right)$; c) $\left(\frac{99}{129}\right)$; e) $\left(\frac{393}{1047}\right)$; g) $\left(\frac{1245}{1899}\right)$;

b) $\left(\frac{129}{337}\right)$; d) $\left(\frac{557}{235}\right)$; f) $\left(\frac{109}{189}\right)$; h) $\left(\frac{2981}{339}\right)$.

(17) Проверьте число n на простоту, используя тест Соловея—Штрассена:

a) $n = 127$; e) $n = 47$; i) $n = 87$;

b) $n = 129$; f) $n = 49$; j) $n = 89$;

c) $n = 131$; g) $n = 53$; k) $n = 35$;

d) $n = 133$; h) $n = 57$; l) $n = 37$.

(18) Убедитесь, что число 561 является псевдопростым Эйлера по основанию 2. Будет ли число 561 псевдопростым числом Ферма?

(19) Является ли число 121 псевдопростым Эйлера по основаниям 2, 3, 4, 5? Будет ли оно псевдопростым числом Ферма по этим основаниям?

(20) Проверьте число n на простоту, используя тест Миллера—Рабина:

a) $n = 127$; e) $n = 47$; i) $n = 87$;

b) $n = 129$; f) $n = 49$; j) $n = 89$;

c) $n = 131$; g) $n = 53$; k) $n = 35$;

d) $n = 133$; h) $n = 57$; l) $n = 37$.

(21) Убедитесь, что число 121 является сильным псевдопростым по основанию 3 и по основанию 9. Является ли оно псевдопростым Эйлера? Псевдопростым Ферма?

(22) Является ли число 91 сильным псевдопростым по основаниям 3, 6, 9? Является ли оно псевдопростым Эйлера? Псевдопростым Ферма?

(23) Проверьте, что числа 9 и 65 являются сильными псевдопростыми по основанию 8.

(24) Будет ли произвольное псевдопростое число псевдпростым Эйлера; сильным псевдопростым? Приведите примеры.

Задачи

[1] Докажите, что для любого натурального числа a существует бесконечно много псевдопростых Ферма по основанию a.

[2] Докажите, что число $(12k+5)(36k+13)(48k+17)$ является числом Кармайкла, если каждый из трех указанных множителей — простое число; докажите, что число $(30k+7)(60k+13)(150k+31)$ является числом Кармайкла, если каждый из трех указанных множителей — простое число. Приведите примеры.

[3] Докажите, что нечетное составное число n, делящееся на квадрат некоторого простого числа, не может быть числом Кармайкла.

[4] Докажите, что для любого фиксированного простого r имеется лишь конечное множество чисел rpq (p и q — простые), являющихся числами Кармайкла.

[5] Докажите, что число $(180k+7)(300k+11)(360k+13)(1200k+41)$ является числом Кармайкла, если все сомножители в скобках — простые числа.

[6] Докажите, что для любого простого числа p и для любого целого a, такого что $(a^2-1,p)=1$, число $\dfrac{a^{2p}-1}{a^2-1}$ является псевдопростым Ферма по основанию a.

[7] Докажите, что если числа p и $2p-1$ простые, то их произведение $n=p(2p-1)$ является псевдопростым Ферма ровно по $\dfrac{\varphi(n)}{2}$ основаниям a: по тем основаниям, которые являются квадратичными вычетами по модулю $2p-1$, то есть по тем a, для которых символ Лежандра $\left(\dfrac{a}{2p-1}\right)=1$.

[8] Пусть n — нечетное составное натуральное число и пусть $(a,n)=1$. Докажите, что если p — простой делитель n, то n является псевдопростым Ферма по основанию a только при $a^{\frac{n}{p}} \equiv 1 \pmod{p}$.

[9] Докажите, что никакое целое число $n=3p$, где $p>3$ — простое число, не может быть псевдопростым Ферма по основаниям 2, 5 или 7.

10 Докажите, что никакое целое число $n = 5p$, где $p > 5$ — простое число, не может быть псевдопростым Ферма по основаниям 2, 3 или 7.

11 Пусть p — простое число. Докажите, что p^2 является псевдопростым Ферма по основанию a тогда и только тогда, когда $a^{p-1} \equiv 1 \pmod{p^2}$.

12 Пусть $n = pq$ — произведение двух различных простых чисел. Пусть $d = (p-1, q-1)$. Докажите, что n является псевдопростым Ферма по основанию a тогда и только тогда, когда $a^d \equiv 1 \pmod{d}$. Выразите через d число различных оснований, по которым n — псевдопростое Ферма.

13 Пусть p — простое число. Сколько имеется оснований, по которым $q = 2p + 1$ — псевдопростое Ферма? Приведите их полный список (в терминах p).

14 Пусть $n = 341$. Какова вероятность того, что случайно выбранное a, взаимно простое с n, будет основанием, по которому n — псевдопростое число Ферма?

15 Найдите составное число n и основание a, для которых $a^{\frac{n-1}{2}} \equiv \equiv \pm 1 \pmod{n}$, но n не является эйлеровым псевдопростым по основанию a.

16 Докажите, что если числа p и $2p - 1$ простые, то их произведение $n = p(2p-1)$ является эйлеровым псевдопростым ровно по $\dfrac{\varphi(n)}{4}$ основаниям.

17 Покажите, что если n — эйлерово псевдопростое по основаниям a_1 и a_2, то оно будет эйлеровым псевдопростым и по основанию $a_1 \cdot a_2$.

18 Пусть $n = (6k+1)(12k+1)(18k+1)$, где числа $6k+1$, $12k+1$ и $18k+1$ — простые. Докажите, что если k нечетное, то n является эйлеровым псевдопростым ровно по $\dfrac{\varphi(n)}{2}$ основаниям; если k четное, то n является эйлеровым псевдопростым ровно по $\dfrac{\varphi(n)}{4}$ основаниям a.

19 Убедитесь, что для всех двузначных простых чисел выполняется утверждение, лежащее в основе теста простоты Миллера—Рабина: если p — простое число и $p - 1 = 2^k d$, где d нечетно, то для любого a, взаимно простого с p, $a^d \equiv 1 \pmod{p}$ или $a^{2^r d} \equiv -1 \pmod{p}$, для некоторого $r \in [0, \ldots k-1]$.

20 Докажите, что натуральное число $n \equiv 3 \pmod 4$ является сильно псевдопростым числом по основанию a тогда и только тогда, когда оно является псевдопростым Эйлера по основанию a. Приведите примеры.

21 Докажите, что если n — сильно псевдопростое по основанию a, то оно сильно псевдопростое по основанию a^k для любого натурального k.

22 Пусть n является псевдопростым по основанию a, но не является сильно псевдопростым по основанию a. Найдите нетривиальный делитель числа n.

23 Докажите, что если число n — псевдопростое Ферма по основанию 2, то число $2^n - 1$ является псевдопростым Ферма по основанию 2; псевдопростым Эйлера по основанию 2; сильно псевдопростым по основанию 2.

24 Используя обозначение «O большое», оцените число двоичных операций в ситуации, когда тест Миллера—Рабина применяется столько раз, что вероятность прохождения составного числа n через эти тесты меньше $1/m$ (n и m очень велики).

25 Предполагая верной обобщенную гипотезу Римана (утверждающую, что все нетривиальные нули L-функций Дирихле лежат на критической прямой), оцените число двоичных операций в ситуации, когда тест Миллера—Рабина применяется столько раз, сколько необходимо для достаточной уверенности в том, что прошедшее все тесты число n является простым.

26 Докажите, что число $n = p^\alpha$, $\alpha > 1$, является сильно псевдопростым по основанию a тогда и только тогда, когда оно является псевдопростым Ферма по основанию a.

27 Докажите, что свойство сохранения сильной простоты числа n при перемножении оснований имеет место тогда и только тогда, когда n — либо степень простого числа, либо делится на простое число, сравнимое с 3 по модулю 4.

28 Докажите, что если найдется такое a, что n является псевдопростым Ферма, но не является сильно псевдопростым по основанию a, то можно быстро найти простой делитель числа n. Объясните, как можно защититься от этого при выборе $n = pq$ в системе *RSA*.

6.3. Детерминированные тесты простоты. Генерация больших простых чисел

Детерминированные тесты можно назвать тестами, доказывающими простоту [22], [29], [37], [68]. Эти тесты вычислительно более сложны, чем вероятностные, поэтому, прежде чем проверять число детерминированным тестом, необходимо проверить его, например, тестом Миллера—Рабина. Всякий детерминированный тест, по сути, представляет собой доказательство теоремы о достаточном условии простоты числа. Поэтому числа, которые считаются простыми на основании прохождения ими детерминированного теста, называются доказуемо простыми.

В некоторых детерминированных тестах используются случайные числа. Однако, в отличие от тестов Ферма, Соловея—Штрассена или Миллера—Рабина, эти тесты дают ответ «Число n простое» или «Число n, вероятно, составное». Поэтому при проверке чисел на простоту можно параллельно выполнять какой-либо вероятностный и детерминированный тест до тех пор, пока один из них не даст определенный ответ.

6.3.1. Проверка простоты с использованием числа $n-1$

Проверка на простоту с использованием числа $n-1$ — хорошо известный класс детерминированных тестов, в которых доказательство простоты числа n основано на исследовании полного или частичного разложения на простые множители числа $n-1$.

Теоретическим основанием тестов такого рода служит [68] (Cabourn Pocklington, 1870–1952): *пусть целое число* $n \geqslant 3$ *имеет вид* $n = q^s R + 1$, *где* q *— простое число,* $s \geqslant 1$, *и* R *не делится на* q. *Если существует такое* a, *что*

$$a^{n-1} \equiv 1 \pmod{n},\ и\ (a^{\frac{n-1}{q}} - 1, n) = 1,$$

то для любого простого делителя p *числа* n *выполняется сравнение* $p \equiv \equiv 1 \pmod{q^s}$.

На основании этого факта формулируется *критерий Поклингтона*: *пусть целое число* $n \geqslant 3$ *имеет вид*

$$n = QR + 1, \quad где \quad (Q, R) = 1, R < Q$$

и $Q = \prod_{j=1}^{t} q_j^{\alpha_j}$ *— каноническое разложение числа* Q. *Если для каждого* q_j *существует целое число* a_j, *для которого*

$$a_j^{n-1} \equiv 1 \pmod{n}, и\ (a_j^{\frac{n-1}{q_j}} - 1, n) = 1,$$

то число n *— простое.*

Пример 6.3.19 Проверим число 229 на простоту с помощью критерия Поклингтона. Сначала запишем его в виде

$$229 = q_1 R + 1 = 19 \cdot 12 + 1.$$

Теперь, чтобы убедиться в простоте числа 229, достаточно найти одно целое число a, для которого $a^{n-1} \equiv 1 \pmod{n}$, и $(a^R - 1, n) = 1$. Этим условиям удовлетворяет, например, число $a = 2$. Таким образом, a — простое. □

Тесты, подобные тесту Поклингтона, могут быть использованы лишь при тестировании чисел n, для которых не составляет труда проанализировать поведение чисел $n-1$. Самыми известными специальными числами, обладающими этим свойством, являются *числа Ферма* $F_n = 2^{2^n}+1$, $n \geqslant 0$. Они получаются при поиске простых вида 2^k+1 (для простоты числа 2^k+1 необходимо, чтобы k было степенью двойки) и имеют вид $F_n = q^s \cdot R + 1$ при $q = 2$, $s = 2^n$, и $R = 1$.

Числа Ферма были введены французским математиком Пьером Ферма (Pierre de Fermat, 1601–1665), который предположил (1640), что они являются простыми числами для всех $n = 0, 1, 2, 3, \ldots$. Первые пять чисел Ферма действительно являются простыми: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Однако в 1732 г. Леонард Эйлер (Leonhard Euler, 1707–1783) доказал, что F_5 является составным:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Таким образом, гипотеза Ферма о простоте чисел F_n была опровергнута. Более того, до сих пор не найдено ни одного простого числа Ферма, большего F_4.

Доказано, что F_n является составным для всех n от 5 до 32 и для многих других значений n, хотя не для всех составных чисел Ферма найдены простые делители. На сегодняшний день известно 227 составных чисел Ферма. Наибольшим известным составным числом Ферма $p = 3 \cdot 2^{2478765} + 1$.

Для исследования чисел Ферма на простоту необходимо изучить вопросы их делимости; в частности, интересны для нас свойства простых делителей чисел Ферма, которые имеют специальную форму [37], [98], [97].

Свойства делимости чисел Ферма

1. $(F_n, F_m) = 1$, если $n \neq m$.
2. $F_n \equiv 2 \pmod 3$, $n \geqslant 1$, то есть 3 не делит F_n, $n \geqslant 1$.
3. $F_n \equiv 2 \pmod 5$, $n \geqslant 2$, то есть 5 не делит F_n, $n \geqslant 2$.
4. $F_n \equiv 3; 5 \pmod 7$, то есть 7 не делит F_n.
5. Любой простой делитель p числа F_n, $n \geqslant 1$, имеет вид $p = 2^{n+1}k + 1$; если $n > 1$, любой простой делитель числа F_n имеет вид $p = 2^{n+2}k+1$.

Итак, простые делители чисел Ферма имеют специальную форму. Это свойство может быть использовано для проверки простоты чисел F_n.

Пример 6.3.20 Исследуем число F_5. Любой простой делитель числа F_5 должен иметь вид $2^7 \cdot k + 1$. Рассматривая числа указанного вида до естественной границы $\sqrt{F_5}$, мы получаем простые числа только для $k = 2$ и $k = 5$: — 257 и 641, соответственно.

Непосредственная проверка показывает, что простое число 641 делит F_5; более того, $F_5 = 641 \cdot 6700417$ представляет собой произведение двух простых чисел. Ландри (Landry, 1880) доказал, что $274177 | F_6$, где $274177 = 256k + 1$, $k = 1071$. Именно, $F_6 = 274177 \cdot 67280421310721$ есть произведение двух простых. Бриллхарт и Моррисон (Brillhart & Morrison, 1975) показали, что $a | F_7$, $a = 512k + 1$, где $k = 1165031037646443$, и F_7 также представляет собой произведение двух простых. □

Другим методом проверки простоты чисел Ферма является *критерий Пепина* (Jean François Theophile Pepin, 1826–1904): *число Ферма* F_n, $n \geqslant 1$, *является простым тогда и только тогда, когда* $F_n | (3^{\frac{F_n-1}{2}} + 1)$.

Пример 6.3.21 Проверим на простоту числа $F_4 = 2^{2^4} + 1$ и $F_5 = 2^{2^5} + 1$. Поскольку

$$3^{\frac{F_4-1}{2}} \equiv 3^{\frac{2^{16}}{2}} \equiv 3^{2^{15}} \equiv -1 \pmod{F_4},$$

то F_4 — простое. Поскольку

$$3^{\frac{F_5-1}{2}} \equiv 3^{\frac{2^{32}}{2}} \equiv 3^{2^{31}} \not\equiv -1 \pmod{F_5},$$

то F_5 — составное. □

Вместо числа 3 можно взять любое число k, для которого символ Якоби $\left(\frac{k}{F_n}\right) = -1$, в частности, k может быть равно 5 (число 5 использовал сам Пепин) или 10.

Именно этим методом было доказано, что числа F_7, F_8, F_{13}, F_{14} и F_{20} являются составными.

Заметим, что этот метод не дает информации о простых множителях тестируемого числа; именно поэтому мы не имеем информации ни об одном простом делителе составного числа F_{20}.

В 1878 г. было получено обобщение критерия Пепина — *теорема Прота* (François Proth, 1852–1879): *число* $n = R \cdot 2^k + 1$, *где* $2^k > R$, *является простым, если существует целое* a, *такое что* $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Мы получаем одно из утверждений теоремы Пепина при $h = 1$ и $a = 3$. Очевидно, теорема Прота является частным случаем критерия Поклингтона для простейшего случая $Q = 2$.

6.3.2. Проверка простоты с использованием числа $n + 1$

Проверка на простоту с использованием числа $n + 1$ подразумевает применение к числу n детерминированных тестов простоты в условиях, когда полностью или частично известно разложение числа $n+1$ ([22], [29], [68] и др.).

Так, нижеследующее утверждение позволяет проверять на простоту произвольное число n, для которого известно разложение на простые числа $n+1$: *пусть числа p и q взаимно просты и пусть последовательность $\{U_i\}_i$ определяется соотношениями $U_0 = 0$, $U_1 = 1$, $U_{i+1} = pU_i - qU_{i-1}$ для $i \geqslant 1$. Положительное нечетное число n является простым, если*:

- $p^2 - 4q$ — квадратичный невычет по модулю n;
- $U_{n+1} \equiv 0 \pmod{n}$;
- $U_{\frac{n+1}{p}} \not\equiv 0 \pmod{n}$ для всех простых делителей p числа $n+1$.

Пример 6.3.22 Исследуем на простоту число $n = 350657$. Прежде всего, разложим на множители число $n+1$: $350658 = 2 \cdot 3^3 \cdot 7 \cdot 11^2 \cdot 23$.

Выберем $p = 3$, $q = 5$; в этом случае $p^2 - 4q = 3^2 - 4 \cdot 5 = -11$. Нетрудно убедиться, что $\left(\frac{-11}{n}\right) = -1$, и первое условие теста выполнено.

Построим последовательность $\{U_i\}_i$, на каждом этапе переходя к вычетам по модулю n: $U_0 = 0, U_1 = 1$, $U_2 = 3$, ..., $U_{n-1} \equiv 280525 \pmod{n}$, $U_n \equiv 350656 \pmod{n}$, $U_{n+1} \equiv 0 \pmod{n}$. Второе условие теста выполнено.

Проверим третье условие: $U_{n/2} \equiv 7281 \pmod{n}$, $U_{n/3} \equiv 155139 \pmod{n}$, $U_{n/7} \equiv 299210 \pmod{n}$, $U_{n/11} \equiv 306723 \pmod{n}$, $U_{n/23} \equiv 51824 \pmod{n}$. Оно тоже выполняется.

Следовательно, мы доказали, что число n простое [68]. □

Тесты такого рода тесно связаны с исследованием еще одного специального вида чисел — *чисел Мерсенна* $2^n - 1, n \in \mathbb{N}$ [37], [97]. Некоторые авторы требуют, чтобы n было простым, поскольку с точки зрения вопросов простоты только такие индексы представляют интерес: если $2^n - 1$ — простое, то n также является простым. Последовательность чисел Мерсенна начинается с чисел 1, 3, 15, 31, 63, 127, 255, 511, 1023, 2047, ...

Хотя числа вида $2^n - 1$ носят имя французского монаха Марена Мерсенна (Marin Mersenne, 1588–1648), рассмотревшего их в своей книге «Cogita physico mathematics» и высказавшего несколько гипотез о их поведении, они были знакомы ученым и до 17-го столетия. В 1536 г. Региус (Regius) показал, что $2^{11} - 1 = 2047$ не является простым, оно равно $23 \cdot 89$; в 1588 г. Катальди (Cataldi) доказал, что $2^{17} - 1$ и $2^{19} - 1$ являются простыми.

Свойства делимости чисел Мерсенна

1. Если $m = nq + r$, $d|M_m$ и $d|M_n$, то $d|M_r$.
2. $(M_m, M_n) = M_{(m,n)}$, в частности, $M_n|M_m$ тогда и только тогда, когда $n|m$.
3. $(M_n, M_m) = 1$ тогда и только тогда, когда $(m, n) = 1$.

4. Если q является простым, $q \equiv \pm 1 \pmod 8$, то $q | M_{\frac{q-1}{2}}$.
5. Если q, p являются простыми, $q | M_p$, то $q = 2pt + 1$.
6. Если q, p являются простыми, $q | M_p$, то $q \equiv \pm 1 \pmod 8$.
7. Если q, p являются простыми, $q | M_p$ и $p = 4t \mp 1$, то $q \in \{8pk + 1, 8pk + 1 \pm 2p\}$.

Таким образом, простые делители q числа Мерсенна M_p с простым индексом p имеют специальную форму: если $q | M_p$ и $p = 4t \mp 1$, то $q \in \{8pk + 1, 8pk + 1 \pm 2p\}$. Следовательно, для проверки простоты числа Мерсенна M_p с простым индексом p достаточно проверить его делимость на простые указанного вида, не превосходящие величины $\sqrt{M_p}$ (число Мерсенна M_n с составным индексом n заведомо является составным).

Пример 6.3.23 Именно этот способ использовал Эйлер (1771) для проверки простоты числа M_{31}, убедившись, что ни одно простое число вида $248n + 1$ или $248n + 63$ до 46339 (имеется только 84 таких простых) не является делителем M_{31}.

Этот способ достаточно продуктивен при относительно малых значениях p. Однако даже урезанное множество возможных делителей становится слишком большим с ростом M_p. □

Другим методом проверки простоты чисел Мерсенна является *тест Люка—Лемера*: *число* M_p (*где* p — *нечетное простое*) *является простым тогда и только тогда, когда оно является делителем* $(p-1)$*-го элемента последовательности* $L_1, L_2, \ldots L_k, \ldots$, *где* $L_1 = 4$, *и* $L_{k+1} = L_k^2 - 2$.

Основы этого теста были заложены Франсуа Люка (François Edouard Anatole Lucas, 1842–1891) в 1870-е годы, когда, исследуя последовательность Фибоначчи $u_1, u_2, \ldots u_n, \ldots$ ($u_1 = u_2 = 1$, и $u_{n+2} = u_{n+1} + u_n$), он открыл следующий факт: если $n \equiv \pm 3 \pmod{10}$ и n — собственный делитель числа u_{n+1}, то n — простое; если $n \equiv \pm 1 \pmod{10}$ и n — собственный делитель числа u_{n-1}, то n — простое. Опираясь на соображения такого типа, Люка доказал в 1876 г. (после 19 лет работы над этой проблемой) простоту числа M_{127}. В 1930 г. Деррик Генри Лемер (Derrick Henry Lehmer, 1905–1991) упростил тест Люка, придав ему современную форму.

Пример 6.3.24 Рассмотрим простое число $p = 11$ и проверим, будет ли простым число $M_{11} = 207$. Для этого построим последовательность $L_1, \ldots, L_{10}$:

$$L_1 = 4, \quad L_2 = 4^2 - 2 = 14, \qquad L_3 = 14^2 - 2 = 194,$$

$$L_4 = 194^2 - 2 \equiv 788 \pmod{2047}, \qquad L_5 = 788^2 - 2 \equiv 701 \pmod{2047},$$

$L_6 = 701^2 - 2 \equiv 119 \pmod{2047}$, $L_7 = 119^2 - 2 \equiv 1877 \pmod{2047}$,

$L_8 = 1877^2 - 2 \equiv 240 \pmod{2047}$, $L_9 = 240^2 - 2 \equiv 282 \pmod{2047}$,

$L_{10} = 282^2 - 2 \equiv 1736 \not\equiv 0 \pmod{2047}$.

Значит, число $M_{11} = 2047$ — составное. В самом деле, $M_{11} = 23 \cdot 89$ [68].

Рассмотрим простое число $p = 13$ и проверим, будет ли простым число $M_{13} = 8191$.

Для этого построим последовательность $L_1, \ldots, L_{12}$:

$L_1 = 4, L_2 = 4^2 - 2 = 14$, $L_3 = 14^2 - 2 = 194$,

$L_4 = 194^2 - 2 \equiv 4870 \pmod{8191}$, $L_5 = 4870^2 - 2 \equiv 3953 \pmod{8191}$,

$L_6 = 3853^2 - 2 \equiv 5970 \pmod{8191}$, $L_7 = 5970^2 - 2 \equiv 1857 \pmod{8191}$,

$L_8 = 1857^2 - 2 \equiv 36 \pmod{8191}$, $L_9 = 36^2 - 2 \equiv 1294 \pmod{8191}$,

$L_{10} = 1294^2 - 2 \equiv 3470 \pmod{2047}$, $L_{11} = 3470^2 - 2 \equiv 128 \pmod{8191}$,

$L_{12} = 128^2 - 2 \equiv 16382 \equiv 0 \pmod{8191}$.

Значит, число $M_{13} = 8191$ — простое [37]. □

После Люка процесс исследования простоты чисел Мерсенна надолго затормозился: следующее простое число Мерсенна было найдено лишь в 1952 г. с помощью компьютера.

Тест Люка—Лемера идеально подходит для бинарных компьютеров, так как вычисление L_k обходится без деления и может быть выполнено только при использовании умножения и сложения, которые бинарные компьютеры выполняют быстро. Для экономии времени L_k вычисляют по модулю $2^p - 1$. Рассматривать L_k по модулю M_n также удобно в двоичной системе, так как здесь M_n представляет собой конечную последовательность единиц.

Именно поэтому числа Мерсенна дают нам почти все известные на сегодняшний день *рекорды простых чисел*. Так, в 1999 г. было найдено первое простое число, имеющее более одного миллиона десятичных знаков (на самом деле, более двух миллионов). Оно является 38-м простым числом Мерсенна, $M_{6972593}$, и имеет 2098960 десятичных знаков. В 2013 г. было получено новое (именно, 48-е известное) простое число Мерсенна, $M_{57885161}$. Оно имеет более 17 миллионов десятичных знаков.

С числами Мерсенна связано много интересных теоретических задач, а также ряд нерешенных теоретико-числовых проблем [37]. Так, до сих пор неизвестно, конечно или бесконечно множество простых чисел Мерсенна. Ответ, возможно, должен быть «да»: используя асимптотический закон

распределения простых чисел, мы можем утверждать, что вероятность «случайного» числа n быть простым не превосходит $\dfrac{A}{\log n}$ для некоторого действительного числа A. Поскольку

$$\frac{A}{\log M_n} > \frac{A}{\log (2^n)} = \frac{A}{n \log 2}, \quad \text{то} \quad \sum_{n=1}^{\infty} \frac{A}{\log M_n} > \frac{A}{\log 2} \sum_{n=1}^{\infty} \frac{1}{n}.$$

Расходимость гармонического ряда позволяет утверждать, что и ряд $\sum\limits_{n=1}^{\infty} \dfrac{1}{\log M_n}$ расходится, что свидетельствует о бесконечности множества простых чисел Мерсенна. Однако в этих рассуждениях мы предполагаем, что простые числа Мерсенна ведут себя как случайные числа, что на самом деле не так: по крайней мере, они имеют простые делители специальной формы.

Конечно, существует и ряд других детерминированных тестов простоты, но их обсуждение выходит за рамки нашего пособия. Упомянем лишь тест Миллера, детерминированный полиномиальный тест простоты, предложенный Гари Миллером (Gary Lee Miller) и впервые опубликованный в 1976 г., и тест Агравала—Каяла—Саксены — универсальный полиномиальный детерминированный тест простоты чисел, предложенный индийскими учеными Маниндрой Агравалом (Manindra Agrawal, род. 1966), Ниражем Каялом (Neeraj Kayal) и Нитином Саксеной (Nitin Saxena, род. 1981) и впервые опубликованный в 2002 г. Тест Миллера основывается на недоказанной расширенной гипотезе Римана, т. е. является условным. Этим тест отличается от теста Агравала—Каяла—Саксены, который полностью доказан. Появление теста Агравала—Каяла—Саксены решило вопрос о принадлежности задачи распознавания простоты классу P, являвшийся до этого открытой проблемой [128].

6.3.3. Генерация простых чисел

Генерация простых чисел — одна из актуальнейших практических задач. Корни этого вопроса уходят в глубочайшую теоретическую проблему нахождения *формулы простых чисел*, под которой понимают формулу, генерирующую простые числа, причем, в идеальном варианте, только и все простые числа, как, например, формулы n^2 и $\dfrac{n(n+1)}{2}$ генерирует все *квадратные* и *треугольные числа*, соответственно. На сегодняшний день такая «идеальная» формула простых чисел неизвестна.

Для частичного решения проблемы последовательного построения больших простых чисел можно использовать детерминированные тесты простоты. Для этого выбирают некоторую последовательность чисел специального вида, среди которых нужно найти простое число, и к каждому из этих чисел применяют детерминированный тест [22], [74].

Пример 6.3.25 Используем тест Поклингтона для того, чтобы найти простое число, имеющее не менее восьми десятичных знаков.

Для этого выберем произвольное простое число $q_1 \geqslant 5$, например, $q_1 = 19$, и четное число R из интервала $[2, q_1 - 3] = [2, 16]$, например, $R = 12$. Положим $n = q_1 R + 1 = 19 \cdot 12 + 1 = 229$.

Согласно теореме Поклингтона, чтобы n было простым, достаточно найти одно целое число a, для которого $a^{n-1} \equiv 1 \pmod{n}$, и $(a^R - 1, n) = 1$. Этим условиям удовлетворяет, например, число $a = 2$. Первое простое число 229 построено.

Возьмем $q_2 = 229$. Выберем четное число R из интервала $[2, q_2 - 3] = [2, 226]$. Пусть, например, $R = 224$. Положим $n = q_2 R + 1 = 229 \cdot 224 + 1 = 51294$. При $a = 2$ получаем, что $a^{n-1} \equiv 4 \pmod{n}$. Значит, число n составное и нужно выбрать другое R. При $R = 222$ получаем $n = 50839$ и условия теоремы выполнены. Второе простое число 50839 получено.

Полагаем $q_3 = n = 50839$. При $R = 300$ получаем $n = q_3 R + 1 = 50839 \cdot 300 + 1 = 15251701$. Условия теоремы выполнены, и число 15251701 — простое, причем требуемой длины [68]. □

Упражнения

1. Используйте тест Поклингтона для проверки на простоту чисел 61, 101, 149.
2. Приведите пример трех чисел, для проверки простоты которых удобно использовать критерий Поклингтона. Осуществите проверку простоты.
3. Докажите, что если число $2^k + 1$ является простым, то $k = 2^n$, то есть мы получаем число Ферма $F_n = 2^{2^n} + 1$.
4. Докажите, что $F_n \neq p + q$ для любых простых p и q и любого $n \neq 1$.
5. Докажите, что $F_n = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} + 2$.
6. Докажите, что $F_n | F_{n+k} - 2$, где $n \geqslant 0, k \geqslant 1$.
7. Докажите, что
   a) $F_n = (F_{n-1} - 1)^2 + 1$;
   b) $F_n = F_{n-1} + 2^{2^{n-1}} F_0 \cdot \ldots \cdot F_{n-2}$;
   c) $F_n = (F_{n-1})^2 - 2(F_{n-2} - 1)^2$.
8. Проверьте простоту чисел F_n, $n = 2, 3, 4$, пользуясь методом пробного деления.
9. Проверьте простоту чисел F_n, $n = 2, 3, 4$, пользуясь критерием Пепина.
10. Приведите пример трех чисел, простоту которых удобно проверять, пользуясь теоремой Прота. Осуществите проверку.

⑪ Проверьте числа 127, 149, 203 на простоту, пользуясь $(n+1)$-тестом простоты.

⑫ Приведите примеры других чисел, которые можно проверить на простоту таким образом.

⑬ Докажите, что если M_n является простым, то и n является простым.

⑭ Докажите, что $M_n | M_{mn}$.

⑮ Докажите, что $M_{m-n} | (M_m - M_n)$ для $m > n$.

⑯ Докажите, что $3|M_n \Leftrightarrow 2|n$, $5|M_n \Leftrightarrow 4|n$, $7|M_n \Leftrightarrow 3|n$, $11|M_n \Leftrightarrow 10|n$, $13|M_n \Leftrightarrow 12|n$, $17|M_n \Leftrightarrow 8|n$, $23|M_n \Leftrightarrow 11|n$.

⑰ Докажите, что если $n \equiv a \pmod 4$, то $M_n \equiv k \pmod{10}$, где $a = 0, 1, 2, 3$, и $k = 5, 1, 3, 7$, соответственно.

⑱ Докажите следующие утверждения:

a) $n \equiv 0 \pmod 4 \Rightarrow M_n \equiv 5 \pmod{10}$;

b) $n \equiv 1 \pmod 4 \Rightarrow M_n \equiv 1 \pmod{10}$;

c) $n \equiv 2 \pmod 4 \Rightarrow M_n \equiv 3 \pmod{10}$;

d) $n \equiv 3 \pmod 4 \Rightarrow M_n \equiv 7 \pmod{10}$.

⑲ Приведите пример функции, значениями которой будут простые числа 2, 3, 5, 7, 11.

⑳ Пользуясь тестом Поклингтона, постройте несколько несколько элементов некоторой возрастающей последовательности простых чисел.

Задачи

[1] Докажите, что, если $a^n + 1$ — простое, то $n = 2^k$.

[2] Докажите, что, если $a^n - 1$ — простое, то $a = 2$, и $n \in P$.

[3] Докажите, что $F_n \neq k^s$; в частности, $F_n \neq k^2$, то есть ни одно число Ферма не является *квадратным числом*.

[4] Докажите, что $F_n \neq \dfrac{k(k+1)}{2}$, то есть ни одно число Ферма не является *треугольным числом*.

[5] Докажите, что если $F_n \in P$, то $F_n \neq k^p - l^p$ $(k, l, p \in \mathbb{N})$.

[6] Докажите, что $F_n | (2^{F_n} - 2)$, то есть *составные числа Ферма являются псевдопростыми числами по основанию* 2.

[7] Докажите, что среди чисел вида $2^{2^n} + 3$ существует бесконечно много составных.

[8] Докажите, что каждое число вида $2^{2^n} + 5$ — составное.

9 Какие из чисел вида $k \cdot 2^m + 1$, $k = 1, 2, \ldots$ являются простыми?

10 Постройте несколько первых *чисел Куллена* $C_n = n \cdot 2^n + 1$. Исследуйте их непростоту.

11 Докажите, что если число Ферма F_n, $n \geqslant 1$, является простым то $F_n | (3^{\frac{F_n - 1}{2}} + 1)$.

12 Докажите, что $F_n \neq p^2 + q^2$, $p, q \in P$.

13 Докажите, что $F_n = p^2 + q^2 + z^2$, $p, q, z \in P$, только при $n = 2$.

14 Докажите, что $F_n^3 + 8 \in S$; $F_n + 4, F_n + 10, F_n^2 + 2, F_n^2 + 8 \in S$, $n \geqslant 1$; $F_n + 8 \in S$, $n \geqslant 2$.

15 Докажите, что $F_n \equiv 2 \pmod{15}$, $F_n \equiv 1 \pmod{16}$, $F_n \equiv 17, 41 \pmod{72}$, $n \geqslant 2$.

16 Докажите, что последняя цифра каждого числа Ферма (кроме чисел 3 и 5) равна 7, то есть $F_n \equiv 7 \pmod{10}$, $n \geqslant 2$.

17 Докажите, что две последние цифры каждого числа Ферма (кроме чисел 3 и 5) равны 17, 37, 57 или 97.

18 Докажите, что F_{73} имеет более $24 \cdot 10^{20}$ цифр.

19 Докажите, что F_{1945} имеет более 10^{582} цифр.

20 Проверьте, что три последние цифры чисел F_{73} и F_{1945} равны 897 и 297 соответственно.

21 Докажите бесконечность множества простых чисел, используя числа Ферма.

22 Пользуясь доказательством бесконечности множества простых чисел с помощью чисел Ферма, докажите бесконечность простых чисел в арифметической прогрессии $4k + 1$.

23 Для данного $t \in \mathbb{N}$ докажите бесконечность простых чисел в арифметической прогрессии $2^t k + 1$.

24 Для заданных $p \in P$ и $t \in \mathbb{N}$ докажите бесконечность простых чисел в арифметической прогрессии $2p^t \cdot k + 1$.

25 Известно, что *правильный n-угольник можно построить циркулем и линейкой тогда и только тогда, когда $n = 2^k \cdot p_1 \cdot \ldots \cdot p_s$, где k — целое неотрицательное число, а $p_1, p_2, \ldots p_s$ — различные простые числа Ферма.* Выпишите все известные на сегодняшний день нечетные значения n. Можно ли построить циркулем и линейкой правильный семиугольник? Правильный 17-угольник?

26 Докажите бесконечность множества простых чисел, используя числа Мерсенна.

27 Пользуясь таблицей известных простых чисел Мерсенна, проверьте истинность *гипотезы Мерсенна*, которая утверждает, что $2^n - 1$ является простым для $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, и является составным для всех остальных показателей $2 \leqslant n \leqslant 257$.

28 Пользуясь таблицей известных простых чисел Мерсенна, для первых простых чисел Мерсенна проверьте истинность *новой гипотезы Мерсенна*, которая состоит в следующем. Пусть p — нечетное натуральное число. Если два из указанных ниже условий выполнены, то выполнено и третье:

a) $p = 2^k \pm 1$ или $p = 4^k \pm 3$;

b) $2^p - 1$ является простым (простым Мерсенна);

c) $\dfrac{2p+1}{3}$ является простым (*простым Вагстаффа*).

29 Докажите, что $3|M_n \Leftrightarrow 2|n$, $5|M_n \Leftrightarrow 4|n$, $7|M_n \Leftrightarrow 3|n$, $9|M_n \Leftrightarrow 6|n$, $11|M_n \Leftrightarrow 10|n$, $13|M_n \Leftrightarrow 12|n$, $17|M_n \Leftrightarrow 8|n$, $23|M_n \Leftrightarrow 11|n$.

30 Докажите, что любое нечетное натуральное число n делит бесконечно много чисел Мерсенна.

31 Проверьте, что M_6 — наименьшее число Мерсенна, содержащее квадрат простого числа. Проверьте, что M_{21} — наименьшее число Мерсенна M_n с нечетным n, содержащее квадрат простого числа.

32 Докажите, что $M_n \neq x^2 + y^2 + z^2$ для $n \geqslant 3$.

33 Найдите все пары *простых-близнецов*, одно из которых является числом Ферма, а другое — числом Мерсенна.

34 Докажите, что число $M_s + 1$ является сильно составным.

35 *Совершенные числа* — натуральные числа, равные сумме их собственных делителей, то есть натуральных делителей, отличных от самого числа. Первыми совершенными числами являются числа 6, 28, 496, 8128, ... *Теорема Евклида—Эйлера* утверждает, что *четное натуральное число n является совершенным тогда и только тогда, когда $n = 2^{k-1}(2^k - 1)$, где $2^k - 1$ — простое число Мерсенна*. Найдите первые пять четных совершенных чисел.

36 Объясните, почему не следует применять тест Ферма по основанию 2 для чисел Ферма и Мерсенна? Как обстоят дела по основанию 2 для других вероятностных тестов при проверке чисел Ферма и Мерсенна?

37 Докажите, что функция

$$f(n) = \left\lfloor \cos^2 \pi \frac{(n-1)! + 1}{n} \right\rfloor$$

принимает значение 1, если n — простое, и 0, если n — составное; кроме того, $f(1) = 1$.

38 Проверьте, что $f(n) \equiv 2 + 2n! \,(\mathrm{mod}(n+1))$ дает простое число p для $n = p - 1$ и равно 2 в остальных случаях.

39 Докажите, что функция $f(n) = (-1)^n + 4$ дает простые числа для любого $n \in \mathbb{N}$.

Литература к главе 6

При подготовке текста главы 6 были использованы следующие источники [2], [20], [22], [29], [36–38], [40], [43], [48], [49], [53–57], [67], [68], [69], [72], [74], [75], [86], [88], [90], [92], [93], [95], [97], [98], [102], [104], [105], [108], [116], [112], [123–127].

Глава 7

Факторизация натуральных чисел

Факторизацией натурального числа называется его разложение в произведение простых множителей. Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из *основной теоремы арифметики* [98].

В отличие от задачи распознавания простоты числа, факторизация предположительно является вычислительно сложной задачей. Это предположение лежит в основе широко используемых алгоритмов, например, *RSA*.

В зависимости от сложности алгоритмы факторизации можно разбить на две группы. Первая группа — экспоненциальные алгоритмы, сложность которых экспоненциально зависит от длины входящих параметров. Вторая группа — субэкспоненциальные алгоритмы.

Вопрос о существовании алгоритма факторизации с полиномиальной сложностью на классическом компьютере является одной из важных открытых проблем современной теории чисел.

7.1. Классические методы факторизации

Задача разложения на множители (факторизации) натуральных чисел имеет длинную и богатую историю, связанную с именами Эратосфена (Eratosthenes of Cyrene, предположительно 284–202 до н. э.), Леонардо Пизанского (Leonardus Pisanus, предположительно 1170–1250), Пьера Ферма (Pierre de Fermat, 1601–1665), Леонарда Эйлера (Leonhard Euler, 1707–1783), Адриена Мари Лежандра (Adrien-Marie Legendre, 1752–1833), Карла Фридриха Гаусса (Johann Carl Friedrich Gauß, 1777–1855) и др., которые занимались ей лишь как следствием (этапом) при решении проблемы определения простоты числа и для эстетического удовольствия. Впоследствии интерес научного общества к этой проблеме сильно уменьшился. Внимание ученых к вопросам факторизации было привлечено вновь во второй половине XX в., после создания в 1977 г. системы *RSA*, базирующейся на предположении о сложности задачи разложения на множители составного числа m, являющегося произведением двух больших

простых чисел p и q. Попытки вскрытия системы *RSA* стимулировали бурные исследования в области факторизации целых чисел, в результате чего было предложено несколько новых и нестандартных идей.

7.1.1. Метод пробного деления

Самым древним известным способом факторизации натуральных чисел является метод *пробного деления* натурального числа n на простые числа p, не превосходящие n, или, с учетом того, что наименьший простой делитель составного числа n не превосходит $\sqrt{n}$, на простые числа $p \leqslant \sqrt{n}$ [98].

Пример 7.1.1 Факторизуем методом пробного деления число $n = 2494633$. Для начала найдем корень из числа n: $\lfloor\sqrt{2494633}\rfloor = 1579$. Для нахождения простого делителя числа n будем последовательно делить его на простые числа p, не превосходящие 1579: $p \in \{2, 3, 5, 7, 11, \ldots 1579\}$. Дойдя до 131, мы получим в процессе деления частное 19043. Таким образом, $2494633 = 131 \cdot 19043$. Используя тот же алгоритм, получим разложение $19043 = 137 \cdot 139$. Поскольку числа 137 и 139 — простые, наша задача полностью решена: каноническое разложение числа n имеет вид $2494633 = 131 \cdot 137 \cdot 139$.

При решении задачи для выделения одного множителя числа 2494633 пришлось осуществлять пробное деление 32 раза, а для полного разложения числа — 34 раз. □

Способ пробного деления отличается простотой и удобством применения. Его основной минус заключается в количестве пробных делений, которое в худшем случае, когда n есть произведение двух простых примерно одинакового размера, может быть достаточно большим: оценка сложности алгоритма имеет вид $O(\sqrt{n}\log^2 n)$. Однако в виду простой реализации он с успехом используется для факторизации сравнительно небольших чисел.

Алгоритм факторизации числа n методом пробного деления можно немного ускорить, если заранее вычислить произведения используемых простых чисел. Находя с помощью алгоритма Евклида наибольший общий делитель d числа n и какого-либо из этих произведений, в случае нетривиального результата можно перейти к факторизации числа $\frac{n}{d}$, повторяя процедуру нужное число раз [68].

Пример 7.1.2 Разложим на множители число $n = 84257901$, используя модифицированный вариант метода пробного деления. Для этого составим базу данных из произведений первых нечетных простых чисел, взятых по три: $q_1 = 3 \cdot 5 \cdot 7 = 105$, $q_2 = 11 \cdot 13 \cdot 17 = 2431$, $q_3 = 19 \cdot 23 \cdot 29 = 12673$.

Применяя алгоритм Евклида, найдем

$$d_{11} = (n, q_1) = (84257901, 105) = 21.$$

Это означает, что n делится на 3 и на 7, и мы можем перейти к числу

$$n_1 = \frac{n}{d_{11}} = \frac{84257901}{21} = 4012281.$$

Далее:

$$d_{12} = (n_1, q_1) = (4012281, 105) = 21, \text{ и } n_2 = \frac{n_1}{d_{12}} = \frac{4012281}{21} = 191061;$$

$$d_{13} = (n_2, q_1) = (191061, 105) = 3, \text{ и } n_3 = \frac{n_2}{d_{13}} = \frac{191061}{3} = 63687;$$

$$d_{14} = (n_3, q_1) = (63687, 105) = 3, \text{ и } n_4 = \frac{n_3}{d_{14}} = \frac{63687}{3} = 21229.$$

Таким образом, число 84257901 делится на 3^4 и на 7^2.

Аналогично,

$$d_{21} = (n_4, q_2) = (21229, 2431) = 13, \text{ и } n_5 = \frac{n}{d_{21}} = \frac{21229}{13} = 1633;$$

$$d_{31} = (n_5, q_3) = (1633, 12673) = 23, \text{ и } n_5 = \frac{n_4}{d_{31}} = \frac{1633}{23} = 71,$$

а 71 — простое число.

Таким образом, наша задача полностью решена:

$$84257901 = 3^4 \cdot 7^2 \cdot 13 \cdot 23 \cdot 71. \qquad \square$$

«Малость» простых делителей, участвующих в построении базы, определяется либо размером числа n, либо объемом памяти компьютера. Перебрав все простые, не превосходящие $\sqrt{n}$, мы гарантированно найдем каноническое разложение n. В худшем случае, когда n есть произведение двух простых примерно одинакового размера, на это потребуется примерно $\sqrt{n}$ делений.

7.1.2. Метод Ферма

Один из наиболее известных методов факторизации, автором которого, вероятно, был П. Ферма, основан на теореме о представлении нечетного натурального числа в виде разности двух квадратов: *любое нечетное натуральное число $n > 1$ представимо в виде разности квадратов двух натуральных чисел; если $n = a \cdot b$, то $n = x^2 - y^2$, где $x = \frac{a+b}{2}$, $y = \frac{a-b}{2}$.*

Поскольку в этом случае $y^2 = x^2 - n$, и $x^2 > n$, мы получаем способ факторизации натуральных чисел, который состоит в последовательном переборе всех натуральных чисел $x > \sqrt{n}$ и исследовании разностей $x^2 - n$. Как только одна из этих разностей окажется квадратом натурального числа, то есть будет выполнено соотношение $x^2 - n = y^2$, мы сможем разложить n на множители: $n = (x + y) \cdot (x - y)$. Для составного числа n это произойдет при некотором $x < \dfrac{n+1}{2}$ [97].

Пример 7.1.3 Факторизуем методом Ферма число $n = 3551$. Чтобы найти разложение $n = x^2 - y^2$, будем рассматривать выражение $x^2 - n$, перебирая все натуральные x, такие что $x^2 > 3551$, или, что то же, $x > \sqrt{3551}$. Так как ближайший к 3551 квадрат равен $3600 = 60^2$, то начнем перебор с $x = 60$:

$$x^2 - n = 3600 - 3551 = 49 = 7^2.$$

Следовательно, уже на первом шаге алгоритма мы получили $y = 7$ и разложение

$$3551 = (60 - 7)(60 + 7) = 53 \cdot 67.$$

Факторизуем тем же методом число $n = 2993$. В этом случае будем перебирать x, удовлетворяющие условию $x > \sqrt{2993}$. Поскольку ближайший квадрат, больший 2993, есть $3025 = 55^2$, то $x \geqslant 55$: перебор значений надо начать с $x = 55$. Для лучшей организации перебора составим таблицу.

x	55	56	57
x^2	3025	3136	3249
$x^2 - 2993$	32	143	$256 = 16^2 = y^2$

Таким образом, задача решена: $x = 57, y = 16$, и

$$2993 = (57 - 16)(57 + 16) = 41 \cdot 73.$$

Заметим, что на практике для промежуточных вычислений используют соотношение $(x + 1)^2 = x^2 + 2x + 1$, избегая многократного возведения в квадрат. □

Модификацией метода Ферма является *метод сдвигов* [97].

Для натурального числа n назовем *n-ым сдвигом последовательности квадратов* последовательность $\{u_k\}_{k=1}^{\infty}$, задаваемую формулой $u_k = n + k^2$, $k \in \mathbb{N}$.

Из теоремы о представлении нечетного натурального числа в виде разности двух квадратов следует, что при построении последовательности n-го сдвига один из ее элементов непременно окажется полным квадратом, что приведет к факторизации числа n.

В частности, для составного натурального числа n, не являющегося полным квадратом и удовлетворяющего условию $(n, 30) = 1$, k-ый член n-го сдвига последовательности квадратов будет квадратом при некотором $k \leqslant \left\lfloor \dfrac{n-49}{14} \right\rfloor$.

Пример 7.1.4 Факторизуем методом сдвигов числа 391 и 1189.

Вычисления, осуществляемые в ходе алгоритма, отражены в таблице.

k	1	2	3	4	5	6
k^2	1	4	9	16	25	36
$u_k = 391 + k^2$	392	395	$400 = 20^2$			
$u_k = 1189 + k^2$	1190	1193	1198	1205	1214	$1125 = 35^2$

Таким образом, мы получаем, что $391 = (20-3)(20+3) = 17 \cdot 23$, и $1189 = (35-6)(35+6) = 29 \cdot 41$. □

Понятно, что чем больше разница между числами a и b в разложении $n = a \cdot b$, тем более трудоемким становится метод Ферма. В этом случае можно воспользоваться обобщением этого метода [24], [68], [97]: для небольшого $k \in \mathbb{N}$ последовательно перебирать $h \geqslant \sqrt{k \cdot n}$ до получения такого числа h, что $h^2 - kn$ является полным квадратом. В этом случае $h^2 - kn = t^2$, и $kn = (h+t)(h-t)$, то есть числа $h-t$ и n имеют нетривиальный общий делитель d. Найдя число d с помощью алгоритма Евклида, мы получим один из множителей в разложении числа n.

Пример 7.1.5 Попробуем факторизовать число $n = 5338771$.

При использовании классического метода Ферма мы лишь на 160-м шаге получим нужную конфигурацию: если

$$x = \lfloor \sqrt{n} \rfloor + 160 = 2310 + 160 = 2470,$$

то

$$y^2 = 2470^2 - 5338771 = 762129 = 873^2.$$

Следовательно, $x = 2470, y = 873, x + y = 3343, x - y = 1597$, и

$$5338771 = (2470 - 873)(2470 + 873) = 1597 \cdot 3343.$$

При использовании обобщенного метода Ферма с $k = 8$ уже со второй попытки получим

$$\left(\lfloor\sqrt{kn}\rfloor + 2\right)^2 - kn = \left(\lfloor\sqrt{8 \cdot 5338771}\rfloor + 2\right)^2 - 8 \cdot 5338771 =$$
$$= 6537^2 - 8 \cdot 5338771 = 22201 = 149^2.$$

Таким образом, $h = 6537, t = 149, h - t = 6537 - 149 = 6388$, и

$$(6388, 5338771) = 1597.$$

Отсюда следует, что $n = 1597 \cdot 3343$. □

Поскольку подобрать такое k не всегда легко, на практике для разложения n достаточно найти такие $h, t \in \mathbb{Z}$, что $h^2 \equiv t^2 \pmod{n}$. Если $h \neq \pm t \pmod{n}$, то n делит произведение $(h+t)(h-t)$, но не делит ни один из сомножителей. Из этого следует, что $(h - t, n)$ (как и $(h + t, n)$) является нетривиальным делителем числа n, а значит искомое разложение n на множители найдено. Одно из таких обобщений метода Ферма было предложено Морисом Крайчиком (Maurice B. Kraichik, 1882–1957) [49].

Пример 7.1.6 С помощью метода Крайчика—Ферма разложим число $n = 2041$. Число 46 является первым, чей квадрат больше числа n: $46^2 = 2116$. Вычисляя значение функции $v(u) = u^2 - n$ для $u = 46, 47, \ldots$ мы получим значения $75, 168, 263, 360, 459, 560, \ldots$. Следуя методу Ферма, вычисления нужно продолжать до нахождения полного квадрата. По методу Крайчика—Ферма, будем последовательно искать такие u_k, для которых полным квадратом является произведение $v(u_1)v(u_2)\ldots v(u_k)$. Обозначая $v(u_1)v(u_2)\ldots v(u_k) = y^2$, и $u_1u_2\ldots u_k = x$, мы получим, что

$$x^2 = u_1^2u_2^2\ldots u_k^2 \equiv (u_1^2 - n) \cdot (u_2^2 - n) \cdots (u_k^2 - n) \equiv$$
$$\equiv v(u_1) \cdot v(u_2) \cdots v(u_k) \equiv y^2 \pmod{n}.$$

В нашем случае, записывая разложения

$$75 = 3 \cdot 5^2,\ 168 = 2^3 \cdot 3 \cdot 7,\ 360 = 2^3 \cdot 3^2 \cdot 5,\ 560 = 2^4 \cdot 5 \cdot 7,$$

мы убеждаемся в том, что произведение полученных четырех чисел будет квадратом:

$$75 \cdot 168 \cdot 360 \cdot 560 = (2^5 \cdot 3^2 \cdot 5^2 \cdot 7)^2.$$

Теперь можно вычислить x и y:

$$x = 46 \cdot 47 \cdot 49 \cdot 51 \equiv 311 \pmod{2041},$$
$$y = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \equiv 1416 \pmod{2041}.$$

Далее с помощью алгоритма Евклида находим $(1416 - 311, 2041) = 13$. Таким образом, $2041 = 13 \cdot 157$. □

Мы уже говорили о том, что наибольшая эффективность расчета методом факторизации Ферма достигается в случае, когда множители числа n примерно равны между собой. В наихудшем варианте, когда, к примеру, a близко к n, а b близко к 1, алгоритм Ферма работает медленнее алгоритма последовательных делений, и оценка сложности метода Ферма имеет вид $O(n)$.

Упражнения

1. Факторизуйте числа 15341,6023,16171,126741 методом последовательного деления (воспользуйтесь таблицей простых чисел). Оцените количество выполненных операций.
2. Факторизуйте числа 15341,6023,16171,126741 с помощью модифицированного метода последовательного деления (воспользуйтесь таблицей простых чисел). Оцените количество выполненных операций. Сравните количество выполненных операций для обоих модификаций алгоритма.
3. Факторизуйте числа 391,1189,1073 методом Ферма. Оцените количество выполненных операций.
4. Факторизуйте числа 3551, 2993, 1406303 методом сдвига. Оцените количество выполненных операций. Сравните количество выполненных операций для метода сдвига и метода Ферма.
5. Факторизуйте числа 3551, 2993, 1406303 улучшенным методом Ферма, выбрав k из промежутка $[2, 10]$. Оцените количество выполненных операций. Сравните количество выполненных операций для метода сдвига и метода Ферма; для метода сдвига и улучшенного метода Ферма; для метода Ферма и улучшенного метода Ферма.
6. Подберите коэффициент из промежутка [2, 10] для улучшенного метода Ферма, позволяющего факторизовать 53387714, выполнив не более 3 проверок.
7. Разложите число 25549949 на множители, используя улучшенный метод Ферма.
8. Разложите число 25549949 на множители, используя метод Крайчека—Ферма. Подсчитайте количество выполненных операций. Сравните эффективность метода Ферма и метода Крайчека—Ферма.

Задачи

1. Оцените число шагов в методе Ферма при условии, что мы рассматриваем только составные числа, не делящиеся на 2, 3 и 5.
2. Оцените число шагов в методе Ферма при условии, что мы рассматриваем только составные числа, не делящиеся на 2, 3, 5 и 11.

3 Факторизуйте числа методом последовательного деления (воспользуйтесь таблицей простых чисел):

a) 4757467; d) 1411308; g) 483875; j) 790229;
b) 1966481; e) 217511; h) 232713; k) 422477;
c) 1775171; f) 2320319; i) 370656; l) 405769.

Оцените количество выполненных операций.

4 Факторизуйте числа задачи 3 с помощью модифицированного метода последовательного деления (воспользуйтесь таблицей простых чисел). Оцените количество выполненных операций. Сравните количество выполненных операций для обоих модификаций алгоритма.

5 Факторизуйте числа методом Ферма, методом сдвига, улучшенным методом Ферма:

a) 7031; c) 9991; e) 38407; g) 41989; i) 44377.
b) 6059; d) 39203; f) 39203; h) 47053;

Оцените количество выполненных операций.

6 Разложите числа 21431227, 19534673 на множители, используя улучшенный метод Ферма.

7 Разложите числа 25549949, 21431227, 19534673 на множители, используя метод Крайчека—Ферма. Подсчитайте количество выполненных операций. Сравните эффективность метода Ферма и метода Крайчека—Ферма.

8 Докажите, что существует бесконечно много простых чисел вида $x^2 - y^2$.

9 Представьте первые двадцать натуральных чисел в виде разности двух квадратов натуральных чисел. Всегда ли это можно сделать? Сколько существует таких представлений?

10 Докажите, что нечетное натуральное число является простым тогда и только тогда, когда оно единственным образом представимо в виде разности квадратов двух натуральных чисел. Останется ли верным утверждение, если натуральные числа заменить на целые?

11 Выясните, простым или составным является число 629, рассмотрев представления этого числа в виде разности квадратов.

12 Представьте первые двадцать натуральных чисел в виде суммы двух квадратов натуральных чисел. Всегда ли это можно сделать? Сколько существует таких представлений?

13 Докажите, что не существует ни одного представления натурального числа вида $4k + 3$ в виде суммы $x^2 + y^2$ двух квадратов натуральных чисел.

14 Докажите, что нечетное натуральное число вида $4k+1$ является простым тогда и только тогда, когда оно единственным образом представимо в виде суммы квадратов двух натуральных чисел x^2+y^2, причем $(x, y) = 1$. Останется ли верным утверждение, если натуральные числа заменить на целые? Если отбросить условие $(x, y) = 1$?

15 Натуральное число кратно 4. Обладает ли оно представлением вида x^2+y^2? Обладает ли оно собственным (то есть с $(x, y) = 1$) представлением вида x^2+y^2?

16 Сколько собственных решений имеет уравнение $x^2+y^2 = 3125$?

17 Докажите, что существует бесконечно много простых чисел вида x^2+y^2.

18 Почему нельзя использовать в качестве основания системы *RSA* составное число, являющееся произведением двух простых-близнецов?

7.2. Современные методы факторизации. Вскрытие системы *RSA*

В связи с появлением в современном мире прикладных криптографических задач, связанных с задачей факторизации, но оперирующих с числами, для которых описанные выше методы являются нерациональными, появилась необходимость поиска новых алгоритмов факторизации, эффективных при исследовании очень больших натуральных чисел с помощью компьютеров [24], [22], [29], [49], [53], [68], [95] и др. В этом разделе мы рассмотрим некоторые из них.

7.2.1. Метод Полларда–Флойда

Метод пробных делений на простые числа, меньшие $\sqrt{n}$, в некоторых случаях может потребовать для своей реализации более $O(\sqrt{n})$ двоичных операций.

Простейший алгоритм факторизации, работающий существенно быстрее — *метод Полларда–Флойда* (*ρ-метод Полларда*, *метод Монте-Карло*) [121], [22], [68].

ρ-алгоритм, предложенный Джоном Поллардом (John Pollard, род. 1941) в 1975 г., основан на алгоритме Роберта Флойда (Robert Floyd, 1936–2001) поиска длины цикла в последовательностях. Для его реализации сначала выберем способ легко вычисляемого отображения множества $\mathbb{Z}_n$ классов вычетов по модулю n в себя, то есть некоторый простой многочлен с целыми коэффициентами, например, $f(x) = x^2+1$. (Важно выбрать многочлен $f(x)$ нерегулярным, случайным образом. В частности, он не должен порождать биекции множества $\mathbb{Z}_n$.) Затем выберем некоторое натуральное x_0 (как правило, случайно порожденное число) и построим

последовательность $x_i = f(x_{i-1})$, $i = 1, 2, 3, \ldots$, шаг за шагом сравнивая между собой числа x_i с целью найти два значения, принадлежащие разным классам по модулю n, но одному и тому же классу по модулю некоторого делителя числа n. Как только такие x_i, x_j найдены, сразу находим собственный делитель числа n как $(x_i - x_j, n)$.

Пример 7.2.7 Пользуясь указанным методом, факторизуем число $n=91$. Выберем $f(x) = x^2 + 1$, и $x_0 = 1$. Тогда $x_1 = 2$, $x_2 = 5$, $x_3 = 26, \ldots$. Исследуя разности $x_i - x_j$, обнаружим, что $(x_3 - x_2, 91) = (21, 91) = 7$, т. е. 7 — делитель числа 91. Таким образом, $91 = 7 \cdot 13$. □

Конечно, с ростом k процесс вычисления $(x_k - x_j, n)$ для всех j становится трудоемким. Однако алгоритм можно модифицировать так, чтобы при каждом k вычислять только один наибольший общий делитель. Для доказательства этого факта заметим, что если при некоторых k_0, j_0 для делителя r числа n выполняется сравнение $x_{k_0} \equiv x_{j_0} \pmod r$, то $x_k \equiv \equiv x_j \pmod r$ для любой последующей пары индексов i, j, имеющих ту же разность: $k - j = k_0 - j_0 = m$. (Примените многочлен $f(x)$ к сравнению $x_{i_0} \equiv x_{j_0} \pmod r$ m раз.)

Работу алгоритма можно организовать так. Последовательно вычисляя x_k, на каждом шаге делаем следующее. Пусть k — $(h+1)$-разрядное число в двоичной системе счисления, то есть $2^h \leqslant k < 2^{h+1}$. Пусть j — наибольшее из h-разрядных двоичных чисел, то есть $h = 2^h - 1$. Сравним x_k с x_j, то есть вычислим $(x_k - x_j, n)$. Если в результате получим нетривиальный делитель n, то останавливаемся, если нет, то переходим к $k+1$.

Пример 7.2.8 Факторизуем число 91, как и в предыдущем примере, используя $f(x) = x^2 + 1$, и $x_0 = 1$. Однако теперь будем сравнивать каждое x_k лишь с одним x_j, для которого j — наибольшее из меньших k чисел вида $2^h - 1$. Для $f(x) = x^2 + 1$ имеем $x_0 = 1$, $x_1 = 2$, $x_2 = 5$, $x_3 = 26$ и $x_4 = 40$ (поскольку $26^2 + 1 \equiv 40 \pmod{91}$). Следуя описанному алгоритму, определяем делитель числа n, вычисляя $(x_4 - x_3, 91) = (14, 91) = 7$.

Разложим на множители число 4087, используя $f(x) = x^2 + x + 1$ и $x_0 = 2$. Последовательность действий будет выглядеть так:

1. $x_1 = f(2) = 7$, $(x_1 - x_0, n) = (7 - 2, 4087) = 1$;
2. $x_2 = f(7) = 57$, $(x_2 - x_1, n) = (57 - 7, 4087) = 1$;
3. $x_3 = f(57) = 3307$, $(x_3 - x_1, n) = (3307 - 7, 4087) = 1$;
4. $x_4 = f(57) \equiv 2745 \pmod n$, $(x_4 - x_3, n) = (2745 - 3307, 4087) = 1$;
5. $x_5 = f(2745) \equiv 1343 \pmod n$ $(x_5 - x_3, n) = (1343 - 3307, 4087) = 1$;
6. $x_6 = f(1343) \equiv 2626 \pmod n$, $(x_6 - x_3, n) = (2626 - 3307, 4087) = 1$;
7. $x_7 = f(2626) \equiv 3734 \pmod n$, $(x_7 - x_3, n) = (3734 - 3307, 4087) = 67$.

Таким образом, мы доказали, что число 4087 делится на 67, откуда следует разложение $4087 = 61 \cdot 67$. □

Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении. Сложность алгоритма оценивается как $O(n^{1/4})$.

7.2.2. ($P-1$)-метод Полларда

Этот метод, впервые описанный в 1974 г. [121], быстро находит небольшие простые делители исследуемого числа n и на практике обычно используется до применения субэкспоненциальных алгоритмов факторизации, чтобы исключить такие небольшие простые делители из рассмотрения. Идея метода состоит в следующем.

Пусть $B = \{p_1, p_2, \ldots p_s\}$ — множество различных простых чисел. Назовем его *базой разложения*. Натуральное число назовем *B-гладким*, если все его простые делители принадлежат B.

Пусть n — нечетное составное число, и p — его нетривиальный делитель, для которого число $p-1$ является B-гладким. Другими словами, $n = pq$, и $p-1 = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Найдем максимальные показатели $l_1, \ldots l_s$, для которых $p_i^{l_i} \leqslant n$: прологарифмировав, получим $l_i \log p_i \leqslant \log n$, то есть $l_i \leqslant \dfrac{\log n}{\log p_i}$, и, учитывая условие максимальности, возьмем $l_i = \left\lfloor \dfrac{\log n}{\log p_i} \right\rfloor$.

Пусть $M = p_1^{\left\lfloor \frac{\log n}{\log p_1} \right\rfloor} p_2^{\left\lfloor \frac{\log n}{\log p_2} \right\rfloor} \cdot \ldots \cdot p_s^{\left\lfloor \frac{\log n}{\log p_s} \right\rfloor}$. Тогда $M = (p-1) \cdot z$ для некоторого целого z. Согласно малой теореме Ферма, для любого a, взаимно простого с p, $a^{p-1} \equiv 1 \pmod p$, и, следовательно, $a^{(h-1)z} = a^M \equiv 1 \pmod p$. Таким образом, если $d = (a^M - 1, n)$, то d делится на p.

Для работы алгоритма зададим базу разложения $B = \{p_1, p_2, \ldots p_s\}$ и выберем случайное целое a, $2 \leqslant a \leqslant n-2$. Вычислим $d = (a, n)$. Если $d \neq 1$, то задача решена: d — нетривиальный делитель n.

Если $d = 1$, то найдем число $a^M = a^{p_1^{\left\lfloor \frac{\log n}{\log p_1} \right\rfloor} p_2^{\left\lfloor \frac{\log n}{\log p_2} \right\rfloor} \ldots p_s^{\left\lfloor \frac{\log n}{\log p_s} \right\rfloor}}$, проводя вычисления по модулю n. Для этого, взяв $a = a_0$, при каждом $i = 1, 2, \ldots s$ вычислим $l_i = \left\lfloor \dfrac{\log n}{\log p_i} \right\rfloor$ и найдем $a_i \equiv a_{i-1}^{p_i^{l_i}} \pmod n$; очевидно, что в этом случае $a_s \equiv a^M \pmod n$.

Вычислим $d = (a_s - 1, n) = (a^M - 1, n)$. При $d = 1$ или $d = n$ получаем результат: «Делитель не найден». В остальных случаях d — нетривиальный делитель n, и задача полностью решена.

Пример 7.2.9 Разложим ($p-1$)-методом Полларда число $n = 1728239$ [68]. Пусть $B = \{2, 3, 5\}$. Пусть $a = 2$ — число, очевидно взаимно простое с нечетным n.

Тогда промежуточные вычисления принимают следующий вид:

$$l_1 = \left\lfloor \frac{\log n}{\log 2} \right\rfloor = 20, \quad a_1 \equiv a^{2^{20}} \equiv 1357228 \pmod{n};$$

$$l_2 = \left\lfloor \frac{\log n}{\log 3} \right\rfloor = 13, \quad a_2 \equiv a_1^{3^{13}} \equiv 987665 \pmod{n};$$

$$l_3 = \left\lfloor \frac{\log n}{\log 5} \right\rfloor = 8, \quad a_3 \equiv a_2^{5^8} \equiv 74463 \pmod{n}.$$

Находим $d = (a_3 - 1, n) = (74462, 1728239) = 1201$. Таким образом, 1201 — нетривиальный делитель числа $n = 1728239$, и $1728239 = 1201 \cdot 1439$.

Для разложения числа $n = 1557697$ используем ту же базу $B = \{2, 3, 5\}$ и то же основание $a = 2$. В этом случае промежуточные вычисления примут вид:

$$l_1 = \left\lfloor \frac{\log n}{\log 2} \right\rfloor = 20, \quad a_1 \equiv a^{2^{20}} \equiv 301549 \pmod{n};$$

$$l_2 = \left\lfloor \frac{\log n}{\log 3} \right\rfloor = 12, \quad a_2 \equiv a_1^{3^{12}} \equiv 953296 \pmod{n};$$

$$l_3 = \left\lfloor \frac{\log n}{\log 5} \right\rfloor = 8, \quad a_3 \equiv a_2^{5^8} \equiv 1 \pmod{n}.$$

Находим $d = (a_3 - 1, n) = (0, 1557697) = 1557697$. Таким образом, $d = n$ и нетривиальный делитель не найден. □

Замечание.

1. *Нам удалось получить нетривиальный делитель* 1201 *числа*

$$n = 1728239 = 1201 \cdot 1439$$

$(p-1)$*-методом Полларда с помощью базы* $B = \{2, 3, 5\}$, *поскольку число* 1200 *является* B*-гладким* $(1201 - 1 = 1200 = 2^4 \cdot 3 \cdot 5)$, *а число* $1438 = 1439 - 1$ B*-гладким не является*: $1438 = 2 \cdot 719$.

2. *Равенство* $d = n$ *второго примера означает, что каноническое разложение числа* $q - 1$ *включает в себя те же простые числа, что и разложение числа* $p - 1$. *В силу малой теоремы Ферма* $a^{p-1} \equiv 1 \pmod{p}$, $a^{q-1} \equiv 1 \pmod{q}$, *и, поскольку в этом случае число* M *делится не только на* $p - 1$, *но и на* $q - 1$, *получаем, что* $a^M \equiv 1 \pmod{p}$, $a^M \equiv 1 \pmod{q}$, *следовательно,* $a^b \equiv 1 \pmod{pq}$. *Именно, в нашем случае* $1557697 = 1201 \cdot 1297$, *при этом* $1297 - 1 = 2^4 \cdot 3^4$, *то есть число* 1296 *также является* B*-гладким.*

3. *Если для разложения числа* $n = 3865489$ *строить базу разложения, начиная с малых простых чисел* 2, 3, 5, ..., *то для нахождения нетривиального делителя при случайных значениях* a *потребуется база, содержащая не менее* 162 *простых. Это объясняется тем, что*

$$n = pq = 1907 \cdot 2027, \text{ и } 1907 - 1 = 2 \cdot 953,$$

где 953 — 162*-е простое число* (*при этом* $2027 - 1 = 2 \cdot 1013$). *Однако при выборе* $a \equiv 1 \pmod{n}$ (*или* $a \equiv 1 \pmod{q}$) *мы уже на четвертом шаге получим* $d = (a - 1, n) = p$ (*или* $d = (a - 1, n) = q$).

$(p - 1)$-метод Полларда имеет ограниченную применимость. В частности, он не приведет к успеху, если наименьший из делителей числа n, искомое p — *сильное простое число* (то есть, в нашем случае, число $p - 1$ имеет большие простые делители). Если $p_i \leqslant P$ для $i = 1, 2, \ldots s$, и модульное умножение выполняется в столбик, то сложность указанного алгоритма равна $O(P \log P \log^2 n)$. Абсолютная оценка сложности имеет вид $O(n^{\frac{1}{2}} \log^c n)$. Размер базы определяется исходя из предполагаемого времени работы алгоритма ([53], [68]).

7.2.3. Вскрытие системы *RSA*

Предполагаемая большая вычислительная сложность задачи факторизации лежит в основе криптостойкости ряда алгоритмов шифрования с открытым ключом, например *RSA*. Однако на практике указанная сложность быстро падает. Это обусловлено как развитием вычислительной техники, так и созданием новых методов факторизации.

Рассмотрим основные идеи того направления развития алгоритмов факторизации, которое привело к разложению в 1994 г. 129-разрядного (428-битового) числа, предложенного в 1977 г. создателями *RSA* [24].

Все началось с Ферма, предложившего представлять разлагаемое число n в виде разности квадратов двух натуральных чисел: $n = x^2 - y^2$. Лежандр заметил, что для факторизации n достаточно получить сравнение $x^2 \equiv y^2 \pmod{n}$. Различные способы нахождения таких чисел x и y предлагали Эйлер и Гаусс. Мы рассмотрим метод Лежандра, который использовал для этой цели разложение числа $\sqrt{n}$ в цепную дробь. Для описания алгоритма нам понадобятся некоторые хорошо известные сведения о цепных дробях [20], [36], [106].

Факторизация натуральных чисел и цепные дроби

Цепная дробь $[a_0, a_1, \ldots a_n, \ldots]$ определяется как формальная сумма

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots \cfrac{1}{a_n + \cdots}}},$$

где a_0 — некоторое целое число, а все a_n, $n \in \mathbb{N}$ — натуральные числа, причем последнее, если оно существует, отлично от 1.

Рациональные числа

$$\delta_k = [a_0, a_1, \ldots a_k] = \frac{P_k}{Q_k}, \quad k = 0, 1, \ldots n, \ldots,$$

называются *подходящими дробями* к цепной дроби $[a_0, a_1, \ldots a_n, \ldots]$. Числа a_k, $k = 0, 1, \ldots n, \ldots$, называются *неполными частными* цепной дроби $[a_0, a_1, \ldots a_n, \ldots]$, в то время как величины $\alpha_k = [a_k, a_{k+1}, \ldots a_n, \ldots]$, $k = 0, 1, \ldots n, \ldots$, называются *полными частными* цепной дроби $[a_0, a_1, \ldots a_n, \ldots]$.

Свойства цепных дробей

1. Если $\delta_k = \dfrac{P_k}{Q_k}$, то $P_0 = a_0$, $P_1 = a_1 a_0 + 1$, и $P_n = a_n P_{n-1} + P_{n-2}$ для всех $n \geqslant 2$.
2. Если $\delta_k = \dfrac{P_k}{Q_k}$, то $Q_0 = 1$, $Q_1 = a_1$, и $Q_n = a_n Q_{n-1} + Q_{n-2}$ для всех $n \geqslant 2$.
3. $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$.
4. $P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n a_n$.
5. $(P_n, Q_n) = 1$.
6. $1 = Q_0 \leqslant Q_1 < Q_2 < \ldots$
7. Если $P_0 > 1$, то $P_1 < P_2 < P_3 < \ldots$
8. $\delta_n - \delta_{n-1} = \dfrac{(-1)^{n-1}}{Q_n Q_{n-1}}$.
9. $\alpha = [a_0, a_1, \ldots a_n, \ldots] = \dfrac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}$; $\alpha_n = \dfrac{P_{n-2} - \alpha Q_{n-2}}{\alpha Q_{n-1} - P_{n-1}}$.

Каждая конечная цепная дробь является рациональным числом, и каждое рациональное число представимо, причем единственным образом в виде конечной цепной дроби. Каждая бесконечная цепная дробь является иррациональным числом, и каждое иррациональное число представимо, причем единственным образом в виде бесконечной цепной дроби. Бесконечная цепная дробь является периодической тогда и только тогда, когда она представляет некоторую *квадратическую иррациональность*, то есть иррациональное число, являющееся корнем квадратного трехчлена с целыми коэффициентами.

Пример 7.2.10 Покажем, как на практике оперировать с цепными дробями.

Прежде всего, разложим в цепную дробь числа $\dfrac{173}{281}$ и $\dfrac{1 - 3\sqrt{5}}{2}$.

В первом случае достаточно записать для чисел 173 и 281 алгоритм Евклида:

$$173 = 281 \cdot 0 + 173; \qquad 108 = 65 \cdot 1 + 43; \qquad 22 = 21 \cdot 1 + 1;$$
$$281 = 173 \cdot 1 + 108; \qquad 65 = 43 \cdot 1 + 22; \qquad 21 = 1 \cdot 21 + 0.$$
$$173 = 108 \cdot 1 + 65; \qquad 43 = 22 \cdot 1 + 21;$$

Теперь нетрудно убедиться в том, что

$$\frac{173}{281} = 0 + \frac{1}{\frac{281}{173}}, \frac{281}{173} = 1 + \frac{1}{\frac{173}{108}}, \ldots, \frac{65}{22} = 1 + \frac{1}{\frac{43}{21}}, \frac{43}{21} = 1 + \frac{1}{\frac{22}{21}}, \text{ и } \frac{22}{21} = 1 + \frac{1}{21}.$$

Следовательно,

$$\frac{173}{281} = 0 + \cfrac{1}{1 + \cfrac{1}{\ldots + \frac{1}{21}}},$$

или, что то же, $\dfrac{173}{281} = [0, 1, 1, 1, 1, 1, 1, 21]$. □

Таким образом, *для того, чтобы получить разложение обыкновенной дроби* $\dfrac{P}{Q} \notin \mathbb{Z}$ *в конечную цепную дробь, достаточно выписать алгоритм Евклида для чисел* P *и* Q *и взять столбец полученных при этом целых частных в качестве неполных частных искомой цепной дроби.*

Для разложения числа $\dfrac{1 - 3\sqrt{5}}{2}$ проведем рассуждения, обобщающие алгоритм Евклида.

Поскольку $6 < \sqrt{45} < 7$, то для числа $\dfrac{1 - 3\sqrt{5}}{2}$, равного $\dfrac{1 - \sqrt{45}}{2}$, имеет место оценка

$$-3 < \frac{1 - 3\sqrt{5}}{2} < -2{,}5,$$

то есть $a_0 = \left\lfloor \dfrac{1 - 3\sqrt{5}}{2} \right\rfloor = -3$. Тогда

$$\alpha_0 = \frac{1 - 3\sqrt{5}}{2} = -3 + \frac{1}{\alpha_1}, \quad \text{где} \quad \frac{1}{\alpha_1} = \frac{1 - 3\sqrt{5}}{2} - (-3) = \frac{7 - 3\sqrt{5}}{2}.$$

Следовательно,

$$\alpha_1 = \frac{2}{7 - 3\sqrt{5}} = \frac{2(7 + 3\sqrt{5})}{(7 - 3\sqrt{5})(7 + 3\sqrt{5})} =$$
$$= \frac{2(7 + 3\sqrt{5})}{49 - 45} = \frac{2(7 + 3\sqrt{5})}{4} = \frac{(7 + 3\sqrt{5})}{2}.$$

Поскольку $6{,}5 < \dfrac{(7+3\sqrt{5})}{2} < 7$, то

$$a_1 = \left\lfloor \frac{(7+3\sqrt{5})}{2} \right\rfloor = 6, \quad \text{и} \quad \alpha_1 = \frac{7+3\sqrt{5}}{2} = 6 + \frac{1}{\alpha_2},$$

где

$$\frac{1}{\alpha_2} = \frac{7+3\sqrt{5}}{2} - 6 = \frac{-5+3\sqrt{5}}{2}.$$

Следовательно,

$$\alpha_2 = \frac{2}{-5+3\sqrt{5}} = \frac{2(-5-3\sqrt{5})}{(-5+3\sqrt{5})(-5-3\sqrt{5})} =$$

$$= \frac{2(-5-3\sqrt{5})}{25-45} = \frac{2(5+3\sqrt{5})}{20} = \frac{(5+3\sqrt{5})}{10}.$$

Поскольку $1{,}1 < \dfrac{(5+3\sqrt{5})}{2} < 1{,}2$, то

$$a_2 = \left\lfloor \frac{(5+3\sqrt{5})}{10} \right\rfloor = 1, \quad \text{и} \quad \alpha_2 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_3},$$

где

$$\frac{1}{\alpha_3} = \frac{5+3\sqrt{5}}{10} - 1 = \frac{-5+3\sqrt{5}}{10}.$$

Следовательно,

$$\alpha_3 = \frac{10}{-5+3\sqrt{5}} = \frac{10(-5-3\sqrt{5})}{(-5+3\sqrt{5})(-5-3\sqrt{5})} =$$

$$= \frac{10(-5-3\sqrt{5})}{25-45} = \frac{10(5+3\sqrt{5})}{20} = \frac{(5+3\sqrt{5})}{2}.$$

Поскольку $5{,}5 < \dfrac{(5+3\sqrt{5})}{2} < 6$, то

$$a_3 = \left\lfloor \frac{(5+3\sqrt{5})}{2} \right\rfloor = 5, \quad \text{и} \quad \alpha_3 = \frac{5+3\sqrt{5}}{2} = 5 + \frac{1}{\alpha_4},$$

где

$$\frac{1}{\alpha_4} = \frac{5+3\sqrt{5}}{2} - 5 = \frac{-5+3\sqrt{5}}{2}.$$

Таким образом, $\frac{1}{\alpha_4} = \frac{1}{\alpha_2}$, то есть $\alpha_4 = \alpha_2$. Отсюда следует, что строка, соответствующая α_4, будет дублировать строку, соответствующую α_2:

$$\alpha_4 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_5}, \quad \text{где} \quad \frac{1}{\alpha_5} = \frac{-5+3\sqrt{5}}{10}.$$

В частности, $a_4 = a_2$ и $\frac{1}{\alpha_5} = \frac{1}{\alpha_3}$, то есть $\alpha_5 = \alpha_3$. Продолжая рассуждения, получим, что $a_5 = a_3$ и $\frac{1}{\alpha_6} = \frac{1}{\alpha_4}$, то есть $\alpha_6 = \alpha_4$; $a_6 = a_4$ и $\frac{1}{\alpha_7} = \frac{1}{\alpha_5}$, то есть $\alpha_7 = \alpha_5$, и т. д. Следовательно,

$$\frac{1-3\sqrt{5}}{2} = [a_0, a_1, a_2, a_3, a_4, \ldots] =$$
$$= [-3, 6, 1, 5, 1, 5, 1, 5, \ldots] = [-3, 6, (1, 5)].$$

Формализуя проведенные рассуждения, мы получим алгоритм разложения числа $\frac{1-3\sqrt{5}}{2}$ в цепную дробь: начиная с $\alpha_0 = \frac{1-3\sqrt{5}}{2}$, выписываем цепочку равенств, связывающих числа α_i, $a_i = \lfloor \alpha_i \rfloor$ и $\frac{1}{\alpha_{i+1}} = \alpha_i - a_i$:

$$\alpha_0 = \frac{1-3\sqrt{5}}{2} = -3 + \frac{1}{\alpha_1}, \quad \text{где} \quad \frac{1}{\alpha_1} = \frac{7-3\sqrt{5}}{2};$$
$$\alpha_1 = \frac{7+3\sqrt{5}}{2} = 6 + \frac{1}{\alpha_2}, \quad \text{где} \quad \frac{1}{\alpha_2} = \frac{-5+3\sqrt{5}}{2};$$
$$\alpha_2 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_3}, \quad \text{где} \quad \frac{1}{\alpha_3} = \frac{-5+3\sqrt{5}}{10};$$
$$\alpha_3 = \frac{5+3\sqrt{5}}{2} = 5 + \frac{1}{\alpha_4}, \quad \text{где} \quad \frac{1}{\alpha_4} = \frac{-5+3\sqrt{5}}{2}.$$

Отслеживая правые части получаемых равенств, мы останавливаемся после первого совпадения величин $\frac{1}{\alpha_k}$ и $\frac{1}{\alpha_{k+s}}$ и выписываем значение $[a_0, a_1, a_2, \ldots]$ соответствующей цепной дроби, раскрывая скобку периода после первого совпадения и закрывая ее после второго: $[a_0, a_1, a_2, \ldots a_k, (a_{k+1}, \ldots a_{k+s})]$. Именно, $\frac{1-3\sqrt{5}}{2} = [-3, 6, (1, 5)]$.

А теперь рассмотрим алгоритмы нахождения значений цепных дробей, проводя вычисления для цепных дробей

$$c[1, 2, 3, 1, 1, 5] \text{ и } [1, 2, 1, (1, 1, 1, 4)].$$

Для нахождения значения цепной дроби $[1, 2, 3, 1, 1, 5]$ вспомним, что

$$[a_0, a_1, \ldots a_n] = \frac{P_n}{Q_n},$$

где

$$P_0 = a_0, Q_0 = 1, P_1 = a_1 a_0 + 1, Q_1 = a_1,$$

и

$$P_n = a_n P_{n-1} + P_{n-2}, Q_n = a_n Q_{n-1} + Q_{n-2}$$

для всех $n \geqslant 2$. Для упрощения вычислений удобно добавить в рассмотрение значения

$$P_{-2} = 0,\ P_{-1} = 1;\ Q_{-2} = 1,\ Q_{-1} = 0.$$

Тогда рекуррентные формулы

$$P_n = a_n P_{n-1} + P_{n-2}, Q_n = a_n Q_{n-1} + Q_{n-2}$$

будут иметь место для любого $n \geqslant 0$.

Результаты вычислений удобно оформить в виде таблицы.

n	-2	-1	0	1	2	3	4	5
a_n			1	2	3	1	1	5
P_n	0	1						
Q_n	1	0						

После вычислений таблица примет нижеследующий вид.

n	-2	-1	0	1	2	3	4	5
a_n			1	2	3	1	1	5
P_n	0	1	1	3	10	13	23	128
Q_n	1	0	1	2	7	9	16	89

Таким образом, $[1, 2, 3, 1, 1, 5] = \dfrac{128}{89}$.

Для нахождения значения цепной дроби $[1, 2, (1, 1, 1, 4)]$ сначала найдем значение соответствующей чисто-периодической цепной дроби $[(1, 1, 1, 4)]$.

Это было сделано в предыдущей задаче: мы получили, что

$$[(1, 1, 1, 4)] = \frac{2 + \sqrt{7}}{3}.$$

Заметим, что для цепной дроби $[1, 2, 1, (1, 1, 1, 4)]$ величина $[(1, 1, 1, 4)]$ является третьим полным частным: $[(1, 1, 1, 4)] = \alpha_3$.

Следовательно, для нахождения значения α цепной дроби $[1,2,1,(1,1,1,4)]$ можно воспользоваться формулой

$$\alpha = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}} \text{ при } n = 3 : \alpha = \frac{\alpha_3 P_2 + P_1}{\alpha_3 Q_2 + Q_1}.$$

При этом значения P_2, P_1, Q_2 и Q_1 можно найти, используя соответствующую таблицу.

n	-2	-1	0	1	2
a_n			1	2	1
P_n	0	1	1	3	4
Q_n	1	0	1	2	3

Таким образом,

$$\alpha = \frac{\frac{2+\sqrt{7}}{3} \cdot 4 + 3}{\frac{2+\sqrt{7}}{3} \cdot 3 + 2}.$$

После очевидных преобразований мы получим окончательный результат: $\alpha = \dfrac{40 - \sqrt{7}}{27}$.

Рассмотрим метод факторизации числа n, основанный на теории цепных дробей [22], [24], [29] [53], [89] и др. Поскольку случай, когда n является полным квадратом, для нашего исследования тривиален, то можно считать, что $\sqrt{n}$ — квадратичная иррациональность.

Известно, что квадратичная иррациональность $\sqrt{n}$ разложима в бесконечную периодическую цепную дробь вида ([20], [106])

$$\sqrt{n} = [a_0, (a_1, \ldots a_{n-1}, 2a_0)].$$

По свойствам цепных дробей, n-е полное частное α_n имеет вид

$$\alpha_n = = \frac{P_{n-2} - \alpha Q_{n-2}}{\alpha Q_{n-1} - P_{n-1}}.$$

Проводя несложные преобразования, убедимся, что

$$\alpha_n = \frac{A_n + \sqrt{n}}{B_n},$$

где $A_n = (-1)^{n-1}(P_{n-1}P_{n-2} - nQ_{n-1}Q_{n-2})$, $B_n = (-1)^n(P_{n-1}^2 - nQ_{n-1}^2)$.

Другими словами, *знаменатели B_i полных частных α_i разложения $\sqrt{n}$ в цепную дробь связаны с числителями P_i подходящих дробей $\delta_i = \dfrac{P_i}{Q_i}$ этого разложения соотношением*

$$(-1)^i B_i \equiv P_{i-1}^2 \pmod{n}.$$

В 1971 г. Даниель Шенкс (Daniel Shanks, 1917–1996) предложил использовать эти соотношение для нахождения натуральных x и y, удовлетворяющих сравнению $x^2 \equiv y^2 \pmod{n}$: если вычисления проводить до тех пор, пока при четном i не получится $B_i = R^2$, $R \in \mathbb{N}$, то пара $\langle B_i, R\rangle$ удовлетворяет сравнению $x^2 \equiv y^2 \pmod{n}$ и с ее помощью можно надеяться получить разложение n.

Пример 7.2.11 Разложим этим методом число $n = 77$.

Для этого рассмотрим квадратичную иррациональность $\sqrt{77}$. Число $\sqrt{77}$ разложимо в бесконечную периодическую цепную дробь

$$\sqrt{77} = [a_0, (a_1, \ldots a_{k-1}, 2a_0)].$$

Разложение проводится по стандартной схеме: начиная с $\alpha_0 = \sqrt{77}$, выписываем цепочку равенств, связывающих числа α_i, $a_i = \lfloor \alpha_i \rfloor$ и $\dfrac{1}{\alpha_{i+1}} = \alpha_i - a_i$:

$$\alpha_0 = \sqrt{77} = a_0 + \frac{1}{\alpha_1}, \quad \text{где} \quad \frac{1}{\alpha_1} = a_0 - \sqrt{N}, \quad \text{и} \quad \alpha_1 = \frac{1}{a_0 - \sqrt{N}} = \frac{A_1 + \sqrt{N}}{B_1};$$

$$\alpha_1 = \frac{A_1 + \sqrt{N}}{B_1} = a_1 + \frac{1}{\alpha_2},$$

где

$$\frac{1}{\alpha_2} = a_0 - \frac{A_1 + \sqrt{N}}{B_1}, \quad \text{и} \quad \alpha_2 = \frac{1}{a_0 - \frac{A_1 + \sqrt{N}}{B_1}} = \frac{A_2 + \sqrt{N}}{B_2},$$

и т. д.

Именно,

$$\alpha_0 = \sqrt{77} = 8 + \frac{1}{\alpha_1}, \quad \text{где} \quad \frac{1}{\alpha_1} = \sqrt{77} - 8, \quad \text{и} \quad \alpha_1 = \frac{\sqrt{77} + 8}{13},$$

то есть $A_1 = 8, B_1 = 13$;

$$\alpha_1 = \frac{\sqrt{77} + 8}{13} = 1 + \frac{1}{\alpha_2},$$

где

$$\frac{1}{\alpha_2} = \frac{\sqrt{77} + 8}{13} - 1 = \frac{\sqrt{77} - 5}{13}, \quad \text{и} \quad \alpha_2 = \frac{\sqrt{77} + 5}{4},$$

то есть $A_2 = 5, B_2 = 4$;

$$\alpha_2 = \frac{\sqrt{77}+5}{4} = 3 + \frac{1}{\alpha_3},$$

где

$$\frac{1}{\alpha_3} = \frac{\sqrt{77}+5}{4} - 3 = \frac{\sqrt{77}-7}{13}, \quad \text{и} \quad \alpha_3 = \frac{\sqrt{77}+7}{7},$$

то есть $A_3 = 7, B_3 = 7$;

$$\alpha_3 = \frac{\sqrt{77}+7}{7} = 3 + \frac{1}{\alpha_4},$$

где

$$\frac{1}{\alpha_4} = \frac{\sqrt{77}+7}{7} - 3 = \frac{\sqrt{77}-14}{7}, \quad \text{и} \quad \alpha_4 = \frac{\sqrt{77}+7}{4},$$

то есть $A_4 = 7, B_4 = 4$;

$$\alpha_4 = \frac{\sqrt{77}+7}{4} = 3 + \frac{1}{\alpha_5},$$

где

$$\frac{1}{\alpha_5} = \frac{\sqrt{77}+7}{4} - 3 = \frac{\sqrt{77}-5}{4}, \quad \text{и} \quad \alpha_5 = \frac{\sqrt{77}+5}{13},$$

то есть $A_5 = 5, B_5 = 13$;

$$\alpha_5 = \frac{\sqrt{77}+5}{13} = 1 + \frac{1}{\alpha_5},$$

где

$$\frac{1}{\alpha_5} = \frac{\sqrt{77}+5}{13} - 1 = \frac{\sqrt{77}-8}{13}, \quad \text{и} \quad \alpha_6 = \frac{\sqrt{77}+8}{1},$$

то есть $A_6 = 8, B_6 = 1$;

$$\alpha_7 = \sqrt{77} + 8 = 16 + \frac{1}{\alpha_7},$$

где

$$\frac{1}{\alpha_7} = \sqrt{77} + 8 - 16 = \sqrt{77} - 8, \quad \text{и} \quad \alpha_7 = \frac{\sqrt{77}+8}{1},$$

то есть $A_7 = 8, B_7 = 1$.

Поскольку $\alpha_7 = \alpha_1$, то процесс закончен. Выписывая неполные частные $a_0 = 8, a_1 = 3, \ldots a_7 = 16$ и учитывая выявленную периодичность, мы получим искомое представление $\sqrt{77} = [8, (1, 3, 2, 3, 1, 16)]$. □

Нас интересует последовательность знаменателей B_i чисел α_1. Из наших вычислений следует, что $B_0 = 1$, $B_1 = 13$, $B_2 = 4$, $B_3 = 7$, $B_4 = 4$, $B_5 = 13$, $B_6 = 1$, далее они будут повторяться.

i	0	1	2	3	4	5	6	7	8	9	10	...
B_i	1	13	4	7	4	13	1	13	4	7	4	...

Поиск полных квадратов в последовательности B_i очень быстро даст результат: уже $B_2 = 4 = 2^2$.

Теперь для нахождения решений сравнения $(-1)^n B_n \equiv P_{n-1}^2 \pmod{77}$ нам осталось только найти значение P_1 числителя δ_1 разложения $\sqrt{77}$ в цепную дробь. Это можно сделать непосредственно. Однако можно и воспользоваться уже знакомой нам таблицей.

i	-2	-1	0	1
a_i			8	1
P_i	0	1	8	9

Таким образом, $P_1 = 9$ и, учитывая, что $B_2 = 4 = 2^2$, мы получаем сравнение $(-1)^2 \cdot 2^2 \equiv 9^2 \pmod{77}$. Следовательно, 77 будет делить разность $9^2 - 2^2 = (9-2)\cdot(9+2)$. Вычисляя $(9-2, 77) = 7$, получаем нетривиальный делитель 7 числа 77, а вместе с ним и разложение $77 = 7 \cdot 11$.

Метод цепных дробей Бриллхарта—Моррисона

В 1975 г. Михаэль Моррисон (*Michael A.* Morrison) и Джон Бриллхарт (John David Brillhart, род. 1930) предложили, для улучшения описанного метода, перемножать сравнения $P_{i-1}^2 \equiv (-1)^i B_i \pmod{n}$ при различных i, чтобы получить квадрат целого числа в правой части [111].

Этот метод, названный *методом цепных дробей* (*алгоритмом Бриллхарта—Моррисона*) позволил разложить на множители седьмое число Ферма $F_7 = 2^{128} + 1$.

В современной трактовке метод выглядит так.

Для реализации алгоритма, применяемого к числу n, строится база $\{p_1, p_2, \ldots p_s\}$, элементы которой p_i — простые числа, ограниченные некоторым параметром, выбранные так, чтобы число n являлось квадратичным вычетом по каждому из модулей p_i: $\left(\frac{n}{p_i}\right) = 1$, $i = 1, 2, 3, \ldots s$.

Собственно алгоритм состоит из двух этапов: сбора данных и обработки получаемой матрицы.

На первом этапе каждое из получаемых в ходе разложения $\sqrt{n}$ в цепную дробь чисел B_i делится на все числа базы и, если не разлагается в произведение степеней этих простых, отбрасывается. Если же в ходе проверки мы получаем разложение $(-1)^i B_i = (-1)^{b_0} \prod_{j=1}^{s} p_j^{b_j}$, то данному номеру i ставится в соответствие вектор $(b_0, b_1, \ldots b_s)$ — вектор показателей разложения числа B_i по факториальной базе.

Вычисления производятся до тех пор, пока не будет построено $s + 2$ вектора показателей.

На втором этапе мы строим из полученных векторов матрицу показателей и подбираем несколько векторов-строк матрицы таким образом, чтобы их сумма была вектором с четными координатами: $2(c_0, c_1, \ldots c_s)$.

Если Δ — множество номеров строк, вошедших в эту сумму, то из сравнения $P_{i-1}^2 \equiv (-1)^i B_i \pmod{n}$ следует, что

$$\left(\prod_{i \in \Delta} P_{i-1}\right)^2 \equiv \left(\prod_{j=1}^{s} p_j^{c_j}\right)^2 \pmod{n},$$

что в большинстве случаев ведет к нахождению нетривиального делителя n и, следовательно, к разложению числа n.

Если же с помощью этого сравнения разложить n не удается, то мы вновь переходим к первому этапу, то есть, продолжая разложение числа $\sqrt{n}$ в цепную дробь, продолжаем выбор векторов показателей и т. д.

Как и в случае метода Ферма, для ускорения процесса вычислений вместо $\sqrt{n}$ можно рассматривать $\sqrt{kn}$, где k мало и подбирается так, чтобы в базу вошли все малые простые числа.

Оценка сложности метода цепных дробей имеет вид

$$O(\exp(\sqrt{1,5 \cdot \log n} \cdot \sqrt{\log \log n})).$$

Это говорит о том, что данный алгоритм является *субэкспоненциальным*. Этот результат был получен в 1982 г. При доказательстве использовались правдоподобные, но не доказанные гипотезы о распределении простых чисел.

Метод квадратичного решета

В 1982 г. Карлом Померанцем (Carl Bernard Pomerance, род. 1944) был предложен *алгоритм квадратичного решета* с оценкой сложности

$$O\left(\exp\left(\sqrt{\frac{9}{8} \cdot \log n \cdot \log \log n}\right)\right),$$

то есть еще один субэкспоненциальный метод факторизации натуральных чисел.

Он базируется на той же идее нахождения двух натуральных чисел, являющихся квадратами по модулю n. В случае квадратичного решета поиск ведется среди чисел, имеющих форму

$$V(x) = (x + m)^2 - n, \quad \text{где } m = \lceil N \rceil.$$

Пример 7.2.12 Факторизуем методом квадратичного решета число $n = 15347$ [128]. Наименьшее число, квадрат которого больше n, равно 124. Следовательно, $V(x) = (x + 124)^2 - 15347$. □

Этап I: сбор данных.

Так как n мало, то для постороения базы не требуется много простых чисел. Первые 4 простых числа p, для которых 15347 является квадратичным вычетом, равны 2, 17, 23 и 29; они и будут формировать базу нашего квадратичного решета.

Построение решета начнем с формирования массива, с которым будем работать: выберем для просеивания первые сто чисел вида

$$V(x) = (x + \lceil \sqrt{n} \rceil)^2 - n = (x + 124)^2 - 15347.$$

Их значения представлены в таблице.

V(0)	V(1)	V(2)	V(3)	V(4)	V(5)	V(6)	V(7)	⋯	V(71)	⋯	V(99)
29	278	529	782	1037	1294	1553	1614	⋯	22678	⋯	34382

Следующим шагом является выполнение просеивания. Для каждого p из факторной базы $\{2, 17, 23, 29\}$ решим сравнение $V(x) = (x+\lceil\sqrt{n}\rceil)^2 - n \equiv 0 \pmod{p}$; это необходимо для нахождения элементов массива, делящихся на p.

Для $p = 2$ сравнение $(x + 124)^2 - 15347 \equiv 0 \pmod 2$ имеет очевидное решение $x \equiv 1 \pmod 2$. Таки образом, начиная с $V(1)$, каждый второй элемент массива будет делиться на 2. Осуществив данное деление, получим модифицированный массив, представленный в таблице.

V(0)	V(1)	V(2)	V(3)	V(4)	V(5)	V(6)	V(7)	⋯	V(71)	⋯	V(99)
29	139	529	391	1037	647	1553	807	⋯	11339	⋯	17191

Для простого числа 17 сравнение $(x + 124)^2 - 15347 \equiv 0 \pmod 7$ имеет два решения $x \equiv 3, 4 \pmod{17}$. Каждое из сравнений $x \equiv a \pmod{17}$ приводит к тому, что $V(x)$ делится на 17 при $x = a, a + p, a + 2p$, и т. д.

Осуществив указанное деление, перейдем к новому массиву, представленному в нижеследующей таблице.

V(0)	V(1)	V(2)	V(3)	V(4)	V(5)	V(6)	V(7)	···	V(71)	···	V(99)
29	139	529	23	61	647	1553	807	···	667	···	17191

Для простого числа 23 сравнение $(x+124)^2-15347\equiv 0 \pmod 7$ имеет два решения $x\equiv 2, 3 \pmod{23}$. Действуя аналогичным образом, переходим к следующему массиву.

V(0)	V(1)	V(2)	V(3)	V(4)	V(5)	V(6)	V(7)	···	V(71)	···	V(99)
29	139	23	1	61	647	1553	807	···	29	···	17191

Наконец, для простого числа 29 сравнение $(x+124)^2-15347\equiv 0 \pmod 7$ имеет два решения $x\equiv 0, 13 \pmod{23}$. Действуя аналогичным образом, переходим к следующему массиву.

V(0)	V(1)	V(2)	V(3)	V(4)	V(5)	V(6)	V(7)	···	V(71)	···	V(99)
1	139	23	1	61	647	1553	807	···	1	···	17191

Элементы последнего массива, равные 1, соответствуют числам $V(x)$, гладким относительно заданной факторной базы: очевидно, что такие $V(x)$ состоят только из простых чисел, базе принадлежащих. В нашем случае гладкими оказались числа $V(0), V(3)$ и $V(71)$.

x	$x+124$	$y=V(x)$	Факторизация y
0	124	29	$2^0\cdot 17^0\cdot 23^0\cdot 29^1$
3	127	782	$2^1\cdot 17^1\cdot 23^1\cdot 29^0$
71	195	22678	$2^1\cdot 17^1\cdot 23^1\cdot 29^1$

Итак, в процессе просеивания мы получили три гладких относительно заданной факторной базы числа вида $(x+\lceil\sqrt{n}\rceil)^2-n$. Первый этап завершен.

Этап II: *обработка матрицы.*

Рассмотрим равенства

$$29=2^0\cdot 17^0\cdot 23^0\cdot 29^1,$$

$$782=2^1\cdot 17^1\cdot 23^1\cdot 29^0,$$

$$22678=2^1\cdot 17^1\cdot 23^1\cdot 29^1,$$

выпишем показатели простых чисел, входящих в канонические разложения чисел 29, 782 и 22628 в виде векторов длины четыре и составим

из полученных векторов матрицу

$$\begin{pmatrix} 0\,0\,0\,1 \\ 1\,1\,1\,0 \\ 1\,1\,1\,1 \end{pmatrix}.$$

Для того чтобы выбрать среди строк матрицы несколько строк таким образом, чтобы получить в сумме четный вектор, решим систему:

$$(s_1, s_2, s_2) \cdot \begin{pmatrix} 0\,0\,0\,1 \\ 1\,1\,1\,0 \\ 1\,1\,1\,1 \end{pmatrix} \equiv \Big(0, 0, 0, 0\Big) \pmod 2.$$

В нашем случае решением данной системы является вектор $\Big(1, 1, 1\Big)$, то есть сумма всех трех строк матрицы дает четный вектор, и, следовательно, что произведение всех трех выделенных ранее гладких чисел является полным квадратом: $29 \cdot 782 \cdot 22678 = 22678^2$. Таким образом, мы получили равенство

$$V(0)V(3)V(71) = (124^2 - 15347)(127^2 - 15347)(195^2 - 15347) = 3070860^2.$$

Переходя к сравнениям по модулю 15347, получим, что

$$124^2 \cdot 127^2 \cdot 195^2 \equiv 3070860^2 \pmod{15347},$$

или, что то же, $22678^2 \equiv 3070860^2 \pmod{15347}$. Задача нахождения двух натуральных чисел, квадраты которых сравнимы по модулю 15347, полностью решена.

Завершим работу. Поскольку $(3070860 - 22678, 15347) = 103$, то 103 является нетривиальным делителем числа 15347. Это ведет к разложению $15347 = 103 \cdot 149$.

Сегодня есть основания полагать, что метод квадратичного решета является наилучшим из известных алгоритмов факторизации для $n < 10^{110}$.

Именно одна из модификаций этого метода позволила команде математиков под руководством Арьена Ленстры (Arjen Klaas Lenstra, род. 1956) разложить на множители 129-разрядное (428 битовое) число N, представляющее собой произведение двух простых и использованное при построении первого шифротекста в системе *RSA*. Именно, исследованию подвергалось число $5N$. Факториальная база состояла из 524338 простых чисел, меньших 16333609. В результате просеивания получилось 6881738

соотношений для элементов рабочего массива. Это заняло 220 дней и потребовало работы большого числа компьютеров. На второй шаг алгоритма ушло всего 45 часов: уже 4-ый вектор с четными показателями привел к искомому разложению.

В печати достаточно часто появляются новые работы, содержащие алгоритмы факторизации с экспоненциальной сложностью. Однако практическая значимость таких алгоритмов, как правило, невелика. Наиболее популярными в практических вычислениях являются методы Полларда. Они используются в сочетании с субэкспоненциальными методами факторизации и применяются, как правило, для предварительного отделения небольших простых делителей у факторизуемого числа.

В настоящее время исследования в области построения быстрых алгоритмов факторизации интенсивно ведутся во всем мире. Ежегодно проводятся десятки конференций по этой тематике, достигаются новые рекорды факторизации длинных чисел, исследуются известные проблемы алгоритмической теории чисел и ставятся новые проблемы. В конце 2009 г. коллективом европейских ученых был установлен новый рекорд по разложению 768-битового натурального числа с помощью метода решета числового поля. Предыдущий рекорд в 512-бит был установлен в 2000 г., т. е. переход от 512-битовых к 768-битовым числам потребовал почти 10 лет. Поэтому следующий рекорд в 1024 бита при сохранении прежних темпов роста исследований планируется выполнить не ранее, чем в 2020 г [128].

Упражнения

(1) Разложите в цепную дробь числа:

a) $\frac{2015}{1999}$; c) $\sqrt{23}$; e) $\frac{10000}{9999}$; g) $\sqrt{23}$; j) $-\sqrt{31}$;
h) $-\sqrt{23}$; k) $\sqrt{41}$;
b) $-\frac{1961}{1812}$; d) $-\frac{1941}{2011}$; f) $-\sqrt{21}$; i) $\sqrt{31}$; l) $-\sqrt{41}$.

(2) Найдите значение цепной дроби:

a) $[1, 2, 3, 4, 5]$; i) $[5, (10)]$; q) $[3, (3, 6)]$;
b) $[2, 2, 2, 3, 3]$; j) $[6, (12)]$; r) $[4, (1, 8)]$;
c) $[3, 1, 1, 2, 2, 9]$; k) $[7, (14)]$; s) $[4, (2, 8)]$;
d) $[7, 1, 3, 1, 1, 2]$; l) $[8, (16)]$; t) $[3, (10, 5)]$;
e) $[1, (2)]$; m) $[2, (1, 4)]$; u) $[3, (1, 5)]$;
f) $[2, (4)]$; n) $[2, (2, 4)]$; v) $[3, (4, 1)]$;
g) $[3, (6)]$; o) $[3, (1, 6)]$; w) $[5, (2, 10)]$;
h) $[4, (8)]$; p) $[3, (2, 6)]$; x) $[-3, 6, (1, 5)]$.

③ Разложите числа на множители, используя ρ-метод Полларда:

a) 235; b) 407; c) 611.

④ Разложите числа на множители, используя $(p-1)$-метод Полларда:

a) 5917; c) 6887; e) 78667; g) 91643; i) 36079.
b) 7957; d) 49771; f) 11413; h) 79213;

⑤ Разложите числа на множители, используя метод цепных дробей:

a) 437; b) 713; c) 6887; d) 7387.

⑥ Разложите числа на множители, используя модифицированный метод цепных дробей:

a) 2279; b) 1591; c) 2867; d) 3763.

⑦ Разложите число 2355343 на множители, используя метод квадратичного решета.

Задачи

[1] Разложите числа на множители, используя ρ-метод Полларда:

a) 66124207; b) 35677933; c) 21478022263.

[2] Разложите числа на множители, используя $(p-1)$-метод Полларда:

a) 8644409; b) 17095777; c) 4839315539.

[3] Разложите числа на множители, используя метод цепных дробей:

a) 2355343; b) 6105409; c) 27658343.

[4] Разложите числа 6105409, 27658343 на множители, используя метод квадратичного решета.

[5] Выберите два трехзначных простых числа и найдите их произведение. Осуществите факторизацию полученного числа каждым из описанных в разделе методов. Сравните число выполненных операций.

[6] Выберите трехзначное и четырехзначное простые числа и найдите их произведение. Осуществите факторизацию полученного числа каждым из описанных в разделе методов. Сравните число выполненных операций.

[7] Разложите на множители число $n = 46648A118EA35141F5_{16}$, если открытый показатель $e = 5$ и сообщения m_1, m_2 связаны соотношением $m_2 = \alpha m_1 + \beta \pmod n$, где $\alpha = 3039_{16}$, $\beta = 12AFF_{16}$ и соответствующие шифротексты $c_1 = 11FFE80B617C5CEFC1_{16}$, $c_2 = 2D1BD236C7D4B841F3_{16}$.

8 Докажите, что описанные в этом разделе методы факторизации будут неэффективны для чисел, являющихся степенями простых чисел.

9 Обоснуйте следующий алгоритм распознавания чисел $n = p^\alpha$, $\alpha > 1$. Для некоторого случайным образом выбранного числа a проверяем выполнимость соотношения $(a^n - a, n) = 1$. В случае положительного ответа можем утверждать, что $n \neq p^\alpha$. В случае отрицательного ответа либо раскладываем n на множители (если $(a^n - a, n) < n$), либо выбираем другое число a и повторяем процедуру. Если после нескольких попыток прояснения ситуации не произошло, объявляем число n степенью простого и пытаемся его факторизовать с помощью извлечения корня второй, третьей, пятой и т. д. степени.

10 Пусть n — нечетное число, не являющееся степенью простого числа. Пусть $1 \leqslant x, y \leqslant n-1$ — случайным образом выбранная пара натуральных чисел, такая что $(x, n) = (y, n) = 1$, и $x^2 \equiv y^2 \pmod{n}$. Докажите, что вероятность события $1 < (x \pm y, n) < n$ будет не меньше $\frac{1}{2}$ [22].

11 Опишите алгоритм факторизации Диксона и разложите с его помощью на множители три выбранных вами составных числа [22].

Литература к главе 7

При подготовке текста главы 7 были использованы следующие источники [2], [4], [13], [20], [22], [24], [29], [36], [40], [49], [52], [53], [55], [57], [68], [71], [74], [75], [88–91], [95], [97], [98], [100], [104–106], [108], [111], [121], [124–128].

Глава 8

Псевдослучайные последовательности над конечным полем

Симметричные криптосистемы — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования симметричное шифрование являлось единственным способом получения шифротекстов. Исторические аспекты симметричных шифров мы рассмотрели в первой главе. Однако не следует думать, что с появлением системы *RSA* и других асимметричных шифров практическая востребованность симметричных шифров сошла на нет. Сегодня симметричные алгоритмы шифрования и дешифрования данных широко применяются в компьютерных системах сокрытия конфиденциальной и коммерческой информации и подразделяются на два основных класса: *блочные шифры* и *потоковые шифры*.

Блочные шифры оперируют группами бит фиксированной длины — блоками, размер которых меняется в пределах 64–256 бит. Фактически блочный шифр представляет собой подстановку на алфавите блоков, которая, как следствие, может быть моно- или полиалфавитной. Блочные шифры являются важной компонентой многих криптографических протоколов и широко используются для защиты данных, передаваемых по сети.

В *поточных криптосистемах* шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования, заключающегося в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Суммирование обычно выполняется в каком-либо конечном поле.

Конечные поля, и прежде всего поля $\mathbb{F}_{2^n}$, широко применяются сегодня как в разработке теоретических основ современных криптосистем, так и при практической реализации новых криптографически стойких шифров.

8.1. Поля и кольца классов вычетов. Характеристика конечного поля

8.1.1. Кольца и поля. Примеры

Система $\mathbb{K} = \langle K, +, \cdot, 0\rangle$ называется *кольцом*, если выполнены следующие условия:

- $\langle K, +, 0\rangle$ — *коммутативная группа*, то есть операция сложения $+$ ассоциативна и коммутативна, 0 — нейтральный элемент по сложению, и для любого элемента $a \in K$ существует противоположный ему элемент $-a \in K$;
- $\langle K\backslash\{0\}, \cdot\rangle$ — *полугруппа*, то есть операция умножения $\cdot$ ассоциативна;
- операция умножения дистрибутивна относительно операции сложения.

Если, кроме того, операция умножения $\cdot$ коммутативна, то кольцо $\mathbb{K} = \langle K, +, \cdot, 0\rangle$ называют *коммутативным*; если же по умножению существует нейтральный элемент 1, то кольцо $\mathbb{K} = \langle K, +, \cdot, 0, 1\rangle$ называют *кольцом с единицей*.

Система $\mathbb{F} = \langle F, +, \cdot, 0, 1\rangle$ называется *полем*, если

- $\langle F, +, 0\rangle$ — коммутативная группа, то есть операция сложения $+$ ассоциативна и коммутативна, 0 — нейтральный элемент по сложению, и для любого элемента $a \in F$ существует противоположный ему элемент $-a \in F$;
- $\langle F\backslash\{0\}, \cdot, 1\rangle$ — коммутативная группа, то есть операция умножения $\cdot$ ассоциативна и коммутативна, 1 — нейтральный элемент по умножению, и для любого элемента $a \in F\backslash\{0\}$ существует обратный ему элемент $a^{-1} \in F\backslash\{0\}$;
- операция умножения дистрибутивна относительно операции сложения.

Другими словами, полем называется коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим. Обозначим множество $F\backslash\{0\}$ ненулевых элементов поля символом F^*. Из определения поля следует, что система $\langle F^*, \cdot, 1\rangle = \langle F\backslash\{0\}, \cdot, 1\rangle$ является коммутативной группой. Ее называют *мультипликативной группой* поля $\mathbb{F}$.

Пример 8.1.1 Нам хорошо знакомы числовые поля $\mathbb{Q} = \langle \mathbb{Q}, +, \cdot, 0, 1\rangle$, $\mathbb{R} = \langle \mathbb{R}, +, \cdot, 0, 1\rangle$ и $\mathbb{C} = \langle \mathbb{C}, +, \cdot, 0, 1\rangle$ рациональных, действительных и комплексных чисел соответственно. Каждое из них имеет бесконечно много элементов. Система целых чисел $\mathbb{Z} = \langle \mathbb{Z}, +, \cdot, 0, 1\rangle$ является кольцом (и даже коммутативным кольцом с единицей), но не полем: обратный элемент существует лишь для единицы: $1^{-1} = 1$, так как $1 \cdot 1 = 1$. □

Поле $\mathbb{F} = \langle F, +, \cdot, 0, 1\rangle$ называется *конечным*, если множество F является конечным. Для обозначения конечного поля из q элементов будем использовать символ $\mathbb{F}_q$.

Наиболее простым и известным примером конечного поля является поле классов вычетов по простому модулю p.

Классом вычетов (числа a) по модулю n называется множество

$$\mathbf{a}_n = \{x \in \mathbb{Z} : x \equiv a \pmod n\} = \{\ldots a-2n, a-n, a, a+n, a+2n, a+3n, \ldots\}$$

всех целых чисел, сравнимых с данным числом a по модулю n. (При работе с конкретным модулем n вместо символа $\mathbf{a}_n$ обычно используется символ $\mathbf{a}$, или, если принадлежность множеству классов вычетов ясна из контекста, просто символ a.)

Поскольку отношение сравнимости на множестве целых чисел является отношением эквивалентности, то фактор-множество $\mathbb{Z}_n$ всех классов вычетов по модулю n превращается в коммутативное кольцо с единицей, содержащее n элементов. Операции в $\mathbb{Z}_n$ индуцируются операциями в $\mathbb{Z}$: $\mathbf{a}_n + \mathbf{b}_n = (\mathbf{a}+\mathbf{b})_n$; $\mathbf{a}_n \cdot \mathbf{b}_n = (\mathbf{a}\cdot\mathbf{b})_n$; $\mathbf{0} = \mathbf{0}_n$; $\mathbf{1} = \mathbf{1}_n$.

Для простого числа p множество $\mathbb{Z}_p$ с заданными операциями сложения и умножения образует поле, то есть множество $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{\mathbf{0}\}$ ненулевых классов вычетов по модулю p образует коммутативную группу по умножению.

Это означает, что *для каждого простого числа p существует конечное поле, содержащее p элементов*. Поскольку множество простых бесконечно, мы можем утверждать, что *существует бесконечно много конечных полей.*

Пример 8.1.2 Рассмотрим множество $\mathbb{Z}_3 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$. Легко убедиться в том, что таблицы сложения и умножения классов вычетов по модулю 3 имеют нижеследующий вид.

- Таблица сложения в $\mathbb{Z}_3$:

$+$	**0**	**1**	**2**
0	**0**	**1**	**2**
1	**1**	**2**	**0**
2	**2**	**0**	**1**

- Таблица умножения в $\mathbb{Z}_3$:

$\cdot$	**0**	**1**	**2**
0	**0**	**0**	**0**
1	**0**	**1**	**2**
2	**0**	**2**	**1**

Пользуясь этими таблицами, легко доказать, что множество $\mathbb{Z}_3$ с заданными на нем операциями сложения и умножения образует поле. В частности, единичным элементом системы $\langle \mathbb{Z}_3, +, \cdot, \mathbf{0}, \mathbf{1}\rangle$ является класс $\mathbf{1}$, и всякий ненулевой элемент множества $\mathbb{Z}_3$ имеет обратный: $\mathbf{1}^{-1} = \mathbf{1}$ (так как $\mathbf{1}\cdot\mathbf{1} = \mathbf{1}$), и $\mathbf{2}^{-1} = \mathbf{2}$ (так как $\mathbf{2}\cdot\mathbf{2} = \mathbf{1}$).

Решая в $\mathbb{Z}_3$ уравнения $\mathbf{2} \cdot \mathbf{x} = \mathbf{1}$ и $\mathbf{x}^2 - \mathbf{1} = \mathbf{0}$, пользуясь построенной выше таблицей умножения, найдем в строке элемента **2** элемент **1**: таким образом, **1** получается при умножении **2** и **2**, то есть $\mathbf{x} = \mathbf{2}$. Для решения второго уравнения найдем на главной диагонали(именно эти элементы представляют квадраты) **1**. Таким образом, уравнение $\mathbf{x}^2 - \mathbf{1} = \mathbf{0}$ имеет два решения: $\mathbf{x} = \mathbf{1}$, $\mathbf{x} = \mathbf{2}$. □

Теперь рассмотрим множество $\mathbb{Z}_4 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$. Легко убедиться в том, что таблицы сложения и умножения его элементов имеют нижеследующий вид.

- Таблица сложения в $\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Таблица умножения в $\mathbb{Z}_4$:

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Учитывая, что операции сложения и умножения классов вычетов по модулю n обладают свойствами ассоциативности, коммутативности и дистрибутивности, мы можем утверждать, что система $\langle \mathbb{Z}_4, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$ образует коммутативное кольцо с единицей.

Пользуясь таблицей, нетрудно проверить, что единичным элементом системы $\langle \mathbb{Z}_4, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$ является класс **1**, однако не всякий ненулевой элемент множества $\mathbb{Z}_4$ имеет обратный: $\mathbf{1}^{-1} = \mathbf{1}$ (так как $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$), $\mathbf{3}^{-1} = \mathbf{3}$ (так как $\mathbf{3} \cdot \mathbf{3} = \mathbf{1}$), но класс **2** не имеет обратного, поскольку $\mathbf{2} \cdot \mathbf{a} \neq \mathbf{1}$ для $\mathbf{a} \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$. Таким образом, поля система $\langle \mathbb{Z}_4, +, \cdot \rangle$ не образует.

Убедиться в том, что в случае модуля 4 поля мы не получили, можно и пользуясь тем, что в кольце классов вычетов по модулю 4 имеются *делители нуля*: ненулевые элементы a и b, произведение которых $a \cdot b = 0$. Таблица умножения позволяет утверждать, что единственным делителем нуля кольца $\langle \mathbb{Z}_4, +, \cdot \rangle$ является класс **2**: $\mathbf{2} \cdot \mathbf{2} = \mathbf{0}$. Поскольку поле делителей нуля содержать не может, то задача полностью решена.

Решая в $\mathbb{Z}_4$ уравнения $\mathbf{3} \cdot \mathbf{x} = \mathbf{2}$ и $\mathbf{x}^2 + \mathbf{1} = \mathbf{0}$, пользуясь таблицей, находим, что решением первого уравнения является класс **2**. Второе уравнение, равносильное уравнению $\mathbf{x}^2 = \mathbf{2}$, решений не имеет, так как на главной диагонали таблицы нет элемента **2**.

Заметим, что класс **2** — единственный ненулевой класс, не взаимно простой с модулем 4. Нетрудно проверить, что именно ненулевые классы, не взаимно простые с модулем, и только они, являются, с одной стороны,

делителями нуля, и, с другой стороны, необратимы в кольце классов вычетов по составному модулю n. Поскольку для простого модуля p все ненулевые элементы множества $\mathbb{Z}_p$ взаимно просты с модулем, то для каждого из них существует обратный, что и ведет к образованию структуры поля.

8.1.2. Натуральные кратные элементов поля и характеристика поля

Для поля $\mathbb{F} = \langle F, +, \cdot, 0, 1\rangle$ определим *натуральное кратное* $n * a$ элемента $a \in F$ как сумму n копий элемента a: $n*a = \sum_{i=1}^{n} a$, $a \in F$, $n \in \mathbb{N}$. (Можно ли определить натуральные кратные для элементов произвольного кольца?)

Пример 8.1.3 Так, для поля $\mathbb{Q}$ рациональных чисел натуральными кратными единицы будут натуральные числа 1, 2, 3, 4, 5, 6, ..., натуральными кратными двойки будут четные натуральные числа 2, 4, 6, 8, 10, ..., в то время как натуральными кратными числа $\frac{1}{2}$ будут рациональные числа $\frac{1}{2}$, 1, $\frac{3}{2}$, 2, $\frac{5}{2}$, ... Нетрудно убедиться, что все натуральные кратные рационального числа, отличного от нуля, различны.

Для поля $\mathbb{Z}_5$ натуральными кратными единичного элемента **1** будут классы вычетов **1**, **2**, **3**, **4**, **5** = **0**, **6** = **1**, ... Натуральными кратными элемента **3** будут классы вычетов **3**, **6** = **1**, **9** = **4**, **12** = **2**, **15** = **0**, **18** = **3**, ... В отличие от предыдущего случая $5*\mathbf{1} = \mathbf{0}$ и $5*\mathbf{3} = \mathbf{0}$, а затем значения кратных периодически повторяются. □

Это не случайно. Оказывается, *в конечном поле* $\mathbb{F}_q = \langle F, +, \cdot, 0, 1\rangle$ *для любого элемента* a *из* F *выполняется соотношение* $q * a = 0$. (Этот результат следует из *теоремы Лагранжа* [60], утверждающей, что число элементов любой подгруппы конечной группы делит число элементов группы.) В частности, $q * 1 = 0$, где 1 — единица поля.

Рассмотрим произвольное поле $\mathbb{F} = \langle F, +, \cdot, 0, 1\rangle$. Если $m * 1 \neq 0$ для любого натурального m, то *характеристикой* поля $\mathbb{F}$ называют число 0 и говорят, что $\mathbb{F}$ — *поле нулевой характеристики*. Если же $m * 1 = 0$ для какого-либо натурального числа m, то *характеристикой поля* $\mathbb{F}$ называют наименьшее такое m и говорят, что $\mathbb{F}$ — поле характеристики m.

Пример 8.1.4 Поле $\mathbb{Q}$ рациональных чисел является классическим примером поля нулевой характеристики, поскольку, как было показано выше, ни одно из натуральных кратных 1, 2, 3, 4, 5, 6, ... единичного элемента поля, числа 1, не равно нулю.

Поле классов вычетов $\mathbb{Z}_5$ является полем характеристики 5, поскольку $5 * 1 = 0$, и $k * 1 \neq 0$ для $k \in \{1, 2, 3, 4\}$. Аналогично, $\mathbb{Z}_2$ — поле характеристики 2, $\mathbb{Z}_3$ — поле характеристики 3, $\mathbb{Z}_7$ — поле характеристики 7 и, для любого простого числа p, $\mathbb{Z}_p$ — поле характеристики p.

Множество рациональных функций

$$\mathbb{Q}(x) = \left\{ \frac{a_m x^m + \ldots + a_{m+n} x^{m+n}}{b_k x^k + \ldots + b_{k+l} x^{k+l}}, \text{ где } a_i, b_j \in \mathbb{Z}_p, a_m \cdot a_{m+n} \cdot b_k \cdot b_{k+l} \neq 0 \right\}$$

над полем $\mathbb{Z}_p$ с заданными на нем обычными сложением и умножением является примером бесконечного поля конечной характеристики: поскольку единицей данного поля является единичный элемент поля $\mathbb{Z}_p$, то, очевидно, характеристика поля рациональных функций над полем $\mathbb{Z}_p$ совпадает с характеристикой поля $\mathbb{Z}_p$ и равна p. □

Во всех рассмотренных примерах полей ненулевой характеристики их характеристика равнялась простому числу. Это неслучайно. Оказывается, имеет место общее утверждение: *характеристика поля ненулевой характеристики есть число простое*. Его доказательство несложно: если составное число $m = ab, 1 < a \leqslant b < m$, то, пользуясь свойствами кратных, получим, что $m * 1 = (a * 1) \cdot (b * 1) = a \cdot b = 0$, то есть произведение $a \cdot b = 0$ для не равных нулю элементов a и b из F; следовательно, элементы a и b являются делителями нуля, что в поле невозможно.

8.1.3. Расширения конечного поля. Существование конечного поля

Поле $\mathbb{F} = \langle F, +, \cdot, 0, 1 \rangle$ называется *подполем* поля $\mathbb{H} = \langle H, +, \cdot, 0, 1 \rangle$, если $F \subset H$. В этом случае поле $\mathbb{H} = \langle H, +, \cdot, 0, 1 \rangle$ называется *расширением поля* $\mathbb{F} = \langle F, +, \cdot, 0, 1 \rangle$. Если поле $\mathbb{F}$ не имеет несобственных (то есть отличных от самого $\mathbb{F}$) подполей, то оно называется *простым*. Если поле H, представляющее собой расширение поля $\mathbb{F}$, является конечным полем, то мы называем его *конечным расширением поля* $\mathbb{F}$. Очевидно, что конечным расширением может обладать лишь конечное поле [64], [14].

Так как в любом поле характеристики p содержатся элементы

$$0 * 1 = 0, 1 * 1 = 1, 2 * 1 = 2, \ldots, (p-1) * 1 = p - 1,$$

и множество этих элементов замкнуто относительно операций поля, то *всякое конечное простое поле* $\mathbb{F}_q = \langle F, +, \cdot, 0, 1 \rangle$ *изоморфно полю* $\mathbb{Z}_p$ *классов вычетов по модулю* p, *а всякое конечное поле* $\mathbb{F}_q = \langle F, +, \cdot, 0, 1 \rangle$ *содержит поле* $\mathbb{Z}_p$ *классов вычетов по модулю* p *в качестве подполя, являясь, таким образом, его конечным расширением*. Теперь нетрудно убедиться (например, еще раз воспользовавшись упомянутой ранее теоремой Лагранжа), что *число элементов конечного поля* $\mathbb{F}_q$ *характеристики* p *есть степень его характеристики*: $q = p^n, n \in \mathbb{N}$.

Пример 8.1.5 Поле рациональных чисел $\mathbb{Q}$ является подполем поля действительных чисел $\mathbb{R}$, которое, в свою очередь, образует подполе поля комплексных чисел $\mathbb{C}$: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Нетрудно убедиться, что поле $\mathbb{Q}$, в отличие от полей $\mathbb{R}$ и $\mathbb{C}$, является простым. Таким образом, можно утверждать, что поля $\mathbb{C}$ и $\mathbb{R}$ являются расширениями (в данном случае, безусловно, бесконечными) простого поля $\mathbb{Q}$. Нетрудно убедиться в том, что *всякое поле нулевой характеристики содержит поле рациональных чисел $\mathbb{Q}$ в качестве подполя*, то есть $\mathbb{Q}$ — *единственное простое поле нулевой характеристики*.

Поле классов вычетов $\mathbb{Z}_5$ является простым полем характеристики 5. Любое его конечное расширение будет иметь 5^n элементов, где n — некоторое натуральное число (приведите пример бесконечного расширения поля $\mathbb{Z}_5$). В общем случае, для любого простого p поле классов вычетов $\mathbb{Z}_p$ является (единственным) простым полем характеристики p и любое его конечное расширение будет иметь p^n элементов, где n — некоторое натуральное число. □

Таким образом, структура и поведение любого конечного поля теснейшим образом связаны с его характеристикой, что отражено в приведенных ниже свойствах.

Свойства характеристики конечного поля

1. Характеристика любого конечного поля — простое число. Для любого простого числа p существует поле характеристики p.
2. Число элементов любого конечного поля есть степень его характеристики.
3. Характеристика поля равна характеристике любого его подполя.
4. Любое поле характеристики p содержит подполе, изоморфное полю классов вычетов по модулю p.
5. Если p — характеристика конечного поля $\mathbb{F}_q$, и m, n, k, l — натуральные числа, то
   a) $m * 1 = n * 1 \Leftrightarrow m \equiv n \pmod{p}$;
   b) $m * 1 + n * 1 = k * 1 \Leftrightarrow m + n \equiv k \pmod{p}$;
   c) $(m * 1) \cdot (n * 1) = l * 1 \Leftrightarrow m \cdot n \equiv k \pmod{p}$.

Для доказательства существования поля из p^k элементов убедимся в том, что в поле $\mathbb{H}$ характеристики p для любого $k \in \mathbb{N}$ и любых элементов $a, b \in H$ имеют место тождества

$$(a+b)^{p^k} = a^{p^k} + b^{p^k},\ (a-b)^{p^k} = a^{p^k} - b^{p^k}, (a \cdot b)^{p^k} = a^{p^k} \cdot b^{p^k},\ \left(\frac{a}{b}\right)^{p^k} = \frac{a^{p^k}}{b^{p^k}}.$$

Для доказательства первого тождества можно провести индукцию по k, опираясь на известное утверждение о том, что коэффициенты $\binom{p}{k}$ разложения

$$(a+b)^p = a^p + \binom{p}{1} * a^{p-1}b + \binom{p}{2} * a^{p-2}b^2 + \ldots + \binom{p}{p-1} * ab^{p-1} + b^p$$

делятся на p при $1 \leqslant n \leqslant p-1$: поскольку p — простое, то $\binom{p}{n} \equiv$ $\equiv 0 \pmod p$ при $1 \leqslant n \leqslant p-1$. Доказательство остальных тождеств очевидно [78].

Теперь для $q = p^n$ попытаемся построить *поле разложения многочлена* $x^q - x$ *над полем* $\mathbb{F}_p$ *— наименьшее расширение поля* $\mathbb{F}_p$, *над которым многочлен* $x^q - x$ *разлагается в произведение линейных множителей.* Ссылаясь на только что доказанные тождества, мы можем утверждать, что множество корней данного многочлена замкнуто относительно сложения, вычитания, умножения и деления, и, следовательно, образует поле. При этом, поскольку $(x^q - x)' = qx^{q-1} - 1 = -1 \neq 0$, то производная многочлена $x^q - x$ и сам многочлен взаимно просты, что говорит о том, что все корни многочлена $x^q - x$ различны. Так как многочлен степени q имеет в своем поле разложения ровно q корней, то мы можем утверждать, что поле разложения многочлена $x^q - x$ состоит из $q = p^n$ элементов, представляющих собой различные корни этого многочлена.

Таким образом, мы доказали, что *конечное поле* $\mathbb{F}_q$, $q = p^n$, *всегда существует.* Учитывая полученные ранее результаты, можно утверждать, что *конечное поле* $\mathbb{F}_q$ *существует тогда и только тогда, когда*

$$q = p^n, p \in P, n \in \mathbb{N}.$$

8.1.4. Мультипликативная группа конечного поля

Перейдем к рассмотрению мультипликативной группы $\mathbb{F}^* = \langle F^*, \cdot, 1\rangle$, $F^* = F\backslash\{0\}$ всех ненулевых элементов конечного поля $\mathbb{F}_q = \langle F, +, \cdot, 0, 1\rangle$.

Поскольку эта группа состоит из $q-1$ элемента, то, вновь используя теорему Лагранжа, получим, что для любого ненулевого элемента a поля $\mathbb{F}_q$ имеет место соотношение $a^{q-1} = 1$.

Наименьшее натуральное число δ, для которого $a^\delta = 1$, называется *порядком* ненулевого *элемента* a поля $\mathbb{F}_q$ и обозначается символом $\operatorname{ord} a$. Поскольку $a^{q-1} = 1$, то для любого ненулевого элемента $\operatorname{ord} a \leqslant q-1$. Элемент, порядок которого равен $q-1$, называется *примитивным элементом поля* $\mathbb{F}_q$.

Свойства порядка ненулевого элемента конечного поля

1. $\operatorname{ord} a \leqslant q-1$.
2. $\operatorname{ord} a | (q-1)$.
3. $a^{q^n-1}=1$; $a^{q^n}=a$.
4. Если $m, n \in \mathbb{N}$, то $a^n = a^m \Leftrightarrow m \equiv n \pmod{\operatorname{ord} a}$.
5. Элементы $1, a, a^2, \ldots a^{\operatorname{ord} a-1}$ различны и являются корнями многочлена $x^{\operatorname{ord} a}-1$.
6. $\operatorname{ord} a^k = \dfrac{\operatorname{ord} a}{(k, \operatorname{ord} a)}$.
7. $\operatorname{ord} a^k = \operatorname{ord} a \Leftrightarrow (k, \operatorname{ord} a) = 1$.
8. Если $\operatorname{ord} a = \delta$, то число элементов мультипликативной группы поля $\mathbb{F}_q$, имеющих порядок δ, равно $\varphi(\delta)$, где $\varphi(\delta)$ — функция Эйлера.
9. Если $\delta \in \mathbb{N}$, $\delta | (q-1)$, то число элементов мультипликативной группы $\mathbb{F}^*$ поля $\mathbb{F}_q$, имеющих порядок δ, равно $\varphi(\delta)$, где $\varphi(\delta)$ — функция Эйлера.

Пример 8.1.6 В поле $\mathbb{F}_5$ порядок элемента 1 равен 1, порядок элемента 2 равен 4, поскольку $2^4=1$, и $2^1 \neq 1$, $2^2 \neq 1$, порядок элемента 3 равен 4, поскольку $3^4=1$, и $3^1 \neq 1$, $3^2 \neq 1$, порядок элемента 4 равен 2, поскольку $4^2=1$, и $4^1 \neq 1$. Примитивными элементами поля $\mathbb{F}_5$ будут элементы 2 и 3. В этом случае их целые неотрицательные степени пробегают множество всех ненулевых элементов поля $\mathbb{F}_p$: для элемента 2 получаем, что $2^0=1$, $2^1=2$, $2^2=4$, $2^3=3$; для элемента 3 получаем, что $3^0=1$, $3^1=3$, $3^2=4$, $3^3=2$. □

Замечание. *Здесь и далее для облегчения записи выкладок и упрощения понимания сути выполняемых операций мы будем обозначать элементы конечного поля $\mathbb{F}_p = \mathbb{Z}_p$ обычными символами $0, 1, 2, .., p-1$, а операции над ними — обычными символами $+$ и $\cdot$.*

Вообще, если $q=p$ — простое число, то элемент a поля $\mathbb{F}_p$ можно рассматривать как класс вычетов по модулю p с представителем a. Условие $a^\delta = 1$ в этом случае равносильно условию $a^\delta \equiv 1 \pmod{p}$, поэтому порядок $\operatorname{ord} a$ любого элемента a мультипликативной группы $\mathbb{F}_p^*$ поля $\mathbb{F}_p$ есть вместе с тем показатель $P_p(a)$, которому принадлежит целое число a по простому модулю p, и свойства порядка соответствуют аналогичным свойствам показателя.

Замечание. *Утверждение о том, что элементы $1, a, a^2, \ldots a^{\operatorname{ord} a-1}$ различны и являются единственными корнями многочлена $x^{\operatorname{ord} a}-1$, верное для конечных полей, может быть неверным для элементов некоторых колец. Например, элемент 3 кольца $\mathbb{Z}_8$ имеет порядок 2. При этом элементы 1, 2, 3, 7 различны и являются корнями многочлена x^2-1.*

Поскольку для любого натурального числа δ, такого что $\delta|(q-1)$, число элементов мультипликативной группы поля $\mathbb{F}_q$, имеющих порядок δ, равно $\varphi(\delta)$, то мы можем утверждать, что в $\mathbb{F}_q^*$ можно найти элементы всех возможных порядков. В частности, число примитивных элементов поля $\mathbb{F}_q$ равно $\varphi(p-1)$: это означает, что примитивные элементы обязательно найдутся.

Следовательно, *любое конечное поле содержит хотя бы один примитивный элемент*. Из этого вытекает, что *мультипликативная группа* $\mathbb{F}_q^*$ *ненулевых элементов конечного поля* $\mathbb{F}_q$ *циклична*: все элементы группы $\mathbb{F}_q^*$ могут быть получены как степени одного из примитивных элементов.

Пример 8.1.7 Как было показано ранее, примитивным элементом поля $\mathbb{F}_5$ является, например, элемент 2. В этом случае целые неотрицательные степени двойки пробегают множество всех ненулевых элементов поля $\mathbb{F}_5$: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$. Это и означает, что мультипликативная группа поля $\mathbb{F}_5$ циклична. Для поля $\mathbb{F}_7$ примитивным элементом будет, например, элемент 3, поскольку $3^6 \equiv 1 \pmod 7$, и $3^1 \not\equiv 1 \pmod 7$, $3^2 \not\equiv 1 \pmod 7$, $3^3 \not\equiv 1 \pmod 7$. Нетрудно убедиться, что целые неотрицательные степени тройки пробегают все ненулевые элементы поля $\mathbb{F}_7$: $3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$. Таким образом, мультипликативная группа поля $\mathbb{F}_7$ циклична. Как уже было сказано, для простого $q = p$ теория порядков элементов мультипликативной группы поля $\mathbb{F}_q$ совпадает с классической теорией показателей по простому модулю. □

Упражнения

1. Составьте таблицы сложения и умножения в кольце классов вычетов по модулю n, $n \in \{5, 6, 7, 8, 9, 10, 11, 12\}$. Образует ли система $\langle \mathbb{Z}_n, +, \cdot, 0\rangle$ кольцо, поле? Укажите все делители нуля кольца $\langle \mathbb{Z}_n, +, \cdot, 0\rangle$. Укажите все обратимые элементы кольца $\langle \mathbb{Z}_n, +, \cdot, 0\rangle$. Решите в $\mathbb{Z}_n$ уравнения $(\mathbf{n}-\mathbf{1})_\mathbf{n} \cdot \mathbf{x_n} = \mathbf{3_n}$; $\mathbf{x_n}^2 + \mathbf{1} = \mathbf{0}$.
2. Найдите все делители нуля в кольце $\mathbb{Z}_n$, где $n \in \{14, 15, 26, 28, 40, 69\}$.
3. В кольце классов вычетов по модулю 21 укажите все делители нуля и решите уравнение $\mathbf{7_{21}} \cdot \mathbf{x_{21}} = \mathbf{0_{21}}$. В кольце классов вычетов по модулю 22 укажите все делители нуля и решите уравнение $\mathbf{4_{22}} \cdot \mathbf{x_{22}} = \mathbf{10_{22}}$. В кольце классов вычетов по модулю 24 укажите все делители нуля и решите уравнение $\mathbf{3_{24}} \cdot \mathbf{x_{24}} = \mathbf{6_{24}}$. В кольце классов вычетов по модулю 25 укажите все делители нуля и решите уравнение $\mathbf{5_{25}} \cdot \mathbf{x_{25}} = \mathbf{0_{25}}$.
4. В поле классов вычетов по модулю 23 решите уравнение $\mathbf{7_{23}} \cdot \mathbf{x_{23}} = \mathbf{10_{23}}$. В поле классов вычетов по модулю 29 решите уравнение $\mathbf{2_{29}} \cdot \mathbf{x_{29}} = \mathbf{11_{29}}$. В поле классов вычетов по модулю 31 решите уравнение $\mathbf{15_{31}} \cdot \mathbf{x_{31}} = \mathbf{0_{31}}$.

(5) В кольце классов вычетов по модулю n, $n \in \{5, 6, 7, 8, 9, 10, 11, 12\}$, найдите все натуральные кратные элементов $\mathbf{0_n}$, $\mathbf{1_n}$, $\mathbf{2_n}$, $\mathbf{3_n}$. Убедитесь, что аддитивная группа $\langle \mathbb{Z}_n, +, 0\rangle$ кольца $\langle \mathbb{Z}_n, +, \cdot, 0, 1\rangle$ циклична, то есть множество $\mathbb{Z}_n$ может быть получено как множество натуральных кратных некоторого элемента из $\mathbb{Z}_n$. Какие из проанализированных вами элементов можно выбрать в качестве образующих элементов группы $\langle \mathbb{Z}_n, +, 0\rangle$?

(6) Определите число простых конечных полей $\mathbb{F}_q$, $q \leqslant 20$. Постройте все такие конечные поля. Найдите порядки всех элементов из $\mathbb{F}_q^*$, укажите все примитивные элементы поля.

(7) Укажите все конечные поля, число элементов в которых не превосходит 100. Найдите характеристику каждого из найденных полей. Какие из найденных полей являются простыми?

(8) Приведите, если это возможно, пример поля характеристики 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 18, 19, 20.

(9) Сколько существует полей характеристики 2, 3, 5, 7, 11 с числом элементов не превосходящим 100? Простых полей данной характеристики?

(10) Существует ли конечное поле порядка n, $n \in \{20,21, \ldots, 30\}$? Какова его характеристика?

(11) Приведите пример:

a) поля нулевой характеристики;
b) простого поля нулевой характеристики;
c) поля нулевой характеристики, не являющегося простым;
d) бесконечного поля ненулевой характеристики;
e) конечного поля ненулевой характеристики;
f) конечного простого поля ненулевой характеристики.

(12) Найдите порядок элемента a конечного поля F_p:

a) $a = 29$; $p = 41$;
b) $a = 67$; $p = 97$;
c) $a = 13$; $p = 61$;
d) $a = 44$; $p = 89$;
e) $a = 33$; $p = 87$;
f) $a = 50$; $p = 57$;
g) $a = 20$; $p = 67$;
h) $a = 28$; $p = 47$.

Задачи

1 Укажите в каком поле $1 = -1$?

2 В кольце классов вычетов по модулю $6n$ укажите все делители нуля и решите уравнение $\mathbf{n_{6n}} \cdot \mathbf{x_{6n}} = \mathbf{0_{6n}}$, если

$$n = N - 4\left\lfloor \frac{N}{4} \right\rfloor + 5, N \in \{1, 2, 3, \ldots 25\}.$$

3 Докажите, что для простого числа p система $\mathbb{Z}_p = \langle \mathbb{Z}_p, +, \cdot, 0, 1\rangle$ является полем, а для составного числа m система $\mathbb{Z}_m = \langle \mathbb{Z}_m, +, \cdot, 0, 1\rangle$ полем не является.

4 Найдите число делителей нуля в $\mathbb{Z}_m$, $m \in \{2, \ldots, 20\}$; докажите, что число делителей нуля кольца классов вычетов по модулю m равно $m - \varphi(m) - 1$.

5 Докажите, что поле не содержит делителей нуля.

6 Решите в $\mathbb{Z}_m$, $m \in \{2, 3, 4, 5, 6\}$, уравнение:

a) $\mathbf{61_m} \cdot \mathbf{x_m} = \mathbf{80_m}$;
c) $\mathbf{35_m} \cdot \mathbf{x_m^2} = \mathbf{100_m}$;
b) $\mathbf{28_m} \cdot \mathbf{x_m} = \mathbf{5_m}$;
d) $\mathbf{8_m^{x_m}} = \mathbf{1_m}$.

7 Пусть θ – корень неприводимого над полем $\mathbb{F}$ многочлена $f(x) \in \mathbb{F}[x]$ степени n. Докажите, что $\mathbb{F}(\theta)$ – простое алгебраическое расширение поля $\mathbb{F}$ степени n. Докажите, что $1, \theta, \theta^2, \ldots, \theta^{n-1}$ – базис данного расширения, то есть любой элемент $\alpha \in F(\theta)$ единственным образом представим в виде $\alpha = a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1}$, $a_i \in F$. Докажите, что существует единственный многочлен $g(x) = x^n + g_{n-1}x^{n-1} + \ldots + g_1x + g_0 \in \mathbb{F}[x]$ такой, что $g(\theta) = 0$, – *минимальный многочлен элемента* θ.

8 Докажите, что множество

$$\mathbb{Q}(\sqrt{7}) = \langle Q(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in Q\}, +, \cdot, 0, 1\rangle$$

является: полем; подполем поля $\mathbb{R}$ действительных чисел; расширением поля $\mathbb{Q}$ рациональных чисел. Найдите степень расширения, укажите его базис.

9 Найдите степени расширений полей

a) $[\,\mathbb{C} : \mathbb{R}\,]$;
c) $[\,\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}\,]$;
b) $[\,\mathbb{Q}(\sqrt{5}) : \mathbb{Q}\,]$;
d) $[\,\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt{2})\,]$.

10 Укажите базисы расширений полей

a) $[\,\mathbb{Q}(\sqrt{5}) : \mathbb{Q}\,]$;
b) $[\,\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}\,]$;
c) $[\,\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\,]$;
d) $\left[\mathbb{R}\left(-\frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right) : \mathbb{R}\right]$;
e) $[\,\mathbb{C} : \mathbb{R}\,]$;
f) $[\,\mathbb{Q} : \mathbb{Q}\,]$.

11 Существуют ли расширения поля $\mathbb{R}$ степени 1; 2; 3; 4?... n?

12 Докажите, что число элементов конечного поля $\mathbb{F}_q$ характеристики p есть степень его характеристики: $q = p^n$, $n \in \mathbb{N}$.

13 Докажите, что если p — характеристика конечного поля $\mathbb{F}_q$, и m, n, k, l — натуральные числа, то имеют место следующие соотношения:

a) $m * 1 = n * 1 \Leftrightarrow m \equiv n \pmod{p}$;

b) $m * 1 + n * 1 = k * 1 \Leftrightarrow m + n \equiv k \pmod{p}$;

c) $(m * 1) \cdot (n * 1) = l * 1 \Leftrightarrow m \cdot n \equiv k \pmod{p}$.

14 Докажите, что простое поле $\mathbb{F}$ нулевой характеристики изоморфно полю $\mathbb{Q}$ рациональных чисел; простое поле $\mathbb{F}$ ненулевой характеристики p изоморфно полю $\mathbb{Z}_p$ классов вычетов по модулю p.

15 Можно ли линейно строго упорядочить конечное поле; бесконечное поле? Приведите примеры.

16 Убедитесь, что сумма элементов конечного поля $\mathbb{F}_p$, $p \in \{2, 3, 5, 7, 11, 13, 17, 19\}$ равна нулю. Докажите, что сумма элементов любого конечного поля равна нулю.

17 Пусть $\mathbb{H}$ — поле характеристики p, $k \in \mathbb{N}$, $a, b \in H$. Докажите, что $(a - b)^{p^k} = a^{p^k} - b^{p^k}$;

18 Пусть $\mathbb{H}$ — поле характеристики p, $k \in \mathbb{N}$, $a, b \in H$. Докажите, что если $b \neq 0$, то $\left(\frac{a}{b}\right)^{p^k} = \frac{a^{p^k}}{b^{p^k}}$.

19 В каком поле выполняются соотношения:

a) $(a - b)(a + b) = a^2 - b^2$;

b) $(a + b)^2 = a^2 + b^2$;

c) $(a + b)^2 \neq a^2 + b^2$?

20 Пусть $f(x) = x^2 + x + 1$. Является ли многочлен $f(x)$ неприводимым над полем $\mathbb{R}$ действительных чисел? Найдите корни θ_1 и θ_2 многочлена $f(x)$. Постройте простые расширения $\mathbb{R}$ с помощью θ_1 и θ_2. Найдите базисы и степени построенных расширений. Являются ли полученные расширения полями разложения многочлена $f(x)$?

8.2. Кольцо многочленов над полем $\mathbb{F}$. Построение конечного поля

Многочленом $f(x)$ над конечным полем $\mathbb{F} = \langle F, +, \cdot, 0, 1\rangle$ называется формальная сумма вида $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, где $a_i \in F$, а n — целое неотрицательное число. Если $a_n \neq 0$, то число n называют *степенью многочлена* $f(x)$ и пишут $\deg f(x) = n$.

Нетрудно убедится, что множество $F[x]$ всех многочленов над полем $\mathbb{F}$ с заданными на нем стандартными операциями сложения и умножения образует коммутативное кольцо с единицей $\mathbb{F}[x] = \langle F[x], +, \cdot, 0, 1\rangle$, которое называют *кольцом многочленов над полем* $\mathbb{F}$ ([60], [14], [78]).

Как обычно, многочлен $f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$ будем называть *нормированным*, если его старший коэффициент a_n равен единице.

Если для некоторого элемента $\theta \in F$ имеет место равенство $f(\theta) = 0$, то θ называют корнем многочлена $f(x) \in F[x]$.

Пример 8.2.8 Рассматривая многочлены $f(x) = 21x^8 - 14x^5 - 6x^4 + 21$, $g(x) = x^4 + x^2 - 20$ как многочлены над полем $\mathbb{Q}$ рациональных чисел, мы можем утверждать, что это многочлены степени 8 и 4, соответственно, причем второй многочлен нормирован. Их сумма

$$f(x) + g(x) = (21x^8 - 14x^5 - 6x^4 + 21) + (x^4 + x^2 - 20)$$

представляет собой многочлен $21x^8 - 14x^5 - 5x^4 + x^2 + 1$ восьмой степени над $\mathbb{Q}$, а их произведение

$$f(x) \cdot g(x) = (21x^8 - 14x^5 - 6x^4 + 21) \cdot (x^4 + x^2 - 20)$$

многочлен $21x^{12} + 21x^{10} - 10x^9 - 428x^8 - 14x^7 - 6x^6 + 280x^5 + 141x^4 + 21x^2 + 420$ двенадцатой степени.

Рассматривая те же многочлены $f(x)$ и $g(x)$ как многочлены над полем $\mathbb{F}_{23}$, мы можем утверждать, что это многочлены

$$f(x) = -2x^8 + 9x^5 - 6x^4 - 2, g(x) = x^4 + x^3 + 3 \in F_{23}[x]$$

степени 8 и 4 соответственно, причем второй многочлен нормирован. Их сумма

$$f(x) + g(x) = (-2x^8 + 9x^5 - 6x^4 - 2) + (x^4 + x^3 + 3)$$

представляет собой многочлен $-2x^8 + 9x^5 - 5x^4 + x^2 + 1$ восьмой степени над $\mathbb{F}_{23}$, а их произведение

$$f(x) \cdot g(x) = (-2x^8 + 9x^5 - 6x^4 - 2) \cdot (x^4 + x^3 + 3)$$

многочлен $-2x^{12} - 2x^{10} + 9x^9 + 11x^8 + 9x^7 - 6x^6 + 4x^5 + 3x^4 - 2x^2 - 6$ двенадцатой степени.

Рассматривая многочлены $f(x)$ и $g(x)$ как многочлены над полем $\mathbb{F}_7$, мы убедимся, что многочлен $f(x) = x^4 \in F_7[x]$ имеет, как и многочлен $g(x) = x^4 + x^2 + 1 \in F_7[x]$, степень 4, и оба многочлена нормированы. Их сумма

$$f(x) + g(x) = x^4 + (x^4 + x^2 + 1) = 2x^4 + x^2 + 1 \in F_7[x]$$

многочлен степени 4, а их произведение

$$f(x) \cdot g(x) = x^4 \cdot (x^4 + x^2 + 1) = x^8 + x^6 + x^4 \in F_7[x]$$

многочлен степени 8. □

8.2.1. Неприводимые над полем многочлены

Многочлен $f(x) \in F[x]$ называется *неприводимым над полем* $\mathbb{F}$ (или в кольце $\mathbb{F}[x]$), если $\deg f(x) > 0$ и из разложения $f(x) = g(x) \cdot h(x)$, где $g(x), h(x) \in F[x]$, следует, что либо $g(x)$, либо $h(x)$ — многочлен нулевой степени. В остальных случаях многочлен положительной степени $f(x) \in F[x]$ называется *приводимым над* $\mathbb{F}$ (или в $\mathbb{F}[x]$): для приводимого многочлена существует хотя бы одно разложение $f(x) = g(x) \cdot h(x)$, где $g(x), h(x) \in F[x]$, $\deg g(x) > 0$ и $\deg h(x) > 0$.

Пример 8.2.9 Проанализируем существование приводимых и неприводимых многочленов малых степеней в кольцах $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ и $\mathbb{F}_2[x]$.

Ясно, что многочлен первой степени всегда неприводим.

Многочлены второй степени всегда приводимы над полем комплексных чисел, но далеко не всегда — над полем действительных и, тем более, рациональных чисел: так, многочлен $x^2 + 1 = (x - i)(x + i)$ приводим в $\mathbb{C}[x]$, но неприводим в $\mathbb{R}[x]$, и, тем более, в $\mathbb{Q}[x]$. А многочлен $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ приводим в $\mathbb{R}[x]$ (и, следовательно, в $\mathbb{C}[x]$), но неприводим в $\mathbb{Q}[x]$. А что произойдет в $\mathbb{F}_2[x]$? Рассмотрим многочлены второй степени над полем $\mathbb{F}_2$. Их всего четыре: $x^2 + x + 1$, $x^2 + x$ $x^2 + 1$, x^2. Многочлены $x^2 + x = x(x + 1)$, $x^2 + 1 = (x + 1)^2$ и $x^2 = x \cdot x$ приводимы. Многочлен $f(x) = x^2 + x + 1$ неприводим: если бы он раскладывался на нетривиальные множители, то каждый из этих множителей имел бы степень 1, следовательно, многочлен $f(x) = x^2 + x + 1$ имел бы корень в $\mathbb{F}_2$, однако $f(0) = f(1) = 1 \neq 0$.

Все многочлены третьей степени приводимы над $\mathbb{R}$, и, тем более, над $\mathbb{C}$, а вот над $\mathbb{Q}$ неприводимые многочлены степени 3 имеются: например, многочлен $x^3 - 2$. Найдем все неприводимые многочлены степени 3 над $\mathbb{F}_2$. Многочлены третьей степени имеют вид $a_3x^3 + a_2x^2 + a_1x + a_0$, где $a_1 \in \{1, 0\}$. Очевидно, $a_3 = 1$, и мы получаем ровно 8 многочленов, однако, если исключить очевидно приводимые многочлены с $a_0 = 0$, то останется всего 4 многочлена:

$$x^3 + x^2 + x + 1, \quad x^3 + x + 1, \quad x^3 + x^2 + 1, \quad x^3 + 1.$$

Для многочлена третьей степени нетривиальное разложение обязательно будет содержать множители первой и второй степени, следовательно, у приводимых многочленов должны быть корни, в частности, для многочленов из нашего списка — корень, равный единице. Непосредственная проверка показывает, что неприводимыми будут лишь многочлены

$$x^3 + x + 1 \quad \text{и} \quad x^3 + x^2 + 1.$$

Продолжая исследование, мы убедимся в том, что все многочлены четвертой степени над полями $\mathbb{C}$ и $\mathbb{R}$ приводимы, существуют многочлены четвертой степени, неприводимые над $\mathbb{Q}$ (например, многочлен x^4-2), а неприводимыми многочленами четвертой степени над $\mathbb{F}_2$ являются многочлены

$$x^4+x^3+1, \quad x^4+x+1, \quad x^4+x^3+x^2+x+1$$

и только они.

Для $n=5$ ситуация аналогична: все многочлены 5-ой степени над полями $\mathbb{C}$ и $\mathbb{R}$ приводимы, существуют многочлены 5-ой степени, неприводимые над $\mathbb{Q}$ (например, многочлен x^5-2), а примером неприводимого многочлена 5-ой степени над $\mathbb{F}_2$ может служить многочлен $x^5+x^4+x^3+x^2+1 \in F_2[x]$.

Действительно, если многочлен пятой пятой степени приводим, то его можно представить в виде произведения многочленов либо первой и четвертой степеней, либо второй и третьей степеней. Первое представление возможно, если у многочлена есть корень. В поле $\mathbb{F}_2$ имеется всего два элемента 1 и 0, и ни один из них не является корнем многочлена $x^5+x^4+x^3+x^2+1$; следовательно, нетривиальное представление в виде произведения многочленов первой и четвертой степеней невозможно. Рассмотрим многочлены второй степени из $\mathbb{F}_2[x]$. Как было доказано ранее, среди них ровно один неприводимый: x^2+x+1. Непосредственная проверка показывает, что x^2+x+1 не делит $x^5+x^4+x^3+x^2+1$:

$$x^5+x^4+x^3+x^2+1=(x^2+x+1)x^3+(x^2+1).$$

Таким образом, рассмотрев все возможные случаи, мы убедились, что многочлен $x^5+x^4+x^3+x^2+1$ неприводим над $\mathbb{F}_2$.

Степень	Кольцо	Неприводимый многочлен	Приводимый многочлен
$n=1$	$\mathbb{C}[x]$	все	нет
	$\mathbb{R}[x]$	все	нет
	$\mathbb{Q}[x]$	все	нет
	$F_2[x]$	все	нет
$n=2$	$\mathbb{C}[x]$	нет	все
	$\mathbb{R}[x]$	x^2+1	x^2-2
	$\mathbb{Q}[x]$	x^2-2	x^2-1
	$\mathbb{F}_2[x]$	x^2+x+1	x^2+1
$n=3$	$\mathbb{C}[x]$	нет	все
	$\mathbb{R}[x]$	нет	все
	$\mathbb{Q}[x]$	x^3-2	x^3-8
	$\mathbb{F}_2[x]$	x^3+x+1	x^3+1

□

Свойства многочленов, неприводимых над конечным полем

1. Неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^n-1}-1$.
2. Неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^n}-x$.
3. Неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^m}-x$ тогда и только тогда, когда $n|m$.
4. $p^n=\sum\limits_{m|n} m\cdot a_p(m)$, где $a_p(m)$ — число нормированных и неприводимых многочленов степени m над полем $\mathbb{F}_p$.
5. Число $a_p(n)$ неприводимых над полем $\mathbb{F}_p$ многочленов степени n вычисляется по формуле

$$a_p(n)=\frac{1}{n}\sum_{m|n} p^{\frac{n}{m}}\mu(m),$$

где $\mu(n)$ — *функция Мебиуса*.

6. Для всякого простого p и для всякого натурального n существуют неприводимые многочлены над полем $\mathbb{F}_p$ степени n.

Пример 8.2.10 Пользуясь формулой $a_p(n)=\frac{1}{n}\sum\limits_{m|n} p^{\frac{n}{m}}\mu(m)$, убедимся, что ранее мы нашли все неприводимые многочлены третьей степени над $\mathbb{F}_2$. (Они, очевидно, нормированы, так как в $\mathbb{F}_2$ нет других ненулевых коэффициентов, кроме 1).

Для использования формулы, позволяющей вычислить $a_p(n)$, нам нужны свойства *функции Мебиуса* $\mu(n)$, которая определена для всех натуральных n и принимает значения из множества $\{-1,0,1\}$ в зависимости от разложения n на простые множители: $\mu(n)=1$, если n — бесквадратное число с четным числом простых делителей; $\mu(n)=-1$, если n — бесквадратное число с нечетным числом простых делителей; $\mu(n)=0$, если n не является бесквадратным [78].

Например,

$$\mu(30)=\mu(2\cdot 3\cdot 5)=(-1)^3=-1,$$
$$\mu(101)=(-1)^1=-1,$$
$$\mu(210)=\mu(2\cdot 3\cdot 5\cdot 7)=(-1)^4=1;$$
$$\mu(300)=\mu(2^2\cdot 3\cdot 5^2)=0.$$

В нашем случае $\mu(1) = 1$, $\mu(3) = -1$, и

$$a_2(3) = \frac{1}{3}\sum_{m|n} p^{\frac{n}{m}}\mu(m) = \frac{1}{3}\left(2^{\frac{3}{1}}\mu(1) + 2^{\frac{3}{3}}\mu(3)\right) =$$

$$= \frac{1}{3}\left(2^3 \cdot 1 + 2^1 \cdot (-1)\right) = \frac{1}{3}(8-2) = 2.$$

Таким образом, над $\mathbb{F}_2$ имеется ровно два нормированных и неприводимых многочлена степени 3, и мы их нашли: это многочлены $x^3 + x^2 + 1$ и $x^3 + x + 1$. □

8.2.2. Сравнимость многочленов и построение конечного поля $\mathbb{F}_{p^n}$

Кольцо многочленов $\mathbb{F}[x]$ над любым полем $\mathbb{F}$ *евклидово* [60], то есть в нем имеется аналог алгоритма Евклида. Следовательно, мы всегда можем *поделить многочлен* $g(x) \in F[x]$ *на многочлен* $f(x) \in F[x]$ положительной степени *с остатком*, то есть получить представление $g(x) = f(x) \cdot q(x) + r(x)$, где $q(x), r(x) \in F[x]$, и $0 \leqslant \deg r(x) < \deg f(x)$.

Отсюда следует, что на множестве $\mathbb{F}[x]$, в частности на множестве $\mathbb{F}_p[x]$, может быть определено отношение сравнимости.

Пусть $f(x) \in F_p[x]$ — многочлен над полем $\mathbb{F}_q$ положительной степени. Два многочлена $g(x)$, $h(x) \in F_p[x]$ называются *сравнимыми по модулю* $f(x)$, если $g(x)$ и $h(x)$ имеют одинаковые остатки при делении на $f(x)$, или, что то же, если $f(x)|(g(x) - h(x))$. В этом случае пишут $g(x) \equiv h(x) \pmod{f(x)}$.

Пример 8.2.11 Например, $x^2+x+1 \equiv 1 \pmod{x}$, поскольку $x^2+x+1 = x(x+1)+1$, причем указанное сравнение верно независимо от поля, над которым рассматриваются многочлены.

Поскольку $x^n = x^k \cdot x^{k-1} + 0$, то выполнено сравнение $x^n \equiv 0 \pmod{x^k}$, $1 \leqslant k \leqslant n-1$.

Поскольку $x^n - 1 = (x-1)g(x)$, то выполнено сравнение $x^n - 1 \equiv 0 \pmod{x-1}$. С другой стороны, очевидно, что $x^n - 1 \equiv 1 \pmod{x^k}$, $1 \leqslant k \leqslant n-1$.

В кольце $\mathbb{F}_7$ имеет место сравнение

$$x^4 + 2x^3 + 2x^2 + 1 \equiv 5x \pmod{(x^2+1)},$$

поскольку $x^4 + 2x^3 + 2x^2 + 1 = (x^2+1) \cdot (x^2+2x+1) + 5x$. □

Отношение сравнимости рефлексивно, симметрично и транзитивно, то есть является *отношением эквивалентности*. Следовательно, это отношение разбивает множество $F_p[x]$ на непересекающиеся классы экви-

валентности, которые образуют фактормножество, состоящее ровно из p^n элементов, где n — степень $f(x)$. Действительно, количество всевозможных остатков $r(x)$ при делении на $f(x)$ равно числу многочленов степени не выше $n-1$ над $\mathbb{F}_p$, которое, очевидно, равно числу наборов $\langle r_0, r_1, \ldots r_{n-1}\rangle, r_i \in F_p$, то есть равно p^n.

Пример 8.2.12 Рассмотрим многочлен $f(x) = x^2+1 \in F_2[x]$ и построим множество $F_2[x]/(x^2+1)$ классов эквивалентности по модулю x^2+1. Его представителями являются многочлены нулевой и первой степени над полем $\mathbb{F}_2$, то есть многочлены $0, 1, x, x+1$. Находя попарные суммы $0+1=1, 1+1=0$, $x+(x+1)=1$ и т. д., мы построим таблицу сложения элементов из $F_2/(x^2+1)$. Для построения таблицы умножения найдем попарные произведения элементов из $F_2/(x^2+1)$, в случае необходимости заменяя полученные многочлены их остатками при делении на x^2+1. Так, например,

$$(x+1)x = x^2 + x \equiv x^2 + 1 + (x+1) \equiv x+1 \,(\mathrm{mod}\, x^2+1).$$

Таким образом, мы получим нижеследующие таблицы сложения и умножения на множестве $F_2/(x^2+1)$.

Таблица сложения в $\mathbb{F}_2/(x^2+1)$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Таблица умножения в $\mathbb{F}_2/(x^2+1)$

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	1	0

Анализируя полученные таблицы сложения и умножения, мы видим, что множество

$$\mathbb{F}_2[x]/(x^2+1) = \langle F_2[x]/(x^2+1), +, \cdot, 0, 1\rangle$$

образует коммутативное кольцо с единицей, не являющееся полем: не у всех элементов существуют обратные; кроме того, имеются и делители нуля. □

Проведем аналогичное исследование для многочлена

$$f(x) = x^2 + x + 1 \in F_2[x].$$

Как и в предыдущем примере, множество $F_2[x]/(x^2+x+1)$ состоит из четырех элементов 0, 1, x, $x+1$. Совпадает с таблицей предыдущего примера и таблица сложения. А вот таблица умножения принимает другой вид.

Таблица сложения в $\mathbb{F}_2[x]/(x^2+x+1)$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Таблица умножения в $\mathbb{F}_2[x]/(x^2+x+1)$

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Исследование таблиц показывает, что

$$\mathbb{F}_2[x]/(x^2+x+1) = \langle F_2[x]/(x^2+x+1), +, \cdot, 0, 1\rangle$$

образует поле: для каждого ненулевого элемента мы можем найти обратный: $1^{-1} = 1$, так как $1 \cdot 1 = 1$, $x^{-1} = x+1$ и $(x+1)^{-1} = x$, так как $x(x+1) = 1$.

Итак, фактор-множество многочленов над полем $\mathbb{F}_2$, модулем которого является неприводимый над $\mathbb{F}_2$ многочлен x^2+x+1 степени 2, представляет собой конечное поле $\mathbb{F}_4 = \mathbb{F}_{2^2}$.

Как и ожидалось, мультипликативная группа построенного поля является циклической; она порождена примитивным элементом x: поскольку $x^0 = 1$ и $x^2 = x+1$, то множество

$$(F_2[x]/(x^2+x+1))^* = (F_2[x]/(x^2+x+1))\backslash\{0\}$$

можно представить как

$$\{1 = x^0, x = x^1, x+1 = x^2\}.$$

Конечно, $(F_2[x]/(x^2+x+1))^*$ можно представить и как множество

$$\{1 = (x+1)^0, x+1 = (x+1)^1, x = (x+1)^2\}$$

степеней $x+1$: в нашей модели поля $\mathbb{F}_4$ элементы x и $x+1$ являются примитивными и каждый из них порождает все ненулевые элементы построенного поля.

Таким образом, для заданного простого числа p и заданного натурального числа n для построения поля $\mathbb{F}_{p^n}$ достаточно найти неприводимый многочлен $f(x) \in F_p[x]$ степени n над полем n (существование такого многочлена доказано), и построить фактормножество $F_p[x]/(f(x))$. Задание на множестве $F_p[x]/(f(x))$ стандартных операций сложения и умножения многочленов по модулю $f(x)$ превратит $F_p[x]/(f(x))$ в поле, число элементов которого равно p^n. Для построения таблиц сложения и умножения используются обычные операции сложения и умножения многочленов, осуществляемые по модулю $f(x)$. Для нахождения обратного элемента достаточно либо воспользоваться построенной таблицей умножения, либо использовать соотношение

$$g(x)u(x) + f(x)v(x) = 1,$$

которое выполняется для некоторых $u(x), v(x) \in F_p[x]$. Поскольку в этом случае $g(x)u(x) \equiv 1 \pmod{f(x)}$, то $u(x) = g^{-1}(x)$.

Пример 8.2.13 Для построения поля $\mathbb{F}_9 = \mathbb{F}_{3^2}$ найдем многочлен степени 2, неприводимый над $\mathbb{F}_3$. Такими являются многочлены

$$x^2+1, \quad x^2+x+2, \quad x^2+2x+2, \quad 2x^2+2, \quad 2x^2+x+1, \quad 2x^2+2x+1.$$

Возьмем, например, многочлен $x^2 + 1$. Тогда искомое поле $\mathbb{F}_9$ есть $\mathbb{F}_3[x]/(x^2+1)$. (Если вместо x^2+1 взять другой многочлен, то получится новое поле, изоморфное уже построенному.) Таблицы сложения и умножения в $\mathbb{F}_9$ принимают нижеследующий вид.

- Таблица сложения в $\mathbb{F}_9$:

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

- Таблица умножения в $\mathbb{F}_9$:

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Для нахождения элемента, обратного данному, достаточно воспользоваться таблицей. Например, поскольку $(2x+2)(2x+1)=1$, то $(2x+2)^{-1}=$ $=2x+1$, и $(2x+1)^{-1}=2x+2$.

Однако, если таблицы под рукой нет, задачу можно решить с помощью простых рассуждений. Поскольку $(2x+2, x^2+1)=1$, то, по критерию взаимной простоты, существуют такие многочлены $u(x)$ и $v(x)$ над полем $\mathbb{F}_3$, что

$$(2x+2)u(x)+(x^2+1)v(x)=1.$$

Но в этом случае

$$(2x+2)u(x)\equiv 1 \pmod{x^2+1},$$

и, следовательно, $(2x+2)^{-1}=u(x)$. Для нахождения $u(x)$ воспользуемся алгоритмом Евклида. Поскольку

$$x^2+1=(2x+2)\cdot 2x+(2x+1),\ 2x+2=(2x+1)\cdot 1+1,$$

то, последовательно пользуясь вторым и первым равенствами, получим, что

$$\begin{aligned}1&=(2x+2)-(2x+1)\cdot 1=\\&=(2x+2)-((x^2+1)-(2x+2)\cdot 2x)\cdot 1=\\&=(2x+2)-(x^2+1)\cdot 2x+(2x+2)\cdot 2x=\\&=(2x+2)\cdot(2x+1)-(x^2+1)\cdot 2x.\end{aligned}$$

Таким образом, $(2x+2)\cdot(2x+1)\equiv 1 \pmod{x^2+1}$, и эти элементы взаимно обратны. □

8.2.3. Порядок многочлена над конечным полем

Не ограничивая общности, далее будем считать, что $f \in F_p[x]$ — нормированный многочлен над полем F_p ненулевой степени n, и $f(0) \neq \neq 0$ [64], [78].

В этом случае среди p^n многочленов $1, x, x^2, x^{p^n-1}$, заведомо не делящихся на f (и, следовательно, имеющих ненулевые остатки при делении на f), найдутся два сравнимых по модулю $f(x)$. Таким образом, $f|(x^i - x^j)$, то есть $f|x^j(x^{i-j}-1)$. Следовательно, в наших условиях $f|(x^{i-j}-1)$, причем $1 \leqslant i-j \leqslant p^n-1$.

Другими словами, мы доказали, что любой нормированный многочлен $f \in F_p[x]$ ненулевой степени n, такой что $f(0) \neq 0$, делит многочлен $x^\delta - 1$ при некотором натуральном δ, $1 \leqslant \delta \leqslant p^n - 1$.

Наименьшее натуральное число δ, такое что $f|(x^\delta - 1)$, будем называть *порядком многочлена* f и обозначать его символом $\operatorname{ord} f(x)$. (Если $f(0) = 0$, то представим его в виде $f(x) = x^\alpha g(x)$, $g(0) \neq 0$ и назовем порядком $f(x)$ порядок многочлена $g(x)$.)

Свойства порядка многочлена над конечным полем

1. $1 \leqslant \operatorname{ord} f(x) \leqslant p^n - 1$.
2. $f(x)|(x^m - 1)$ тогда и только тогда, когда $\operatorname{ord} f(x)|m$.
3. Порядок многочлена f над полем $\mathbb{F}_p$ равен порядку этого многочлена над любым расширением поля $\mathbb{F}_p$.
4. $\operatorname{ord} f(x) = \operatorname{ord} \theta$, если $f(x) \in F_p[x]$ — неприводимый многочлен, θ — его ненулевой корень, и $\operatorname{ord} \theta$ — порядок элемента $\theta \in F_p^*$.
5. $\operatorname{ord} f(x)|(p^n - 1)$, если $f(x) \in F_p[x]$ — неприводимый многочлен.
6. $\operatorname{ord}(f(x))^n = p^t \operatorname{ord} f(x)$, где t - наименьшее целое число, такое что $p^t \geqslant n$, и $f(x) \in F_p[x]$ — неприводимый многочлен.
7. Если $(g_i(x), g_j(x)) = 1$ для $i \neq j$, то $\operatorname{ord}(g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_k(x)) = = [\operatorname{ord} g_1(x), \ldots \operatorname{ord} g_k(x)]$.
8. Если $f(x) = f_1^{m_1}(x) \cdot \ldots \cdot f_k^{m_k}(x)$, где $f_i \in F_p[x]$ — неприводимые многочлены, то $\operatorname{ord} f(x) = p^t[\operatorname{ord} f_1(x), \ldots \operatorname{ord} f_k(x)]$, где t — наименьшее целое число, такое что $p^t \geqslant \max\{m_1, \ldots m_k\}$.

Пример 8.2.14 Найдем порядок многочлена

$$f(x) = (x^2 + x + 1)^3(x^4 + x + 1)(x^3 + 1)$$

над полем $\mathbb{F}_2$.

Как было доказано ранее, многочлены $x^2 + x + 1$ и $x^4 + x + 1$ неприводимы. С другой стороны, многочлен $x^3 + 1$ приводим: $x^3 + 1 = = (x+1)(x^2+x+1)$. Таким образом, $f(x) = (x^2+x+1)^4(x^4+x+1)(x+1)$.

По свойствам порядка многочлена,

$$\operatorname{ord} f(x) = 2^t[\operatorname{ord}(x^2+x+1), \operatorname{ord}(x^4+x+1), \operatorname{ord}(x+1)].$$

1. $\operatorname{ord}(x^2+x+1) | (2^2-1)$, $\operatorname{ord}(x^2+x+1) \neq 1$, следовательно, $\operatorname{ord}(x^2+x+1) = 3$.

2. $\operatorname{ord}(x^4+x+1) | (2^4-1) = 15$, то есть принадлежит множеству $\{1, 3, 5, 15\}$. Непосредственная проверка показывает, что $x^4+x+1 \nmid (x^1-1)$, $x^4+x+1 \nmid (x^3-1)$, $x^4+x+1 \nmid (x^5-1)$ (при делении многочлена на многочлен мы получаем, что $x^5-1 = (x^4+x+1)\cdot x + (x^2+x+1)$). Таким образом, $\operatorname{ord}(x^4+x+1) = 15$.

3. $\operatorname{ord}(x+1) | (2^1-1) = 1$, то есть $\operatorname{ord}(x+1) = 1$.

Наибольшая из степеней вхождения многочленов в произведение

$$f(x) = (x^2+x+1)^4(x^4+x+1)(x+1)$$

равна 4, то есть для нахождения t нужно рассмотреть соотношение $2^t \geqslant 4$, из которого следует, что $t = 2$.

Таким образом, $\operatorname{ord} f(x) = 2^2 \cdot [3, 15, 1] = 60$. □

Замечание. *Заметим, что «суммарная» степень многочлена $f(x)$ равна* 13, *но* $60 \nmid 2^{13}-1$, *то есть для приводимого многочлена $f(x)$ аналог свойства* $\operatorname{ord} f | (x^{p^{\deg f}}-1)$, *имеющего место для неприводимых многочленов, нарушен.*

8.2.4. Примитивные многочлены над конечным полем

Многочлен $f \in F_p[x]$ степени n над полем $\mathbb{F}_p$ называется *примитивным*, если $\operatorname{ord}(f(x)) = p^n - 1$. Другими словами, примитивным мы называем многочлен, имеющий максимальный возможный порядок [64], [78].

Пример 8.2.15 При рассмотрении предыдущего примера мы доказали, что над полем $\mathbb{F}_2$

$$\operatorname{ord}(x^2+x+1) = 3 = 2^2-1,$$
$$\operatorname{ord}(x^4+x+1) = 15 = 2^4-1,$$
$$\operatorname{ord}(x+1) = 1 = 2^1-1,$$

и $f(x) = (x^2+x+1)^3(x^4+x+1)(x^3+1) = 60 \neq 2^{13}-1$. Отсюда следует, что первые три многочлена являются примитивными, а последний — нет. □

Свойства примитивных многочленов над конечным полем

1. Любой примитивный многочлен f над полем $\mathbb{F}_p$ неприводим над полем $\mathbb{F}_p$.

2. Если $f \in F_p[x]$ — примитивный многочлен степени n над полем $\mathbb{F}_p$, и θ — один из корней $f(x)$ в его поле разложения, то $\mathbb{F}_p(\theta)$ — конечное поле из p^n элементов, и каждый элемент $\alpha \in F_p(\theta)$ однозначно представим в виде

$$\alpha = \alpha(\theta) = a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1}, \text{ где } a_0, a_1, \ldots, a_{n-1} \in F_p.$$

3. Число $b_p(n)$ примитивных многочленов степени n над полем $\mathbb{F}_p$ можно вычислить по формуле $b_p(n) = \dfrac{\varphi(p^n - 1)}{n}$.
4. Для любого простого числа p и любого натурального числа n существует примитивный над полем $\mathbb{F}_p$ многочлен степени n.

Пример 8.2.16 Найдем число примитивных многочленов 3 степени над $\mathbb{F}_2$: $b_2(3) = \dfrac{\varphi(2^3 - 1)}{3} = 2$. Таким образом, оба найденные ранее неприводимых многочлена $x^3 + x^2 + 1$ и $x^3 + x + 1$ степени 3 над $\mathbb{F}_2$ являются примитивными и имеют порядок $2^3 - 1 = 7$. □

Упражнения

(1) Найдите сумму, разность и произведение многочленов $f(x) = 12x^6 + 36x - 14$ и $g(x) = 2x^2 - 18$ в $\mathbb{R}[x]$, в $\mathbb{F}_2[x]$, в $\mathbb{F}_3[x]$, в $\mathbb{F}_{11}[x]$; найдите корни всех полученных многочленов.

(2) Найдите все нормированные многочлены степени n над полем $\mathbb{F}_p$, если $n = 2, 3, 4, 5, 6, 7, 8$, а $p = 2, 3, 5, 7$.

(3) Укажите число многочленов степени n над $\mathbb{F}_2$, над $\mathbb{F}_3$, над $\mathbb{F}_5$; число нормированных многочленов степени n над $\mathbb{F}_2$, над $\mathbb{F}_3$, над $\mathbb{F}_5$.

(4) Укажите число многочленов над полем $\mathbb{F}_p$; число нормированных многочленов степени n над полем $\mathbb{F}_p$.

(5) Приведите примеры приводимых и неприводимых в $\mathbb{F}[x]$ многочленов степени n, если $n \in \{1, 2, 3, 4, 5, 6, 7\}$, а $\mathbb{F} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}\}$. Опишите все неприводимые многочлены в $\mathbb{C}[x]$, в $\mathbb{R}[x]$.

(6) Приведите пример неприводимого в $\mathbb{Q}[x]$ многочлена степени n.

(7) Является ли неприводимым над $\mathbb{C}$ (над $\mathbb{R}$, над $\mathbb{Q}$, над $\mathbb{F}_2$, над $\mathbb{F}_3$, над $\mathbb{F}_5$) многочлен:

a) $x^2 + x + 1$; c) $x^4 - 1$; e) $x^3 + 2x + 3$;
b) $x^2 + x - 1$; d) $x^4 + 2x^2 + 1$; f) $x^3 + x + 5$?

(8) Найдите все нормированные неприводимые многочлены степени 2, степени 3, степени 4 над $\mathbb{F}_2$, над $\mathbb{F}_3$, над $\mathbb{F}_5$.

⑨ Докажите, что многочлены неприводимы над $\mathbb{F}_2$:

a) x^3+x^2+1;
b) $x^6+x^5+x^3+x^2+1$;
c) x^4+x^3+1;
d) $x^6+x^5+x^4+x^2+1$;
e) x^4+x^2+1;
f) $x^6+x^4+x^3+x+1$;
g) $x^5+x^4+x^3+x^2+x+1$;
h) $x^6+x^5+x^2+x+1$.

⑩ Докажите, что многочлен x^6+x+1 неприводим над $\mathbb{F}_2$.

⑪ Сколько существует неприводимых многочленов степени 2, степени 3, степени 4, степени 5 над $\mathbb{F}_2$, над $\mathbb{F}_3$, над $\mathbb{F}_5$?

⑫ Найдите число нормированных неприводимых многочленов степени 7 над $\mathbb{F}_5$; степени 11 над $\mathbb{F}_3$.

⑬ Найдите число нормированных неприводимых многочленов степени n над $\mathbb{F}_p$, если $n=50, 51, \ldots 100$, $p=17, 19, 23, 29$.

⑭ Верно ли в $\mathbb{F}_3[x]$ сравнение $2x^6+x^3+2x \equiv x+2 \pmod{x^4+x^2+2x}$?

⑮ Найдите все многочлены $f(x)$, для которых выполнено сравнение $g(x) \equiv h(x) \pmod{f(x)}$, если $g(x)=x^4+1$, $h(x)=x^2-1$, и многочлены рассматриваются над полем $\mathbb{F}_p$, $p=2, 3, 5, 7, 11$.

⑯ Разделите многочлен на многочлен с остатком в $\mathbb{Q}[x]$, в $\mathbb{F}_2[x]$, в $\mathbb{F}_3[x]$, в $\mathbb{F}_5[x]$:

(a) $2x^5+x^4+4x+3$ на $3x^2+1$;
(b) x^4-1 на $x-1$;
(c) x^6-x+1 на $x-1$;
(d) $x-1$ на x^2+x+5.

⑰ Рассматривая кольцо многочленов над полем $\mathbb{Q}$ (над полем $\mathbb{F}_2$, над полем $\mathbb{F}_3$, над полем $\mathbb{F}_5$), найдите многочлен $r(x)$, такой что $f(x) \equiv r(x) \pmod{g(x)}$, и $\deg r(x) < \deg g(x)$:

a) $f(x)=x^3+x^2+2x+2$, $g(x)=x^2+1$;
b) $f(x)=8x^8+6x^6+4x^4+2x^2$, $g(x)=6x+3$;
c) $f(x)=x^{20}+x^{10}+1$, $g(x)=x^5+1$.

⑱ Пусть $f(x)=x^3+x+1 \in \mathbb{F}_2[x]$. Постройте кольцо $\mathbb{F}_2[x]/(f(x))$. Является ли оно полем? Найдите его характеристику и порядок. Является ли оно изоморфным кольцу $\mathbb{Z}_8$? Имеет ли $f(x)$ корни в $\mathbb{F}_2[x]/(f(x))$?

⑲ Пусть $f(x)=x^2+x+2 \in \mathbb{F}_3[x]$. Докажите, что $f(x)$ неприводим. Постройте $\mathbb{F}_3[x]/(f(x))$. Является ли оно кольцом? Полем? Чему равна его характеристика? Порядок?

⑳ Найдите неприводимый многочлен степени 3 над $\mathbb{F}_2$ (над $\mathbb{F}_3$). Постройте поле $\mathbb{F}_8$ (поле $\mathbb{F}_{27}$). Сколько существует неприводимых многочленов степени 3 над $\mathbb{F}_2$? Сколько существует способов построения поля $\mathbb{F}_8$? Являются ли полученные поля изоморфными?

(21) Найдите два неприводимых многочлена третьей (четвертой) степени над $\mathbb{F}_2$. Постройте $\mathbb{F}_8$ ($\mathbb{F}_{16}$) двумя способами. Какие порядки могут иметь элементы поля $\mathbb{F}_8^*$ (поля $\mathbb{F}_{16}^*$)? Приведите примеры. Установите изоморфизм двух получившихся полей.

(22) Найдите порядки многочленов $x+1$, x^2+x+1, x^3+x+1, x^4+x+1 над $\mathbb{F}_2$.

(23) Найдите порядки многочленов $x+1$, $x+2$, x^2+1, x^2+x+2 над $\mathbb{F}_3$.

(24) Найдите все нормированные неприводимые многочлены степени 2, степени 3, степени 4 над $\mathbb{F}_2$ (над $\mathbb{F}_3$, над $\mathbb{F}_5$). Укажите их порядки.

(25) Найдите порядок:

a) многочлена$(x^2+x+1)^5(x^3+x+1)$ над $\mathbb{F}_2$;

b) многочлена $x^7-x^6+x^4-x^2+x$ над $\mathbb{F}_3$;

c) многочлена $x^8+x^7+x^3+x+1$ над $\mathbb{F}_2$.

(26) Над $\mathbb{F}_2$ и $\mathbb{F}_3$ найдите все нормированные, неприводимые и нормированные, примитивные многочлены 1-ой, 2-ой и 3-ей степени.

(27) Существуют ли над полем $\mathbb{F}_5$ неприводимый многочлен 7-ой степени; примитивные многочлены 3-ей степени?

(28) Найдите число примитивных многочленов степени 1, 2, 3, 4, 5 над $\mathbb{F}_2$ (над $\mathbb{F}_3$, над $\mathbb{F}_5$). Приведите примеры.

Задачи

[1] Разложите на множители:

a) $x^{64}-x$ над $\mathbb{F}_2$; c) $x^{27}-x$ над $\mathbb{F}_3$; e) $x^{125}-x$ над $\mathbb{F}_5$;

b) x^9-x над $\mathbb{F}_3$; d) $x^{25}-x$ над $\mathbb{F}_5$; f) x^8-x над $\mathbb{F}_2$.

[2] Докажите, что для любых натуральных чисел m и n имеет место соотношение $(x^n-1)|(x^m-1) \Leftrightarrow n|m$.

[3] Докажите, что неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^n-1}-1$; многочлен $x^{p^n}-x$.

[4] Докажите, что неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^m}-x$ тогда и только тогда, когда $n|m$.

[5] Докажите, что $p^n=\sum\limits_{m|n} m\cdot a_p(m)$, где $a_p(m)$ — число нормированных и неприводимых многочленов степени m над полем $\mathbb{F}_p$.

[6] Докажите, что функция Мебиуса *мультипликативна*, то есть $\mu(mn)=$ $=\mu(m)\cdot\mu(n)$ для взаимно простых натуральных чисел m и n.

[7] Докажите, что $\sum\limits_{d|n}\mu(d)=1$ для $n=1$, и $\sum\limits_{d|n}\mu(d)=0$ для $n>1$.

8 Докажите *формулу обращения Мебиуса*: $F(n) = \sum\limits_{d|n} f(d)$ тогда и только тогда, когда $f(n) = \sum\limits_{d|n} \mu(d) F\left(\frac{n}{d}\right)$.

9 Убедитесь, что

a) $\sum\limits_{d|n} \mu(d)\tau\left(\frac{n}{d}\right) = 1$;

b) $\sum\limits_{d|n} \mu(d)\frac{n}{d} = \varphi(n)$;

c) $\sum\limits_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = n$.

10 Докажите, что число $a_p(n)$ неприводимых над полем $\mathbb{F}_p$ многочленов степени n вычисляется по формуле $a_p(n) = \frac{1}{n}\sum\limits_{m|n} p^{\frac{n}{m}}\mu(m)$, где $\mu(n)$ — функция Мебиуса.

11 Докажите, что для всякого простого p и для всякого натурального n существуют неприводимые многочлены над полем $\mathbb{F}_p$ степени n.

12 Постройте конечное поле, содержащее ровно q элементов:

a) $q = 9$; d) $q = 27$; g) $q = 64$;
b) $q = 16$; e) $q = 32$; h) $q = 81$.
c) $q = 25$; f) $q = 49$;

13 Какие из указанных многочленов можно использовать для построения конечного поля характеристики 2, 3?

a) $x^2 + x + 1$; c) $x^4 + x^3 + x^2 + x + 1$;
b) $x^6 + x + 1$; d) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

14 Зная, что многочлен $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ неприводим над полем $\mathbb{F}_5$, найдите порядок многочлена

$$f(x) = x^4(x^2 + 1)^3(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^7$$

над $\mathbb{F}_5$.

15 Зная, что многочлен $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ неприводим над полем $\mathbb{F}_3$, найдите порядок многочлена

$$f(x) = x^5(x^2 + x + 1)^3(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^5$$

над $\mathbb{F}_3$.

16 Зная, что многочлен $x^6 + x + 1$ неприводим над полем $\mathbb{F}_5$, найдите порядок многочлена $f(x) = x^4(x^4 + 1)^3(x^6 + x + 1)^8$ над $\mathbb{F}_5$.

17 Зная, что многочлен $x^4 + x^3 + x^2 + x + 1$ неприводим над полем $\mathbb{F}_7$, найдите порядок многочлена $f(x) = x^4(x^2 + 1)^9(x^4 + x^3 + x^2 + x + 1)^7$ над F_7.

18 Зная, что многочлен $x^4+x^3+x^2+x+1$ неприводим над полем $\mathbb{F}_{13}$, найдите порядок многочлена $f(x)=x^4(x+1)^9(x^4+x^3+x^2+x+1)^3$ над $\mathbb{F}_{13}$.

19 Докажите, что примитивными могут быть только неприводимые многочлены.

20 Найдите минимальный многочлен для элемента α над полем $\mathbb{F}$:

a) $\alpha=-i$, $\mathbb{F}=\mathbb{R}$;

b) $\alpha=i\sqrt{2}$, $\mathbb{F}=\mathbb{C}$;

c) $\alpha=i\sqrt{2}$, $\mathbb{F}=\mathbb{Q}$;

d) $\alpha=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $\mathbb{F}=\mathbb{Q}$;

e) $\alpha=\sqrt[4]{2}$, $\mathbb{F}=\mathbb{Q}$;

f) $\alpha=\sqrt[4]{2}$, $\mathbb{F}=\mathbb{Q}[\sqrt{2}]$.

21 Найдите поля разложения многочленов x^4-x и $x^{16}-x$: над $\mathbb{R}$; над $\mathbb{F}_2$; над $\mathbb{F}_4$.

22 Пусть $a, b\in\mathbb{F}_{2^n}$, $2\nmid n$. Докажите, что $a^2+ab+b^2=0$ тогда и только тогда, когда $a=b=0$.

23 Пусть $a, b\in\mathbb{F}_{3^n}$, $7\nmid n$. Докажите, что $a^7+a^2b^5+2b^7=0$ тогда и только тогда, когда $a=b=0$.

24 Пусть $a, b\in\mathbb{F}_{5^n}$, $4\nmid n$. Докажите, что $a^4+3b^4=0$ тогда и только тогда, когда $a=b=0$.

25 Пусть $a\in\mathbb{F}_q$, $n\in\mathbb{N}$. Докажите, что многочлен $x^{q^n}-x+na$ делится на x^q-x+a в $\mathbb{F}_q[x]$.

26 Пусть $a\in\mathbb{F}_q^*$, $2\nmid q$. Докажите, что a — квадрат в $\mathbb{F}_q$ тогда и только тогда, когда $a^{(q-1)/2}=1$.

27 Пусть $a\in\mathbb{F}_q^*$, $k\in\mathbb{N}$, $d=(q-1,k)$. Докажите, что a — k-я степень в $\mathbb{F}_q$ тогда и только тогда, когда $a^{(q-1)/d}=1$.

28 Пусть $f(x)=x^2+x+1\in\mathbb{F}_2[x]$. Является ли $\mathbb{F}_2[x]/(f(x))$ расширением $\mathbb{F}_2$? Простым расширением? Конечным расширением? Указать базис и степень расширения.

29 Проведите по схеме задачи 28 анализ полей $\mathbb{F}_9=\mathbb{F}_3[x]/(f(x))$, $\mathbb{F}_{25}=\mathbb{F}_5[x]/(f(x))$, $\mathbb{F}_8=\mathbb{F}_2[x]/(f(x))$, $\mathbb{F}_{16}=\mathbb{F}_2[x]/(f(x))$, где в каждом из случаев $f(x)$ — соответствующий неприводимый многочлен.

30 Найдите все подполя поля $\mathbb{F}_{2^{100}}$ (поля $\mathbb{F}_{3^{24}}$, поля $\mathbb{F}_{5^{48}}$). Составьте диаграмму включений. Какие из подполей простые? Какие являются простыми конечными расширениями? Алгебраическими расширениями?

31 Найдите неприводимый многочлен степени 2 (3, 4) в $\mathbb{F}_4[x]$. Является ли он неприводимым в $\mathbb{F}_8[x]$? в $\mathbb{F}_{16}[x]$? в $\mathbb{F}_{32}[x]$? Какое поле будет его полем разложения?

32 Укажите поле разложения многочлена $f(x) = x^2 + x + 1$ над $\mathbb{F}_2$. Является ли оно расширением $\mathbb{F}_2$? Какой степени?

33 Укажите поле разложения многочлена $f(x) = x^3 - x$ над $\mathbb{F}_2$. Является ли оно расширением $\mathbb{F}_2$? Какой степени?

34 Элементы каких порядков входят в подполе $\mathbb{F}_2$ поля $\mathbb{F}_4$; в подполе $\mathbb{F}_4$ поля $\mathbb{F}_{16}$; в подполе $\mathbb{F}_3$ поля $\mathbb{F}_9$? Укажите эти элементы.

35 Докажите, что любой многочлен второй степени из $\mathbb{F}_q[x]$ разложим в $\mathbb{F}_{q^2}[x]$ на линейные множители.

36 Чему равна сумма элементов подполя $\mathbb{F}$ поля $\mathbb{F}_q$?

37 Пусть $a \in \mathbb{F}_{q^2}$. Докажите, что $a^{q+1} \in \mathbb{F}_q$.

8.3. Линейные рекуррентные последовательности над конечным полем

8.3.1. Псевдослучайные последовательности

Функционирование поточных криптосистем основано на использовании операции *гаммирования*, заключающейся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Указанная последовательность случайных чисел называется *гамма-последовательностью* и используется для шифрования и дешифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Поскольку для кодирования любого множества сообщений достаточно алфавита из двух символов, можно использовать конечное поле $\mathbb{F}_2$, в котором суммирование принимает простейший вид: $0 + 0 = 1 + 1 = 0$, $1 + 0 = 0 + 1 = 1$.

На практике невозможно получить истинно случайную последовательность, поскольку при генерации любой последовательности мы пользуемся тем или иным алгоритмом. Используемые на практике последовательности, генерируемые с помощью различных, как правило, арифметических алгоритмов, называются *псевдослучайными* [78].

Пример 8.3.17 Рассмотрим несколько псевдослучайных последовательностей, которые можно получить с помощью арифметических функций.

Если $\alpha_n = \lfloor \pi \cdot 10^n \rfloor - 10 \cdot \lfloor \pi \cdot 10^{n-1} \rfloor$, то для $n = 0, 1, 2, 3, \ldots$ мы получаем $\alpha_n = 3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5, 8, 9, 7, 9, \ldots$.

Если $\alpha_n = \left\lfloor \frac{1}{7} \cdot 10^n \right\rfloor - 10 \cdot \left\lfloor \frac{1}{7} \cdot 10^{n-1} \right\rfloor$, то для $n = 0, 1, 2, 3, \ldots$ мы получаем $\alpha_n = 0, 1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, 1, 4, \ldots$.

Если же $\alpha_0 = 0$, $\alpha_1 = 1$ и $\alpha_{n+1} = \mathrm{rest}(\alpha_n + \alpha_{n-1}, 2)$ при любом натуральном n, то значения начнут очень быстро повторяться: $\alpha_n = 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots$. □

В современных потоковых криптосистемах применяются периодические псевдослучайные последовательности $\alpha = \{\alpha_n\}_{n=0}^{\infty}$ (или, коротко, $\alpha = \{\alpha_n\}_n$) с большими периодами: если период последовательности достаточно велик, то вскрытие системы путем подбора ключа практически невозможно.

Простейшая криптосистема, позволяющая осуществлять передачу сколь угодно большого объема сообщений, выглядит следующим образом. Схема состоит из передатчика и приемника. В передатчик входит преобразователь, который преобразует поступающую информацию в двоичную последовательность $\{\alpha_n\}_n$ и передает в сумматор $\boxplus$. Устройство Γ вырабатывает гамма-последовательность — псевдослучайную периодическую последовательность $\{\gamma_n\}_n$ с весьма большим периодом, и также передает ее в сумматор $\boxplus$. Полученные символы α_n и γ_n сумматор $\boxplus$ перерабатывает в символ $\beta_n = \alpha_n + \gamma_n$, руководствуясь правилами $1+1=0+0=0$, $1+1=0+1=1$. Выходной преобразователь преобразует полученную таким образом последовательность $\{\beta_n\}_n$ в последовательность электромагнитных импульсов и отправляет ее в эфир или по телеграфу.

Переданная серия попадает во входной преобразователь, преобразуется в последовательность $\{\beta_n\}_n$, а затем подается в сумматор $\boxplus_1$. Устройство Γ_1 приемника, как и устройство Γ передатчика, вырабатывает псевдослучайную последовательность $\{\gamma_n\}_n$ и передает ее в сумматор $\boxplus_1$. Полученные символы сумматор $\boxplus_1$ переводит в последовательность $\{\alpha_n\}_n$ путем повторного двоичного суммирования и отправляет ее в выходной преобразователь. В результате корреспондент получит отправленное сообщение. Для успешной работы необходимо, чтобы устройства Γ и Γ_1, генерирующие гамма-последовательность, работали синхронно.

Для этого можно воспользоваться такой упрощенной процедурой. Два корреспондента заранее договорившись о выборе некоторого ненулевого (желательно — примитивного) элемента поля $\mathbb{F}_{2^n}$, независимо друг от друга выбирают натуральные числа α и β, меньшие $2^n - 1$. Возводя g в степень α, первый корреспондент получает значение g^α, в то время как второй — значение g^β. Обмениваясь результатами и повторно возводя полученную от партнера величину в «свою» степень, они получают искомый общий ключ $g^{\alpha\beta}$. Этот ключ в заранее определенное время они и закладывают в шифрующее устройство, определяющее псевдослучайную последовательность.

Предполагаемся, что противнику известна оговоренная заранее величина β, а также перехваченные величины g^α и g^β. Для решения задачи восстановления общего ключа респондентов $g^{\alpha\beta}$ остается найти величину α (или β), что приводит нас к задаче дискретного логарифмирования в поле $\mathbb{F}_{2^n}$ [78].

8.3.2. Последовательности над конечным полем

Для генерации псевдослучайных последовательностей можно использовать многочлены над конечными полями. Рассмотрим основы теории таких построений [78], [55].

Пусть $S(\mathbb{F}_p) = \{\alpha = \{\alpha_n\}_n | n = 0, 1, 2, \ldots \alpha_n \in F_p\}$ — множество всех последовательностей $\alpha = \{\alpha_n\}_n$ элементов поля $\mathbb{F}_p$.

Определим на множестве $S(\mathbb{F}_p)$ бинарную операцию $+$ и две унарные операции — *умножение на элемент с поля* $\mathbb{F}_p$ и *сдвиг* T:

$$\alpha + \beta = \{\alpha_n\}_n + \{\beta_n\}_n = \{\alpha_n + \beta_n\}_n;$$

$$c\alpha = c\{\alpha_n\}_n = \{c\alpha_n\}_n,\ T \bullet \alpha = T \bullet \{\alpha_n\}_n = \{\alpha_{n+1}\}_n.$$

Нетрудно убедиться, что теперь множество $S(\mathbb{F}_p)$ образует векторное пространство над полем $\mathbb{F}_p$, замкнутое относительно сдвига.

С каждым многочленом $g(\lambda) = b_0 + b_1\lambda + b_2\lambda^2 + \ldots + b_k\lambda_k \in F_p[\lambda]$ сопоставим *полиномиальный оператор* g^T, определяемый по следующему закону:

$$g^T \bullet \alpha = g^T \bullet \{\alpha_n\}_n = \{\beta_n\}_n = \beta,$$

где, для любого целого неотрицательного n,

$$\beta_n = b_0 \cdot \alpha_n + b_1\alpha_{n+1} + b_2\alpha_{n+2} + \ldots + b_k\alpha_{n+k}.$$

Свойства полиномиальных операторов

1. $g^T \bullet (\alpha + \beta) = g^T \bullet \alpha + g^T \bullet \beta$.
2. $(g + f)^T \bullet \alpha = g^T \bullet \alpha + f^T \bullet \alpha$.
3. $g^T \bullet (h^T \bullet \alpha) = (gh)^T \bullet \alpha$.
4. $g(\lambda) \equiv h(\lambda) \Leftrightarrow \ \forall\, \alpha \in S\ g^T \bullet \alpha = h^T \bullet \alpha$.
5. Если $g(\lambda) = \lambda + 1$, то $g^T \bullet \alpha = T \bullet \alpha$.
6. Если $g(\lambda) \equiv c$, $c \in F_p$, то $g^T \bullet \alpha = c\alpha$.

Пример 8.3.18 Если $g(\lambda) = x^2 + x + 1 \in F_2[x]$, $\alpha = \{\alpha_n\}_n \in S(\mathbb{F}_2)$, то $g^T \bullet \alpha = g^T \bullet \{\alpha_n\}_n = \{\alpha_n + \alpha_{n+1} + \alpha_{n+2}\}_n$. Последовательность $\varepsilon = \{1\}_n$, состоящая из одних единиц (как и последовательность $\theta = \{0\}_n$, состоящая из одних нулей), перейдет при этом отображении в себя, а, например, последовательность $000100010001\ldots$ — в последовательность $101110111011\ldots$. Многочлен $g(\lambda) = 1 + x$ соответствует сдвигу T, переводя последовательность ε (как и последовательность θ) в себя, а последовательность $000100010001\ldots$ — в последовательность $001000100010\ldots$. Многочлен $g(\lambda) \equiv c$ соответствует оператору умножения на элемент $c \in F_p$. Над полем $\mathbb{F}_2$ мы имеем ровно две возможности: при $c = 1$ оператор $g(\lambda) \equiv c$ переводит каждую последовательность в себя, в то время как при $c = 0$ оператор $g(\lambda) \equiv c$ переводит каждую последовательность в нулевую последовательность $\theta = \{0\}_n$. □

8.3.3. Линейные рекуррентные последовательности

Назовем уравнение вида

$$\delta_{x+n} = a_{n-1} \cdot \delta_{x+n-1} + a_{n-2} \cdot \delta_{x+n-2} + \ldots + a_0 \cdot \delta_x, \quad \text{где } a_i \in F_p,$$

линейным рекуррентным уравнением порядка n над полем F_p, а многочлен $f(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - \ldots - a_0 \in F_p[x]$ — *характеристическим многочленом* этого уравнения.

Уравнение определяет *линейную рекуррентную последовательность* $\{\delta_x\}_x$ над полем F_p, которая называется *решением* данного линейного уравнения и однозначно определяется своими начальными членами $\delta_0, \delta_1, \ldots \delta_{n-1}$: зная $\delta_0, \delta_1, \ldots \delta_{n-1}$, мы найдем $\delta_n = a_{n-1} \cdot \delta_{n-1} + a_{n-2} \cdot \delta_{n-2} + \ldots + a_0 \cdot \delta_0$; зная $\delta_1, \delta_2, \ldots \delta_n$, мы найдем $\delta_{n+1} = a_{n-1} \cdot \delta_n + a_{n-2} \cdot \delta_{n-1} + \ldots + a_0 \cdot \delta_1$; зная $\delta_2, \delta_3, \ldots \delta_{n+1}$, мы найдем $\delta_{n+2} = a_{n-1} \cdot \delta_{n+1} + a_{n-2} \cdot \delta_n + \ldots + a_0 \cdot \delta_2$, и т. д.

Пример 8.3.19 Рассмотрим линейное рекуррентное уравнение второго порядка $\delta_{x+2} = \delta_{x+1} + \delta_x$ над полем F_2, отвечающее характеристическому многочлену $f(\lambda) = \lambda^2 - \lambda - 1$. Решениями уравнения являются четыре последовательности, три из которых ненулевые. Все три ненулевые последовательности имеют период 3 и являются сдвигами друг друга.

x	0	1	2	3	4	5	6	...	
δ_x	0	0	0	0	0	0	0	...	$\operatorname{per}\delta = 1$
δ_x	0	1	1	0	1	1	0	...	$\operatorname{per}\delta = 3$
δ_x	1	0	1	1	0	1	1	...	$\operatorname{per}\delta = 3$
δ_x	1	1	0	1	1	0	1	...	$\operatorname{per}\delta = 3$

Линейное рекуррентное уравнение $\delta_{x+2} = \delta_x$ второго порядка над полем F_2 отвечает характеристическому многочлену $g(\lambda) = \lambda^2 - 1$. Как и в предыдущем случае, решениями уравнения являются четыре последовательности, три из которых ненулевые. Среди ненулевых последовательностей две имеют период 2, и одна — период 1. При этом последовательности, имеющие период 2, являются сдвигами друг друга.

x	0	1	2	3	4	5	6	...	
δ_x	0	0	0	0	0	0	0	...	$\operatorname{per}\delta = 1$
δ_x	0	1	0	1	0	1	0	...	$\operatorname{per}\delta = 2$
δ_x	1	0	1	0	1	0	1	...	$\operatorname{per}\delta = 2$
δ_x	1	1	1	1	1	1	1	...	$\operatorname{per}\delta = 1$

Видимо, отличие в поведении решений двух рассмотренных линейных рекуррентных уравнений связано с тем, что первый многочлен $f(\lambda)$ неприводим, а второй многочлен $g(\lambda)$ — приводим в $F_2[\lambda]$. □

Рассматривая пример, мы убедились, что число решений линейного рекуррентного уравнения конечно, и каждое решение — периодично. Оба этих факта тривиальны. Поскольку решение линейного рекуррентного уравнения однозначно определяется начальным набором $\delta_0, \delta_1, \ldots \delta_{n-1}$, и над полем $\mathbb{F}_p$ существует ровно p^n таких наборов, то *число решений* $|S(f)|$ *уравнения*

$$\delta_{x+n} = a_{n-1} \cdot \delta_{x+n-1} + a_{n-2} \cdot \delta_{x+n-2} + \ldots + a_0 \cdot \delta_x$$

отвечающего характеристическому многочлену $f(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - \ldots - a_0$, *равно* p^n.

Из конечности числа возможных наборов $(\delta_x, \delta_{x+1}, \ldots \delta_{x+n-1})$ длины n над конечным полем $\mathbb{F}_p$ следует и периодичность линейных рекуррентных последовательностей: для любого решения $\delta = \{\delta_x\}_x \in S(f)$ линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену степени n, существует натуральное τ, такое что $\delta_x = \delta_{x+\tau}$ для любого целого неотрицательного x.

Наименьший натуральный период τ решения δ называется *примитивным периодом* решения δ и обозначается символом $\operatorname{per}\delta$. Поскольку число ненулевых наборов $(\delta_x, \delta_{x+1}, \ldots \delta_{x+n-1})$ длины n над конечным полем $\mathbb{F}_p$ равно $p^n - 1$, то наименьший натуральный период τ решения δ не превосходит $p^n - 1$.

Эти и другие свойства линейных рекуррентных последовательностей делают их необычайно полезными при решении практических криптографических задач [78], [55].

Свойства линейных рекуррентных последовательностей

1. Нулевая последовательность $\theta = \{0\}_n \in S(\mathbb{F}_p)$ является решением любого линейного рекуррентного уравнения над полем $\mathbb{F}_p$; ее называют *нулевым решением*.
2. Число решений линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену $f \in F_p[\lambda]$ степени n на полем $\mathbb{F}_p$, равно p^n: $|S(f)| = p^n = p^{\deg f}$; число ненулевых решений равно $p^n - 1$.
3. Множество $S(f)$ замкнуто относительно сложения, умножения на элементы поля $\mathbb{F}_p$ и сдвига: если $\delta, \gamma \in S(f)$, и $c \in F_p$, то $\delta + \gamma \in S(f)$, $c\delta \in S(f)$, $T \bullet \alpha \in S(f)$.
4. Множество $S(f)$ замкнуто относительно действия любого полиномиального оператора: если $\delta \in S(f)$ и $g \in F_p[\lambda]$, то $g^T \bullet \delta \in S(f)$.

5. Множество $S(f)$ решений линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену $f \in F_p[\lambda]$ степени n над полем $\mathbb{F}_p$, образует n-мерное векторное пространство над полем F_p.
6. Любое решение линейного рекуррентного уравнения над полем F_p, отвечающего характеристическому многочлену $f \in F_p[\lambda]$ степени n, периодично с примитивным периодом τ, не превосходящим $p^n - 1$.

Поскольку множество $S(f)$ решений линейного рекуррентного уравнения, отвечающего характеристическому многочлену $f(\lambda) \in F_p[\lambda]$, замкнуто относительно сложения и умножения на элементы поля $\mathbb{F}_p$, то оно формирует векторное пространство над полем $\mathbb{F}_p$. Сопоставив каждой линейной рекуррентной последовательности $\delta = \{\delta_x\}_x$ вектор $(\delta_0, \delta_1, \ldots \delta_n)$ ее начальных значений (полностью эту последовательность задающий), мы убедимся, что векторное пространство решений линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену степени n, изоморфно классическому n-мерному векторному пространству над полем $\mathbb{F}_p$.

Назовем решение $\delta = \{\delta_x\}_x$ линейного рекуррентного уравнения *главным*, если вместе со своими сдвигами оно образует базис пространства $S(f)$ всех решений данного линейного рекуррентного уравнения. *Максимальной линейной рекуррентной последовательностью порядка* n назовем любое главное решение линейного рекуррентного уравнения порядка n.

Пример 8.3.20 Для рассмотренного выше линейного рекуррентного уравнения второго порядка $\delta_{x+2} = \delta_{x+1} + \delta_x$ над полем $\mathbb{F}_2$, отвечающего характеристическому многочлену $f(\lambda) = \lambda^2 - \lambda - 1$, главным решением является любое ненулевое решение, так как все остальные ненулевые решения являются его сдвигами, а нулевое есть сумма всех этих сдвигов. Следовательно, каждое из указанных трех ненулевых решений является максимальной линейной рекуррентной последовательностью порядка 2.

Для линейного рекуррентного уравнения $\delta_{x+2} = \delta_x$ второго порядка над полем $\mathbb{F}_2$, отвечающего характеристическому многочлену $g(\lambda) = \lambda^2 - 1$, в качестве главных решений могут выступать только второе и третье решения. Четвертое (ненулевое) решение вместе со своими сдвигами не может породить все пространство решений, в то время как сумма второго и третьего (сдвига второго) дают нам четвертое решение, а нулевое решение может быть получено путем сложения четвертого решения с его копией.

□

8.3.4. Аннулирующие многочлены

Многочлен $g(\lambda) \in F_2[\lambda]$ называют *аннулирующим последовательность* $\delta = \{\delta_n\}_n \in S(\mathbb{F}_p)$, если $g^T \bullet \delta = \theta$, где $\theta = \{0\}_n$ — последовательность, состоящая из одних нулей. Нормированный и наименьшей степени многочлен, аннулирующий $\delta = \{\delta_n\}_n \in S(\mathbb{F}_p)$, называют *минимальным многочленом последовательности* δ и обозначают символом $m_\delta(\lambda)$.

Пример 8.3.21 Нетрудно убедиться в том, что для нулевой последовательности $\theta = \{0\}_n$ любой многочлен будет аннулирующим, и, следовательно, $m_\theta(\lambda) \equiv 1$.

Для единичной последовательности $\varepsilon = \{1\}_n$ любой многочлен $\lambda^k - 1$, $k \in \mathbb{N}$, будет аннулирующим, и, следовательно, $m_\varepsilon(\lambda) = \lambda - 1$. Аналогичный результат можно получить для любой ненулевой последовательности — константы $\delta = \{\delta\}_n$.

Для последовательности 010101010101... аннулирующим будет любой многочлен $\lambda^{2k} - 1$, $k \in \mathbb{N}$. Непосредственная проверка показывает, что минимальным многочленом данной последовательности будет многочлен $\lambda^2 - 1$. Вспомнив, что последовательность 010101010101... является одним из решений линейного рекуррентного уравнения $\delta_{x+2} = \delta_x$, отвечающего характеристическому многочлену $f(\lambda) = \lambda^2 - 1$, мы замечаем, что минимальный многочлен одного из решений линейного рекуррентного уравнения $\delta_{x+2} = \delta_x$ совпадает с характеристическим многочленом данного линейного рекуррентного уравнения. Случайность ли это? □

Для того чтобы ответить на этот вопрос, рассмотрим поведение многочленов, аннулирующих линейные рекуррентные последовательности [78], [55]. Как и ранее, будем считать, что $S(f)$ — множество решений линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену $f(\lambda)$ степени n.

Свойства аннулирующих многочленов линейных рекуррентных последовательностей

1. Минимальный многочлен любого ненулевого решения $\delta \in S(f)$ является многочленом ненулевой степени: $\delta \neq \theta \Leftrightarrow \deg m_\delta(\lambda) \geqslant 1$.
2. Если τ — примитивный период решения $\delta \in S(f)$, то многочлен $\lambda^\tau - 1$ является аннулирующим для решения $\delta \in S(f)$.
3. Характеристический многочлен линейного рекуррентного уравнения аннулирует любое решение этого уравнения.
4. Пусть $\delta \in S(\mathbb{F}_p)$, и $f(\lambda) = \lambda^n - a_1\lambda^{n-1} - \ldots - a_{n-1}\lambda - a_n$ — нормированный многочлен степени n над полем $\mathbb{F}_p$ с не равным нулю свободным

членом. Оператор f^T аннулирует последовательность δ тогда и только тогда, когда δ — решение линейного рекуррентного уравнения с характеристическим многочленом f.

5. Многочлен g над полем $\mathbb{F}_p$ аннулирует последовательность $\delta \in S(\mathbb{F}_p)$ тогда и только тогда, когда g делится на минимальный многочлен последовательности δ (*основное свойство минимального многочлена*): $g^T \bullet \delta = \theta \Leftrightarrow m_\delta(\lambda) | g(\lambda)$.
6. Минимальный многочлен главного решения уравнения есть характеристический многочлен этого уравнения.
7. Пусть $\delta \in S(f)$. Тогда $\operatorname{per} \delta = \operatorname{ord} m_\delta(\lambda)$.
8. Для главного решения δ линейного рекуррентного уравнения, отвечающего характеристическому многочлену $f(\lambda)$, $per\ \delta = \operatorname{ord} f(\lambda)$.
9. Если характеристический многочлен $f(\lambda)$ линейного рекуррентного уравнения неприводим, то $f(\lambda) = m_\delta(\lambda)$ для любого ненулевого решения δ этого уравнения.
10. Если δ — ненулевое решение линейного рекуррентного уравнения с неприводимым характеристическим многочленом $f(\lambda)$, то $\operatorname{per} \delta | (p^n - 1)$, в частности, $\operatorname{per} \delta = p^n - 1$, если $f(\lambda)$ — примитивный многочлен.

Изучая свойства аннулирующих многочленов, мы убеждаемся в том, что длина периода того или иного решения δ линейного рекуррентного уравнения над полем $\mathbb{F}_p$ с характеристическим многочленом $f(\lambda)$ степени n зависит как от свойств самой последовательности δ — для практических целей целесообразно использовать главные решения линейного рекуррентного уравнения — так и от свойств характеристического многочлена $f(\lambda)$. Если он неприводим, то все ненулевые решения линейного рекуррентного уравнения становятся в некотором смысле «равноправными», то есть нас может не заботить их оптимальный выбор. Если же, кроме того, многочлен $f(\lambda)$ примитивен, то генерируемые соответствующим линейным рекуррентным уравнением последовательности будут иметь максимально возможный период.

Так, работая над полем F_2 и имея в запасе примитивный многочлен степени 100 над F_2, мы имеем возможность, задавая вектор начальных условий относительно небольшой длины 100, получать на выходе последовательность, период которой $2^{100} - 1$ необычайно велик. Это определяет высокую меру близости заданной псевдослучайной последовательности к случайной.

Еще одним техническим, но существенным преимуществом генерирования псевдослучайных последовательностей является необычайная простота технической реализации этого процесса, выражающаяся в использо-

вании специальной электронной схемы: *регистра сдвига*, получающегося комбинацией ячеек памяти и сумматора, в котором происходит побитовое сложение приходящей на два имеющихся у него входа информации [78].

Пример 8.3.22 Рассмотрим уравнение $\delta_{x+5} = \delta_x + \delta_{x+3}$. Его характеристический многочлен имеет вид $f(\lambda) = \lambda^5 + \lambda^3 + 1$. Пользуясь представленной в главе 10 таблицей, убеждаемся, что он примитивен. Следовательно, период любого ненулевого решения заданного линейного рекуррентного уравнения должен быть равен 31.

Выбирая первоначальное заполнение $\delta_0 = 1$, $\delta_1 = 0$, $\delta_2 = 0$, $\delta_3 = 0$, $\delta_4 = 0$, получим периодическую последовательность

$$10000101011101100011111001101001000 0 \ldots .$$

Непосредственная проверка показывает, что примитивный период этой последовательности равен 31. Это означает, что, шаг за шагом рассматривая 5-символьные наборы $(\delta_x, \delta_{x+1}, \delta_{x+2}, \delta_{x+3}, \delta_{x+4})$ элементов нашей последовательности для $x = 0$ (набор 10000), $x = 1$ (набор 00001), ..., $x = 30$ (набор 01000), мы получим каждый ненулевой набор из пяти знаков 0 и 1 ровно один раз. Если с набором $(\delta_x, \delta_{x+1}, \delta_{x+2}, \delta_{x+3}, \delta_{x+4})$ сопоставить число $a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + a_4 \cdot 2^4$, то нашу линейную рекуррентную последовательность можно рассматривать и как последовательность чисел 1 16 8 20 10 21 26 29 14 23 27 13 6 3 17 24 28 30 31 15 7 19 25 12 22 11 5 18 9 4 2 ....

Нетрудно убедиться, что период этой последовательности равен 31, и каждое из чисел от 1 до 31 встречается на начальном отрезке последовательности ровно один раз.

Всего у уравнения $2^5 = 32$ решения, из них 31 ненулевое. При этом остальные ненулевые решения — это 30 различных сдвигов решения, полученного выше. В таблице представлено нулевое решение, рассмотренное ненулевое решение и три его сдвига — «первый», «второй» и «последний».

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0
0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1
0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0
...																														
0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0

□

Пример 8.3.23 Рассмотрим уравнение $\delta_{x+5} = \delta_x + \delta_{x+4}$. Его характеристический многочлен имеет вид $f(\lambda) = \lambda^5 + \lambda^4 + 1$. Он приводим над полем $\mathbb{F}_2$: $\lambda^5 + \lambda^4 + 1 = (\lambda^3 + \lambda + 1) \cdot (\lambda^2 + \lambda + 1)$.

В этом случае $\operatorname{ord} f(\lambda) = [\operatorname{ord}(\lambda^2+\lambda+1), \operatorname{ord}(\lambda^3+\lambda+1)] = [3, 7] = 21$. Следовательно, мы можем получить 21 главное решение (с примитивным периодом 21), минимальным многочленом каждого из которых является многочлен $\lambda^5+\lambda^4+1$, 3 решения с примитивным периодом 3, минимальным многочленом каждого из которых является многочлен $\lambda^2 + \lambda + 1$, и 7 решений с примитивным периодом 7, минимальным многочленом для каждого из которых является многочлен $\lambda^3 + \lambda + 1$. Добавив нулевое решение, получаем все $21 + 3 + 7 + 1 = 32$ решения нашего линейного рекуррентного уравнения. В таблице представлены все четыре класса решений; жирным шрифтом выделено первое повторение начальных значений последовательности.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	**0**	**0**	**0**	**1**	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	1	**0**	**0**	**0**	**0**	**1**
0	**1**	**1**	**0**	**1**	**1**	0	1	1	0	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1
0	**0**	**1**	**0**	**1**	1	1	**0**	**0**	**1**	**0**	**1**	1	1	0	0	1	0	1	1	1	0	0	1	0	1

□

Упражнения

(1) Вычислите 15 первых членов последовательности $\alpha = \{\alpha_n\}_n$:

a) $\alpha_n = (\mu(n))^2$;

b) $\alpha_0 = b$, $\alpha_{n+1} = \operatorname{rest}(\alpha_n + a, m)$, $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$;

c) $\alpha_n = \lfloor e \cdot 10^{n+1} \rfloor - 10^2 \cdot \lfloor e \cdot 10^{n-1} \rfloor$;

d) $\alpha_n = \operatorname{sign}(\sin n!)$;

e) $\alpha_n = 2 + \operatorname{rest}(2n!, n + 1)$.

(2) Вычислите 15 первых членов последовательности $\alpha = \{\alpha_n\}_n \in \mathbb{Z}_p$, $p \in \{2, 3, 5, 7\}$:

a) $\alpha_0 = 1$, и $\alpha_{n+1} \equiv \alpha_n^4 + \alpha_n^2 - 1 \pmod p$;

b) $\alpha_0 = 0$, и $\alpha_{n+1} \equiv \alpha_n^5 - \alpha_n + 13 \pmod p$;

c) $\alpha_0 = 1$, и $\alpha_{n+1} \equiv \lfloor \sqrt{\alpha_n^3} \rfloor + 2 \pmod p$;

d) $\alpha_0 = 1, \alpha_1 = 0$, и $\alpha_{n+2} \equiv \alpha_{n+1}^2 - (-1)^{\alpha_n} \pmod p$;

e) $\alpha_0 = 1, \alpha_1 = 1$, и $\alpha_{n+2} \equiv \alpha_{n+1}^{\mathrm{rest}(\alpha_n, 3)} \pmod p$;

f) $\alpha_0 = 1,\ \alpha_1 = 0,\ \alpha_{n+2} \equiv \alpha_{n+1}^3 + \alpha_n^3 \pmod p$;

g) $\alpha_0 = 1, \alpha_1 = 1, \alpha_2 = 1$, и $\alpha_{n+3} \equiv \alpha_{n+2} - \alpha_{n+1} \cdot \lceil \cos \alpha_n \rceil \pmod p$;

h) $\alpha_0 = 1,\ \alpha_1 = 0$, и $\alpha_{n+2} \equiv (-1)^{\alpha_n} + \alpha_{n+1}\alpha_n \pmod p$.

③ Для $\alpha \in S(\mathbb{F}_2)$ найдите последовательности $c\alpha$ $(c \in F_2)$, $T \bullet \alpha$ и $g^T \bullet \alpha$ $(g(x) = x^3 + x + 1 \in F_2[x])$:

a) $\alpha = \theta = \{0\}_n$;

b) $\alpha = \varepsilon = \{1\}_n$;

c) $\alpha = 010101010101\ldots$;

d) $\alpha = 111011101110\ldots$;

e) $\alpha = 011111011111\ldots$;

f) $\alpha = 110011001100\ldots$.

Приведите пример многочлена, аннулирующего последовательность α.

④ Постройте последовательность $\beta = g^T \bullet \alpha$, если:

a) $g(x) \equiv 1 \in F_2[x]$, $\alpha_n \equiv n^2 \pmod 2 \in F_2$;

b) $g(x) = x \in F_3[x]$, $\alpha_n \equiv 2n^3 - n + 1 \pmod 3 \in F_3$;

c) $g(x) = x + 1 \in F_2[x]$, $\alpha_n \equiv n^{3n^2-1} \pmod 2 \in F_2$;

d) $g(x) = x^2 + 1 \in F_3[x]$, $\alpha_n = Rest(n_n^3, 2) \in F_3$;

e) $g(x) = x^3 + 3x + 2 \in F_5[x]$, $\alpha_n \equiv n^3 + n \pmod 5 \in F_5$;

f) $g(x) = x^4 + 1 \in F_5[x]$, $\alpha_n = REST(3^n, 4) \in F_5$.

⑤ Пусть $\alpha = \{\alpha_n\}_n$ — одна из последовательностей упражнения 2. Постройте последовательность $\beta = g^T \bullet \alpha$, если:

a) $g(x) \equiv 3 \in F_p[x]$;

b) $g(x) = x \in F_p[x]$;

c) $g(x) = x + 1 \in F_p[x]$;

d) $g(x) = x^2 + 1 \in F_p[x]$;

e) $g(x) = x^3 + 3x + 2 \in F_p[x]$;

f) $g(x) = x^4 + 1 \in F_p[x]$.

⑥ Найдите все решения линейного рекуррентного уравнения:

a) $\delta_{x+4} = \delta_x + \delta_{x+3}$;

b) $\delta_{x+4} = \delta_x + \delta_{x+1} + \delta_{x+2} + \delta_{x+3}$.

Определите период каждого из найденных решений. Укажите все главные решения.

⑦ Сколько ненулевых решений имеют линейные рекуррентные уравнения:

a) $\delta_{x+4} = \delta_x + \delta_{x+3}$;

b) $\delta_{x+6} = \delta_x + \delta_{x+1} + \delta_{x+2} + \delta_{x+3}$;

c) $\delta_{x+5} = \delta_x + \delta_{x+3}$;

d) $\delta_{x+4} = \delta_x + \delta_{x+1} + \delta_{x+2} + \delta_{x+3}$?

⑧ Покажите, что характеристический многочлен является аннулирующим для любого решения линейного рекуррентного уравнения. Проверьте это для решений линейных рекуррентных уравнений упражнений 6 и 7. Приведите для каждого из рассмотренных линейных

рекуррентных уравнений пример еще одного многочлена, аннулирующего каждое решение; пример многочлена, аннулирующего только одно решение.

(9) Укажите число решений и найдите все решения линейного рекуррентного уравнения над полем $\mathbb{F}_2$ (над полем $\mathbb{F}_3$):

a) $\delta_{x+2} = \delta_{x+1} + \delta_x$;
b) $\delta_{x+3} = \delta_{x+2} + 2\delta_{x+1} + \delta_x$;
c) $\delta_{x+4} = \delta_{x+3} + \delta_x$;
d) $\delta_{x+5} = \delta_{x+3} + \delta_x$;
e) $\delta_{x+4} = \delta_{x+3} + \delta_{x+2} + \delta_{x+1} + \delta_x$;
f) $\delta_{x+5} = \delta_{x+4} + \delta_x$.

Укажите период каждого решения. Проанализируйте свойства характеристических многочленов заданных линейных рекуррентных уравнений (приводимые, неприводимые, примитивные). Сделайте вывод о периоде τ_δ каждого из решений.

(10) Составьте линейное рекуррентное уравнение порядка n, $n \in \{1, 2, 3, 4, 5, 6\}$ над полем $\mathbb{F}_p$, $p \in \{2, 3\}$, используя в качестве характеристического многочлена примитивный многочлен над $\mathbb{F}_p$. Решите полученное уравнение. Убедитесь, что все ненулевые решения являются главными. Каков период каждого из ненулевых решений?

Задачи

1 Вычислите 15 членов псевдослучайной последовательности по методу середин квадратов: предыдущее случайное число возводится в квадрат, а затем из результата извлекаются средние цифры.

2 Вычислите 15 членов псевдослучайной последовательности α по линейному конгруэнтному методу: выбрав случайным образом α_0 из множества $\{0, 1, 2, \ldots m-1\}$, положим $\alpha_{n+1} \equiv a\alpha_n + c \pmod m$, где m — натуральное число, большее единицы, и $a, c \in \mathbb{Z}$. Используйте эту задачу для построения псевдослучайных последовательностей над конечным полем.

3 Докажите, что множество всех последовательностей элементов конечного поля образует векторное пространство, замкнутое относительно сдвига.

4 Докажите, что если $g(\lambda)$ и $h(\lambda) \in \mathbb{F}_p[\lambda]$, и $\alpha, \beta \in S(\mathbb{F}_p)$, то $g^T \bullet (\alpha+\beta) = g^T \bullet \alpha + g^T \bullet \beta$; $(g^T + h^T) \bullet \alpha = g^T \bullet \alpha + h^T \bullet \alpha$; $g^T \bullet (h^T \bullet \alpha) = (g^T \cdot h^T) \bullet \alpha$.

5 Докажите, что множество полиномиальных операторов над полем $\mathbb{F}_p$ образует кольцо, изоморфное кольцу многочленов $\mathbb{F}_q[x]$.

6 Докажите, что множество решений линейного рекуррентного уравнения степени n над $\mathbb{F}_q$ образует векторное пространство размерности n над $\mathbb{F}_q$, замкнутое относительно сдвига.

7 Докажите, что если $\delta \in S(f)$, где $f \in F_p[\lambda]$ — многочлен степени n, то $\operatorname{per}\delta \leqslant p^n - 1$. Докажите, что если $\delta \in S(f)$, и многочлен $f \in F_p[x]$ степени n неприводим, то $\operatorname{per}\delta | (p^n - 1)$.

8 Выясните, являются ли многочлены $\lambda^5+\lambda^3+1$, $\lambda^4+\lambda^3+1$, $\lambda^4+\lambda^3+\lambda^2+\lambda+1$ над $\mathbb{F}_2$ неприводимыми; примитивными. Чему равны их порядки? Для каждого из заданных многочленов постройте и решите соответствующее ему линейное рекуррентное уравнение. Проанализируйте полученные результаты.

9 Пусть f — неприводимый многочлен четвертой степени над полем $\mathbb{F}_2$ (над полем $\mathbb{F}_3$, над полем $\mathbb{F}_5$). Может ли период ненулевого решения линейного рекуррентного уравнения с характеристическим многочленом f быть равным 1; 2; 3; ...20?

10 Найдите многочлен, период главного решения которого будет равен 15; 6; 8; 12. Найдите как минимум по два решения к каждому случаю.

11 Пусть характеристический многочлен линейного рекуррентного уравнения над $\mathbb{F}_3$ неприводим и имеет степень 4. Может ли период ненулевого решения этого уравнения быть равным 5; 3; 4; 20?

12 Приведите пример линейного рекуррентного уравнения, решением которого является последовательность с периодом 11.

13 Может ли линейное рекуррентное уравнение иметь решения ровно пяти различных периодов? Четырех различных периодов?

14 Для какого из приведенных ниже многочленов решения линейного рекуррентного уравнения, определенного этими многочленами, имеют наибольший период:

a) $f(\lambda) = \lambda^5 - \lambda^3 + \lambda + 1$;
b) $f(\lambda) = \lambda^5 - \lambda^3 + \lambda^2 + 1$;
c) $f(\lambda) = \lambda^4 - \lambda^3 + \lambda + 1$;
d) $f(\lambda) = \lambda^6 - \lambda^3 + \lambda + 1$;
e) $f(\lambda) = \lambda^5 - \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$;
f) $f(\lambda) = \lambda^6 - 1$?

Литература к главе 8

При подготовке текста главы 8, были использованы следующие источники [1], [9], [14], [30], [55], [60], [64], [67], [77], [78], [103], [105], [109].

Глава 9

Задания для организации промежуточного и итогового контроля

9.1. Контрольные вопросы

1. Что такое шифр?
2. В чем отличие шифра от кода?
3. Каким требованиям должен отвечать шифр?
4. Чем характеризуются шифры простой замены?
5. Что из себя представляют перестановочные шифры?
6. Какие существуют особенности использования перестановочных шифров?
7. Для каких шифров используется метод частотного анализа?
8. Какие способы существуют для осложнения частотного анализа?
9. Что такое стеганография и чем она отличается от криптографии?
10. Что понимают под криптостойкостью шифра?
11. Чему равно количество всех ключей в шифрах-перестановках?
12. Что называется k-граммой?
13. Как задаются аффинные отображения?
14. Какие параметры аффинного отображения являются сменными, а какие постоянными?
15. Каковы условия однозначности аффинного отображения?
16. Какие существуют частные случаи аффинного отображения?
17. Является ли отображение, обратное к аффинному, аффинным?
18. Как найти отображение, обратное к аффинному?
19. Сколько элементов необходимо угадать, чтобы вскрыть линейное отображение; сдвиг; произвольное аффинное отображение?
20. Что представляет собой k-грамма при матричном шифровании?
21. При каком условии для матрицы $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_N)$ существует обратная ей матрица? Для матрицы $A \in M_k(\mathbb{Z}_N)$?
22. Как найти для матрицы $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_N)$ обратную ей матрицу?

23. Как найти обратное матричное аффинное отображение?
24. Какое минимальное количество биграмм необходимо угадать для вскрытия:
    a) линейного матричного шифрования;
    b) матричного сдвига;
    c) аффинного матричного шифрования?
25. Чем идентификация отличается от аутентификации?
26. В чем заключается смысл понятия «односторонняя функция»?
27. Как найти ключи для системы «без передачи ключей»?
28. В чем слабые стороны использования системы *RSA*?
29. Что называют электронной подписью?
30. Каким должен быть порядок использования ключей в электронной области?
31. Какой алгоритм называют полиномиальным?
32. Каков принцип действия вероятностного алгоритма?
33. Как производится оценка сложности алгоритма?
34. В каком случае обычный алгоритм Евклида может опережать бинарный?
35. Предложите способы проверки быстродействия алгоритмов.
36. Является ли линейное представление наибольшего общего делителя двух чисел единственным и почему?
37. Является ли оптимизацией алгоритмов проверки чисел на простоту предварительное применение к этим числам признаков делимости на другие числа?
38. Какие числа называют псевдопростыми?
39. Какие разновидности псевдопростых чисел вы знаете?
40. Укажите основания для заданного целого числа, по которым оно всегда будет псевдопростым; эйлеровым псевдопростым; сильным псевдопростым.
41. Какие тесты простоты вам известны?
42. В каких ситуациях предпочтительнее тот или иной алгоритм проверки чисел на простоту?
43. Что называют факторизацей?
44. Какие современные методы факторизации вам известны?
45. Что такое факторные базы?
46. Какую мощность могут иметь конечные поля?
47. Как построить конечное поле заданного порядка?

48. Что такое псевдослучайные последовательности? Как они применяются в криптографии?
49. Как построить псевдослучайную последовательность с заданным периодом?
50. Существует ли такие натуральные числа, что псевдослучайной последовательности с таким периодом не существует?

9.2. Типовые задания обязательного минимума по основам криптографии

Задания к разделу «Из истории криптографии»

1. Зашифруйте с помощью шифра Цезаря (шифра Августа) сообщение и проверьте результат, осуществив дешифрование полученного шифротекста:
   a) «ЗНАНИЕСИЛА»;
   b) «ВЕЧНЫЙЗОВ»;
   c) «ТРИПЛЮСДВА»;
   d) «ГОРОДМАСТЕРОВ»;
   e) «ALTEREGO»;
   f) «IAMSTUDENT».
2. Зашифруйте сообщение с помощью шифра простой перестановки, выбрав таблицу подходящего размера; проверьте результат, осуществив дешифрование полученного шифротекста:
   a) «ТЕНИ ИСЧЕЗАЮТ В ПОЛДЕНЬ»;
   b) «МОСКВА НЕ СРАЗУ СТРОИЛАСЬ»;
   c) «МНОГО ШУМА ИЗ НИЧЕГО»;
   d) «БЕДНОСТЬ НЕ ПОРОК»;
   e) «В ТЕСНОТЕ ДА НЕ В ОБИДЕ»;
   f) «КОНЧИЛ ДЕЛО ГУЛЯЙ СМЕЛО».
3. Используя шифр Тритемиуса и ключевое слово «K», зашифруйте фразу «F»; проверьте результат, осуществив расшифровку полученного шифротекста:
   a) «K = МЯЧ», «F = ВОЛЕЙБОЛ»;
   b) «K = ДОМ», «F = КОМНАТА»;
   c) «K = СОМ», «F = РЫБАЛКА»;
   d) «K = ДЫМ», «F = ПОЖАРНЫЙ»;
   e) «K = ЛУЧ», «F = СИЯНИЕ»;
   f) «K = КОТ», «F = ЖИВОТНОЕ».

4. Используя таблицу Виженера и ключевое слово «K», зашифруйте фразу «F»; проверьте результат, осуществив расшифровку полученных шифротекстов:

   a) «K = ТРИ», «F = СТОДВАДЦАТЬ»;

   b) «K = ДВА», «F = ДВЕСТИВОСЕМЬ»;

   c) «K = ПЯТЬ», «F = ТРИСТАТРИДЦАТЬ»;

   d) «K = СЕМЬ», «F = ЧЕТЫРЕСТАДВА»;

   e) «K = ОДИН», «F = ПЯТЬСОТШЕСТЬ»;

   f) «K = ШЕСТЬ», «F = СЕМЬСОТДЕВЯТЬ».

5. Зашифруйте сообщение, используя решетку Кардано:

   a) «МОЛЧАНЬЕ ЗОЛОТО»;

   b) «ЛИХА БЕДА НАЧАЛО»;

   c) «МОЯ ХАТА С КРАЮ»;

   d) «ГЛАЗА ЗЕРКАЛО ДУШИ»;

   e) «ШИВОРОТ НАВЫВОРОТ»;

   f) «ВЕК ЖИВИ ВЕК УЧИСЬ».

6. Восстановите по шифротектсту сообщение, зашифрованное с помощью щифра Цезаря с некоторым сдвигом k:

   a) «ЁЛБУЁСЙОБ»;

   b) «ЗЛКОПЭКФЁЪ»;

   c) «ОВТКВППВ»;

   d) «ДКЗЖЯБДСЯ»;

   e) «ОТСОТФЗМГ»;

   f) «КЮНБЮНЖРЮ».

7. Восстановите по шифротектсту сообщение, зашифрованное с помощью шифра простой перестановки:

   a) «ВСВЕМТЕЛЕЕСО»;

   b) «ГУЙГОБВОЛОАН»;

   c) «ККИЕРОЛИОДГА»;

   d) «ВЕЙТЕЛВЕСЫЕР»;

   e) «БЕЕНУТСКДПЕА»;

   f) «ВОБЕОЛЕЗПЕРА».

Задания к разделу «Простейшие симметричные криптосистемы»

1. Укажите число аффинных преобразований для алфавита длины N:

   a) $N = 10$; c) $N = 14$; e) $N = 16$; g) $N = 20$;

   b) $N = 12$; d) $N = 15$; f) $N = 18$; h) $N = 21$.

   Сколько среди них линейных преобразований; преобразований сдвига?

2. Зашифруйте сообщение F, записанное в алфавите 0, 1, 2, 3, 4, 5, 6, 7, 8, с помощью шифрующего преобразования f; проверьте результат, осуществив дешифрование полученного шифротекста:

   a) $F =$ «112»; $f(x) \equiv 7x + 1 \pmod 9$;
   b) $F =$ «007»; $f(x) \equiv 2x + 5 \pmod 9$;
   c) $F =$ «232»; $f(x) \equiv 4x + 8 \pmod 9$;
   d) $F =$ «554»; $f(x) \equiv 5x + 4 \pmod 9$;
   e) $F =$ «877»; $f(x) \equiv 8x + 2 \pmod 9$;
   f) $F =$ «003»; $f(x) \equiv 2x + 5 \pmod 9$.

3. Зашифруйте сообщение F, записанное в алфавите А = 0, ..., Я = 32, с помощью шифрующего преобразования f; проверьте результат, осуществив дешифрование полученного шифротекста:

   a) $F=$ «КЛЮЧ»; $f(x) \equiv x + 7 \pmod{33}$;
   b) $F=$ «ШИФР»; $f(x) \equiv x + 5 \pmod{33}$;
   c) $F=$ «ТЕКСТ»; $f(x) \equiv x + 8 \pmod{33}$;
   d) $F=$ «СБОЙ»; $f(x) \equiv x + 4 \pmod{33}$;
   e) $F=$ «ПРИЕМ»; $f(x) \equiv x + 6 \pmod{33}$;
   f) $F=$ «ОТКАЗ»; $f(x) \equiv x + 9 \pmod{33}$.

4. Найдите аффинное преобразование, обратное преобразованию $y \equiv \equiv ax + b \pmod N$, и дешифруйте шифротекст «АБВ»:

   a) $a = 3$, $b = 1$, $N = 8$;
   b) $a = 4$, $b = 3$, $N = 9$;
   c) $a = 2$, $b = 5$, $N = 7$;
   d) $a = 5$, $b = 4$, $N = 8$;
   e) $a = 7$, $b = 2$, $N = 9$;
   f) $a = 5$, $b = 3$, $N = 7$.

5. Известно, что аффинное преобразование $y \equiv ax + b \pmod N$ над алфавитом 0, 1, 2, ..., $N - 1$ переводит символы x_1 и x_2 в символы y_1 и y_2, соответственно. Найдите обратное аффинное преобразование и дешифруйте шифротекст «007»:

   a) $x_1 = 1$, $x_2 = 2$, $y_1 = 3$, $y_2 = 6$, $N = 8$;
   b) $x_1 = 2$, $x_2 = 3$, $y_1 = 5$, $y_2 = 2$, $N = 7$;
   c) $x_1 = 3$, $x_2 = 2$, $y_1 = 6$, $y_2 = 8$, $N = 9$;
   d) $x_1 = 4$, $x_2 = 3$, $y_1 = 5$, $y_2 = 2$, $N = 8$;
   e) $x_1 = 2$, $x_2 = 1$, $y_1 = 4$, $y_2 = 6$, $N = 7$;
   f) $x_1 = 3$, $x_2 = 4$, $y_1 = 5$, $y_2 = 3$, $N = 9$.

   Восстановите преобразование $y \equiv ax + b \pmod N$ и, зашифровав сообщение «112», отправьте его противнику.

Задания к разделу «Шифрующие матрицы»

1. Найдите матрицу, обратную матрице $A \in M_2(\mathbb{Z}_n)$:

a) $A = \begin{pmatrix} 0 & 1 \\ 3 & 5 \end{pmatrix}$, $n = 10$;

b) $A = \begin{pmatrix} 1 & 0 \\ 2 & 5 \end{pmatrix}$, $n = 8$;

c) $A = \begin{pmatrix} 0 & 2 \\ 1 & 5 \end{pmatrix}$, $n = 9$;

d) $A = \begin{pmatrix} 3 & 0 \\ 2 & 15 \end{pmatrix}$, $n = 10$;

e) $A = \begin{pmatrix} 2 & 0 \\ 2 & 4 \end{pmatrix}$, $n = 9$;

f) $A = \begin{pmatrix} 0 & 3 \\ 1 & 5 \end{pmatrix}$, $n = 8$.

2. Зашифруйте сообщение X, записанное в алфавите 0, 1, 2, 3, 4, 5, 6, 7, 8, с помощью матричного шифрующего преобразования $f(X) \equiv \equiv A \cdot X \pmod 9$; проверьте результат, осуществив дешифрование полученного шифротекста:

a) X= «01»; $A = \begin{pmatrix} 0 & 1 \\ 2 & 5 \end{pmatrix}$;

b) X= «02»; $A = \begin{pmatrix} 2 & 0 \\ 4 & 5 \end{pmatrix}$;

c) X= «03»; $A = \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix}$;

d) X= «07»; $A = \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}$;

e) X= «12»; $A = \begin{pmatrix} 3 & 0 \\ 6 & 1 \end{pmatrix}$;

f) X= «13»; $A = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix}$.

3. Зашифруйте сообщение X, записанное в алфавите А=0, ..., Я=32, с помощью матричного шифрующего преобразования $f(X) \equiv A \cdot X \pmod{33}$; проверьте результат, осуществив дешифрование полученного шифротекста:

a) X= «КЛЮЧ»; $A = \begin{pmatrix} 2 & 0 \\ 4 & 5 \end{pmatrix}$;

b) X= «ШИФР»; $A = \begin{pmatrix} 1 & 0 \\ 5 & 2 \end{pmatrix}$;

c) X= «НОЛЬ»; $A = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$;

d) X= «ДРУГ»; $A = \begin{pmatrix} 2 & 0 \\ 3 & 1 \end{pmatrix}$;

e) X= «СБОЙ»; $A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$;

f) X= «ПЯТЬ»; $A = \begin{pmatrix} 0 & 2 \\ 4 & 1 \end{pmatrix}$.

4. Расшифруйте шифротекст F с помощью обратного матричного преобразования $X \equiv A' \cdot f(X) \pmod{N}$, и, восстановив матричное шифрующее преобразование $f(X) \equiv A \cdot X \pmod{N}$, отправьте противнику сообщение L:

   a) $F =$ «0102», $A' = \begin{pmatrix} 0 & 1 \\ 3 & 5 \end{pmatrix}$, $N = 10$, $L =$ «99»;

   b) $F =$ «0203», $A' = \begin{pmatrix} 1 & 0 \\ 2 & 5 \end{pmatrix}$, $N = 8$, $L =$ «77»;

   c) F«0304», $A' = \begin{pmatrix} 0 & 2 \\ 1 & 5 \end{pmatrix}$, $N = 9$, $L =$ «88»;

   d) $F =$ «0506», $A' = \begin{pmatrix} 3 & 0 \\ 2 & 15 \end{pmatrix}$, $N = 10$, $L =$ «77»;

   e) $F =$ «0105», $A' = \begin{pmatrix} 2 & 0 \\ 2 & 4 \end{pmatrix}$, $N = 9$, $L =$ «66»;

   f) $F =$ «0106», $A' = \begin{pmatrix} 0 & 3 \\ 1 & 5 \end{pmatrix}$, $N = 8$, $L =$ «55».

Задания к разделу «Система RSA. Дискретный логарифм»

1. Подготовив к работе систему «без передачи ключей» по модулю p, осуществите отправку сообщения m абоненту B:

   a) $p = 11$, $m = 3$;
   b) $p = 11$, $m = 8$;
   c) $p = 13$, $m = 4$;
   d) $p = 13$, $m = 9$;
   e) $p = 7$, $m = 3$;
   f) $p = 7$, $m = 5$.

2. Подготовьте к работе систему «с открытым ключом» на базе модулей 35 и 33: рассмотрев модуль $35 = 5 \cdot 7$, вычислите $\varphi(35)$ и подберите пару ключей (a, α) для абонента A; рассмотрев модуль $33 = 3 \cdot 11$, вычислите $\varphi(33)$ и подберите пару ключей (b, β) для абонента B. Осуществите отправку сообщения m абоненту B:

   a) $m = 10$;
   b) $m = 11$;
   c) $m = 12$;
   d) $m = 13$;
   e) $m = 14$;
   f) $m = 15$;
   g) $m = 16$;
   h) $m = 17$.

3. Решите задачу дискретного логарифмирования $a^x \equiv b \pmod{p}$:

   a) $p = 5, a = 2, b = 3$;
   b) $p = 7, a = 3, b = 5$;
   c) $p = 11, a = 8, b = 6$;
   d) $p = 5, a = 3, b = 2$;
   e) $p = 7, a = 5, b = 2$;
   f) $p = 11, a = 6, b = 7$.

Задания к разделу «Вычислительные алгоритмы и их трудоемкость»

1. Переведите число n в систему с основанием q:

   a) $n = 10011_2, q = 4$;
   b) $n = 7077_8, q = 2$;
   c) $n = 21021_4, q = 16$;
   d) $n = 2320_4, q = 2$;
   e) $n = 10001_2, q = 16$;
   f) $n = 11091_{16}, q = 4$.

2. Найдите наибольший общий делитель чисел a и b, пользуясь алгоритмом Евклида, бинарным алгоритмом Евклида:

   a) $a = 32, b = 14$;
   b) $a = 48, b = 21$;
   c) $a = 64, b = 28$;
   d) $a = 18, b = 10$;
   e) $a = 27, b = 15$;
   f) $a = 26, b = 18$.

3. Решите неопределенное уравнение $ax + by = c$ двумя способами:

   a) $a = 20, b = 14, c = 6$;
   b) $a = 30, b = 21, c = 9$;
   c) $a = 40, b = 28, c = 8$;
   d) $a = 34, b = 10, c = 14$;
   e) $a = 51, b = 15, c = 3$;
   f) $a = 68, b = 20, c = 12$.

4. Вычислите степень a^d по модулю n классическим способом и с помощью алгоритма возведения в степень; сравните трудоемкость двух методов:

   a) $n = 16, a = 14, d = 10$;
   b) $n = 14, a = 5, d = 12$;
   c) $n = 15, a = 11, d = 13$;
   d) $n = 16, a = 12, d = 11$;
   e) $n = 14, a = 7, d = 10$;
   f) $n = 15, a = 13, d = 11$.

Задания к разделу «Простые и псевдопростые числа»

1. Простым или составным является число:

   a) 4975; c) 6327; e) 8421; g) 1111; i) 2167; k) 2127;
   b) 6395; d) 7113; f) 9543; h) 1133; j) 1233; l) 2827?

2. Укажите все простые числа на промежутке:

   a) (13,22); c) (17,29]; e) (31,44); g) (57,69]; i) (71,83); k)(93,104];
   b) [15,24]; d) [21,31); f) [44,57]; h) [63,73); j) [82,93]; l) [19,29).

3. Докажите простоту числа:

   a) 101; c) 107; e) 113; g) 1201; i) 1409; k) 2179;
   b) 103; d) 109; f) 127; h) 1213; j) 1427; l) 2207.

4. Убедитесь, что число n является псевдопростым по основанию a:

   a) $n = 91$, $a = 3$; d) $n = 4$, $a = 5$; g) $n = 35$, $a = 6$;
   b) $n = 25$, $a = 7$; e) $n = 21$, $a = 8$; h) $n = 9$, $a = 8$.
   c) $n = 15$, $a = 4$; f) $n = 6$, $a = 7$;

5. Найдите остаток $\mathrm{rest}(M_k, F_n)$ от деления k-го числа Мерсенна $M_k = 2^k - 1$ на n-е число Ферма $F_n = 2^{2^n} + 1$:

   a) $k = 11$, $n = 0$; d) $k = 8$, $n = 3$; g) $k = 14$, $n = 0$;
   b) $k = 10$, $n = 1$; e) $k = 7$, $n = 2$; h) $k = 13$, $n = 1$.
   c) $k = 9$, $n = 2$; f) $k = 11$, $n = 1$;

   Являются ли числа $\mathrm{rest}(M_k, F_n)$, M_k и F_n простыми?

Задания к разделу «Факторизация натуральных чисел»

1. Разложите на простые множители числа:

   a) 1566; c) 1625; e) 1720; g) 1881; i) 1954; k) 1980;
   b) 1602; d) 1647; f) 1805; h) 1926; j) 1963; l) 2016.

2. Пользуясь методом Ферма или его модификацией, факторизуйте числа:

   a) 143; b) 323; c) 187; d) 221; e) 247; f) 391.

Задания к разделу «Псевдослучайные последовательности над конечным полем»

1. Выполните действия в поле $\mathbb{F}_p$:

   a) $(1 + 2 \cdot 4) \div 3$, $p = 5$; d) $(3 \cdot 3 - 2) \div 4$, $p = 5$;
   b) $(3 \cdot 5 - 1) \div 2$, $p = 7$; e) $(4 - 3 \cdot 2) \div 5$, $p = 7$;
   c) $(1 - 3 \cdot 8) \div 4$, $p = 11$; f) $(1 + 8 \cdot 4) \div 5$, $p = 11$.

2. Укажите многочлен, сравнимый с $g(x)$ по модулю $f(x)$ в кольце $\mathbb{F}_2[x]$:

   a) $g(x) = x^5 + x^4 + 1$, $f(x) = x + 1$;
   b) $g(x) = x^4 + x^3 + 1$, $f(x) = x^2 + 1$;
   c) $g(x) = x^6 + x^5 + x^2$, $f(x) = x^3$;
   d) $g(x) = x^5 + x^4 + x$, $f(x) = x^2$;
   e) $g(x) = x^4 + x^2 + 1$, $f(x) = x^2 + 1$;
   f) $g(x) = x^6 + x^3 + x^2$, $f(x) = x^3 + 1$.

3. Докажите, что многочлен $f(x)$ неприводим, а многочлен $g(x)$ приводим над полем $\mathbb{F}_p$:
   a) $f(x) = x^3 + x + 1$, $g(x) = x^2 + x$, $p = 2$;
   b) $f(x) = x^3 + 2x + 1$, $g(x) = x^2$, $p = 3$;
   c) $f(x) = x^3 + x^2 + 1$, $g(x) = x^3$, $p = 2$;
   d) $f(x) = x^2 + 2x + 2$, $g(x) = x^3 + x^2$, $p = 3$;
   e) $f(x) = x^2 + x + 1$, $g(x) = x^3 + x$, $p = 2$;
   f) $f(x) = x^2 + x + 2$, $g(x) = x^3 + 1$, $p = 3$.
4. Постройте, если это возможно, поля, число элементов в которых равно q_1, q_2 и q_3:
   a) $q_1 = 10, q_2 = 5, q_3 = 9$;
   b) $q_1 = 7, q_2 = 8, q_3 = 12$;
   c) $q_1 = 4, q_2 = 11, q_3 = 6$;
   d) $q_1 = 9, q_2 = 14, q_3 = 7$;
   e) $q_1 = 5, q_2 = 15, q_3 = 8$;
   f) $q_1 = 18, q_2 = 4, q_3 = 13$.
5. Решите линейное рекуррентное уравнение над полем $\mathbb{F}_2$:
   a) $\delta_{x+2} = \delta_x$;
   b) $\delta_{x+3} = \delta_x$;
   c) $\delta_{x+3} = \delta_{x+2} + \delta_x$;
   d) $\delta_{x+3} = \delta_{x+1}$;
   e) $\delta_{x+3} = \delta_{x+1} + \delta_x$;
   f) $\delta_{x+2} = \delta_{x+1} + \delta_x$.

   Убедитесь, что найдены все решения линейного рекуррентного уравнения. Найдите примитивный период каждого из решений. Выделите главные решения.

9.3. Задания для творческих лабораторных работ к разделу «Из истории криптографии»

Творческие лабораторные работы по истории криптографии могут выполняться как индивидуально, так и в небольших по размеру группах.

9.3.1. Таблица Виженера

1. Используя таблицу Виженера и ключевое слово длины n, зашифруйте (вручную или с помощью компьютера) отрывок выбранной вами книги, содержащий не менее m символов (табл. 9.1).
2. Обменяйтесь криптограммами с группой-напарником.
3. Расшифруйте полученные криптограммы.
4. Попробуйте найти длину ключа, используя метод Касиски.

5. Подготовьте отчет. В отчете отразите пошаговые действия для вскрытия сообщения группы-напарника. Проанализируйте, насколько вам помогло знание длины ключа.

Таблица 9.1

Варианты заданий

Вариант	n	m	Вариант	n	m	Вариант	n	m
1	5	200	8	4	200	15	4	250
2	6	200	9	3	300	16	5	300
3	7	200	10	4	300	17	5	250
4	6	250	11	5	350	18	5	250
5	5	250	12	6	400	19	6	250
6	4	250	13	5	200	20	7	300
7	3	200	14	4	250	21	4	250

9.3.2. Шифр по книге

1. Выберите книгу, которую будете использовать в секретной переписке.
2. Составьте сообщение, пользуясь произвольно выбранной вами фразой из книги как ключом, длина которого равна длине вашего сообщения: записав буквы вашего сообщения под выбранной фразой и складывая по модулю 33 числовые эквиваленты соответствующих букв ключевой фразы и сообщения, получите числовые эквиваленты букв шифротекста и сам шифротекст.
3. Передайте группе-напарнику шифрованное сообщение вместе с ключом, содержащим пару чисел: номер страницы книги, на которой расположена выбранная вами фраза, и номер строки, с которой эта фраза начинается.
4. Получите аналогичное шифрованное сообщение от группы-напарника и расшифруйте его.
5. Проверьте полученные результаты.
6. Подготовьте отчет.

9.3.3. Частотный анализ

1. Расшифруйте текст на русском языке (табл. 9.2), применяя метод частотного анализа при использовании таблицы частот, приведенной в главе 10. (Знаки препинания сохранены для облегчения работы с текстом.)

2. Подготовьте отчет с промежуточными результатами, включающими в себя:
   — таблицу частот появления символов в шифротексте;
   — обоснование выбора символов перехода;
   — указание ошибочных предположений и выводы, приведшие к исправлению ошибок;
   — анализ совпадения частот появления символов в шифротексте и среднестатистических показателей (см. главу 10).

Таблица 9.2

Варианты заданий

Вариант	Номер текста	Вариант	Номер текста	Вариант	Номер текста
1	1	8	8	15	6
2	2	9	9	16	7
3	3	10	1	17	8
4	4	11	2	18	9
5	5	12	3	19	1
6	6	13	4	20	2
7	7	14	5	21	3

Тексты для анализа.

- **Текст 1**

91 15 55 10 91 10 81, 77 28 91 66 30 15 55 77 15 91 77 30 18 63 73 81 70 42 87 10 35 91 10 55 98 73 55 43 30 23 50 77 73 41 28 23 85 63 73 81 70 23 15 50 30 28 30 43 10 73 41 15 99 98 66 70 73 85 66 10 45 30 66 98 22 30 43 45 10 73 30 30, 22 30 43 50 10 81 15 23 73 55 10 28, 22 77 55 30 35 70 77 43, 70 77 99 10 50 30 28 30 43 10 73 28 30 70 77 70 43 77 15 98 73 91 77 87 91 43 10 55 98 55 41 30 30. 28 77 91 15 81 30 50 77 43 10 15 15 30 81 28 28 77 15 55 41 98 28 30 23 66 30 28 41 30 91 77 18 55 98 91 15 10 73 77 28 98 50 77 91 77 43 98 55 41 91 28 30 66 91 42 99 23 70 10 73 98 15 41 91 42 43 10 45 30 28 98 30 66 22 77 13 43 77 22 23 63 98 81, 70 43 77 15 55 77 55 42 98 15 99 43 77 66 28 77 15 55 98.

- **Текст 2**

99 28 81 45 28 14 57 73 32 28 23 73 42 13 14 73 14 15 41; 94 28 14 69 94 22 28 81 73 14 15 41 15 88 94 18 45 32 28 32 27 87 76 32 28 81 85 26 32 85 15 81 23 73 42 13 99 94 18 91 69 94 73 28 32 99 54 14 15 27 91 94 18 45 32 28 26 27 28 42, 15 99 94 88 94 54 94 85 94 28 14 91 94 63 73 14 91 50 94 15 88 27 28 23 85. 15 73 32 50 99 14 63 23 76 81 15 91 94 32 85 13 32 73 94 85 13 14 73 41 28 94 85 54 94 13 94 18, 23 13 54 14 28 28 94 85 69 73 85 26 94 76 27 76 94 35 94 76, 27 13 73 32 15 88 81 13 32 73 27 87 28 94 18 69 73 32 11, 50 73 81 28 80 32 76 91

94 73 94 15 27 13 54 27 73 73 27 14 28 88 94 91, 94 28 14 69 54 94 63 73 14 76 32 45 22 23 54 14 15 15 88 23 69 27 91 63 27 76 27 15 81 76 23 45 11 27 28 14 76 27 27 69 54 81 76 94, 28 32 50 73 81 22 81 28 27 28 14 99 94 50 94, 28 94 91 15 32 76 23 73 42 13 14 81 15 41 27 99 14 99 13 42 73 85 13 32 87 28 94 69 54 32 22 94 15 88 14 91 73 81 81 99 14 45 22 94 76 23 69 54 14 91 94 73 85 13 94 91 14 88 41 15 81 99 54 14 15 94 88 94 85 15 91 94 32 50 94 15 88 14 28 14.

- **Текст 3**

50 27 91 31 54 82 10 82 88 96 10 13 31 51 70 77 96 77 18 82 77 77 50 73 81 22 42 91 10 73 10 51 41, 96 10 96 13 42 70 54 34 50 77 88 10 91 73 34 91 10 81 51 41 96 77 88 70 77 54 27, 31 45 31 73 34 13 42 96 88 77 91 87 22 27 66 10 73 77 13 34 22 31 88 41 22 31 88 31 18. 50 27 91 31 54 82 3514-82 31 66 31 80 51 88 10 54 10 73 51 81 87 10 70 77 66 82 34 88 41 91 51 31 54 77 22 42 96 27 63 10 82 34 18, 22 31 51 31 54 88 77 91 34 91 34 82, 51 88 31 66 11 88 77 13 42 77 70 34 51 10 88 41 91 51 31 70 77 22 54 77 13 82 77 91 70 34 51 41 66 10 35 96 22 77 66 10 63 82 34 66 91 50 31 54 66 10 82 34 85, 34 91 31 51 41 66 10 77 13 34 45 10 73 51 81 88 31 66, 11 88 77 22 91 77 54 31 80 96 34 18 51 87 10 91 31 54 82 27 88 77 85 91 51 10 73 49 31 88 96 27 13 27 88 42 73 96 77 18 77 13 82 77 51 34 73 31 50 77.

- **Текст 4**

10 28 28 10 70 10 91 73 77 91 28 10 70 54 17 91 31 88 15 88 91 77 91 10 73 10 31 50 77 70 77 99 73 77 28 77 66, 77 88 28 77 15 81 26 17 66 15 81 99 73 85 22 81 66 15 10 66 77 18 28 17 87 63 31 18 17 31 54 10 54 35 17 17 91 31 31 15 10 73 77 28 31. 28 77, 28 31 15 66 77 88 54 81 28 10 57 88 77 28 17 87 63 31 31 70 77 15 91 77 31 66 23 15 77 54 88 23 70 54 17 91 31 88 15 88 91 17 31, 70 54 17 91 17 22 31 91 77 63 31 22 63 31 50 77 70 41 31 54 10 91 73 17 80 31 10 28 28 42 70 10 91 73 77 91 28 42 17 87 77 13 54 10 87 17 73 77 15 41 13 31 15 70 77 99 77 18 15 88 91 77 17 15 88 54 10 35, 70 77 22 77 13 28 42 18 88 77 66 23, 99 77 88 77 54 42 18 91 42 54 10 45 10 31 88 15 81 70 54 17 91 17 22 31 11 31 50 77–28 17 13 23 22 41 15 73 17 63 99 77 66 77 50 54 77 66 28 77 50 77 17 28 31 15 91 77 18 15 88 91 31 28 28 77 50 77 66 31 15 88 23.

- **Текст 5**

99 28 81 45 28 14 57 73 32 28 23 73 42 13 14 73 14 15 41; 94 28 14 69 94 22 28 81 73 14 15 41 15 88 94 18 45 32 28 32 27 87 76 32 28 81 85 26 32 85 15 81 23 73 42 13 99 94 18 91 69 94 73 28 32 99 54 14 15 27 91 94 18 45 32 28 26 27 28 42, 15 99 94 88 94 54 94 85 94 28 14 91 94 63 73 14 91 50 94 15 88 27 28 23 85. 57 73 32 28 13 42 73 14 88 14 99 35 94 54 94 63 14, 11 88 94 28 32 88 94 73 41 99 94 28 32 13 42 73 94 91 28 32 18 87 14 76 32 88 28 94 27 88 32 28 27 99 94 99 32 88 15 88 91 14, 28 94, 28 14 69 54 94 88 27 91, 32 18 99 14 99 13 23 22 88 94 15 94 91 32 15 88 28 94 13 42 73 94 87 14 15 91 94 85 28 32 15 94 76 28 32 28 28 23 85 27 15 73 27 63 99 94 76 15 27 73 41 28 94 27 69 94 13 32 22 27 88 32 73 41 28 94 22 32 18 15 88 91 23 85 26 23 85 99 54 14 15 94 88 23.

- **Текст 6**

  82 34 96 77 73 10 18 51 34 22 31 73 22 10 73 31 96 77 77 88 51 77 82 34, 70 77 22 73 31 45 85 73 34 96 10 54 10 50 34 82 77 18, 34 77 70 81 88 41 51 88 77 18 45 31 82 31 91 77 73 41 82 77 18 27 73 42 13 96 77 18 11 88 77–88 77 50 77 91 77 54 34 73 51 82 31 18. 51 77 82 81 27 73 42 13 10 73 10 51 41 70 10 54 10 22 82 77, 82 77, 91 34 22 34 66 77, 66 27 11 34 73 10 51 41 54 31 91 82 77 51 88 41 85: 88 77 13 73 31 22 82 31 73 10, 88 77 96 54 10 51 82 31 73 10 34 91 51 31 66 34 51 34 73 10 66 34 70 54 34 51 73 27 63 34 91 10 73 10 51 41 96 88 77 66 27, 11 88 77 50 77 91 77 54 34 73 34 66 31 45 22 27 51 77 13 77 85 82 34 96 77 73 10 18 34 45 85 73 34.

- **Текст 7**

  15 73 32 50 99 14 63 23 76 81 15 91 94 32 85 13 32 73 94 85 13 14 73 41 28 94 85 54 94 13 94 18, 23 13 54 14 28 28 94 85 69 73 85 26 94 76 27 76 94 35 94 76, 27 13 73 32 15 88 81 13 32 73 27 87 28 94 18 69 73 32 11, 50 73 81 28 80 32 76 91 94 73 94 15 27 13 54 27 73 73 27 14 28 88 94 91, 94 28 14 69 54 94 63 73 14 76 32 45 22 23 54 14 15 15 88 23 69 27 91 63 27 76 27 15 81 76 23 45 11 27 28 14 76 27 27 69 54 81 76 94, 28 32 50 73 81 22 81 28 27 28 14 99 94 50 94, 28 94 91 15 32 76 23 73 42 13 14 81 15 41 27 99 14 99 13 42 73 85 13 32 87 28 94 69 54 32 22 94 15 88 14 91 73 81 81 99 14 45 22 94 76 23 69 54 14 91 94 73 85 13 94 91 14 88 41 15 81 99 54 14 15 94 88 94 85 15 91 94 32 50 94 15 88 14 28 14, 69 94 73 28 42 35 69 73 32 11, 94 11 32 28 41 94 88 99 54 42 88 94 18, 69 94 88 94 50 22 14 63 28 32 18 76 94 22 32, 50 54 23 22 27 27 15 69 27 28 42, 27 99 14 99 13 23 22 88 94 91 28 94 15 81 15 15 94 13 94 85 13 73 32 15 99 13 14 73 14, 69 94 22 94 63 73 14 99 14 28 28 32 69 14 91 73 94 91 28 32.

- **Текст 8**

  70 41 30 43 13 42 73 28 30 23 99 73 85 45. 55 77 73 15 55 42 18, 91 42 63 30 77 13 42 99 28 77 91 30 28 28 77 50 77 43 77 15 55 10, 63 98 43 77 99 98 18, 15 77 50 43 77 66 28 42 66 98 99 43 10 15 28 42 66 98 43 23 99 10 66 98, 77 28, 99 10 99 50 77 91 77 43 98 55 15 81, 28 30 23 66 30 73 91 77 18 55 98 91 15 10 73 77 28 98 30 26 30 66 30 28 30 30 23 66 30 73 98 87 28 30 50 77 91 42 18 55 98, 55 77 30 15 55 41 70 30 43 30 22 91 42 35 77 22 77 66 15 99 10 87 10 55 41 11 55 77–28 98 13 23 22 41 77 15 77 13 30 28 28 77 70 43 98 81 55 28 77 30. 99 43 77 66 30 55 77 50 77, 77 28 13 42 73 43 10 15 15 30 81 28.

- **Текст 9**

  91 15 99 77 54 31 70 77 15 73 31 66 10 73 31 28 41 99 77 18 99 28 81 50 17 28 17 91 77 63 31 73 66 10 15 15 17 91 28 42 18, 88 77 73 15 88 42 18 66 77 73 77 22 77 18 11 31 73 77 91 31 99 15 15 88 54 17 45 31 28 77 85 50 77 73 77 91 77 18, 91 77 11 99 10 35, 15 91 31 88 73 42 35 70 10 28 88 10 73 77 28 10 35 70 77 88

77 50 22 10 63 28 31 18 66 77 22 31, 15 91 42 15 77 99 17 66 45 10 13 77 17 91 99 77 54 17 11 28 31 91 77 66 49 54 10 99 31. 57 88 77 88 88 77 73 15 88 42 18 66 77 73 77 22 77 18 11 31 73 77 91 31 99 13 42 73 28 31 87 10 99 77 28 28 42 18 15 42 28 87 28 10 66 31 28 17 88 77 50 77 31 99 10 88 31 54 17 28 17 28 15 99 77 50 77 91 31 73 41 66 77 45 17, 50 54 10 49 10 13 31 87 23 35 77 91 10, 23 66 17 54 10 91 63 31 50 77 88 31 70 31 54 41 91 66 77 15 99 91 31. 77 28 28 17 50 22 31 28 31 15 73 23 45 17 73 31 26 31, 88 77 73 41 99 77 11 88 77 70 54 17 31 35 10 73 17 87–8710 50 54 10 28 17 80 42, 50 22 31 77 28 91 77 15 70 17 88 42 91 10 73 15 81, 17 13 42 73 70 31 54 91 42 18 54 10 87 91 77 13 26 31 15 88 91 31.

9.3.4. Решетки Кардано

1. Подготовьте трафарет заданного размера (табл. 9.3). Используйте его для шифрования.
2. Подберите два текста, укладывающиеся в вашу решетку.
3. Зашифруйте тексты, используя различный порядок шифрования (отражения, повороты).
4. Отправьте шифротексты группе-напарнику.
5. Получите от группы-напарника сообщения и расшифруйте их.
6. Подготовьте отчет. В отчете проанализируйте, сколько различных шифротекстов можно получить, используя одну и ту же решетку и один и тот же текст. Помогло ли вам знание двух шифровок одного сообщения?

Таблица 9.3

Варианты заданий

Вариант	Размер решетки	Вариант	Размер решетки	Вариант	Размер решетки
1	2 × 16	8	8 × 8	15	20 × 2
2	4 × 6	9	12 × 4	16	2 × 18
3	6 × 6	10	6 × 8	17	4 × 18
4	8 × 6	11	2 × 14	18	6 × 6
5	10 × 4	12	4 × 14	19	10 × 6
6	2 × 12	13	8 × 8	20	10 × 8
7	4 × 10	14	12 × 6	21	10 × 10

9.3.5. Двойная перестановка

1. Расшифруйте фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки), если символ ⌣ используется, как знак пробела (табл. 9.4).
2. Подгóтовьте отчет с промежуточными результатами. В отчете обоснуйте выбор размерности решетки и опишите основные логические шаги при вскрытии сообщения. Возможны ли двойные толкования вашего шифротекста?

Таблица 9.4

Варианты заданий

Вариант	Шифротекст	Вариант	Шифротекст
1	«СЯСЕ⌣ ⌣ЛУНЫИАККННОГЯДУЧАТН»	11	«МСЕЫ⌣ЛЫВЕНТОСАНТУЕИ⌣РЛПОБ»
2	«МСЕЫ⌣ЛЫВЕНТОСАНТУЕИ⌣РЛПОБ»	12	«АМНРИД⌣УЕБСЫ⌣ЕЙРСООКОТНВ⌣»
3	«ОПЧУЛС⌣БООНЕВ⌣ОЖАЕОНЕЩЕИН»	13	«ЕШИАНИРЛПГЕЧАВРВ⌣СЕЫНА⌣ЛО»
4	«АРАВНРСВЕЕОАВ⌣ЗАНЯА⌣КМРЕИ»	14	«А⌣ЛТАВЙООЛСО⌣ТВ⌣ШЕЕНЕСТ⌣Ь»
5	«ФИ⌣ЗИММУЫНУУБК⌣Е⌣ДЬШЫИВЧУ»	15	«ВР⌣ЕСДЕИ⌣ТПХРОИ⌣ЗБУАДНУА⌣»
6	«ЦТААЙПЕЕ⌣ТБГУРРСВЬЕ⌣ОРЗВВ»	16	«АВАРНСЧАА⌣НЕДВЕДЕРПЕОЙ⌣ИС»
7	«ДОПК⌣СОПАЛЕЧНЛ⌣ГИНЙОИЖЕ⌣Т»	17	«ЛУАЗИЯНСА⌣ДТДЕАИ⌣ШРФЕОНГ⌣»
8	«С⌣ОЯНВ⌣СЬСЛААВРЧЕАРТОГДЕС»	18	«КЭЕ⌣ТДУМБ⌣ЬСЗЕДНЕЗМАОР⌣ТУ»
9	«⌣ЕАЛЯРАНВЯАЧДА⌣ЕРПЕСАНВ⌣Ч»	19	«⌣И⌣ЕНТРЗИ⌣ОКЕВНОДЛЕША⌣ИМП»
10	«РОБДОЕВПС⌣МСХЬА⌣ ⌣ИВПСНИОТ»	20	«ЗШАФИПРАЛОЕНЖ⌣ОЬН⌣ДАРВОНА»

9.4. Задания для лабораторных работ к разделу «Простейшие симметричные криптосистемы. Шифрующие матрицы»

9.4.1. Аффинные криптосистемы

1. Используя метод аффинного шифрования (вручную или с использованием компьютера) над 34-буквенным русским алфавитом (добавьте символ пробела) с ключом (a, b), зашифруйте отрывок выбранной вами книги, содержащий не менее M символов (знаками препинания пренебречь) (табл. 9.5).

2. Обменяйтесь шифротекстами с группой-напарником. Дайте группе-напарнику две подсказки о переходах букв, предварительно убедившись, что с их помощью можно получить дешифрующее преобразование.
3. Осуществите вскрытие шифротекста товарища.
4. Найдите ключ товарища и отправьте ему сообщение «ГОТОВО».
5. Подготовьте отчет.

Примечание. При использовании компьютера рекомендуется проводить шифрование биграмм текста.

9.4.2. Шифрующие матрицы

1. Используя метод линейного матричного шифрования (вручную или с использованием компьютера) над 34-буквенным русским алфавитом (добавьте символ пробела) с ключом $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ зашифруйте отрывок выбранной вами книги, содержащий не менее M символов (знаками препинания пренебречь). Для этого используйте данные табл. 9.5: возьмите пару (a, b) и подберите значения c и d таким образом, чтобы определитель матрицы был взаимно прост с 34.

Таблица 9.5

Варианты заданий

Вариант	a	b	M	Вариант	a	b	M
1	3	0	280	11	5	7	220
2	7	11	200	12	9	12	200
3	3	13	250	13	1	27	300
4	19	3	180	14	21	0	200
5	1	30	300	15	11	11	200
6	9	9	200	16	15	24	180
7	23	1	250	17	1	33	300
8	5	5	250	18	7	7	240
9	27	0	250	19	3	17	220
10	13	13	180	20	17	30	170

2. Обменяйтесь шифротекстами с группой-напарником. При этом дайте две подсказки о переходах биграмм, убедившись, что с их помощью можно получить дешифрующую матрицу.
3. Осуществите вскрытие шифротекста товарища.
4. Найдите ключ товарища и отправьте ему сообщение «ПРИНЯЛ».
5. Подготовьте отчет.

9.4.3. Содержание отчета

- Постановка задачи.
- Теоретические сведения: определения, свойства аффинных криптосистем, критерии однозначности;
- Результаты работы, в том числе:
  — обоснование работы криптосистемы;
  — для матричного шифрования — описание построения шифрующей матрицы;
  — описание получения подсказок, обоснование их достаточности;
  — описание получения ключей дешифрования и шифрования группы-напарника.
- Теоретическое обоснование полученных результатов.
- Выводы по работе.

9.5. Задания для лабораторных работ к разделу «Система *RSA*. Дискретный логарифм»

9.5.1. Система без передачи ключей

1. Используя простое число из заданного промежутка $[a, b]$ (табл. 9.6) в качестве модуля, приготовьте ключи для работы в системе «без передачи ключей».
2. Возьмите в качестве сообщения число m из заданного промежутка, зашифруйте с помощью одного из ваших ключей и передайте группе-напарнику. Выполните подтверждение (шифрование) при запросе группы-напарника.
3. Получите зашифрованное сообщение от группы-напарника. Начните процесс дешифрования. Отправьте запрос о подтверждении. При получении вскройте сообщение. Сверьте полученные данные с группой-напарником.
4. Подготовьте отчет о проделанной работе с обоснованием работы системы.

9.5.2. Система с открытым ключом

1. Используя простые числа из промежутка $[a, b]$ (табл. 9.6), создайте свой электронный адрес и ключи для работы в системе «с открытым ключом». Передайте свой адрес и открытый ключ группе-напарнику. Получите у них адрес и ключ.
2. Возьмите в качестве сообщения число m, не превосходящее адрес (модуль) группы-напарника, зашифруйте с помощью открытого ключа группы-напарника и передайте им.
3. Получите сообщение от группы-напарника, дешифруйте его. В качестве проверки отошлите полученное сообщение группе-напарнику, используя их адрес и ключ.
4. Получите ответ на ваше первое сообщение и сравните с ним. Сверьте полученные данные с группой-напарником.
5. Подготовьте отчет о проделанной работе с обоснованием работы системы.

Таблица 9.6

Варианты заданий

Вариант	a	b	Вариант	a	b	Вариант	a	b	Вариант	a	b
1	50	100	6	40	90	11	60	110	16	30	70
2	20	50	7	36	60	12	40	70	17	50	80
3	60	90	8	70	100	13	60	100	18	50	90
4	20	70	9	30	40	14	40	70	19	30	60
5	30	80	10	60	100	15	20	60	20	30	50

9.5.3. Электронная подпись

1. Используя простые числа из промежутка $[a, b]$ (табл. 9.6), создайте свой электронный адрес и ключи для работы в системе «электронная подпись». Передайте свой адрес и открытый ключ группе-напарнику. Получите у них адрес и ключ.
2. Возьмите в качестве сообщения число m, меньше каждого из адресов, зашифруйте с помощью открытого ключа группы-напарника и своего секретного ключа и передайте им.
3. Получите сообщение от группы-напарника, дешифруйте его. Сверьте полученные данные с группой-напарником.
4. Подготовьте отчет о проделанной работе с обоснованием работы системы.

9.5.4. Дискретный логарифм

1. Напишите программу, реализующую алгоритм нахождения дискретного логарифма двумя методами из трех: методом согласования, методом Сильвестра—Полига—Хеллмана, методом базы разложения. Убедитесь в их работоспособности.
2. Решите задачу нахождения дискретного алгоритма числа b с основанием a по модулю n (табл. 9.7). Для метода базы разложения, учитывая вероятностную природу метода, проведите решение несколько раз, выбор вероятностного параметра задайте строго случайный.
3. Сравните методы по количеству проводимых операций умножения/деления и возведения в степень. Подготовьте отчет.

Таблица 9.7

Варианты заданий

Вариант	a	b	n	Вариант	a	b	n
1	110	12	11807	11	11	11291	21599
2	12	9000	32033	12	3	250	1307
3	11	11291	21599	13	10	1000500	406981
4	3	250	1307	14	22	456789	671233
5	110	12	11807	15	11	11291	21599
6	10	1000500	406981	16	47	123456	537241
7	22	456789	671233	17	110	12	11807
8	110	12	11807	18	12	9000	32033
9	10	1000500	406981	19	47	123456	537241
10	47	123456	537241	20	12	9000	32033

9.5.5. Содержание отчета

- Постановка задачи.
- Теоретические сведения: определения, свойства и теоремы, на которые опираются алгоритмы лабораторной работы.
- Описание алгоритмов, используемых в работе.
- Результаты работы, в том числе:
  — тексты программ, реализующих использованные алгоритмы;
  — примеры работы программ: демонстрация корректной и ошибочной работы алгоритмов в зависимости от входных данных;
  — результаты статистического исследования корректности работы алгоритмов;

— результаты исследования скорости работы алгоритмов для различных входных данных.

- Теоретическое обоснование полученных результатов.
  Оцените среднее количество случайных выборов вероятностного параметра, использованных для решения задачи.
- Выводы по работе.

9.6. Задания для лабораторных работ к разделу «Вычислительные алгоритмы и их трудоемкость»

9.6.1. Алгоритм Евклида, его модификации и их трудоемкость

1. Напишите программы, реализующие алгоритмы нахождения наибольшего общего делителя и его линейного представления (обычный, бинарный, расширенный и расширенный бинарный), убедитесь в их работоспособности.
2. Сравните время работы алгоритмов для различных входных данных:
   a) примените все 4 алгоритма для нахождения (m, n) и (a, b) (табл. 9.8). Используя функцию оценки времени работы алгоритма, сравните временные затраты (используйте многократное применение алгоритма для замедления работы);
   b) выберите многократно случайным образом пары чисел из одного диапазона (диапазон A, табл. 9.8), сравните время работы алгоритмов для нахождения их наибольшего общего делителя, проанализируйте результаты;
   c) выберите многократно случайным образом пары чисел из разных диапазонов (диапазоны A и B, табл. 9.8), сравните время работы алгоритмов для нахождения их наибольшего общего делителя, проанализируйте результаты.
3. Оформите результаты в виде таблиц и приведите обоснование.

9.6.2. Применение алгоритма Евклида к решению неопределенных уравнений первой степени

1. Напишите программы, реализующие алгоритмы нахождения частного решения неопределенного уравнения первой степени (расширенный алгоритм Евклида, расширенный бинарный алгоритм Евклида, матричный алгоритм на основании алгоритма Евклида), убедитесь в их работоспособности.

Таблица 9.8

Варианты заданий

Вариант	m	n	a	b	A	B
1	22431	1023	1236	6132	1–500	21000–21500
2	23367	1032	1326	6123	500–1000	20500–21000
3	24261	1302	1263	6213	1000–1500	200000–205000
4	25329	1203	1623	6312	1500–2000	195000–200000
5	26409	1230	1362	6321	1–500	20000–20500
6	27483	1320	1632	6231	500–1000	19500–20000
7	23181	1722	2136	3612	1000–1500	21000–21500
8	24351	3171	2316	3621	1500–2000	200000–200500
9	26043	2751	2361	3261	1–500	19500–20000
10	38549	2751	2163	3162	500–1000	21000–21500
11	38899	3171	2613	3126	1000–1500	19500–20000
12	43383	1722	2631	3216	1500–2000	20000–20500
13	42847	3906	2631	6132	1–500	21000–21500
14	42917	1302	1632	3612	500–1000	20500–21000
15	38689	3157	1236	2136	1000–1500	20000–20500
16	38689	3157	1236	2136	1000–1500	20000–20500
17	38689	3157	1236	2136	1000–1500	20000–20500
18	38689	3157	1236	2136	1000–1500	20000–20500
19	38689	3157	1236	2136	1000–1500	20000–20500
20	38689	3157	1236	2136	1000–1500	20000–20500

2. Используя разработанные программы, найдите частные решения уравнений $ax + by = c$ и $mx + ny = l$ (табл. 9.9).
3. Сравните время работы алгоритмов для решения ваших уравнений, используя функцию оценки времени работы алгоритма. (Используйте многократное применение алгоритма для замедления работы.)
4. Оформите результаты в виде таблиц и приведите обоснование оценок.

Таблица 9.9

Варианты заданий

Вариант	a	b	c	m	n	l
1	270	285	2115	180	264	2304
2	150	−190	1210	187	−154	1551
3	290	−140	1640	323	−285	3496
4	414	−198	4824	510	−323	4709
5	275	−176	2981	110	260	1010
6	425	−238	4012	140	−190	2460
7	216	204	3000	275	−121	2959
8	375	285	2985	276	−264	1908
9	405	−390	2355	190	−290	2071
10	225	240	1695	406	−322	2940
11	110	−187	1628	460	340	5240
12	442	−493	4131	195	−345	1935
13	570	−209	3097	304	−192	3824
14	156	−336	2868	252	−270	4752
15	297	−319	2112	289	−255	4522
16	143	−234	3029	156	−216	2448
17	460	−600	5060	253	−187	3179
18	198	187	2761	351	−364	1469
19	198	−486	1872	165	−435	2115
20	250	170	1540	390	−285	4485

9.6.3. Содержание отчета

- Постановка задачи.
- Теоретические сведения: определения, свойства и теоремы, на которые опираются алгоритмы лабораторной работы.
- Описание алгоритмов, используемых в работе.
- Результаты работы, в том числе:
  - — тексты программ, реализующих используемые алгоритмы;
  - — промежуточные результаты;

— результаты исследования скорости работы алгоритмов для различных входных данных, оформленных в таблицах.

- Теоретическое обоснование полученных результатов по скорости работы алгоритмов.
- Выводы по работе.

9.7. Задания для лабораторных работ к разделу «Простые и псевдопростые числа»

9.7.1. Простейшие алгоритмы проверки чисел на простоту

1. Напишите программы, реализующие алгоритмы проверки чисел на простоту методом последовательного перебора и методом Ферма.
2. Убедитесь в работоспособности алгоритмов.
3. Реализуйте алгоритмы для проверки простоты чисел a и b (табл. 9.10).
4. Исследуйте зависимость результатов тестирования от свойств тестируемых чисел.
5. Обработайте полученные статистические данные.
6. Измерьте и сравните время работы алгоритмов.
7. Оформите результаты в виде таблиц и графиков и проведите обоснование.

9.7.2. Вероятностные алгоритмы проверки чисел на простоту

1. Напишите программу, реализующую вероятностные алгоритмы проверки чисел на простоту (тест Ферма, тест Соловея—Штрассена, тест Миллера—Рабина).
2. Убедитесь в работоспособности алгоритмов (учитывая вероятностный характер тестирования).
3. Реализуйте алгоритмы для проверки на простоту чисел a и b (табл. 9.10).
4. Исследуйте алгоритмы с точки зрения числа ошибок, допускаемых ими в зависимости: а) от вида числа; б) от числа прогонов теста.
5. Исследуйте зависимость результатов тестирования от свойств используемого генератора псевдослучайных чисел.
6. Обработайте полученные статистические данные.
7. Измерьте и сравните время работы алгоритмов.
8. Оформите результаты в виде таблиц и графиков и проведите обоснование.

Таблица 9.10

Варианты заданий

Вариант	a	b	Вариант	a	b	Вариант	a	b	Вариант	a	b
1	325	29341	6	527	15841	11	629	10585	16	631	8911
2	703	6601	7	2047	2243	12	2101	2821	17	2353	2465
3	3277	1307	8	1103	3467	13	29341	703	18	629	15841
4	527	3701	9	1729	1763	14	3277	1103	19	641	8911
5	1319	2101	10	2821	3277	15	629	1729	20	929	29341

9.7.3. Содержание отчета

- Постановка задачи.
- Теоретические сведения: теоретико-числовые теоремы, на которых базируются использованные методы.
- Результаты работы, в том числе:

  — текст программ, реализующих алгоритмы тестирования, текст подпрограмм для анализа эффективности и быстродействия тестов;

  — примеры работы программ: демонстрация корректной и ошибочной работы алгоритмов в зависимости от входных данных, заполненная таблица результатов работы (табл. 9.11), анализ причин некорректной работы алгоритма;

Таблица 9.11

Результаты работы

Тестируемое число	Число повторов теста	Результат: тест Ферма	Результат: тест Соловея — Штрассена	Результат: тест Милера — Рабина

  — результаты статистического исследования корректности работы алгоритмов, заполненная таблица с числом ошибок, допущенных тестами для каждого из чисел (табл. 9.12);

  — результаты исследования скорости работы алгоритмов для различных входных данных, обратить внимание на работу алгоритмов с числами Кармайкла. Для получения объективной оценки быстродействия алгоритмов нужно применить их к простым числам (подобрать самостоятельно, если в варианте такое не представлено).

Таблица 9.12

Результаты статистического исследования

Число повторов	Тест Ферма	Тест Соловея—Штрассена	Тест Милера—Рабина
1			
2			
3			
...			

- Теоретическое обоснование полученных результатов. Предложения по оптимизации алгоритмов.
- Выводы по работе.

9.8. Задания для лабораторных работ к разделу «Факторизация натуральных чисел»

9.8.1. Классические методы факторизации

1. Используя одну из модификаций метода Ферма, разложите на множители числа a и b (табл. 9.13).
2. Разложите эти же числа на множители, используя метод цепных дробей.
3. Сравните трудоемкость этих способов путем оценки количества шагов и выполненных операций с учетом их временных оценок.
4. Оформите результаты и проведите их обоснование.

9.8.2. Методы факторизации Полларда

1. Напишите программу, реализующую алгоритмы разложения чисел на множители ρ-методом Полларда и $(p-1)$-методом Полларда.
2. Убедитесь в работоспособности алгоритмов.
3. Реализуйте алгоритмы для факторизации чисел a и b (табл. 9.13). Перед началом работы проверьте числа на простоту.
4. Исследуйте алгоритмы с точки зрения их результативности и эффективности в зависимости от вида раскладываемых чисел.
5. Оформите результаты в виде таблиц и проведите их обоснование.

9.8.3. Содержание отчета

- Постановка задачи.
- Теоретические сведения.

Таблица 9.13

Варианты заданий

Вариант	a	b	Вариант	a	b	Вариант	a	b	Вариант	a	b
1	2491	3007	6	2773	3293	11	2867	3403	16	3149	3397
2	2279	3431	7	2551	2929	12	2623	1763	17	2021	3763
3	2987	3599	8	1927	3193	13	2173	1591	18	2491	3391
4	2867	1927	9	3149	3599	14	5183	2927	19	3293	2021
5	2537	1763	10	3403	2021	15	3431	2491	20	3599	3191

- Результаты работы, в том числе:
  — тексты программ, реализующих алгоритмы разложения чисел на множители, и подпрограмм возведения в степень по модулю n, вычисления наибольшего общего делителя чисел, проверки чисел на простоту (для классических методов возможно предоставление «ручных» расчетов);
  — примеры работы программ: демонстрация корректной и некорректной работы алгоритмов в зависимости от входных данных;
  — для классических методов результаты исследования скорости работы алгоритмов на основе оценки количества проделанных значимых операций;
  — для алгоритмов Полларда (табл. 9.14) — сравнительный анализ эффективности;

Таблица 9.14

Результаты анализа эффективности алгоритмов

Тестируемое число	Делитель: ρ-метод	Делитель: $(p-1)$-метод

  — результаты исследования скорости работы алгоритмов для различных входных данных (табл. 9.15).
- Теоретическое обоснование полученных результатов.
- Выводы по работе. Предложения по оптимизации алгоритмов.

Таблица 9.15

Результаты исследования скорости работы алгоритмов

Тестируемое число	Делитель: ρ-метод	Время: ρ-метод	Делитель: $(p-1)$-метод	Время: $(p-1)$-метод

9.9. Задания для лабораторной работы к разделу «Псевдослучайные последовательности над конечным полем»

1. Воспользовавшись многочленом $f(\lambda)$ над полем F_2 (табл. 9.16), найдите:
   a) линейное рекуррентное уравнение, соответствующее этому многочлену;
   b) число решений этого уравнения;
   c) главное решение этого уравнения;
   d) период главного решения этого уравнения;
   e) все возможные периоды решений этого уравнения; приведите примеры таких решений.
2. Приведите пример линейного рекуррентного уравнения, решение которого имеет период T (табл. 9.16).
3. Постройте конечное поле, состоящее из q элементов (табл. 9.16). Укажите, если это возможно, еще один способ построения данного поля.
4. Подготовьте отчет с теоретическими обоснованиями результатов.

9.9.1. Содержание отчета

- Постановка задачи.
- Теоретические сведения:
  — о построении конечного поля;
  — о решениях линейных рекуррентных уравнений;
  — о периодах указанных решений.
- Результаты работы, в том числе:
  — таблица с примерами решений линейных рекуррентных уравнений;
  — описание построения решения заданного периода;
  — таблица умножения построенного конечного поля с промежуточными результатами вычислений;
  — подробное описание процесса поиска решений линейных рекуррентных уравнений с заданным периодом (желательно предоставить несколько вариантов уравнений).

Таблица 9.16

Варианты заданий

Вариант	$f(\lambda)$	T	q
1	$\lambda^5 - \lambda^3 + \lambda^2 + 1$	9	81
2	$\lambda^4 - \lambda^3 + \lambda + 1$	31	125
3	$\lambda^6 - \lambda^3 + \lambda + 1$	15	121
4	$\lambda^5 - \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$	49	27
5	$\lambda^6 - 1$	93	25
6	$\lambda^5 - \lambda^3 + \lambda + 1$	14	64
7	$\lambda^4 - \lambda + 1$	27	32
8	$\lambda^6 - \lambda^2 + \lambda + 1$	42	16
9	$\lambda^5 - \lambda^4 + \lambda^2 + \lambda + 1$	12	81
10	$\lambda^5 - 1$	21	49
11	$\lambda^7 - \lambda^3 + \lambda^2 + 1$	9	81
12	$\lambda^4 - \lambda^3 + \lambda + 1$	31	125
13	$\lambda^6 - \lambda^3 + \lambda + 1$	15	121
14	$\lambda^5 - \lambda^3 + \lambda^2 + \lambda + 1$	49	27
15	$\lambda^6 - \lambda^3 + \lambda^2 + \lambda + 1$	93	25
16	$\lambda^5 + \lambda^3 + +1$	14	64
17	$\lambda^6 - \lambda^5 + \lambda + 1$	27	32
18	$\lambda^6 - \lambda^3 + \lambda^2 + 1$	42	16
19	$\lambda^5 + \lambda^2 + \lambda + 1$	12	81
20	$\lambda^5 + \lambda^2 + 1$	21	49

Глава 10

Таблицы

В этой главе пособия собраны полезные для освоения курса справочные материалы, представленные в виде таблиц.

10.1. Таблицы числовых эквивалентов символов русского и английского алфавитов

Современные методы шифрования оперируют с теми или иными числовыми эквивалентами обрабатываемых сообщений. В этом разделе приведены наиболее распространенные варианты числовой замены букв русского и английского алфавитов.

Таблица 10.1

Числовые эквиваленты букв русского алфавита

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	пробел
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Таблица 10.2

Числовые эквиваленты букв английского алфавита

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z	пробел	
14	15	16	17	18	19	20	21	22	23	24	25	26	

10.2. Таблицы Виженера

Таблицы Виженера лежат в основе классического полиалфавитного метода шифрования буквенного текста. В этом разделе приведены таблицы Виженера, составленные для русского и английского алфавитов.

Таблица 10.3

Таблица Виженера для русского алфавита

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э
Я	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я

Таблица 10.4

Таблица Виженера для английского алфавита

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

10.3. Таблицы частотности

Частотность — термин лексикостатистики, предназначенный для определения наиболее употребительных элементов (букв, слов, биграмм и т. д.) того или иного языка. Расчет осуществляется по формуле $\frac{N_x}{N}$, где N_x — количество употреблений в том или ином массиве информации элемен-

та x, а N — общее количество употреблений аналогичных элементов в том же массиве. Многие виды шифров могут быть раскрыты с помощью статистического анализа, потому что все естественные языки имеют характерное частотное распределение букв.

В таблице 10.5 представлена частотность букв русского языка, найденная на основе анализа их встречаемости букв в *Большом академическом словаре* — самом значительным по объему нормативной лексики словаре русского языка, который содержит более 150 000 слов, для построения которых использовано более чем $4,76 \cdot 10^8$ букв. Буквы расположены в таблице в порядке убывания их частотности.

Таблица 10.5

Частотность букв русского языка I

Ранг	Буква	Число употреблений	Частотность	Ранг	Буква	Число употреблений	Частотность
1	О	52295949	0,10983	17	Ы	9036813	0,01898
2	Е	40392978	0,08483	18	Ь	8263123	0,01735
3	А	38081816	0,07998	19	Г	8031521	0,01687
4	И	35075552	0,07367	20	З	7811723	0,01641
5	Н	31900994	0,067	21	Б	7579289	0,01592
6	Т	30084462	0,06318	22	Ч	6904749	0,0145
7	С	26058590	0,05473	23	Й	5753983	0,01208
8	Р	22595850	0,04746	24	Х	4597146	0,00966
9	В	21582499	0,04533	25	Ж	4476464	0,0094
10	Л	20678280	0,04343	26	Ш	3420179	0,00718
11	К	16599539	0,03486	27	Ю	3044673	0,00639
12	М	15252377	0,03203	28	Ц	2314208	0,00486
13	Д	14173134	0,02977	29	Щ	1719607	0,00361
14	П	13349597	0,02804	30	Э	1573696	0,00331
15	У	12452612	0,02615	31	Ф	1268926	0,00267
16	Я	9528713	0,02001	32	Ъ	175908	0,00037
				33	Ё	63623	0,00013

В таблице 10.6 буквы русского языка для удобства использования информации расположены в алфавитном порядке, а частотность выражена в процентах.

Таблица 10.6

Частотность букв русского языка II

Буква	Частотность, %	Буква	Частотность, %	Буква	Частотность, %
А	7,5	К	3,4	Ф	0,2
Б	1,7	Л	4,2	Х	1,1
В	4,6	М	3,1	Ц	0,5
Г	1,6	Н	6,5	Ч	1,5
Д	3,0	О	11,0	Ш	0,7
Е, Ё	8,7	П	2,8	Щ	0,4
Ж	0,9	Р	4,8	Ь, Ъ	1,7
З	1,8	С	5,5	Ы	1,9
И	7,5	Т	6,5	Э	0,3
Й	1,2	У	2,5	Ю	2,2
				Я	0,022

Таблица 10.7 содержит информацию о частотности букв английского языка. Буквы расположены в алфавитном порядке, а частотность выражена в процентах.

Таблица 10.7

Частотность букв английского языка

Буква	Частотность, %	Буква	Частотность, %	Буква	Частотность, %
A	8.1	K	0.4	V	0.9
B	1.4	L	3.4	W	1.5
C	2.7	M	2.5	X	0.2
D	3.9	N	7.2	Y	1.9
E	13.0	O	7.9	Z	0.1
F	2.9	P	2.0		
G	2.0	R	6.9		
H	5.2	S	6.1		
I	6.5	T	10.5		
J	0.2	U	2.4		

В таблицах 10.8 и 10.9 представлены наиболее часто встречающиеся слова русского и английского языков соответственно.

Таблица 10.8

Наиболее часто встречающиеся слова русского языка

Ранг	Слово	Ранг	Слово	Ранг	Слово	Ранг	Слово
1	и	13	к	25	ты	37	меня
2	в	14	это	26	они	38	был
3	не	15	все	27	было	39	только
4	на	16	по	28	мы	40	когда
5	что	17	из	29	бы	41	их
6	я	18	у	30	ее	42	или
7	с	19	она	31	вы	43	чтобы
8	он	20	за	32	для	44	сказал
9	а	21	от	33	мне	45	до
10	как	22	так	34	если	46	уже
11	но	23	же	35	то	47	ему
12	его	24	о	36	еще	48	да

Таблица 10.9

Наиболее часто встречающиеся слова английского языка

Ранг	Слово	Ранг	Слово	Ранг	Слово	Ранг	Слово
1	you	13	in	25	be	37	he
2	I	14	this	26	on	38	oh
3	to	15	know	27	your	39	about
4	the	16	I'm	28	was	40	right
5	a	17	for	29	we	41	you're
6	and	18	N	30	it's	42	get
7	that	19	have	31	with	43	here
8	it	20	my	32	so	44	out
9	of	21	don't	33	but	45	going
10	me	22	just	34	all	46	like
11	what	23	not	35	well	47	yeah
12	is	24	do	36	are	48	if

В таблице 10.10 собрана информация о наиболее часто встречающихся элементах (буквах, биграммах и триграммах) ряда европейских языков. (Для запоминания: десять наиболее часто встречающихся букв русского алфавита составляют слово «*СЕНОВАЛИТР*»; десять наиболее частых букв английского языка составляют слово "*TETRIS-HONDA*".)

Таблица 10.10

Наиболее часто встречающиеся элементы европейских языков

Русский язык: буквы	О, Е (Ё), А, И, Т, Н, С, Р, В, Л
Русский язык: биграммы	СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО
Русский язык: триграммы	СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА, ...
Английский язык: буквы	E, T, A, I, N, R, O, S, H, D
Английский язык: биграммы	TH, HE, AN, IN, ER, RE, ES, ON, EA, TI
Французский язык: буквы	E, S, A, N, T, I, R, U, L, O
Немецкий язык: буквы	E, N, I, S, T, A, H, D, U
Испанский язык: бкувы	E, A, O, S, I, R, N, L, D, C
Итальянский язык: буквы	I, E, A, O, N, T, R, L, S, T

10.4. Таблицы простых чисел

Простые числа играют важнейшую роль в современной криптографии. В этом разделе представлены необходимая для практических применений информация о простых числах.

Приведенный ниже список содержит *все простые числа, не превосходящие* 10000.

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659

661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
4327	4337	4339	4349	4357	4363	4373	4391	4397	4409

4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831
4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693
5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857
5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053
6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221
6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367
6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571
6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761
6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917
6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103
7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297
7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499
7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643
7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829
7841	7853	7867	7873	7877	7879	7883	7901	7907	7919
7927	7933	7937	7949	7951	7963	7993	8009	8011	8017
8039	8053	8059	8069	8081	8087	8089	8093	8101	8111
8117	8123	8147	8161	8167	8171	8179	8191	8209	8219
8221	8231	8233	8237	8243	8263	8269	8273	8287	8291
8293	8297	8311	8317	8329	8353	8363	8369	8377	8387
8389	8419	8423	8429	8431	8443	8447	8461	8467	8501
8513	8521	8527	8537	8539	8543	8563	8573	8581	8597
8599	8609	8623	8627	8629	8641	8647	8663	8669	8677

8681	8689	8693	8699	8707	8713	8719	8731	8737	8741
8747	8753	8761	8779	8783	8803	8807	8819	8821	8831
8837	8839	8849	8861	8863	8867	8887	8893	8923	8929
8933	8941	8951	8963	8969	8971	8999	9001	9007	9011
9013	9029	9041	9043	9049	9059	9067	9091	9103	9109
9127	9133	9137	9151	9157	9161	9173	9181	9187	9199
9203	9209	9221	9227	9239	9241	9257	9277	9281	9283
9293	9311	9319	9323	9337	9341	9343	9349	9371	9377
9391	9397	9403	9413	9419	9421	9431	9433	9437	9439
9461	9463	9467	9473	9479	9491	9497	9511	9521	9533
9539	9547	9551	9587	9601	9613	9619	9623	9629	9631
9643	9649	9661	9677	9679	9689	9697	9719	9721	9733
9739	9743	9749	9767	9769	9781	9787	9791	9803	9811
9817	9829	9833	9839	9851	9857	9859	9871	9883	9887
9901	9907	9923	9929	9931	9941	9949	9967	9973	

Таблица 10.12 содержит полный список известных простых чисел Мерсенна $M_p = 2^p - 1$ [122]. В таблице указаны: порядковый номер числа в последовательности простых чисел Мерсенна (знак «?» означает, что не все числа Мерсенна, меньшие данного, проверены на простоту); показатель степени p; число знаков в десятичном представлении M_p; год доказательства простоты числа; автор(ы) результата; дополнительно указано число знаков в десятичной записи соответствующего числу $M_p = 2^p - 1$ совершенного числа $P_p = 2^{p-1}(2^p - 1)$.

Таблица 10.12

№	Показатель p	Число знаков в M_p	Число знаков в P_p	Год	Автор
1	2	1	1	—	—
2	3	1	2	—	—
3	5	2	3	—	—
4	7	3	4	—	—
5	13	4	8	1456	anonymous
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers

Продолжение таблицы 10.12

№	Показатель p	Число знаков в M_p	Число знаков в P_p	Год	Автор
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll, Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson, Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt, Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski, Gage et al.
33	859433	258716	517430	1994	Slowinski, Gage
34	1257787	378632	757263	1996	Slowinski, Gage
35	1398269	420921	841842	1996	Armengaud, Woltman et al.
36	2976221	895932	1791864	1997	Spence, Woltman et al.

Продолжение таблицы 10.12

№	Показатель p	Число знаков в M_p	Число знаков в P_p	Год	Автор
37	3021377	909526	1819050	1998	Clarkson, Woltman, Kurowski et al.
38	6972593	2098960	4197919	1999	Hajratwala, Woltman, Kurowski et al.
39	13466917	4053946	8107892	2001	Cameron, Woltman, Kurowski et al.
40	20996011	6320430	12640858	2003	Shafer, Woltman, Kurowski et al.
41	24036583	7235733	14471465	2004	Findley, Woltman, Kurowski et al.
42	25964951	7816230	15632458	2005	Nowak, Woltman, Kurowski et al.
43	30402457	9152052	18304103	2005	Cooper, Boone, Woltman, Kurowski et al.
44	32582657	9808358	19616714	2006	Cooper, Boone, Woltman, Kurowski et al.
45 (?)	37156667	11185272	22370543	2008	Elvenich, Woltman, Kurowski et al.
46 (?)	42643801	12837064	25674127	2009	Strindmo, Woltman, Kurowski et al.
47 (?)	43112609	12978189	25956377	2008	Smith, Woltman, Kurowski et al.
48 (?)	57885161	17425170	34850339	2013	Cooper, Woltman, Kurowski et al.

В таблице 10.13 собраны известные рекорды простых чисел [122]. Кроме самого простого числа, в таблице указаны: его порядковый номер в последовательности наибольших известных простых чисел; количество знаков в десятичной записи числа; год доказательства простоты числа; если это возможно — тип числа. (Обобщенное число Ферма имеет вид $F_{n,b} = b^{2^n} + 1$.)

Таблица 10.13

Наибольшие известные простые числа

Номер	Простое число	Число знаков	Год	Тип простого числа
1	$2^{57885161} - 1$	17425170	2013	48 (?)-е простое Мерсенна
2	$2^{43112609} - 1$	12978189	2008	47 (?)-е простое Мерсенна
3	$2^{42643801} - 1$	12837064	2009	46 (?)-е простое Мерсенна
4	$2^{37156667} - 1$	11185272	2008	45 (?)-е простое Мерсенна
5	$2^{32582657} - 1$	9808358	2006	44-е простое Мерсенна
6	$2^{30402457} - 1$	9152052	2005	43-е простое Мерсенна
7	$2^{25964951} - 1$	7816230	2005	42-е простое Мерсенна
8	$2^{24036583} - 1$	7235733	2004	40-е простое Мерсенна
9	$2^{20996011} - 1$	6320430	2003	40-е простое Мерсенна
10	$2^{13466917} - 1$	4053946	2001	39-е простое Мерсенна
11	$19249 \cdot 2^{13018586} + 1$	3918990	2007	
12	$3 \cdot 2^{11731850} - 1$	3531640	2015	
13	$3 \cdot 2^{11484018} - 1$	3457035	2014	
14	$3 \cdot 2^{10829346} + 1$	3259959	2014	Делитель $F_{10829343,3}$
15	$475856^{524288} + 1$	2976633	2012	Обобщенное число Ферма
16	$356926^{524288} + 1$	2911151	2012	Обобщенное числ Ферма
17	$341112^{524288} + 1$	2900832	2012	Обобщенное число Ферма
18	$27653 \cdot 2^{9167433} + 1$	2759677	2005	
19	$90527 \cdot 2^{9162167} + 1$	2758093	2010	
20	$75898^{524288} + 1$	2558647	2011	Обобщенное число Ферма

В таблице 10.14 дана информация о современном статусе чисел Ферма $F_n = 2^{2^n} + 1$. (Из таблицы следует, что F_4 — наибольшее известное простое число Ферма; F_{11} — наибольшее из полностью факторизованных составных чисел Ферма; $F_{2478782}$ — наибольшее известное составное число Ферма; F_{33} — наименьшее число Ферма, характер которого неизвестен.)

Таблица 10.14

Статус исследованных чисел Ферма

Простые	$n = 0, 1, 2, 3, 4$
Полностью факторизованные	$n = 5, 6, 7, 8$ (два простых множителя в каждом), 9 (3 множителя), 10 (4 множителя), 11 (5 множителей)
известно пять простых множителей	$n = 12$
известно четыре простых множителя	$n = 13$
известно три простых множителя	$n = 15, 25$
известно два простых множителя	$n = 16, 18, 19, 27, 30, 36, 38, 52, 77, 147, 150, 284, 416$
известен один простой множитель	$n = 17, 21, 23, 26, 28, 29, 31, 32, 37, 39, 42, 43$ и 190 значений n с $43 < n \leqslant 2478782$
составное, но не известно ни одного простого множителя	$n = 14, 20, 22, 24$
характер неизвестен	$n = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, \ldots$

Простые делители чисел Ферма имеют специальную форму: любой делитель F_n, $n > 2$, имеет вид $k \cdot 2^{n+2} + 1$ для некоторого натурального k. Информация об известных простых делителях чисел Ферма представлена в таблице 10.15 [122]. Как и ранее, помимо самого простого числа, в таблице содержится его порядковый номер в последовательности известных простых делителей чисел Ферма, количество знаков в десятичной записи числа, год нахождения числа, и, наконец, информация о числах Ферма, на него делящихся.

Таблица 10.15

Простые делители чисел Ферма

Номер	Простое число	Число знаков	Год	Делимое
1	$193 \cdot 24^{3329782} + 1$	1002367	2014	$F_{3329780}$
2	$57 \cdot 2^{2747499} + 1$	827082	2013	$F_{2747497}$
3	$267 \cdot 2^{2662090} + 1$	801372	2015	$F_{2662088}$
4	$9 \cdot 2^{2543551} + 1$	765687	2011	$F_{2543548}$
5	$3 \cdot 2^{2478785} + 1$	746190	2003	$F_{2478782}$
6	$7 \cdot 2^{2167800} + 1$	652574	2007	$F_{2167797}$
7	$3 \cdot 2^{2145353} + 1$	645817	2003	$F_{2145351}$
8	$25 \cdot 2^{2141884} + 1$	644773	2011	$F_{2141872}$
9	$183 \cdot 2^{1747660} + 1$	526101	2013	$F_{1747656}$
10	$131 \cdot 2^{1494099} + 1$	449771	2012	$F_{1494096}$
11	$329 \cdot 2^{1246017} + 1$	375092	2012	$F_{1246013}$
12	$2145 \cdot 2^{1099064} + 1$	330855	2013	$F_{1099061}$
13	$11 \cdot 2^{960901} + 1$	289262	2005	F_{960897}
14	$1705 \cdot 2^{906110} + 1$	272770	2012	F_{906108}
15	$27 \cdot 2^{672007} + 1$	202296	2005	F_{672005}
16	$659 \cdot 2^{617815} + 1$	185984	2009	F_{617813}
17	$151 \cdot 2^{585044} + 1$	176118	2007	F_{585042}
18	$519 \cdot 2^{567235} + 1$	170758	2009	F_{567233}
19	$243 \cdot 2^{495732} + 1$	149233	2007	F_{495728}
20	$651 \cdot 2^{476632} + 1$	143484	2008	F_{476624}

10.5. Таблицы неприводимых и примитивных многочленов

В этом разделе собрана справочная информация о неприводимых и примитивных многочленах над конечными полями, играющих важнейшую роль в вопросах практического использования теории конечных полей для нужд криптографии [78].

В таблице 10.16 представлены число $a_p(n)$ неприводимых многочленов степени n над полем F_p, $p \in P$ и число $b_p(n)$ примитивных многочленов степени n над полем F_p, $p \in P$.

Таблица 10.16

Число неприводимых и примитивных многочленов над полем F_p

1	2	1	3	1	5	2	7	2
2	1	1	3	2	10	4	21	8
3	2	2	8	4	40	20	112	36
4	3	2	18	8	150	48	588	160
5	6	6	48	22	624	304		
6	9	6	116	48				
7	18	18	312	156				
8	30	16						
9	56	48						
10	99	60						
11	186	176						

В таблице 10.17 дан полный список всех неприводимых многочленов над полем F_2 степени $n \leqslant 6$. Многочлен $f(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n \in \in F_2[x]$ представлен набором $a_0a_1a_2 \ldots a_n$ его коэффициентов. Для каждого многочлена f в таблице указан и его порядок $\operatorname{ord} f$.

Таблица 10.17

Неприводимые многочлены над полем F_2

$n = 1; a_0, a_1$	$\operatorname{ord} f$	$n = 5; a_0, a_1, a_2, a_3, a_4, a_5$	$\operatorname{ord} f$
11	1	100101	31
$n = 2; a_0, a_1, a_2$		101001	31
111	3	101111	31
$n = 3; a_0, a_1, a_2, a_3$		111011	31
1011	7	110111	31
1101	7	111101	31
$n = 4; a_0, a_1, a_2, a_3, a_4$		$n = 6; a_0, a_1, a_2, a_3, a_4, a_5, a_6$	
10011	15	1000011	63
11001	15	1100001	63
11111	5	1100111	63
		1110011	63
		1011011	63
		1101101	63
		1010111	21
		1110101	21
		1001001	9

10.6. Таблицы индексов

В этом разделе представлены таблицы индексов для простых чисел p, меньших 100. Они полезны для нахождения дискретных логарифмов по модулю p.

Таблица 10.18

$p = 3, p - 1 = 2, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1								0	1	2								

Таблица 10.19

$p = 5, p - 1 = 2^2, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2						0	1	2	4	3						

Таблица 10.20

$p = 7, p - 1 = 2 \cdot 3, g = 3.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3				0	1	3	2	6	4	5				

Таблица 10.21

$p = 11, p - 1 = 2 \cdot 5, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6	0	1	2	4	8	5	10	9	7	3	6
1	5										1										

Таблица 10.22

$p = 13, p - 1 = 2^2 \cdot 3, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8	0	1	2	4	8	3	6	12	11	9	5
1	10	7	6								1	10	7								

Таблица 10.23

$p = 17$, $p - 1 = 2^4$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2	0	1	3	9	10	3	5	15	11	16	14
1	3	7	13	4	9	6	8					1	8	7	4	12	2	6			

Таблица 10.24

$p = 19$, $p - 1 = 2 \cdot 3^2$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8	0	1	2	4	8	16	13	7	14	9	18
1	17	12	15	5	7	11	4	10	9		1	17	15	11	3	6	12	5	10		

Таблица 10.25

$p = 23$, $p - 1 = 2 \cdot 11$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10	0	1	5	2	10	4	20	8	17	16	11
1	3	9	20	14	21	127	8	7	12	15	1	9	22	18	21	13	19	3	15	6	7
2	5	13	11								2	12	14								

Таблица 10.26

$p = 29$, $p - 1 = 2^2 \cdot 7$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10	0	1	2	4	8	16	3	6	12	24	19
1	23	25	7	18	13	27	4	21	11	9	1	9	18	7	14	28	27	25	21	13	26
2	24	17	26	20	8	16	19	15	14		2	23	17	5	10	20	11	22	15		

Таблица 10.27

$p = 31$, $p - 1 = 2 \cdot 3 \cdot 5$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2	0	1	3	9	27	19	26	16	17	20	29
1	14	23	19	11	22	21	6	7	26	4	1	25	13	8	24	10	30	28	22	4	12
2	8	29	17	27	13	10	5	3	16	9	2	5	15	14	11	2	6	18	23	7	21
3	15																				

Таблица 10.28

$p = 37,\ p - 1 = 2^2 \cdot 3^2,\ g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16	0	1	2	4	8	16	32	27	17	34	31
1	24	30	28	11	33	13	4	7	17	35	1	25	13	26	15	30	23	9	18	36	35
2	25	22	31	15	29	10	12	6	34	21	2	33	29	21	5	10	20	3	6	12	24
3	14	9	5	20	8	19	18				3	11	22	7	14	28	19				

Таблица 10.29

$p = 41,\ p - 1 = 2^3 \cdot 5,\ g = 6.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	21	1	39	38	30	0	1	6	36	11	25	27	39	29	10	19
1	8	3	27	31	25	37	24	33	16	9	1	32	28	4	24	21	3	18	26	33	34
2	34	14	29	36	13	4	17	5	11	7	2	40	35	5	30	16	14	2	12	31	22
3	23	28	10	18	19	21	2	32	35	6	3	9	13	37	17	20	38	23	15	8	7
4	20																				

Таблица 10.30

$p = 47,\ p - 1 = 2 \cdot 23,\ g = 5.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40	0	1	5	25	31	14	23	21	11	8	40
1	19	7	10	11	4	21	26	16	12	45	1	12	13	18	43	27	41	17	38	2	10
2	37	6	25	5	28	2	29	14	22	35	2	3	15	28	46	42	22	16	33	24	26
3	39	3	44	27	34	33	30	42	17	31	3	36	39	7	35	34	29	4	20	6	30
4	9	15	24	13	43	41	23				4	9	45	37	44	32	19				

Таблица 10.31

$p = 53,\ p - 1 = 2^2 \cdot 13,\ g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34	0	1	2	4	8	16	32	11	22	44	35
1	48	6	19	24	15	12	4	10	35	37	1	17	34	15	30	7	14	28	3	6	12
2	49	31	7	39	20	42	25	51	16	46	2	24	48	43	33	13	26	52	51	49	45
3	13	33	5	23	11	9	36	30	38	41	3	37	21	42	31	9	18	36	19	38	23
4	50	45	32	22	8	29	40	44	21	28	4	46	39	25	50	47	41	29	5	10	20
5	43	27	26								5	40	27								

Таблица 10.32

$p = 59,\ p - 1 = 2 \cdot 29,\ g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42	0	1	2	4	8	16	32	5	10	20	40
1	7	25	52	45	19	56	4	40	43	38	1	21	42	25	50	41	23	46	33	7	14
2	8	10	26	15	53	12	46	34	20	28	2	28	56	53	47	35	11	22	44	29	58
3	57	49	5	17	41	24	44	55	39	37	3	57	55	51	43	27	54	49	39	19	38
4	9	14	11	33	27	48	16	23	54	36	4	17	34	9	18	36	13	26	52	45	31
5	13	32	47	22	35	31	21	30	29		5	3	6	12	24	48	37	15	30		

Таблица 10.33

$p = 61,\ p - 1 = 2^2 \cdot 3 \cdot 5,\ g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12	0	1	2	4	8	16	32	3	6	12	24
1	23	15	8	40	50	28	4	47	13	26	1	48	35	9	18	36	11	22	44	27	54
2	24	55	16	57	9	44	41	18	51	35	2	47	33	5	10	10	40	19	38	15	30
3	29	59	5	21	48	11	14	39	27	46	3	60	59	57	53	45	29	58	55	49	37
4	25	54	56	43	17	34	58	20	10	38	4	13	26	52	43	25	50	39	17	34	7
5	45	53	42	33	19	37	52	32	36	31	5	14	28	56	51	41	21	42	23	46	31
6	30																				

Таблица 10.34

$p = 67, p - 1 = 2 \cdot 3 \cdot 11, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12	0	1	2	4	8	16	32	64	61	55	43
1	16	59	41	19	24	54	4	64	13	10	1	19	38	9	18	36	5	10	20	40	13
2	17	62	60	28	42	30	20	51	25	44	2	26	52	37	7	14	28	56	45	23	46
3	55	47	5	32	65	38	14	22	11	58	3	25	50	33	66	65	63	59	51	35	3
4	18	53	63	9	61	27	29	50	43	46	4	6	12	24	48	29	58	49	31	62	57
5	31	37	21	57	52	8	26	49	45	36	5	47	27	54	41	15	30	60	53	39	11
6	56	7	48	35	6	34	33				6	22	44	21	42	17	34				

Таблица 10.35

$p = 71$, $p - 1 = 2 \cdot 5 \cdot 7$, $g = 7$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52	0	1	7	49	59	58	51	2	14	27	47
1	34	31	38	39	7	54	24	49	58	16	1	45	31	4	28	54	23	19	62	8	56
2	40	27	37	15	44	56	45	8	13	68	2	37	46	38	53	16	41	3	21	5	35
3	60	11	30	57	55	29	64	20	22	65	3	32	11	6	42	10	70	64	22	12	13
4	46	25	33	48	43	10	21	9	50	2	4	20	69	57	44	24	26	40	67	43	17
5	62	5	51	23	14	59	19	42	4	3	5	48	52	9	63	15	34	25	33	18	55
6	66	69	17	53	36	67	63	47	61	41	6	30	68	50	66	36	39	60	65	29	61
7	35																				

Таблица 10.36

$p = 73$, $p - 1 = 2^3 \cdot 3^2$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12	0	1	5	25	52	41	59	3	15	2	10
1	9	55	22	59	41	7	32	21	20	62	1	50	31	9	45	6	30	4	20	27	62
2	17	39	63	46	30	2	67	18	49	35	2	18	17	12	60	8	40	54	51	36	34
3	15	11	40	61	29	34	28	64	70	65	3	24	47	16	7	35	29	72	68	48	21
4	25	4	47	51	71	13	54	31	38	66	4	32	14	70	58	71	63	23	42	64	28
5	10	27	3	53	26	56	57	68	43	5	5	67	43	69	53	46	11	55	56	61	13
6	23	58	19	45	48	60	69	50	37	52	6	65	33	19	22	37	39	49	26	57	66
7	42	44	36								7	38	44								

Таблица 10.37

$p = 79$, $p - 1 = 2 \cdot 3 \cdot 13$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0	0	4	1	8	62	5	53	12	2	0	1	3	9	27	2	6	18	54	4	12	
1	66	68	9	34	57	63	16	21	6	32	1	36	29	8	24	72	58	16	48	65	37
2	70	54	72	26	13	46	38	3	61	11	2	32	17	51	74	64	34	23	69	49	68
3	67	56	20	69	25	37	10	19	36	35	3	46	59	19	57	13	39	38	35	26	78
4	74	75	58	49	76	64	30	59	17	28	4	76	70	52	77	73	61	25	75	67	43
5	50	22	42	77	7	52	65	33	15	31	5	50	71	55	7	21	63	13	14	42	47
6	71	45	60	55	24	18	73	48	29	27	6	62	28	5	15	45	56	10	30	11	33
7	41	51	14	44	23	47	40	43	39		7	20	60	22	66	40	41	44	53		

Таблица 10.38

$p = 83$, $p - 1 = 2 \cdot 41$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0	0	1	72	2	27	73	8	3	62	0	1	2	4	8	16	32	64	45	7	14	
1	28	24	74	77	9	17	4	56	63	47	1	28	56	29	58	33	66	49	15	30	60
2	29	80	25	60	75	54	78	52	10	12	2	37	74	65	47	11	22	44	5	10	20
3	18	38	5	14	57	35	64	20	48	67	3	40	80	77	71	59	35	70	57	31	62
4	30	40	81	71	26	7	61	23	76	16	4	41	82	81	79	75	67	51	19	38	76
5	55	46	79	59	53	51	11	37	13	34	5	69	55	27	54	25	50	17	34	68	53
6	19	66	39	70	6	22	15	45	58	50	6	23	46	9	18	36	72	61	39	78	73
7	36	33	65	69	21	44	49	32	68	43	7	63	43	3	6	12	24	48	13	26	52
8	31	42	41								8	21	42								

Таблица 10.39

$p = 89$, $p - 1 = 2^3 \cdot 11$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2	0	1	3	9	27	81	65	17	51	64	14
1	86	84	33	23	9	71	64	6	18	35	1	42	37	22	66	20	60	2	6	18	54
2	14	82	12	57	49	52	39	3	25	59	2	73	41	34	13	39	28	84	74	44	43
3	87	31	80	85	22	63	34	11	51	24	3	40	31	4	12	36	19	57	82	68	26
4	30	21	10	29	28	72	73	54	65	74	4	78	56	79	59	88	86	80	62	8	24
5	68	7	55	78	19	66	41	36	75	43	5	72	38	25	75	47	52	67	23	69	29
6	15	69	47	83	8	5	13	56	38	58	6	87	83	71	35	16	48	55	76	50	61
7	79	62	50	20	27	53	67	77	40	42	7	5	15	45	46	49	58	85	77	53	70
8	46	4	37	61	26	76	45	60	44		8	32	7	21	63	11	33	10	30		

Таблица 10.40

$p = 97$, $p - 1 = 2^5 \cdot 3$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44	0	1	5	25	28	43	21	8	40	6	30
1	35	86	42	25	65	71	40	89	78	81	1	53	71	64	29	48	46	36	83	27	38
2	69	5	24	77	76	2	59	18	3	13	2	93	77	94	82	22	13	65	34	73	74
3	9	46	74	60	27	32	16	91	19	95	3	79	7	35	78	2	10	50	56	86	42
4	7	85	39	4	58	45	15	84	14	62	4	16	80	12	60	9	45	31	58	96	92
5	36	63	93	10	52	87	37	55	47	67	5	72	69	54	76	89	57	91	67	44	26
6	43	64	80	75	12	26	94	57	61	51	6	33	68	49	51	61	14	70	59	4	20
7	66	11	50	28	29	72	53	21	33	30	7	3	15	75	84	32	63	24	23	18	90
8	41	88	23	17	73	90	38	83	92	54	8	62	19	95	87	47	41	11	55	81	17
9	79	56	49	20	22	82	48				9	85	37	88	52	66	39				

Ответы и решения

В этом разделе представлены ответы, указания и решения для избранных задач пособия.

1 глава 1.1 параграф.

15. **Ответ:** «КВАДРАТ».
17. **Ответ:** при поворотах трафарета по часовой стрелке после 120 поворотов, против часовой стрелки — после 66.

1 глава 1.2 параграф.

4. **Ответ:** "DQTTR EBRTT KVLQR".
5. **Ответ:** «ЭТОТ ШИФР НАЗЫВАЕТСЯ ПОВОРОТНАЯ РЕШЕТКА». (В этой задаче надо было догадаться, что картинка соответствует трафарету, накладывая который всеми возможными способами на квадрат с шифротекстом, выписываем буквы из «окошек» и получаем искомый текст.)
6. **Ответ:** «В ПОСЛЕДНИЕ ГОДЫ СФЕРА РЕАЛЬНЫХ И ПОТЕНЦИАЛЬНЫХ ПРИЛОЖЕНИЙ КРИПТОГРАФИИ РАСШИРИЛАСЬ И ВКЛЮЧИЛА В СЕБЯ РЯД ДРУГИХ ОБЛАСТЕЙ, В КОТОРЫХ СИСТЕМЫ СВЯЗИ ИГРАЮТ ВАЖНЕЙШУЮ РОЛЬ СОЗДАНИЕ И ХРАНЕНИЕ БАЗ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ЭЛЕКТРОННЫЕ ФИНАНСОВЫЕ РАСЧЕТЫ И ТАК ДАЛЕЕ ЗАЧАСТУЮ ИМЕЕТСЯ БОЛЬШАЯ СЕТЬ ПОЛЬЗОВАТЕЛЕЙ ЛЮБЫЕ ДВА ИЗ КОТОРЫХ ДОЛЖНЫ ИМЕТЬ ВОЗМОЖНОСТЬ СДЕЛАТЬ ПЕРЕПИСКУ МЕЖДУ НИМИ СЕКРЕТНОЙ КАК ДЛЯ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ТАК И ДЛЯ ПОСТОРОННИХ МНОЖЕСТВО УЧАСТНИКОВ, МЕЖДУ КОТОРЫМИ ПОДДЕРЖИВАЕТСЯ СВЯЗЬ, МОЖЕТ СОСТОЯТЬ».
7. **Ответ:** «ШИРОКО ИСПОЛЬЗУЮТСЯ КОМБИНАТОРНЫЕ И АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ».
11. **Ответ:** «КАК ВЫБРАТЬ СРЕДСТВО ЗАЩИТЫ ОТ ЭТИХ УГРОЗ МОЖНО ПОЛНОСТЬЮ ДОВЕРИТЬСЯ ПРОДАВЦУ СОВЕРШЕННО НЕ ПОНИМАЯ НА ЧЁМ ОСНОВАНЫ ЕГО ОБЕЩАНИЯ ОБЕСПЕЧИТЬ ВАМ ГАРАНТИРОВАННУЮ ЗАЩИТУ ИЛИ МОЖНО СДЕЛАТЬ САМОСТОЯТЕЛЬНЫЙ ОСОЗНАННЫЙ ВЫБОР ВО ВТОРОМ СЛУЧАЕ ВАМ НЕ ОБОЙТИСЬ БЕЗ ЗНАНИЙ НАУЧНЫХ ОСНОВ КРИПТОГРАФИИ».
12. **Ответ:** «РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ».

13. **Ответ:** «НА ПЕРВЫЙ ВЗГЛЯД КАЖЕТСЯ ЧТО ЧЕМ ХИТРЕЕ СИМВОЛЫ ТЕМ ТРУДНЕЕ ВСКРЫТЬ СООБЩЕНИЕ ЭТО КОНЕЧНО НЕ ТАК ЕСЛИ КАЖДОМУ СИМВОЛУ ОДНОЗНАЧНО СОПОСТАВИТЬ КАКУЮ ЛИБО БУКВУ ИЛИ ЧИСЛО ТО ЛЕГКО ПЕРЕЙТИ К ЗАШИФРОВАННОМУ СООБЩЕНИЮ ИЗ БУКВ ИЛИ ЧИСЕЛ С ТОЧКИ ЗРЕНИЯ КРИПТОГРАФОВ ИСПОЛЬЗОВАНИЕ РАЗЛИЧНЫХ СЛОЖНЫХ СИМВОЛОВ НЕ УСЛОЖНЯЕТ ШИФРА».

14. **Ответ:** «ЗАМЕТИМ⌣ЧТО ⌣СИСТЕМА ⌣С ⌣ОТКРЫТЫМ ⌣КЛЮЧОМ ⌣ПОЗВОЛИТ ⌣ДВУМ ⌣УЧАСТНИКАМ ⌣НАЧАТЬ ⌣СЕКРЕТНЫЙ ⌣ОБМЕН ⌣ДАННЫМИ ⌣БЕЗ ⌣ПРЕДВАРИТЕЛЬНОГО ⌣КОНТАКТА ⌣БЕЗ ⌣ВЗАИМНОЙ ⌣ПРОВЕРКИ ⌣И ⌣БЕЗ ⌣ПРЕДВАРИТЕЛЬНОГО ⌣ОБМЕНА ⌣КАКОЙ ⌣ЛИБО ⌣ИНФОРМАЦЕЙ ⌣ВСЯ НЕОБХОДИМАЯ ⌣ДЛЯ ⌣ПОСЫЛКИ ⌣ШИФРОВАННОГО ⌣СООБЩЕНИЯ ⌣ИНФОРМАЦИЯ ⌣ ⌣ОБЩЕДОСТУПНА».

16. **Ответ:** «БЫК ВЯЗ ГНОЙ ДИЧЬ ПЛЮЩ СЪЁМ ЦЕХ ШУРФ ЭТАЖ».

17. **Ответ:** «ЧТОБЫ ПОЛУЧИТЬ ПЯТЬ НУЖНО ОТЛИЧНО ЗНАТЬ ПОЛУЧИЛОСЬ НЕПЛОХО».

1 глава 1.3 параграф.

2. **Ответ:** число комбинаций, получаемых за 25 и 32 щелчка, совпадают, комбинаций для 33 щелчков меньше.

3. **Ответ:** шифр второго криптографа содержит больше ключей.

4. **Ответ:** нельзя.

5. **Ответ:** «СВЯЗЬ-ПО-РАДИО».

8. **Ответ:** «НАУКА».

11. **Ответ:** «ПЕРЕСТАВЬТЕБУКВЫ».

12. **Ответ:** ключевое слово — «РУСЬ»; исходное сообщение — «Истина не рождается из истины. Истина рождается из ошибок. Капица.»

16. **Ответ:** нас устроят все абонентские номера, кратные $[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] = 5 \cdot 7 \cdot 8 \cdot 9 = 20520$.

17. **Ответ:** количество различных перестановок, получающихся в результате двукратного применения перестановки шести элементов, равно 270.

18. **Ответ:** «ПЕРЕБОР КЛЮЧЕЙ».

20. **Ответ:** искомой ключевой комбинацией является участок алфавита, начинающийся с $(k+1)$-й и заканчивающийся m-й буквой.

22. **Ответ:** «Кавалергардов век недолог, и потому так сладок он. Труба трубит, откинут полог».

23. **Ответ:** недостаток способа Ватсона состоит в том, что злоумышленник C может перехватить и заменить сообщение от A; способ Холмса не позволяет злоумышленнику получить секретное сообщение.

2 глава 2.2 параграф.

1. **Ответ:** "AGENT 006 IS DEAD 007".
2. **Ответ:** «СРОЧНО ПРИЕЗЖАЙ! МАМА».
3. **Ответ:** «ЗАДАНИЕ ПОЛУЧЕНО. БОБ».
7. **Ответ:** "FOUNDTHEGOLD"; "AWOFUWAE".

3 глава 1.3 параграф. Указания

10. **Указание:** определитель взаимно прост с p^α в том и только в том случае, когда он взаимно прост с p.
11. **Указание:** используя формулу $\varphi(N) = N\prod\limits_{p|N}(1-p^{-1})$ для числа $\varphi(N)$ элементов множества $(\mathbb{Z}_N)^*$, запишите формулу для $\varphi_2(N)$ в аналогичном виде.

3 глава 3.2 параграф.

1. **Ответ:** «ПРИВЕТ».
2. **Ответ:** «РЕШЕНА».
4. **Ответ:** «ГОТОВО».
5. **Ответ:** "STRIKE AT NOON! KARLA".
17. **Ответ:** $29^8(29^2-1)(29^2-29) = 341208073352438880$.
18. **Ответ:** $A^{-1} = \begin{pmatrix} 18 & 21 & 19 \\ 13 & 18 & 3 \\ 3 & 19 & 11 \end{pmatrix}$; "SENDROSESANDCAVIARJAMESBOND".

7 глава 7.1 параграф.

1. **Ответ:**
   a) $66124207 = 3571 \cdot 18517$;
   b) $35677933 = 1823 \cdot 19571$;
   c) $21478022263 = 33457 \cdot 641959$.

2. **Ответ:**
   a) $8644409 = 3251 \cdot 2659 (3251 - 1 = 2 \cdot 5^2 \cdot 13)$;
   b) $17095777 = 4931 \cdot 3467 (4931 - 1 = 2 \cdot 5 \cdot 17 \cdot 29)$;
   c) $4839315539 = 65521 \cdot 73859 (65521 - 1 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13)$.
3. **Ответ:**
   a) $2355343 = 1321 \cdot 1783$ (база $B = \{2, 3, 7, 11\}$, B-гладкими являются числа P_1^2, P_3^2);
   b) $6105409 = 2137 \cdot 2857$ (база $B = \{2, 3, 5\}$, B-гладкими являются числа P_1^2, P_3^2);
   c) $27658343 = 4703 \cdot 5881$ (база $B = \{2, 19, 31\}$, B-гладкими являются числа P_5^2, P_7^2).

8 глава 8.2 параграф.

7. **Решение:** для $n = 1$ доказательство очевидно; если $n \neq 1$, то $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, и $\sum\limits_{d|n} \mu(d) = \prod\limits_{i=1}^{k} (1 + \mu(p_1) + \mu(p_1^2) + \dots) = \prod\limits_{i=1}^{k} (1 - 1 + 0 + \dots) = 0$.
8. **Решение:** с одной стороны, $\sum\limits_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum\limits_{d|n} \mu(d) \sum\limits_{c|\frac{n}{d}} f(c) = \sum\limits_{cd|n} \mu(d) \times \times f(c) = \sum\limits_{c|n} f(c) \sum\limits_{d|\frac{n}{c}} \mu(d) = f(n)$; с другой стороны, $\sum\limits_{d|n} f(d) = \sum\limits_{d|n} \sum\limits_{c|d} \mu(c) \times \times F\left(\frac{d}{c}\right) = \sum\limits_{k|n} F(k) \sum\limits_{c} \frac{n}{k} \mu(c) = F(n)$.
11. **Решение:** так как $\mu(n) \geqslant -1$, то из формулы $n \cdot a_p(n) = \sum\limits_{m|n} p^{\frac{m}{n}} \mu(m)$ следует, что $n \cdot a_p(n) \geqslant p^m - p^{m-1} - \dots - p = \frac{p^{n+1} - 2p^n + p}{p-1} > 0$.

Словарь терминов

- *Алгоритм* — набор инструкций, описывающих порядок действий исполнителя для достижения результата решения задачи за конечное число действий.
- *Асимметричный шифр* (*двухключевой шифр*, *шифр с открытым ключом*) — шифр, в котором используются два ключа, шифрующий и расшифровывающий.
- *Аутентификация* — проверка подлинности чего-либо или кого-либо.
- *Блочный шифр* — разновидность симметричного шифра, оперирующего группами бит фиксированной длины — блоками, размер которых меняется в пределах 64–256 бит.
- *Взлом* (*вскрытие*) — расшифрование зашифрованного сообщения без знания ключа.
- *Вероятностный алгоритм* — алгоритм, для которого выполняется одно из следующих утверждений: результат работы алгоритма является решением поставленной задачи с некоторой вероятностью; алгоритм оканчивает свою работу с некоторой вероятностью; оценка числа шагов алгоритма является случайной величиной.
- *Гаммирование* — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст.
- *Декодирование* — процесс, обратный кодированию.
- *Детерминированный алгоритм* — алгоритм, результат работы которого после фиксированного числа шагов (операций над элементами конечного множества) всегда является решением поставленной задачи.
- *Дешифрование* (*дешифровка*) — синоним расшифрования.
- *Идентификация* — описательное представление какого-либо субъекта.
- *Имитозащита* — защита от навязывания ложной информации, возможность проверить, что текст (открытого) сообщения не был изменен. Имитозащита достигается обычно за счет включения в пакет передаваемых данных *имитовставки* — блока информации, зависящего от ключа и данных.
- *Ключ* — параметр шифра, определяющий выбор конкретного преобразования данного текста.

- *Кодирование* — фиксированное преобразование информации из одного вида в другой (обычно в целях, не связанных с защитой информации от несанкционированного доступа).
- *Криптоанализ* — наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа. *Криптоаналитик* — ученый, создающий и применяющий методы криптоанализа.
- *Криптографическая атака* — попытка вызвать отклонения в атакуемой защищенной системе обмена информацией. *Взлом* — успешная криптографическая атака.
- *Криптографическая стойкость* — способность криптографического алгоритма противостоять криптоанализу.
- *Криптография* — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.
- *Криптология* — криптография и криптоанализ как единая наука о создании и взломе шифров.
- *Моноалфавитный шифр* (*шифр простой замены*) — простейший случай симметричного шифрования: каждому символу открытого текста соответствует единственный символ шифротекста.
- *Неподвижный символ* — символ, который при данном шифрующем преобразовании переходит в себя.
- *Однозвучный шифр* — шифр, в котором каждому символу открытого текста соответствует один, или, в случае символов открытого текста с большей частотой, несколько возможных символов-заменителей, что «сглаживает» частоту употребления символов в шифротексте.
- *Открытый ключ* — тот из двух ключей асимметричной системы, который свободно распространяется.
- *Открытый текст* (*исходный текст*) — данные (не обязательно текстовые), передаваемые без использования криптографии.
- *Перестановка* (*шифр перестановки*) — простейший случай симметричного шифрования, в котором элементы открытого текста (биты, буквы, символы) переставляют в некотором новом порядке.
- *Полиалфавитный шифр* — шифр, состоящий в циклическом применении нескольких моноалфавитных шифров к определенному числу букв шифруемого текста.

- *Полиномиальный алгоритм* — «быстрый» алгоритм: оценка времени его работы представима в виде многочлена от размера входных данных.
- *Потоковый шифр* — симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста.
- *Полиграммный шифр* — шифр, при котором заменяются не один символ открытого текста, а два, три или целая группа.
- *Принцип Керкгоффса* — правило разработки криптографических систем, согласно которому в засекреченном виде держится только определенный набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования предполагается открытым.
- *Псевдослучайная последовательность* — числовая последовательность, полученная по некоторому определенному арифметическому правилу, но имеющая все свойства случайной последовательности чисел в рамках решаемой задачи.
- *Псевдопростое число* — натуральное число, обладающее некоторыми свойствами простых чисел, являясь тем не менее составным.
- *Расшифровывание* — преобразование в криптосистемах, обратное шифрованию.
- *Секретный ключ* (*закрытый ключ*) — тот из двух ключей асимметричной криптографической системы, который хранится в секрете.
- *Симметричное шифрование* — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ (ключ дешифрования легко может быть получен из ключа шифрования, и наоборот).
- *Стеганография* — наука о скрытой передаче информации путем сохранения в тайне самого факта передачи.
- *Субэкспоненциальный алгоритм* — алгоритм, который работает более, чем за полиномиальное время (сверхполиномиальное), но менее, чем за экспоненциальное время (субэкспоненциальное).
- *Тест простоты* (*распознавание простоты числа*) — алгоритм, позволяющий выяснить, является ли заданное натуральное число простым. Вероятностный тест простоты может гарантировать, что исследуемое число — составное; детерминированный тест простоты может гарантировать, что исследуемое число — простое.
- *Транспозиция* (*маршрутная транспозиция*, *постолбцовая транспозиция*) — перестановочный табличный шифр, использующий нестандартный маршрут заполнения таблицы, усложняющий алгоритм.

- *Факторизация* — декомпозиция объекта (числа, полинома и др.) в произведение других объектов (как правило, базовых: числа — в произведение простых чисел, многочлена — в произведение неприводимых многочленов). Факторизация целых чисел обеспечивается основной теоремой арифметики, а многочленов — основной теоремой алгебры.
- *Частотный анализ* (*частотный криптоанализ*) — метод криптоанализа, основывающийся на нетривиальном статистическом распределении отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, сохраняется в ходе шифрования и дешифрования.
- *Шифр* (*криптосистема*) — семейство обратимых преобразований открытого текста в шифрованный.
- *Шифрование* — процесс применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.
- *Шифротекст* (*шифрованный текст*, *закрытый текст*) — данные, полученные после применения криптографического преобразования.
- *Экспоненциальный алгоритм* — «медленный» алгоритм, оценка времени работы которого зависит от размерности входных данных экспоненциально.
- *Электронная цифровая подпись* (*электронная подпись*) — асимметричная имитовставка (ключ защиты отличается от ключа проверки); другими словами, имитовставка, которую проверяющий не может подделать.

Литература

[1] *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.

[2] *Александров В. А., Горшенин С. М.* Задачник-практикум по теории чисел. М.: Просвещение, 1972. 82 с.

[3] *Алексеев А. П.* Изучение криптографии на уроках // Информатика и образование. 2003. № 4. С. 33–60.

[4] *Алферов А. П., Зубов А. Ю.* Основы криптографии. М.: Гелиос АРВ, 2001. 480 с.

[5] *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2002.

[6] *Антонов А. К., Артюшенко В. М.* Защита информации. Методы защиты информации. М.: ГОУВПО МГУС, 2005.

[7] *Арнольд И. В.* Теоретическая арифметика. М.: УЧПЕДГИЗ, 1938. 480 с.

[8] *Аршинов М. Н., Садовский Л. Е.* Коды и математика (рассказы о кодировании). М.: Наука, 1983. 146 с.

[9] *Астрахан В. И., Гусев В. В., Павлов В. В., Чернявский Б. Г.* Становление и развитие правительственной связи в России. Орел: ВИПС, 1996. С. 79–80.

[10] *Бабаш А. В.* Криптография в XIX веке // Первое сентября. 2004. № 33. С. 17.

[11] *Бабаш А. В., Шанкин Г. П.* История криптографии. Ч. I. М.: Гелиос АРВ, 2002. 240 с.

[12] *Баврин И. И., Фрибус Е. А.* Старинные задачи. М.: Просвещение, 1994. 128 с.

[13] *Баричев С. Г., Серов Р. Е.* Основы современной криптографии. М.: Горячая Линия-Телеком, 2002. 152 с.

[14] *Баулина Ю. Н., Деза Е. И. Математические модели, методы и теории.* М.: МПГУ, 2004. 16 с.

[15] *Белецкий А. Я., Белецкий А. А.* Блочный криптоалгоритм с динамическим управлением параметрами шифрования // Системи обробки інформації, 2009. Вып. 7. С. 125–126.

[16] *Бернет С., Пэйн С.* Криптография. Официальное руководство RSA Security. М.: Бином-Пресс, 2002. 384 с.

[17] *Биркгоф Г., Барти Т.* Современная прикладная алгебра. М.: Мир, 1976. 400 с.

[18] *Болл У., Коксетер Г.* Математические эссе и развлечения. М.: Мир, 1986. 472 с.

[19] *Брассар Ж.* Современная криптология. М.: Полимед, 1999. 176 с.

[20] *Бухштаб А. А.* Теория чисел. М.: Просвещение, 1966. 380 с.

[21] *Василенко О. Н., Галочкин А. И.* Сборник задач по теории чисел. М.: Издательство МГУ, 1995. 128 с.

[22] *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.

[23] *Варфоломеев А. А., Жуков А. Е., Пудовкина М. А.* Поточные криптосистемы. Основные свойства и методы анализа стойкости. М.: ПАИМС, 2000. 36 с.

[24] Введение в криптографию / Под общей ред. В. В. Ященко. М.: МЦНМО, 2012. 348 с.

[25] *Виленкин Н. Я.* Математика и шифры // Квант, 1977. № 8. С. 52–56.

[26] *Виноградов И. М.* Основы теории чисел. М.: Наука, 1981. 178 с.

[27] *Галкин В. Я., Сычугов Д. Ю., Хорошилова Е. В.* Конкурсные задачи, основанные на теории чисел. М.: Факультет ВМиК МГУ, 2002. 180 с.

[28] *Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б.* Введение в теорию чисел. М.: Издательство МГУ, 1995. 160 с.

[29] *Герман О. Н., Нестеренко Ю. В.* Теоретико-числовые методы в криптографии. М.: Академия, 2012. 272 с.

[30] *Гарднер М.* От мозаик Пенроуза к надежным шифрам. М.: Мир, 1993. 416 с.

[31] *Гельфанд И. М.* Лекции по линейной алгебре. М.: МЦНМО, 1998. 319 с.

[32] *Грибанов В. У., Титов П. И.* Сборник упражнений по теории чисел. М.: Просвещение, 1964. 844 с.

[33] *Девеннорт Г.* Мультипликативная теория чисел. М.: Наука, 1971. 200 с.

[34] *Девеннорт Г.* Высшая арифметика. М.: URSS, 2010. 176 с.

[35] *Депман И. Я.* История арифметики. М.: Просвещение, 1965. 416 с.

[36] *Деза Е. И., Котова Л. В.* Сборник задач по теории чисел. М.: Ленанд/URSS, 2018. 224 с.

[37] *Деза Е. И.* Специальные числа натурального ряда. М.: Ленанд/URSS, 2017. 240 с.

[38] *Диффи У., Хелмэн М.* Защищенность и имитостойкость. Введение в криптографию // ТИИЭР, 1979. Т. 67. № 3. С. 71–109.

[39] *Добльхофер Э.* Знаки и чудеса. М.: Восточная литература, 1963. 388 с.

[40] *Дориченко С. Я., Ященко В. В.* 25 этюдов о шифрах. М.: Теис, 1994. 72 с.

[41] *Жданов О. Н., Куденкова И. А.* Криптоанализ классических шифров / Лаб. практикум для студ. Красноярск: СГАУ, 2008. 107 с.

[42] *Жельников В.* Криптография от папируса до компьютера. М.: ABF, 1996. 335 с.

[43] *Жмулева А. В.* Сборник задач по теории чисел. М.: ЦПИ МГУ, 2009.

[44] *Зубов А. Ю.* XIV олимпиада по математике и криптографии для школьников // Информатика. 2005. № 7. С. 29–32.

[45] *Зубов А. Ю., Зязин А. В., Овчинников В. Н., Рамоданов С. М.* Олимпиады по криптографии и математике. М.: МЦНМО, 2006. 136 с.

[46] *Зязин А. В.* Олимпиады, конкурсы, викторины и игры на уроках информатики // Информатика в школе. 2003. № 5. С. 101–113.

[47] *Зязин А. В.* Заочные конкурсы по математике и криптографии для школьников // Информатика. 2004. № 31. С. 4–26.

[48] *Ингам А. Е.* Распределение простых чисел. М.: Мир, 1936. 160 с.

[49] *Ишмухаметов Ш. Т.* Методы факторизации натуральных чисел. Казань: Казанский университет, 2011. 190 с.

[50] *Карацуба А. А.* Основы аналитической теории чисел. М.: Наука, 1983. 240 с.

[51] *Карацуба А. А., Офман Ю.* Умножение многозначных чисел на автоматах // Докл. Академии Наук СССР. 1962. Т. 145. № 2. С. 293–294.

[52] *Кнут Д.* Искусство программирования для ЭВМ. М.: Мир, 1977.

[53] *Коблиц Н.* Курс теории чисел и криптографии. М.: Научное издательство ТВП, 2001. 260 с.

[54] *Кордемский Б. А.* Так или не так действовал Ферма? // Квант. 1972. № 7. С. 11–13.

[55] *Котова Л. В.* Сборник задач по дисциплине «Методы и средства защиты информации». М.: МПГУ, 2015. 44 с.

[56] *Коэн Х., Ленстра Х.* Проверка чисел на простоту и суммы Якоби // Кибернетический сборник. 1987. № 24. С.99–146.

[57] *Коробейников А. Г., Гатчин Ю. А.* Из истории криптографии. Математические основы криптологии. СПб.: СПб ГУ ИТМО, 2004. С. 10–13.

[58] *Коробейников А. Г., Гатчин Ю. А.* Математические основы криптологии / Учеб. пособ. СПб: СПб ГУ ИТМО, 2004. 106 с.

[59] *Кострикин А. И., Манин Ю. И.* Линейная алгебра и геометрия. М.: Наука, 1986. 304 с.

[60] *Кострикин А. И.* Введение в алгебру. М.: Наука, 2004. 368 с.

[61] *Коутихот С.* Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. 328 с.

[62] *Курант Р., Робертс Г.* Что такое математика? М.: МЦНМО, 2010.

[63] *Лебедев А. Н.* Криптография с открытым ключом и возможности ее практического применения // Защита информации. 1992. Вып. 2. С. 129–147.

[64] *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. 820 с.

[65] *Лунин А. В., Сальников А. А.* Перспективы развития и использования асимметричных алгоритмов в криптографии // Конфидент. № 24. С. 15–22.

[66] *Мальцев А. И.* Основы линейной алгебры. М.: Наука, 1970. 400 с.

[67] *Манин Ю. И., Панчишкин А. А.* Введение в современную теорию чисел. М.: МЦНМО, 2009. 550 с.

[68] *Маховенко Е. Б.* Теоретико-числовые методы в криптографии. М.: Гелиос, 2006. 320 с.

[69] *Миллер Г. Л.* Гипотеза Римана и способы проверки простоты чисел // Кибернетический сборник. 1986. №23. С.31–50.

[70] *Михелович Ш. Х.* Теория чисел. М.: Высшая школа, 1967. 338 с.

[71] *Молдовян А. А., Молдовян Н. А., Советов Б. Я.* Криптография. СПб.: Лань, 2000. 224 с.

[72] Неопубликованные материалы Эйлера по теории чисел / Под ред. Невской Н. И. СПб.: Наука, 1997. 256 с.

[73] *Нестеренко А. Ю., Крупицын Е. С.* Теоретико-числовые методы в криптографии. Учеб.-метод. материалы для проведения контр. раб. М: МГИЭМ, 2011. 32 с.

[74] *Нестеренко А. Ю.* Теоретико-числовые методы в криптографии. М: МГИЭМ, 2012. 224 с.

[75] *Нестеренко Ю. В.* Теория чисел. М.: Академия, 2008. 272 с.

[76] *Нечаев В. И.* К вопросу о сложности детерминированного алгоритма для дискретного логарифма // Математические заметки, 1994. Т. 55. Вып. 2. С. 91–101.

[77] *Нечаев В. И.* Распределение на части периода линейной рекуррентной последовательности над конечным полем // Тезисы III Междунар. конф. «Совр. проблемы теории чисел и ее прил.». Тула: ТГПУ, 1996. С. 107.

[78] *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999. 109 с.

[79] *Ожигова Е. П.* Развитие теории чисел в России. М.: URSS, 2011. 360 с.

[80] *Осипян В. О., Осипян К. В.* Криптография в упражнениях и задачах. М.: Гелиос, 2004. 144 с.

[81] *Перельман Я. И.* Занимательная арифметика. Загадки и диковинки в мире чисел. М.: Русанова, 1994. 192 с.

[82] *Петров А. А.* Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2000. 448 с.

[83] *Пилиди В. С.* Криптография. Вводные главы. Ростов-на-Дону: ЮФУ, 2009. 110 с.

[84] *Плутарх.* Сравнительные жизнеописания. М.: Наука, 1994. 1042 с.

[85] *Полибий.* Всеобщая история в сорока книгах. / пер. с греч. Ф. Г. Мищенко. Т. 2 М., 1895.

[86] *Прахар К.* Распределение простых чисел. М.: Мир, 1967. 514 с.

[87] *Радемахер Г., Теплиц О.* Числа и фигуры. Опыты математического мышления. М.: Наука, 1966. 264 с.

[88] *Рожков А. В., Ниссенбаум О. В.* Теоретико-числовые методы в криптографии. Тюмень: Изд. ТюмГУ, 2007. 180 с.

[89] *Ростовцев А. Г., Маховенко Е. Б.* Теоретическая криптография. М.: Профессионал, 2005. 490 с.

[90] *Рябко Б. Я., Фионов А. Н.* Криптографические методы защиты информации. М.: Горячая линия-Телеком, 2005. 230 с.

[91] *Саломаа А.* Криптография с открытым ключом, М.: Мир, 1996. 318 с.

[92] *Серпинский В.* Что мы знаем и чего не знаем о простых числах. Л.: ГИФМЛ, 1963. 92 с.

[93] *Серпинский В.* 250 задач по элементарной теории чисел. М.: Просвещение, 1968. 162 с.

[94] *Сидельников В. М.* Криптография и теория кодирования. М.: Физматлит, 2008. С. 324.

[95] *Смарт Н.* Криптография. М.: Техносфера, 2005. 528 с.

[96] *Соболева Т. А.* Тайнопись в истории России. М.: Международные отношения, 1994. 384 с.

[97] *Степанова Л. Л.* Избранные главы элементарной теории чисел. М.: Прометей, 2001. 112 с.

[98] *Степанова Л. Л., Жмулева А. В., Деза Е. И.* Практикум по элементарной математике: Арифметика. М.: МЦНМО, 2008. 208 с.

[99] *Стренг Г.* Линейная алгебра и ее применения. М.: Мир, 1980. 454 с.

[100] *Тилборг ван Х. К. А.* Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. с. 471.

[101] *Топунов В. Л.* Комбинаторика. М.: МПГУ, 1988. С. 79.

[102] *Уильямс Х.* Проверка чисел на простоту с помощью вычислительных машин // Кибернет. сб. 1986. № 23. С. 51–99.

[103] *Фаддеев Д. К.* Лекции по алгебре. СПб.: Лань, 2007. 416 с.

[104] *Фергюсон Н., Шнайер Б.* Практическая криптография. М.: Диалектика, 2005. 416 с.

[105] *Фомичев В. М.* Дискретная математика и криптология. М.: Диалог МИФИ, 2003. 400 с.

[106] *Хинчин А. Я.* Цепные дроби. М.: URSS, 2018. 112 с.

[107] *Чандрасекхаран К.* Арифметические функции. М.: Наука, 1975. 272 с.

[108] *Черемушкин А. В.* Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.

[109] *Шафаревич И. Р., Ремизов А. О.* Линейная алгебра и геометрия. М.: Физматлит, 2009. 511 с.

[110] *Шнайер Б.* Криптоанализ. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.

[111] *Brillhart J., Morrison M. A.* A method of factoring and the factorization of F_7 // Math. Comp. 1975. Vol. 29. P. 183–205.

[112] *Alford W. R., Granville A., Pomerance C.* There are Infinitely Many Carmichael Numbers // Annals of Math. 1994. № 139. P. 703–722.

[113] *Conway J. H., Guy R. K.* The Book of Numbers. NY: Springer-Verlag, 1996. 310 p.

[114] *Dickson L. E.* History of the Theory of Numbers. NY: Dover, 2005. Vol. 1. 486 p.

[115] *Gauss C. F.* Disquisitiones Arithmeticae. Leipzig, 1801. 478 p.

[116] *Guy R. K.* Unsolved Problems in Number Theory. NY: Springer-Verlag, 2004. 438 p.

[117] *Hardy G. H., Wright E. M.* An Introduction to the Theory of Numbers. Oxford: Clarendon Press, 1979. 456 p.

[118] *Kahn D.* The Codebreakers The Story of Secret Writing. NY: Charles Scribner's Sons, 1967. 473 с.

[119] *Kerckhoffs A.* La cryptographie militaire // J. des sciences militaires. 1883. Jan. Vol. IX. P. 5–38.

[120] *Ore O.* Number Theory and Its History. Dover Publications, 1948. 400 p.

[121] *Pollard J. M.* Theorems on factorization and primality testing // Proc. Cambridge Phil. Soc. 1974. Vol. 76. P.521–528.

[122] The Prime Pages. (дата обращения: 5.08.2015) [Электронный ресурс] https://primes.utm.edu/

[123] *Ribenboim P.* New Book of Prime Number Records. NY: Springer-Verlag, 1996. 566 p.

[124] *Riesel H.* Prime Numbers and Computer Methods for Factorization. Basel: Birkhouser, 1994. 464 p.

[125] *Shanks D.* Solved and Unsolved Problems in Number Theory. NY: Chelsea, 1993. 258 p.

[126] *Sloane N. J.* The On-line Encyclopedia of Integer Sequences. (дата обращения 5.08.2015) [Электронный ресурс]. http://www.research.att.com/ñjas/sequences/

[127] *Singh S.* The Code book: the Secret History of Codes and Code-breaking. London: Forth Estate, 2000. 402 p.

[128] Wikipedia, the Free Encyclopedia. (дата обращения: 8.08.2015) [Электронный ресурс] http://en.wikipedia.org/

Издательская группа URSS представляет

Д. А. Борзых

ЭКОНОМЕТРИКА В ЗАДАЧАХ

Базовый курс

- С примерами в среде **MATLAB**
- Около **100** задач с решениями

Предлагаемый вниманию читателей сборник задач в первую очередь ориентирован на базовый курс эконометрики бакалавриата экономических факультетов университетов. Также задачник может быть использован в магистратуре при повторении бакалаврского курса.

Тематический состав большей части задачника вполне традиционен для курса бакалавриата: метод наименьших квадратов и теорема Гаусса–Маркова, доверительные интервалы, проверка статистических гипотез, фиктивные переменные и тест Чоу, гетероскедастичность, автокорреляция, тесты на правильную спецификацию модели: тест Рамсея и тест Бокса–Кокса, мультиколлинеарность, оценивание параметров методом максимального правдоподобия.

Помимо этого, задачник расширен более продвинутыми темами, относящимися к магистратуре: тестирование гипотез с помощью метода максимального правдоподобия: тест отношения правдоподобия, тест множителей Лагранжа, тест Вальда, модели бинарного выбора: logit- и probit-модели, элементы теории бутстрапирования (bootstrap).

В приложении содержатся элементарные сведения о свойствах ковариационных матриц, а также о распределении квадратичных форм, связанных с многомерным нормальным распределением.

Основной особенностью предлагаемого пособия является то, что помимо большого количества задач, которые предполагается решать «вручную», книга содержит задачи (как правило, с решениями), состоящие в написании программ, реализующих ту или иную эконометрическую процедуру. Автор уверен, что написание таких программ наиболее эффективно способствует прочному усвоению эконометрических процедур и их глубокому смысловому пониманию.

В задачнике в качестве среды программирования выбрана программа **MATLAB**. Опыт показывает, что **MATLAB** является достаточно простым и **доступным языком программирования** для большинства студентов экономических специальностей.

Пособие предназначено для **студентов** экономических специальностей и **преподавателей**, ведущих практические занятия по курсу **эконометрики**.

Кудряшов Н. А.

БЕРИЯ И СОВЕТСКИЕ УЧЕНЫЕ В АТОМНОМ ПРОЕКТЕ:

Книга 1. Выдающиеся ученые-ядерщики Советского Союза

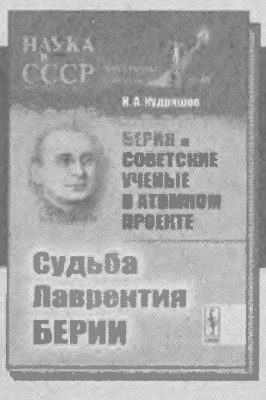
Создание атомного оружия в Советском Союзе – одна из выдающихся страниц истории нашей страны. В реализации этого невероятно трудного технологического прорыва принимало участие несколько сотен тысяч человек, но особая ответственность легла на интеллектуальное «ядро» создателей атомного оружия.

В первой части монографии Н. А. Кудряшова обсуждается участие в Советском атомном проекте выдающихся ученых и организаторов производства: Б. Л. Ванникова, П. Л. Капицы, И. В. Курчатова, Ю. Б. Харитона, К. И. Щёлкина, Я. Б. Зельдовича, И. Е. Тамма, А. Д. Сахарова, А. П. Александрова, А. Л. Минца и М. Г. Мещерякова. Связующим звеном сюжета книги являются отношения ученых и председателя специального комитета при Совете Министров СССР Лаврентия Берии.

Книга содержит много любопытных эпизодов и фактов из истории создания атомного оружия в Советском Союзе.

БЕРИЯ И СОВЕТСКИЕ УЧЕНЫЕ В АТОМНОМ ПРОЕКТЕ:

Книга 2. Судьба Лаврентия Берии



Вторая часть научно-исторического исследования Н. А. Кудряшова посвящена описанию жизни и деятельности руководителя специального комитета при Совете Министров СССР Лаврентия Берии. Дается анализ его роли в Советском атомном проекте и его участия в разрешении идеологического спора между физиками и философами, позволившего сохранить высокий уровень физической науки в СССР.

Обсуждается попытка проведения реформ в Советском Союзе, предпринятая Берией после смерти Сталина. Описаны события, происходившие после ареста Лаврентия Берии: выступления на июльском пленуме его «вчерашних друзей».

Обсуждаются материалы следствия по делу Берии и его расстрел. Даны детальные характеристики его помощников и заместителей. Книга содержит много новых фактов о деятельности Берии и его окружения.

Издательская группа URSS представляет

Свердлик А. Г.

Как **ЭМОЦИИ** влияют на **АБСТРАКТНОЕ МЫШЛЕНИЕ** и **ПОЧЕМУ МАТЕМАТИКА** невероятно **ТОЧНА**

Как устроена кора головного мозга, почему её возможности ограничены и **КАК ЭМОЦИИ,** дополняя работу **КОРЫ,** позволяют человеку **СОВЕРШАТЬ НАУЧНЫЕ ОТКРЫТИЯ**

Математика, в отличие от прочих дисциплин, универсальна и предельно точна. Она создаёт логическую структуру всех естественных наук. «Непостижимая эффективность математики», как в своё время определил этот феномен Э. Вигнер, горячо дискутируется в научной среде со времен Платона, но объяснение ему не найдено.

Автор, впервые в истории изучения этого вопроса, пытается подойти к нему с позиций нейронауки. В книге описаны анатомо-физиологические механизмы, лежащие в основе абстрактного мышления и формальной логики. Показано, что эти механизмы неизбежно закладывают погрешности в любые модели, которые создаёт кора головного мозга, и делают её в принципе неспособной к идеальным логическим построениям.

Далее обсуждаются эмоциональные и телесные аспекты процесса мышления, которые не только участвуют в поиске решения проблем, но и корректируют погрешности формальных когнитивных схем, давая нам таким образом возможность постигать математические истины.

Книга рассчитана на широкий круг читателей, интересующихся работой мозга и природой абстрактного мышления. Она написана лёгким и доступным языком, не содержит формул и не требует специального технического или гуманитарного образования.

Д. М. Златопольский

СИСТЕМЫ СЧИСЛЕНИЯ

УЧЕБНЫЕ И ЗАНИМАТЕЛЬНЫЕ МАТЕРИАЛЫ

- **Более 100 содержательных задач**
- **Фокусы, головоломки, исторические факты**
- **Решение задач из ЕГЭ по информатике**
- **Вопросы для конкурсов «Что? Где? Когда?» и «Брейн-ринг»**

В книге приведены задачи, фокусы, головоломки и другие увлекательнейшие материалы, связанные с недесятичными системами счисления. Ее материалы можно использовать на уроках, в качестве домашних заданий, на кружках и факультативах, во внеклассной работе.

Книга состоит из 18 глав и содержит 13 приложений. В ней приводятся: задачи разного уровня сложности; методика решения типовых задач на системы счисления, представленных в Едином государственном экзамене по информатике; арифметические и геометрические прогрессии чисел в недесятичных системах; логические и сдвиговые операции; основные принципы создания так называемых «помехоустойчивых» кодов; математические фокусы, головоломки, игры с числами в недесятичных системах счисления.

Все задания, представленные в книге, имеют развивающее значение для интеллекта, формируют общеучебные навыки и способствуют повышению интереса учащихся к математике и информатике. Ко всем заданиям даны ответы и разъяснения.

В приложениях описываются различные методы (в том числе малоизвестные) перевода из одной системы счисления в другую целых чисел и правильных дробей, программы (с методикой их разработки) решения задач, связанных с системами счисления, решением головоломок и демонстрацией фокусов, рассмотренных ранее, а также представлены материалы исторического характера (такие материалы имеются и в основной части книги в виде «врезок»).

Елена Ивановна ДЕЗА

Доктор педагогических наук (2012), кандидат физико-математических наук (1993). В 1983 г. окончила математический факультет Московского государственного педагогического института имени В. И. Ленина (МГПИ), в 1992 г. — аспирантуру по кафедре теории чисел МГПИ (ныне — Московский педагогический государственный университет, МПГУ), в 2010 г. — докторантуру по кафедре теоретической информатики и дискретной математики МПГУ. С 1988 г. — преподаватель кафедры теории чисел математического факультета МПГУ, с 2006 г. — профессор кафедры теоретической информатики и дискретной математики математического факультета МПГУ. Область научных интересов: теория чисел, дискретная математика, дидактика высшей школы. Автор нескольких монографий, более 10 учебных и учебно-методических пособий, более 150 научных публикаций.

Лидия Владимировна КОТОВА

Окончила математический факультет Московского педагогического государственного университета (МПГУ) в 2000 г., аспирантуру по кафедре теории чисел в 2003 г. С 2000 г. преподает на кафедре теории чисел МПГУ. Область научных интересов — теория чисел, криптография и дидактика высшей школы. Автор (совместно с Е. И. Деза) «Сборника задач по теории чисел» (М.: URSS) и учебных пособий по теории чисел и криптографии. В последние годы активно занимается разработкой методического обеспечения дисциплины «Методы и средства защиты информации» и курсов смежной тематики.
