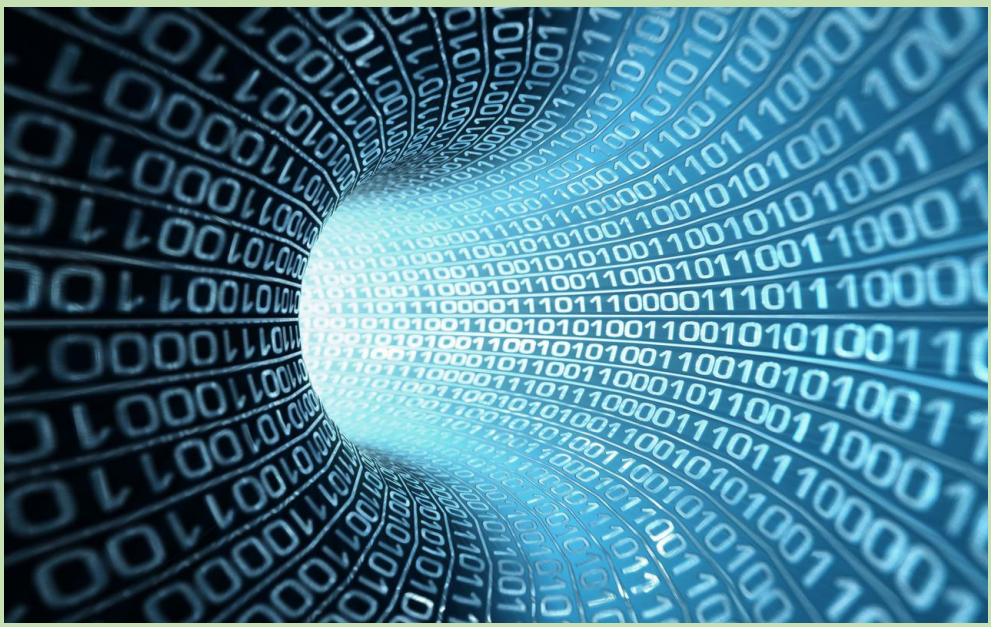
Ю. В. КУЛАКОВ, В. Е. ДИДРИХ, И. В. ДИДРИХ,
А. И. ЕЛИСЕЕВ, Н. Г. ШАХОВ,

ВВЕДЕНИЕ В КРИПТОЛОГИЮ

В четырех частях

Часть 2



Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2023

Министерство науки и высшего образования Российской Федерации

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Тамбовский государственный технический университет»**

**Ю. В. КУЛАКОВ, В. Е. ДИДРИХ, И. В. ДИДРИХ,
Н. Г. ШАХОВ, А. И. ЕЛИСЕЕВ**

ВВЕДЕНИЕ В КРИПТОЛОГИЮ

В четырех частях

Часть 2

Утверждено Ученым советом университета в качестве
учебного пособия для студентов направлений подготовки
09.03.02, 09.04.02 «Информационные системы и технологии»,
27.04.03 «Системный анализ и управление», 38.03.05 «Бизнес-информатика»
и специальностей 10.05.03 «Информационная безопасность автоматизированных систем»,
38.05.01 «Экономическая безопасность» очной и заочной форм обучения

Учебное электронное издание

Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2023

УДК 51(075.8)
ББК з811я73
В24

Рецензенты:

Доктор физико-математических наук, профессор
ФГБОУ ВО «ТГУ им. Г. Р. Державина»
Е. С. Жуковский

Кандидат технических наук, доцент,
заведующий кафедрой «Системы автоматизированной поддержки
принятия решений» ФГБОУ ВО «ТГТУ»
И. Л. Коробова

В24 **Введение** в криптологию [Электронный ресурс] : учебное пособие : в 4-х ч. / Ю. В. Кулаков, О. Г. Иванова, Н. Г. Шахов, А. И. Елисеев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2021.
ISBN 978-5-8265-2366-7.

Ч. 2. – Ю. В. Кулаков, В. Е. Дидрих, И. В. Дидрих, А. И. Елисеев, Н. Г. Шахов. – 2023. – 1 электрон. опт. диск (CD-ROM). – Системные требования : ПК не ниже класса Pentium II ; CD-ROM-дисковод ; 1,9 Mb ; RAM ; Windows 95/98/XP ; мышь. – Загл. с экрана.
ISBN 978-5-8265-2666-8.

Содержит теоретический материал по основным понятиям, определениям и алгоритмам арифметики остатков, конечных групп и полей и список рекомендуемой литературы.

Предназначено для студентов направлений подготовки 09.03.02, 09.04.02 «Информационные системы и технологии», 27.04.03 «Системный анализ и управление», 38.03.05 «Бизнес-информатика» и специальностей 10.05.03 «Информационная безопасность автоматизированных систем», 38.05.01 «Экономическая безопасность» очной и заочной форм обучения.

УДК 51(075.8)
ББК з811я73

ISBN 978-5-8265-2366-7 (общ.)
ISBN 978-5-8265-2666-8 (ч. 2)

ВВЕДЕНИЕ

Во второй части учебного пособия представлен материал, который ориентирован на изучение вопросов, связанных с дополнительными алгоритмами и элементами теории вероятностей в арифметике остатков, групп и конечных полей.

Среди вопросов, связанных с дополнительными алгоритмами в арифметике остатков, рассматриваются понятия: символ Лежандра, символ Якоби, извлечение корня по модулю составного числа.

В материале по элементам теории вероятностей обсуждается: понятие случайной величины, теорема Байеса, парадокс дней рождения.

Новизна данного учебного пособия, в сравнении с ранее изданной литературой по вопросам введения в криптологию [1 – 18], заключается в рассмотрении примеров практически к каждому даваемому понятию, определению и алгоритму.

Применение данного пособия будет способствовать формированию у выпускников следующих компетенций по направлениям подготовки и специальностям.

По направлению подготовки 09.03.02 «Информационные системы и технологии»: способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3).

По направлению подготовки 09.04.02 «Информационные системы и технологии»: способен разрабатывать требования к информационным системам (ИС) и осуществлять организационное и технологическое обеспечение возможности их реализации в ИС (ПК-1).

По направлению 27.04.03 «Системный анализ и управление»: способен решать задачи системного анализа и управления в технических системах на базе последних достижений науки и техники (ОПК-3).

По направлению 38.03.05 «Бизнес-информатика»: способен организовывать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия (ПК-1).

По специальности 10.05.03 «Информационная безопасность автоматизированных систем»: способен использовать математические методы, необходимые для решения

задач профессиональной деятельности (ОПК-3); способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10); способен разрабатывать компоненты систем защиты информации автоматизированных систем (ОПК-11).

По специальности 38.05.01 «Экономическая безопасность»: способен работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12); способен соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20).

1. АРИФМЕТИКА ОСТАТКОВ, ГРУППЫ, КОНЕЧНЫЕ ПОЛЯ

1.4. ДОПОЛНИТЕЛЬНЫЕ АЛГОРИТМЫ

1.4.1. СИМВОЛ ЛЕЖАНДРА

Пусть p является простым числом, бóльшим, чем 2. Рассмотрим отображение:

$$\mathbf{F}_p \to \mathbf{F}_p,\ \alpha \mapsto \alpha^2, \tag{1.66}$$

сопоставляющее каждому элементу α поля $\mathbf{F}_p$ его квадрат α^2, который также принадлежит полю $\mathbf{F}_p$.

Например, возьмем $p = 7$. Тогда упомянутое отображение (1.66) можно представить табл. 1.64.

На множестве ненулевых элементов поля $\mathbf{F}_p$ это отображение является отображением в точности «два-в-один».

В нашем примере (при $p = 7$) на множестве ненулевых элементов {1, 2, 3, 4, 5, 6} поля $\mathbf{F}_7$ отображение (из) $\mathbf{F}_7$ в $\mathbf{F}_7$ является строго отображением «два-в-один» (табл. 1.64):

– для двухэлементного прообраза {1, 6} образом является элемент 1;

– для двухэлементного прообраза {3, 4} образом является элемент 2;

– для двухэлементного прообраза {2, 5} образом является элемент 4.

Если из ненулевого элемента $x \in \mathbf{F}_p$ можно извлечь квадратный корень, то таких корней у него ровно 2.

В нашем примере (при $p = 7$), обратное к отображению (1.66) отношение на множестве ненулевых элементов {1, 2, 3, 4, 5, 6} поля $\mathbf{F}_7$ представлено табл. 1.65.

Таблица 1.64

x	$x^2 \pmod 7$
0	0
1	1
2	4
3	2

Таблица 1.65

x	$\sqrt{x} \pmod 7$
4	2
5	4
6	1
1	{1, 6}
2	{3, 4}
3	–
4	{2, 5}
5	–
6	–

Из таблицы видно, что:

- квадратным корнем из элемента 1 является как элемент 1, так и элемент 6;
- квадратным корнем из элемента 2 является как элемент 3, так и элемент 4;
- квадратным корнем из элемента 4 является как элемент 2, так и элемент 5;
- квадратного корня из элементов 3, 5 и 6 не существует.

Заметим, что ровно половина элементов из (поля вычетов без 0) $\mathbf{F}_p^* = \{1, \ldots, p-1\}$ является полными квадратами. В нашем случае, в поле $\mathbf{F}_7^* = \{1, 2, \ldots, 6\}$ полными квадратами являются элементы 1, 2 и 4 (см. табл. 1.64).

Полные квадраты в $\mathbf{F}_p^*$ называются *квадратичными вычетами* по модулю p. В нашем примере полные квадраты 1, 2 и 4 из $\mathbf{F}_7^*$ являются квадратичными вычетами по модулю 7.

Множество всех квадратичных вычетов по модулю p является подгруппой мощности, равной $(p-1)/2$, в мультипликативной группе $\mathbf{F}_p^*$. Для нашего примера множество всех квадратичных вычетов {1, 2, 4} по модулю 7 является подгруппой мощности $(7-1)/2 = 3$ в мультипликативной группе $\mathbf{F}_7^*$.

Элементы группы $\mathbf{F}_p^*$, из которых нельзя извлечь квадратный корень, называются *квадратичными невычетами*. В нашем примере элементы 3, 5 и 6 группы $\mathbf{F}_7^*$ являются квадратичными невычетами (см. табл. 1.65).

Таблица 1.66

$a \in \mathbf{F}_7$	a делится на p	a – квадратичный вычет по модулю p	a – квадратичный невычет по модулю p	Значение $\left(\frac{a}{p}\right)$
0	1	0	0	0
1	0	1	0	+1
2	0	1	0	+1
3	0	0	1	–1
4	0	1	0	+1
5	0	0	1	–1
6	0	0	1	–1

Множество всех квадратичных невычетов по модулю p также является подгруппой мощности, равной $(p - 1) / 2$, в мультипликативной группе $\mathbf{F}_p^*$. Для нашего примера множество всех квадратичных вычетов {1, 2, 4} по модулю 7 является подгруппой мощности $(7 – 1) / 2 = 3$ в мультипликативной группе $\mathbf{F}_7^*$.

Для выявления полных квадратов по простому модулю p вводится символ Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ +1, & \text{если } a - \text{квадратичный вычет по модулю } p; \\ -1, & \text{если } a - \text{квадратичный невычет.} \end{cases} \qquad (1.67)$$

Значения символа Лежандра $\left(\frac{a}{p}\right)$ для нашего примера (когда $p = 7$), полученные в соответствии с определением (1.67), представлены в табл. 1.66.

Заметим, что значение символа Лежандра можно вычислить, например, по формуле Эйлера:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}. \qquad (1.68)$$

Вычислить значения символа Лежандра можно по формуле (1.68) в нашем случае (при $p = 7$):

$$\left(\frac{0}{7}\right) = 0^{(7-1)/2} \pmod 7 = 0^3 \pmod 7 = 0 \pmod 7 = 0,$$

$\left(\frac{1}{7}\right) = 1^{(7-1)/2} \pmod 7 = 1^3 \pmod 7 = 1 \pmod 7 = +1,$

$\left(\frac{2}{7}\right) = 2^{(7-1)/2} \pmod 7 = 2^3 \pmod 7 = 8 \pmod 7 = 1 \pmod 7 = +1,$

$\left(\frac{3}{7}\right) = 3^{(7-1)/2} \pmod 7 = 3^3 \pmod 7 = 27 \pmod 7 = -1 \pmod 7 = -1,$

$\left(\frac{4}{7}\right) = 4^{(7-1)/2} \pmod 7 = 4^3 \pmod 7 = 16 \cdot 4 \pmod 7 = 2 \cdot 4 \pmod 7 =$

$= 8 \pmod 7 = 1 \pmod 7 = +1,$

$\left(\frac{5}{7}\right) = 5^{(7-1)/2} \pmod 7 = 5^3 \pmod 7 = 25 \cdot 5 \pmod 7 = 4 \cdot 5 \pmod 7 =$

$= 20 \pmod 7 = -1 \pmod 7 = -1,$

$\left(\frac{6}{7}\right) = 6^{(7-1)/2} \pmod 7 = 6^3 \pmod 7 = 36 \cdot 6 \pmod 7 = 1 \cdot 6 \pmod 7 =$

$= 6 \pmod 7 = -1 \pmod 7 = -1.$

Использование формулы Эйлера для определения символа Лежандра $\left(\frac{a}{p}\right)$ в поле $\mathbf{F}_p$ сопряжено с вычислениями больших степеней значения a, равных $(p - 1) / 2$. Поэтому на практике можно пользоваться *законом квадратичной взаимности*:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}, \qquad (1.69)$$

где p и q – неравные нечетные простые числа.

Заметим, что все нечетные простые числа разбиты на два класса: класс $K_1 = \{4 \cdot m + 1 \mid m = 1, 2, 3, \ldots\}$ нечетных простых чисел, сравнимых с числом один по модулю четыре, и класс $K_2 = \{4 \cdot m + 3 \mid m = 0, 1, 2, \ldots\}$ нечетных простых чисел, сравнимых с числом три по модулю четыре.

Рассмотрим ряд первых десяти нечетных простых чисел p на предмет их принадлежности классам K_1 и K_2, а также четности или нечетности $\frac{p-1}{2}$ и результаты сведем в табл. 1.67.

Таблица 1.67

p	p (mod 4)	$p \in K_1$	$p \in K_2$	$\frac{p-1}{2}$	Четность $\frac{p-1}{2}$
3	3	0	1	1	0
5	1	1	0	2	1
7	3	0	1	3	0
11	3	0	1	5	0
13	1	1	0	6	1
17	1	1	0	8	1
19	3	0	1	9	0
23	3	0	1	11	0
29	1	1	0	14	1
31	3	0	1	15	0

Из таблицы видно, что среди первых десяти нечетных простых чисел p принадлежат классу K_1 числа 5, 13, 17 и 29, а частное $\frac{p-1}{2}$ четно тогда и только тогда, когда $p \in K_1$.

Заметим также, что нечетным числом является произведение только нечетного числа на нечетное число, а в остальных случаях произведение (четного числа на четное или четного числа на нечетное) представляет собой число четное. Поэтому произведение $\frac{p-1}{2} \cdot \frac{q-1}{2}$ в формуле (1.69) будет нечетным тогда и только тогда, когда нечетны как $\frac{p-1}{2}$, так и $\frac{q-1}{2}$, т.е. произведение $\frac{p-1}{2} \cdot \frac{q-1}{2}$ будет нечетным тогда и только тогда, когда $p \in K_2 = \{4 \cdot m + 3 \mid m = 0, 1, 2, \ldots\}$ и $q \in K_2 = \{4 \cdot m + 3 \mid m = 0, 1, 2, \ldots\}$.

Таким образом, в соответствии с вышесказанным и формулой (1.69) имеем:

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), \text{ если } p \in K_2 \text{ и } q \in K_2; \\ \left(\frac{p}{q}\right), \text{ если из } p \text{ и } q \text{ хотя бы одно принадлежит } K_1. \end{cases} \quad (1.70)$$

При вычислении значения символа Лежандра большую помощь оказывают следующие дополнительные формулы:

$$\left(\frac{q}{p}\right) = \left(\frac{q\,(\mathrm{mod}\,p)}{p}\right), \tag{1.71}$$

$$\left(\frac{q\cdot r}{p}\right) = \left(\frac{q}{p}\right)\cdot\left(\frac{r}{p}\right), \tag{1.72}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}. \tag{1.73}$$

Определим значения символа Лежандра $\left(\frac{a}{p}\right)$ для $a \neq 0$ в случае, когда $p = 7$, с использованием формул (1.68), (1.70) – (1.73) с минимальными вычислениями больших степеней:

$\left(\frac{1}{7}\right)$ = (по формуле (1.68), единица в любой степени равна единице) =

$= 1^{(7-1)/2} \pmod 7 = 1 \pmod 7 = +1;$

$\left(\frac{2}{7}\right)$ = (по формуле (1.73), (–1) в нечетной степени равно (–1), в четной – единице) =

$= (-1)^{(7^2-1)/8} = (-1)^{(49-1)/8} = (-1)^{48/8} = (-1)^6 = 1 = +1;$

$\left(\frac{3}{7}\right)$ = (по формуле (1.70), $q = 3 \in K_2$, $p = 7 \in K_2$) =

$= -\left(\frac{7}{3}\right)$ (по формуле (1.71))

$= -\left(\frac{7\,(\mathrm{mod}\,3)}{3}\right) = -\left(\frac{1}{3}\right)$ = (по формуле (1.68), единица в любой степени равна единице) =

$= -(1^{(3-1)/2} \pmod 3) = -(1^1 \pmod 3) = -1;$

$\left(\frac{4}{7}\right) = \left(\frac{2\cdot 2}{7}\right)$ = (по формуле (1.72)) =

$= \left(\frac{2}{7}\right)\cdot\left(\frac{2}{7}\right)$ (как ранее было вычислено, $\left(\frac{2}{7}\right) = 1$) =

$= 1 \cdot 1 = 1 = +1;$

$\left(\frac{5}{7}\right)$ = (по формуле (1.70), $q = 5 \in K_1$, $p = 7 \in K_2$) =

= $\left(\frac{7}{5}\right)$ (по формуле (1.71)) = $\left(\frac{7 \pmod 5}{5}\right)$ =

= $\left(\frac{2}{5}\right)$ (по формуле (1.73), (–1) в нечетной степени равно (–1), в четной – единице) =

= $(-1)^{(5^2-1)/8} = (-1)^{(25-1)/8} = (-1)^{24/8} = (-1)^3 = -1$;

$\left(\frac{6}{7}\right) = \left(\frac{2 \cdot 3}{7}\right)$ = (по формуле (1.72)) =

= $\left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right)$ (как ранее было вычислено, $\left(\frac{2}{7}\right) = 1$, $\left(\frac{3}{7}\right) = -1$) =

= $1 \cdot (-1) = -1$.

В качестве еще одного примера вычислим символ Лежандра $\left(\frac{15}{17}\right)$, используя разложение на множители:

$\left(\frac{15}{17}\right) = \left(\frac{3 \cdot 5}{17}\right)$ = (по формуле (1.72)) =

= $\left(\frac{3}{17}\right) \cdot \left(\frac{5}{17}\right)$ = (для первого сомножителя по формуле (1.70), $q = 3 \in K_2$, $p = 17 \in K_1$) =

= $\left(\frac{17}{3}\right) \cdot \left(\frac{5}{17}\right)$ = (для второго сомножителя по формуле (1.70), $q = 5 \in K_1$, $p = 17 \in K_1$) =

= $\left(\frac{17}{3}\right) \cdot \left(\frac{17}{5}\right)$ = (для первого и второго сомножителя по формуле (1.71)) =

= $\left(\frac{17 \pmod 3}{3}\right) \cdot \left(\frac{17 \pmod 5}{5}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right)$ = (по формуле (1.73)) =

= $(-1)^{(3^2-1)/8} \cdot (-1)^{(5^2-1)/8} = (-1)^{(9-1)/8} \cdot (-1)^{(25-1)/8}$ =

= $(-1)^{8/8} \cdot (-1)^{24/8} = (-1)^1 \cdot (-1)^3 = (-1)^4 = 1 = +1$.

Заметим, что немного позже рассмотрим более эффективный алгоритм вычисления значения символа Лежандра, который не зависит от возможности разложения числа на множители, а пока изучим задачу извлечения квадратного корня из квадратичного вычета a по модулю p. Данная задача может быть решена по алгоритму Шэнкса, представленного ниже словесно по шагам.

Шаг 1. Выбрать наугад такое число n, что

$$\left(\frac{n}{p}\right) = -1.$$

Шаг 2. Подобрать e, q – целые числа с нечетным q, удовлетворяющие соотношению

$$p - 1 = 2^e q.$$

Шаг 3. Положить $y = n^q \pmod p$, $r = e$, $x = a^{(q-1)/2} \pmod p$.

Шаг 4. Положить $b = a \cdot x^2 \pmod p$, $x = a \cdot x \pmod p$.

Шаг 5. Пока $b \neq 1 \pmod p$:

– найти наименьшее число m, такое что $b^{2^m} = 1 \pmod p$;

– положить $t = y^{2^{r-m-1}} \pmod p$, $y = t^2 \pmod p$, $r = m$;

– положить $x = x \cdot t \pmod p$, $b = b \cdot y \pmod p$.

Шаг 6. Вывести x. ■

Пример (1) применения алгоритма Шэнкса для вычисления корня из квадратичного вычета $a = 1$ по модулю $p = 7$.

Шаг 1. Выберем наугад такое число n, что

$$\left(\frac{n}{p}\right) = -1 = \left(\frac{3}{7}\right), \Rightarrow n = 3.$$

Шаг 2. Пусть e, q – целые числа с нечетным q, удовлетворяющие соотношению

$$(p - 1 = 2^e q) = (7 - 1 = 2^e q) = (6 = 2^e q) = (6 = 2^1 \cdot 3) \Rightarrow e = 1, q = 3.$$

Шаг 3. Положим

$$y = n^q \pmod p = 3^3 \pmod 7 = 9 \pmod 7 = 2 \pmod 7,$$
$$r = e = 1,$$
$$x = a^{(q-1)/2} \pmod p = 1^{(3-1)/2} \pmod 7 = 1^1 \pmod 7 = 1 \pmod 7.$$

Шаг 4. Положим

$$b = a \cdot x^2 \pmod p = 1 \cdot 1^2 \pmod 7 = 1 \cdot 1 \pmod 7 = 1 \pmod 7,$$
$$x = a \cdot x \pmod p = 1 \cdot 1 \pmod 7 = 1 \pmod 7.$$

Шаг 5. Пока ($b \neq 1 \pmod p$) = ($1 \neq 1 \pmod 7$) = ложь:

– найти наименьшее число m, такое что $b^{2^m} = 1 \pmod p$;

– положить $t = y^{2^{r-m-1}} \pmod p$, $y = t^2 \pmod p$, $r = m$;

– положить $x = x \cdot t \pmod p$, $b = b \cdot y \pmod p$.

Шаг 6. Выведем $x = 1$.

Таким образом, применение алгоритма Шэнкса для вычисления корня x из квадратичного вычета $a = 1$ по модулю $p = 7$ при выборе $n = 3$ дает $x = 1$.

Пример (2) вычисления корня из квадратичного вычета $a = 2$ по модулю $p = 7$.

Шаг 1. Выберем наугад такое число n, что

$$\left(\frac{n}{p}\right) = -1 = \left(\frac{3}{7}\right) \Rightarrow n = 3.$$

Шаг 2. Пусть e, q – целые числа с нечетным q, удовлетворяющие соотношению

$$(p - 1 = 2^e q) = (7 - 1 = 2^e q) = (6 = 2^e q) = (6 = 2^1 \cdot 3) \Rightarrow e = 1, q = 3.$$

Шаг 3. Положим

$$y = n^q \pmod p = 3^3 \pmod 7 = 9 \pmod 7 = 2 \pmod 7,$$
$$r = e = 1,$$
$$x = a^{(q-1)/2} \pmod p = 2^{(3-1)/2} \pmod 7 = 2^1 \pmod 7 = 2 \pmod 7.$$

Шаг 4. Положим

$$b = a \cdot x^2 \pmod p = 2 \cdot 2^2 \pmod 7 = 8 \pmod 7 = 1 \pmod 7,$$
$$x = a \cdot x \pmod p = 2 \cdot 2 \pmod 7 = 4 \pmod 7.$$

Шаг 5. Пока ($b \neq 1 \pmod p$) = ($1 \neq 1 \pmod 7$) = ложь:

– найти наименьшее число m, такое, что $b^{2^m} = 1 \pmod p$;

– положить $t = y^{2^{r-m-1}} \pmod p$, $y = t^2 \pmod p$, $r = m$;

– положить $x = x \cdot t \pmod p$, $b = b \cdot y \pmod p$.

Шаг 6. Выведем $x = 4$.

Таким образом, применение алгоритма Шэнкса для вычисления корня x из квадратичного вычета $a = 2$ по модулю $p = 7$ при выборе $n = 3$ дает $x = 4$.

Пример (3) вычисления корня из квадратичного вычета $a = 4$ по модулю $p = 7$.

Шаг 1. Выберем наугад такое число n, что

$$\left(\frac{n}{p}\right) = -1 = \left(\frac{3}{7}\right) \Rightarrow n = 3.$$

Шаг 2. Пусть e, q – целые числа с нечетным q, удовлетворяющие соотношению

$$(p - 1 = 2^e q) = (7 - 1 = 2^e q) = (6 = 2^e q) = (6 = 2^1 \cdot 3) \Rightarrow e = 1, q = 3.$$

Шаг 3. Положим

$$y = n^q \pmod p = 3^3 \pmod 7 = 9 \pmod 7 = 2 \pmod 7,$$
$$r = e = 1,$$
$$x = a^{(q-1)/2} \pmod p = 4^{(3-1)/2} \pmod 7 = 4^1 \pmod 7 = 4 \pmod 7.$$

Шаг 4. Положим

$$b = a \cdot x^2 \pmod p = 4 \cdot 4^2 \pmod 7 = 4 \cdot 16 \pmod 7 = 4 \cdot 2 \pmod 7 = 8 \pmod 7 = 1 \pmod 7,$$
$$x = a \cdot x \pmod p = 4 \cdot 4 \pmod 7 = 16 \pmod 7 = 2 \pmod 7.$$

Шаг 5. Пока $(b \neq 1 \pmod p) = (1 \neq 1 \pmod 7)$ = ложь:

– найти наименьшее число m, такое, что $b^{2^m} = 1 \pmod p$;

– положить $t = y^{2^{r-m-1}} \pmod p$, $y = t^2 \pmod p$, $r = m$;

– положить $x = x \cdot t \pmod p$, $b = b \cdot y \pmod p$.

Шаг 6. Выведем $x = 2$.

Таким образом, применение алгоритма Шэнкса для вычисления корня x из квадратичного вычета $a = 4$ по модулю $p = 7$ при выборе $n = 3$ дает $x = 2$.

Заметим, что если $p = 3 \pmod 4$, то для извлечения корня из a можно использовать формулу

$$x = a^{(p+1)/4} \pmod p, \qquad (1.74)$$

которая имеет неоспоримое преимущество перед общим алгоритмом Шэнкса ввиду ее явности и эффективности. Формула дает правильный ответ, потому что:

$$x^2 = (a^{(p+1)/4} (\mathrm{mod}\, p))^2 = a^{(p+1)/2} (\mathrm{mod}\, p) = a^{p/2+1/2} (\mathrm{mod}\, p) =$$

$$= a^{p/2-1/2+1} (\mathrm{mod}\, p) = a^{p/2-1/2} \cdot a \,(\mathrm{mod}\, p) = a^{(p-1)/2} \cdot a \,(\mathrm{mod}\, p) = \text{(по формуле (1.68))} =$$

$$= \left(\frac{a}{p}\right) \cdot a \,(\mathrm{mod}\, p) = a \,(\mathrm{mod}\, p).$$

В этой цепочке равенств последнее равенство верно ввиду предположения о том, что a – квадратичный вычет, а, следовательно, значение соответствующего символа Лежандра $\left(\frac{a}{p}\right)$ равно +1.

Например, вычислим по формуле (1.74) корни x из квадратичных вычетов a = 1, 2, 4 по модулю p = 7, которую можно применить, поскольку $p = 7 \,(\mathrm{mod}\, 4) = 3 \,(\mathrm{mod}\, 4)$:

$$x = a^{(p+1)/4} (\mathrm{mod}\, p) = 1^{(7+1)/4} (\mathrm{mod} 7) = 1^2 (\mathrm{mod} 7) = 1 \,(\mathrm{mod} 7),$$

$$x = a^{(p+1)/4} (\mathrm{mod}\, p) = 2^{(7+1)/4} (\mathrm{mod} 7) = 2^2 (\mathrm{mod} 7) = 4 \,(\mathrm{mod} 7),$$

$$x = a^{(p+1)/4} (\mathrm{mod}\, p) = 4^{(7+1)/4} (\mathrm{mod} 7) = 4^2 (\mathrm{mod} 7) = 16 \,(\mathrm{mod} 7) = 2 \,(\mathrm{mod} 7).$$

1.4.2. СИМВОЛ ЯКОБИ

Символ Лежандра $\left(\frac{a}{p}\right)$ в предыдущем пункте был введен для простого числа p. Если знаменатель в этой дроби будет не простым числом p, а составным числом n, то получим *символ Якоби* $\left(\frac{a}{n}\right)$, обобщающий символ Лежандра. Пусть n – нечетное число, большее, чем 2, и

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}.$$

Тогда символ Якоби определяется через символы Лежандра простых делителей $p_1, p_2, \ldots, p_k$ числа n следующим образом:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{e_k}. \qquad (1.75)$$

Пусть, например, $a = 217$ и $n = 221 = 13^1 \cdot 17^1$. Тогда символ Якоби $\left(\frac{217}{221}\right)$ можно вычислить по формуле (1.75), в которой $k = 2$, $p_1 = 13$, $p_2 = 17$, $e_1 = 1$, $e_2 = 1$:

$$\left(\frac{217}{221}\right) = \left(\frac{217}{13}\right)^1 \cdot \left(\frac{217}{17}\right)^1 = \left(\frac{217}{13}\right) \cdot \left(\frac{217}{17}\right) = 1 \cdot 1 = 1 = +1.$$

Здесь символы Лежандра $\left(\frac{217}{13}\right) = +1$ и $\left(\frac{217}{17}\right) = +1$ были вычислены предварительно:

$\left(\frac{217}{13}\right)$ = (по формуле (1.71)) =

$= \left(\frac{217\,(\mathrm{mod}13)}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{3 \cdot 3}{13}\right)$ = (по формуле (1.72)) =

$= \left(\frac{3}{13}\right) \cdot \left(\frac{3}{13}\right)$ = (по формуле (1.70), $q = 3 \in K_2$, $p = 13 \in K_1$) =

$= \left(\frac{13}{3}\right) \cdot \left(\frac{13}{3}\right)$ = (по формуле (1.71)) =

$= \left(\frac{13\,(\mathrm{mod}\,3)}{3}\right) \cdot \left(\frac{13\,(\mathrm{mod}\,3)}{3}\right) = \left(\frac{1}{3}\right) \cdot \left(\frac{1}{3}\right)$ = (по формуле (1.68), единица в любой степени равна единице) =

$= 1^{(3-1)/2} \pmod 7 \cdot 1^{(3-1)/2} \pmod 7 = 1 \pmod 7 \cdot 1 \pmod 7 = 1 \cdot 1 = 1 = +1;$

$\left(\frac{217}{17}\right)$ = (по формуле (1.71)) =

$= \left(\frac{217\,(\mathrm{mod}17)}{17}\right) = \left(\frac{13}{17}\right)$ = (по формуле (1.70), $q = 13 \in K_1$, $p = 17 \in K_1$) =

$= \left(\frac{17}{13}\right)$ = (по формуле (1.71)) =

$= \left(\frac{17\,(\mathrm{mod}13)}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2 \cdot 2}{13}\right)$ = (по формуле (1.72)) =

$= \left(\frac{2}{13}\right) \cdot \left(\frac{2}{13}\right)$ = (по формуле (1.73), единица в квадрате и (–1) в квадрате равна 1) =

$= 1 = +1.$

Заметим, что символ Якоби можно вычислять так же, как и символ Лежандра, опираясь на тождество, выведенное из закона квадратичной взаимности:

$$\left(\frac{a}{n}\right)=\left(\frac{2}{n}\right)^{e}\cdot\left(\frac{n\,(\mathrm{mod}a_1)}{a_1}\right)(-1)^{(a_1-1)(n-1)/4}, \tag{1.76}$$

где $a = 2^e a_1$, причем a_1 – нечетное число. Кроме того, полезно знать еще несколько формул, справедливых при нечетном n:

$$\left(\frac{1}{n}\right) = 1, \tag{1.77}$$

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}, \tag{1.78}$$

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}. \tag{1.79}$$

Формулы (1.76) – (1.79) обеспечивают быстрый процесс вычисления значения символа Якоби $\left(\frac{a}{n}\right)$ и, соответственно, символа Лежандра $\left(\frac{a}{p}\right)$ (как его частный случай) без трудоемкого разложения целого числа на множители. Единственное, что при этом нужно сделать, это выделить из a максимальную степень числа 2.

Пусть, например, необходимо вычислить значение символа Якоби $\left(\frac{96}{221}\right)$. В нем значение $a = 96$ и n – нечетное. Выделим из значения $a = 96$ максимальную степень двойки: $a = 96 = 2^5 \cdot 3$. Следовательно, в формуле (1.76) значение $e = 5$, $a_1 = 3$:

$\left(\frac{96}{221}\right)$ = (по формуле (1.76)) =

$$= \left(\frac{2}{221}\right)^5\cdot\left(\frac{221\,(\mathrm{mod}3)}{3}\right)(-1)^{(3-1)(221-1)/4} = \left(\frac{2}{221}\right)^5\cdot\left(\frac{2\,(\mathrm{mod}3)}{3}\right)(-1)^{110} =$$

$$= \left(\frac{2}{221}\right)^5\cdot\left(\frac{2\,(\mathrm{mod}3)}{3}\right) = \text{(по формуле (1.78))} =$$

$$= \left((-1)^{(221^2-1)/8}\right)^5\cdot\left((-1)^{(3^2-1)/8}\right) = \left((-1)^{(48841-1)/8}\right)^5\cdot\left((-1)^{(9-1)/8}\right) =$$

$$= \left((-1)^{48840/8}\right)^5\cdot\left((-1)^{8/8}\right) = \left((-1)^{6105}\right)^5\cdot\left((-1)^1\right) = (-1)^5\cdot(-1) = (-1)\cdot(-1) = 1 = +1.$$

Определим значения символа Лежандра $\left(\frac{a}{p}\right)$ для $a \neq 0$ в случае, когда $p = 7$, как частного случая символа Якоби $\left(\frac{a}{n}\right)$ с использованием формул (1.76) – (1.79):

$\left(\frac{1}{7}\right)$ = (по формуле (1.77)) = 1 = +1;

$\left(\frac{2}{7}\right)$ = (по формуле (1.78)) =

$= (-1)^{(7^2-1)/8} = (-1)^{(49-1)/8} = (-1)^{48/8} = (-1)^6 = 1 = +1;$

$\left(\frac{3}{7}\right)$ = (по формуле (1.76), $e = 0$, $a_1 = a = 3$) =

$= \left(\frac{2}{7}\right)^0 \cdot \left(\frac{7 \,(\mathrm{mod}\, 3)}{3}\right)(-1)^{(3-1)(7-1)/4} = \left(\frac{1}{3}\right)(-1)^{(2\cdot 6)/4}$ = (по формуле (1.77)) =

$= (-1)^{(2\cdot 6)/4} = (-1)^3 = -1.$

$\left(\frac{4}{7}\right)$ = (по формуле (1.76), $e = 2$, $a_1 = 1$) =

$= \left(\frac{2}{7}\right)^2 \cdot \left(\frac{1}{7}\right)$ = (как ранее было вычислено, $\left(\frac{2}{7}\right) = 1$) =

$= \left(\frac{1}{7}\right)$ = (по формуле (1.77)) = 1 = +1;

$\left(\frac{5}{7}\right)$ = (по формуле (1.76), $e = 0$, $a_1 = a = 5$) =

$= \left(\frac{5}{7}\right)^0 \cdot \left(\frac{7 \,(\mathrm{mod}\, 5)}{5}\right)(-1)^{(5-1)(7-1)/4} = \left(\frac{2}{5}\right)(-1)^{(4\cdot 6)/4} = \left(\frac{2}{5}\right)(-1)^6 = \left(\frac{2}{5}\right) =$

= (по формуле (1.78)) = $(-1)^{(5^2-1)/8} = (-1)^3 = -1;$

$\left(\frac{6}{7}\right)$ = (по формуле (1.76), $e = 1$, $a_1 = 3$) =

$= \left(\frac{2}{7}\right)^1 \cdot \left(\frac{7 \,(\mathrm{mod}\, 3)}{3}\right)(-1)^{(3-1)(7-1)/4} = \left(\frac{2}{7}\right) \cdot \left(\frac{1}{3}\right)(-1)^3 = \left(\frac{2}{7}\right) \cdot \left(\frac{1}{3}\right)(-1)$ = (по формуле (1.77)) =

$= \left(\frac{2}{7}\right)(-1)$ = (по формуле (1.78) =

$= (-1)^{(7^2-1)/8}(-1) = (-1)^{(49-1)/8}(-1) = (-1)^{48/8}(-1) = (-1)^7 = -1.$

Рассмотрим алгоритм вычисления значения символа Якоби (и, соответственно, символа Лежандра как его частный случай), который использует свойство символа Якоби – квадратичный закон взаимности. Благодаря использованию этого свойства данный алгоритм похож на алгоритм Евклида нахождения наибольшего общего делителя двух чисел, в котором также аргументы на каждом шаге меняются местами. Аналогично алгоритму Евклида, при перестановке аргументов больший из аргументов заменяется на остаток от деления большего на меньший аргумент. Это возможно благодаря свойству периодичности символа Якоби. Однако, поскольку символ Якоби определен только при условии нечетности второго аргумента, то до осуществления перестановки выделяется четная часть первого аргумента.

Формально входными данными являются: целое число a и натуральное, нечетное, большее единицы число b, а выходными данными – значение символа Якоби $\left(\frac{a}{b}\right)$.

Опишем алгоритм словесно по шагам.

Шаг 1 (*Проверка взаимной простоты*). Если НОД ($|a|$, b) $\neq 1$, то выйти из алгоритма со значением 0.

Шаг 2 (*Инициализация*). Положить $r = 1$.

Шаг 3 (*Переход к положительным числам*).

Если $a < 0$, то положить $a = -a$ и если $b \bmod 4 = 3$, то положить $r = -r$; в противном случае перейти к следующему шагу.

Шаг 4 (*Избавление от четности*).

Положить $t = 0$.

Пока a является четным числом:

– увеличить t на 1;

– уменьшить a в два раза.

Если t является нечетным числом и если $b \pmod 8$ равно 3 или равно 5, то положить $r = -r$; в противном случае перейти к следующему шагу.

Шаг 5 (*Квадратичный закон взаимности*).

Если $a \pmod 4 = b \pmod 4 = 3$, то положить $r = -r$.

Положить $c = a$.

Положить $a = b \pmod c$.

Положить $b = c$.

Шаг 6 (*Выход из алгоритма*?). Если $a \neq 0$, то вернуться к шагу 4; иначе выйти из алгоритма со значением r. ■

Заметим, что в алгоритме везде берется наименьший положительный вычет (остаток от деления). На четвертом шаге используется мультипликативность символа Якоби, а затем вычисляется значение символа Якоби $\left(\frac{2}{b}\right)$ как $(-1)^{\frac{b^2-1}{8}}$. Для того, чтобы избежать лишнего возведения в степень, проверяется остаток от деления b на 8. На пятом шаге тоже вместо возведения в степень используется проверка остатков от деления. Сложность алгоритма равна $O(\log a \cdot \log b)$ битовых операций.

Рассмотрим, например, процесс вычисления значения символа Лежандра $\left(\frac{219}{383}\right)$ с помощью символа Якоби по представленному алгоритму.

Входные данные: $a = 219$ – целое число, $b = 383$ – натуральное, нечетное, большее единицы число.

Выходные данные: $\left(\frac{a}{b}\right) = \left(\frac{219}{383}\right)$ – символ Якоби.

Шаг 1 (*Проверка взаимной простоты*).

НОД (a, b) = НОД (219, 383) = 1. Переход к следующему шагу.

Шаг 2 (*Инициализация*). Положим $r = 1$.

Шаг 3 (*Переход к положительным числам*).

($a < 0$) = (219 < 0) = ложь.

Шаг 4 (*Избавление от четности*).

Положим $t = 0$.

(a – четное) = (219 – четное) = ложь.

(t – нечетное) = (0 – нечетное) = ложь.

Шаг 5 (*Квадратичный закон взаимности*).

($a \pmod 4 = b \pmod 4 = 3$) = ($219 \pmod 4 = 383 \pmod 4 = 3$) = (3 = 3 = 3) = истина. Положим $r = -r = -1$.

Положим $c = a = 219$.

Положим $a = b \pmod c = 383 \pmod{219} = 164$.

Положим $b = c = 219$.

$(\left(\frac{219}{383}\right) \rightarrow -\left(\frac{164}{219}\right))$.

Шаг 6 (*Выход из алгоритма?*).

$(a \neq 0) = (164 \neq 0)$ = истина. Возврат к шагу 4.

Шаг 4 (*Избавление от четности*).

Положим $t = 0$.

(a – четное) = (164 – четное) = истина.

Положим $t = t + 1 = 0 + 1 = 1$.

Положим $a = a / 2 = 164 / 2 = 82$.

(a – четное) = (82 – четное) = истина.

Положим $t = t + 1 = 1 + 1 = 2$.

Положим $a = a / 2 = 82 / 2 = 41$.

(a – четное) = (41 – четное) = ложь.

(t – нечетное) = (2 – нечетное) = ложь.

Шаг 5 (*Квадратичный закон взаимности*).

($a \pmod 4 = b \pmod 4 = 3$) = ($41 \pmod 4 = 219 \pmod 4 = 3$) = ($1 = 3 = 3$) = ложь.

Положим $c = a = 41$.

Положим $a = b \pmod c = 219 \pmod{41} = 14$.

Положим $b = c = 41$.

$(-\left(\frac{164}{219}\right) \rightarrow -\left(\frac{14}{41}\right))$.

Шаг 6 (*Выход из алгоритма?*).

$(a \neq 0) = (14 \neq 0)$ = истина. Возврат к шагу 4.

Шаг 4 (*Избавление от четности*).

Положим $t = 0$.

(a – четное) = (14 – четное) = истина.

Положим $t = t + 1 = 0 + 1 = 1$.

Положим $a = a / 2 = 14 / 2 = 7$.

(a – четное) = (7 – четное) = ложь.

(t – нечетное) = (1 – нечетное) = истина.

($b \pmod 8 = 3$ или 5) = ($41 \pmod 8 = 3$ или 5) = ($1 = 3$ или 5) = ложь.

Шаг 5 (*Квадратичный закон взаимности*).

(a (mod 4) = b (mod 4) = 3) = (7 (mod 4) = 41 (mod 4) = 3) = (3 = 1 = 3) = ложь.

Положим $c = a = 7$.

Положим $a = b$ (mod c) = 41 (mod 7) = 6;

Положим $b = c = 7$.

$(-\left(\frac{14}{41}\right) \rightarrow -\left(\frac{6}{7}\right))$.

Шаг 6 (*Выход из алгоритма?*).

($a \neq 0$) = ($6 \neq 0$) = истина. Возврат к шагу 4.

Шаг 4 (*Избавление от четности*).

Положим $t = 0$.

(a – четное) = (6 – четное) = истина.

Положим $t = t + 1 = 0 + 1 = 1$.

Положим $a = a / 2 = 6 / 2 = 3$.

(a – четное) = (3 – четное) = ложь.

(t – нечетное) = (1 – нечетное) = истина.

(b (mod 8) = 3 или 5) = (7 (mod 8) = 3 или 5) = (7 = 3 или 5) = ложь.

Шаг 5 (*Квадратичный закон взаимности*).

(a (mod 4) = b (mod 4) = 3) = (3 (mod 4) = 7 (mod 4) = 3) = (3 = 3 = 3) = истина.

Положим $r = -r = -(-1) = 1$.

Положим $c = a = 3$.

Положим $a = b$ (mod c) = 7 (mod 3) = 1.

Положим $b = c = 3$.

$(-\left(\frac{6}{7}\right) \rightarrow \left(\frac{1}{3}\right))$.

Шаг 6 (*Выход из алгоритма?*).

($a \neq 0$) = ($1 \neq 0$) = истина. Возврат к шагу 4.

Шаг 4 (*Избавление от четности*).

Положим $t = 0$.

(a – четное) = (1 – четное) = ложь.

(t – нечетное) = (0 – нечетное) = ложь.

Шаг 5 (*Квадратичный закон взаимности*).

(a (mod 4) = b (mod 4) = 3) = (1 (mod 4) = 3 (mod 4) = 3) = (1 = 3 = 3) = ложь.

Положим $c = a = 1$.

Положим $a = b$ (mod c) = 3 (mod 1) = 0.

Положим $b = c = 1$.

$(\left(\frac{1}{3}\right) \rightarrow \left(\frac{0}{1}\right))$.

Шаг 6 (*Выход из алгоритма?*).

($a \neq 0$) = ($0 \neq 0$) = ложь. Выход из алгоритма со значением $r = 1$.

Разработанная программа *sJacobi* на языке Си, которая реализует алгоритм вычисления значения символа Якоби (и, соответственно, символа Лежандра как его частный случай), использующий свойство символа Якоби – квадратичный закон взаимности, приведена на листинге 1.1.

Листинг 1.1. Программа, реализующая алгоритм вычисления значения символа Якоби (и, соответственно, символа Лежандра как его частный случай), который использует свойство символа Якоби – квадратичный закон взаимности:

```
#include <stdio.h> // Описания функций стандартного ввода-вывода
#include <stdlib.h> // Описания стандартных функций
#include <conio.h> // Описания функций консольного ввода-вывода
#include <math.h> // Описания стандартных математических функций
int main()
{
 int a, // Первый аргумент символа Якоби
 b, // Второй аргумент символа Якоби
 r, // Значение символа Якоби
 t,
 c;
 // Прототип функции NOD (наибольший общий делитель)
 int NOD(int m, int n);
 printf("Введите целое число a\n");
 scanf("%d", &a);
 L:printf("Введите натуральное, нечетное, большее 1 число b:\n");
 scanf("%d", &b);
 if(b<=1 || b%2==0) goto L;
```

```
// Шаг 1. Проверка взаимной простоты
if(a==0)
{
printf("(%d/%d)=0\n", a,b);
getch();
return 0;
}
else
if (NOD(abs(a),b)!=1)
{
printf("(%d/%d)=0\n", a,b);
getch();
return 0;
}
printf("(%d/%d)=", a,b);
// Шаг 2. Инициализация
r=+1;
// Шаг 3. Переход к положительным числам
if (a<0)
{
a=-a;
if (b%4==3) r=-r;
}
// Шаг 4. Избавление от четности
L4:t=0;
while(a%2==0)
{
t=t+1; a=a/2;
}
if(t%2!=0)
if(b%8==3 || b%8==5)
r=-r;
// Шаг 5. Квадратичный закон взаимности
if(a%4==3 && b%4==3)
r=-r;
c=a; a=b%c; b=c;
// Шаг 6. Выход из алгоритма?
```

```
 if(a!=0)
 goto L4;
 else
 {
 printf("%+d\n", r);
 getch();
 return 0;
 }
}
// Представление функции NOD (наибольший общий делитель)
int NOD(int m, int n)
{
 while(m!=n)
 {
 if(m>n)
 m=m-n;
 else
 n=n-m;
 }
 return m;
}
```

Напомним, что значение символа Лежандра $\left(\frac{a}{p}\right)$ говорит о том, является ли a полным квадратом по модулю простого числа p (можно извлечь квадратный корень из a по модулю простого числа p) или нет. Символ же Якоби $\left(\frac{a}{n}\right)$ не определяет возможность извлечения квадратного корня из a по модулю составного числа n. Если a действительно является квадратом по модулю n, то символ Якоби будет равен +1. Но из равенства $\left(\frac{a}{n}\right) = +1$ вовсе не следует, что a является полным квадратом по модулю n.

Разработанная программа *square* на языке Си, которая проверяет существование квадратного корня из a по модулю простого числа p или по модулю составного числа n, приведена на листинге 1.2.

Листинг 1.2. Программа проверки существования квадратного корня из a по модулю простого числа p или по модулю составного числа n:

```
#include <stdio.h> // Описания функций стандартного ввода-вывода
int main()
{
 long a0; // Изначальный числитель символа Лежандра или Якоби
 long a; // Нормализованный числитель символа Лежандра или Якоби
 long z; // Знаменатель символа Лежандра или Якоби (p или n)
 long y; // Значение символа Лежандра или Якоби
 int i; // Претендент на квадратный корень из a
 long square_i; // Квадрат претендента на квадратный корень из a
 printf("Числитель символа Лежандра или Якоби: ");
 scanf("%ld",&a0);
 printf("a0 = %ld\n",a0);
 printf("Знаменатель символа Лежандра или Якоби: ");
 scanf("%ld",&z);
 printf("z = %ld\n",z);

 // Нормализация числителя символа Лежандра или Якоби
 a=a0;
 while(a<0)
 {
 a+=z;
 }
 while(a>=z)
 {
 a-=z;
 }
 printf("Числитель символа Лежандра или Якоби после нормали-
зации) = %ld\n",a);

 // Проверка существования квадратного корня из a по модулю z
 if (a==0)
 {
 printf("(%ld/%ld) = 0\n",a0,z);
 return 0;
 }
 else
 {
```

```
i=1;
do
{
square_i=i*i;
while(square_i>z)
{
square_i-=z;
}
i++;
} while ((square_i != a) && (i < z));
if (i != z)
{
printf("(%ld/%ld) = +1\n",a0,z);
}
else
{
printf("(%ld/%ld) = -1\n",a0,z);
}
}
return 0;
}
```

Результаты использования программ *square* и *sJacobi* для установления соответствия отмеченным выше особенностям символа Лежандра $\left(\frac{a}{p}\right)$ и символа Якоби $\left(\frac{a}{n}\right)$ по характеризации возможности извлечения квадратного корня из a по модулю простого числа p или по модулю составного числа n, приведены в табл. 1.68. В ее третьем столбце для символа Лежандра $\left(\frac{a}{p}\right)$ или символа Якоби $\left(\frac{a}{n}\right)$ выставлено полученное по программе *square*: значение 0, если a делится соответственно на p или на n; значение +1, если существует квадратный корень из a соответственно по модулю p или n; значение минус 1, если квадратный корень из a соответственно по модулю p или n не существует. В четвертом и пятом столбцах выставлены значения символов Лежандра $\left(\frac{a}{p}\right)$ или символов Якоби $\left(\frac{a}{n}\right)$, полученные соответственно по расчетным формулам и по программе *sJacobi*.

Таблица 1.68

Символ Лежандра $\left(\frac{a}{p}\right)$	Символ Якоби $\left(\frac{a}{n}\right)$	Существование корня из a по модулю p или n по программе *square*	Значение символа Лежандра или символа Якоби, полученное	
			по расчетным формулам	по программе *sJacobi*
(0/7)		0	0	0
(1/7)		+1	+1	+1
(2/7)		+1	+1	+1
(3/7)		–1	–1	–1
(4/7)		+1	+1	+1
(5/7)		–1	–1	–1
(6/7)		–1	–1	–1
(7/3)		+1	+1	+1
(2/5)		–1	–1	–1
(2/13)		–1	–1	–1
(11/3)		–1	–1	–1
(3/11)		+1	+1	+1
(11/5)		+1	+1	+1
(5/11)		+1	+1	+1
(15/11)		+1	+1	+1
(–1/7)		–1	–1	–1
(15/17)		+1	+1	+1
	(217/221)	+1	+1	+1
(217/13)		+1	+1	+1
(3/13)		+1	+1	+1
(217/17)		+1	+1	+1
	(96/221)	–1	+1	+1
(96/13)		–1	–1	–1
(96/17)		–1	–1	–1
	(219/383)	+1	+1	+1

Заметим, что, во-первых, полученные значения в четвертом и пятом столбцах таблицы всегда совпадают, а это говорит об успешном испытании программы *sJacobi* на конечном наборе тестов, заданной этой таблицей. Во-вторых, полученные значения в третьем, четвертом и пятом столбцах таблицы всегда совпадают, за исключением четвертой снизу строку для символа Якоби $\left(\frac{96}{221}\right)$. Это как раз пример такого случая, когда символ Якоби $\left(\frac{a}{n}\right)$ не определяет возможность извлечения квадратного корня из a по модулю составного числа n.

Рассмотрим далее более системно вопрос о том, когда символ Якоби $\left(\frac{a}{n}\right)$ не определяет возможность извлечения квадратного корня из a по модулю числа n.

Пусть n – нечетное число, большее 3. Обозначим через Q_n подмножество полных квадратов в множестве $(\mathbf{Z}/N\mathbf{Z})^*$ – множестве обратимых в $\mathbf{Z}/N\mathbf{Z}$ элементов:

$$Q_n = \left\{ x^2 (\mathrm{mod} n) \mid x \in (\mathbf{Z}/n\mathbf{Z})^* \right\}. \tag{1.80}$$

Напомним, что $(\mathbf{Z}/N\mathbf{Z})^* = \{x \in \mathbf{Z}/N\mathbf{Z} \mid \text{НОД}\ (x, N) = 1\}$. Когда $N = p$ – простое число $(\mathbf{Z}/N\mathbf{Z})^* = (\mathbf{Z}/p\mathbf{Z})^* = \{1, \ldots, p - 1\}$. Например, для $N = 7$ множество $\mathbf{Z}/N\mathbf{Z} = \{0, 1, \ldots, 6\}$, а $(\mathbf{Z}/N\mathbf{Z})^* = \{1, 2, \ldots, 6\}$.

Нарастив таблицу квадратов по модулю $p = 7$ (см. табл. 1.64) столбцами для символа Якоби $\left(\frac{x}{7}\right)$ и корня из x, получим табл. 1.69.

Из этой таблицы видно, что при простом $n = 7$ по формуле (1.80) имеем:

$$Q_n = \left\{ x^2 (\mathrm{mod} n) \mid x \in (\mathbf{Z}/n\mathbf{Z})^* \right\} = Q_7 = \left\{ x^2 (\mathrm{mod} 7) \mid x \in \{1, 2, \cdots, 6\} \right\} = \{1, 2, 4\}.$$

Пусть при нечетном n, большем 3, J_n обозначает подмножество элементов в $(\mathbf{Z}/n\mathbf{Z})^*$, чей символ Якоби равен +1:

$$J_n = \left\{ x \in (\mathbf{Z}/n\mathbf{Z})^* \,\middle|\, \left(\frac{x}{n}\right) = 1 \right\}. \tag{1.81}$$

При простом $n = 7$ (см. табл. 1.69):

$$J_n = \left\{ x \in (\mathbf{Z}/n\mathbf{Z})^* \,\middle|\, \left(\frac{x}{n}\right) = 1 \right\} = J_7 = \left\{ x \in \{1, 2, \cdots, 6\} \,\middle|\, \left(\frac{x}{7}\right) = 1 \right\} = \{1, 2, 4\}.$$

Таблица 1.69

x	$x^2 \pmod 7 = a$	Символ Якоби $\left(\frac{x}{7}\right)$	$\sqrt{x}$
0	0	0	0
1	1	+1	1, 6
2	4	+1	3, 4
3	2	–1	–
4	2	+1	2, 5
5	4	–1	–
6	1	–1	–

Заметим, что в рассмотренном примере (при $n = 7$)

$$Q_7 = \left\{ x^2 (\mathrm{mod} 7) \mid x \in \{1, 2, \cdots, 6\} \right\} = \{1, 2, 4\} = \; J_7 = \left\{ \; x \in \{1, 2, \cdots, 6\} \mid \left(\frac{x}{7}\right) = 1 \right\} = \{1, 2, 4\}.$$

Это подтверждает то, что символ Якоби $\left(\frac{a}{n}\right)$ определяет возможность извлечения квадратного корня из a по простому модулю n.

Пусть теперь n будет составным числом.

Определим множества Q_n и J_n для составного числа $n = p \cdot q$ при $p = 3$ и $q = 5$, т.е. для составного числа $n = 3 \cdot 5 = 15$. В этом нам поможет табл. 1.70, в которой символ Якоби $\left(\frac{x}{15}\right)$ вычислен как произведение символов Лежандра $\left(\frac{x}{3}\right)$ и $\left(\frac{x}{5}\right)$, а также по программе *sJacobi*.

Из таблицы следует, что при составном $n = 15$:

$$Q_n = \left\{ x^2 (\mathrm{mod} n) \mid x \in (\mathbf{Z} / n\mathbf{Z})^* \right\} = \; Q_{15} = \left\{ x^2 (\mathrm{mod} 15) \mid x \in \{1, 2, \cdots, 14\} \right\} = \{1, 4, 6, 9, 10\},$$

$$J_n = \left\{ \; x \in (\mathbf{Z} / n\mathbf{Z})^* \middle| \left(\frac{x}{n}\right) = 1 \right\} \; = \; J_{15} = \left\{ \; x \in \{1, 2, \cdots, 14\} \mid \left(\frac{x}{15}\right) = 1 \right\} \; = \{1, 2, 4, 8\}.$$

Заметим, что множество всех псевдоквадратов, т.е. квадратичных невычетов, чей символ Якоби равен +1, представляет собой разность $J_n \setminus Q_n$. В нашем примере (при составном $n = 15$) множество всех псевдоквадратов $J_{15} \setminus Q_{15} = \{1, 2, 4, 8\} \setminus \{1, 4, 6, 9, 10\} = \{2, 8\}$.

Таблица 1.70

x	$x^2 \pmod{15}$	Символ Лежандра $\left(\frac{x}{3}\right)$	Символ Лежандра $\left(\frac{x}{5}\right)$	Символ Якоби $\left(\frac{x}{15}\right) = \left(\frac{x}{3}\right)\cdot\left(\frac{x}{5}\right)$	Символ Якоби $\left(\frac{x}{15}\right)$, рассчитанный по программе *sJacobi*	$\sqrt{x}$
0	0	0	0	0	0	0
1	1	+1	+1	+1	+1	1, 4, 11, 14
2	4	–1	–1	+1	+1	–
3	9	0	–1	0	0	–
4	1	+1	+1	+1	+1	2, 7, 8, 13
5	10	–1	0	0	0	–
6	6	0	+1	0	0	6, 9
7	4	+1	–1	–1	–1	–
8	4	–1	–1	+1	+1	–
9	6	0	+1	0	0	3, 12
10	10	+1	0	0	0	5, 10
11	1	–1	+1	–1	–1	–
12	9	0	–1	0	0	–
13	4	+1	–1	–1	–1	–
14	1	–1	+1	–1	–1	–

Рассмотрим еще один пример определения множества псевдоквадратов для составного числа $n = p \cdot q$, теперь при $p = 5$ и $q = 7$, т.е. для составного числа $n = 5 \cdot 7 = 35$.

В этом нам поможет аналогичная предыдущей таблице табл. 1.71.

Из таблицы следует, что при составном $n = 35$:

$$Q_n = \left\{ x^2 (\mathrm{mod} n) \mid x \in (\mathbf{Z}/n\mathbf{Z})^* \right\} = Q_{35} = \left\{ x^2 (\mathrm{mod} 35) \mid x \in \{1, 2, \cdots, 34\} \right\} =$$

$$= \{1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30\},$$

$$J_n = \left\{ x \in (\mathbf{Z}/n\mathbf{Z})^* \middle| \left(\frac{x}{n}\right) = 1 \right\} = J_{35} = \left\{ x \in \{1, 2, \cdots, 34\} \middle| \left(\frac{x}{35}\right) = 1 \right\} =$$

$$= \{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33\}.$$

Таблица 1.71

x	$x^2 \pmod{35}$	Символ Лежандра $\left(\frac{x}{5}\right)$	Символ Лежандра $\left(\frac{x}{7}\right)$	Символ Якоби $\left(\frac{x}{35}\right) = \left(\frac{x}{5}\right)\cdot\left(\frac{x}{7}\right)$	Символ Якоби $\left(\frac{x}{35}\right)$, рассчитанный по программе *sJacobi*	$\sqrt{x}$
0	0	0	0	0	0	0
1	1	+1	+1	+1	+1	1, 6, 29, 34
2	4	–1	+1	–1	–1	–
3	9	–1	–1	+1	+1	–
4	16	+1	+1	+1	+1	2, 12, 23, 33
5	25	0	–1	0	0	–
6	1	+1	–1	–1	–1	–
7	14	–1	0	0	0	–
8	29	–1	+1	–1	–1	–
9	11	+1	+1	+1	+1	3, 17, 18, 32
10	30	0	–1	0	0	–
11	16	+1	+1	+1	+1	9, 16, 19, 26
12	4	–1	–1	+1	+1	–
13	29	–1	–1	+1	+1	–
14	21	+1	0	0	0	7, 28
15	15	0	+1	0	0	15, 20
16	11	+1	+1	+1	+1	4, 11, 24, 31
17	9	–1	–1	+1	+1	–
18	9	–1	+1	–1	–1	–
19	11	+1	–1	–1	–1	–
20	15	0	–1	0	0	–
21	21	+1	0	0	0	14, 21
22	29	–1	+1	–1	–1	–
23	4	–1	+1	–1	–1	–
24	16	+1	–1	–1	–1	–

Продолжение табл. 1.71

x	$x^2 \pmod{35}$	Символ Лежандра $\left(\frac{x}{5}\right)$	Символ Лежандра $\left(\frac{x}{7}\right)$	Символ Якоби $\left(\frac{x}{35}\right) = \left(\frac{x}{5}\right) \cdot \left(\frac{x}{7}\right)$	Символ Якоби $\left(\frac{x}{35}\right)$, рассчитанный по программе *sJacobi*	$\sqrt{x}$
25	30	0	+1	0	0	5, 30
26	11	+1	–1	–1	–1	–
27	29	–1	–1	+1	+1	–
28	14	–1	0	0	0	–
29	1	+1	+1	+1	+1	8, 13, 22, 27
30	25	0	+1	0	0	10, 25
31	16	+1	–1	–1	–1	–
32	9	–1	+1	–1	–1	–
33	4	–1	–1	+1	+1	–
34	1	+1	–1	–1	–1	–

В этом примере (при составном $n = 35$) множество всех псевдоквадратов $J_{35} \setminus Q_{35}$ = = {1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33}\{1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30} = = {3, 12, 13, 17, 27, 33}.

Заметим, что криптографов интересуют именно эти два относительно простых случая, т.е. когда n является простым числом или произведением двух простых чисел.

Если n – простое число, то $Q_n = J_n$ и $\#Q_n = (n - 1)/2$. Заметим, что в рассмотренном ранее примере (при простом числе $n = 7$) $Q_7 = \left\{ x^2 (\mathrm{mod} 7) \mid x \in \{1, 2, \cdots, 6\} \right\} = \{1, 2, 4\} =$ $= J_7 = \left\{ x \in \{1, 2, \cdots, 6\} \mid \left(\frac{x}{7}\right) = 1 \right\} = \{1, 2, 4\}$ и $\#Q_n = \#Q_7 = 3 = (n - 1) / 2 = (7 - 1) / 2 =$ $= 6 / 2 = 3$.

Если n является произведением двух простых чисел p и q, то $\#(J_n \setminus Q_n) = (p - 1) \times$ $\times (q - 1) / 4)$. В рассмотренных ранее примерах (при составных $n = 15$ и $n = 35$):

$$Q_{15} = \left\{ x^2 (\mathrm{mod} 7) \mid x \in \{1, 2, \cdots, 6\} \right\} = \{1, 4, 6, 9, 10\},$$

$$J_{15} = \left\{ x \in \{1, 2, \cdots, 14\} \,\middle|\, \left(\frac{x}{15}\right) = 1 \right\} = \{1, 2, 4, 8\},$$

$$\#(J_n \setminus Q_n) = \#(J_{15} \setminus Q_{15}) = \#(\{1, 2, 4, 8\} \setminus \{1, 4, 6, 9, 10\}) = \#(\{2, 8\}) = 2 =$$
$$= (p - 1) \cdot (q - 1) / 4 = (3 - 1) \cdot (5 - 1) / 4 = 2 \cdot 4 / 4 = 2.$$

$$Q_{35} = \left\{ x^2 (\mathrm{mod} 35) \,|\, x \in \{1, 2, \cdots, 34\} \right\} = \{1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30\},$$

$$J_{35} = \left\{ x \in \{1, 2, \cdots, 34\} \,\middle|\, \left(\frac{x}{35}\right) = 1 \right\} = \{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33\},$$

$$\#(J_n \setminus Q_n) = \#(J_{35} \setminus Q_{35}) = \#(\{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33\} \setminus$$
$$\setminus \{1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30\}) = \#(\{3, 12, 13, 17, 27, 33\}) = 6 =$$
$$= (p - 1) \cdot (q - 1) / 4 = (5 - 1) \cdot (7 - 1)/4 = 4 \cdot 6 / 4 = 6.$$

1.4.3. ИЗВЛЕЧЕНИЕ КОРНЯ ПО МОДУЛЮ СОСТАВНОГО ЧИСЛА

Рассмотрим способ извлечения корня из числа a по модулю составного числа n, представляющего собой произведение простых чисел p и q.

Как было отмечено в предыдущем пункте, если число a действительно является полным квадратом по составному модулю $n = p \cdot q$, то символ Якоби $\left(\frac{a}{n}\right) = +1$. Кроме того, как следует из данных табл. 1.70, 1.71, если число a действительно является полным квадратом по составному модулю $n = p \cdot q$ и символ Якоби $\left(\frac{a}{n}\right) = +1$, то

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = +1. \qquad (1.82)$$

Для вычисления корня из a по модулю n сначала извлечем корень из a по модулю p и обозначим его через s_p. Затем извлечем корень из a по модулю q и обозначим его через s_q. И, наконец, для вычисления искомого корня из a по модулю n применим китайскую теорему об остатках к системе уравнений:

$$\begin{cases} x = s_p (\mathrm{mod}\, p), \\ x = s_q (\mathrm{mod} q). \end{cases} \qquad (1.83)$$

Пример 1 извлечения корня из a по модулю n. В нем вычислим корень из $a = 11$ по модулю $n = 35 = p \cdot q = 5 \cdot 7$.

Для определения всех корней из 11 по модулю 35 построим табл. 1.72.

Таблица 1.72

x	$x^2 \pmod{35}$
0	0
1	1
2	4
3	9
4	16
5	25
6	1
7	14
8	29
9	11
10	30
11	16
12	4
13	29
14	21
15	15
16	11
17	9
18	9
19	11
20	15
21	21
22	29
23	4
24	16
25	30

Продолжение табл. 1.72

x	$x^2 \pmod{35}$
26	11
27	29
28	14
29	1
30	25
31	16
32	9
33	4
34	1

Из данных этой таблицы квадратов по модулю 35 следует, что корнями из 11 по модулю 35 являются числа 9, 16, 19 и 26.

Вычислим все значения квадратного корня из 11 по модулю 35 в соответствии с рассмотренным выше способом, основанным на отмеченном свойстве символа Якоби (1.82) и применении китайской теоремы об остатках к системе уравнений (1.83).

Заметим, что число $a = 11$, действительно, является полным квадратом по модулю $n = 35 = p \cdot q = 5 \cdot 7$, поскольку

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = \left(\frac{11}{5}\right) = \left(\frac{11}{7}\right) = +1.$$

Сначала определим корень из $a = 11$ по модулю $p = 5$ с помощью построенной табл. 1.73 и обозначим его через $s_p = s_5$.

Из данных этой таблицы следует, что $\sqrt{11} \pmod{5} = 1$ или 4, поскольку $1^2 \pmod 5 = 4^2 \pmod 5 = 1 \pmod 5 = 6 \pmod 5 = 11 \pmod 5$. Таким образом, корнем из $a = 11$ по модулю $p = 5$ является $s_p = s_5 = 1$ или 4.

Затем определим корень из $a = 11$ по модулю $q = 7$ с помощью построенной табл. 1.74 и обозначим его через $s_q = s_7$.

Из данных этой таблицы следует, что $\sqrt{11} \pmod{7} = 2$ или 5, поскольку $2^2 \pmod 7 = 5^2 \pmod 7 = 4 \pmod 7 = 11 \pmod 7$. Таким образом, корнем из $a = 11$ по модулю $q = 7$ является $s_q = s_7 = 2$ или 5.

Таблица 1.73

x	$x^2 \pmod 5$
0	0
1	1 (mod 5) = 6 (mod 5) = 11 (mod 5)
2	4
3	4
4	1 (mod 5) = 6 (mod 5) = 11 (mod 5)

Таблица 1.74

x	$x^2 \pmod 7$
0	0
1	1
2	4 (mod 7) = 11 (mod 7)
3	2
4	2
5	4 (mod 7) = 11 (mod 7)
6	1

И, наконец, для вычисления искомого корня из $a = 11$ по модулю $n = 35 = p \cdot q = 5 \cdot 7$ применим китайскую теорему об остатках к системе уравнений (1.83):

$$\begin{cases} x = s_p \pmod p, \\ x = s_q \pmod q. \end{cases} = \begin{cases} x = s_5 \pmod 5, \\ x = s_7 \pmod 7. \end{cases}$$

Поскольку корень s_5 из 11 по модулю 5 принимает два значения (1 или 4) и корень s_7 из 11 по модулю 7 принимает два значения (2 или 5), для получения всех корней из 11 по модулю $5 \cdot 7 = 35$ с применением китайской теоремы об остатках необходимо решить четыре системы уравнений:

$$\begin{cases} x = 1 \pmod 5, \\ x = 2 \pmod 7. \end{cases} \quad (1.84)$$

$$\begin{cases} x = 1 \pmod 5, \\ x = 5 \pmod 7. \end{cases} \quad (1.85)$$

$$\begin{cases} x = 4\,(\mathrm{mod}5), \\ x = 2\,(\mathrm{mod}7). \end{cases} \tag{1.86}$$

$$\begin{cases} x = 4\,(\mathrm{mod}5), \\ x = 5\,(\mathrm{mod}7). \end{cases} \tag{1.87}$$

Из данных табл. 1.75 следует, что решением системы уравнений (1.84) является $x = 16\ (\mathrm{mod}\ 35)$.

Таблица 1.75

x (mod 35)	x (mod 5)	x (mod 7)
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	0	5
6	1	6
7	2	0
8	3	1
9	4	2
10	0	3
11	1	4
12	2	5
13	3	6
14	4	0
15	0	1
16	1	2
17	2	3
18	3	4
19	4	5
20	0	6
21	1	0
22	2	1

Продолжение табл. 1.75

$x \pmod{35}$	$x \pmod 5$	$x \pmod 7$
23	3	2
24	4	3
25	0	4
26	1	5
27	2	6
28	3	0
29	4	1
30	0	2
31	1	3
32	2	4
33	3	5
34	4	6

Решим эту же систему уравнений (1.84) аналитически.

Если $x = 2 \pmod 7$ и $x = 1 \pmod 5$, то путем ввода дополнительной переменной u получим:

$$x = 2 + 7 \cdot u \pmod 7 \text{ и } x = 1 \pmod 5.$$

Подставив выражение для x из первого уравнения $x = 2 + 7 \cdot u \pmod 7$ во второе $x = 1 \pmod 5$, получим:

$$2 + 7 \cdot u = 1 \pmod 5,$$

$$2 + 2 \cdot u = 1 \pmod 5,$$

$$2 \cdot u = -1 \pmod 5,$$

$$2 \cdot u = 4 \pmod 5.$$

Вспомним, что если НОД $(a, N) = 1$, то уравнение вида $a \cdot x = b \pmod N$ имеет решение, причем единственное. В нашем случае НОД $(2, 5) = 1$, вычислим единственный корень уравнения $2 \cdot u = 4 \pmod 5$:

$$2 \cdot u = 4 \pmod 5,$$

$$2 \cdot 2^{-1} \cdot u = 4 \cdot 2^{-1} \pmod 5,$$

$$u = 4 \cdot 3 \pmod 5 = 12 \pmod 5 = 2 \pmod 5.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 2 + 7 \cdot u$, получим решение системы уравнений (1.84) по модулю 35:

$$x = 2 + 7 \cdot u \pmod{35} = 2 + 7 \cdot 2 = 16 \pmod{35}.$$

Из данных табл. 1.76 видно, что решением второй из четырех систем уравнений, системы (1.85) является $x = 26 \pmod{35}$.

Таблица 1.76

$x \pmod{35}$	$x \pmod 5$	$x \pmod 7$
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	0	5
6	1	6
7	2	0
8	3	1
9	4	2
10	0	3
11	1	4
12	2	5
13	3	6
14	4	0
15	0	1
16	1	2
17	2	3
18	3	4
19	4	5
20	0	6
21	1	0
22	2	1

Продолжение табл. 1.76

x (mod 35)	x (mod 5)	x (mod 7)
23	3	2
24	4	3
25	0	4
26	1	5
27	2	6
28	3	0
29	4	1
30	0	2
31	1	3
32	2	4
33	3	5
34	4	6

Решим эту же систему уравнений (1.85) аналитически.

Если $x = 5 \pmod 7$ и $x = 1 \pmod 5$, то путем ввода дополнительной переменной u получим:

$$x = 5 + 7 \cdot u \pmod 7 \text{ и } x = 1 \pmod 5.$$

Подставив выражение для x из первого уравнения $x = 5 + 7 \cdot u \pmod 7$ во второе $x = 1 \pmod 5$, получим:

$$5 + 7 \cdot u = 1 \pmod 5,$$

$$0 + 2 \cdot u = 1 \pmod 5,$$

$$2 \cdot u = 1 \pmod 5.$$

Заметим, что если НОД $(a, N) = 1$, то уравнение вида $a \cdot x = b \pmod N$ имеет решение, причем единственное. В нашем случае НОД $(2, 5) = 1$, вычислим единственный корень уравнения $2 \cdot u = 1 \pmod 5$:

$$2 \cdot u = 1 \pmod 5,$$

$$2 \cdot 2^{-1} \cdot u = 1 \cdot 2^{-1} \pmod 5,$$

$$u = 1 \cdot 3 \pmod 5 = 3 \pmod 5.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 5 + 7 \cdot u$, получим решение системы (1.85) по модулю 35:

$$x = 5 + 7 \cdot u \pmod{35} = 5 + 7 \cdot 3 = 26 \pmod{35}.$$

Из данных табл. 1.77 следует, что решением третьей из четырех систем уравнений системы (1.86) является $x = 9 \pmod{35}$.

Таблица 1.77

$x \pmod{35}$	$x \pmod{5}$	$x \pmod{7}$
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	0	5
6	1	6
7	2	0
8	3	1
9	4	2
10	0	3
11	1	4
12	2	5
13	3	6
14	4	0
15	0	1
16	1	2
17	2	3
18	3	4
19	4	5
20	0	6
21	1	0
22	2	1
23	3	2
24	4	3
25	0	4
26	1	5
27	2	6
28	3	0
29	4	1

Продолжение табл. 1.77

x (mod 35)	x (mod 5)	x (mod 7)
30	0	2
31	1	3
32	2	4
33	3	5
34	4	6

Решим эту же систему уравнений (1.86) аналитически.

Если $x = 2 \pmod 7$ и $x = 4 \pmod 5$, то путем ввода дополнительной переменной u получим:

$$x = 2 + 7 \cdot u \pmod 7 \text{ и } x = 4 \pmod 5.$$

Подставив выражение для x из первого уравнения $x = 2 + 7 \cdot u \pmod 7$ во второе $x = 4 \pmod 5$, получим:

$$2 + 7 \cdot u = 4 \pmod 5,$$

$$2 + 2 \cdot u = 4 \pmod 5,$$

$$2 \cdot u = 2 \pmod 5.$$

В случае, когда НОД $(a, N) = 1$, уравнение вида $a \cdot x = b \pmod N$ имеет решение, причем единственное. В нашем случае НОД $(2, 5) = 1$, следовательно, уравнение $2 \cdot u = 2 \pmod 5$ имеет единственный корень, вычислим его:

$$2 \cdot u = 2 \pmod 5,$$

$$2 \cdot 2^{-1} \cdot u = 2 \cdot 2^{-1} \pmod 5,$$

$$u = 1 \pmod 5.$$

Подставим найденное значение введенной дополнительной переменной u в выражение $x = 2 + 7 \cdot u$ и получим решение системы (1.86) по модулю 35:

$$x = 2 + 7 \cdot u \pmod{35} = 2 + 7 \cdot 1 = 9 \pmod{35}.$$

Из данных табл. 1.78 видно, что решением последней из четырех систем уравнений, системы (1.87), является $x = 19 \pmod{35}$.

Таблица 1.78

$x \pmod{35}$	$x \pmod{5}$	$x \pmod{7}$
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	0	5
6	1	6
7	2	0
8	3	1
9	4	2
10	0	3
11	1	4
12	2	5
13	3	6
14	4	0
15	0	1
16	1	2
17	2	3
18	3	4
19	4	5
20	0	6
21	1	0
22	2	1
23	3	2
24	4	3
25	0	4
26	1	5
27	2	6
28	3	0
29	4	1

Продолжение табл. 1.78

$x \pmod{35}$	$x \pmod 5$	$x \pmod 7$
30	0	2
31	1	3
32	2	4
33	3	5
34	4	6

Решим эту же систему уравнений (1.87) аналитически.

Если $x = 5 \pmod 7$ и $x = 4 \pmod 5$, то, введя в первое соотношение дополнительную переменную u, получим:

$$x = 5 + 7 \cdot u \pmod 7 \text{ и } x = 4 \pmod 5.$$

Подставив выражение для x из первого уравнения $x = 5 + 7 \cdot u \pmod 7$ во второе $x = 4 \pmod 5$, получим:

$$5 + 7 \cdot u = 4 \pmod 5,$$

$$0 + 2 \cdot u = 4 \pmod 5,$$

$$2 \cdot u = 4 \pmod 5.$$

Если НОД $(a, N) = 1$, то уравнение вида $a \cdot x = b \pmod N$ имеет решение, причем единственное. В нашем случае НОД $(2, 5) = 1$, поэтому уравнение $2 \cdot u = 4 \pmod 5$ имеет единственный корень:

$$2 \cdot u = 4 \pmod 5,$$

$$2 \cdot 2^{-1} \cdot u = 4 \cdot 2^{-1} \pmod 5,$$

$$u = 4 \cdot 3 \pmod 5,$$

$$u = 12 \pmod 5,$$

$$u = 2 \pmod 5.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 5 + 7 \cdot u$, получим решение системы (1.87) по модулю 35:

$$x = 5 + 7 \cdot u \pmod{35} = 5 + 7 \cdot 2 = 19 \pmod{35}.$$

Пример 2 извлечения корня из a по модулю n. В нем вычислим значения корня из $a = 217$ по модулю $n = 221 = p \cdot q = 13 \cdot 17$.

При рассмотрении этого примера не будем строить таблицу квадратов по модулю 221 для того, чтобы увидеть все корни из 217 по модулю 221 вследствие ее больших размеров.

Вычислим все значения квадратного корня из 217 по модулю 221 в соответствии с рассмотренным выше способом, основанном на отмеченном свойстве символа Якоби (1.82) и применении китайской теоремы об остатках к системе уравнений вида (1.83).

Отметим, что число $a = 217$ действительно является полным квадратом по модулю $n = 221 = p \cdot q = 13 \cdot 17$, поскольку

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = \left(\frac{217}{13}\right) = \left(\frac{217}{17}\right) = +1.$$

Сначала определим корень из $a = 217$ по модулю $p = 13$ с помощью построенной табл. 1.79 и обозначим его через $s_p = s_{13}$.

Из данных этой таблицы следует, что $\sqrt{217} \pmod{13} = 3$ или 10, поскольку $3^2 \pmod{13} = 10^2 \pmod{13} = 9 \pmod{13} = 217 \pmod{13}$. Таким образом, корнем из $a = 217$ по модулю $p = 13$ является $s_p = s_{13} = 3$ или 10.

Затем определим корень из $a = 217$ по модулю $q = 17$ с помощью построенной табл. 1.80 и обозначим его через $s_q = s_{17}$.

Таблица 1.79

x	$x^2 \pmod{13}$
0	0
1	1
2	4
3	9 (mod 13) = 217 (mod 13)
4	3
5	12
6	10
7	10
8	12
9	3
10	9 (mod 13) = 217 (mod 13)
11	4
12	1

Таблица 1.80

x	$x^2 \pmod{17}$
0	0
1	1
2	4
3	9
4	16
5	8
6	2
7	15
8	13 (mod 17) = 217 (mod 17)
9	13 (mod 17) = 217 (mod 17)
10	15
11	2
12	8
13	16
14	9
15	4
16	1

Из данных этой таблицы следует, что $\sqrt{217}\,(\mathrm{mod}17) = 8$ или 9, поскольку $8^2 \pmod{17} = 9^2 \pmod{17} = 13 \pmod{17} = 217 \pmod{17}$. Таким образом, корнем из $a = 217$ по модулю $q = 17$ является $s_q = s_{17} = 8$ или 9.

И, наконец, для вычисления искомого корня из $a = 217$ по модулю $n = 221 = p \cdot q = 13 \cdot 17$ применим китайскую теорему об остатках к системе уравнений (1.83):

$$\begin{cases} x = s_p (\mathrm{mod}\, p), \\ x = s_q (\mathrm{mod} q). \end{cases} = \begin{cases} x = s_{13} (\mathrm{mod} 13), \\ x = s_{17} (\mathrm{mod} 17). \end{cases}$$

Поскольку корень s_{13} из 217 по модулю 221 принимает два значения (3 или 10) и корень s_{17} из 217 по модулю 17 принимает два значения (8 или 9), для получения всех корней из 217 по модулю $13 \cdot 17 = 221$ с применением китайской теоремы об остатках необходимо решить четыре системы уравнений:

$$\begin{cases} x = 3\,(\mathrm{mod}13), \\ x = 8\,(\mathrm{mod}17). \end{cases} \tag{1.88}$$

$$\begin{cases} x = 3\,(\mathrm{mod}13), \\ x = 9\,(\mathrm{mod}17). \end{cases} \tag{1.89}$$

$$\begin{cases} x = 10\,(\mathrm{mod}13), \\ x = 8\,(\mathrm{mod}17). \end{cases} \tag{1.90}$$

$$\begin{cases} x = 10\,(\mathrm{mod}13), \\ x = 9\,(\mathrm{mod}17). \end{cases} \tag{1.91}$$

Здесь мы не будем строить таблицы для определения решений этих систем уравнений, а сразу решим их аналитически и выполним проверку найденных решений.

Если в соответствии с системой (1.88) $x = 8 \pmod{17}$ и $x = 3 \pmod{13}$, то, введя в первое соотношение дополнительную переменную u, получим:

$$x = 8 + 17 \cdot u \pmod{17} \text{ и } x = 3 \pmod{13}.$$

Подставив выражение для x из первого уравнения $x = 8 + 17 \cdot u \pmod{17}$ во второе $x = 3 \pmod{13}$, получим:

$$8 + 17 \cdot u = 3 \pmod{13},$$
$$8 + 4 \cdot u = 3 \pmod{13},$$
$$4 \cdot u = -5 \pmod{13},$$
$$4 \cdot u = 8 \pmod{13}.$$

Если НОД $(a, N) = 1$, то уравнение вида $a \cdot x = b \pmod{N}$ имеет решение, причем единственное. В нашем случае НОД $(4, 13) = 1$, поэтому уравнение $4 \cdot u = 8 \pmod{13}$ имеет единственный корень:

$$4 \cdot u = 8 \pmod{13},$$
$$4 \cdot 4^{-1} \cdot u = 8 \cdot 4^{-1} \pmod{13},$$
$$u = 8 \cdot 10 \pmod{13} = 80 \pmod{13} = 2 \pmod{13}.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 8 + 17 \cdot u$, получим решение системы (1.88) по модулю 221:

$$x = 8 + 17 \cdot u \pmod{221} = 8 + 17 \cdot 2 \pmod{221} = 42 \pmod{221}.$$

Проверка этого решения дает положительный результат:

$$42^2 \pmod{221} = 1764 \pmod{221} = 217.$$

Если в соответствии с системой (1.89) $x = 9 \pmod{17}$ и $x = 3 \pmod{13}$, то, введя в первое соотношение дополнительную переменную u, получим:

$$x = 9 + 17 \cdot u \pmod{17} \text{ и } x = 3 \pmod{13}.$$

Подставив выражение для x из первого уравнения $x = 9 + 17 \cdot u \pmod{17}$ во второе $x = 3 \pmod{13}$, получим:

$$9 + 17 \cdot u = 3 \pmod{13},$$
$$9 + 4 \cdot u = 3 \pmod{13},$$
$$4 \cdot u = -6 \pmod{13},$$
$$4 \cdot u = 7 \pmod{13}.$$

Если НОД $(a, N) = 1$, то уравнение вида $a \cdot x = b \pmod{N}$ имеет решение, причем единственное. В нашем случае НОД $(4, 13) = 1$, поэтому уравнение $4 \cdot u = 7 \pmod{13}$ имеет единственный корень:

$$4 \cdot u = 7 \pmod{13},$$
$$4 \cdot 4^{-1} \cdot u = 7 \cdot 4^{-1} \pmod{13},$$
$$u = 7 \cdot 10 \pmod{13} = 70 \pmod{13} = 5 \pmod{13}.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 9 + 17 \cdot u$, получим решение системы (1.89) по модулю 221:

$$x = 9 + 17 \cdot u \pmod{221} = 9 + 17 \cdot 5 \pmod{221} = 94 \pmod{221}.$$

Проверка этого решения дает положительный результат:

$$94^2 \pmod{221} = 8836 \pmod{221} = 217.$$

Если в соответствии с системой (1.90) $x = 8 \pmod{17}$ и $x = 10 \pmod{13}$, то, введя в первое соотношение дополнительную переменную u, получим:

$$x = 8 + 17 \cdot u \pmod{17} \text{ и } x = 10 \pmod{13}.$$

Подставив выражение для x из первого уравнения $x = 8 + 17 \cdot u \pmod{17}$ во второе $x = 10 \pmod{13}$, получим:

$$8 + 17 \cdot u = 10 \pmod{13},$$
$$8 + 4 \cdot u = 10 \pmod{13},$$
$$4 \cdot u = 2 \pmod{13}.$$

Если НОД (a, N) = 1, то уравнение вида $a \cdot x = b \pmod N$ имеет решение, причем единственное. В нашем случае НОД (4, 13) = 1, поэтому уравнение $4 \cdot u = 2 \pmod{13}$ имеет единственный корень:

$$4 \cdot u = 2 \pmod{13},$$
$$4 \cdot 4^{-1} \cdot u = 2 \cdot 4^{-1} \pmod{13},$$
$$u = 2 \cdot 10 \pmod{13} = 20 \pmod{13} = 7 \pmod{13}.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 8 + 17 \cdot u$, получим решение системы (1.90) по модулю 221:

$$x = 8 + 17 \cdot u \pmod{221} = 8 + 17 \cdot 7 \pmod{221} = 127 \pmod{221}.$$

Проверка этого решения дает положительный результат:

$$127^2 \pmod{221} = 16129 \pmod{221} = 217.$$

Если в соответствии с системой (1.91) $x = 9 \pmod{17}$ и $x = 10 \pmod{13}$, то, введя в первое соотношение дополнительную переменную u, получим:

$$x = 9 + 17 \cdot u \pmod{17} \text{ и } x = 10 \pmod{13}.$$

Подставив выражение для x из первого уравнения $x = 9 + 17 \cdot u \pmod{17}$ во второе $x = 10 \pmod{13}$, получим:

$$9 + 17 \cdot u = 10 \pmod{13},$$
$$9 + 4 \cdot u = 10 \pmod{13},$$
$$4 \cdot u = 1 \pmod{13}.$$

Если НОД (a, N) = 1, то уравнение вида $a \cdot x = b \pmod N$ имеет решение, причем единственное. В нашем случае НОД (4, 13) = 1, поэтому уравнение $4 \cdot u = 1 \pmod{13}$ имеет единственный корень:

$$4 \cdot u = 1 \pmod{13},$$
$$4 \cdot 4^{-1} \cdot u = 1 \cdot 4^{-1} \pmod{13},$$
$$u = 1 \cdot 10 \pmod{13} = 10 \pmod{13}.$$

Подставив найденное значение введенной дополнительной переменной u в выражение $x = 9 + 17 \cdot u$, получим решение системы (1.91) по модулю 221:

$$x = 9 + 17 \cdot u \pmod{221} = 9 + 17 \cdot 10 \pmod{221} = 179 \pmod{221}.$$

Проверка этого решения дает положительный результат:

$$179^2 \pmod{221} = 32041 \pmod{221} = 217.$$

Таким образом, корнями из 217 по модулю 221 являются числа 42, 94, 127 и 179.

1.5. ВЕРОЯТНОСТЬ

1.5.1. СЛУЧАЙНАЯ ВЕЛИЧИНА

Случайной величиной называется переменная X, которая в результате определенных испытаний принимает свои значения с некоторой вероятностью. Если переменная X принимает значение x с вероятностью 0,05, то будем писать:

$$p(X = x) = 0{,}05. \tag{1.92}$$

Пусть, например, случайная величина T представляет собой результат испытания, заключающегося в подбрасывании симметричной монеты. Тогда переменная T в результате подбрасывания принимает значения герба (Г) и цифры (Ц) с равной вероятностью

$$p(T = \text{Г}) = \frac{1}{2},\ p(T = \text{Ц}) = \frac{1}{2}.$$

В другом примере пусть случайная величина B принимает значения цвета выбранного наугад шара из («несимметричной» в смысле неодинакового количества шаров разного цвета) урны с шестнадцатью желтыми, двумя зелеными, десятью красными и четырьмя синими шарами. Тогда переменная B в результате случайного выбора шара из урны принимает значения желтый (Ж), зеленый (З), красный (К) и синий (С) с различными вероятностями:

$$p(B = \text{Ж}) = \frac{16}{16+2+10+4} = \frac{16}{16+2+10+4} = \frac{16}{32} = \frac{1}{2},$$

$$p(B = \text{З}) = \frac{2}{32} = \frac{1}{16},$$

$$p(B = \text{К}) = \frac{10}{32} = \frac{5}{16},$$

$$p(B = \text{С}) = \frac{4}{32} = \frac{1}{8}.$$

Пусть в третьем примере случайная величина E принимает значения в результате испытаний, заключающихся в (несимметричном) выборе буквы из большого текста, написанного на английском языке. Тогда можно представить в основном неповторяющиеся вероятности случайного выбора той или иной буквы из этого текста следующим образом:

$$p(E = \text{‘}a\text{’}) = 0{,}082,\ p(E = \text{‘}b\text{’}) = 0{,}015,$$
$$p(E = \text{‘}c\text{’}) = 0{,}028,\ p(E = \text{‘}d\text{’}) = 0{,}042,$$
$$p(E = \text{‘}e\text{’}) = 0{,}127,\ p(E = \text{‘}f\text{’}) = 0{,}022,$$
$$p(E = \text{‘}g\text{’}) = 0{,}020,\ p(E = \text{‘}h\text{’}) = 0{,}061,$$
$$p(E = \text{‘}i\text{’}) = 0{,}070,\ p(E = \text{‘}j\text{’}) = 0{,}001,$$
$$p(E = \text{‘}k\text{’}) = 0{,}008,\ p(E = \text{‘}l\text{’}) = 0{,}040,$$
$$p(E = \text{‘}m\text{’}) = 0{,}024,\ p(E = \text{‘}n\text{’}) = 0{,}067,$$
$$p(E = \text{‘}o\text{’}) = 0{,}075,\ p(E = \text{‘}p\text{’}) = 0{,}019,$$
$$p(E = \text{‘}q\text{’}) = 0{,}001,\ p(E = \text{‘}r\text{’}) = 0{,}060,$$
$$p(E = \text{‘}s\text{’}) = 0{,}063,\ p(E = \text{‘}t\text{’}) = 0{,}091,$$
$$p(E = \text{‘}u\text{’}) = 0{,}028,\ p(E = \text{‘}v\text{’}) = 0{,}010,$$
$$p(E = \text{‘}w\text{’}) = 0{,}024,\ p(E = \text{‘}x\text{’}) = 0{,}001,$$
$$p(E = \text{‘}y\text{’}) = 0{,}020,\ p(E = \text{‘}z\text{’}) = 0{,}001.$$

Если случайная величина X является дискретной случайной величиной, т.е. множество ее значений конечно или счетно, то множество вероятностей всех ее значений называют *распределением вероятностей дискретной случайной величины X*. При этом функцию $p(X = x)$, сопоставляющую каждому значению x переменной X соответствующее значение вероятности, называют *плотностью распределения вероятностей дискретной случайной величины X*. В общем случае плотность распределения вероятностей дискретной случайной величины обладает следующими свойствами:

$$p(X = x) \geq 0, \tag{1.93}$$

$$\sum_x p(X = x) = 1. \tag{1.94}$$

Упомянутые выше в примерах дискретные случайные величины T, B и E имеют распределения вероятностей $\left\{\frac{1}{2}\right\}$, $\left\{\frac{1}{16}, \frac{1}{8}, \frac{5}{16}, \frac{1}{2}\right\}$ и {0,001; 0,008; 0,010; 0,015; 0,019; 0,020; 0,022; 0,024; 0,028; 0,040; 0,042; 0,060; 0,061; 0,063; 0,067; 0,070; 0,075; 0,082; 0,091; 0,127}, а плотности распределения вероятностей этих величин представлены табл. 1.81 – 1.83 соответственно.

Таблица 1.81

x	$p(T = x)$
Г	$\frac{1}{2}$
Ц	$\frac{1}{2}$

Таблица 1.82

x	$p(B = x)$
Ж	$\frac{1}{2}$
З	$\frac{1}{16}$
К	$\frac{5}{16}$
С	$\frac{1}{8}$

Таблица 1.83

x	$p(E = x)$	x	$p(E = x)$
‘*a*’	0,082	‘*n*’	0,067
‘*b*’	0,015	‘*o*’	0,075
‘*c*’	0,028	‘*p*’	0,019
‘*d*’	0,042	‘*q*’	0,001
‘*e*’	0,127	‘*r*’	0,060
‘*f*’	0,022	‘*s*’	0,063
‘*g*’	0,020	‘*t*’	0,091
‘*h*’	0,061	‘*u*’	0,028
‘*i*’	0,070	‘*v*’	0,010
‘*j*’	0,001	‘*w*’	0,024
‘*k*’	0,008	‘*x*’	0,001
‘*l*’	0,040	‘*y*’	0,020
‘*m*’	0,024	‘*z*’	0,001

Плотности распределения вероятностей дискретных случайных величин *T*, *B* и *E* удовлетворяют свойству (1.93).

Для дискретной случайной величины *T*:

$$p(T = \text{Г}) = \frac{1}{2} \geq 0, \quad p(T = \text{Ц}) = \frac{1}{2} \geq 0.$$

Для дискретной случайной величины *B*:

$$p(B = \text{Ж}) = \frac{1}{2} \geq 0, \quad p(B = \text{З}) = \frac{1}{16} \geq 0,$$

$$p(B = \text{К}) = \frac{5}{16} \geq 0, \quad p(B = \text{С}) = \frac{1}{8} \geq 0.$$

Для дискретной случайной величины *E*:

$$p(E = \text{‘}a\text{’}) = 0{,}082 \geq 0,\ p(E = \text{‘}b\text{’}) = 0{,}015 \geq 0,$$

$$p(E = \text{‘}c\text{’}) = 0{,}028 \geq 0,\ p(E = \text{‘}d\text{’}) = 0{,}042 \geq 0,$$

$$p(E = \text{‘}e\text{’}) = 0{,}127 \geq 0,\ p(E = \text{‘}f\text{’}) = 0{,}022 \geq 0,$$

$$p(E = \text{‘}g\text{’}) = 0{,}020 \geq 0,\ p(E = \text{‘}h\text{’}) = 0{,}061 \geq 0,$$

$$p(E = \text{‘}i\text{’}) = 0{,}070 \geq 0,\ p(E = \text{‘}j\text{’}) = 0{,}001 \geq 0,$$

$$p(E = \text{‘}k\text{’}) = 0{,}008 \geq 0,\ p(E = \text{‘}l\text{’}) = 0{,}040 \geq 0,$$

$$p(E = \text{‘}m\text{’}) = 0{,}024 \geq 0,\ p(E = \text{‘}n\text{’}) = 0{,}067 \geq 0,$$

$$p(E = \text{‘}o\text{’}) = 0{,}075 \geq 0,\ p(E = \text{‘}p\text{’}) = 0{,}019 \geq 0,$$

$$p(E = \text{‘}q\text{’}) = 0{,}001 \geq 0,\ p(E = \text{‘}r\text{’}) = 0{,}060 \geq 0,$$

$$p(E = \text{‘}s\text{’}) = 0{,}063 \geq 0,\ p(E = \text{‘}t\text{’}) = 0{,}091 \geq 0,$$

$$p(E = \text{‘}u\text{’}) = 0{,}028 \geq 0,\ p(E = \text{‘}v\text{’}) = 0{,}010 \geq 0,$$

$$p(E = \text{‘}w\text{’}) = 0{,}024 \geq 0,\ p(E = \text{‘}x\text{’}) = 0{,}001 \geq 0,$$

$$p(E = \text{‘}y\text{’}) = 0{,}020 \geq 0,\ p(E = \text{‘}z\text{’}) = 0{,}001 \geq 0.$$

Плотности распределения вероятностей дискретных случайных величин *T*, *B* и *E* удовлетворяют и свойству (1.94).

Для дискретной случайной величины *T*:

$$\sum_x p(T = x) = p(T = \text{Г}) + p(T = \text{Ц}) = \frac{1}{2} + \frac{1}{2} = 1.$$

Для дискретной случайной величины B:

$$\sum_x p(B = x) = p(B = \text{Ж}) + p(B = \text{З}) + p(B = \text{К}) + p(B = \text{С}) =$$

$$= \frac{1}{2} + \frac{1}{16} + \frac{5}{16} + \frac{1}{8} = \frac{8}{16} + \frac{1}{16} + \frac{5}{16} + \frac{2}{16} = \frac{8+1+5+2}{16} = \frac{16}{16} = 1.$$

Для дискретной случайной величины E:

$$\sum_x p(B = x) = p(E = \text{‘}a\text{’}) + p(E = \text{‘}b\text{’}) + p(E = \text{‘}c\text{’}) + p(E = \text{‘}d\text{’}) + p(E = \text{‘}e\text{’}) +$$

$$+ p(E = \text{‘}f\text{’}) + p(E = \text{‘}g\text{’}) + p(E = \text{‘}h\text{’}) + p(E = \text{‘}i\text{’}) + p(E = \text{‘}j\text{’}) + p(E = \text{‘}k\text{’}) +$$

$$+ p(E = \text{‘}l\text{’}) + p(E = \text{‘}m\text{’}) + p(E = \text{‘}n\text{’}) + p(E = \text{‘}o\text{’}) + p(E = \text{‘}p\text{’}) + p(E = \text{‘}q\text{’}) +$$

$$+ p(E = \text{‘}r\text{’}) + p(E = \text{‘}s\text{’}) + p(E = \text{‘}t\text{’}) + p(E = \text{‘}u\text{’}) + p(E = \text{‘}v\text{’}) + p(E = \text{‘}w\text{’}) +$$

$$+ p(E = \text{‘}x\text{’}) + p(E = \text{‘}y\text{’}) + p(E = \text{‘}z\text{’}) =$$

$$= 0{,}082 + 0{,}015 + 0{,}028 + 0{,}042 + 0{,}127 + 0{,}022 + 0{,}020 + 0{,}061 + 0{,}070 +$$

$$+ 0{,}001 + 0{,}008 + 0{,}040 + 0{,}024 + 0{,}067 + 0{,}075 + 0{,}019 + 0{,}001 + 0{,}060 +$$

$$+ 0{,}063 + 0{,}091 + 0{,}028 + 0{,}010 + 0{,}024 + 0{,}001 + 0{,}020 + 0{,}001 = 1.$$

Предположим, что X и Y являются дискретными случайными величинами с плотностями распределения вероятностей $p(X = x)$ и $p(Y = y)$ соответственно. Тогда вероятность того, что дискретная переменная X примет значение x и, одновременно, дискретная переменная Y примет значение y называется *совместной вероятностью* с плотностью распределения вероятностей $p(X = x, Y = y)$. Совместная вероятность $p(X = x, Y = y)$ наступления двух случайных событий $X = x$ и $Y = y$ равна произведению вероятности $p(X = x)$ наступления первого события $X = x$ на вероятность $p(Y = y)$ наступления второго события $Y = y$, при условии, что первое событие $X = x$ уже наступило.

Пусть для нашего примера «несимметричной» урны с шестнадцатью желтыми, двумя зелеными, десятью красными и четырьмя синими шарами в качестве переменной X выступит дискретная случайная величина цвета первого выбранного наугад шара из урны B_1, а в качестве переменной Y – дискретная случайная величина цвета второго выбранного наугад шара из урны B_2. Тогда вероятность $p(B_1 = b_1, B_2 = b_2)$ совместного наступления двух событий $B_1 = b_1$ и $B_2 = b_2$ будет равна произведению вероятности цвета выбранного шара при первом выборе $p(B_1 = b_1)$ на вероятность цвета выбранного шара при втором выборе $p(B_2 = b_2)$, с учетом того, что первое событие $B_1 = b_1$ уже наступило и в урне осталось на один шар цвета b_1 меньше:

$$p(B_1 = \text{Ж}, B_2 = \text{Ж}) = \frac{16}{32} \cdot \frac{15}{31} = \frac{1}{2} \cdot \frac{15}{31} = \frac{15}{2 \cdot 31} = \frac{15}{62},$$

$$p(B_1 = \text{Ж}, B_2 = \text{З}) = \frac{16}{32} \cdot \frac{2}{31} = \frac{1}{2} \cdot \frac{2}{31} = \frac{1}{31},$$

$$p(B_1 = \text{Ж}, B_2 = \text{К}) = \frac{16}{32} \cdot \frac{10}{31} = \frac{1}{2} \cdot \frac{10}{31} = \frac{5}{31},$$

$$p(B_1 = \text{Ж}, B_2 = \text{С}) = \frac{16}{32} \cdot \frac{4}{31} = \frac{1}{2} \cdot \frac{4}{31} = \frac{2}{31},$$

$$p(B_1 = \text{З}, B_2 = \text{Ж}) = \frac{2}{32} \cdot \frac{16}{31} = \frac{1}{16} \cdot \frac{16}{31} = \frac{1}{31},$$

$$p(B_1 = \text{З}, B_2 = \text{З}) = \frac{2}{32} \cdot \frac{1}{31} = \frac{1}{16} \cdot \frac{1}{31} = \frac{1}{16 \cdot 31} = \frac{1}{496},$$

$$p(B_1 = \text{З}, B_2 = \text{К}) = \frac{2}{32} \cdot \frac{10}{31} = \frac{1}{16} \cdot \frac{10}{31} = \frac{5}{8 \cdot 31} = \frac{5}{248},$$

$$p(B_1 = \text{З}, B_2 = \text{С}) = \frac{2}{32} \cdot \frac{4}{31} = \frac{1}{16} \cdot \frac{4}{31} = \frac{1}{4 \cdot 31} = \frac{1}{124},$$

$$p(B_1 = \text{К}, B_2 = \text{Ж}) = \frac{10}{32} \cdot \frac{16}{31} = \frac{5}{16} \cdot \frac{16}{31} = \frac{5}{31},$$

$$p(B_1 = \text{К}, B_2 = \text{З}) = \frac{10}{32} \cdot \frac{2}{31} = \frac{5}{16} \cdot \frac{2}{31} = \frac{5}{8 \cdot 31} = \frac{5}{248},$$

$$p(B_1 = \text{К}, B_2 = \text{К}) = \frac{10}{32} \cdot \frac{9}{31} = \frac{5}{16} \cdot \frac{9}{31} = \frac{45}{496},$$

$$p(B_1 = \text{К}, B_2 = \text{С}) = \frac{10}{32} \cdot \frac{4}{31} = \frac{5}{16} \cdot \frac{4}{31} = \frac{5}{4 \cdot 31} = \frac{5}{124},$$

$$p(B_1 = \text{С}, B_2 = \text{Ж}) = \frac{4}{32} \cdot \frac{16}{31} = \frac{1}{8} \cdot \frac{16}{31} = \frac{2}{31},$$

$$p(B_1 = \text{С}, B_2 = \text{З}) = \frac{4}{32} \cdot \frac{2}{31} = \frac{1}{8} \cdot \frac{2}{31} = \frac{1}{4 \cdot 31} = \frac{1}{124},$$

$$p(B_1 = \text{С}, B_2 = \text{К}) = \frac{4}{32} \cdot \frac{10}{31} = \frac{1}{8} \cdot \frac{10}{31} = \frac{5}{124},$$

$$p(B_1 = \text{С}, B_2 = \text{С}) = \frac{4}{32} \cdot \frac{3}{31} = \frac{1}{8} \cdot \frac{3}{31} = \frac{3}{8 \cdot 31} = \frac{3}{248}.$$

Заметим, что порядок наступления дискретных случайных событий B_1 и B_2 не влияет на значение их совместной вероятности, что подтверждает симметричность относительно главной диагонали соответствующей матрицы, представленной табл. 1.84.

Таблица 1.84

B_2 \ B_1	Ж	З	К	С
Ж	$\frac{15}{62}$	$\frac{1}{31}$	$\frac{5}{31}$	$\frac{2}{31}$
З	$\frac{1}{31}$	$\frac{1}{496}$	$\frac{5}{248}$	$\frac{1}{124}$
К	$\frac{5}{31}$	$\frac{5}{248}$	$\frac{45}{496}$	$\frac{5}{124}$
С	$\frac{2}{31}$	$\frac{1}{124}$	$\frac{5}{124}$	$\frac{3}{248}$

Случайные величины X и Y называются *независимыми случайными величинами*, если наступление одного события $X = x$ не может повлиять на вероятность наступления другого события $Y = y$.

Таким образом, в рассмотренном выше примере с «несимметричной» урной с шестнадцатью желтыми, двумя зелеными, десятью красными и четырьмя синими шарами дискретные случайные величины B_1 и B_2 нельзя считать независимыми, поскольку наступление первого события $B_1 = b_1$ влияет на вероятность наступления второго события $B_2 = b_2$ вследствие того, что после наступления первого события в урне остается на один шар цвета b_1 меньше.

Заметим, что в нашем примере с «несимметричной» урной дискретные случайные величины B_1 и B_2 будем считать независимыми, если после наступления первого события $B_1 = b_1$ и перед случайным выбором второго шара, первый шар цвета b_1 будет возвращен в урну. Тогда вероятность $p(B_1 = b_1, B_2 = b_2)$ совместного наступления двух событий $B_1 = b_1$ и $B_2 = b_2$ будет равна произведению вероятности цвета выбранного наугад шара при первом выборе $p(B_1 = b_1)$ на вероятность цвета выбранного наугад шара при втором выборе $p(B_2 = b_2)$ по сути из одной и той же урны (с шестнадцатью желтыми, двумя зелеными, десятью красными и четырьмя синими шарами):

$$p(B_1 = \text{Ж}, B_2 = \text{Ж}) = \frac{16}{32} \cdot \frac{16}{32} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4},$$

$$p(B_1 = \text{Ж}, B_2 = \text{З}) = \frac{16}{32} \cdot \frac{2}{32} = \frac{1}{2} \cdot \frac{1}{16} = \frac{1}{32},$$

$$p(B_1 = \text{Ж}, B_2 = \text{К}) = \frac{16}{32} \cdot \frac{10}{32} = \frac{1}{2} \cdot \frac{5}{16} = \frac{5}{32},$$

$$p(B_1 = \text{Ж}, B_2 = \text{С}) = \frac{16}{32} \cdot \frac{4}{32} = \frac{1}{2} \cdot \frac{4}{32} = \frac{2}{32},$$

$$p(B_1 = \text{З}, B_2 = \text{Ж}) = \frac{2}{32} \cdot \frac{16}{32} = \frac{1}{16} \cdot \frac{1}{2} = \frac{1}{32},$$

$$p(B_1 = \text{З}, B_2 = \text{З}) = \frac{2}{32} \cdot \frac{2}{32} = \frac{1}{16} \cdot \frac{1}{16} = \frac{1}{256},$$

$$p(B_1 = \text{З}, B_2 = \text{К}) = \frac{2}{32} \cdot \frac{10}{32} = \frac{1}{16} \cdot \frac{5}{16} = \frac{5}{256},$$

$$p(B_1 = \text{З}, B_2 = \text{С}) = \frac{2}{32} \cdot \frac{4}{32} = \frac{1}{16} \cdot \frac{1}{8} = \frac{1}{128},$$

$$p(B_1 = \text{К}, B_2 = \text{Ж}) = \frac{10}{32} \cdot \frac{16}{32} = \frac{5}{16} \cdot \frac{1}{2} = \frac{5}{32},$$

$$p(B_1 = \text{К}, B_2 = \text{З}) = \frac{10}{32} \cdot \frac{2}{32} = \frac{5}{16} \cdot \frac{1}{16} = \frac{5}{256},$$

$$p(B_1 = \text{К}, B_2 = \text{К}) = \frac{10}{32} \cdot \frac{10}{32} = \frac{5}{16} \cdot \frac{5}{16} = \frac{25}{256},$$

$$p(B_1 = \text{К}, B_2 = \text{С}) = \frac{10}{32} \cdot \frac{4}{32} = \frac{5}{16} \cdot \frac{1}{8} = \frac{5}{128},$$

$$p(B_1 = \text{С}, B_2 = \text{Ж}) = \frac{4}{32} \cdot \frac{16}{32} = \frac{1}{8} \cdot \frac{1}{2} = \frac{1}{16},$$

$$p(B_1 = \text{С}, B_2 = \text{З}) = \frac{4}{32} \cdot \frac{2}{32} = \frac{1}{8} \cdot \frac{1}{16} = \frac{1}{8 \cdot 16} = \frac{1}{128},$$

$$p(B_1 = \text{С}, B_2 = \text{К}) = \frac{4}{32} \cdot \frac{10}{32} = \frac{1}{8} \cdot \frac{5}{16} = \frac{5}{128},$$

$$p(B_1 = \text{С}, B_2 = \text{С}) = \frac{4}{32} \cdot \frac{4}{32} = \frac{1}{8} \cdot \frac{1}{8} = \frac{1}{64}.$$

В качестве еще одного примера независимых случайных величин можно рассмотреть дискретные случайные величины, получаемые в результате эксперимента, который заключается в последовательном подбрасывании двух симметричных монет. Если через T_1 обозначить результат подбрасывания первой монеты t_1, а через T_2 – результат подбрасывания второй монеты t_2, то в силу физических законов получим следующие возможные варианты значений совместной вероятности $p(T_1 = t_1, T_2 = t_2)$:

$$p(T_1 = \Г, T_2 = \Г) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}, p(T_1 = \Г, T_2 = \text{Ц}) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4},$$

$$p(T_1 = \text{Ц}, T_2 = \Г) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}, p(T_1 = \text{Ц}, T_2 = \text{Ц}) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}.$$

1.5.2. ТЕОРЕМА БАЙЕСА

Условной вероятностью $p(X = x \mid Y = y)$ случайных величин X и Y называют вероятность того, что в результате некоторого эксперимента переменная X примет значение x, при условии, что переменная Y имеет значение y.

Возвращаясь к экспериментам с («несимметричной» в смысле неодинакового количества шаров разного цвета) урной с шестнадцатью желтыми, двумя зелеными, десятью красными и четырьмя синими шарами из предыдущего пункта, рассмотрим несколько примеров условных вероятностей.

Если, например, из такой урны (с 32 шарами) в первом эксперименте случайным образом выбран один из 16 шаров желтого цвета, что ограничивает выбор желтых шаров на один, то к началу второго эксперимента у нас в урне есть только 15 шаров желтого цвета среди оставшегося 31 шара:

$$p(B_2 = \text{Ж} \mid B_1 = \text{Ж}) = \frac{15}{31}.$$

В другом примере, если из такой урны в первом эксперименте случайным образом выбран один из шаров желтого цвета, что уменьшает общее количество шаров в урне до 31, то к началу второго эксперимента у нас в урне есть два шара зеленого цвета:

$$p(B_2 = \text{З} \mid B_1 = \text{Ж}) = \frac{2}{31}.$$

Если, в третьем примере, из урны (с 32 шарами) в первом эксперименте случайным образом выбран один из двух шаров зеленого цвета, что ограничивает выбор зеленых шаров на один, то к началу второго эксперимента у нас в урне есть только один шар зеленого цвета среди оставшегося 31 шара:

$$p(B_2 = \text{З} \mid B_1 = \text{З}) = \frac{1}{31}.$$

В четвертом примере, если из урны в первом эксперименте случайным образом выбран один из шаров синего цвета, что уменьшает общее число шаров с 32 до 31, то к началу второго эксперимента у нас в урне среди всех оставшихся шаров есть 10 шаров красного цвета:

$$p(B_2 = \text{К} \mid B_1 = \text{С}) = \frac{10}{31}.$$

Одной из основных теорем элементарной теории вероятностей является *теорема Байеса*, которая утверждает, что если $p(Y = y) > 0$, то

$$p(X = x \mid Y = y) = \frac{p(X = x) \cdot p(Y = y \mid X = x)}{p(Y = y)} =$$

$$= \frac{p(X = x, Y = y)}{p(Y = y)}. \qquad (1.95)$$

Применим теорему Байеса к рассмотренным выше четырем примерам условных вероятностей при проведении экспериментов с нашей несимметричной урной с 32 разноцветными шарами. Тогда в качестве случайной переменной X будет выступать дискретная случайная переменная B_2, а в качестве случайной переменной Y – дискретная случайная переменная B_1.

В первом примере вероятность $p(B_2 = \text{Ж} \mid B_1 = \text{Ж})$ того, что в результате случайного выбора из урны шара желтого цвета, при условии, что из нее уже был выбран один желтый шар, в соответствии с формулой (1.95) теоремы Байеса равна частному совместной вероятности $p(B_2 = \text{Ж}, B_1 = \text{Ж})$ и вероятности $p(B_1 = \text{Ж})$:

$$p(B_2 = \text{Ж} \mid B_1 = \text{Ж}) = \frac{p(B_2 = \text{Ж}, B_1 = \text{Ж})}{p(B_1 = \text{Ж})} =$$

$$= \frac{p(B_1 = \text{Ж}, B_2 = \text{Ж})}{p(B = \text{Ж})} = \frac{15}{62} \cdot \left(\frac{1}{2}\right)^{-1} =$$

$$= \frac{15}{62} \cdot \frac{2}{1} = \frac{15}{31}.$$

Во втором примере вероятность $p(B_2 = \text{З} \mid B_1 = \text{Ж})$ того, что в результате случайного выбора из урны шара зеленого цвета, при условии, что из нее уже был выбран один желтый шар, в соответствии с формулой (1.95) теоремы Байеса равна частному совместной вероятности $p(B_2 = \text{З}, B_1 = \text{Ж})$ и вероятности $p(B_1 = \text{Ж})$:

$$p(B_2 = \text{З} \mid B_1 = \text{Ж}) = \frac{p(B_2 = \text{З}, B_1 = \text{Ж})}{p(B_1 = \text{Ж})} = \text{(см. табл. 1.84)} =$$

$$= \frac{p(B_1 = \text{Ж}, B_2 = \text{З})}{p(B = \text{Ж})} = \frac{1}{31} \cdot \left(\frac{1}{2}\right)^{-1} =$$

$$= \frac{1}{31} \cdot \frac{2}{1} = \frac{2}{31}.$$

Во третьем примере вероятность $p(B_2 = \text{З} \mid B_1 = \text{З})$ того, что в результате случайного выбора из урны шара зеленого цвета, при условии, что из нее уже был выбран один зеленый

шар, в соответствии с формулой (1.95) теоремы Байеса равна частному совместной вероятности $p(B_2 = З, B_1 = З)$ и вероятности $p(B_1 = З)$:

$$p(B_2 = З \mid B_1 = З) = \frac{p(B_2 = З, B_1 = З)}{p(B_1 = З)} =$$

$$= \frac{p(B_1 = З, B_2 = З)}{p(B = З)} = \frac{1}{496} \cdot \left(\frac{1}{16}\right)^{-1} =$$

$$= \frac{1}{496} \cdot \frac{16}{1} = \frac{1}{31}.$$

В четвертом примере вероятность $p(B_2 = К \mid B_1 = С)$ того, что в результате случайного выбора из урны шара красного цвета, при условии, что из нее уже был выбран один синий шар, в соответствии с формулой (1.95) теоремы Байеса равна частному совместной вероятности $p(B_2 = К, B_1 = С)$ и вероятности $p(B_1 = С)$:

$$p(B_2 = К \mid B_1 = С) = \frac{p(B_2 = К, B_1 = С)}{p(B_1 = С)} = \text{(см. табл. 1.84)} =$$

$$= \frac{p(B_1 = С, B_2 = К)}{p(B = С)} = \frac{5}{124} \cdot \left(\frac{1}{8}\right)^{-1} =$$

$$= \frac{5}{124} \cdot \frac{8}{1} = \frac{5}{31} \cdot \frac{2}{1} = \frac{10}{31}.$$

Заметим, что если случайные величины X и Y независимы, то условная вероятность $p(X = x \mid Y = y)$ инвариантна по отношению к значению переменной Y, т.е. равна вероятности наступления события $X = x$:

$$p(X = x \mid Y = y) = \frac{p(X = x, Y = y)}{p(Y = y)} = p(X = x). \qquad (1.96)$$

Так, для независимых случайных величин B_1 и B_2 в экспериментах с урной с 32 шарами четырех цветов (когда первый выбранный наугад шар перед выбором второго шара возвращается в урну), например, имеем:

$$p(B_2 = Ж \mid B_1 = Ж) = \frac{p(B_2 = Ж, B_1 = Ж)}{p(B_1 = Ж)} =$$

$$= \frac{p(B_1 = Ж, B_2 = Ж)}{p(B = Ж)} = \frac{1}{4} \cdot \left(\frac{1}{2}\right)^{-1} =$$

$$= \frac{1}{4} \cdot \frac{2}{1} = \frac{1}{2} = p(B_2 = Ж) = p(B = Ж),$$

$$p(B_2 = \text{З} \mid B_1 = \text{Ж}) = \frac{p(B_2 = \text{З}, B_1 = \text{Ж})}{p(B_1 = \text{Ж})} =$$

$$= \frac{p(B_1 = \text{Ж}, B_2 = \text{З})}{p(B = \text{Ж})} = \frac{1}{32} \cdot \left(\frac{1}{2}\right)^{-1} =$$

$$= \frac{1}{32} \cdot \frac{2}{1} = \frac{1}{16} = p(B_2 = \text{З}) = p(B = \text{З}),$$

$$p(B_2 = \text{З} \mid B_1 = \text{З}) = \frac{p(B_2 = \text{З}, B_1 = \text{З})}{p(B_1 = \text{З})} =$$

$$= \frac{p(B_1 = \text{З}, B_2 = \text{З})}{p(B = \text{З})} = \frac{1}{256} \cdot \left(\frac{1}{16}\right)^{-1} =$$

$$= \frac{1}{256} \cdot \frac{16}{1} = \frac{1}{16} = p(B_2 = \text{З}) = p(B = \text{З}),$$

$$p(B_2 = \text{К} \mid B_1 = \text{С}) = \frac{p(B_2 = \text{К}, B_1 = \text{С})}{p(B_1 = \text{С})} =$$

$$= \frac{p(B_1 = \text{С}, B_2 = \text{К})}{p(B = \text{С})} = \frac{5}{128} \cdot \left(\frac{1}{8}\right)^{-1} =$$

$$= \frac{5}{128} \cdot \frac{8}{1} = \frac{5}{16} = p(B_2 = \text{К}) = p(B = \text{К}).$$

1.5.3. ПАРАДОКС ДНЕЙ РОЖДЕНИЯ

Парадоксом дней рождения называется утверждение о том, что в группе из 23 или более человек вероятность совпадения дней рождения (число и месяц рождения) хотя бы у двух человек превышает 50%.

Попробуем разобраться в справедливости этого утверждения, которое названо парадоксом, поскольку оно на первый взгляд может показаться далеко не очевидным.

Для этого вначале рассмотрим группу из двух человек: $Ч_1$ и $Ч_2$. Дискретные случайные величины их дней рождения обозначим через D_1 и D_2. Если через d_1 обозначить любой день невисокосного календарного года (состоящего из 365 дней), то вероятность того, что случайная переменная D_1 примет значение d_1, будет $p(D_1 = d_1) = 1$ – человек $Ч_1$ родился в любой день невисокосного календарного года (состоящего из 365 дней) с вероятностью, равной одному.

Пусть человек Ч$_2$ родился в день d_2 такого же года. Тогда этот день может совпасть или не совпасть с днем d_1, и вероятности наступления событий $D_2 = d_2$ ($d_2 = d_1$) и $D_2 = d_2$ ($d_2 \neq d_1$) будут следующими:

$$p(D_2 = d_2\ (d_2 = d_1)) = \frac{1}{365},\ p(D_2 = d_2\ (d_2 \neq d_1)) = \frac{365-1}{365} = \frac{364}{365}$$

и, следовательно, совместные вероятности наступления случайных событий $D_1 = d_1$ и $D_2 = d_2$ будут такими:

$$p(D_1 = d_1, D_2 = d_2\ (d_2 = d_1)) = p(D_1 = d_1) \cdot p(D_2 = d_2\ (d_2 = d_1)) = 1 \cdot \frac{1}{365} = \frac{1}{365},$$

$$p(D_1 = d_1, D_2 = d_2\ (d_2 \neq d_1)) = p(D_1 = d_1) \cdot p(D_2 = d_2\ (d_2 \neq d_1)) = 1 \cdot \frac{364}{365} = \frac{364}{365}.$$

Таким образом, вероятность совпадения дней рождения в группе из двух человек $p(2) = p(D_1 = d_1, D_2 = d_2\ (d_2 = d_1)) = \frac{1}{365}$, а вероятность несовпадения дней рождения в такой группе $\bar{p}(2) = p(D_1 = d_1,\ D_2 = d_2\ (d_2 \neq d_1)) = \frac{364}{365}$. Представим вышесказанное деревом, изображенным на рис. 1.2.

Естественно, что вероятность совпадения дней рождения $p(2)$ можно вычислить как разность числа один и вероятности несовпадения $\bar{p}(2)$:

$$p(2) = 1 - \bar{p}(2) = 1 - \frac{364}{365} = \frac{365}{365} - \frac{364}{365} = \frac{1}{365}.$$

Добавив к группе из двух человек третьего человека, получим группу из трех человек: Ч$_1$, Ч$_2$ и Ч$_3$.

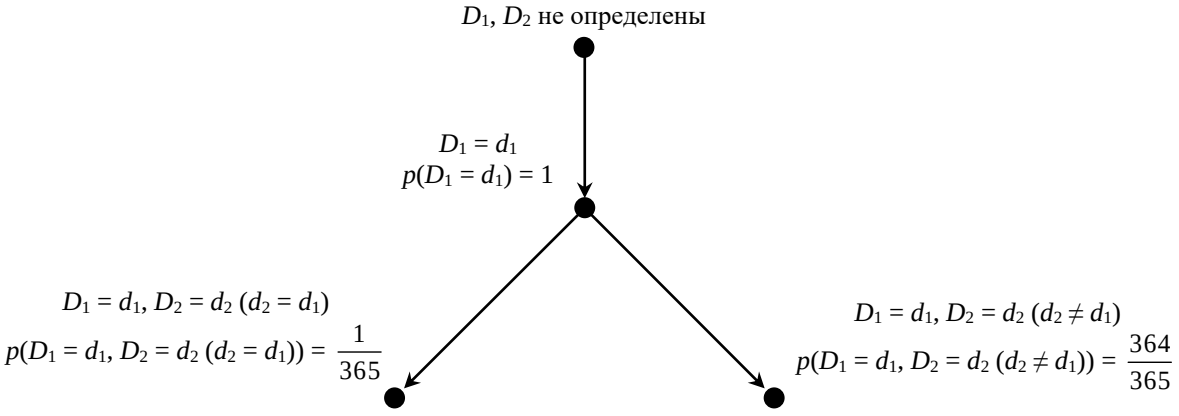


Рис. 1.2

Пусть человек Ч$_3$ родился в день d_3. Этот день d_3 может совпасть или не совпасть с днями d_1 и d_2, которые в свою очередь могут быть одинаковыми ($d_2 = d_1$) или разными ($d_2 \neq d_1$). Поэтому вероятности наступления событий $D_3 = d_3$ ($d_3 = d_2$, $d_2 = d_1$), $D_3 = d_3$ ($d_3 \neq d_2$, $d_2 = d_1$), $D_3 = d_3$ ($d_3 = d_2$, $d_2 \neq d_1$) и $D_3 = d_3$ ($d_3 = d_1$, $d_2 \neq d_1$) будут:

$$p(D_3 = d_3\ (d_3 = d_2,\ d_2 = d_1)) = \frac{1}{365},$$

$$p(D_3 = d_3\ (d_3 \neq d_2,\ d_2 = d_1)) = \frac{364}{365},$$

$$p(D_3 = d_3\ (d_3 = d_2,\ d_2 \neq d_1)) = \frac{1}{365},$$

$$p(D_3 = d_3\ (d_3 = d_1,\ d_2 \neq d_1)) = \frac{1}{365},$$

а совместные вероятности наступления случайных событий $D_1 = d_1$, $D_2 = d_2$ и $D_3 = d_3$, когда среди трех дней рождения, как минимум, два совпадают (см. рис. 1.3):

$$p(D_1 = d_1,\ D_2 = d_2\ (d_2 = d_1),\ D_3 = d_3\ (d_3 = d_2)) =$$
$$= p(D_1 = d_1) \cdot p(D_2 = d_2\ (d_2 = d_1)) \cdot p(D_3 = d_3\ (d_3 = d_2)) =$$
$$= 1 \cdot \frac{1}{365} \cdot \frac{1}{365} = \frac{1}{365} \cdot \frac{1}{365} = \frac{1}{365 \cdot 365},$$

$$p(D_1 = d_1,\ D_2 = d_2\ (d_2 = d_1),\ D_3 = d_3\ (d_3 \neq d_2)) =$$
$$= p(D_1 = d_1) \cdot p(D_2 = d_2\ (d_2 = d_1)) \cdot p(D_3 = d_3\ (d_3 \neq d_2)) =$$
$$= 1 \cdot \frac{1}{365} \cdot \frac{364}{365} = \frac{1}{365} \cdot \frac{364}{365} = \frac{364}{365 \cdot 365},$$

$$p(D_1 = d_1,\ D_2 = d_2\ (d_2 \neq d_1),\ D_3 = d_3\ (d_3 = d_2)) =$$
$$= p(D_1 = d_1) \cdot p(D_2 = d_2\ (d_2 \neq d_1)) \cdot p(D_3 = d_3\ (d_3 = d_2)) =$$
$$= 1 \cdot \frac{364}{365} \cdot \frac{1}{365} = \frac{364}{365} \cdot \frac{1}{365} = \frac{364}{365 \cdot 365},$$

$$p(D_1 = d_1,\ D_2 = d_2\ (d_2 \neq d_1),\ D_3 = d_3\ (d_3 = d_1)) =$$
$$= p(D_1 = d_1) \cdot p(D_2 = d_2\ (d_2 \neq d_1)) \cdot p(D_3 = d_3\ (d_3 = d_1)) =$$
$$= 1 \cdot \frac{364}{365} \cdot \frac{1}{365} = \frac{364}{365} \cdot \frac{1}{365} = \frac{364}{365 \cdot 365}.$$

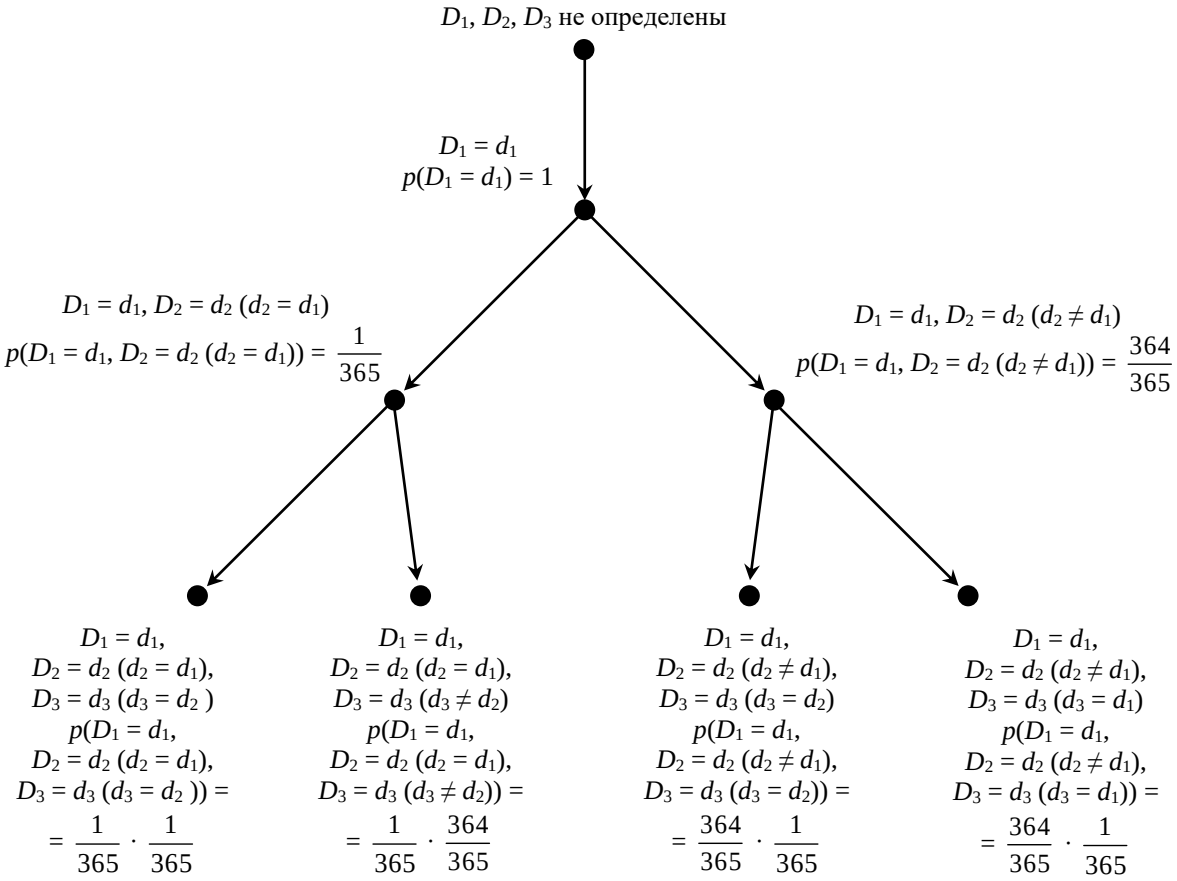


Рис. 1.3

Вычислим вероятность совпадения дней рождения хотя бы у двух людей в группе из трех человек:

$$p(3) = p(D_1 = d_1, D_2 = d_2\ (d_2 = d_1), D_3 = d_3\ (d_3 = d_2)) +$$
$$+ p(D_1 = d_1, D_2 = d_2\ (d_2 = d_1), D_3 = d_3\ (d_3 \neq d_2)) +$$
$$+ p(D_1 = d_1, D_2 = d_2\ (d_2 \neq d_1), D_3 = d_3\ (d_3 = d_2)) +$$
$$+ p(D_1 = d_1, D_2 = d_2\ (d_2 \neq d_1), D_3 = d_3\ (d_3 = d_1)) =$$
$$= \frac{1}{365 \cdot 365} + \frac{364}{365 \cdot 365} + \frac{364}{365 \cdot 365} + \frac{364}{365 \cdot 365} =$$
$$= \frac{1 + 364 + 364 + 364}{365 \cdot 365} = \frac{1 + 364 + 364 + 364}{365 \cdot 365} = \frac{1093}{365 \cdot 365}.$$

Заметим, что вероятность несовпадения дней рождения ни у каких двух людей в группе из трех человек:

$$\overline{p}(3) = p(D_1 = d_1, D_2 = d_2\ (d_2 \neq d_1), D_3 = d_3\ (d_2 \neq d_1, d_3 \neq d_2, d_3 \neq d_1)) =$$
$$= 1 \cdot \frac{364}{365} \cdot \frac{363}{365} = \frac{364 \cdot 363}{365 \cdot 365} = \frac{132\ 132}{365 \cdot 365}.$$

Естественно, ту же самую вероятность совпадения дней рождения хотя бы у двух людей в группе из трех человек $p(3)$ можно вычислить и как разность числа один и вероятности того, что у всех трех человек дни рождения будут разными $\bar{p}(3)$:

$$p(3) = 1 - \bar{p}(3) = 1 - \frac{132132}{365 \cdot 365} = \frac{365 \cdot 365 - 132132}{365 \cdot 365} =$$

$$= \frac{133225 - 132132}{365 \cdot 365} = \frac{1093}{365 \cdot 365}.$$

Поскольку определение вероятности совпадения дней рождения хотя бы у двух людей в группе из n человек прямым способом, особенно при больших значениях n, гораздо сложнее, чем через определение вероятности несовпадения, вероятность совпадения обычно определяют вторым способом. В общем случае (для произвольного n) вероятность того, что в группе из n человек все дни рождения будут различными вычисляется по формуле

$$\bar{p}(n) = 1 \cdot \frac{364}{365} \cdot \frac{363}{365} \cdot \ldots \cdot \frac{365 - n + 1}{365} =$$

$$= \frac{365}{365} \cdot \frac{365 - 1}{365} \cdot \frac{365 - 2}{365} \cdot \ldots \cdot \frac{365 - n + 1}{365} =$$

$$= \frac{365}{365} \cdot \frac{365 - 1}{365} \cdot \frac{365 - 2}{365} \cdot \ldots \cdot \frac{365 - (n-1)}{365} =$$

$$= \frac{365 \cdot (365 - 1) \cdot (365 - 2) \cdot \ldots \cdot (365 - (n-1))}{365^n} =$$

$$= \frac{365 \cdot (365 - 1) \cdot (365 - 2) \cdot \ldots \cdot (365 - (n-1)) \cdot (365 - n)!}{365^n \cdot (365 - n)!} =$$

$$= \frac{365!}{365^n \cdot (365 - n)!}. \qquad (1.97)$$

Тогда вероятность того, что хотя бы у двух из n человек дни рождения совпадут, равна:

$$p(n) = 1 - \bar{p}(n) = 1 - \frac{365!}{365^n \cdot (365 - n)!}. \qquad (1.98)$$

Разработанная программа *coincidences* на языке Си, которая вычисляет вероятность совпадения дней рождения хотя бы у двух людей в группе из n человек, приведена на листинге 1.3.

Листинг 1.3. Программа вычисления вероятности совпадения дней рождения хотя бы у двух людей в группе из *n* человек:

```
#include <stdio.h>
int main()
{
 int n; // Количество людей в группе
 double pn; // Вероятность совпадения дней рождения
 // хотя бы у двух из n человек
 double negation_pn; // Вероятность несовпадения дней рождения ни у каких
 // двух людей в группе из n человек
 int i; // Переменная цикла

 printf("n = ");
 scanf("%d",&n);
 negation_pn=1;
 for(i=2;i<=n;i++)
 {
 negation_pn*=(365.0-i+1)/365.0;
 }
 pn=1.0-negation_pn;
 printf("n=%d pn=%13.10lf%c",n,pn*100,'%');

 return 0;
}
```

Результаты расчетов по программе *coincidences* для некоторых значений *n* приведены в табл. 1.85.

Заметим, что наша задача определения вероятности несовпадения дней рождения ни у каких двух людей в группе из *n* человек является классической «задачей о совпадениях», если при этом использовать указанные в скобках альтернативные формулировки:

– в году содержится 365 дней (в урне с шарами находится 365 шаров);

– дни года пронумерованы числами от 1 до 365 (шары в урне пронумерованы числами от 1 до 365);

– рассматриваются дни рождения *n* человек (анализируется выборка *n* шаров из урны, при этом каждый выбранный шар возвращается в урну перед выбором следующего шара);

Таблица 1.85

Количество людей в группе n	Вероятность совпадения дней рождения хотя бы у двух из n человек $p(n)$, %
2	0,2739726027
3	0.8204165885
4	1.6355912467
10	11,6948177711
20	41,1438383581
22	47,5695307663
23	50,7297234324
24	53,8344257915
30	70,6316242719
50	97,0373579578
100	99,9999692751

– необходимо определить вероятность того, что у всех n человек дни рождения будут разными (вычислить вероятность события, заключающегося в отсутствии повторения номеров шаров в произведенной выборке из n шаров).

Вычисление вероятности события, заключающегося в отсутствии повторения номеров шаров в произведенной выборке из n шаров аналогично вычислению по формуле (1.97) вероятности того, что у всех n человек дни рождения будут разными.

Кроме того, задачу определения вероятности несовпадения дней рождения ни у каких двух людей в группе из n человек можно решить и с помощью комбинаторного подхода. Так, пусть каждый день года представляет некоторую букву из алфавита, состоящего из 365 символов. Тогда дни рождения людей в группе из n человек могут быть представлены строкой из n букв такого алфавита. По известной формуле из понятия хартлиевского количества информации число $m_{\text{общ}}$ всевозможных строк, состоящих из n букв алфавита мощности 365, равно:

$$m_{\text{общ}} = 365^n, \tag{1.99}$$

а количество строк $m_{\text{ун}}$, состоящих из n букв алфавита мощности 365, в которых буквы не повторяются:

$$m_{\text{ун}} = \frac{365!}{(365-n)!}. \tag{1.100}$$

Если строки, состоящие из n букв алфавита мощности 365, в которых буквы не повторяются, выбираются случайным образом, то вероятность выбора такой строки вычисляется по формуле

$$\bar{p}(n) = \frac{m_{\text{ун}}}{m_{\text{общ}}} = \frac{\frac{365!}{(365-n)!}}{365^n} =$$

$$= \frac{365}{365} \cdot \frac{365-1}{365} \cdot \frac{365-2}{365} \cdot \ldots \cdot \frac{365-n+1}{365} =$$

$$= \frac{365}{365} \cdot \frac{365-1}{365} \cdot \frac{365-2}{365} \cdot \ldots \cdot \frac{365-(n-1)}{365} =$$

$$= \frac{365 \cdot (365-1) \cdot (365-2) \cdot \ldots \cdot (365-(n-1))}{365^n} =$$

$$= \frac{365 \cdot (365-1) \cdot (365-2) \cdot \ldots \cdot (365-(n-1)) \cdot (365-n)!}{365^n \cdot (365-n)!} =$$

$$= \frac{365!}{365^n \cdot (365-n)!},$$

которая полностью совпадает с формулой (1.97).

Формулу (1.97) определения вероятности несовпадения дней рождения ни у каких двух людей в группе из n человек можно аппроксимировать с использованием разложения функции e^x в ряд Тейлора, более простой (приближенной) формулой

$$\bar{p}(n) \approx 1 \cdot e^{-1/365} \cdot e^{-2/365} \cdot \ldots \cdot e^{-(n-1)/365} =$$

$$= 1 \cdot e^{-(1+2+\ldots+(n-1))/365} = e^{-\frac{n(n-1)}{2 \cdot 365}}. \qquad (1.101)$$

Тогда вероятность того, что хотя бы у двух из n человек дни рождения совпадут:

$$p(n) = 1 - \bar{p}(n) \approx 1 - e^{-\frac{n(n-1)}{2 \cdot 365}}. \qquad (1.102)$$

Разработанная программа *approximation* на языке Си, которая вычисляет вероятность совпадения дней рождения хотя бы у двух людей в группе из n человек точно и приближенно по формуле (1.102), а также находит относительную погрешность приближенного значения вероятности, приведена на листинге 1.4.

Листинг 1.4. Программа вычисления вероятности совпадения дней рождения хотя бы у двух людей в группе из *n* человек, а также относительной погрешности приближенного значения вероятности:

```
#include <stdio.h>
#include <math.h>
int main()
{
 int n; // Количество людей в группе
 double pn; // Вероятность совпадения дней рождения
 // хотя бы у двух из n человек
 double negation_pn; // Вероятность несовпадения дней рождения ни у каких
 // двух людей в группе из n человек
 double pn_app; // Приближенная вероятность совпадения дней рождения
 // хотя бы у двух из n человек
 double negation_pn_app; // Приближенная вероятность несовпадения дней
 // рождения ни у каких двух людей в группе из n человек
 double eps; // Относительная погрешность приближенной вероятности
 // несовпадения дней рождения ни у каких двух людей
 // в группе из n человек
 int i; // Переменная цикла
 printf("n = ");
 scanf("%d",&n);
 negation_pn=1;
 for(i=2;i<=n;i++)
 {
 negation_pn*=(365.0-i+1)/365.0;
 }
 pn=1.0-negation_pn;
 negation_pn_app=exp((-n*(n-1))/(2.0*365.0));
 pn_app=1-negation_pn_app;
 eps=fabs(pn-pn_app)/pn;
 printf("n=%d pn=%8.5lf%c pn_app=%8.5lf%c eps=%7.5lf%c",
 n,pn*100,'%',pn_app*100,'%',eps*100,'%');
 return 0;
}
```

Результаты расчетов по программе *approximation* для некоторых значений *n* приведены в табл. 1.86.

Как видно из этой таблицы, относительная погрешность приближенной вероятности совпадения дней рождения хотя бы у двух людей в группе из $n \in \{2, 3, 4, 10, 20, 22, 23, 24, 30, 50, 100\}$ человек не превышает 1,46%.

Заметим, что и упрощенная аппроксимация вероятности совпадения дней рождения хотя бы у двух людей в группе из *n* человек:

$$p(n) = 1 - \bar{p}(n) \approx 1 - e^{-\frac{n^2}{2 \cdot 365}} \qquad (1.103)$$

достаточно точно представляет эту зависимость.

Программа *simplified_approximation* на языке Си, которая вычисляет вероятность совпадения дней рождения хотя бы у двух людей в группе из *n* человек точно и упрощенно приближенно по формуле (1.103), а также находит относительную погрешность приближенного значения вероятности, приведена на листинге 1.5.

Таблица 1.86

Количество людей в группе	Вероятность совпадения дней рождения, %	Приближенная вероятность совпадения дней рождения, %	Относительная погрешность приближенной вероятности, %
2	0,27397	0,27360	0,13686
3	0,82042	0,81855	0,22760
4	1,63559	1,63040	0,31749
10	11,69482	11,59907	0,81874
20	41,14384	40,58051	1,36916
22	47,56953	46,89381	1,42049
23	50,72972	50,00018	1,43811
24	53,83443	53,05363	1,45036
30	70,63162	69,63200	1,41526
50	97,03736	96,51313	0,54024
100	99,99997	99,99987	0,00010

Листинг 1.5. Программа вычисления вероятности совпадения дней рождения хотя бы у двух людей в группе из *n* человек, а также относительной погрешности упрощенного приближенного значения вероятности:

```
#include <stdio.h>
#include <math.h>
int main()
{
 int n; // Количество людей в группе
 double pn; // Вероятность совпадения дней рождения
 // хотя бы у двух из n человек
 double negation_pn; // Вероятность несовпадения дней рождения ни у
каких
 // двух людей в группе из n человек
 double pn_app; // Приближенная вероятность совпадения дней рожде-
ния
 // хотя бы у двух из n человек
 double negation_pn_app; // Приближенная вероятность несовпадения
дней
 // рождения ни у каких двух людей в группе из n человек
 double eps; // Относительная погрешность приближенной вероятности
 // несовпадения дней рождения ни у каких двух людей
 // в группе из n человек
 int i; // Переменная цикла
 printf("n = ");
 scanf("%d",&n);
 negation_pn=1;
 for(i=2;i<=n;i++)
 {
 negation_pn*=(365.0-i+1)/365.0;
 }
 pn=1.0-negation_pn;
 negation_pn_app=exp((-n*n)/(2.0*365.0));
 pn_app=1-negation_pn_app;
 eps=fabs(pn-pn_app)/pn;
 printf("n=%d pn=%8.5lf%c pn_app=%8.5lf%c eps=%7.5lf%c",
 n,pn*100,'%',pn_app*100,'%',eps*100,'%');
 return 0;
}
```

Результаты расчетов по программе *simplified_approximation* для тех же значений $n \in \{2, 3, 4, 10, 20, 22, 23, 24, 30, 50, 100\}$ приведены в табл. 1.87.

Как видно из этой таблицы, относительная погрешность упрощенной приближенной вероятности совпадения дней рождения хотя бы у двух людей в группе из n человек при достаточно больших значениях $n \in \{22, 23, 24, 30, 50, 100\}$ не превышает 1,9%.

Еще одна аппроксимация формулы (1.97) может быть основана на вероятности несовпадения дней рождения у двух человек, которая, как ранее отмечалось, равна $\frac{364}{365}$. Заметим, что в группе из n человек может быть образовано всего $C_n^2 = \frac{n!}{2!\cdot(n-2)!} = \frac{n(n-1)}{2}$ пар людей. При условии независимости событий, заключающихся в несовпадении дней рождения в парах людей, вероятность $\bar{p}(n)$ несовпадения дней рождения ни у каких двух людей в группе из n человек может быть аппроксимирована следующей зависимостью:

$$\bar{p}(n) \approx \left(\frac{364}{365}\right)^{C_n^2} = \left(\frac{364}{365}\right)^{\frac{n(n-1)}{2}}. \qquad (1.104)$$

Таблица 1.87

Количество людей в группе	Вероятность совпадения дней рождения, %	Упрощенная приближенная вероятность совпадения дней рождения, %	Относительная погрешность упрощенной приближенной вероятности, %
2	0,27397	0,54645	99,45305
3	0,82042	1,22531	49,35192
4	1,63559	2,16794	32,54753
10	11,69482	12,80178	9,46543
20	41,14384	42,18635	2,53381
22	47,56953	48,47040	1,89379
23	50,72972	51,55095	1,61883
24	53,83443	54,57198	1,37004
30	70,63162	70,85471	0,31584
50	97,03736	96,74396	0,30236
100	99,99997	99,99989	0,00008

Следовательно, искомым приближением для вероятности совпадения дней рождения хотя бы у двух людей в группе из n человек будет:

$$p(n) = 1 - \bar{p}(n) \approx 1 - \left(\frac{364}{365}\right)^{\frac{n(n-1)}{2}}. \qquad (1.105)$$

Разработанная программа *approximation*2 на языке Си, которая вычисляет вероятность совпадения дней рождения хотя бы у двух людей в группе из n человек точно и приближенно по формуле (1.105), а также находит относительную погрешность приближенного значения вероятности, приведена на листинге 1.6.

Листинг 1.6. Программа вычисления вероятности совпадения дней рождения хотя бы у двух людей в группе из n человек, а также относительной погрешности приближенного значения вероятности:

```
#include <stdio.h>
#include <math.h>
int main()
{
 int n; // Количество людей в группе
 double pn; // Вероятность совпадения дней рождения
 // хотя бы у двух из n человек
 double negation_pn; // Вероятность несовпадения дней рождения ни у
каких
 // двух людей в группе из n человек
 double pn_app; // Приближенная вероятность совпадения дней рожде-
ния
 // хотя бы у двух из n человек
 double negation_pn_app; // Приближенная вероятность несовпадения
дней
 // рождения ни у каких двух людей в группе из n человек
 double eps; // Относительная погрешность приближенной вероятности
 // несовпадения дней рождения ни у каких двух людей
 // в группе из n человек
 int i; // Переменная цикла
 printf("n = ");
 scanf("%d",&n);
```

```
 negation_pn=1;
 for(i=2;i<=n;i++)
 {
 negation_pn*=(365.0-i+1)/365.0;
 }
 pn=1.0-negation_pn;
 negation_pn_app=1;
 for(i=1;i<=n*(n-1)/2;i++)
 {
 negation_pn_app*=(364.0/365.0);
 }
 pn_app=1-negation_pn_app;
 eps=fabs(pn-pn_app)/pn;
 printf("n=%d pn=%8.5lf%c pn_app=%8.5lf%c eps=%7.5lf%c",
 n,pn*100,'%',pn_app*100,'%',eps*100,'%');
 return 0;
}
```

Результаты расчетов по программе *approximation*2 для некоторых значений *n* приведены в табл. 1.88.

Таблица 1.88

Количество людей в группе	Вероятность совпадения дней рождения, %	Приближенная вероятность совпадения дней рождения, %	Относительная погрешность приближенной вероятности, %
2	0,27397	0,27397	0
3	0,82042	0,81967	0,09124
4	1,63559	1,63262	0,18181
10	11,69482	11,61402	0,69085
20	41,14384	40,62295	1,26603
22	47,56953	46,93992	1,32357
23	50,72972	50,04772	1,34440
24	53,83443	53,10233	1,35991
30	70,63162	69,68163	1,34500
50	97,03736	96,52915	0,52373
100	99,99997	99,99987	0,00010

Как видно из этой таблицы, относительная погрешность приближенной вероятности совпадения дней рождения хотя бы у двух людей в группе из $n \in \{2, 3, 4, 10, 20, 22, 23, 24, 30, 50, 100\}$ человек не превышает 1,36%.

Таким образом, последняя из трех рассмотренных аппроксимаций (1.102), (1.103), (1.105) вероятности совпадения дней рождения хотя бы у двух людей в группе из $n \in \{2, 3, 4, 10, 20, 22, 23, 24, 30, 50, 100\}$ человек является наиболее точной.

Заметим, что парадокс дней рождения в общем виде применим к хеш-функциям, значениями которых могут быть равные хеш-коды на разных входных данных (возникновение так называемых коллизий). Атаки на криптографические хеш-функции, использующие рассматриваемый парадокс, называются атаками «дней рождения».

ЗАКЛЮЧЕНИЕ

Вторая часть учебного пособия по введению в криптологию посвящена изучению вопросов, связанных с дополнительными алгоритмами арифметики остатков, групп и конечных полей и элементами теории вероятностей.

Среди дополнительных алгоритмов арифметики остатков, групп и конечных полей рассмотрены: алгоритм Шэнкса для эффективного вычисления значения символа Лежандра; алгоритм вычисления значения символа Якоби; метод извлечения корня из числа по модулю составного числа.

В качестве элементов теории вероятностей, касающихся арифметики остатков, групп и конечных полей, обсуждены: понятие случайной величины; теорема Байеса; парадокс дней рождения, который может быть использован для организации атак на криптографические хеш-функции.

Надеемся, что изучение подробных примеров практически к каждому даваемому определению, понятию и алгоритму позволит студентам досконально разобраться с учебным материалом пособия и подготовиться к применению полученных знаний в профессиональной деятельности при решении различных прикладных задач.

Авторы планируют подготовку и издание других частей данного пособия, посвященных, в частности, эллиптическим кривым.

СПИСОК ЛИТЕРАТУРЫ

1. **Алгоритмические основы** эллиптической криптографии / А.А. Болотов и др. – М. : МЭИ, 2000. – 100 с.

2. **Василенко, О. Н.** Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

3. **Введение** в криптографию / под общ. ред. Ященко. – 4-е изд., доп. – М. : МЦМНО, 2012. – 348 с.

4. **Глухов, М. М.** Алгебра : учебник : в 2-х т. Т. I / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М. : Гелиос АРВ, 2003. – 336 с.

5. **Глухов, М. М.** Алгебра : учебник : в 2-х т. Т. II / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М. : Гелиос АРВ, 2003. – 416 с.

6. **Запечников, С. В.** Криптографические методы защиты информации / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – М. : Юрайт, 2019. – 309 с.

7. **Коблиц, Н.** Курс теории чисел и криптографии / Н. Коблиц : пер. с англ. – М. : Научное изд-во ТВП, 2001. – 254 с.

8. **Коробейников, А. Г.** Математические основы криптологии : учебное пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб. : СПб ГУ ИТМО, 2004. – 106 с.

9. **Нечаев, В. И.** Элементы криптографии (Основы теории защиты информации) : учебное пособие для ун-тов и пед. вузов / В. И. Нечаев ; под ред. В. А. Садовничего. – М. : Высшая школа, 1999. – 109 с.

10. **Новиков, В. Е.** Введение в криптологию : учебное пособие для студентов, специализирующихся в обл. защиты информ. / В. Е. Новиков, В. В. Ридель. – Саратов : Изд-во Сарат. ун-та, 2000. – 101 с.

11. **Основы** криптографии : учебное пособие / А. П. Алферов и др. – М. : Гелиос АРВ, 2001. – 480 с.

12. **Романьков, В. А.** Введение в криптографию. Курс лекций / В. А. Романьков. – М. : ФОРУМ, 2012. – 240 с.

13. **Ростовцев, А. Г.** Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – СПб. : НПО «ПРОФЕССИОНАЛ», 2004. – 485 с.

14. **Секей, Г.** Парадоксы в теории вероятностей и математической статистике / Г. Секей ; пер. с англ. – М. : Мир, 1990. – 240 с.

15. **Смарт, Н.** Криптография / Н. Смарт ; пер. с англ. – М. : Техносфера, 2005. – 528 с.

16. **Тилборг, ванн Х. К. А.** Основы криптологии. Профессиональное руководство и интерактивный учебник / Тилборг, ванн Х. К. А. – М. : Мир, 2006. – 471 с.

17. **Харин, Ю. С.** Математические основы криптологии : учебное пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. – Мн. : БГУ, 1999. – 319 с.

18. **Черемушкин, А. В.** Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. – М. : МЦНМО, 2002. – 104 с.

ОГЛАВЛЕНИЕ

Учебное электронное издание

КУЛАКОВ Юрий Владимирович
ДИДРИХ Валерий Евгеньевич
ДИДРИХ Ирина Валерьевна
ЕЛИСЕЕВ Алексей Игоревич
ШАХОВ Николай Гурьевич

ВВЕДЕНИЕ В КРИПТОЛОГИЮ

Учебное пособие

В четырех частях

Часть 2

Редактирование И. В. Калистратовой
Графический и мультимедийный дизайнер Т. Ю. Зотова
Обложка, упаковка, тиражирование И. В. Калистратовой

ISBN 978-5-8265-2666-8

Подписано к использованию 31.10.2023.
Тираж 50 шт. Заказ № 136

Издательский центр ФГБОУ ВО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14
Телефон 8(4752) 63-81-08
E-mail: izdatelstvo@tstu.ru