

АЛЕКСЕЙ ЮРЬЕВИЧ НЕСТЕРЕНКО

# ВВЕДЕНИЕ В СОВРЕМЕННУЮ КРИПТОГРАФИЮ

*Избранные вопросы алгоритмической теории чисел*

Москва

*в авторской редакции от 31 октября 2013 г.*

# ОГЛАВЛЕНИЕ

<b>Оглавление</b>	<b>2</b>
<b>1 Элементарная теория делимости</b>	<b>4</b>
1.1 Наибольший общий делитель . . . . .	5
1.2 Алгоритм Эвклида . . . . .	6
1.3 Простые числа . . . . .	10
<b>2 Сравнения</b>	<b>14</b>
2.1 Сравнения первой степени . . . . .	15
2.2 Китайская теорема об остатках . . . . .	19
2.3 Функция Эйлера . . . . .	23
2.4 Первообразные корни . . . . .	26
2.4.1 Первообразные корни по модулю простого числа $p$	28
2.4.2 Первообразные корни по модулю $p^\alpha$ . . . . .	34
2.5 Алгебраическое отступление . . . . .	37
<b>3 Многочлены</b>	<b>39</b>
3.1 Элементарные операции . . . . .	39
3.2 Алгоритм Эвклида для многочленов . . . . .	43
3.3 Основная теорема арифметики для многочленов . . . . .	46
3.4 Дифференцирование многочленов . . . . .	50
3.5 Решение сравнений по составному модулю . . . . .	51
<b>4 Сравнения старших степеней</b>	<b>56</b>
4.1 Квадратичные вычеты . . . . .	56
4.2 Символ Якоби . . . . .	64
4.3 Вычисление квадратного корня . . . . .	69
4.4 Вероятностный алгоритм вычисления корней многочленов	77
<b>5 Непрерывные дроби</b>	<b>82</b>
5.1 Конечные непрерывные дроби . . . . .	83
5.2 Понятие подходящей дроби . . . . .	84
5.3 Квадратичные иррациональности . . . . .	90
5.4 Иррациональности старших степеней . . . . .	101
5.5 Эквивалентность действительных чисел . . . . .	104
5.6 Наилучшие приближения . . . . .	109

<b>6</b>	<b>Простые числа</b>	<b>113</b>
6.1	Вероятностные тесты проверки простоты . . . . .	115
6.1.1	Тест Соловея-Штрассена . . . . .	119
6.1.2	Тест Миллера-Рабина . . . . .	122
6.2	$N - 1$ методы доказательства простоты . . . . .	127
6.3	Числа Мерсенна . . . . .	132
6.4	$N + 1$ метод доказательства простоты . . . . .	135
6.5	Алгоритмы построения простых чисел . . . . .	143
6.5.1	Рекурсивный алгоритм построения простых по известному разложению $p - 1$ . . . . .	143
6.5.2	Алгоритм построения сильно простого числа . . . . .	146
<b>7</b>	<b>Факторизация целых чисел</b>	<b>151</b>
7.1	Метод пробного деления . . . . .	151
7.2	Метод Ферма . . . . .	152
7.2.1	Вычисление квадратного корня . . . . .	153
7.2.2	Как быстро проверить, что число является полным квадратом . . . . .	154
7.3	Метод Лемана . . . . .	158
7.4	Метод Полларда-Флойда . . . . .	161
7.5	Метод Брента . . . . .	163
7.6	Методы факторизации чисел частного вида . . . . .	164
7.6.1	$p - 1$ метод Полларда . . . . .	165
7.6.2	$p + 1$ метод Вильямса . . . . .	166
7.6.3	Оптимизация алгоритмов Полларда и Вильямса . . . . .	168
7.6.4	Метод Женга . . . . .	174
<b>8</b>	<b>Факторизация целых чисел II</b>	<b>177</b>
8.1	Метод Крайчика . . . . .	178
8.2	Метод непрерывных дробей . . . . .	179
8.2.1	Первый вариант . . . . .	180
8.2.2	Второй вариант . . . . .	182
8.2.3	Метод Моррисона и Бриллхарта . . . . .	183
8.2.4	Как выбрать множитель $k$ . . . . .	185
8.2.5	Как выбрать квадратичную иррациональность . . . . .	188
8.2.6	Асимптотическая оценка сложности . . . . .	190
8.3	Метод линейного решета . . . . .	193
8.4	Метод квадратичного решета . . . . .	195
8.4.1	MPQS – метод нескольких многочленов . . . . .	197

<b>9</b>	<b>Дискретное логарифмирование</b>	<b>201</b>
9.1	Метод согласования . . . . .	203
9.2	Логарифмирование в подгруппе составного порядка . . . . .	205
9.3	Вероятностные методы . . . . .	210
9.3.1	Метод Полларда-Флойда . . . . .	210
9.3.2	Метод Госпера . . . . .	212
9.4	Субэкспоненциальный метод . . . . .	214
9.4.1	Идеология Крайчика . . . . .	215
9.4.2	Алгоритм Адлемана . . . . .	217
9.4.3	Решение систем линейных сравнений . . . . .	219
9.4.4	Асимптотическая оценка метода . . . . .	224
9.5	Двучленные сравнения . . . . .	225
<b>11</b>	<b>Схемы асимметричного шифрования</b>	<b>229</b>
11.1	Схема шифрования RSA. Теория . . . . .	230
11.1.1	Факторизация при известном значении $\varphi(m)$ . . . . .	232
11.1.2	Факторизация при известном значении $d$ . . . . .	232
11.1.3	Атака Винера на секретный ключ . . . . .	235
11.1.4	Случай использования общего модуля . . . . .	237
11.1.5	Случай использования малой экспоненты . . . . .	238
11.1.6	Метод итерационного шифрования . . . . .	239
11.1.7	Фиксированные точки . . . . .	239
11.1.8	Случай большого общего делителя . . . . .	241
11.1.9	Случай алгебраической зависимости открытых текстов . . . . .	242
11.1.10	Свойство мультипликативности и контроль целостности . . . . .	243
11.1.11	Семантическая стойкость . . . . .	244
11.2	Схема шифрования RSA. Практика . . . . .	245
11.2.1	RSAES: схема с добавлением случайного вектора . . . . .	247
11.2.2	RSA-OAEP: оптимальная асимметричная схема шифрования . . . . .	248
11.3	Схема шифрования Рабина . . . . .	252
11.3.1	Об эквивалентности задач факторизации и вычисления квадратного корня . . . . .	253
11.4	Схема шифрования Эль-Гамала . . . . .	254
<b>A</b>	<b>Случайные отображения</b>	<b>255</b>
A.1	Орбиты элементов . . . . .	255
A.2	Поиск длин циклов в последовательностях . . . . .	259

---

A.2.1	Алгоритм Флойда . . . . .	260
A.2.2	Алгоритм Брента . . . . .	260
A.2.3	Алгоритм Госпера . . . . .	263
A.2.4	Алгоритм Ниваша . . . . .	265
<b>В</b>	<b>Аналитические результаты</b>	<b>268</b>
В.1	Количественные оценки простых чисел . . . . .	268
В.2	Количественные оценки чисел с маленькими простыми делителями . . . . .	269
	<b>Литература</b>	<b>271</b>
	<b>Предметный указатель</b>	<b>275</b>

# ВВЕДЕНИЕ

Основная цель настоящего пособия заключается в изложении методов

# ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ДЕЛИМОСТИ

Операция деления, деление с остатком - Наибольший общий делитель, его свойства - Алгоритм Эвклида - Теорема Ламе - Двоичный алгоритм Эвклида - Простые числа - Основная теорема арифметики.

Мы начнем изложение с простейших вопросов и рассмотрим множество целых чисел

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Множество целых чисел образует кольцо относительно операций сложения и умножения. Введем на этом множестве операцию деления.

**Определение 1.1.** Пусть  $a, b$  целые числа. Мы будем говорить, что  $a$  делит  $b$  и использовать запись  $a|b$ , если найдется такое целое число  $d$ , что  $ad = b$ .

Хорошо известно, что операция деления не может быть определена для двух произвольных целых чисел  $a, b$ . Легко привести пример, например, число 3 не делит число 7, ибо нельзя найти целое число  $d$  такое, что  $3d = 7$ .

С другой стороны, мы можем ввести другую операцию — операцию деления с остатком, которая определена для любой пары целых чисел  $a, b$ . Нам потребуется следующая лемма.

**Лемма 1.1.** Пусть  $a, b$  целые числа, тогда существуют единственные целые числа  $q, r$  такие, что

$$b = aq + r, \quad 0 \leq r < |a|. \quad (1.1)$$

*Доказательство.* Без ограничения общности будем считать, что  $a > 0$ . Тогда найдется наибольшее целое число  $q$  такое, что  $aq \leq b$  и  $b < a(q+1)$ . Обозначая  $r = b - aq$ , получим неравенство  $0 \leq r < a$  и представление (1.1).

Допустим, что представление (1.1) не единственно. Тогда найдутся такие целые числа  $q_1, r_1$ , что выполнены равенства  $b = aq_1 + r_1$  и

$$aq + r = aq_1 + r_1.$$

Из последнего равенства следует, что  $a|(r_1 - r)$ . Из определения чисел  $r, r_1$  следует, что  $|r_1 - r| < a$ . Таким образом,  $r_1 - r = 0$  и  $r_1 = r$ ,  $q_1 = q$ . Лемма доказана.  $\square$

**Определение 1.2.** Пусть  $a, b$  целые числа. Мы будем называть целое число  $r$ ,  $0 \leq r < |a|$ , остатком от деления  $b$  на  $a$ , если выполнено представление (1.1) или, что аналогично,  $a|(b - r)$ .

## 1.1 Наибольший общий делитель

**Определение 1.3.** Мы будем называть натуральное число  $d$  наибольшим общим делителем двух целых чисел  $a, b$  если

1.  $d$  является общим делителем, то есть  $d|a$ ,  $d|b$ ;
2.  $d$  является наибольшим, то есть для любого общего делителя  $c$  выполнено  $c|d$ .

Мы будем обозначать наибольший общий делитель двух целых чисел  $a, b$  символом  $\text{НОД}(a, b)$ .

Легко видеть, что данное определение неоднозначно. Действительно, для каждого  $d > 0$ , удовлетворяющего определению 1.3, существует целое число  $-d$ , которое удовлетворяет первому и второму условию определения 1.3. Далее мы будем считать, что  $\text{НОД}(a, b) > 0$ .

**Определение 1.4.** Если наибольший общий делитель двух целых чисел  $a, b$  равен единице, то они называются взаимно простыми числами.

Приведем несколько свойств наибольшего общего делителя, которые будут использованы нами в дальнейшем.

**Лемма 1.2.** Пусть  $a, b$  и  $c$  целые числа. Выполнены следующие утверждения.

1.  $\text{НОД}(a, b) = \text{НОД}(b, a)$ ,
2.  $\text{НОД}(-a, b) = \text{НОД}(a, b)$ ,
3.  $\text{НОД}(a, a) = \text{НОД}(a, 0) = |a|$ ,
4.  $\text{НОД}(ac, bc) = |c| \cdot \text{НОД}(a, b)$ ,
5. Если  $\text{НОД}(a, c) = 1$ , то  $\text{НОД}(a, cb) = \text{НОД}(a, b)$ ,
6.  $\text{НОД}(a, b) = \text{НОД}(a \pm b, a)$ ,
7.  $\text{НОД}(a, b) = \text{НОД}(a, r)$ , где  $r$  остаток деления  $b$  на  $a$ .



*Доказательство.* Поскольку большинство утверждений леммы достаточно очевидно, мы докажем только последние два.

Пусть  $r$  остаток от деления числа  $b$  на  $a$  и, следуя лемме (1.1),  $b = aq + r$ , где  $0 \leq r < |a|$ . Обозначим  $d = \text{НОД}(a, b)$ , тогда найдутся такие целые числа  $k, l$ , что  $a = kd, b = ld$ . Следовательно,

$$a \pm b = d(k \pm l), \quad r = b - aq = d(l - kq)$$

и  $d$  является общим делителем чисел  $a, b, a \pm b, r$ . Покажем, что  $d$  наибольший делитель.

Пусть  $d_1$  является общим делителем чисел  $(a \pm b)$  и  $a$ . Тогда, что легко показать,  $d_1$  делит и  $b$ , то есть является общим делителем чисел  $a$  и  $b$  и, следовательно,  $d_1 | \text{НОД}(a, b) = d$  и  $d_1 \leq d$ .

Аналогично, пусть  $d_2$  является общим делителем чисел  $r$  и  $a$ . Тогда  $a = d_2k_2, r = d_2r_2$  и выполнено равенство  $b = qa + r = d_2(qa_2 + r_2)$ , из которого следует, что  $d_2 | b$ . Таким образом,  $d_2$  является общим делителем чисел  $a, b$  и  $d_2 | \text{НОД}(a, b) = d$  и  $d_2 \leq d$ .  $\square$

Если нам известны все общие делители чисел  $a$  и  $b$ , то вычисление наибольшего общего делителя не представляет труда: мы можем перебрать все делители и выбрать максимальный. Однако на практике нам неизвестны все общие делители. Более того, как мы покажем далее, задача поиска делителей значительно сложнее, чем вычисление наибольшего общего делителя.

Основываясь на утверждениях доказанной леммы, мы можем предъявить сразу несколько алгоритмов вычисления наибольшего общего делителя.

Вначале заметим, что из второго и третьего утверждения леммы 1.2 следует, что нам достаточно ограничиться только натуральными числами  $a, b$ . Читателю предлагается самостоятельно получить простейший алгоритм вычисления наибольшего делителя, который основывается на шестом утверждении леммы и использует только операцию вычитания натуральных чисел.

## 1.2 Алгоритм Эвклида

Мы же, основываясь на седьмом утверждении леммы 1.2, получим алгоритм, который принято называть алгоритмом Эвклида вычисления наибольшего общего делителя.

Будем считать, что  $b > a > 0$ . Используя деление с остатком, см. (1.1), определим  $r_{-1} = b, r_0 = a$  и последовательность

$$\begin{aligned}
b &= aq_1 + r_1, \\
a &= r_1q_2 + r_2, \\
r_1 &= r_2q_3 + r_3, \\
&\dots \\
r_{k-1} &= r_kq_{k+1} + r_{k+1}, \\
&\dots \\
r_{n-1} &= r_nq_{n+1}, \quad r_{n+1} = 0, \quad n \in \mathbb{N}.
\end{aligned} \tag{1.2}$$

**Теорема 1.1.** Пусть  $b > a > 0$  — целые числа. Определим последовательности  $r_{-1}, r_0, \dots, r_{n+1}$  и  $q_1, \dots, q_{n+1}$  равенствами (1.2). Тогда найдется такое натуральное число  $n$ , что  $r_{n+1} = 0$  и

$$r_n = \text{НОД}(a, b).$$

*Доказательство.* В силу леммы 1.1 для всех  $n = 0, 1, \dots$  выполнено равенство  $0 \leq r_{n+1} < r_n$ . Следовательно, члены последовательности  $r_{-1}, r_0, \dots$  убывают и найдется такой индекс, при котором последний остаток  $r_{n+1}$  окажется равным нулю.

Из седьмого и третьего утверждений леммы 1.2 следуют равенства

$$\text{НОД}(a, b) = \text{НОД}(r_1, a) = \dots = \text{НОД}(r_n, 0) = r_n$$

и утверждение теоремы. □

Вычисление последовательности остатков  $r_{-1}, r_0, \dots, r_{n+1}$  и является алгоритмом Эвклида. Мы можем минимизировать количество используемых вспомогательных переменных и переписать алгоритм Эвклида в виде, который может быть легко запрограммирован.

### Алгоритм 1.1 (Алгоритм Эвклида)

**Вход:** целые числа  $a, b$  такие, что  $b > a > 0$ .

**Выход:**  $\text{НОД}(a, b)$  — наибольший общий делитель чисел  $a$  и  $b$ .

1. Определить переменные  $r_{-1} = b, r_0 = a$ .

2. Пока  $r_0 > 0$  **выполнить**

2.1. Определить  $q = \left\lfloor \frac{r_{-1}}{r_0} \right\rfloor$ .

2.2. Определить  $r = r_{-1} - qr_0$  и присвоить  $r_{-1} = r_0, r_0 = r$ .

3. Определить  $\text{НОД}(a, b) = r_{-1}$ . □

Следующая теорема позволяет оценить число шагов алгоритма Эвклида.

**Теорема 1.2** (Ламе<sup>1</sup>, 1844). Пусть  $a, b$  целые числа и  $b > a > 0$ . Количество операций деления с остатком в алгоритме 1.1 может быть оценено сверху величиной  $1 + c \log_2 b$ , где  $c$  положительная, эффективно вычисляемая константа.

Для доказательства этой теоремы нам потребуется сделать небольшое отступление.

**Определение 1.5.** Мы будем называть рекуррентную последовательность целых чисел

$$\begin{aligned} A_0 &= 0, & A_1 &= 1, \\ A_{n+1} &= A_n + A_{n-1}, & \text{при } n &= 1, 2, \dots \end{aligned} \quad (1.3)$$

последовательностью Фибоначчи.

**Лемма 1.3.** Пусть  $z = \frac{1+\sqrt{5}}{2}$  действительный, положительный корень уравнения  $z^2 = z + 1$ . Тогда для последовательности Фибоначчи при всех натуральных  $n$  выполнено неравенство

$$A_{n+1} \geq z^{n-1}.$$

*Доказательство.* При  $n = 1$ , очевидно,  $A_2 = 1 > 0$  и утверждение леммы выполнено. Далее проведем доказательство по индукции. Пусть условие леммы выполнено для всех индексов, меньших либо равных  $n$ . Тогда, в силу выбора  $z$ , выполнено неравенство

$$A_{n+1} = A_n + A_{n-1} \geq z^{n-2} + z^{n-3} = z^{n-3}(z + 1) = z^{n-1}.$$

□

*Доказательство теоремы Ламе.* Вначале мы докажем неравенство

$$r_{k-1} \geq A_{n+1-k}, \quad \text{при } k = 0, 1, \dots, n, \quad (1.4)$$

где последовательность  $r_{-1}, r_0, \dots, r_n$  определена равенством (1.2), а последовательность Фибоначчи  $A_1, A_2, \dots$  равенством (1.3).

При  $k = n$  выполнено  $r_{n-1} = r_n q_{n+1} \geq 1 = A_1$ . Далее по индукции. Пусть для всех  $n, n-1, \dots, k$  неравенство (1.4) выполнено. Тогда

$$r_{k-1} = r_k q_{k+1} + r_{k+1} \geq r_k + r_{k+1} \geq A_{n-k} + A_{n-(k+1)} = A_{n+1-k}.$$

---

<sup>1</sup>Габриель Ламе (Gabriel Lamé) — французский математик, физик и инженер. В 1820—1832 гг. работал в Институте корпуса инженеров путей сообщения в Петербурге.

Из неравенства (1.4) и леммы 1.3 при  $k = 0$  получаем

$$b = r_{-1} \geq A_{n+1} \geq z^{n-1} \quad \text{или} \quad n \leq 1 + \log_z b.$$

Учитывая значение  $z = \frac{1 + \sqrt{5}}{2}$ , мы получаем неравенство

$$n \leq 1 + \frac{\log_2 b}{\log_2(1 + \sqrt{5})},$$

которое завершает доказательство теоремы.  $\square$

Использование вычислительных машин накладывает специфические требования к реализуемым на них алгоритмам. Хорошо известно, что операция деления целых чисел в общем случае выполняется на ЭВМ достаточно медленно. Тем не менее, в частном случае, когда целое число делится на двойку, операция деления может быть реализована в виде двоичного сдвига и выполняется очень быстро.

Этот факт привел к разработке некоторого класса алгоритмов, в которых операция деления на произвольное целое число заменяется операцией деления на двойку. Одним из ярких представителей подобного рода алгоритмов является бинарный алгоритм вычисления наибольшего общего делителя двух целых чисел  $a, b$ .

## Алгоритм 1.2 (Бинарный алгоритм вычисления НОД)

**Вход:** целые числа  $a, b$  такие, что  $b > a > 0$ .

**Выход:** НОД( $a, b$ ) – наибольший общий делитель чисел  $a$  и  $b$ .

1. Определить  $x = b, y = a, c = 1$ .
2. Пока  $2|x$  и  $2|y$  выполнить
  - 2.1. Определить  $c = 2c, x = \frac{x}{2}$  и  $y = \frac{y}{2}$ .
3. Пока  $x \neq y$  выполнить
  - 3.1. Если  $2|x$ , то определить  $x = \frac{x}{2}$  и вернуться на шаг 3.
  - 3.2. Если  $2|y$ , то определить  $y = \frac{y}{2}$  и вернуться на шаг 3.
  - 3.3. Если  $x > y$ , то определить  $x = \frac{x-y}{2}$  и вернуться на шаг 3.
  - 3.4. Если  $y > x$ , то определить  $y = \frac{y-x}{2}$  и вернуться на шаг 3.
4. Определить НОД( $a, b$ ) =  $cx$ .  $\square$

Корректность данного алгоритма основывается на четвертом и пятом утверждениях леммы 1.2. Согласно четвертому утверждению, на втором шаге алгоритма мы вычисляем целую константу  $c = 2^k$ , при некотором целом  $k \geq 0$ , такую, что  $c|a, c|b$  и НОД( $a, b$ ) =  $c \cdot \text{НОД}(x, y)$ , где  $a = cx, b = cy$ .

Поскольку  $x$  и  $y$  не могут быть одновременно четными, мы пользуемся либо пятым, либо шестым утверждением леммы 1.2 в зависимости от того делится  $x$  или  $y$  на двойку, либо  $x$  и  $y$  одновременно нечетные целые числа.

Для бинарного алгоритма вычисления наибольшего общего делителя не известен аналог теоремы Ламе, позволяющий точно оценить число делений на двойку. Вместе с тем, при каждом повторении второго или третьего шага алгоритма 1.2 либо  $x$ , либо  $y$  уменьшается вдвое. Таким образом, сложность бинарного алгоритма вычисления наибольшего общего делителя может быть оценена величиной  $O(\log_2 b)$ .

Нам также потребуется следующая лемма.

**Лемма 1.4.** Пусть  $a, b, u, v$  натуральные числа такие, что  $au = bv$  и  $\text{НОД}(a, b) = 1$ . Тогда  $a|v$  и  $b|u$ .

*Доказательство.* Рассмотрим частный случай  $a = b = 1$ . Очевидно, что для него утверждение леммы выполнено. Далее будем рассматривать случай  $a + b > 2$ .

Предположим, что для всех пар  $a, b$  таких, что  $\text{НОД}(a, b) = 1$  и  $a + b < k$ ,  $k > 2$ , утверждение леммы выполнено. Покажем, что оно выполнено и для пары  $a + b = k$ .

Так как  $\text{НОД}(a, b) = 1$ , то  $a \neq b$ . Далее, без ограничения общности, будем считать, что  $b > a > 0$ . Из равенства  $au = bv$  следует

$$(b - a)v = a(u - v).$$

Поскольку  $\text{НОД}(b - a, a) = 1$ , в силу шестого утверждения леммы 1.2, и  $(b - a) + a = b < k$ , то по предположению индукции  $a|v$  или, что равносильно, найдется целое  $v_1$  такое, что  $v = v_1 a$ . Таким образом, из равенства  $au = bv$  следует равенство  $au = bv_1 a$ . Сокращая на  $a \neq 0$ , получаем утверждение леммы.  $\square$

### 1.3 Простые числа

Простые числа играют основополагающую роль в криптографии. В этом разделе мы только сформулируем необходимые определения и докажем основную теорему арифметики. Позднее, мы посвятим изучению свойств простых чисел отдельную главу.

**Определение 1.6.** Натуральное число  $p > 1$  называется простым, если оно не имеет других натуральных делителей, отличных от 1 и самого себя.

Рассматривая ряд натуральных чисел, мы можем выделить в нем простые числа, а именно,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

Как мы покажем немного позже, этот ряд бесконечен.

**Определение 1.7.** *Натуральное число  $n$  называется составным, если оно имеет делитель, отличный от 1 и  $n$ .*

Из данного нами определения следует, что для составного числа  $n$  всегда найдутся такие натуральные числа  $a, b$ , что

$$n = ab \quad \text{и} \quad 1 < a < n, \quad 1 < b < n.$$

**Лемма 1.5.** *Наименьший, отличный от единицы натуральный делитель составного числа  $n > 1$  есть простое число.*

*Доказательство.* Рассмотрим множество всех делителей числа  $n$  и выберем в нем наименьший делитель  $q$ . Тогда  $q$  является простым числом. В противном случае существует натуральное число  $q_1$  такое, что  $q_1|q$ ,  $1 < q_1 < q$  и  $q_1|n$ . Но это противоречит тому, что  $q$  наименьший делитель числа  $n$ .  $\square$

Легко доказать следующую простую лемму.

**Лемма 1.6.** *Наименьший простой делитель  $p$  составного числа  $n > 1$  удовлетворяет неравенству  $p \leq \sqrt{n}$ .*

*Доказательство.* Пусть  $n = pt$ , где  $p$  наименьший простой делитель числа  $n$ , тогда  $n > t > p > 1$ . Если мы предположим, что  $p > \sqrt{n}$ , то будет выполнено неравенство  $n = pt > p^2 > (\sqrt{n})^2 = n$ , противоречащее утверждению леммы.  $\square$

Теперь мы докажем следующий результат, принадлежащий Эвклиду.

**Теорема 1.3** (Эвклид). *Множество простых чисел бесконечно.*

*Доказательство.* Предположим, что утверждение теоремы неверно и существует лишь конечное число простых чисел, скажем  $p_1, \dots, p_n$ .

Рассмотрим целое число  $N = p_1 \cdots p_n + 1$ . Число  $N$  не делится на цело ни на одно простое число  $p_1, \dots, p_n$ , так как остаток от деления отличен от нуля и равен единице. Тогда, либо число  $N$  простое, либо согласно лемме 1.5 у него есть наименьший простой делитель, отличный от  $p_1, \dots, p_n$ . Таким образом, мы нашли еще одно простое число, что противоречит нашему предположению.  $\square$

Следующая теорема позволяет говорить о том, что множество простых чисел служит базой для генерации множества всех целых чисел.

**Теорема 1.4** (Основная теорема арифметики). *Пусть  $n > 1$  натуральное число. Можно представить  $n$  в виде произведения простых сомножителей единственным образом, с точностью до перестановки сомножителей.*

*Доказательство.* Согласно лемме 1.5 число  $n$  имеет наименьший простой делитель  $p_1$  и выполнено равенство  $n = p_1 a_1$ . Если  $a_1 > 1$ , то применяя утверждение леммы к числу  $a_1$ , аналогично, получаем равенство  $a_1 = p_2 a_2$ , где  $p_2$  наименьший простой делитель числа  $a_1$ . Если  $a_2 > 1$ , то продолжаем далее.

Поскольку числа  $a_1, a_2, \dots$  убывают, то на некотором шаге  $k$  процесс прервется и будет выполнено равенство  $a_k = 1$ . Для каждого простого  $p_j$  выполнено  $p_j | n$ ,  $1 \leq j \leq k$ . Следовательно, для числа  $n$  выполнено равенство

$$n = p_1 \cdots p_k. \quad (1.5)$$

Докажем единственность представления (1.5). Для этого предположим, что существует другое разложение числа  $n$  в произведение простых сомножителей, а именно  $n = q_1 \cdots q_s$ . В этом случае выполнено равенство

$$p_1 \cdots p_k = q_1 \cdots q_s. \quad (1.6)$$

Будем считать, что  $s \geq k$ . В противном случае, мы можем поменять местами обозначения  $k$  и  $s$  местами.

В силу того, что все числа, входящие в произведение (1.6), являются простыми, то из утверждения леммы 1.4 следует, что либо  $p_1 = q_1$ , либо  $p_1 | q_2 \cdots q_s$ . Применяя лемму 1.4 последовательно к произведению  $q_j \cdots q_s$ ,  $2 \leq j \leq s$ , найдем такой индекс  $j$ , что  $p_1 = q_j$ . Переставляя множители  $q_j$  будем считать, что  $j = 1$  и  $p_1 = q_1$ .

Теперь, сокращая обе части равенства (1.6) на  $p_1 = q_1$ , получим

$$p_2 \cdots p_k = q_2 \cdots q_s.$$

Применяя к полученному равенству рассуждения, аналогичные приведенным выше, мы получим равенство  $p_3 \cdots p_k = q_3 \cdots q_s$  и так далее, до тех пор, пока не получим  $p_{s+1} \cdots p_k = 1$ .

В силу того, что все простые числа  $p_{s+1}, \dots, p_k$  больше единицы, то последнее равенство невозможно и мы получаем, что  $k = s$  и разложения в равенстве (1.6) совпадают.  $\square$

Перемножая в равенстве (1.5) одинаковые сомножители получим

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}, \quad r \in \mathbb{N}, \quad (1.7)$$

где  $p_i$  различные простые числа, а  $\alpha_i$  натуральные числа, кратности, с которыми простые числа входят в разложение (1.5).

**Определение 1.8.** *Полученное нами равенство (1.7) называется каноническим разложением натурального числа  $n > 1$  на простые сомножители.*

Задача определения для заданного натурального числа его канонического разложения на простые сомножители является одной из самых старых и хорошо известных задач теории чисел. Иногда эту задачу называют задачей факторизации натурального числа.

Для чисел большого размера решение задачи разложения на простые сомножители является сложным. Так, для разложения на множители одного натурального числа, имеющего в своей десятичной записи более 100 знаков, может потребоваться более шести месяцев непрерывных вычислений на ЭВМ. Именно высокая сложность решения задачи разложения на множители сделала ее привлекательной для применения в криптографических схемах и протоколах.



---

## СРАВНЕНИЯ

Вычеты по модулю целых чисел - Теорема о числе решений сравнения первой степени - Лемма Безу - Расширенный алгоритм Эвклида - Китайская теорема об остатках - Алгоритм Гарнера - Функция Эйлера - Теоремы Эйлера и Ферма - Первообразные корни - Теоремы о существовании первообразных корней по простому и составному модулям.

Введем одно из фундаментальных понятий в алгебре и теории чисел, а именно, понятие вычета по модулю целого числа.

**Определение 2.1.** Пусть  $a, b$  целые числа, и  $m > 0$  натуральное число. Мы будем говорить, что числа  $a$  и  $b$  сравнимы по модулю  $m$  и записывать  $a \equiv b \pmod{m}$ , если  $m \mid (a - b)$  или, что аналогично,  $a = b + km$  для некоторого целого значения  $k$ .

Из определения 2.1 следует, что решениями сравнения

$$x \equiv b \pmod{m}$$

являются все целые числа вида  $b + km$ , где  $k$  некоторое целое число. Данные числа образуют класс чисел по модулю  $m$ .

**Определение 2.2.** Любое число из класса  $b + km$ ,  $k \in \mathbb{Z}$ , мы будем называть вычетом по модулю числа  $m$ . Вычет  $x$ , удовлетворяющий неравенству  $0 \leq x < m$ , будем называть наименьшим неотрицательным вычетом.

Возьмем из каждого класса по модулю  $m$  по одному представителю – наименьшему неотрицательному вычету. Легко видеть, что таких вычетов всего  $m$  штук и все они различны.

**Определение 2.3.** Мы будем называть полной системой вычетов множество всех наименьших неотрицательных вычетов по модулю  $m$ .

В дальнейшем нам потребуется и другой способ определения представителей классов вычетов, основанный на величине абсолютного значения представителя.

**Определение 2.4.** Мы будем называть абсолютно-наименьшим вычетом по модулю числа  $m$  вычет  $x$ , если он удовлетворяет неравенству

$$1. \quad -\frac{m}{2} < x \leq \frac{m}{2} \text{ при четном } m;$$

$$2. \quad -\frac{m-1}{2} \leq x \leq \frac{m-1}{2} \text{ при нечетном } m.$$

**Определение 2.5.** Аналогично определению 2.3, мы будем называть полной системой абсолютно-наименьших вычетов – множество всех абсолютно-наименьших вычетов по модулю  $m$ .

## 2.1 Сравнения первой степени

Рассмотрим сравнение

$$ax \equiv b \pmod{m}. \quad (2.1)$$

Мы будем искать решения данного сравнения не в целых числах, а в вычетах по модулю  $m$ . Будем считать, что вычеты  $x$  и  $x_1$  различны, если они принадлежат разным классам вычетов. Верна следующая теорема.

**Теорема 2.1.** Пусть  $a, b$  целые числа и  $m > 0$  натуральное число. Тогда для числа решений  $N$  сравнения  $ax \equiv b \pmod{m}$  выполнены равенства

1.  $N = 1$ , если  $\text{НОД}(a, m) = 1$ ;
2.  $N = d$ , если  $\text{НОД}(a, m) = d$  и  $d|b$ ;
3.  $N = 0$ , в противном случае.

Прежде чем приступать к доказательству теоремы, сформулируем ряд вспомогательных утверждений.

**Лемма 2.1.** Пусть  $m > 0$  натуральное число и  $a, b$  целые числа для которых выполнено сравнение  $a \equiv b \pmod{m}$ .

1. Если  $\text{НОД}(c, m) = 1$ , то  $ac \equiv bc \pmod{m}$ ,
2. Пусть  $\text{НОД}(a, b) = d$  и  $d|m$ , тогда  $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ,
3. Если существует целое число  $c$  такое, что  $c|a$  и  $c|m$ , тогда  $c|b$ .

Доказательство утверждений достаточно просто и мы оставляем его в качестве упражнения.

*Доказательство теоремы 2.1.* Начнем доказательство с первого утверждения теоремы. Допустим, что выполнено условие  $\text{НОД}(a, m) = 1$  и существуют два решения  $x, x_1$  сравнения (2.1), тогда  $ax \equiv ax_1 \equiv b \pmod{m}$  или, что равносильно,  $ax = b + km, ax_1 = b + k_1m$  при некоторых целых  $k, k_1$ . Тогда  $a(x - x_1) = m(k - k_1)$  и, в силу леммы 1.4, выполнено условие  $m|(x - x_1)$ . Таким образом,  $x \equiv x_1 \pmod{m}$  и  $x, x_1$  принадлежат одному классу вычетов по модулю  $m$ .

Пусть  $\text{НОД}(a, m) = d$ , тогда из третьего утверждения леммы 2.1 следует, что  $d|b$ . В противном случае решений нет.

Определим целые числа  $a_1, b_1, m_1$  равенствами  $a = da_1, b = db_1$  и  $m = dm_1$ . Тогда согласно второму утверждению леммы 2.1 следует, что любое решение сравнения (2.1) удовлетворяет сравнению  $a_1x \equiv b_1 \pmod{m_1}$ , число решений которого, согласно первому утверждению теоремы, равно одному.

Пусть  $x_1$  решение сравнения  $a_1x \equiv b_1 \pmod{m_1}$ , тогда найдется целое число  $l$  такое, что  $a_1x_1 = b_1 + m_1l$ . Обозначим  $x = x_1 + m_1k$ , где  $k$  произвольное целое число, тогда из равенства

$$ax = da_1(x_1 + m_1k) = db_1 + dm_1l + dm_1k = b + m(l + k)$$

следует, что  $x$  удовлетворяет исходному сравнению  $ax \equiv b \pmod{m}$ . Поскольку число возможных значений  $k$ , позволяющих получить различные вычеты по модулю  $m$ , равно  $d$ , то и число решений исходного сравнения равно  $d$ .  $\square$

Для поиска решений сравнения  $ax \equiv b \pmod{m}$  предположим, для начала, что  $\text{НОД}(a, m) = 1$ , и рассмотрим вычет  $z$ , удовлетворяющий сравнению

$$az \equiv 1 \pmod{m}, \quad \text{НОД}(a, m) = 1. \quad (2.2)$$

Как следует из теоремы 2.1,  $z$  существует, единственен и решение  $x$  сравнения (2.1) определяется сравнением  $x \equiv zb \pmod{m}$ .

В случае, если  $\text{НОД}(a, m) = d$  мы можем рассмотреть сравнение

$$a_1z \equiv b_1 \pmod{m_1},$$

где

$$a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d}, \quad m_1 = \frac{m}{d}, \quad a_1, b_1, m_1 \in \mathbb{Z}, \quad \text{НОД}(a_1, m_1) = 1,$$

решение которого сводится к первому случаю. При этом, все решения сравнения (2.1) будут иметь вид

$$z + km_1, \quad k = 0, \dots, d - 1. \quad (2.3)$$

Действительно, подставляя в сравнение (2.1) равенство (2.3) получаем

$$\begin{aligned} a(z + km_1) &= d(a_1z + ka_1m_1) = d(b_1 + lm_1 + ka_1m_1) = \\ &= db_1 + (l + ka_1)m \equiv b \pmod{m}. \end{aligned}$$

при некотором натуральном  $l$ .

Так или иначе, но решение сравнения (2.1) сводится к решению сравнения  $az \equiv 1 \pmod{m}$ , где  $\text{НОД}(a, m) = 1$ . Верно следующее утверждение, авторство которого приписывается<sup>1</sup> французскому математику Этьену Безу (Etienne Bezout).

**Лемма 2.2** (Безу). Пусть  $a, m$  целые числа. Тогда найдутся такие целые  $z, w$ , что

$$az + mw = \text{НОД}(a, m). \quad (2.4)$$

Из утверждения леммы следует, что в случае  $\text{НОД}(a, m) = 1$ , выполнено

$$az + mw = 1 \quad \text{или} \quad az \equiv 1 \pmod{m}.$$

Заметим также, что решение уравнения (2.4) неоднозначно. Действительно, легко проверить следующий факт: если  $z_0, w_0$  некоторая пара целых чисел, удовлетворяющая равенству (2.4), то для любого целого значения  $k$  пара

$$z_k = z_0 - \frac{km}{\text{НОД}(a, m)}, \quad w_k = w_0 + \frac{ka}{\text{НОД}(a, m)}, \quad k \in \mathbb{Z}$$

также удовлетворяет равенству (2.4).

Мы приведем алгоритм поиска коэффициентов  $z, w$  в соотношении (2.4), который принято называть расширенным алгоритмом Эвклида. Из доказательства корректности данного алгоритма будет следовать корректность сформулированной нами леммы.

### Алгоритм 2.1 (Расширенный алгоритм Эвклида)

**Вход:** целые числа  $a, m$  такие, что  $m > a > 0$ .

**Выход:** целые числа  $z, w$  такие, что  $az + bw = \text{НОД}(a, b)$ .

1. Определить  $r_{-1} = m, r_0 = a, w_{-1} = 1, w_0 = 0, z_{-1} = 0, z_0 = 1$ .
2. Пока  $r_0 > 0$  выполнить

$$\text{2.1. Определить } q = \left\lfloor \frac{r_{-1}}{r_0} \right\rfloor.$$

<sup>1</sup>Впервые данное утверждение было доказано в 1624 году французским математиком Клодом Гаспаром Баше (Claude Gaspard Bachet) для случая взаимно простых чисел  $a$  и  $m$ . В конце 18-го века Этьен Безу обобщил утверждение, распространив его на кольцо многочленов, см. лемму 3.3.

- 2.2. Определить  $r = r_{-1} - qr_0$  и присвоить  $r_{-1} = r_0$ ,  $r_0 = r$ .  
 2.3. Определить  $z = z_{-1} - qz_0$  и присвоить  $z_{-1} = z_0$ ,  $z_0 = z$ .  
 2.4. Определить  $w = w_{-1} - qw_0$  и присвоить  $w_{-1} = w_0$ ,  $w_0 = w$ .  
 3. Определить **НОД**( $a$ ,  $m$ ) =  $r_{-1}$ ,  $z = z_{-1}$ ,  $w = w_{-1}$ . □

Докажем, что предложенный алгоритм корректно находит решение поставленной задачи.

**Теорема 2.2.** Пусть  $a$ ,  $m$  целые числа,  $m > a > 0$ . Алгоритм 2.1 позволяет находить целые числа  $z$ ,  $w$ , удовлетворяющие равенству

$$az + mw = \text{НОД}(a, m).$$

*Доказательство.* Алгоритм Эвклида вычисляет убывающую последовательность остатков  $r_{-1} = m$ ,  $r_0 = a$ , ...,  $r_n$ ,  $r_{n+1} = 0$ , связанных соотношением (1.2)

$$r_{k-1} - q_k r_k = r_{k+1}, \quad k = -1, 0, 1, \dots$$

Расширенный алгоритм Эвклида добавляет вычисление еще двух последовательностей  $\{z_n\}$  и  $\{w_n\}$ , удовлетворяющих равенству

$$az_k + mw_k = r_k, \quad k = -1, 0, \dots, n, \quad (2.5)$$

где

$$\begin{aligned} z_{k+1} &= z_{k-1} - q_k z_k, & z_{-1} &= 0, & z_0 &= 1, \\ w_{k+1} &= w_{k-1} - q_k w_k, & w_{-1} &= 1, & w_0 &= 0. \end{aligned} \quad (2.6)$$

Для  $k = -1, 0$  равенство (2.5) выполнено в силу выбора значений начальных  $z_{-1}$ ,  $z_0$ ,  $w_{-1}$ ,  $w_0$ . Предположим, что оно выполнено и для всех индексов, не превосходящих некоторого индекса  $k$ . Тогда

$$\begin{aligned} az_{k+1} + mw_{k+1} &= a(z_{k-1} - q_k z_k) + m(w_{k-1} - q_k w_k) = \\ &= az_{k-1} + mw_{k-1} - q(az_k + mw_k) = r_{k-1} - q r_k = r_{k+1}. \end{aligned}$$

Поскольку  $r_n = \text{НОД}(a, m)$ , то утверждение теоремы выполнено. □

Заметим, что в случае, когда мы хотим найти только решение сравнения (2.2), нам достаточно вычислять лишь последовательности  $\{r_k\}$   $\{w_k\}$ , не производя вычисления на шаге 2.3 алгоритма 2.1.

В дальнейшем мы будем использовать для вычета  $z$ , являющегося решением сравнения  $az \equiv 1 \pmod{m}$ , обозначение  $z \equiv a^{-1} \pmod{m}$ . Прежде чем двигаться дальше, обобщим лемму Безу на случай нескольких неизвестных.

**Лемма 2.3.** Пусть  $n \geq 2$  натуральное число и  $a_1, \dots, a_n$  произвольные целые числа. Тогда найдутся такие целые числа  $z_1, \dots, z_n$ , что

$$a_1 z_1 + \dots + a_n z_n = \text{НОД}(a_1, \dots, a_n).$$

*Доказательство.* Определим последовательность целых чисел  $d_1, \dots, d_n$  условиями

$$d_1 = a_1, \quad d_k = \text{НОД}(d_{k-1}, a_k), \quad \text{для всех } k = 2, \dots, n.$$

Тогда, очевидно, последний элемент  $d_n$  будет являться наибольшим общим делителем чисел  $a_1, \dots, a_n$ . С другой стороны, воспользовавшись алгоритмом 2.1 мы можем последовательно найти целые значения  $u_k$  и  $v_k$  удовлетворяющие равенствам

$$u_k d_{k-1} + v_k a_k = \text{НОД}(d_{k-1}, a_k) = d_k, \quad \text{для всех } k = 2, \dots, n.$$

Откуда получаем равенства

$$\begin{aligned} z_n &= v_n, \\ z_{n-1} &= u_n v_{n-1}, \\ z_{n-2} &= u_n u_{n-1} v_{n-2}, \\ &\dots \\ z_2 &= u_n u_{n-1} \dots u_3 v_2, \\ z_1 &= u_n u_{n-1} \dots u_3 u_2. \end{aligned}$$

Лемма доказана. □

## 2.2 Китайская теорема об остатках

Перейдем к рассмотрению систем сравнений и рассмотрим систему

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1}, \\ \dots \\ a_k x \equiv b_k \pmod{m_k}. \end{cases}$$

Используя описанную выше технику, мы можем независимо свести каждое уравнение этой системы к системе, в которой в левой части сравнения вместо коэффициентов будут стоять единицы. Для нахождения решения полученной системы может быть использована следующая теорема.

**Теорема 2.3** (Китайская теорема об остатках, 1247). Пусть  $k$  натуральное число и  $m_1, \dots, m_k$  целые, взаимно простые числа, произведение которых равно  $M = \prod_{j=1}^k m_j$ . Тогда любого набора целых чисел  $a_1, \dots, a_k$  решение системы сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots \\ x \equiv a_k \pmod{m_k}, \end{cases} \quad (2.7)$$

единственно по модулю  $M$  и удовлетворяет сравнению

$$x \equiv \sum_{i=1}^k a_i b_i c_i \pmod{M}, \quad (2.8)$$

где  $b_i = \frac{1}{m_i} \left( \prod_{j=1}^k m_j \right) = \frac{M}{m_i}$  и  $c_i \equiv b_i^{-1} \pmod{m_i}$ .

*Доказательство.* В силу выбора параметров  $b_i, c_i$  для каждого члена суммы, стоящей в правой части сравнения (2.8), выполнены сравнения

$$a_i b_i c_i \equiv a_i \pmod{m_i}, \quad a_i b_i c_i \equiv 0 \pmod{m_j}, \quad j \neq i, \quad i = 1, \dots, k,$$

из которых следует, что  $x$  удовлетворяет системе уравнений (2.7).

Покажем, что данное решение по модулю  $M$  единственно. Для этого предположим, что существует другое решение, скажем,  $y$ . Тогда выполнены сравнения  $x - y \equiv 0 \pmod{m_i}$  для  $i = 1, \dots, k$ , или

$$x - y = m_1 c_1 = m_2 c_2 = \dots = m_k c_k,$$

при некоторых целых значениях  $c_1, \dots, c_k$ . Поскольку все числа  $m_1, \dots, m_k$  взаимно просты, то применяя лемму 1.4, получаем, что  $m_i | c_j$  при всех  $i \neq j$ , что равносильно  $x - y \equiv 0 \pmod{M}$ . Последнее сравнение завершает доказательство теоремы.  $\square$

**Следствие 1.** Двум различным наборам чисел  $a_1, \dots, a_k$  и  $a'_1, \dots, a'_k$  соответствуют два различных решения  $x$  и  $x'$  системы (2.7).

*Доказательство.* Пусть наборы чисел  $a_1, \dots, a_k$  и  $a'_1, \dots, a'_k$  таковы, что найдется хотя бы один индекс  $j$ ,  $j = 1, \dots, k$  такой, что  $a_j \not\equiv a'_j \pmod{m_j}$ .

Определим, согласно (2.8), решения

$$x \equiv \sum_{i=1}^k a_i b_i c_i \pmod{M}, \quad x' \equiv \sum_{i=1}^k a'_i b_i c_i \pmod{M}$$

и предположим, что  $x \equiv x' \pmod{M}$ . Тогда для выбранного ранее индекса  $j$  будет выполнено  $m_j | M$  и, следовательно,  $x \equiv x' \pmod{m_j}$ . Последнее сравнение равносильно  $a_j \equiv a'_j \pmod{m_j}$ , что противоречит нашему предположению.  $\square$

Рассмотрим частный случай, который будет нам встречаться впоследствии несколько раз.

**Следствие 2.** Пусть для всех индексов  $i = 1, \dots, k$  выполнено неравенство  $a < m_i$ , тогда система сравнений

$$\begin{cases} x \equiv a \pmod{m_1}, \\ \dots \\ x \equiv a \pmod{m_k}, \end{cases}$$

имеет единственное решение  $x \equiv a \pmod{M = m_1 \cdots m_k}$ .

*Доказательство.* Очевидно, что  $x \equiv a \pmod{M}$  удовлетворяет указанной системе сравнений. В силу первого следствия, такое решение единственно.  $\square$

Утверждение теоремы 2.3 позволяет предложить следующий алгоритм вычисления вычета  $x \pmod{M}$ , удовлетворяющего системе сравнений (2.7).

## Алгоритм 2.2

**Вход:** целые числа  $k, m_1, \dots, m_k$  и  $a_1, \dots, a_k$ , удовлетворяющие теореме 2.3.

**Выход:** вычет  $x$ ,  $0 \leq x < M$  – решение системы сравнений (2.7).

1. Определить  $x = 0$ ,  $i = 1$  и  $M = \prod_{j=1}^k m_j$ .
2. Пока  $i \leq k$  **выполнить**
  - 2.1. Вычислить  $b = \frac{M}{m_i}$  и определить  $c \equiv b^{-1} \pmod{m_i}$ .
  - 2.2. Вычислить  $x \equiv x + a_i b c \pmod{M}$ .
  - 2.3. Определить  $i = i + 1$ .

3. Вернуть значение  $x$ .  $\square$

Остановимся на реализации шага 2.2. Нам надо добавить к текущему значению переменной  $x$  произведение  $a_i b c$ , для которого верна оценка сверху

$$0 \leq a_i b c < AM, \quad \text{где} \quad A = \max_{i=1, \dots, k} a_i.$$

После сложения, нам необходимо произвести операцию деления по модулю числа  $M$  и вычислить вычет  $x$ .



Поскольку операция приведения по модулю  $M$  является достаточно трудоемкой, мы приведем другой алгоритм восстановления значения  $x$  по множеству известных остатков  $a_1, \dots, a_k$ . Он основывается на следующей теореме.

**Теорема 2.4.** Пусть  $m_1, \dots, m_k$  целые, взаимно простые числа, произведение которых равно  $M = \prod_{j=1}^k m_j$ . Пусть  $x < M$  целое число, удовлетворяющее системе сравнений (2.7). Тогда найдутся такие целые  $x_1, \dots, x_k$ , что  $x_i < m_i$  для всех  $i = 1, \dots, k$  и

$$x = x_1 + x_2 m_1 + x_3 m_1 m_2 + \dots + x_k m_1 \cdots m_{k-1}. \quad (2.9)$$

*Доказательство.* Начнем с того, что определим константы  $b_1, \dots, b_k$  равенствами

$$b_1 = 1, \quad b_i = \prod_{j=1}^{i-1} m_j, \quad i = 2, \dots, k.$$

Теперь мы можем переписать равенство (2.9) в виде  $x = \sum_{i=1}^{k-1} x_i b_i$ . Введем еще один набор значений  $s_1, \dots, s_k$ , зависящий от величины  $x$  следующим образом:  $s_i = \sum_{j=1}^i x_j b_j$ , тогда  $x = s_k$  и

$$s_1 = x_1, \quad s_i = s_{i-1} + x_i b_i, \quad \text{для всех } i = 2, \dots, k. \quad (2.10)$$

Теперь мы можем определить величины  $x_1, \dots, x_k$  используя следующее рекуррентное соотношение

$$x_1 = a_1, \quad x_i \equiv b_i^{-1}(a_i - s_{i-1}) \pmod{m_i}, \quad \text{при } i = 2, \dots, k, \quad (2.11)$$

где величина  $b_i^{-1}$  определяется из сравнения  $b_i b_i^{-1} \equiv 1 \pmod{m_i}$ . Поскольку  $\text{НОД}(b_i, m_i) = 1$ , то данное определение величины  $b_i^{-1}$  корректно. Заметим, что, в силу определения, для коэффициентов  $x_i$  выполнены неравенства  $x_i < m_i$  для всех  $i = 1, \dots, k$ .

Изучая равенство (2.9), заметим, что для всех индексов  $i = 1, \dots, k$  выполнено сравнение  $x \equiv s_i \pmod{m_i}$ . Тогда из (2.10) и (2.11) получаем

$$x \equiv s_{i-1} + x_i b_i \equiv s_{i-1} + b_i^{-1}(a_i - s_{i-1}) b_i \equiv a_i \pmod{m_i},$$

и число  $x$  действительно удовлетворяет системе сравнений (2.7).

Нам осталось показать, что выполнено неравенство  $x < M$ . Для этого докажем, по индукции, что выполнено неравенство  $s_i < m_i b_i$  для любого индекса  $i = 1, \dots, k$ . Для  $s_1 = x_1 < m_1$  неравенство очевидно. Далее, пусть оно выполнено для всех индексов, меньших  $i$ . Тогда  $s_{i-1} < m_{i-1} b_{i-1} = b_i$  и

$$s_i = s_{i-1} + x_i b_i < b_i + (m_i - 1) b_i < m_i b_i.$$

Применяя полученное неравенство к индексу  $i = k$ , получаем, что  $x = s_k < m_k b_k = M$ . Теорема доказана.  $\square$

Основываясь на данной теореме, мы можем предложить эффективный алгоритм вычисления значения  $x$ . Отметим, что для случая  $k = 2$  описание алгоритма может быть найдено в книге Антона Казимировича Сушкевича [10]. Добавим, что в англоязычной и переводной литературе этот алгоритм, применительно к произвольному значению  $k$ , носит имя американского математика Харви Гарнера (Harvey L. Garner), см. [25].

### Алгоритм 2.3 (Алгоритм Гарнера)

**Вход:** целые числа  $k, m_1, \dots, m_k$  и  $a_1, \dots, a_k$ , удовлетворяющие теореме 2.3.

**Выход:**  $x, 0 \leq x < M$  – решение системы сравнений (2.7).

1. Определить  $i = 2, b = 1, s = a_1 \pmod{m_1}$ .
2. Пока  $i \leq k$  выполнить
  - 2.1. Определить  $b = b m_{i-1}$  и  $d \equiv b^{-1} \pmod{m_i}$ ,
  - 2.2. Вычислить  $x \equiv d(a_i - s) \pmod{m_i}$ ,
  - 2.3. Вычислить  $s = s + xb$  и положить  $i = i + 1$ .
3. Вернуть значение  $s$ .  $\square$

Основное преимущество алгоритма Гарнера заключается в том, что в нем вычисления производятся с числами, не превышающими величину модуля  $M$ . Более того, не требуется операция приведения по модулю  $M$ , которая заменена операциями приведения по модулю множителей  $m_i$ , входящих в разложение числа  $M$ .

## 2.3 Функция Эйлера

Рассмотрим целое неотрицательное число  $m$  и его полную систему вычетов

$$0, 1, \dots, m - 1.$$

Среди этого множества выберем вычеты, взаимно простые с  $m$ .

**Определение 2.6.** Множество вычетов по модулю  $m$ , взаимно простых с модулем  $m$ , называется приведенной системой вычетов. Мощность этого множества обозначается символом  $\varphi(m)$ . Функция целочисленного аргумента  $\varphi(m)$  называется функцией Эйлера.

Для вычисления значения функции Эйлера может быть использована следующая теорема.

**Теорема 2.5.** Пусть  $m$  натуральное целое число, для которого известно разложение на простые множители  $m = \prod_{i=1}^r p_i^{\alpha_i}$ ,  $p_i$  – простые числа. Тогда

$$\varphi(m) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}), \quad (2.12)$$

в частности, если  $p$  – простое, то

$$\varphi(p) = p - 1, \quad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

*Доказательство.* Если  $p$  простое число, то среди чисел  $0, 1, \dots, p-1$  взаимно простых с  $p$  ровно  $p-1$  в силу условия  $\text{НОД}(0, p) = p$  (см. третье утверждение леммы 1.2). Следовательно,  $\varphi(p) = p-1$ .

Пусть  $m = p^\alpha$  для некоторого целого  $\alpha > 1$ . Тогда для любого наименьшего неотрицательного вычета  $z$ ,  $0 \leq z < p^\alpha$ , выполнено либо равенство  $\text{НОД}(z, p^\alpha) = 1$ , либо условие  $p \mid \text{НОД}(z, p^\alpha)$ . Поскольку среди чисел  $0, 1, \dots, p^\alpha-1$  чисел кратных  $p$  ровно  $p^{\alpha-1}$ , то мы получаем, что  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ .

Для доказательства основного утверждения теоремы нам осталось доказать, что функция Эйлера мультипликативна, то есть для любых взаимно простых чисел  $a, b$  выполнено равенство

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Тогда подставляя в это равенство разложение  $m$  на множители, получим утверждение теоремы.

Пусть  $\alpha$  один из вычетов по модулю  $a$ , а  $\beta$ , соответственно, вычет по модулю  $b$ . Тогда согласно китайской теореме об остатках, теорема 2.3, существует единственный вычет  $\gamma \pmod{ab}$  такой, что

$$\gamma \equiv \alpha \pmod{a}, \quad \gamma \equiv \beta \pmod{b}.$$

В случае, если  $\alpha$  не взаимно просто с  $a$ ,  $\text{НОД}(\alpha, a) > 1$  или  $\beta$  не взаимно просто с  $b$ ,  $\text{НОД}(\beta, b) > 1$ , то мы сразу получаем, что  $\text{НОД}(\gamma, ab) > 1$ . И наоборот,  $\text{НОД}(\gamma, ab) = 1$  только тогда, когда  $\alpha$  и  $\beta$  взаимно просты, соответственно, с  $a$  и  $b$ .

Таким образом, мы получаем взаимно однозначное соответствие между двумя множествами – множеством взаимно простых вычетов по модулю  $ab$  и множеством вычетов по модулю  $a$  и  $b$ , следовательно,  $\varphi(ab) = \varphi(a)\varphi(b)$ . Теорема доказана.  $\square$

Вынося в равенстве (2.12) за скобки общий множитель  $m$ , мы получаем следующее соотношение.

**Следствие 1.** Для  $\varphi(m)$  выполнено равенство

$$\varphi(m) = m \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Функция Эйлера играет важнейшую роль не только в теории чисел, но и в криптографии. Ее применение основывается на следующей важной теореме.

**Теорема 2.6** (Теорема Эйлера). Пусть  $a, m > 0$  взаимно простые целые числа, то есть  $\text{НОД}(a, m) = 1$ . Тогда

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

*Доказательство.* Рассмотрим приведенную систему вычетов по модулю  $m$

$$1, \dots, m-1,$$

состоящую из  $\varphi(m)$  различных вычетов.

Домножим каждый из вычетов данной системы на  $a$  и получим то же самое множество вычетов, только записанное в другом порядке. Это позволяет нам получить равенство

$$(1)a \cdot \dots \cdot (m-1)a \equiv 1 \cdot \dots \cdot m-1 \pmod{p}.$$

Сокращая на множитель, стоящий в правой части сравнения, получим утверждение теоремы.  $\square$

Частным случаем теоремы Эйлера является хорошо известная малая теорема Ферма. Действительно, применяя утверждение теоремы 2.5, получим следующий результат.

**Теорема 2.7** (Малая теорема Ферма). Пусть  $p$  простое число и  $a$  целое, взаимно простое с  $p$  число. Тогда выполнено сравнение

$$a^{p-1} \equiv 1 \pmod{p}.$$

Еще одним следствием теоремы Эйлера может служить способ вычисления обратного элемента по модулю составного числа. Если числа  $a$  и  $m$  взаимно просты, то для вычисления  $a^{-1} \pmod{m}$  можно воспользоваться сравнением

$$a^{\varphi(m)} \equiv a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m},$$

откуда

$$a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}. \quad (2.13)$$

Вычисление по формуле (2.13) может быть использовано в тех ситуациях, когда не реализована операция деления с остатком, либо эта операция выполняется слишком медленно.

## 2.4 Первообразные корни

Рассмотрим вопросы, связанные с понятием первообразного корня целого числа.

**Определение 2.7.** Пусть  $a$  и  $m > 0$  целые взаимно простые числа. Мы будем называть показателем числа  $a$  по модулю  $m$  минимальное из целых чисел  $q$  таких, что  $a^q \equiv 1 \pmod{m}$ , и использовать обозначение

$$\text{ord}_m a = \min \{q \in \mathbb{Z}, q > 0 : a^q \equiv 1 \pmod{m}\}.$$

Из теоремы Эйлера (теорема 2.6) следует, что показатель числа  $a$  существует всегда, например, им может являться значение функции Эйлера.

**Лемма 2.4.** Пусть  $a, m > 0$  целые числа такие, что  $\text{НОД}(a, m) = 1$ , и показатель числа  $a$  по модулю  $m$  равен  $q$ . Тогда выполнены следующие условия

1. Числа  $1, a, a^2, \dots, a^{q-1}$  не сравнимы друг с другом по модулю  $m$ .
2. Если выполнено сравнение  $a^k \equiv a^l \pmod{m}$ , то  $k \equiv l \pmod{q}$ .
3. Пусть  $s$  натуральное число такое, что  $a^s \equiv 1 \pmod{m}$ , тогда  $q | s$ . В частности, показатель  $q$  делит значение  $\varphi(m)$  функции Эйлера.

*Доказательство.* Докажем первое утверждение леммы. Пусть найдутся такие показатели  $k$  и  $l$ ,  $0 \leq k < l < q$ , что  $a^k \equiv a^l \pmod{m}$ . Тогда из сравнения  $a^{l-k} \equiv 1 \pmod{m}$  и неравенства  $l - k < q$  получаем, что  $q$  не является показателем числа  $a$  и противоречие условию леммы.

Для доказательства второго утверждения леммы, используя деление с остатком (см. лемму 1.1), получим представления  $k = k_1 q + r_1$ , где  $0 \leq r_1 < q$  и  $l = l_1 q + r_2$ , где  $0 \leq r_2 < q$ .

Из сравнения  $a^k \equiv a^l \pmod{m}$  следует, что

$$a^{r_1} \equiv (a^q)^{k_1} a^{r_1} \equiv (a^q)^{l_1} a^{r_2} \equiv a^{r_2} \pmod{m}.$$

Поскольку  $r_1 < q$ ,  $r_2 < q$ , то из первого утверждения леммы следует равенство  $r_1 = r_2$  и доказательство второго утверждения.

Третье утверждение леммы является частным случаем второго. Действительно из сравнения

$$a^s \equiv 1 \equiv a^0 \pmod{m},$$

получаем, что  $s \equiv 0 \pmod{q}$  и  $s = cq$ , при некотором значении числа  $c$ , то есть  $q|s$ .  $\square$

Из утверждения леммы следует, что для каждого целого числа  $a$  его показатель по модулю числа  $m$  является делителем значения функции Эйлера  $\varphi(m)$ . Таким образом, множество всех возможных делителей числа  $\varphi(m)$  образует множество всех возможных значений показателей. Следующее определение задает класс чисел, имеющих максимально возможное значение показателя.

**Определение 2.8.** Пусть  $a, m > 0$  целые взаимно простые числа. Число  $a$  называется первообразным корнем по модулю  $m$ , если показатель  $a$  по модулю  $m$  равен  $\varphi(m)$ , то есть  $\text{ord}_m a = \varphi(m)$ .

Сделаем следующее замечание. В отечественной учебной литературе по криптографии термины «показатель числа» и «первообразный корень» не прижились. Обычно они заменяются их алгебраическими синонимами: «порядок элемента» и «примитивный элемент», вводимыми в случае, когда модуль  $m$  является простым числом.

**Определение 2.9.** Пусть  $p$  нечетное простое число и  $a$  целое число такое, что  $\text{НОД}(a, p) = 1$ . Тогда порядком числа  $a$  по модулю  $p$  называется показатель числа  $a$  по модулю  $p$ , то есть минимальное из чисел  $q$  таких, что  $a^q \equiv 1 \pmod{p}$

$$\text{ord}_p a = \min_{q>0} \{a^q \equiv 1 \pmod{p}\}.$$

Соответственно,  $a$  называется примитивным элементом по модулю  $p$ , если показатель числа  $a$  равняется  $p - 1$ , то есть  $a$  является первообразным корнем по модулю простого числа  $p$ .

Вопрос о существовании первообразных корней зависит от того, какой модуль  $m$  мы рассматриваем. Далее мы покажем, что первообразные корни существуют по модулю  $m = p^\alpha$  для некоторого нечетного простого числа  $p$  и  $\alpha \geq 1$ .

### 2.4.1 Существование первообразных корней по модулю простого числа $p$

Вначале мы сформулируем следующий результат.

**Теорема 2.8.** *Пусть  $p$  нечетное простое число, тогда найдется целое число  $a$ , являющееся первообразным корнем по модулю  $p$ .*

Перед доказательством теоремы мы исследуем ряд свойств первообразных корней по модулю простого числа  $p$ .

**Лемма 2.5.** *Пусть  $a, b$  целые числа,  $p$  простое число.*

1. *Если показатель числа  $a$  по модулю  $p$  равен  $xy$ ,  $\text{ord}_p a = xy$ , то выполнено  $\text{ord}_p a^x = y$ .*
2. *Если  $\text{ord}_p a = x$ ,  $\text{ord}_p b = y$  и  $\text{НОД}(x, y) = 1$ , то  $\text{ord}_p(ab) = xy$ .*

*Доказательство.* Докажем первое утверждение леммы. Предположим, что показатель числа  $a^x$  равен  $t$ , тогда  $(a^x)^t \equiv a^{xt} \equiv 1 \pmod{p}$ . Тогда, согласно второму утверждению леммы 2.4, выполнено  $xt \equiv xy \pmod{xy}$  или  $xt = xyc$  при некотором целом  $c$ . Сокращая на  $x$ , получим, что  $y|t$ .

С другой стороны, из сравнения  $1 \equiv a^{xy} \equiv (a^x)^y \pmod{p}$  следует, что  $y \equiv t \pmod{t}$ , следовательно,  $t|y$ . Таким образом,  $y = t$  и первое утверждение леммы доказано.

Пусть показатель элемента  $ab$  равен  $t$ , тогда

$$1 \equiv ((ab)^t)^x \equiv a^{tx} b^{tx} \equiv b^{tx} \pmod{p}.$$

Используя второе утверждение леммы 2.4, получим, что  $tx \equiv y \pmod{y}$  или  $tx = yc$  при некотором целом  $c$ . Поскольку  $\text{НОД}(x, y) = 1$ , то из леммы 1.4 получаем, что  $y|t$ . Аналогично, заменяя в предыдущей цепочке сравнений  $x$  на  $y$ , получаем, что  $x|t$  и  $xy|t$ .

С другой стороны, из второго утверждения леммы 2.4 и сравнения

$$(ab)^{xy} \equiv 1 \pmod{p}$$

получаем, что  $ab \equiv t \pmod{t}$  и  $t|xy$ , следовательно,  $xy = t$ . □

Введем понятие наименьшего общего кратного и докажем несколько свойств, которым оно удовлетворяет.

**Определение 2.10.** Пусть  $a, b$  натуральные, отличные от нуля числа. Наименьшим общим кратным мы будем называть наименьшее натуральное число  $m$  такое, что  $a|m$ ,  $b|m$ . Для обозначения наименьшего общего кратного мы будем использовать символ

$$\text{НОК}(a, b) = \min\{m \in \mathbb{N} : a|m, b|m\}.$$

Данное определение может быть обобщено на несколько целых чисел

$$\text{НОК}(a_1, \dots, a_k) = \min\{m \in \mathbb{N} : a_1|m, \dots, a_k|m\}.$$

**Лемма 2.6.** Верны следующие утверждения:

1. Любое общее кратное нескольких чисел  $a_1, \dots, a_k$  делится на их наименьшее общее кратное.
2. Наименьшее общее кратное взаимно простых чисел  $a_1, \dots, a_k$  равно их произведению, то есть  $\text{НОК}(a_1, \dots, a_k) = \prod_{i=1}^k a_i$ .
3. Если число  $b$  делится на каждое из попарно взаимно простых чисел  $a_1, \dots, a_k$ , то оно делится и на их произведение.

*Доказательство.* Начнем доказательство с первого утверждения леммы. Обозначим символом  $m = \text{НОК}(a_1, \dots, a_k)$ , а символом  $s$  – какое-нибудь произвольное общее кратное чисел  $a_1, \dots, a_k$ . Поскольку  $m$  наименьшее общее кратное, мы можем записать равенство

$$s = mq + r, \quad 0 \leq r < m,$$

где  $q, r$  некоторые натуральные числа. В силу определения общего делителя, находим, что  $r = s - mq$  делится на каждое из чисел  $a_1, \dots, a_k$  и, следовательно, является их общим делителем. Но поскольку мы предположили, что  $r < m$  и  $m$  – наименьший общий делитель, то данное свойство возможно только при  $r = 0$ . Первое утверждение доказано.

Согласно основной теореме арифметики, см. теорему 1.4, разложим  $a_1$  в произведение простых чисел  $a_1 = \prod_{i=1}^{k_1} p_i^{\alpha_i}$ . Каждое  $p_i^{\alpha_i}$  из этого произведения делит  $\text{НОК}(a_1, \dots, a_k)$ , в силу определения наименьшего общего кратного, но не делит остальные  $a_i$  при  $i > 1$ , в силу их взаимной простоты. Аналогичное свойство выполняется для всех  $a_i$ ,  $i = 2, \dots, k$ .

Таким образом,  $\prod_i^k a_i$  делит  $\text{НОК}(a_1, \dots, a_k)$ . Поскольку  $\prod_i^k a_i$  также является общим кратным чисел  $a_1, \dots, a_k$ , то второе утверждение леммы выполнено.



Третье утверждение леммы тривиально следует из двух первых. Действительно, из первого утверждения леммы следует, что  $b$  делится на  $\text{НОК}(a_1, \dots, a_k)$ , а в силу второго утверждения следует утверждение, поскольку  $\text{НОК}(a_1, \dots, a_k) = \prod_i^k a_i$ .  $\square$

Теперь мы можем перейти собственно к доказательству теоремы 2.8.

*Доказательство теоремы 2.8.* Для доказательства теоремы нам достаточно предъявить число  $a$ , показатель которого по модулю  $p$  равняется  $p - 1$ .

Пусть  $\{t_1, \dots, t_k\}$  множество различных показателей, которым принадлежат числа  $1, 2, \dots, p - 1$ . Определим  $\tau = \text{НОК}(t_1, \dots, t_k)$  и разложим его в произведение простых делителей

$$\tau = q_1^{\alpha_1} \cdots q_r^{\alpha_r}.$$

В силу определения наименьшего общего кратного для множителя  $q_1^{\alpha_1}$  найдется некоторый показатель  $t_i$ ,  $1 \leq i \leq k$ , такой, что  $q_1^{\alpha_1} | t_i$  или, что равносильно,  $t_1 = c_1 q_1^{\alpha_1}$  для некоторого целого  $c_1$ . Пусть  $a_1$  целое число, показатель которого равен  $t_i$ . Тогда из первого утверждения леммы 2.5 получаем, что показатель числа  $b_1 \equiv a_1^{c_1} \pmod{p}$  равен  $q_1^{\alpha_1}$ .

Выполняя аналогичные рассуждения далее, мы найдем для каждого простого делителя  $q_i$  числа  $\tau$  число  $b_i$  такое, что  $\text{ord}_p b_i = q_i^{\alpha_i}$  для всех  $i = 1, \dots, r$ .

Тогда, согласно второму утверждению леммы 2.5, показатель элемента  $b \equiv b_1 \cdots b_r \pmod{p}$  равен  $\tau$ . Из третьего утверждения леммы 2.4, получаем  $\tau | \varphi(p) = p - 1$ .

С другой стороны, в силу построения  $\tau$ , для любого индекса  $i$  выполнено  $t_i | \tau$ , следовательно, для каждого целого  $b$  из интервала  $1, \dots, p - 1$  найдется индекс  $i$  такой, что  $\text{ord } b = t_i$  и  $b^\tau \equiv 1 \pmod{p}$ . Отсюда мы выводим, что  $p - 1 | \tau$  и завершаем доказательство теоремы.  $\square$

Теперь мы знаем, что для нечетного простого числа  $p$  обязательно найдется первообразный корень. Протестировать, является ли заданное число  $a$  первообразным корнем по модулю  $p$ , позволяет следующая теорема.

**Теорема 2.9.** Пусть  $p$  нечетное простое число и  $a$  целое число, взаимно простое с  $p$ . Известно разложение числа  $\varphi(p) = p - 1$  на простые сомножители  $p - 1 = \prod_{i=1}^r q_i^{\alpha_i}$ , где  $q_1, \dots, q_r$  различные простые числа, а  $\alpha_1, \dots, \alpha_r$  натуральные числа.

Число  $a$  является первообразным корнем по модулю  $p$  тогда и только тогда, когда выполнены условия

$$a^{\frac{p-1}{q_1}} \not\equiv 1 \pmod{p}, \quad \dots, \quad a^{\frac{p-1}{q_r}} \not\equiv 1 \pmod{p}.$$

*Доказательство.* Если  $a$  первообразный корень по модулю  $p$ , то в силу определения первообразного корня, для любого  $c \mid \text{ord}_p a = \varphi(p) = p - 1$  выполнено  $a^{\frac{\text{ord}_p a}{c}} \not\equiv 1 \pmod{p}$ , следовательно, выполнено и утверждение теоремы.

Обратно, пусть для числа  $a$  выполнены условия теоремы и его показатель равен  $t$ . Тогда, из третьего утверждения леммы 2.4 следует, что найдется некоторое натуральное число  $c$  такое, что  $ct = p - 1 = \varphi(p)$ . Если  $c = 1$ , то показатель элемента  $a$  равен  $p - 1$ , то есть он является первообразным корнем.

Допустим, что это не так, тогда выполнено неравенство  $c > 1$ . Обозначим какой-нибудь простой делитель числа  $c$  символом  $q$ , тогда  $p - 1 = qut$  для некоторого целого числа  $u$  и выполнено сравнение

$$a^{\frac{p-1}{q}} \equiv (a^t)^u \equiv 1 \pmod{p},$$

что противоречит нашему предположению, поскольку мы предъявили простой делитель  $q$ , для которого не выполнено условие теоремы.  $\square$

**Пример 2.1.** Воспользуемся доказанной нами теоремой и покажем, что число  $a = 2$  является первообразным корнем по модулю простого числа  $p = 211$ . В начале, запишем разложение числа  $\varphi(211)$  на простые множители, а именно,

$$\varphi(211) = 210 = 2 \cdot 3 \cdot 5 \cdot 7.$$

Далее, вычислим вычеты

$$\begin{aligned} 2^{\frac{210}{2}} &\equiv 2^{105} \equiv -1 \pmod{211}, & 2^{\frac{210}{3}} &\equiv 2^{70} \equiv 196 \pmod{211}, \\ 2^{\frac{210}{5}} &\equiv 2^{42} \equiv 107 \pmod{211}, & 2^{\frac{210}{7}} &\equiv 2^{30} \equiv 171 \pmod{211}. \end{aligned}$$

Поскольку не один из вычисленных вычетов не является единицей, то, из утверждения теоремы 2.9, следует, что  $a = 2$  является первообразным корнем по модулю  $p = 211$ .

---

Оценить количество первообразных корней по модулю простого числа  $p$  нам поможет следующая теорема.

**Теорема 2.10.** Пусть  $p$  нечетное простое число и  $q$  натуральное число такое, что  $q|p-1$ . Тогда найдется вычет  $a$  по модулю  $p$  такой, что его показатель равен  $q$ .

Более того, показатель каждого вычета из множества

$$a^n \pmod{p} \quad \text{для всех} \quad 1 \leq n \leq q-1, \quad \text{НОД}(n, q) = 1, \quad (2.14)$$

равен  $q$  и других вычетов, показатель которых равен  $q$ , не существует.

*Доказательство.* Вначале покажем, что для любого натурального  $q$  такого, что  $q|p-1$  найдется вычет  $a$ , показатель которого равен  $q$ . В силу доказанной нами ранее теоремы 2.8 найдется вычет  $b$ , являющийся первообразным корнем по модулю  $p$ . Обозначим  $p-1 = qt$  тогда, в силу первого утверждения леммы 2.5, получаем, что вычет  $a \equiv b^t \pmod{p}$  имеет порядок, равный  $q$ .

Зафиксируем некоторое целое число  $n \neq 1$ , удовлетворяющее условию теоремы. Обозначим величиной  $l$  показатель элемента  $a^n$  по модулю  $p$ . Тогда выполнено сравнение

$$(a^n)^l \equiv a^{nl} \equiv 1 \pmod{p}$$

и, в силу третьего утверждения леммы 2.4, получаем, что  $q|nl$ . Поскольку для индекса  $n$  выполнено условие  $\text{НОД}(n, q) = 1$ , то  $q|l$ .

С другой стороны, поскольку выполнено сравнение

$$(a^n)^q \equiv (a^q)^n \equiv 1^n \equiv 1 \pmod{p}$$

и  $l$  является показателем вычета  $a^n$ , получаем, что  $l|q$ . Таким образом, выполнено равенство  $q = l$  и все вычеты, удовлетворяющие условию (2.14), также имеют показатель, равный  $q$ .

Для доказательства оставшегося утверждения теоремы рассмотрим сравнение

$$x^q - 1 \equiv 0 \pmod{p}. \quad (2.15)$$

Очевидно, что все вычеты, чьи показатели равны  $q$ , должны удовлетворять данному сравнению.

С другой стороны, согласно теореме 3.3<sup>2</sup>, доказательство которой мы приведем в следующей главе, сравнение (2.15) выполнено не более, чем для  $q$  различных значений неизвестной  $x$ . Все эти  $q$  значений содержатся среди вычетов

$$a^n \pmod{p} \quad \text{для всех} \quad n = 1, 2, \dots, q,$$

---

<sup>2</sup>Теорема 3.3 говорит о максимально возможном числе корней многочлена, её доказательство не зависит от материала, изложенного в данной главе.

поскольку для любого индекса  $n$  из указанного интервала следует сравнение  $(a^n)^q \equiv (a^q)^n \equiv 1 \pmod{p}$ . Следовательно, для доказательства теоремы нам осталось показать, что среди множества  $a^n \pmod{p}$  при  $n = 1, \dots, q$ , только элементы множества (2.14) имеют показатель, равный  $q$ .

Другими словами, нам надо показать, что если  $\text{НОД}(n, q) = d > 1$ , то показатель вычета  $a^n$  меньше  $q$ . Предположим обратное, тогда выполнено  $(a^n)^q \equiv 1 \pmod{p}$ . Введем величины  $u, w$  равенствами  $q = du$  и  $n = dw$ . Тогда, вспоминая, что  $a^q \equiv 1 \pmod{p}$ , получим сравнение

$$(a^n)^u \equiv (a^w)^{du} \equiv (a^q)^w \equiv 1^w \equiv 1 \pmod{p},$$

из которого вытекает противоречие нашему предположению. Действительно, при  $u < q$  величина  $q$  не может быть показателем вычета  $a^n$  по модулю  $p$ .  $\square$

Из доказанной теоремы следует, что количество вычетов, чей показатель равен  $q$  по модулю  $p$ , оценивается величиной  $\varphi(q)$ . В частном случае  $q = p - 1$  получаем следующий результат.

**Следствие 1.** *Количество первообразных корней по модулю  $p$  равно  $\varphi(p - 1)$ .*

Нам, потребуется еще одно следствие из доказанной теоремы.

**Следствие 2.** *Пусть  $p$  нечетное простое число и  $q$  натуральное число такое, что  $q \mid p - 1$ . Тогда количество вычетов, показатель которых  $d$  удовлетворяет условию  $d \mid q$ , равно  $q$ .*

*Доказательство.* Зафиксируем некоторый вычет  $a$ , показатель которого по модулю  $p$  равен  $q$  и рассмотрим множество вычетов

$$a^n \pmod{p}, \quad n = 1, \dots, q. \quad (2.16)$$

Согласно первому утверждению леммы (2.4), все вычеты несравнимы друг с другом по модулю  $p$ . Поскольку  $(a^n)^q \equiv (a^q)^n \equiv 1 \pmod{p}$ , то все вычеты, показатель которых делит  $q$ , содержатся во множестве (2.16).

Пусть  $d$  произвольный делитель  $q$ , тогда  $q = du$ . Определим вычет  $b \equiv a^u \pmod{p}$ . Легко видеть, что  $b^d \equiv a^{du} \equiv a^q \equiv 1 \pmod{p}$ . Поскольку величина  $ru$  не делит  $q$  для всех  $r = 1, \dots, d - 1$ , то выполнено условие  $b^r \equiv a^{ru} \not\equiv 1 \pmod{p}$ . Таким образом, показатель вычета  $b$  по модулю  $p$  равен  $d$ .

Согласно доказанной теореме 2.10 все вычеты, показатель которых равен  $d$ , имеют вид  $b^r \pmod{p}$  при  $r = 1, \dots, d$  и  $\text{НОД}(r, d) = 1$ .

Для каждого из таких вычетов выполнено сравнение

$$b^r \equiv a^{ru} \equiv a^n \pmod{p}, \quad \text{при } n = ru < q,$$

то есть принадлежит множеству (2.16). Утверждение леммы следует из произвольности выбора делителя  $d$ .  $\square$

Доказанные выше теоремы 2.9 и 2.10 позволяют нам не только привести алгоритм построения первообразного корня по модулю нечетного простого числа  $p$ , но и оценить вероятность его успешного завершения.

### Алгоритм 2.4 (Вычисление первообразного корня)

**Вход:** Целое число  $p$  и разложение значения  $p - 1 = \prod_{i=1}^k q_i^{\alpha_i}$  на простые сомножители.

**Выход:** Число  $a$  такое, что  $\text{ord}_p a = p - 1$ .

1. Выбрать случайно элемент  $a$ , удовлетворяющий неравенству  $1 \leq a < p$ .
2. Определить  $i = 1$ .
3. Пока  $i \leq k$  **выполнить**

**3.1.** Если  $a^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$ , то вернуться на шаг 1.

4. Вернуть значение  $a$ .  $\square$

При случайном выборе вычета  $a$  вероятность того, что он окажется первообразным корнем, равна  $\pi = \frac{\varphi(p-1)}{p-1}$ . Если нам известно полное разложение  $p - 1$  на простые сомножители, то есть  $p - 1 = \prod_{i=1}^k q_i^{\alpha_i}$ , то мы можем записать равенство

$$\pi = \frac{q_1^{\alpha_1-1}(q_1-1) \cdots q_k^{\alpha_k-1}(q_k-1)}{q_1^{\alpha_1} \cdots q_k^{\alpha_k}} = \prod_{i=1}^k \left(1 - \frac{1}{q_i}\right).$$

Полученное нами значение величины  $\pi$  близко к единице, следовательно, вероятность того, что случайный вычет  $a$  окажется первообразным корнем, достаточно велика.

### 2.4.2 Существование первообразных корней по модулю $p^\alpha$

Мы также можем доказать, что первообразные корни существуют по модулю составного числа  $m$ , являющегося степенью нечетного простого. Верна следующая теорема.

**Теорема 2.11.** Пусть  $p$  нечетное простое число, а целое число  $m$  удовлетворяет равенству  $m = p^\alpha$  для некоторого натурального  $\alpha > 1$ . Тогда найдется первообразный корень  $a$  по модулю  $p$  такой, что

$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

и  $a$  является первообразным корнем по модулю  $m$ .

*Доказательство.* Вначале найдем вычет  $a$ , удовлетворяющий условию теоремы. Рассмотрим произвольный первообразный корень  $a$  по модулю  $p$ . Тогда вычет  $b = a + p \equiv a \pmod{p}$  также является первообразным по модулю  $p$ .

Покажем, что один из вычетов  $a$  или  $b$  удовлетворяет условию теоремы. Вспомним формулу бинома Ньютона

$$(a + p)^n = \sum_{k=0}^n C_k^n a^{n-k} p^k, \quad \text{где} \quad C_k^n = \frac{n!}{k!(n-k)!} \quad (2.17)$$

и предположим, что наше утверждение не верно. Тогда выполнены сравнения  $a^{p-1} \equiv 1 \pmod{p^2}$  и  $(a + p)^{p-1} \equiv 1 \pmod{p^2}$ .

Вычитая первое сравнение из второго и используя формулу бинома Ньютона, получаем

$$\begin{aligned} 0 &\equiv (a + p)^{p-1} - a^{p-1} = \\ &= a^{p-1} + (p-1)a^{p-2}p + \frac{(p-1)(p-2)}{2}a^{p-3}p^2 + \dots + p^{p-1} - a^{p-1} \equiv \\ &\equiv (p-1)a^{p-2}p \equiv -a^{p-2}p \pmod{p^2}. \end{aligned}$$

Поскольку  $\text{НОД}(a, p) = 1$ , то последнее сравнение невозможно, следовательно, один из вычетов  $a$  или  $b$  удовлетворяет условию теоремы. Далее будем считать, что этим вычетом является  $a$ .

В завершение первой части доказательства заметим: поскольку  $a$  удовлетворяет условию теоремы, то выполнены условия  $a^{p-1} \equiv 1 \pmod{p}$  и  $a^{p-1} \not\equiv 1 \pmod{p^2}$ , из которых следует равенство

$$a^{p-1} = 1 + hp \quad (2.18)$$

для некоторого натурального  $h$ , взаимно простого с  $p$ .

Во второй части доказательства мы воспользуемся индуктивным подходом и покажем, что найденный нами вычет  $a$  является первообразным корнем для всех модулей

$$m = p^2, \quad \dots, \quad m = p^\alpha,$$

для произвольного значения  $\alpha \geq 2$ .

Для начала рассмотрим случай  $\alpha = 2$ . Пусть показатель вычета  $a$  по модулю  $p^2$  равен  $s$ , тогда  $a^s \equiv 1 \pmod{p^2} \equiv 1 \pmod{p}$  и мы получаем, что, в силу третьего утверждения леммы 2.4,  $p - 1 | s$ . С другой стороны, в силу той же леммы,  $s | \varphi(p^2) = p(p - 1)$ .

Мы получили два условия, из которых вытекает, что выполнено либо равенство  $s = p - 1$ , либо равенство  $s = p(p - 1)$ . Первое равенство не верно в силу выбора  $a$ , поскольку  $a^{p-1} \not\equiv 1 \pmod{p^2}$ . Следовательно, выполнено второе равенство  $s = p(p - 1) = \varphi(p^2)$  и  $a$  является первообразным корнем по модулю  $p^2$ .

Теперь сделаем индуктивный переход и предположим, что для всех значений  $m = p, p^2, \dots, p^{\alpha-1}$  вычет  $a$ , удовлетворяющий условию теоремы, является первообразным корнем. Обозначим  $s$  показатель вычета  $a$  по модулю  $p^\alpha$ , тогда  $a^s \equiv 1 \pmod{p^\alpha} \equiv 1 \pmod{p^{\alpha-1}}$ , следовательно,  $\varphi(p^{\alpha-1}) = p^{\alpha-2}(p - 1) | s$ .

С другой стороны, в силу леммы 2.4,  $s | \varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ . Мы снова получили, что величина  $s$  может принимать только два значения, а именно, либо  $s = \varphi(p^{\alpha-1})$ , либо  $\varphi(p^\alpha)$ .

Предположим, что показатель  $s$  удовлетворяет первому равенству, то есть выполнено сравнение  $a^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}$ . Тогда, учитывая (2.18), получаем

$$1 \equiv a^{\varphi(p^{\alpha-1})} \equiv (a^{p-1})^{p^{\alpha-2}} \equiv (1 + ph)^{p^{\alpha-2}} \equiv 1 + hp^{\alpha-1} \pmod{p^\alpha},$$

что равносильно  $hp^{\alpha-1} \equiv 0 \pmod{p^\alpha}$  или  $h \equiv 0 \pmod{p}$ . Последнее сравнение не выполняется в силу определения величины  $h$ . Таким образом, наше предположение о равенстве  $s = \varphi(p^{\alpha-1})$  неверно и выполнено равенство  $s = \varphi(p^\alpha)$ . Теорема доказана.  $\square$

Из утверждения теоремы 2.11 следует, что для модуля  $m = p^\alpha$  при  $\alpha > 1$  всегда существует первообразный корень. Для его нахождения необходимо воспользоваться алгоритмом 2.4 и выбрать произвольный первообразный корень  $a$  по модулю  $p$ . Если для  $a$  выполнены условия теоремы, то есть  $a^{p-1} \not\equiv 1 \pmod{p^2}$ , то он и будет первообразным корнем по модулю  $m$ . В противном случае, первообразным корнем будет величина  $b = a + p$ .

**Пример 2.2.** Построим первообразный корень по модулю  $m = 2197$ . Поскольку  $2197 = 13^3$ , то для начала найдем первообразный корень по модулю 13.

Выберем случайно  $a = 2$ . Поскольку выполнено равенство  $13 - 1 = 12 = 2^2 \cdot 3$ , нам достаточно проверить, что выполнены сравнения

$$2^{\frac{12}{2}} \equiv 12 \not\equiv 1 \pmod{13}, \quad 2^{\frac{12}{3}} \equiv 3 \not\equiv 1 \pmod{13}.$$

Следовательно, найденный нами вычет  $a = 2$  является первообразным корнем по модулю 13.

Поскольку выполнено сравнение  $a^{12} \equiv 40 \not\equiv 1 \pmod{13^2}$ , то вычет  $a$  является первообразным корнем по модулю  $2197 = 13^3$ .

## 2.5 Алгебраическое отступление

В отечественной литературе по криптографии наибольшее распространение получила терминология, пришедшая из алгебры, а не из теории чисел. В связи с этим, нам понадобится напомнить ряд определений, вводимых в курсе алгебры.

Зафиксируем натуральное число  $m > 0$  и рассмотрим полную систему вычетов по модулю  $m$

$$\mathbb{Z}_m = \{0, 1, \dots, m-1\}.$$

Данное множество является кольцом, поскольку на нем определены две операции – сложения и умножения, и при этом относительно операции сложения множество  $\mathbb{Z}_m$  образует группу. Мы не приводим доказательство сформулированного утверждения, поскольку оно носит технический характер и заключается в проверке всех аксиом определения кольца.

Мы будем называть элемент  $a \in \mathbb{Z}_m$  обратимым, если для него найдется такой элемент  $b \in \mathbb{Z}_m$ , что  $ab \equiv 1 \pmod{m}$ . Легко показать, что множество обратимых элементов образует группу  $\mathbb{Z}_m^* \subset \mathbb{Z}_m$  относительно операции умножения. Данную группу принято называть группой обратимых элементов.

Из леммы Безу, см. лемму 2.2, следует, что элемент является обратимым в том случае, когда он взаимно прост с модулем  $m$ . Таким образом, группа  $\mathbb{Z}_m^*$  состоит из элементов, взаимно простых с  $m$ , а ее порядок, то есть количество элементов в группе, равен  $\varphi(m)$ .

В случае, когда  $m = p$  простое число, мы получаем, что группа обратимых элементов совпадает со всем множеством ненулевых элементов кольца  $\mathbb{Z}_m$ . В этом случае, кольцо  $\mathbb{Z}_m$  удовлетворяет всем аксиомам поля. Мы будем называть это поле конечным, поскольку оно состоит из  $p$  элементов и обозначать его символом  $\mathbb{F}_p$ .



В случае, когда кольцо  $\mathbb{Z}_m$  является полем, его группа обратимых элементов, традиционно, называется мультипликативной группой поля и обозначается символом  $\mathbb{F}_p^*$

$$\mathbb{F}_p^* = \{1, 2, \dots, p-1\}.$$

Существует другой способ построения мультипликативной группы поля  $\mathbb{F}_p^*$ . Поскольку  $p$  простое число, то согласно теореме 2.8, найдется  $a$  – первообразный корень по модулю  $p$ . Тогда, согласно определению первообразного корня, каждый элемент из  $\mathbb{F}_p^*$  может быть представлен в виде некоторой степени элемента  $a$ , а сама группа имеет вид

$$\mathbb{F}_p^* = \langle a \rangle = \{a, a^2 \pmod{p}, \dots, a^{p-1} \pmod{p}\},$$

то есть является циклической. Все подгруппы мультипликативной группы поля являются циклическими и имеют порядок, делящий  $p-1$ . Доказательство этого факта хорошо известно и может быть найдено, например, в [6, гл.4, § 3].

В криптографических приложениях наиболее востребованными являются циклические группы, поэтому либо мультипликативная группа поля, либо ее подгруппы простого порядка являются подходящим материалом для реализации криптографических приложений. Более подробно мы поговорим об этом в следующих главах.

# МНОГОЧЛЕНЫ

Определение элементарных операций - Алгоритмы умножения многочленов - Операция деления с остатком - Алгоритм Эвклида - Лемма Безу - Основная теорема арифметики для многочленов - Теорема о числе корней многочленов - Дифференцирование многочленов - Полиномиальные сравнения по составному модулю - Теоремы о подъеме решений.

Формализуем наши знания о многочленах: введем формальное понятие многочлена от одной переменной, определим для многочленов операции сложения, умножения и деления с остатком, покажем, что для многочленов также можно доказать теорему об однозначном разложении на множители.

## 3.1 Элементарные операции

Мы будем обозначать символом  $\mathbb{U}$  произвольное коммутативное кольцо с единицей. В качестве примеров таких колец можно рассмотреть кольцо целых чисел  $\mathbb{Z}$ , кольцо  $\mathbb{Z}_m$  вычетов по модулю целого числа  $m$ . Поскольку поля также являются и кольцами, то в качестве кольца  $\mathbb{U}$  мы будем рассматривать поля рациональных чисел  $\mathbb{Q}$ , действительных чисел  $\mathbb{R}$ , а также конечное поле  $\mathbb{F}_p$

$$\mathbb{F}_p = \{0, 1, \dots, p-1, \quad p - \text{простое}\},$$

которое образует полная система вычетов по модулю простого числа  $p$ . Доказательство того факта, что множество  $\mathbb{F}_p$  действительно образует поле, заключается в проверке всех аксиом и вытекает из результатов предыдущей главы.

**Определение 3.1.** Пусть  $\mathbb{U}$  произвольное коммутативное кольцо с единицей,  $a, b$  – ненулевые элементы кольца  $\mathbb{U}$ .

Мы будем говорить, что  $a$  делит  $b$  и использовать обозначение  $a|b$  или  $b \equiv 0 \pmod{a}$ , если в кольце  $\mathbb{U}$  найдется такой элемент  $d$ , что  $ad = b$ . Элемент  $a$  мы будем называть делителем числа  $b$ .

Очевидно, что для кольца целых чисел  $\mathbb{Z}$  это определение совпадает с введенным ранее определением 1.1.

**Определение 3.2.** Мы будем называть элемент  $\varepsilon$  кольца  $\mathbb{U}$  обратимым, если он является делителем единицы, то есть для него найдется некоторый элемент  $\varepsilon^{-1}$  того же кольца такой, что  $\varepsilon\varepsilon^{-1} = 1$ . Для обозначения обратного элемента мы также будем использовать обозначение  $\frac{1}{\varepsilon}$ .

Относительно операции умножения обратимые элементы образуют группу. Действительно, если  $a, b$  два обратимых элемента кольца  $\mathbb{U}$ , то существуют элементы  $a^{-1}, b^{-1} \in \mathbb{U}$  такие, что  $aa^{-1} = bb^{-1} = 1$ . Тогда, в силу коммутативности кольца  $\mathbb{U}$ , получаем равенство

$$1 = aa^{-1} \cdot bb^{-1} = ab \cdot a^{-1}b^{-1},$$

из которого следует, что элемент  $ab$  также является обратимым.

В кольце целых чисел  $\mathbb{Z}$  существует всего два обратимых элемента 1 и  $-1$ , которые также содержатся и в любом другом кольце. Произвольные кольца могут содержать более двух обратимых элементов, например, в поле все отличные от нуля элементы обратимы.

Обратимый элемент  $\varepsilon$  делит любой элемент кольца  $\mathbb{U}$ . Действительно, для любого элемента  $a$  выполнено равенство  $a = \varepsilon b$ , где  $b = a\varepsilon^{-1}$ .

**Пример 3.1.** Рассмотрим кольцо вычетов  $\mathbb{Z}_{15}$ . Тогда группа его обратимых элементов состоит из следующих вычетов

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Из леммы Безу, см. лемму 2.2, следует, что обратимыми элементами являются только вычеты, взаимно простые с модулем. Количество таких чисел определяется значением функции Эйлера  $\varphi(15)$  и, согласно теореме 2.5, равно 8.

Дадим несколько важных определений и введем понятие кольца многочленов от одной переменной  $\mathbb{U}[x]$ , которое будет многократно использовано нами в дальнейшем.

**Определение 3.3.** Пусть  $\mathbb{U}$  произвольное коммутативное кольцо с единицей и  $n \geq 0$  целое число. Многочленом  $a(x)$  от одной переменной  $x$  мы будем называть сумму

$$a(x) = \sum_{k=0}^n a_k x^k, \quad a_n \neq 0. \quad (3.1)$$

Величины  $a_0, \dots, a_n \in \mathbb{U}$  мы будем называть коэффициентами многочлена, коэффициент  $a_n$  – старшим коэффициентом.

При некотором фиксированном значении  $x \in \mathbb{U}$  значение многочлена  $a(x)$  мы будем называть значение выражения (3.1), принадлежащее кольцу  $\mathbb{U}$ .

Целое число  $n$  мы будем называть степенью многочлена и обозначать символом  $\deg a(x) = n$ . Многочлены степени один мы будем называть линейными.

Как следует из данного нами определения, все элементы кольца  $\mathbb{U}$  могут рассматриваться как многочлены нулевой степени. Это утверждение неверно лишь для нуля, ибо у него всегда выполнено  $a_n = 0$ . Поэтому мы будем дополнительно считать, что  $\deg 0 = -1$ .

**Определение 3.4.** Многочлен  $a(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ , старший коэффициент которого равен единице, называется унитарным<sup>1</sup>.

Далее мы будем обозначать символом  $\mathbb{U}[x]$  множество многочленов от одной переменной  $x$  с коэффициентами из кольца  $\mathbb{U}$ . Пусть

$$a(x) = \sum_{k=0}^n a_k x^k, \quad b(x) = \sum_{k=0}^m b_k x^k$$

два произвольных многочлена. Без ограничения общности будем считать, что  $m \geq n$ . Определим их сумму равенством

$$a(x) + b(x) = \sum_{k=0}^m (a_k + b_k) x^k,$$

где коэффициенты  $a_{n+1}, \dots, a_m$  полагаются равными нулю. Легко видеть, что  $\deg(a(x) + b(x)) \leq \max\{\deg a(x), \deg b(x)\}$ . Знак «меньше» возникает в том случае, когда сумма старших коэффициентов равна нулю.

Определим произведение многочленов равенством

$$a(x) \cdot b(x) = \sum_{k=0}^{n+m} c_k x^k, \quad \text{где} \quad c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, \dots, n+m,$$

также выполнено равенство  $\deg a(x)b(x) = \deg a(x) + \deg b(x)$ .

<sup>1</sup>В русскоязычных изданиях нет устоявшегося названия для данного многочлена. В литературе по теории чисел традиционно используется понятие *примитивного* многочлена, в пособиях по алгебре – понятия *унитарного*, *нормированного* или *приведенного* многочлена.

Введенные нами операции позволяют определить на множестве  $\mathbb{U}[x]$  структуру коммутативного кольца, единица и ноль которого совпадают с единицей и нулем кольца  $\mathbb{U}$ . Доказательство этого утверждения проводится проверкой всех свойств, которым должно удовлетворять кольцо.

Мы будем говорить, что многочлен

$$a(x) = \sum_{k=0}^n a_k x^k$$

делит многочлен  $b(x)$ , если для некоторого многочлена  $u(x) \in \mathbb{U}[x]$  выполнено равенство  $a(x)u(x) = b(x)$ . Исходя из определения операции умножения многочленов, мы сразу заключаем, что  $\deg a(x) \leq \deg b(x)$ .

Заметим, что если старший коэффициент  $a_n$  многочлена  $a(x)$  является обратимым, то мы можем записать многочлен  $a(x)$  в виде

$$a(x) = a_n \sum_{k=0}^n a_k a_n^{-1} x^k = v(x)u(x),$$

где  $v(x) = a_n$  и  $u_x = \sum_{k=0}^n u_k x^k$  унитарный многочлен, коэффициенты которого определены равенствами  $u_k = a_k a_n^{-1}$  для  $k = 0, \dots, n$ .

Таким образом, многочлен  $a(x) \in \mathbb{U}[x]$  с обратимым старшим коэффициентом может быть представлен в виде произведения многочлена нулевой степени на унитарный многочлен степени, равной степени многочлена  $a(x)$ . Очевидно, что если кольцо  $\mathbb{U}$  является полем, то это верно для любого многочлена положительной степени.

**Определение 3.5.** *Многочлен  $a(x) \in \mathbb{U}[x]$  называется неприводимым, если равенство  $a(x) = u(x)v(x)$ , где  $u(x), v(x) \in \mathbb{U}[x]$  возможно только в том случае, когда один из многочленов  $u(x), v(x)$  имеет нулевую степень и, таким образом, является элементом кольца  $\mathbb{U}$ .*

Решение задачи о проверке, является ли заданный многочлен неприводимым, существенно зависит от кольца, над которым рассматривается многочлен. Как хорошо известно из курса алгебры, любой многочлен с коэффициентами из поля комплексных чисел является приводимым, поскольку раскладывается на линейные множители, см. [6, гл.6, § 3].

Для произвольного кольца это, конечно, неверно. Однако мы можем доказать теорему о разложении многочленов на множители, аналогичную основной теореме арифметики для целых чисел.

## 3.2 Алгоритм Эвклида для многочленов

Пусть  $a(x)$  и  $b(x)$  два многочлена из кольца  $\mathbb{U}[x]$ , при этом старший коэффициент многочлена  $a(x)$  является обратимым, в частности,  $a(x)$  может быть унитарным многочленом.

Аналогично кольцу целых чисел  $\mathbb{Z}$ , введем операцию деления многочленов с остатком и определим два многочлена  $q(x), r(x)$  кольца  $\mathbb{U}[x]$ , удовлетворяющих равенству

$$b(x) = a(x)q(x) + r(x), \quad \deg r(x) < \deg a(x). \quad (3.2)$$

Многочлен  $q(x)$  мы будем называть *частным* от деления, а многочлен  $r(x)$  – *остатком* от деления многочленов.

Мы дадим определение операции деления с остатком при помощи следующего алгоритма, который часто называют «школьным алгоритмом деления многочленов».

### Алгоритм 3.1 (Деление многочленов с остатком)

**Вход:** Многочлены  $a(x) = \sum_{k=0}^n a_k x^k$ ,  $b(x) = \sum_{k=0}^m b_k x^k$  и  $a_n$  обратим.

**Выход:** Многочлены  $q(x), r(x)$  такие, что  $b(x) = a(x)q(x) + r(x)$  и  $\deg r(x) < \deg a(x)$ .

1. Определить  $n = \deg a(x)$  и  $r(x) = b(x)$ ,  $q(x) = 0$ .
2. Определить  $k = \deg r(x)$ . Если выполнено  $k < n$ , то закончить алгоритм.
3. Определить  $c = r_k a_n^{-1}$ , где  $r_k$  старший коэффициент многочлена  $r(x)$ , и вычислить

$$r(x) = r(x) - c \cdot a(x) \cdot x^{k-n}, \quad q(x) = q(x) + c \cdot x^{k-n}.$$

Вернуться на шаг 2.

□

Данный алгоритм выполнит операцию деления с остатком за конечное число шагов. Легко видеть, что после каждого выполнения третьего шага алгоритма степень многочлена  $r(x)$  уменьшается. Поскольку степень многочлена является целым числом, то число шагов алгоритма конечно и не превышает величины  $m - n$ .

**Лемма 3.1.** *Полученное нами представление (3.2) единственно.*

*Доказательство.* Рассмотрим равенство

$$b(x) = a(x)q(x) + r(x) = a(x)q_1(x) + r_1(x),$$

где  $\deg a(x) > \deg r(x)$ ,  $\deg a(x) > \deg r_1(x)$ . Следовательно, многочлен  $a(x)$  делит разность многочленов  $r_1(x) - r(x)$ , то есть

$$a(x)(q(x) - q_1(x)) = (r_1(x) - r(x)). \quad (3.3)$$

В силу выбора многочленов  $r(x), r_1(x)$ , выполнено неравенство

$$\deg(r_1(x) - r(x)) \leq \max\{\deg r_1(x), \deg r(x)\} < \deg a(x),$$

следовательно, многочлен, стоящий справа в равенстве (3.3), имеет степень меньшую, чем многочлен, стоящий слева. Таким образом, равенство возможно только в том случае, если многочлены справа и слева равны нулю, откуда следует единственность представления (3.2).  $\square$

Равенство (3.2) мы будем также записывать в виде

$$b(x) \equiv r(x) \pmod{a(x)},$$

используя обозначения, аналогичные кольцу целых чисел.

Операция деления с остатком, как следует из ее определения, может быть определена для любого многочлена  $a(x)$  со старшим коэффициентом  $a_n$ , обратимым в кольце  $\mathbb{U}$ . Далее нам потребуется, чтобы у многочленов обратимыми являлись все коэффициенты. Поэтому мы будем считать, что кольцо  $\mathbb{U}$  является *полем*.

Теперь мы можем ввести понятие наибольшего общего делителя двух многочленов.

**Определение 3.6.** Пусть  $a(x)$  и  $b(x)$  два многочлена из кольца  $\mathbb{U}[x]$ . Многочлен  $u(x)$  называется наибольшим общим делителем многочленов  $a(x), b(x)$  если

- многочлен  $u(x)$  является общим делителем, то есть  $u(x)|a(x)$ ,  $u(x)|b(x)$ , и
- для любого другого общего делителя  $v(x)$  многочленов  $a(x), b(x)$  выполнено  $\deg u(x) > \deg v(x)$ .

Мы будем использовать для обозначения наибольшего общего делителя обозначение, аналогичное принятому для целых чисел, то есть  $u(x) = \mathbf{НОД}(a(x), b(x))$ .

Введенное нами определение неоднозначно. Действительно, пусть выполнено равенство  $u(x) = \mathbf{НОД}(a(x), b(x))$ , тогда для любого обратимого элемента  $\alpha \in \mathbb{U}$  будет выполнено  $\alpha \cdot u(x) = \mathbf{НОД}(a(x), b(x))$ . Поэтому для определенности, мы будем считать, что наибольший общий делитель двух многочленов  $a(x)$  и  $b(x)$  является унитарным многочленом кольца  $\mathbb{U}[x]$ .

**Определение 3.7.** Пусть  $a(x)$ ,  $b(x)$  многочлены из кольца  $\mathbb{U}[x]$ . Мы будем называть их взаимно простыми, если  $\text{НОД}(a(x), b(x)) = 1$ , то есть их наибольший общий делитель является унитарным многочленом степени ноль.

Свойства наибольшего общего делителя двух многочленов во многом аналогичны свойствам наибольшего общего делителя двух целых чисел. Сформулируем следующую лемму

**Лемма 3.2.** Пусть  $a(x)$ ,  $b(x)$  два многочлена кольца  $\mathbb{U}[x]$ , старшие коэффициенты которых обратимы в кольце  $\mathbb{U}$ . Тогда выполнены следующие утверждения.

1.  $\text{НОД}(a(x), b(x)) = \text{НОД}(b(x), a(x))$ .
2.  $\text{НОД}(a(x), a(x)) = \text{НОД}(a(x), 0) = a_n^{-1}a(x)$ , где  $a_n$  старший коэффициент многочлена  $a(x)$ .
3.  $\text{НОД}(a(x), b(x)) = \text{НОД}(a(x), r(x))$ , где  $r(x)$  остаток от деления многочлена  $b(x)$  на многочлен  $a(x)$ .

Доказательство данной леммы проводится аналогично доказательству леммы 1.2, поэтому мы его не приводим.

Для кольца многочленов, так же как и для кольца целых чисел, существует алгоритм, основывающийся на последнем утверждении леммы 3.2 и позволяющий эффективно вычислять значение наибольшего общего делителя двух многочленов.

### Алгоритм 3.2 (Алгоритм Эвклида для многочленов)

**Вход:** Многочлены  $a(x)$ ,  $b(x)$  кольца  $\mathbb{U}[x]$  такие, что их старшие коэффициенты обратимы в кольце  $\mathbb{U}$  и выполнено неравенство  $\deg b(x) \geq \deg a(x) > 0$ .

**Выход:**  $\text{НОД}(a(x), b(x))$  – наибольший общий делитель многочленов  $a(x)$  и  $b(x)$ .

1. Определить  $u(x) = b(x)$ ,  $v(x) = a(x)$ .
2. Пока  $v(x) \neq 0$  выполнить
  - 2.1. Используя алгоритм 3.1, определить многочлены  $q(x)$ ,  $r(x)$ , удовлетворяющие равенству  $u(x) = v(x)q(x) + r(x)$ .
  - 2.2. Определить  $u(x) = v(x)$  и  $v(x) = r(x)$ .
3. Определить  $\text{НОД}(a(x), b(x)) = u_n^{-1}u(x)$ , где  $u_n$  старший коэффициент многочлена  $u(x)$ . □

Корректность приведенного алгоритма, очевидно, следует из последнего утверждения леммы 3.2. Количество шагов алгоритма, то есть операций деления с остатком на втором шаге алгоритма, не превышает величины  $\deg b(x)$ .



### 3.3 Основная теорема арифметики для многочленов

Сформулируем лемму Безу для многочленов.

**Лемма 3.3** (Лемма Безу для многочленов). Пусть  $a(x)$  и  $m(x)$  два многочлена из кольца  $\mathbb{U}[x]$ . Тогда найдутся взаимно простые многочлены  $u(x)$  и  $v(x)$  такие, что

$$a(x)u(x) + m(x)v(x) = \text{НОД}(a(x), m(x)). \quad (3.4)$$

В предыдущей главе для доказательства леммы Безу в кольце целых чисел мы предложили алгоритм, позволяющий в явном виде найти неизвестные коэффициенты. Данный алгоритм может быть легко, практически без модификаций, перенесен на случай кольца многочленов. Доказательство этого факта оставляем читателю. Мы же, следуя монографии [28], дадим чисто алгебраическое доказательство леммы Безу.

*Доказательство.* Рассмотрим множество  $\mathcal{D} = \{a(x)u(x) + m(x)v(x)\}$ , для произвольных многочленов  $u(x), v(x) \in \mathbb{U}[x]$ . Поскольку  $\mathbb{U}$  является полем, то мы можем выбрать в множестве  $\mathcal{D}$  унитарный многочлен

$$d(x) = a(x)u_1(x) + m(x)v_1(x) \quad (3.5)$$

наименьшей степени. Если  $\deg d(x) = 1$ , то, в силу унитарности, он равен единице и, таким образом, является общим делителем многочленов  $a(x)$  и  $m(x)$ .

Если степень многочлена  $d(x)$  больше единицы, то, используя алгоритм 3.1, разделим многочлен  $m(x)$  на  $d(x)$  с остатком и определим многочлен

$$r(x) = m(x) - q(x)d(x), \quad \deg r(x) < \deg d(x),$$

для некоторого частного от деления  $q(x) \in \mathbb{U}[x]$ . Используя выражение  $d(x)$  через многочлены  $a(x)$  и  $m(x)$ , запишем равенство

$$\begin{aligned} r(x) &= m(x) - q(x)(a(x)u_1(x) + m(x)v_1(x)) = \\ &= -a(x)q(x)u_1(x) + m(x)(1 - q(x)v_1(x)), \end{aligned}$$

из которого следует, что многочлен  $r(x)$  также принадлежит нашему множеству  $\mathcal{D}$ . Учитывая, что степень  $r(x)$  меньше степени  $d(x)$ , и  $d(x)$  выбран в множестве  $\mathcal{D}$  минимальным, получаем, что  $\deg r(x) = 0$ . Последнее равенство означает, что  $m(x) = q(x)d(x)$ , то есть многочлен  $d(x)$

делит  $m(x)$ . Применяя аналогичные рассуждения к многочлену  $a(x)$  получаем, что  $d(x)$  делит и многочлен  $a(x)$ , то есть является общим делителем многочленов  $a(x)$  и  $m(x)$ .

Легко показать, что  $d(x)$  является наибольшим общим делителем. Действительно, из равенства (3.5) следует, что любой общий делитель многочленов  $a(x)$  и  $m(x)$  является и делителем многочлена  $d(x)$ . Равенство (3.5) определяет многочлены  $u(x)$  и  $v(x)$ , возникающие в утверждении леммы.

Для завершения доказательства леммы заметим, что если найдется другой многочлен  $d_1$ , обладающий такими же свойствами, что и многочлен  $d(x)$ , то будет выполнено

$$d_1(x)|d(x) \quad \text{и} \quad d(x)|d_1(x).$$

То есть многочлены  $d(x)$  и  $d_1(x)$  отличаются только множителем. Поскольку они унитарны, то они совпадают и  $d(x) = d_1(x)$ .  $\square$

Нам потребуется еще одна лемма.

**Лемма 3.4.** Пусть  $f(x)$  неприводимый многочлен из кольца  $\mathbb{U}[x]$ , который делит произведение многочленов  $g(x)h(x)$  из  $\mathbb{U}[x]$ . Тогда либо  $f(x)|g(x)$ , либо  $f(x)|h(x)$ .

*Доказательство.* Из условия леммы следует, что найдется некоторый многочлен  $t(x) \in \mathbb{U}[x]$  такой, что выполнено равенство

$$f(x)t(x) = g(x)h(x). \quad (3.6)$$

Пусть многочлен  $f(x)$  не делит многочлен  $g(x)$ . Тогда, в силу неприводимости многочлена  $f(x)$ , выполнено  $\text{НОД}(f(x), g(x)) = 1$  и, в силу леммы Безу, см. лемму 3.3, найдутся такие многочлены  $u(x), v(x) \in \mathbb{U}[x]$ , что

$$u(x)f(x) + v(x)g(x) = 1.$$

Домножая последнее равенство на многочлен  $h(x)$  и используя равенство (3.6), получаем

$$u(x)f(x)h(x) + v(x)f(x)t(x) = h(x) \quad \text{или} \quad f(x)r(x) = h(x),$$

где  $r(x) = u(x)h(x) + v(x)t(x)$ . Таким образом, согласно определению, многочлен  $h(x)$  делится на многочлен  $f(x)$ . Лемма доказана.  $\square$

**Теорема 3.1** (Основная теорема арифметики для многочленов). Пусть  $f(x)$  произвольный многочлен из кольца  $\mathbb{U}[x]$ ,  $\deg f(x) > 0$ . Тогда он может быть представлен в виде

$$f(x) = cf_1^{\alpha_1}(x) \cdots f_k^{\alpha_k}(x), \quad (3.7)$$

где  $c \in \mathbb{U}$ , а  $f_1(x), \dots, f_k(x)$  различные унитарные неприводимые многочлены,  $\alpha_1, \dots, \alpha_k$  натуральные числа. Более того, это разложение однозначно с точностью до перестановки множителей.

*Доказательство.* Мы проведем доказательство теоремы индукцией по степени многочлена  $f(x)$ . В случае, когда  $\deg f(x) = 1$ ,  $f(x) = a_1x + a_0$  мы тривиально получаем представление  $f(x) = a_1(x + a_1^{-1}a_0)$ .

Предположим теперь, что условие теоремы выполнено для всех многочленов степени, меньшей чем  $n$ . Рассмотрим многочлен  $f(x)$  такой, что  $\deg f(x) = n$ . Если многочлен  $f(x)$  неприводим, то мы получаем требуемое представление  $f(x) = a_n(a_n^{-1}f(x))$ , где  $a_n$  старший коэффициент многочлена  $f(x)$  и многочлен  $a_n^{-1}f(x)$  унитарен.

Если многочлен  $f(x)$  приводим, то представим его в виде произведения  $f(x) = g(x)h(x)$ , где  $\deg g(x) < n$ ,  $\deg h(x) < n$ . Согласно предположению индукции, многочлены  $g(x), h(x)$  могут быть представлены в виде (3.7), следовательно, и многочлен  $f(x)$  представим в виде (3.7).

Полученное представление единственно. Действительно, предположим, что это не так и многочлен  $f(x)$  имеет два разложения вида (3.7)

$$f(x) = cf_1^{\alpha_1}(x) \cdots f_k^{\alpha_k}(x) = dh_1^{\beta_1}(x) \cdots h_s^{\beta_s}(x). \quad (3.8)$$

Поскольку все многочлены  $f_1(x), \dots, f_k(x)$  и  $h_1(x), \dots, h_s(x)$  унитарны, мы получаем, что значения  $c$  и  $d$  совпадают. Без ограничения общности будем считать, что  $s \geq k$  и рассмотрим неприводимый многочлен  $f_1(x)$ , стоящий в левой части равенства (3.8). В силу леммы 3.4 в правой части равенства (3.8) найдется многочлен  $h_{i_1}(x)$  такой, что  $f_1(x) | h_{i_1}(x)$ . Поскольку многочлен  $h_{i_1}(x)$  унитарен и неприводим, то условие делимости возможно только в случае, когда  $f_1 = h_{i_1}(x)$ .

Мы можем сократить равенство (3.8) на общий множитель и повторить эту процедуру далее для многочлена  $f_2(x)$ . Проведя  $k$  сокращений, мы получим равенство

$$1 = f_1^{|\alpha_1 - \beta_1|}(x) \cdots f_k^{|\alpha_k - \beta_k|}(x) h_{k+1}^{\beta_{k+1}}(x) \cdots h_s^{\beta_s}(x).$$

Поскольку в левой части полученного равенства стоит многочлен нулевой степени, мы получаем, что  $k = s$ ,  $\alpha_i = \beta_i$ ,  $i = 1, \dots, k$ , откуда вытекает утверждение теоремы.  $\square$

Дадим еще одно важное определение.

**Определение 3.8.** Элемент  $e \in \mathbb{U}$  называется корнем или нулем многочлена  $f(x) \in \mathbb{U}[x]$ , если  $f(e) = 0$ .

**Теорема 3.2.** Элемент  $e \in \mathbb{U}$  является корнем многочлена  $f(x) \in \mathbb{U}[x]$  в том и только в том случае, когда многочлен  $x - e$  делит  $f(x)$ .

*Доказательство.* Применяя алгоритм 3.1 деления с остатком, получим представление многочлена  $f(x)$  в виде

$$f(x) = (x - e)q(x) + c,$$

где  $c$  некоторый элемент из  $\mathbb{U}$ . Подставляя в полученное равенство вместо переменной  $x$  значение  $e$ , получаем  $f(e) = c$ . Таким образом, если элемент  $e$  является корнем многочлена  $f(x)$ , выполнено равенство  $c = 0$  и теорема доказана.  $\square$

**Определение 3.9.** Пусть  $e \in \mathbb{U}$  корень многочлена  $f(x) \in \mathbb{U}[x]$ . Мы будем называть кратностью корня  $e$  такое максимально возможное натуральное число  $\alpha$ , что  $(x - e)^\alpha | f(x)$ .

**Теорема 3.3.** Пусть  $f(x) \in \mathbb{U}[x]$  произвольный многочлен и  $\deg f(x) = n > 0$ . Тогда многочлен  $f(x)$  может иметь не более  $n$  корней.

*Доказательство.* Пусть  $e_1, \dots, e_s \in \mathbb{U}$  корни многочлена  $f(x)$ . Тогда из теоремы 3.2 следует, что найдутся натуральные числа  $\alpha_1, \dots, \alpha_s \geq 1$  такие, что

$$(x - e_i)^{\alpha_i} | f(x), \quad i = 1, \dots, s.$$

Рассматривая разложение многочлена  $f(x)$  на неприводимые множители, согласно теореме 3.1, получим равенство

$$f(x) = a_n(x - e_1)^{\alpha_1} \cdots (x - e_s)^{\alpha_s} u(x),$$

где  $a_n$  старший коэффициент многочлена  $f(x)$ , а многочлен  $u(x)$  либо равен 1, либо раскладывается в произведение неприводимых многочленов степени большей единицы. Учитывая, что степень многочлена  $f(x)$  равна  $n$ , мы получаем неравенство

$$\alpha_1 + \cdots + \alpha_s \leq n,$$

из которого следует утверждение теоремы.  $\square$

### 3.4 Дифференцирование многочленов

Рассмотрим многочлен  $f(x) = \sum_{k=0}^n a_k x^k$ ,  $f(x) \in \mathbb{U}[x]$ . Пусть  $c \in \mathbb{U}$  произвольный, отличный от нуля элемент, тогда

$$f(x+c) = \sum_{k=0}^n a_k (x+c)^k = f(x) + cf_1(x) + c^2 f_2(x) + \dots$$

Мы разложили значение многочлена  $f(x+c)$  по степеням  $c$ . Полученное равенство может быть также записано в виде сравнения

$$f(x+c) \equiv f(x) + cf_1(x) \pmod{c^2}, \quad c \neq 0. \quad (3.9)$$

**Определение 3.10.** Пусть  $f(x), f_1(x) \in \mathbb{U}[x]$  многочлены, удовлетворяющие равенству (3.9). Мы будем называть многочлен  $f_1(x)$  производной многочлена  $f(x)$  и обозначать символом  $f'(x)$ .

**Лемма 3.5.** Пусть  $f(x), g(x)$  два многочлена кольца  $\mathbb{U}[x]$ . Тогда выполнены следующие соотношения

1.  $(f(x) + g(x))' = f'(x) + g'(x)$  (производная суммы),
2.  $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$  (производная произведения).

*Доказательство.* Первое утверждение следует из определения производной и соотношения

$$\begin{aligned} f(x+c) + g(x+c) &\equiv f(x) + cf'(x) + g(x) + cg'(x) \equiv \\ &\equiv (f(x) + g(x)) + c(f'(x) + g'(x)) \pmod{c^2}. \end{aligned}$$

Аналогично, доказательство второго утверждения следует из определения производной и соотношения

$$\begin{aligned} f(x+c)g(x+c) &\equiv (f(x) + cf'(x))(g(x) + cg'(x)) \equiv \\ &\equiv f(x)g(x) + c(f'(x)g(x) + f(x)g'(x)) \pmod{c^2}. \end{aligned}$$

□

Обобщая утверждения леммы, мы получаем равенства

$$(f_1(x) + \dots + f_k(x))' = f_1'(x) + \dots + f_k'(x), \quad (3.10)$$

$$(f_1(x) \cdots f_k(x))' = f_1'(x)f_2(x) \cdots f_k(x) + \dots + f_1(x) \cdots f_{k-1}'(x)f_k(x). \quad (3.11)$$

Из (3.11) получаем равенство

$$(ax^k)' = akx^{k-1}, \quad \text{для } a \neq 0, k > 0. \quad (3.12)$$

Из (3.10) и последнего равенства (3.12) следует соотношение

$$\begin{aligned} f'(x) &= \left( \sum_{k=0}^n a_k x^k \right)' = \sum_{k=1}^n k a_k x^{k-1} = \\ &= \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k = n a_n x^{n-1} + \dots + 2 a_2 x + a_1, \end{aligned} \quad (3.13)$$

которое традиционно используется для определения производной многочлена  $f(x)$ .

### 3.5 Решение сравнений по составному модулю

Рассмотрим вопрос о нахождении корней многочлена. Выберем некоторое целое число  $m > 0$  с известным разложением на простые множители

$$m = \prod_{i=1}^k p_i^{\alpha_i}, \quad \alpha_i \in \mathbb{N}, \quad \alpha_i > 0, \quad (3.14)$$

и будем считать, что  $\mathbb{U} = \mathbb{Z}_m$ .

Рассмотрим произвольный многочлен  $f(x)$  с целыми коэффициентами и зададимся вопросом о том, как найти его корни в кольце  $\mathbb{Z}_m$ . Другими словами, необходимо найти все решения уравнения  $f(x) \equiv 0 \pmod{m}$  в кольце  $\mathbb{Z}_m$ .

**Теорема 3.4.** Пусть  $f(x)$  многочлен с целыми коэффициентами и  $m > 0$  целое число, для которого известно разложение на простые множители (3.14). Тогда множества целых чисел, удовлетворяющих сравнению

$$f(x) \equiv 0 \pmod{m} \quad (3.15)$$

и системе сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \dots, \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}, \end{cases} \quad (3.16)$$

совпадают.

Обозначим символом  $N(m)$  число решений сравнения (3.15), тогда выполнено равенство

$$N(m) = N(p_1^{\alpha_1}) \cdots N(p_k^{\alpha_k}).$$

*Доказательство.* Пусть целое число  $e$  удовлетворяет сравнению (3.15). Тогда  $m|f(e)$  и для любого индекса  $i = 1, \dots, k$ , выполнено  $p_i^{\alpha_i}|f(e)$ , следовательно,  $e$  удовлетворяет системе сравнений (3.16).

Обратно, если  $e$  удовлетворяет системе сравнений (3.16), то  $p_i^{\alpha_i}|f(e)$  для любого  $i = 1, \dots, k$ , то есть  $f(e)$  является общим кратным чисел  $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$ . Согласно лемме 2.6 наименьшее кратное чисел  $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$  есть  $m$ . Следовательно,  $m|f(e)$  и  $e$  является решением системы сравнений (3.16).

Предъявим способ построения решения сравнения (3.15) по известным решениям системы (3.16). Пусть числа  $a_1, \dots, a_k$  являются решением системы сравнений (3.16). Согласно «китайской теореме об остатках», теорема 2.3, найдется вычет  $e$  по модулю  $m$  такой, что  $e \equiv a_i \pmod{p_i^{\alpha_i}}$  для всех  $i = 1, \dots, k$ . Тогда  $f(e) \equiv f(a_i) \equiv 0 \pmod{p_i^{\alpha_i}}$  и, по доказанному ранее,  $e$  является решением сравнения (3.15).

Далее, пусть числа  $a_1, \dots, a_k$  пробегают все возможные наборы значений, являющихся решением системы (3.16), тогда, согласно следствию к теореме 2.3, соответствующие им решения принимают различные значения по модулю  $m$ . Таким образом, число решений сравнения (3.15) не менее  $N(p_1^{\alpha_1}) \cdots N(p_k^{\alpha_k})$ .

По доказанному ранее, каждое решение  $e$  сравнения (3.15) удовлетворяет системе сравнений (3.16) и, следовательно, ему соответствует некоторый набор чисел  $a_1, \dots, a_k$ . Это доказывает, что других решений, отличных от построенных, сравнение (3.15) не имеет.  $\square$

Доказанная нами теорема сводит поиск корней сравнения (3.15) к поиску корней сравнения  $f(x) \equiv 0 \pmod{p^\alpha}$  для некоторого простого числа  $p$  и натурального  $\alpha$ .

Легко видеть, что если  $e$  является корнем  $f(x) \pmod{p^\alpha}$ , то это же значение должно являться корнем  $f(x) \pmod{p}$ : из условия  $p^\alpha|f(e)$  очевидным образом следует условие  $p|f(e)$ . Таким образом, существование корня многочлена  $f(x) \pmod{p}$  становится необходимым признаком существования корня многочлена  $f(x) \pmod{p^\alpha}$ .

Допустим, что нам известен корень многочлена  $f(x) \pmod{p}$ . Следующая теорема дает ответ на вопрос – как найти корень многочлена  $f(x) \pmod{p^\alpha}$ .

**Теорема 3.5.** Пусть  $p$  простое число,  $f(x)$  многочлен с целыми коэффициентами и  $e$  целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \not\equiv 0 \pmod{p}.$$

Тогда при любом натуральном  $\alpha \geq 1$  существует единственное решение сравнения

$$f(x) \equiv 0 \pmod{p^\alpha},$$

принадлежащее классу вычетов  $x \equiv e \pmod{p}$ .

*Доказательство.* Докажем теорему индукцией по степеням простого числа  $p$ . При  $\alpha = 1$ , утверждение теоремы, очевидно, выполняется.

Предположим, что утверждение теоремы выполнено для всех целых степеней, меньших либо равных  $\alpha$ , и обозначим  $e_\alpha$  корень многочлена  $f(x) \pmod{p^\alpha}$ , то есть  $f(e_\alpha) \equiv 0 \pmod{p^\alpha}$  и  $e_\alpha \equiv e \pmod{p}$ .

Обозначим  $e_{\alpha+1}$  корень многочлена  $f(x) \pmod{p^{\alpha+1}}$  и будем искать его в виде

$$e_{\alpha+1} = e_\alpha + tp^\alpha, \quad t \in \mathbb{Z}, \quad 0 \leq t < p. \quad (3.17)$$

Тогда  $e_{\alpha+1} \equiv e_\alpha \equiv e \pmod{p}$ . Воспользуемся равенством (3.9) и запишем сравнение

$$f(e_{\alpha+1}) = f(e_\alpha + tp^\alpha) \equiv f(e_\alpha) + tp^\alpha f'(e_\alpha) \pmod{p^{2\alpha}}.$$

Поскольку мы считаем, что  $e_{\alpha+1}$  является корнем, то мы можем записать равенство

$$0 = f(e_\alpha) + tp^\alpha f'(e_\alpha) + hp^{\alpha+1},$$

для некоторого целого значения  $h$ . По предположению индукции  $f(e_\alpha)$  делится на  $p^\alpha$ , следовательно, сокращая полученное равенство на  $p^\alpha$ , получаем сравнение

$$t \equiv -\frac{f(e_\alpha)}{p^\alpha f'(e_\alpha)} \pmod{p}. \quad (3.18)$$

Поскольку  $f'(e_\alpha) \not\equiv 0 \pmod{p}$ , то неизвестное значение  $t$  единственным образом определяется сравнением (3.18).  $\square$

Таким образом, если нам известны корни многочлена  $f(x)$  по модулю простого числа  $p$ , то теорема 3.5 дает нам способ определения всех корней многочлена  $f(x)$  по модулю  $p^\alpha$ . Этот способ часто называют подъемом решения. Однако он не работает, если многочлен  $f(x)$  имеет кратные корни.



Действительно, согласно основной теореме арифметики для многочленов, если  $e$  корень многочлена  $f(x) \pmod{p}$ , то

$$f(x) \equiv (x - e)^\gamma u(x) \pmod{p}, \quad \text{НОД}((x - e), u(x)) = 1,$$

где натуральное число  $\gamma \geq 1$  является кратностью корня  $e$ . Для производной многочлена выполнено сравнение

$$\begin{aligned} f'(x) &\equiv \gamma(x - e)^{\gamma-1}u(x) + (x - e)^\gamma u'(x) \equiv \\ &\equiv (x - e)^{\gamma-1}(\gamma u(x) + u'(x)) \pmod{p}, \end{aligned}$$

из которого следует, что при  $\gamma > 1$  выполнено  $f'(e) \equiv 0 \pmod{p}$  и условия теоремы 3.5 не выполнены.

**Теорема 3.6.** Пусть  $p$  простое число,  $f(x)$  многочлен с целыми коэффициентами и  $e$  целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \equiv 0 \pmod{p}.$$

Пусть  $\beta \geq 1$  максимальное число такое, что  $f(e) \equiv 0 \pmod{p^\beta}$ . Тогда сравнение  $f(x) \equiv 0 \pmod{p^\alpha}$  разрешимо только при  $\alpha \leq \beta$  и корнем является значение  $e$ .

*Доказательство.* Очевидно, что при  $\alpha \leq \beta$  из сравнения  $f(e) \equiv 0 \pmod{p^\beta}$  следует утверждение теоремы. Покажем, что при  $\alpha > \beta$  решений не существует.

Обозначим  $e_{\beta+1} = e + tp^{\beta+1}$  и запишем сравнение

$$f(e_{\beta+1}) = f(e) + tp^{\beta+1}f'(e) \pmod{p^{2(\beta+1)}}.$$

Если  $p^{\beta+1}$  не делит  $f(e)$ , то правая часть в приведенном сравнении не делится на  $p^{\beta+1}$ . Отсюда следует, что  $f(e_{\beta+1})$  не делится на  $p^{\beta+1}$ , следовательно, теорема доказана.  $\square$

Суммируя утверждения двух последних теорем, мы можем предложить алгоритм для подъема решения.

### Алгоритм 3.3 (Алгоритм подъема решения)

**Вход:** Простое число  $p$ , натуральное число  $\alpha > 1$ , многочлен  $f(x)$  и целое число  $e$  такое, что  $f(e) \equiv 0 \pmod{p}$ .

**Выход:** Целое число  $e_\alpha$  такое, что  $f(e_\alpha) \equiv 0 \pmod{p^\alpha}$ .

1. Вычислить многочлен  $f'(x)$ .
  2. Если  $f'(e) \equiv 0 \pmod{p}$ , то перейти на шаг 7.
- Иначе определить  $e_k = e$  и  $k = 1$ .

**3. Пока  $k \leq \alpha$  выполнить****3.1.** Вычислить вычет  $t \equiv -\frac{f(e_k)}{p^k f'(e_k)} \pmod{p}$  и определить  $e_k = e_k + tp^k$ .**3.2.** Вычислить  $k = k + 1$ .**4.** Закончить алгоритм и вернуть значение  $e_\alpha = e_k$ .**5.** Определить  $t = f(e)$ .**6. Если  $t \equiv 0 \pmod{p^\alpha}$ , то вернуть значение  $e_\alpha = e$  и закончить алгоритм.****Иначе закончить алгоритм с уведомлением о том, что решений нет.** □

Приведенный алгоритм проверяет значение производной многочлена  $f(x)$  в точке  $e$  и в зависимости от того, равно ли это значение нулю или нет, следует утверждениям теорем 3.5 и 3.6.

**Пример 3.2.** Приведем пример применения данного алгоритма и найдем корни многочлена  $f(x) = x^3 + 2x^2 + 3x + 2$  по модулю 49. Рассмотрим сравнение  $f(x) \equiv 0 \pmod{7}$ , которое имеет два корня  $e = 6$  и  $\hat{e} = 3$ . Вычислим производную  $f'(x) = 3x^2 + 4x + 3$  и определим кратности корней.

Поскольку  $f'(6) = 135 \equiv 2 \pmod{7}$ , то кратность первого корня  $e = 6$  равна единице. Вычисляя  $f'(3) = 42 \equiv 0 \pmod{7}$ , получаем, что кратность второго корня  $\hat{e} = 3$  больше единицы. Так как многочлен  $f(x)$  имеет не более трех корней, заключаем, что кратность корня  $\hat{e} = 3$  равна двум.

Найдем корень  $e_2$  многочлена  $f(x)$  по модулю 49 такой, что  $e_2 \equiv e \pmod{7}$ . Для этого, используя утверждение теоремы 3.5, вычислим

$$t \equiv -\frac{f(6)}{7f'(6)} \equiv -\frac{308}{7 \cdot 132} \equiv 6 \pmod{7}.$$

и определим  $e_2 = 6 + 6 \cdot 7 = 48$ . Проверяя, получаем  $f(48) \equiv f(-1) \equiv 0 \pmod{49}$ , следовательно, найденное нами значение  $e_2$  действительно является корнем многочлена  $f(x)$  по модулю 49.

Рассмотрим второй корень  $\hat{e} = 3$ . Поскольку  $f'(3) \equiv 0 \pmod{7}$ , нам достаточно вычислить  $f(3) = 56$ . Поскольку  $f(3) \not\equiv 0 \pmod{49}$ , то из утверждения теоремы 3.6 следует, что значения  $\hat{e}_2$  такого, что  $f(\hat{e}_2) \equiv 0 \pmod{49}$  и  $\hat{e}_2 \equiv \hat{e} \pmod{7}$ , не существует. Таким образом, исходное сравнение  $f(x) \equiv 0 \pmod{49}$  имеет только одно решение и оно равно 48.

В следующей главе мы подробно рассмотрим вопрос о том, как находить решения полиномиальных сравнений по простому модулю.

## СРАВНЕНИЯ СТАРШИХ СТЕПЕНЕЙ

Определение квадратичного вычета - Символ Лежандра - Теорема о числе решений - Свойства символа Лежандра - Определение символа Якоби, его свойства - Алгоритм вычисления символа Якоби - Вычисление квадратного корня: частные случаи - Алгоритм Тонелли-Шенкса - Общее квадратное уравнение - Вероятностный алгоритм вычисления корней многочлена

Рассмотрим вопрос о нахождении корней многочленов по модулю простого числа  $p$ . Вначале мы рассмотрим случай многочленов второй степени, а потом перейдем к поиску корней многочленов произвольной степени.

Мы начнем с самого простого случая, а именно, с уравнения

$$x^2 \equiv a \pmod{p}. \quad (4.1)$$

Для  $x$ , удовлетворяющего (4.1), мы будем использовать выражение «квадратный корень из  $a$  по модулю простого числа  $p$ ».

### 4.1 Квадратичные вычеты

Рассмотрим вопрос о разрешимости сравнения (4.1).

**Лемма 4.1.** Пусть  $p$  нечетное простое число,  $a$  – целое число, взаимно простое с  $p$ . Если сравнение (4.1) разрешимо, то оно имеет два различных решения.

*Доказательство.* Вначале заметим, что из условия  $\text{НОД}(a, p) = 1$  и третьего утверждения леммы 1.2 следует, что  $a \not\equiv 0 \pmod{p}$ .

Пусть  $x_1$  – некоторое, отличное от нуля решение сравнения (4.1). Обозначим  $x_2 \equiv -x_1 \pmod{p}$ . Тогда  $x_2$  также является решением сравнения (4.1), в силу того, что  $(x_2)^2 \equiv (-x_1)^2 \equiv a \pmod{p}$ .

Второе решение отлично от первого, так как в противном случае были бы выполнены сравнения

$$x_2 \equiv x_1 \pmod{p} \quad \text{или} \quad 2x_1 \equiv 0 \pmod{p},$$

что невозможно, так как  $\text{НОД}(2, p) = \text{НОД}(x_1, p) = 1$  и  $x_1 \not\equiv 0$ .  $\square$

В случае, когда  $p$  четное простое число, то есть  $p = 2$ , решения сравнения (4.1) легко выписать в явном виде. Действительно, для  $a$  возможно всего два варианта  $a = 0$  или  $1$ , из чего вытекает, что  $x \equiv a \pmod{2}$ .

**Определение 4.1.** Пусть  $a, p$  – целые, взаимно простые числа. Мы будем называть целое число  $a$  квадратичным вычетом по модулю  $p$ , если разрешимо сравнение (4.1). В противном случае мы будем называть число  $a$  квадратичным невычетом.

Следующая лемма позволяет получить узнать точное число квадратичных вычетов и квадратичных невычетов по модулю простого числа.

**Лемма 4.2.** Пусть  $p$  нечетное простое число. Среди чисел  $1, 2, \dots, p-1$  содержится равное число квадратичных вычетов и квадратичных невычетов по модулю  $p$ .

*Доказательство.* Среди вычетов  $1, 2, \dots, p-1$  квадратичными вычетами являются только те, квадраты которых сравнимы с числами

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2. \quad (4.2)$$

Для вычетов  $k$  таких, что  $1 \leq k \leq \frac{p-1}{2}$ , это очевидно. Для остальных вычетов, при  $\frac{p-1}{2} < k \leq p-1$ , выполнено

$$k^2 \equiv (p-k)^2 \equiv l^2 \pmod{p}, \quad \text{где } 1 \leq l < \frac{p-1}{2}.$$

Пусть среди чисел (4.2) найдется хотя бы одна пара совпадающих, то есть

$$k^2 \equiv l^2 \pmod{p}, \quad 1 \leq k < l \leq \frac{p-1}{2}.$$

Тогда сравнению  $x^2 \equiv l^2 \pmod{p}$  удовлетворяет четыре решения:  $k, l, -k$  и  $-l$ , что противоречит лемме 4.1.

Следовательно, числа (4.2) попарно несравнимы и среди всех вычетов по модулю  $p$ :  $1, 2, \dots, p-1$  найдется ровно  $\frac{p-1}{2}$  квадратичных вычетов. Остальные – квадратичные невычеты.  $\square$

Введем в рассмотрение функцию, которая позволяет говорить о разрешимости сравнения (4.1) и проверять, является ли целое число квадратичным вычетом или нет.

**Определение 4.2.** Пусть  $p$  нечетное простое число,  $a$  – целое число, взаимно простое с  $p$ . Мы будем называть символом Лежандра и обозначать символом  $\left(\frac{a}{p}\right)$  функцию, удовлетворяющую равенству

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ квадратичный вычет,} \\ -1, & \text{если } a \text{ квадратичный невычет.} \end{cases}$$

Сформулируем теорему о числе решений сравнения (4.1).

**Теорема 4.1.** Пусть  $p$  нечетное простое число. Тогда число решений сравнения  $x^2 \equiv a \pmod{p}$  может равняться нулю, если  $\left(\frac{a}{p}\right) = -1$ , единице, если  $a \equiv 0 \pmod{p}$ , и двум, если  $\left(\frac{a}{p}\right) = 1$ .

*Доказательство.* Доказательство первого и третьего утверждений теоремы, очевидно, следует из леммы 4.1 и определения символа Лежандра.

Нам осталось доказать второе утверждение при  $a \equiv 0 \pmod{p}$ . Легко видеть, что  $x \equiv 0 \pmod{p}$  является решением сравнения (4.1). Пусть существует второе решение  $z$  такое, что  $z \not\equiv 0 \pmod{p}$ . Тогда равенство (4.1) можно записать в виде

$$zz = kp, \quad (4.3)$$

при некотором целом  $k$ .

Поскольку  $p$  простое число, то  $\text{НОД}(z, p) = 1$  и из леммы 1.4 следует, что  $k|z$ . Тогда, сокращая в равенстве (4.3) множитель  $z \neq 0$ , получаем, что  $z = lp$  или, что равносильно,  $z \equiv 0 \pmod{p}$ . Мы получили противоречие с выбором  $z$ , которое завершает доказательство теоремы.  $\square$

Для проверки разрешимости сравнения (4.1) нам нужен эффективный алгоритм вычисления символа Лежандра. Докажем лемму, утверждения которой позволяют предъявить искомый алгоритм.

**Лемма 4.3.** Пусть  $p$  нечетное простое число,  $a$  целое число, взаимно простое с  $p$ , тогда для символа Лежандра  $\left(\frac{a}{p}\right)$  выполнены следующие свойства.

1. Если  $a \equiv b \pmod{p}$ , то  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .
2. Выполнено сравнение  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ , которое принято называть «критерием Эйлера».
3. Верны равенства  $\left(\frac{1}{p}\right) = 1$  и  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ .
4. Если  $a = bc$ ,  $a \neq 0$ , где  $b, c$  целые числа, то  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \left(\frac{c}{p}\right)$ .
5. Выполнено сравнение  $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$ .

6. Пусть числа  $a$  и  $p$  – нечетные простые, тогда

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

Последнее равенство принято называть «квадратичным законом взаимности Гаусса».

*Доказательство.* Первое утверждение леммы следует из того, что разрешимость сравнения (4.1) не зависит от представителя класса вычетов по модулю  $p$ .

Перейдем к доказательству с критерия Эйлера. Поскольку  $p - 1$  является четным числом, то в силу малой теоремы Ферма, см. теорему 2.7, выполнено сравнение

$$a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Тогда из леммы 1.4 следует, что для любого  $a$ ,  $\text{НОД}(a, p) = 1$ , выполнено одно из сравнений

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad (4.4)$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (4.5)$$

Пусть  $a$  квадратичный вычет по модулю  $p$  и  $x$  решение сравнения (4.1). Поскольку  $x$  взаимно просто с  $p$ , то применяя малую теорему Ферма, см теорему 2.7, получаем

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Следовательно, любой квадратичный вычет  $a$  удовлетворяет сравнению (4.4).

Оставшиеся  $\frac{p-1}{2}$  значений удовлетворяют сравнению (4.5) и, согласно лемме 4.2, являются квадратичными невычетами. Критерий Эйлера доказан.

Третье утверждение леммы, очевидно, вытекает из второго и не требует отдельного доказательства.

Критерий Эйлера позволяет доказать и четвертое утверждение леммы. Действительно, если  $a = bc$ , то

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \left(b^{\frac{p-1}{2}}\right) \cdot \left(c^{\frac{p-1}{2}}\right) \equiv \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \pmod{p}.$$

Из четвертого утверждения леммы следует, что в числителе символа Лежандра можно отбросить любой квадратный множитель, то есть выполнено равенство

$$\left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right).$$

□

Для доказательства двух последних утверждений леммы нам потребуются дополнительные усилия. Из достаточно обширного списка опубликованных на русском языке доказательств квадратичного закона взаимности, мы остановимся на классическом доказательстве, изложенном в книге [10]. Это третье доказательство квадратичного закона взаимности из шести, данных Гауссом, последняя его часть принадлежит Кронекеру. Нам потребуется еще одна лемма.

**Лемма 4.4** (Гаусс). Пусть  $p$  нечетное простое число,  $a$  целое число, взаимно простое с  $p$ ,  $\text{НОД}(a, p) = 1$ , тогда для символа Лежандра  $\left(\frac{a}{p}\right)$  выполнено равенство

$$\left(\frac{a}{p}\right) = (-1)^\mu,$$

где  $\mu$  число отрицательных абсолютно-наименьших вычетов по модулю  $p$  (см. определение 2.4) среди чисел  $a, 2a, \dots, \frac{p-1}{2}a$ .

*Доказательство.* Обозначим символами

$$a_1, a_2, \dots, a_\lambda, -b_1, -b_2, \dots, -b_\mu, \quad (4.6)$$

абсолютно наименьшие вычеты чисел  $a, 2a, \dots, \frac{p-1}{2}a$  по модулю  $p$ , то есть для всех  $i = 1, \dots, \lambda, j = 1, \dots, \mu$  выполнено

$$-\frac{p-1}{2} \leq a_i \leq \frac{p-1}{2}, \quad -\frac{p-1}{2} \leq -b_j \leq \frac{p-1}{2}.$$

Мы считаем, что все  $a_i, b_j$  положительны, поэтому в (4.6) содержится  $\lambda$  положительных чисел и  $\mu$  отрицательных и  $\lambda + \mu = \frac{p-1}{2}$ . Все числа

$$a_1, a_2, \dots, a_\lambda, b_1, b_2, \dots, b_\mu,$$



целые, положительные, **различные** по модулю  $p$  и меньшие, чем  $\frac{p}{2}$ , следовательно, ими исчерпывается множество всех целых чисел от 1 до  $\frac{p-1}{2}$ . Перемножая их, получим равенство

$$a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu = \left(\frac{p-1}{2}\right)! \quad (4.7)$$

Каждое из чисел (4.6) сравнимо только с одним произведением  $ka$ , где  $k = 1, \dots, \frac{p-1}{2}$ , таким образом, с учетом равенства (4.7) получаем сравнение

$$\begin{aligned} \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} &= a \cdot 2a \cdots \frac{p-1}{2} \equiv a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu (-1)^\mu \equiv \\ &\equiv \left(\frac{p-1}{2}\right)! (-1)^\mu \pmod{p}. \end{aligned}$$

Сокращая обе части сравнения на множитель  $\left(\frac{p-1}{2}\right)!$  получаем сравнение

$$(-1)^\mu \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

которое выполнено в силу критерия Эйлера, см. утверждение 2 леммы 4.3. Учитывая, что в правой и левой частях приведенного сравнения стоят числа, не превосходящие по абсолютной величине единицы, то разность между ними, по абсолютной величине, не превосходит двух и меньше любого нечетного простого числа  $p$ . Следовательно, мы можем заменить знак сравнения на знак равенства. Лемма доказана.  $\square$

*Завершение доказательства леммы 4.3.* Рассмотрим оставшиеся утверждения. Для этого зафиксируем множество чисел  $a, 2a, \dots, \frac{p-1}{2}a$  и разделим каждое из них с остатком на  $p$

$$\begin{cases} a = q_1 p + r_1, \\ 2a = q_2 p + r_2, \\ \dots \\ \frac{p-1}{2}a = q_{\frac{p-1}{2}} p + r_{\frac{p-1}{2}}, \end{cases} \quad (4.8)$$

где  $0 \leq r_k < p$ ,  $1 \leq k \leq \frac{p-1}{2}$ . В обозначениях леммы Гаусса (лемма 4.4) получаем, что остатки  $r_k$  совпадают со множеством чисел

$$a_1, a_2, \dots, a_\lambda, p - b_1, p - b_2, \dots, p - b_\mu,$$



следовательно, можно записать равенство

$$\sum_{k=1}^{\frac{p-1}{2}} r_k = A - B + \mu p, \quad A = a_1 + \dots + a_\lambda, \quad B = b_1 + \dots + b_\mu.$$

Сложим почленно все равенства в (4.8) и, учитывая равенство<sup>1</sup>

$$1 + 2 + \dots + \frac{p-1}{2} = \left(1 + \frac{p-1}{2}\right) \frac{p-1}{4} = \frac{p^2-1}{8},$$

получим

$$a \left( \frac{p^2-1}{8} \right) = p \sum_{k=1}^{\frac{p-1}{2}} q_k + A - B + \mu p. \quad (4.9)$$

Из доказательства леммы Гаусса следует, что все числа  $a_1, \dots, a_\lambda$  и  $b_1, \dots, b_\mu$  суть числа от 1 до  $\frac{p-1}{2}$ . Следовательно,


$$A + B = 1 + 2 + \dots + \frac{p-1}{2} = \frac{p^2-1}{8}, \quad \text{или} \quad A = \frac{p^2-1}{8} - B.$$

Подставляя в (4.9) полученные равенства и перенося  $\frac{p^2-1}{8}$  в правую часть, получим

$$\frac{p^2-1}{8}(a-1) = p \sum_{k=1}^{\frac{p-1}{2}} q_k - 2B + \mu p. \quad (4.10)$$

Поскольку  $p$  нечетное число, то выполнено сравнение  $p \equiv 1 \pmod{2}$ . Пусть  $a = 2$ , тогда равенство (4.10) может быть записано в виде сравнения

$$\frac{p^2-1}{8} \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu \pmod{2}.$$

Заметим, что при  $a = 2$  значения всех  $q_k$ ,  $1 \leq k \leq \frac{p-1}{2}$ , определяемых равенствами (4.8), равны нулю. Это, очевидно, следует из того, что все числа вида  $ka$  при всех  $1 \leq k \leq \frac{p-1}{2}$  не превосходят величины  $p$ . Таким образом, 

$$\frac{p^2-1}{8} \equiv \mu \pmod{2}$$

---

<sup>1</sup>Мы используем равенство  $1 + 2 + \dots + m = \frac{m(m+1)}{2}$ , при  $m = \frac{p-1}{2}$ .

и, учитывая лемму Гаусса, мы завершаем доказательство пятого утверждения леммы

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

Перейдем к доказательству последнего, шестого утверждения леммы – квадратичного закона взаимности Гаусса. Пусть  $a$  нечетное простое число, отличное от  $p$ . Тогда равенство (4.10) может быть записано в виде сравнения

$$0 \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu \pmod{2} \quad \text{или} \quad \sum_{k=1}^{\frac{p-1}{2}} q_k \equiv \mu \pmod{2}.$$

В силу определения, выполнено равенство  $q_k = \left\lfloor \frac{ka}{p} \right\rfloor$  и  $\mu \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$ , откуда, по лемме Гаусса, получаем

$$\left(\frac{a}{p}\right) = (-1)^\mu = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

Аналогичными рассуждениями получаем равенство  $\left(\frac{p}{a}\right) = (-1)^{\sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor}$ , следовательно,

$$\left(\frac{a}{p}\right) \left(\frac{p}{a}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor}.$$

Нам осталось вычислить сумму, образующую степень, в которую возводится  $-1$ , и показать, что выполнено равенство

$$S_1 + S_2 = \frac{(p-1)(a-1)}{4}, \quad \text{где} \quad S_1 = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor, \quad S_2 = \sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor.$$

Воспользуемся геометрическими рассуждениями и покажем, что искомая сумма равна количеству точек с целыми координатами, расположенными внутри некоторого прямоугольника.

Рассмотрим сумму  $S_1$ . При фиксированном индексе  $k$  из интервала  $1 \leq k \leq \frac{p-1}{2}$  величина  $\left\lfloor \frac{ka}{p} \right\rfloor$  есть количество целых чисел  $y$ , удовлетворяющих неравенству  $0 \leq y < \frac{ka}{p}$ . Заметим, что мы можем не учитывать нулевые значения величины  $y$ , поскольку они не изменяют величину  $S_1$ .

Подставляя первое неравенство во второе и замечая, что интервал  $(\frac{p-1}{2}, \frac{p}{2})$  не содержит целых точек, мы получаем, что  $S_1$  есть число всех точек  $(k, y)$ , с целыми координатами, удовлетворяющими неравенствам

$$0 < k < \frac{p}{2}, \quad 0 < y < \frac{a}{2}, \quad py - ak < 0.$$

Аналогичным способом получаем, что  $S_2$  есть количество точек  $(k, y)$ , с целыми координатами, удовлетворяющими неравенствам

$$0 < k < \frac{p}{2}, \quad 0 < y < \frac{a}{2}, \quad py - ak > 0.$$

Поскольку в указанных границах не найдется ни одной пары целых чисел таких, что  $py = ak$ , то мы получаем, что сумма  $S_1 + S_2$  есть количество точек с целыми координатами, расположенными внутри прямоугольника со сторонами  $\frac{p}{2}$  и  $\frac{a}{2}$ . Поскольку числа  $p$  и  $a$  нечетны, то  $S_1 + S_2 = \frac{p-1}{2} \cdot \frac{a-1}{2}$ . Лемма доказана.  $\square$

Скажем несколько слов о способах вычисления символа Лежандра. Наиболее очевидный способ заключается в использовании критерия Эйлера. Однако при больших значениях чисел  $a, p$  возведение в степень может быть реализовано только с использованием специальных вычислителей или ЭВМ.

Второй подход к вычислению символа Лежандра основывается на факторизации числа  $a$  на множители и последующем применении четвертого, пятого и шестого утверждений леммы. Поскольку задача факторизации является, в общем случае, значительно более сложной задачей, то подобный подход тоже не является эффективным.

Для быстрого вычисления символа Лежандра принято использовать его обобщение – символ Якоби. Использование вычислений с символом Якоби оказывается не только эффективнее, чем использование критерия Эйлера, но и позволяет вычислять символ Лежандра для достаточно больших значений  $p$  и  $a$  без использования специальных вычислителей.

## 4.2 Символ Якоби

**Определение 4.3.** Пусть  $m > 0$  – нечетное целое число, для которого известно каноническое разложение на простые сомножители

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i},$$

где  $p_i$  простые числа,  $\alpha_i$  целые неотрицательные числа,  $k$  натуральное и  $1 \leq i \leq k$ .

Рассмотрим целое число  $a$  и определим символ Якоби равенством

$$\left(\frac{a}{m}\right) = \begin{cases} 0, & \text{если } \text{НОД}(a, m) > 1, \\ \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}, & \text{если } \text{НОД}(a, m) = 1, \end{cases}$$

где в последнем произведении используется символ Лежандра.

Символ Якоби вводится для эффективного вычисления символа Лежандра и не несет другой смысловой нагрузки.

Приведем пример и рассмотрим случай  $m = pq$ , где  $p, q$  – простые числа. Выберем квадратичный невычет  $a$  по модулям  $p$  и  $q$ , тогда каждое уравнение системы

$$\begin{cases} x^2 \equiv a \pmod{p}, \\ x^2 \equiv a \pmod{q}, \end{cases}$$

не имеет решений. Таким образом, система решений не имеет и, следовательно, сравнение  $x^2 \equiv a \pmod{m}$  также не имеет решений. В то же время выполнено равенство  $\left(\frac{a}{m}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) = (-1)^2 = 1$ .

**Лемма 4.5.** Пусть  $m > 0$  – нечетное целое,  $a$  – произвольное целое число. Для символа Якоби  $\left(\frac{a}{m}\right)$  выполнены следующие свойства.

1. Если  $b \equiv a \pmod{m}$ , то  $\left(\frac{b}{m}\right) = \left(\frac{a}{m}\right)$ .
2. Выполнены равенства  $\left(\frac{1}{m}\right) = 1$  и  $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ .
3. Если  $a = 2$ , то  $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$ .
4. Если  $a = bc$ , то  $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right) \left(\frac{c}{m}\right)$ .
5. Если  $n, m$  нечетные целые числа, то

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

*Доказательство.* Мы построим доказательство основываясь на утверждениях леммы 4.3.

Пусть  $m = \prod_{i=1}^k p_i^{\alpha_i}$  – каноническое разложение числа  $m$  на простые сомножители. Для всех простых делителей  $p_i$  числа  $m$  из сравнения  $b \equiv a$

$(\bmod m)$  следует сравнение  $b \equiv a \pmod{p_i}$ . Тогда, в силу первого утверждения леммы 4.3, получаем равенство

$$\left(\frac{b}{m}\right) = \prod_{i=1}^k \left(\frac{b}{p_i}\right)^{\alpha_i} = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{\alpha_i} = \left(\frac{a}{m}\right),$$

из которого следует первое утверждение леммы.

Равенство  $\left(\frac{1}{m}\right) = 1$  доказывается аналогично. Для доказательства равенства  $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$  заметим, что выполнено равенство

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right) = (-1)^{\sum_{i=1}^r \frac{p_i-1}{2}} = (-1)^{2N + \sum_{i=1}^r \frac{p_i-1}{2}},$$

для произвольного целого значения  $N$ . Отметим, что произведение и суммирование производится по всем простым сомножителям  $m$  с учетом их кратности.

Воспользовавшись равенством

$$\begin{aligned} \frac{m-1}{2} &= \frac{p_1 \cdots p_r - 1}{2} = \\ &= \frac{\left(1 + 2 \cdot \frac{p_1-1}{2}\right) \cdots \left(1 + 2 \cdot \frac{p_r-1}{2}\right) - 1}{2} = \\ &= \frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} + 2N, \end{aligned}$$

получим равенство  $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ , которое завершает доказательство второго утверждения леммы.

Третье утверждение леммы доказывается при помощи аналогичного технического приема. Выполнено равенство

$$\left(\frac{2}{m}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right) = (-1)^{\sum_{i=1}^r \frac{p_i^2-1}{8}} = (-1)^{2N + \sum_{i=1}^r \frac{p_i^2-1}{8}},$$

для произвольного целого значения  $N$ .

Тогда, воспользовавшись равенством

$$\begin{aligned} \frac{m^2-1}{8} &= \frac{p_1^2 \cdots p_r^2 - 1}{8} = \\ &= \frac{\left(1 + 8 \cdot \frac{p_1^2-1}{8}\right) \cdots \left(1 + 8 \cdot \frac{p_r^2-1}{8}\right) - 1}{8} = \\ &= \frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8} + 2N, \end{aligned}$$

получим третье утверждение леммы.

Легко заметить, что четвертое утверждение леммы доказывается тем же способом, что и первое утверждение леммы. Действительно,

$$\left(\frac{a}{m}\right) = \prod_{i=1}^k \left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{\alpha_i} \cdot \prod_{i=1}^k \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{b}{m}\right) \left(\frac{c}{m}\right).$$

Согласно четвертому утверждению леммы получаем, что в случае, если  $a = b^2c$  и  $\text{НОД}(a, m) = 1$ , то

$$\left(\frac{a}{m}\right) = \left(\frac{b^2c}{m}\right) = \left(\frac{c}{m}\right).$$

Последнее утверждение леммы является аналогом квадратичного закона взаимности Гаусса для символа Якоби. Пусть, как и ранее,  $m = \prod_{i=1}^r p_i$  – каноническое разложение числа  $m$  на простые сомножители, с учетом их кратности, а  $n = \prod_{i=1}^s q_i$  – разложение числа  $n$ . Тогда, следуя квадратичному закону взаимности, получим

$$\begin{aligned} \left(\frac{n}{m}\right) &= \prod_{i=1}^r \left(\frac{n}{p_i}\right) = \prod_{j=1}^s \prod_{i=1}^r \left(\frac{q_j}{p_i}\right) = \\ &= (-1)^{\sum_{j=1}^s \sum_{i=1}^r \frac{q_j-1}{2} \cdot \frac{p_i-1}{2}} \prod_{j=1}^s \prod_{i=1}^r \left(\frac{p_i}{q_j}\right) = \\ &= (-1)^{\left(\sum_{j=1}^s \frac{q_j-1}{2}\right) \cdot \left(\sum_{i=1}^r \frac{p_i-1}{2}\right)} \left(\frac{m}{n}\right). \end{aligned}$$

Аналогично рассуждениям, высказанным при доказательстве второго утверждения данной леммы, получим равенства

$$\frac{m-1}{2} = \sum_{i=1}^r \frac{p_i-1}{2} + 2N_1, \quad \frac{n-1}{2} = \sum_{i=1}^s \frac{q_i-1}{2} + 2N_2,$$

где  $N_1, N_2$  некоторые целые числа, и равенство

$$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{n}\right),$$

которое завершает доказательство леммы. □

Свойства символа Якоби, которые мы только что доказали, позволяют предложить алгоритм нахождения символа Якоби, который не использует полной факторизации числа. Этот алгоритм использует только

деление на двойку, что может быть программно реализовано как сдвиг вправо на один разряд.

Подставляя в символ Якоби вместо  $m$  простое число  $p$ , мы получим способ вычисления символа Лежандра.

**Пример 4.1.** Перед тем как привести алгоритм, мы рассмотрим пример вычисления символа Якоби, состоящий из последовательного применения утверждений леммы 4.5.

$$\begin{aligned} \left(\frac{158}{57}\right) &= \left(\frac{44}{57}\right) = \left(\frac{2^2}{57}\right) \left(\frac{11}{57}\right) = \left(\frac{11}{57}\right) = \\ &= (-1)^{\frac{(11-1)(57-1)}{4}} \left(\frac{57}{11}\right) = \left(\frac{57}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1. \end{aligned}$$

Теперь мы можем описать собственно алгоритм вычисления символа Якоби.

#### Алгоритм 4.1 (Вычисление символа Якоби)

**Вход:** нечетное целое число  $m > 0$  и целое число  $a$ .

**Выход:** символ Якоби  $\left(\frac{a}{m}\right)$ .

1. Если  $a = 0$ , то определить  $\left(\frac{a}{m}\right) = 0$  и закончить алгоритм.
2. Если  $a < 0$ , то определить  $x = -a$ ,  $y = m$ ,  $s = (-1)^{\frac{m-1}{2}}$ .  
Иначе определить  $x = a$ ,  $y = m$ ,  $s = 1$ .
3. Вычислить  $c \equiv x \pmod{y}$  и определить  $x = c$ ,  $t = 0$ .
4. Если  $x = 0$ , то определить  $\left(\frac{a}{m}\right) = 1$  и закончить алгоритм.
5. Пока  $2|x$  выполнить

5.1. Определить  $x = \frac{x}{2}$  и  $t = t + 1$ .

6. Если  $t$  - нечетно, то определить  $s = s \cdot (-1)^{\frac{y^2-1}{8}}$ .

7. Если  $a > 1$ , то

7.1. Определить  $s = s \cdot (-1)^{\frac{x-1}{2} \frac{y-1}{2}}$ .

7.2. Определить  $c = x$ ,  $x = y$ ,  $y = c$  и вернуться на шаг 3.

8. Определить символ Якоби равенством  $\left(\frac{a}{m}\right) = s$  и закончить алгоритм. □

Сделаем некоторые замечания, касающиеся практической реализации изложенного алгоритма.

Значение  $s = (-1)^{\frac{m-1}{2}}$  на втором шаге алгоритма может быть вычислено следующим образом: если  $m$  нечетное число и  $m \equiv 1 \pmod{4}$ , то  $s = 1$ , в противном случае  $s = -1$ .

Действительно, если  $m \equiv 1 \pmod{4}$ , то

$$m - 1 = 4k \quad \text{и} \quad (-1)^{\frac{m-1}{2}} = (-1)^{2k} = 1,$$

для некоторого целого числа  $k$ . Это же замечание относится и к седьмому шагу алгоритма.

Аналогично вычисляется множитель для  $s$  на шестом шаге алгоритма. Если  $m$  нечетное число, то  $m = 4k \pm 1$  для некоторого целого числа  $k$ . Тогда

$$\frac{m^2 - 1}{8} = \frac{(4k \pm 1)^2 - 1}{8} = 2k^2 \pm k.$$

Получаем, что при четном  $k$ , выполнено равенство  $(-1)^{\frac{m^2-1}{2}} = 1$ , а при нечетном  $k$  – равенство  $(-1)^{\frac{m^2-1}{2}} = -1$ .

Таким образом, если  $m \equiv 1, 7 \pmod{8}$ , что равносильно тому, что  $k$  четно, то на шестом шаге алгоритма ничего не происходит. В противном случае, когда  $m \equiv 3, 5 \pmod{8}$ , величина  $s$  меняет знак.

### 4.3 Вычисление квадратного корня

В предыдущем разделе мы рассмотрели вопрос разрешимости сравнения (4.1)

$$x^2 \equiv a \pmod{p},$$

где  $p$  нечетное простое число. Теперь мы покажем, как найти решение данного сравнения.

Вначале нам потребуется получить несколько вспомогательных результатов.

**Лемма 4.6.** Пусть  $p$  нечетное простое число,  $a$  – целое число, взаимно простое с  $p$ . Если сравнение  $x^2 \equiv a \pmod{p}$  разрешимо, то выполнены следующие утверждения.

1. Если  $p \equiv 3 \pmod{4}$ , то  $x \equiv a^{\frac{p+1}{4}} \pmod{p}$ .

2. Если  $p \equiv 5 \pmod{8}$ , то

a) если  $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$ , то  $x \equiv a^{\frac{p+3}{8}} \pmod{p}$ ,

b) если  $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$ , то

$$x \equiv 2a(4a)^{\frac{p-5}{8}} \pmod{p}.$$



*Доказательство.* Рассмотрим случай  $p \equiv 3 \pmod{4}$ . Если  $x$  удовлетворяет сравнению  $x \equiv a^{\frac{p+1}{4}} \pmod{p}$ , то, учитывая критерий Эйлера (см. лемму 4.3), получим

$$x^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \cdot \left(\frac{a}{p}\right) \equiv a \pmod{p}.$$

Первое утверждение леммы доказано.

Для доказательства второго утверждения заметим, что если выполнено  $p \equiv 5 \pmod{8}$ , то  $4|p-1$  и дробь  $\frac{p-1}{4}$  является целым числом.

Поскольку  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , то выполнено одно из двух сравнений

$$a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}.$$

Рассмотрим случай  $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$  и определим  $x \equiv a^{\frac{p+3}{8}} \pmod{p}$ , тогда

$$x^2 \equiv a^{\frac{p+3}{4}} \equiv \left(a^{\frac{p-1}{4}}\right) a \equiv a \pmod{p}.$$

В случае, когда  $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$ , определим  $x$  в соответствии с утверждением леммы, тогда

$$x^2 \equiv 4a^2 (4a)^{\frac{p-5}{4}} \equiv a (4a)^{1+\frac{p-5}{4}} \equiv a 2^{\frac{p-1}{2}} a^{\frac{p-1}{4}} \pmod{p}. \quad (4.11)$$

В силу второго и третьего утверждений леммы 4.3 следует, что

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \equiv -1 \pmod{p},$$

так как  $\frac{p^2-1}{8}$  нечетно. Действительно, вспоминая, что  $p \equiv 5 \pmod{8}$ , получим  $\frac{p^2-1}{8} = \frac{(5+8k)^2-1}{8} = 1 + 2(1 + 5k + 4k^2)$ , для некоего целого  $k$ . Тогда, возвращаясь к (4.11), получим сравнение

$$x^2 \equiv a 2^{\frac{p-1}{2}} a^{\frac{p-1}{4}} \equiv a(-1)(-1) \equiv a \pmod{p},$$

которое завершает доказательство леммы. □

Из утверждений леммы 4.6 следует, что остался лишь один случай, для которого неизвестен способ определения решения сравнения (4.1), а именно, случай  $p \equiv 1 \pmod{8}$ .

Мы начнем с доказательства одной «замечательной» леммы. Мы называем ее замечательной, поскольку она будет нами использована не только в данной, но и в последующих главах.

**Лемма 4.7.** Пусть  $p = 2^n q + 1$  простое число,  $q$  нечетное целое и  $a$  целое число такое, что  $\text{НОД}(a, p) = 1$ . Тогда

- либо  $a^q \equiv 1 \pmod{p}$ ,
- либо найдется такое целое число  $k$ ,  $0 \leq k < n$ , что

$$a^{2^k q} \equiv -1 \pmod{p}.$$

*Доказательство.* В силу малой теоремы Ферма (см. теорему 2.7) выполнено сравнение

$$a^{p-1} - 1 \equiv a^{2^n q} - 1 \equiv \left(a^{2^{n-1} q} - 1\right) \left(a^{2^{n-1} q} + 1\right) \equiv 0 \pmod{p}. \quad (4.12)$$

Тогда, в силу леммы 1.4, либо правая скобка, либо левая скобка в сравнении (4.12) делится на  $p$ . Если это правая скобка, то выполнено сравнение  $a^{2^{n-1} q} \equiv -1 \pmod{p}$  и  $k = n - 1$ . Если же это левая скобка, то мы получаем сравнение

$$a^{2^{n-1} q} - 1 \equiv \left(a^{2^{n-2} q} - 1\right) \left(a^{2^{n-2} q} + 1\right) \equiv 0 \pmod{p}.$$

Аналогично сравнению (4.12) получаем, что либо  $a^{2^{n-2} q} \equiv -1 \pmod{p}$  и  $k = n - 2$ , либо  $a^{2^{n-2} q} - 1 \equiv 0 \pmod{p}$ .

Продолжим далее и, если ни для одного  $k = n - 2, \dots, 1$  не будет выполнено утверждение леммы, придем к сравнению

$$(a^q + 1)(a^q - 1) \equiv 0 \pmod{p},$$

из которого вытекает сравнение  $a^q \equiv \pm 1 \pmod{p}$ , а также доказательство леммы.  $\square$

Из первого утверждения доказанной нами леммы получаем следующий результат. Если  $a$  квадратичный вычет по модулю  $p$  и выполнено первое утверждение леммы 4.7, то есть  $a^q \equiv 1 \pmod{p}$ , то решение сравнения  $x^2 \equiv a \pmod{p}$  определяется сравнением

$$x \equiv a^{\frac{q+1}{2}} \pmod{p}.$$

Действительно,

$$x^2 \equiv \left(a^{\frac{q+1}{2}}\right)^2 \equiv a \cdot a^q \equiv a \pmod{p}.$$

Полученная нами формула является частным случаем более общей ситуации. Основная идея решения сравнения (4.1) заключается в следующем. Легко видеть, что для любого нечетного натурального  $q$  выполнено сравнение

$$\left(a^{\frac{q+1}{2}}\right)^2 \equiv a \cdot a^q \pmod{p}.$$

Предположим, что нам известен элемент  $w$  такой, что

$$w^2 a^q \equiv 1 \pmod{p}, \quad (4.13)$$

тогда решение сравнения (4.1) примет вид  $x \equiv wa^{\frac{q+1}{2}} \pmod{p}$ . Действительно,

$$x^2 \equiv w^2 a^{q+1} \equiv a \cdot w^2 a^q \equiv a \pmod{p}.$$

Рассмотренный нами выше случай выполняется при  $w = 1$ . Для поиска вычетов  $w$ , отличных от единицы, нам необходимо рассмотреть случай, когда выполнено второе утверждение леммы 4.7. Для этого нам потребуется еще одна лемма, которая описывает свойства элементов, показатели которых по модулю  $p$  являются степенями двойки.

**Лемма 4.8.** Пусть  $p = 2^n q + 1$  простое число,  $q$  нечетное целое число и  $c$  — произвольный квадратичный невычет по модулю  $p$ . Выполнены следующие утверждения.

1. Обозначим  $z \equiv c^q \pmod{p}$ , тогда показатель  $z$  по модулю  $p$  равен  $2^n$ , то есть  $\text{ord}_p z = 2^n$ .
2. Обозначим  $z_k \equiv z^{2^k} \pmod{p}$ , тогда  $z_k \equiv z_{k-1}^2 \pmod{p}$  и  $\text{ord}_p z_k = 2^{n-k}$ .
3. Пусть  $u, v$  вычеты такие, что  $\text{ord}_p u = \text{ord}_p v = 2^{k+1}$ , тогда выполнено условие  $\text{ord}_p(uv) \mid 2^k$ .

*Доказательство.* Рассмотрим произвольный квадратичный невычет  $c$  по модулю  $p$ . Тогда  $\left(\frac{c}{p}\right) = -1$  и из критерия Эйлера (см. лемму 4.3), малой теоремы Ферма (см. теорему 2.7) и сравнений

$$\begin{aligned} c^{\frac{p-1}{2}} &\equiv c^{2^{n-1}q} \equiv z^{2^{n-1}} \equiv -1 \pmod{p}, \\ c^{p-1} &\equiv c^{2^n q} \equiv z^{2^n} \equiv 1 \pmod{p}, \end{aligned}$$

следует, что  $\text{ord}_p z = 2^n$ , то есть первое утверждение леммы.

Легко видеть, что  $z_k \equiv z^{2^k} \equiv \left(z^{2^{k-1}}\right)^2 \equiv z_{k-1}^2 \pmod{p}$ . Более того, из первого утверждения леммы 2.5 следует, что

$$\text{ord}_p z_k = \text{ord}_p z^{2^k} = \frac{\text{ord}_p z}{2^k} = 2^{n-k},$$

то есть второе утверждение леммы.

Рассмотрим третье утверждение леммы. Поскольку  $\text{ord}_p u = \text{ord}_p v = 2^{k+1}$ , то выполнены сравнения

$$u^{2^k} \equiv -1 \pmod{p}, \quad v^{2^k} \equiv -1 \pmod{p}.$$

Перемножая указанные сравнения, получим  $(uv)^{2^k} \equiv 1 \pmod{p}$ . Учитывая третье утверждение леммы 2.4, получим  $\text{ord}_p(uv) \mid 2^k$ . Лемма доказана.  $\square$

Введенные нами в утверждении леммы вычеты  $z_k$  будут использованы для построения вычета  $w$  такого, что выполнено сравнение (4.13)

$$w^2 a^q \equiv 1 \pmod{p}.$$

При этом заметим, что выполнение данного сравнения равносильно выполнению равенства  $\text{ord}_p(w^2 a^q) = 1$ . Напомним, что в силу леммы 4.7, найдется такой индекс  $k$ ,  $0 \leq k < n$ , что  $a^{2^{k+1}} \equiv -1 \pmod{p}$ , следовательно,  $\text{ord}_p a^q = 2^{k+1}$ .

Определим конечную последовательность  $u_1, u_1, \dots, u_{r+1}$  сравнениями

$$\begin{aligned} u_1 &\equiv a^q \pmod{p}, \\ u_2 &\equiv z_{l_1} u_1 \pmod{p}, \\ &\dots \\ u_{r+1} &\equiv z_{l_r} u_r \pmod{p}, \end{aligned}$$

где индексы  $l_j$  выбираются из условия  $\text{ord}_p u_j = \text{ord}_p z_{l_j}$ ,  $j = 1, \dots, r$ , а вычеты  $z_{l_j}$  определяются вторым утверждением леммы 4.8.

Из третьего утверждения леммы 4.8 следует, что

$$\text{ord}_p u_j \mid \text{ord}_p u_{j-1}, \quad \text{при } j = 2, \dots, r,$$

и выполнена цепочка неравенств

$$\text{ord}_p u_1 > \text{ord}_p u_2 > \dots > \text{ord}_p u_{r+1} = 1$$

для некоторого значения  $r \geq 1$ . Таким образом, мы получаем, что

$$u_{r+1} \equiv z_{l_1} \cdots z_{l_r} \cdot a^q \equiv 1 \pmod{p}.$$

Вспомним, что из второго утверждения леммы 4.8 следуют сравнения  $z_{l_j} \equiv z_{l_j-1}^2 \pmod{p}$  и обозначим  $w = z_{l_1-1} \cdots z_{l_r-1}$ . Тогда выполняется нужное нам сравнение (4.13)

$$z_{l_1} \cdots z_{l_r} \cdot a^q \equiv (z_{l_1-1} \cdots z_{l_r-1})^2 a^q \equiv w^2 a^q \equiv 1 \pmod{p}$$

и мы можем определить неизвестное  $x$  сравнением

$$x \equiv (z_{l_1-1} \cdots z_{l_r-1}) \cdot a^{\frac{q+1}{2}} \pmod{p}.$$

Мы рассмотрели все варианты, возникающие при вычислении решения сравнения  $x^2 \equiv a \pmod{p}$ . Суммируем все изложенное выше и приведем алгоритм, который позволяет находить решения рассматриваемого сравнения.

### Алгоритм 4.2 (Алгоритм Тонелли-Шенкса)

**Вход:** нечетное простое число  $p = 2^n q + 1$ ,  $q$  – нечетное целое и целое число  $a$  такое, что  $\left(\frac{a}{p}\right) = 1$ .

**Выход:** вычет  $x$  такой, что  $x^2 \equiv a \pmod{p}$ .

1. Если  $p \equiv 3 \pmod{4}$ , то определить  $x \equiv a^{\frac{p+1}{4}} \pmod{p}$  и остановиться.
2. Если  $p \equiv 5 \pmod{8}$ , то
  - 2.1. Если  $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$ , то определить  $x \equiv a^{\frac{p+3}{8}} \pmod{p}$  и остановиться.
  - 2.2. Если  $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$ , то определить  $x \equiv 2a(4a)^{\frac{p-5}{8}} \pmod{p}$  и остановиться.
3. Выбирая случайным образом, найти квадратичный невычет  $c$  и определить

$$z \equiv c^q \pmod{p}, \quad r = n.$$

4. Определить

$$t \equiv a^{\frac{q-1}{2}} \pmod{p}, \quad x \equiv at \pmod{p}, \quad b \equiv xt \pmod{p}.$$

5. Если  $x \equiv 1 \pmod{p}$ , то закончить вычисления,  
Иначе вычислить наименьшее  $m$  такое, что  $b^{2^m} \equiv 1 \pmod{p}$ .
6. Определить  $t \equiv z^{2^{r-m-1}} \pmod{p}$ ,

$$z \equiv t^2 \pmod{p}, \quad x \equiv xt \pmod{p}, \quad b \equiv bz \pmod{p}, \quad r = m$$

и вернуться на шаг 5. □

Приведенный алгоритм позволяет найти один корень уравнения  $x^2 \equiv a \pmod{p}$ , скажем  $e_1$ . Второй корень  $e_2$ , очевидно, находится из равенства  $e_2 = p - e_1$ .

Легко видеть, что в случае  $p \not\equiv 1 \pmod{8}$  трудоемкость приведенного алгоритма сравнима с трудоемкостью возведения вычета  $a$  в степень и может быть оценена величиной  $O(\log p)$ .

Теперь мы можем рассмотреть общий случай. Рассмотрим сравнение второй степени

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad (4.14)$$

где  $p$  – нечетное простое число,  $a \not\equiv 0 \pmod{p}$  и  $b, c$  – произвольные вычеты по модулю  $p$ .

Верна следующая теорема.

**Теорема 4.2.** Пусть  $p$  нечетное простое число,  $a, b, c$  целые числа и  $a$  взаимно просто с  $p$ . Пусть  $D \equiv b^2 - 4ac \pmod{p}$ . Тогда

1. если  $\left(\frac{D}{p}\right) = -1$ , то сравнение (4.14) не имеет решений,
2. если  $D \equiv 0 \pmod{p}$ , то сравнение (4.14) имеет единственное решение  $e \equiv -\frac{b}{2a} \pmod{p}$ ,
3. если  $\left(\frac{D}{p}\right) = 1$ , то сравнение (4.14) имеет два различных решения  $e_1, e_2$ , которые удовлетворяют сравнениям

$$e_1 \equiv \frac{-b - \xi}{2a} \pmod{p}, \quad e_2 \equiv \frac{-b + \xi}{2a} \pmod{p},$$

где  $\xi^2 \equiv D \pmod{p}$ .

*Доказательство.* Легко заметить, что решения сравнения  $ax^2 + bx + c \equiv 0 \pmod{p}$  удовлетворяют также сравнению

$$x^2 + \frac{bx}{a} + \frac{c}{a} \equiv \left(x + \frac{b}{2a}\right)^2 - \left(\frac{D}{4a^2}\right) \equiv 0 \pmod{p}$$

и разрешимость сравнения (4.14) эквивалентна разрешимости сравнения

$$z^2 \equiv D \pmod{p}, \quad \text{где } z \equiv 2ax + b \pmod{p}.$$

Таким образом, мы свели поиск корней многочлена второй степени к поиску квадратных корней из  $D$ . Теперь все утверждения доказываемой нами теоремы вытекают из теоремы 4.1.  $\square$

Мы доказали результат о разрешимости сравнения (4.14) по модулю простого числа  $p$  в зависимости от величины дискриминанта  $D$ . Теперь получим обратное утверждение – о разрешимости сравнения (4.14) для бесконечного множества простых чисел.

**Теорема 4.3.** Пусть сравнение  $ax^2 + bx + c \equiv 0 \pmod{p}$  разрешимо для некоторого нечетного простого числа  $p$ , тогда оно разрешимо для всех простых чисел, сравнимых с  $p$  по модулю  $4|D|$ , где  $D = b^2 - 4ac$ .

*Доказательство.* Из утверждения теоремы 4.2 следует, что разрешимость исходного сравнения равносильна разрешимости сравнения  $z^2 \equiv D \pmod{p}$ . Таким образом, для доказательства нашей теоремы достаточно показать, что  $\left(\frac{D}{p}\right) = \left(\frac{D}{p_1}\right)$  при  $p_1 \equiv p \pmod{4|D|}$ .

Разложим дискриминант  $D$  в произведение простых сомножителей, с учетом знака, то есть

$$D = (-1)^{\alpha_1} 2^{\alpha_2} \prod_{i=3}^k q_i^{\alpha_i},$$

при некотором натуральном  $k$ , где  $q_i$  различные нечетные простые числа,  $\alpha_i$  неотрицательные целые числа, и рассмотрим несколько случаев.

Случай первый. Поскольку  $p_1 \equiv p \pmod{4|D|}$ , то  $p_1 \equiv p \pmod{4}$  и выполнено сравнение  $\frac{p_1-1}{2} \equiv \frac{p-1}{2} \pmod{2}$ . Используя третье утверждение леммы 4.3, получаем

$$\left(\frac{-1}{p_1}\right) = (-1)^{\frac{p_1-1}{2}} = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right).$$

Случай второй. Предположим, что  $\alpha_2 \geq 1$ . Тогда  $2|D$ , выполнено сравнение  $p_1 \equiv p \pmod{8}$  и  $8|(p_1-p)$ . Учитывая, что числа  $p, p_1$  нечетны, мы получаем

$$\frac{p_1^2-1}{8} - \frac{p^2-1}{8} = (p_1+p)\frac{(p_1-p)}{8} \equiv 0 \pmod{2}.$$

Тогда из пятого утверждения леммы 4.3 следует равенство

$$\left(\frac{2}{p_1}\right) = (-1)^{\frac{p_1^2-1}{8}} = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right).$$

Случай третий. Пусть  $q$  произвольный нечетный делитель числа  $D$ . Если  $p_1 \equiv p \pmod{4|D|}$ , то  $p_1 \equiv p \pmod{q}$  и, в силу первого утверждения леммы 4.3,  $\left(\frac{p_1}{q}\right) = \left(\frac{p}{q}\right)$ .

С другой стороны, поскольку  $4|(p_1-p)$ , получаем

$$\frac{(p_1-1)(q-1)}{2} - \frac{(p-1)(q-1)}{2} = (q-1)\frac{(p_1-p)}{4} \equiv 0 \pmod{2}.$$

Воспользовавшись квадратичным законом взаимности, см. лемму 4.3, запишем равенство

$$\left(\frac{q}{p_1}\right) = (-1)^{\frac{p_1-1}{2} \frac{q-1}{2}} \left(\frac{p_1}{q}\right) = (-1)^{\frac{p_1-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Собирая все рассмотренные случаи вместе, получаем

$$\begin{aligned} \left(\frac{D}{p_1}\right) &= \left(\frac{-1}{p_1}\right)^{\alpha_1} \left(\frac{2}{p_1}\right)^{\alpha_2} \prod_{i=3}^k \left(\frac{q_i}{p_1}\right)^{\alpha_i} = \\ &= \left(\frac{-1}{p}\right)^{\alpha_1} \left(\frac{2}{p}\right)^{\alpha_2} \prod_{i=3}^k \left(\frac{q_i}{p}\right)^{\alpha_i} = \left(\frac{D}{p}\right). \end{aligned}$$

Теорема доказана.  $\square$

Утверждение доказанной теоремы позволяет в явном виде определить множество всех простых чисел, при которых разрешимо сравнение (4.14) при фиксированных значениях параметров  $a$ ,  $b$  и  $c$ .

## 4.4 Вероятностный алгоритм вычисления корней многочленов

Теперь мы зафиксируем простое число  $p$ , рассмотрим произвольный многочлен  $f(x) = \sum_{k=0}^n a_k x^k$  и зададимся вопросом о поиске решений сравнения

$$f(x) \equiv 0 \pmod{p}.$$

В случае, когда  $p$  есть маленькое простое число, мы можем в явном виде перебрать все значения  $e = 0, 1, \dots, p-1$  и проверить, вычисляя значения  $f(e) \pmod{p}$ , какое из них является корнем многочлена. При больших значениях  $p$ , очевидно, перебор не является наилучшим способом вычисления корней многочленов.

Далее мы будем считать, что  $p$  нечетное, большое простое число. Нам потребуется несколько вспомогательных теоретических результатов.

**Лемма 4.9.** *Для каждого простого числа  $p$  справедливо сравнение*

$$x^p - x \equiv x(x-1)(x-2) \cdots (x-p+1) = \prod_{k=0}^{p-1} (x-k) \pmod{p}. \quad (4.15)$$



*Доказательство.* Согласно малой теореме Ферма, см. теорему 2.7, для каждого целого числа  $e$ ,  $0 \leq e < p$ , выполнено сравнение  $e^p \equiv e \pmod{p}$ . Следовательно, каждое число  $e$  из указанного интервала является корнем многочлена  $x^p - x$  в кольце  $\mathbb{F}_p[x]$ .

С другой стороны, согласно теореме 3.2, для каждого корня  $e$  многочлена  $f(x)$  выполнено  $f(x) \equiv 0 \pmod{x - e}$ , то есть многочлен  $x - e$  делит многочлен  $f(x)$  нацело. Таким образом, в поле  $\mathbb{F}_p[x]$  многочлен  $\prod_{k=0}^{p-1} (x - k)$  делит нацело многочлен  $(x^p - x)$ .

Поскольку степени обоих многочленов совпадают, а также совпадают коэффициенты при старших степенях, мы делаем вывод о том, что выполнено искомое сравнение (4.15). Лемма доказана.  $\square$

**Лемма 4.10.** Пусть  $f(x)$  произвольный многочлен из  $\mathbb{F}_p[x]$ . Определим многочлен  $h(x)$

$$h(x) = \text{НОД}(x^p - x, f(x)).$$

Тогда каждый корень многочлена  $h(x)$  является корнем многочлена  $f(x)$  и наоборот, то есть множества корней многочленов  $h(x)$  и  $f(x)$  совпадают.

*Доказательство.* Согласно основной теореме арифметики для многочленов, см. теорему 3.1, мы можем представить  $f(x) = \sum_{k=0}^n a_k x^k$  в виде

$$f(x) = a_n (x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x),$$

где  $e_1, \dots, e_k$  различные корни многочлена  $f(x)$ , а многочлен  $u(x) \in \mathbb{F}_p[x]$  является произведением неприводимых, то есть не имеющих корней в  $\mathbb{F}_p[x]$ , многочленов.

Согласно лемме 4.9 многочлен  $x^p - x$  в кольце  $\mathbb{F}_p[x]$  раскладывается в произведение  $p$  различных линейных множителей, следовательно,

$$h(x) = \text{НОД}(x^p - x, f(x)) = (x - e_1) \cdots (x - e_r) \in \mathbb{F}_p[x].$$

Последнее равенство завершает доказательство леммы.  $\square$

Согласно утверждению последней леммы, мы можем свести задачу определения корней многочлена  $f(x)$  к определению корней многочлена  $h(x)$ , раскладывающегося в произведение линейных множителей, такого, что  $\deg h(x) \leq \deg f(x)$ .

Теперь опишем вероятностный алгоритм поиска корней многочлена  $h(x)$  по модулю простого нечетного числа  $p$ . Мы считаем, что  $\deg h(x) = r > 1$ , поскольку в противном случае он либо является константой, при

$\deg h(x) = 0$ , либо линейен, то есть  $h(x) = x - e$ . В последнем случае вычисление корня тривиально.

### Алгоритм 4.3 (Вычисление случайного корня многочлена)

**Вход:** Нечетное простое число  $p$  и многочлен  $h(x) \equiv \prod_{k=1}^r (x - e_k) \pmod{p}$ , распадающийся на линейные множители в  $\mathbb{F}_p[x]$  с неизвестными значениями  $e_1, \dots, e_r$ .

**Выход:** Корень многочлена – одно из значений  $e_1, \dots, e_r$ .

1. Выбрать случайное значение  $c \in \mathbb{F}_p$ . Если  $h(c) \equiv 0 \pmod{p}$ , то закончить алгоритм и вернуть значение  $c$  в качестве корня многочлена  $h(x)$ .
2. Вычислить многочлен  $d(x) \in \mathbb{F}_p[x]$

$$d(x) = \text{НОД} \left( h(x), (x - c)^{\frac{p-1}{2}} - 1 \right).$$

3. Если  $\deg d(x) < 1$  или  $\deg d(x) = \deg h(x)$ , то вернуться на шаг 1).
4. Если  $\deg d(x) = 1$ , то закончить алгоритм и вернуть в качестве корня значение свободного члена многочлена  $d(x)$ .
5. Определить  $f(x) = d(x)$  и вернуться на шаг 1). □

Алгоритм 4.3 носит вероятностный характер. Алгоритм случайным образом находит какой-нибудь корень многочлена  $h(x)$ . При фиксированном числе выборов случайного значения  $c$  на первом шаге алгоритма можно оценить вероятность успешного завершения алгоритма.

**Лемма 4.11.** Пусть многочлен  $h(x)$  удовлетворяет входным данным алгоритма 4.3. Тогда выполнены следующие утверждения.

1. Алгоритм 4.3 действительно находит корень многочлена  $h(x)$ .
2. Вероятность того, что на шаге 2 алгоритма будет найден многочлен  $d(x)$  такой, что  $\deg d(x) > 0$ , не менее  $\frac{1}{2}$ .

*Доказательство.* Покажем, что алгоритм действительно находит корень многочлена  $h(x)$ . Завершение работы алгоритма на первом и четвертом шагах очевидно. В первом случае мы в явном виде предъявляем корень, которым является значение  $e$ . Во втором случае мы находим многочлен  $d(x) = x - e$  такой, что  $d(x) | h(x) = \prod_{k=1}^r (x - e_k)$ . Следовательно, согласно теореме 3.2, значение  $e$  – свободный член многочлена  $d(x)$  будет являться корнем многочлена  $h(x)$ .

Если многочлен  $d(x) = \text{НОД} \left( h(x), (x - c)^{\frac{p-1}{2}} - 1 \right)$  имеет степень большую единицы, то в силу того, что  $d(x) | h(x)$ , он является произведением линейных множителей, свободные члены которых являются корнями многочлена  $h(x)$ . Заметим, что  $\deg d(x) < \deg h(x)$ , следовательно, после присваивания на 5 шаге алгоритма, степень многочлена уменьшается. Таким образом, после не более чем  $r$  делений, мы получим в

качестве  $d(x)$  многочлен первой степени, что даст нам искомое значение корня.

Для доказательства первого утверждения леммы нам осталось показать, что на втором шаге мы действительно вычислим многочлен  $d(x)$  такой,  $d(x)|f(x)$  и  $\deg d(x) > 0$ .

Поскольку мы считаем, что  $\deg h(x) > 1$ , то зафиксируем два произвольных корня  $e_1, e_2$  и определим множество  $\mathcal{D}$

$$\mathcal{D} = \{c \in \mathbb{F}_p : (e_1 - c)^{\frac{p-1}{2}} \not\equiv (e_2 - c)^{\frac{p-1}{2}} \pmod{p}\}.$$

Выберем некоторый вычет  $c \in \mathcal{D}$  и рассмотрим многочлен

$$v(x) = (x - c)^{\frac{p-1}{2}} - 1, \quad \deg v(x) = \frac{p-1}{2}.$$

В силу критерия Эйлера и свойств символа Лежандра, см. лемму 4.3, для каждого вычета  $e \in \mathbb{F}_p$ ,  $e \not\equiv c \pmod{p}$  выполнено либо сравнение  $v(e) \equiv 0 \pmod{p}$ , либо сравнение  $v(e) \equiv -2 \pmod{p}$ . В первом случае, очевидно, получаем, что  $e$  является корнем многочлена  $v(x)$  по модулю  $p$ .

Поскольку вычетов и невычетов по модулю  $p$  ровно  $\frac{p-1}{2}$ , то получаем, что многочлен  $v(x)$  раскладывается в произведение  $\frac{p-1}{2}$  линейных множителей

$$v(x) = (x - \gamma_1) \cdots (x - \gamma_{\frac{p-1}{2}}),$$

где  $\gamma_i$  вычеты, такие что  $\gamma_i - c$  является квадратичным вычетом по модулю  $p$ . В силу выбора элемента  $c \in \mathcal{D}$  по крайней мере один корень многочлена  $h(x)$  либо  $e_1$ , либо  $e_2$  входит в множество вычетов  $\gamma_1, \dots, \gamma_{\frac{p-1}{2}}$ . Следовательно, степень многочлена  $d(x) = \text{НОД}(h(x), v(x))$  больше нуля. Первое утверждение леммы доказано.

Для утверждения второго утверждения леммы нам достаточно оценить мощность множества  $\mathcal{D}$ .

Рассмотрим многочлен  $(e_1 - x)^{\frac{p-1}{2}} - (e_2 - x)^{\frac{p-1}{2}}$  степени  $\frac{p-3}{2}$ . Согласно теореме 3.3 в поле  $\mathbb{F}_p$  этот многочлен имеет не более  $\frac{p-3}{2}$  корней. Поскольку корни рассматриваемого многочлена не принадлежат множеству  $\mathcal{D}$ , мы получаем, что мощность множества  $\mathcal{D}$  удовлетворяет неравенству

$$|\mathcal{D}| \geq p - \frac{p-3}{2} = \frac{p+3}{2}.$$

Таким образом выбирая случайное значение  $c$  в интервале  $0, \dots, p-1$ , мы с вероятностью  $\frac{p+3}{2p} > \frac{1}{2}$  выберем значение, принадлежащее множеству  $\mathcal{D}$ . Из этого следует второе утверждение леммы.  $\square$

Из утверждений доказанной леммы следует, что в среднем нам потребуется две попытки выбора значения  $s$  для того, чтобы разложить на множители многочлен  $h(x)$  на втором шаге алгоритма 4.3. Учитывая, что полученное разложение может не дать нам многочлен первой степени, нам потребуется, в среднем,  $2r$  попыток выбора значения  $s$  для того, чтобы определить корень многочлена  $h(x)$ . Таким образом, мы можем оценить среднюю трудоемкость алгоритма 4.3 величиной  $O(\deg h(x))$ .

Теперь суммируем полученные результаты. Пусть нам задан многочлен  $f(x) = \sum_{k=0}^n a_k x^k$  с целыми коэффициентами и мы хотим не только найти его корни в поле  $\mathbb{F}_p$ , то есть решить сравнение  $f(x) \equiv 0 \pmod{p}$ , но и представить его в виде

$$f(x) \equiv a_n(x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x) \pmod{p},$$

где  $u(x)$  есть произведение неприводимых в  $\mathbb{F}_p[x]$  многочленов. Для нахождения неизвестных значений  $e_1, \dots, e_r, \alpha_1, \dots, \alpha_r$  и  $u(x)$  можно предложить следующий алгоритм.

#### Алгоритм 4.4 (Вычисление всех корней многочлена)

**Вход:** Простое нечетное число  $p$  и многочлен  $f(x) = \sum_{k=0}^n a_k x^k$  такой, что  $a_n \not\equiv 0 \pmod{p}$ .

**Выход:** Значения  $e_1, \dots, e_r, \alpha_1, \dots, \alpha_r$  и многочлен  $u(x) \in \mathbb{F}_p[x]$  такие, что выполнено сравнение  $f(x) \equiv a_n(x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x) \pmod{p}$ .

1. Если  $a_n \not\equiv 1 \pmod{p}$ , то сделать многочлен  $f(x)$  унитарным, то есть определить  $f(x) \equiv a_n^{-1} f(x) \pmod{p}$ .
2. Определить многочлены  $u(x) = f(x)$  и  $h(x) = \text{НОД}(x^p - x, f(x))$ .
3. Если  $\deg h(x) = 0$ , то закончить алгоритм.
4. Используя алгоритм 4.3 вычислить  $e \in \mathbb{F}_p$  такой, что  $h(e) \equiv 0 \pmod{p}$  и определить  $\alpha = 0$ .
5. Пока  $f(x) \equiv 0 \pmod{x - e}$  выполнить
  - 5.1. Определить  $f(x) = \frac{f(x)}{(x - e)}$  и вычислить  $\alpha = \alpha + 1$ .
6. Вычислить  $u(x) = \frac{u(x)}{(x - e)^\alpha}$  и  $h(x) = \frac{h(x)}{(x - e)}$ .
7. Добавить пару  $e, \alpha$  в список корней и их кратностей и перейти на шаг 3.  $\square$

Мы могли бы оптимизировать число делений многочлена  $h(x)$ , возникающих при вызове алгоритма 4.3. Это привело бы нас к рекурсивной версии алгоритма. Поскольку рекурсии являются достаточно медленными при практической реализации на ЭВМ, мы пожертвовали возможностью снизить трудоемкость алгоритма за счет снижения времени его работы: нерекурсивная версия алгоритма на практике работает быстрее.

## НЕПРЕРЫВНЫЕ ДРОБИ

**Определение непрерывной дроби - Понятие подходящей дроби - Теорема о наилучшем приближении - Квадратичные иррациональности и их свойства - Иррациональности старших степеней - Эквивалентные числа - Подходящие дроби и наилучшие приближения.**

Рассмотрим непрерывные дроби действительных чисел.

**Определение 5.1.** Пусть  $\alpha$  действительное число. Мы будем называть целой частью  $\alpha$ , которую мы обозначаем символом  $[\alpha]$ , наибольшее целое число, меньшее, либо равное  $\alpha$ . В частном случае: целая часть целого числа совпадает с ним.

Отметим, что  $\alpha$  может быть как отрицательным, так и положительным числом. Например  $[\sqrt{13}] = 3$ , в то время как  $[-\sqrt{13}] = -4$ . В любом случае выполнено неравенство  $[\alpha] \leq \alpha$ .

Пусть  $\alpha_0$  действительное число и  $\alpha_0 \neq 0$ . Определим последовательность действительных чисел  $\alpha_1, \alpha_2, \dots$  следующим рекуррентным соотношением

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \quad \text{где } a_n = [\alpha_n]. \quad (5.1)$$

В случае, если  $\alpha_n$  является целым числом, то есть выполнено равенство  $a_n = \alpha_n$ , мы будем считать, что последовательность (5.1) обрывается.

Записав равенство (5.1) в виде  $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$ , мы можем выразить число  $\alpha_0$  в виде

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} = \dots$$

или, в общем виде,

$$\alpha_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\alpha_n}}}}, \quad (5.2)$$

для произвольного индекса  $n$ .

Для упрощенной записи равенства (5.2) мы будем использовать обозначение  $\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n]$ .

**Определение 5.2.** Пусть  $\alpha_0 \neq 0$  действительное число. Мы будем называть представление (5.2)

$$\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\alpha_n}}}},$$

$n = 1, 2, \dots$  непрерывной или цепной дробью числа  $\alpha_0$ . Элементы последовательности  $a_0, a_1, \dots$  мы будем называть неполными частными, а элементы последовательности  $\alpha_1, \alpha_2, \dots$  полными частными.

Заметим, что из соотношения (5.1) и неравенства  $[\alpha] \leq \alpha$  вытекает выполнимость следующих неравенств

$$0 \leq \alpha_n - [\alpha_n] < 1 \quad \text{и} \quad \alpha_n > 1, \quad a_n \geq 1 \quad \text{при} \quad n \geq 1. \quad (5.3)$$

## 5.1 Конечные непрерывные дроби

Остановимся на частном случае, когда последовательность полных частных  $\alpha_0, \alpha_1, \dots, \alpha_n$  конечна. Верна следующая лемма.

**Лемма 5.1.** Пусть  $\alpha_0 \neq 0$  действительное число. Последовательность полных частных  $\alpha_1, \alpha_2, \dots$ , определяемая соотношениями (5.1), обрывается тогда и только тогда, когда  $\alpha_0$  рациональное число.

*Доказательство.* Если последовательность конечна, то найдется индекс  $n$ , такой что  $\alpha_n$  целое число и  $\alpha_n = a_n$ . Тогда  $\alpha_{n-1} = a_{n-1} + \frac{1}{a_n}$  является рациональным числом. Выполняя аналогичные рассуждения для всех индексов, меньших  $n$ , получаем, что  $\alpha_0$  является рациональным числом.

Если  $\alpha_0$  рациональное число, то оно представимо в виде несократимой дроби  $\alpha_0 = \frac{p}{q}$ . Применим к числам  $p, q$  алгоритм Эвклида, см. алгоритм 1.1, а именно представим

$$p = a_0 q + r_1, \quad \text{где} \quad 0 \leq r_1 < q.$$

Тогда  $\alpha_0 = \frac{p}{q} = a_0 + \frac{1}{\alpha_1}$ , где  $\alpha_1 = \frac{q}{r_1}$ . Производя деление  $q$  на  $r_1$  с остатком, получим

$$q = a_1 r_1 + r_2, \quad \text{где} \quad 0 \leq r_2 < r_1,$$

что равносильно  $\alpha_1 = \frac{q}{r_1} = a_1 + \frac{1}{\alpha_2}$ , где  $\alpha_2 = \frac{r_1}{r_2}$ .

Продолжая этот процесс, мы получим равенство

$$\alpha_n = \frac{r_{n-1}}{r_n},$$

где

$$\begin{aligned} r_{-1} &= p, \quad r_0 = q, \\ r_{n-1} &= a_n r_n + r_{n+1}, \quad 0 \leq r_{n+1} < r_n. \end{aligned} \quad (5.4)$$

Последовательность  $r_0, r_1, \dots$  образует строго убывающую последовательность неотрицательных целых чисел, следовательно, найдется такой индекс  $n$ , что  $r_{n+1} = 0$ . Из этого равенства следует, что  $\alpha_n = a_n = \frac{r_{n-1}}{r_n}$  является целым числом. Последнее рассуждение завершает доказательство леммы.  $\square$

Из утверждения доказанной нами леммы следует, что рассматриваемая последовательность  $\alpha_1, \alpha_2, \dots$  бесконечна, если  $\alpha_0$  является действительной иррациональностью, то есть не может быть представлено в виде несократимой дроби.

## 5.2 Понятие подходящей дроби

Для каждого индекса  $n$  мы можем рассмотреть рациональную дробь  $\frac{P_n}{Q_n}$ , определяемую равенством

$$\frac{P_n}{Q_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}} = [a_0, a_1, \dots, a_{n-1}, a_n]. \quad (5.5)$$

**Определение 5.3.** Пусть  $\alpha_0 \neq 0$  действительное число. Дробь  $\frac{P_n}{Q_n}$ , определяемая равенством (5.5), называется подходящей дробью к числу  $\alpha_0$ .

Нам потребуются следующие леммы, описывающие свойства числителей и знаменателей подходящих дробей.

**Лемма 5.2.** Пусть  $\alpha_0 \neq 0$  действительное число. Для числителей  $P_n$  и знаменателей  $Q_n$  подходящих дробей числа  $\alpha_0$  выполнены следующие рекуррентные соотношения

$$\begin{aligned} P_{n+1} &= a_{n+1}P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1}Q_n + Q_{n-1}, \end{aligned} \quad (5.6)$$

где  $P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1$ .

*Доказательство.* Из определения 5.3 следуют равенства

$$\frac{P_0}{Q_0} = a_0, \quad \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1},$$

которые задают начальные значения для соотношений (5.6).

Проведем доказательство по индукции. Предположим, что утверждение леммы выполнено для всех индексов равных или меньших  $n$ , то есть выполнено равенство

$$\frac{P_n}{Q_n} = [a_0, a_1, \dots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}}.$$

Тогда утверждение леммы следует из следующего равенства

$$\begin{aligned} \frac{P_{n+1}}{Q_{n+1}} &= [a_0, a_1, \dots, a_n, a_{n+1}] = \\ &= \left[ a_0, a_1, \dots, a_n + \frac{1}{a_{n+1}} \right] = \frac{\left( a_n + \frac{1}{a_{n+1}} \right) P_{n-1} + P_{n-2}}{\left( a_n + \frac{1}{a_{n+1}} \right) Q_{n-1} + Q_{n-2}} = \\ &= \frac{a_{n+1} (a_n P_{n-1} + P_{n-2}) + P_{n-1}}{a_{n+1} (a_n Q_{n-1} + Q_{n-2}) + Q_{n-1}} = \frac{a_{n+1} P_n + P_{n-1}}{a_{n+1} Q_n + Q_{n-1}}. \end{aligned}$$

□

Основываясь на доказательстве леммы 5.2, легко заметить, что из равенства

$$[a_0, \dots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}},$$

следует равенство

$$\alpha_0 = [a_0, \dots, \alpha_{n+1}] = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}. \quad (5.7)$$

Отметим, что неравенство (5.3) и формулы (5.6) позволяют заключить, что числители и знаменатели подходящих дробей удовлетворяют неравенствам

$$P_n > 0, \quad Q_n > 0.$$

Далее мы будем считать, что действительное число  $\alpha$  является как рациональным, так и иррациональным.



**Лемма 5.3.** При всех индексах  $n = 0, 1, \dots$  для числителей  $P_n$  и знаменателей  $Q_n$  подходящих дробей выполнено следующее соотношение

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^n. \quad (5.8)$$

*Доказательство.* Используя равенства (5.6), получим следующие равенства

$$\begin{aligned} P_{n+1}Q_n - Q_{n+1}P_n &= (a_{n+1}P_n + P_{n-1})Q_n - (a_{n+1}Q_n + Q_{n-1})P_n = \\ &= -(P_nQ_{n-1} - Q_nP_{n-1}) = (-1)^2(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) = \dots \\ &= (-1)^k(P_{n-k+1}Q_{n-k} - Q_{n-k+1}P_{n-k}), \end{aligned}$$

для любого  $k = 1, 2, \dots$

Подставляя в полученные равенства  $k = n + 1$  и начальные значения  $P_{-1} = 1, P_0 = a_0, Q_{-1} = 0, Q_0 = 1$  из (5.6), получим равенство

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^{n+2},$$

которое равносильно утверждению леммы.  $\square$

**Следствие 1.** Для любого индекса  $n = 0, 1, \dots$  подходящая дробь  $\frac{P_n}{Q_n}$  несократима.

*Доказательство.* Следствие очевидным образом следует из равенства (5.8). Если предположить обратное, то найдется целое число  $d_n$  такое, что  $\text{НОД}(P_n, Q_n) = d_n > 1$  и  $d_n | (-1)^{n+1}$ . Последнее условие невыполнимо.  $\square$

Докажем еще одно следствие, которое может быть использовано для решения сравнений первой степени.

**Следствие 2.** Пусть  $a$  и  $m$  взаимно простые целые числа и  $\frac{P_0}{Q_0}, \dots, \frac{P_n}{Q_n}$  последовательность подходящих дробей к числу  $\alpha = \frac{m}{a}$ . Тогда решение уравнения  $ax \equiv b \pmod{m}$  удовлетворяет сравнению

$$x \equiv (-1)^n b P_{n-1} \pmod{m}$$

для некоторого натурального индекса  $n$ .

*Доказательство.* Разложим число  $\alpha = \frac{m}{a}$  в непрерывную дробь и определим последовательность подходящих дробей  $\frac{P_0}{Q_0}, \dots, \frac{P_n}{Q_n}$ . Поскольку  $\alpha$  рациональное число, то согласно лемме 5.1, непрерывная дробь конечна и найдется индекс  $n$  такой, что  $\frac{P_n}{Q_n} = \frac{m}{a}$ .

Поскольку дробь  $\frac{P_n}{Q_n}$  несократима, а числа  $m$ ,  $a$  взаимно просты, то выполнены равенства  $P_n = m$ ,  $Q_n = a$ . Тогда, из равенства (5.8) следует, что

$$mQ_{n-1} - aP_{n-1} = (-1)^{n-1}, \quad \text{или} \quad aP_{n-1} = (-1)^n + mQ_{n-1}.$$

Последнее равенство позволяет нам записать сравнение  $aP_{n-1} \equiv (-1)^n \pmod{m}$  или, домножая на  $(-1)^nb$ , сравнение  $a(-1)^nbP_{n-1} \equiv b \pmod{m}$ . Последнее сравнение в явном виде определяет значение неизвестного  $x$ , а именно,  $x \equiv (-1)^nbP_{n-1} \pmod{m}$ . Следствие доказано.  $\square$

Внимательному читателю остается показать, в качестве упражнения, что алгоритм решения сравнения  $ax \equiv b \pmod{m}$ , основанный на доказанном следствии, полностью аналогичен расширенному алгоритму Эвклида, см. алгоритм 2.1.

Далее нам потребуется следующая лемма.

**Лемма 5.4.** *При всех индексах  $n = 0, 1, \dots$  для числителей  $P_n$  и знаменателей  $Q_n$  подходящих дробей выполнено следующее соотношение*

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(-1)^{n+1}. \quad (5.9)$$

*Доказательство.* Для доказательства леммы домножим первое равенство в (5.6) на  $Q_{n-1}$  и вычтем из полученного второе равенство из (5.6), домноженное на  $P_{n-1}$ . Учитывая предыдущую лемму, получаем, с точностью до показателя степени при  $-1$ , искомое равенство

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(P_nQ_{n-1} - Q_nP_{n-1}) = a_{n+1}(-1)^{n-1}.$$

$\square$

Доказанные нами леммы 5.3 и 5.4 позволяют получить явное представление о расположении на действительной оси элементов последовательности подходящих дробей. Согласно утверждению леммы 5.3 выполнены неравенства  $\frac{P_{2k+1}}{Q_{2k+1}} > \frac{P_{2k}}{Q_{2k}}$  при некотором натуральном  $k$ . Далее, из утверждения леммы 5.4 следует, что  $\frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}}$  и  $\frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}}$  при некотором натуральном  $k$ , то есть элементы последовательности с нечетными номерами образуют возрастающую подпоследовательность, а элементы с четными номерами – убывающую. Получаем цепочку неравенств

$$\dots \frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}} > \dots > \frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}} > \dots \quad (5.10)$$

из которой следует, что последовательность подходящих дробей сходится и имеет предел. Чему равен этот предел определяет теорема 5.1, к доказательству которой мы скоро приступим.

**Лемма 5.5.** Для всех индексов  $n = 1, 2, \dots$  знаменатели  $Q_n$  подходящих дробей удовлетворяют неравенству  $Q_{n+1} > 2^{\lceil \frac{n}{2} \rceil}$  или, что равносильно

$$\begin{cases} Q_{n+1} \geq 2^{\frac{n}{2}}, & \text{при четном } n, \\ Q_{n+1} \geq 2^{\frac{n+1}{2}}, & \text{при нечетном } n. \end{cases} \quad (5.11)$$

*Доказательство.* Из соотношений (5.3) и (5.6) следует неравенство

$$Q_{n+1} = a_{n+1}Q_n + Q_{n-1} \geq Q_n + Q_{n-1} \geq 2Q_{n-1} + Q_{n-2} \geq 2Q_{n-1},$$

из которого следует утверждение леммы – при нечетном  $n$  выполнено неравенство  $Q_{n+1} \geq 2^{\frac{n+1}{2}}Q_0 = 2^{\frac{n+1}{2}}$ , а при четном  $n$  – выполнено неравенство  $Q_{n+1} \geq 2^{\frac{n}{2}}Q_1 \geq 2^{\frac{n}{2}}$ .  $\square$

Теперь мы можем доказать теорему о приближении числа  $\alpha_0$  последовательностью подходящих дробей.

**Теорема 5.1.** Пусть  $\alpha_0 \neq 0$  действительное число. Тогда последовательность подходящих дробей сходится к  $\alpha_0$ , то есть выполнено условие

$$\alpha_0 = \lim_{n \rightarrow \infty} \frac{P_n}{Q_n}.$$

*Доказательство.* Сначала мы покажем, что последовательность подходящих дробей сходится. Действительно, из леммы 5.3 получаем равенство

$$\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n Q_{n+1}} |P_{n+1}Q_n - Q_{n+1}P_n| = \frac{1}{Q_n Q_{n+1}}.$$

Из этого равенства и из утверждения леммы 5.5 следует, что последовательность подходящих дробей сходится, то есть

$$\lim_{n \rightarrow \infty} \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = 0.$$

Нам осталось выяснить чему равен предел последовательности подходящих дробей. Учитывая равенство (5.7) и утверждение леммы 5.3, получим следующее равенство

$$\begin{aligned} \alpha_0 - \frac{P_n}{Q_n} &= \frac{1}{Q_n} (\alpha_0 Q_n - P_n) = \\ &= \frac{1}{Q_n} \left( Q_n \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}} - P_n \right) = \\ &= \frac{1}{Q_n} \left( \frac{Q_n P_{n-1} - P_n Q_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}} \right) = \frac{(-1)^n}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})}. \end{aligned} \quad (5.12)$$

Вспоминая, что  $\alpha_n$  и  $Q_n$  положительны при всех  $n \geq 1$ , получаем неравенство

$$\left| \alpha_0 - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})} \leq \frac{1}{Q_n (a_{n+1} Q_n + Q_{n-1})} = \frac{1}{Q_{n+1} Q_n}, \quad (5.13)$$

из которого вытекает утверждение теоремы.  $\square$

Из доказанной нами теоремы следует, что мы можем приблизить действительное число  $\alpha_0$  при помощи рациональной дроби с любой степенью точности. В качестве такой дроби выступает некоторая подходящая дробь. Используя подходящие дроби, можно производить эффективные вычисления с действительными числами, при некотором, заранее заданном, уровне погрешности вычислений.

**Пример 5.1.** Отойдём от общего случая и рассмотрим частный пример, а именно, разложим  $\alpha_0 = \sqrt{29}$  в непрерывную дробь.

Используя равенства (5.1) и (5.6), запишем

$$\begin{aligned} \alpha_0 &= \sqrt{29} \sim 5.3851648, \quad a_0 = \lfloor \sqrt{29} \rfloor = 5, \quad P_0 = 5, Q_0 = 1, \\ \alpha_1 &= \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{(\sqrt{29} - 5)(\sqrt{29} + 5)} = \frac{\sqrt{29} + 5}{4}, \\ a_1 &= \lfloor \alpha_1 \rfloor = \left\lfloor \frac{\sqrt{29} + 5}{4} \right\rfloor = 2, \quad P_1 = 11, \quad Q_1 = 2, \quad \frac{P_1}{Q_1} = 5.5, \end{aligned}$$

аналогично мы получим следующие равенства

$$\begin{aligned} \alpha_2 &= \frac{1}{\frac{\sqrt{29} + 5}{4} - 2} = \frac{\sqrt{29} + 3}{5}, \quad a_2 = 1, \quad \frac{P_2}{Q_2} = \frac{16}{3} = 5.333333, \\ \alpha_3 &= \frac{1}{\frac{\sqrt{29} + 3}{5} - 1} = \frac{\sqrt{29} + 2}{5}, \quad a_3 = 1, \quad \frac{P_3}{Q_3} = \frac{27}{5} = 5.4, \\ \alpha_4 &= \frac{1}{\frac{\sqrt{29} + 2}{5} - 1} = \frac{\sqrt{29} + 3}{4}, \quad a_4 = 2, \quad \frac{P_4}{Q_4} = \frac{70}{13} = 5.3846154, \\ \alpha_5 &= \frac{1}{\frac{\sqrt{29} + 3}{4} - 2} = \sqrt{29} + 5, \quad a_5 = 10, \quad \frac{P_5}{Q_5} = \frac{727}{135} = 5.3851852, \\ \alpha_6 &= \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{4}, \quad a_6 = 2, \quad \frac{P_6}{Q_6} = \frac{1524}{283} = 5.385159, \\ \alpha_7 &= \frac{1}{\frac{\sqrt{29} + 5}{4} - 2} = \frac{\sqrt{29} + 3}{5}, \quad a_7 = 1, \quad \frac{P_7}{Q_7} = \frac{2251}{418} = 5.3851675. \end{aligned}$$

Мы остановим наши вычисления и заметим, что выполнены равенства

$$\alpha_6 = \alpha_1, \quad \alpha_7 = \alpha_2, \quad \dots,$$

то есть наша последовательность полных частных заиклилась и имеет период равный 5. Мы можем записать непрерывную дробь для  $\alpha_0 = \sqrt{29}$  в виде

$$\sqrt{29} = [5; 2, 1, 1, 2, 10, 2, 1, 1, 2, 10, \dots]$$

или, в еще более короткой форме,  $\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$ . Отметим, что всего за семь шагов мы получили очень хорошее приближение к  $\alpha_0$ . Действительно,

$$\left| \alpha_0 - \frac{P_7}{Q_7} \right| = 0.0000027 < \frac{1}{Q_8 Q_7} = \frac{1}{701 \cdot 418} = 0.0000034.$$

### 5.3 Квадратичные иррациональности

Напомним, что целое число  $D$  называется полным квадратом, если найдется целое число  $d$  такое, что  $D = d^2$ .

**Определение 5.4.** Действительное число  $\alpha$  называется квадратичной иррациональностью, если найдутся такие целые, взаимно простые числа  $u > 0$ ,  $v$ ,  $w$ , что значение  $v^2 - 4uw > 0$  не является полным квадратом, а  $\alpha$  является одним из корней многочлена  $f(x) = ux^2 + vx + w$ , то есть  $f(\alpha) = 0$ .

Величина  $D = v^2 - 4uw$  называется дискриминантом квадратичной иррациональности  $\alpha$ .

**Пример 5.2.** Проиллюстрируем понятие квадратичной иррациональности. Легко видеть, что значение  $\alpha = \sqrt{29}$  является корнем многочлена  $f(x) = x^2 - 29$  и, соответственно, квадратичной иррациональностью. Также квадратичной иррациональностью является корень многочлена  $f(x) = 3x^2 - 5x - 7$  равный  $\alpha = \frac{5 + \sqrt{109}}{2}$ .

Из определения 5.4 следует, что любая квадратичная иррациональность может быть представлена в виде

$$\alpha = \frac{A + \sqrt{D}}{B}, \tag{5.14}$$

где  $A, B, D$  – целые числа,  $D = v^2 - 4uw$  не является полным квадратом и

$$\begin{cases} A = -v, B = 2u, & \text{либо} \\ A = v, B = -2u, \end{cases} \quad (5.15)$$

в зависимости от того, какой из двух корней многочлена  $f(x)$  выбирается. Если величина  $D$  удовлетворяет сравнению  $D \equiv 0 \pmod{4}$ , то из равенства  $v^2 = D + 4uv$  следует, что величина  $v$  четна. Тогда равенства (5.15) принимают вид

$$A = \mp v, B = \pm u. \quad (5.16)$$

Возникает вопрос: единственно ли указанное представление? Для ответа на него предположим, что равенство (5.14) не единственно, то есть найдется еще одна пара целых чисел  $C, E$  таких, что  $\alpha = \frac{C + \sqrt{D}}{E}$ . Тогда выполнено равенство

$$E(A + \sqrt{D}) = B(C + \sqrt{D}),$$

откуда

$$EA - BC = (B - E)\sqrt{D}. \quad (5.17)$$

В левой части равенства (5.17), в силу выбора значений  $A, B, C, E$ , находится целое число. В правой части – произведение целого числа на корень из  $N$ , не являющегося полным квадратом, то есть действительное число. Таким образом, равенство (5.17) может быть выполнено только в том случае, если в обеих его частях находятся нули. Из этого следует, что  $B = E$ ,  $A = C$  и представление (5.17) единственно.

**Определение 5.5.** Пусть  $\alpha = \frac{A + \sqrt{D}}{B}$  квадратичная иррациональность – корень многочлена  $f(x) = ux^2 + vx + w$ . Тогда второй корень этого многочлена

$$\hat{\alpha} = \frac{A - \sqrt{D}}{B}$$

называется квадратичной иррациональностью, сопряженной с  $\alpha$ .

Легко показать, что каждое действительное число, представимое в виде (5.14), является квадратичной иррациональностью. Введем многочлен с целыми коэффициентами

$$\begin{aligned} f(x) &= B^2(x - \alpha)(x - \hat{\alpha}) = \\ &= (Bx - A - \sqrt{D})(Bx - A + \sqrt{D}) = \\ &= (Bx - A)^2 - D = B^2x^2 - 2ABx + A^2 - D. \end{aligned} \quad (5.18)$$

Получаем, что  $\alpha$  является корнем многочлена  $f(x)$  второй степени с целыми коэффициентами. Если  $A^2 - D$  делится на  $B$ , то коэффициенты многочлена можно сократить на общий множитель.

Используя преобразование (5.1), разложим квадратичную иррациональность  $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ , являющуюся корнем многочлена  $f(x) = ux^2 + vx + w$ , в непрерывную дробь.

Для полного частного  $\alpha_1$  выполнено равенство

$$\begin{aligned} \alpha_1 &= \frac{1}{\alpha_0 - a_0} = \frac{1}{\frac{A_0 + \sqrt{D}}{B_0} - a_0} = \frac{B_0}{(A_0 - a_0 B_0) + \sqrt{D}} = \\ &= \frac{B_0 (A_0 - a_0 B_0) - B_0 \sqrt{D}}{(A_0 - a_0 B_0)^2 - D}. \end{aligned} \quad (5.19)$$

Обозначим символом  $\hat{\alpha}_0 = \frac{A_0 - \sqrt{D}}{B_0}$  второй корень многочлена  $f(x)$ . Тогда, используя теорему Виета, получим равенство

$$\alpha_0 \hat{\alpha}_0 = \left( \frac{A_0 + \sqrt{D}}{B_0} \right) \left( \frac{A_0 - \sqrt{D}}{B_0} \right) = \frac{w}{u},$$

откуда  $A_0^2 - D = \frac{wB_0^2}{u}$ . Обозначим  $B_{-1} = -\frac{wB_0}{u}$  и получим необходимое нам равенство  $-B_{-1}B_0 = A_0^2 - D$ , при этом из (5.15) и (5.16) следует, что  $B_{-1}$  является целым числом. Подставляя полученное равенство в (5.19) и сокращая на  $-B_0$ , получим

$$\alpha_1 = \frac{(a_0 B_0 - A_0) + \sqrt{D}}{2a_0 A_0 - a_0^2 B_0 + B_{-1}} = \frac{A_1 + \sqrt{D}}{B_1},$$

где

$$\begin{aligned} A_1 &= a_0 B_0 - A_0, \\ B_1 &= a_0(2A_0 - a_0 B_0) + B_{-1} = a_0(A_0 - A_1) + B_{-1}. \end{aligned}$$

Мы получили, что полное частное  $\alpha_1$  имеет такой же вид, как  $\alpha_0$  и также является квадратичной иррациональностью. Более того, значения  $A_1, B_1$  могут быть выражены через значения  $A_0, B_0$  и коэффициенты многочлена  $f(x)$ . Обобщим полученный результат и докажем следующую лемму.

**Лемма 5.6.** Пусть  $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$  квадратичная иррациональность, являющаяся корнем многочлена  $f(x) = ux^2 + vx + w$ ,  $D = v^2 - 4uw$ , и  $\alpha_0, \alpha_1, \dots, \alpha_n, \dots$  последовательность полных частных.

Тогда для каждого полного частного  $\alpha_{n+1}$  выполнено равенство

$$\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}},$$

где

$$\begin{aligned} A_{n+1} &= a_n B_n - A_n, \\ B_{n+1} &= a_n(A_n - A_{n+1}) + B_{n-1}, \end{aligned} \quad (5.20)$$

при  $B_{-1} = -\frac{wB_0}{u}$ , а также выполнено равенство

$$-B_n B_{n+1} = (A_{n+1}^2 - D).$$

*Доказательство.* Мы проведем доказательство по индукции. Выполнимость утверждений леммы для  $\alpha_1$  мы проверили выше. Предположим, что для всех индексов  $1, \dots, n$  утверждение леммы выполнено, тогда, аналогично (5.19), получаем

$$\begin{aligned} \alpha_{n+1} &= \frac{1}{\alpha_n - a_n} = \frac{B_n}{(A_n - a_n B_n) + \sqrt{D}} = \\ &= \frac{-B_n (A_{n+1} + \sqrt{D})}{A_{n+1}^2 - D}, \end{aligned} \quad (5.21)$$

где  $A_{n+1} = (a_n B_n - A_n)$ .

Покажем, что  $B_n | (A_{n+1}^2 - D)$ . В силу предположения индукции выполнено  $B_n | (A_n^2 - D)$ . Тогда из (5.21) и следующего равенства

$$A_{n+1}^2 - D = (a_n B_n - A_n)^2 - D = a_n^2 B_n^2 - 2a_n A_n B_n + A_n^2 - D$$

следует, что  $B_n | (A_{n+1}^2 - D)$ . Обозначим  $B_{n+1} = \frac{A_{n+1}^2 - D}{-B_n}$ , тогда

$$-B_n B_{n+1} = (A_{n+1}^2 - D). \quad (5.22)$$

Подставляя (5.22) в (5.21), получим приведенное в утверждении леммы равенство  $\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}}$ . Нам осталось получить рекуррентную формулу для  $B_{n+1}$ .

Из (5.21), с учетом изменения индексов в равенстве (5.22), получаем

$$\begin{aligned} B_{n+1} &= \frac{A_{n+1}^2 - D}{-B_n} = \frac{(a_n B_n - A_n)^2 - D}{-B_n} = \\ &= \frac{-B_n(2a_n A_n - a_n^2 B_n) + A_n^2 - D}{-B_n} = \\ &= a_n(2A_n - a_n B_n) + B_{n-1} = a_n(A_n - A_{n+1}) + B_{n-1}. \end{aligned}$$

□



Доказанная лемма определяет соотношения (5.20), которые используются для эффективного разложения квадратичной иррациональности в непрерывную дробь.

В рассмотренном нами ранее на стр. 89 примере разложение квадратичной иррациональности в непрерывную дробь оказалось периодично. Покажем, что это свойство верно для любой квадратичной иррациональности.

Для этого нам потребуется ввести еще одно определение и доказать две вспомогательные леммы.

**Определение 5.6.** Пусть  $\alpha$  – квадратичная иррациональность и  $\hat{\alpha}$ , сопряженная с  $\alpha$ . Тогда  $\alpha$  называется приведенной квадратичной иррациональностью, если

$$\alpha > 1 \quad \text{и} \quad -1 < \hat{\alpha} < 0. \quad (5.23)$$

**Лемма 5.7.** Пусть  $\alpha = \frac{A + \sqrt{D}}{B}$  приведенная квадратичная иррациональность. Тогда

$$\begin{aligned} 0 < A < \sqrt{D}, \\ 0 < B < 2\sqrt{D}. \end{aligned}$$

*Доказательство.* Пусть  $\alpha$  удовлетворяет условию леммы, тогда из неравенств (5.23) вытекают следующие утверждения.

1. Так как  $\alpha - \hat{\alpha} = \frac{2\sqrt{D}}{B} > 0$  и  $\sqrt{D} > 0$ , то выполнено  $B > 0$ .
2. Так как  $\alpha - \hat{\alpha} = \frac{2\sqrt{D}}{B} > 1$ , то выполнено  $2\sqrt{D} > B$ .
3. Так как  $\alpha + \hat{\alpha} = \frac{2A}{B} > 0$  и  $B > 0$ , то выполнено  $A > 0$ .
4. Так как  $\hat{\alpha} = \frac{A - \sqrt{D}}{B} < 0$  и  $B > 0$ , то выполнено неравенство  $A < \sqrt{D}$  и лемма доказана.

□

**Лемма 5.8.** Пусть  $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$  квадратичная иррациональность и  $\hat{\alpha}_1, \hat{\alpha}_2, \dots$  сопряженные полных частных ее разложения в непрерывную дробь. Тогда выполнены следующие утверждения.

1. Для всех  $n \geq 0$  верно равенство

$$\hat{\alpha}_{n+1} = \frac{1}{\hat{\alpha}_n - a_n}. \quad (5.24)$$

2. Значение  $\hat{\alpha}_{n+1}$  удовлетворяет равенству

$$\hat{\alpha}_{n+1} = -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n}. \quad (5.25)$$

*Доказательство.* Учитывая (5.22), первое утверждение леммы получаем из равенства

$$\begin{aligned} \frac{1}{\hat{\alpha}_n - a_n} &= \frac{B_n}{(A_n - a_n B_n) - \sqrt{D}} = \\ &= \frac{B_n (-A_{n+1} + \sqrt{D})}{A_{n+1}^2 - D} = \frac{-A_{n+1} + \sqrt{D}}{-B_{n+1}} = \hat{\alpha}_{n+1}. \end{aligned}$$

Докажем второе утверждение леммы. Используя первое утверждение леммы, разложим  $\hat{\alpha}_0$  в непрерывную дробь

$$\hat{\alpha}_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\hat{\alpha}_{n+1}}}}}.$$

Таким образом, последовательность подходящих дробей для  $\hat{\alpha}_0$  совпадает с последовательностью подходящих дробей  $\frac{P_n}{Q_n}$  для  $\alpha_0$  и, согласно (5.7), выполнено равенство

$$\hat{\alpha}_0 = \frac{\hat{\alpha}_{n+1} P_n + P_{n-1}}{\hat{\alpha}_{n+1} Q_n + Q_{n-1}}.$$

Выражая из него  $\hat{\alpha}_{n+1}$ , получим соотношение (5.25). □

**Теорема 5.2.** Пусть  $\alpha = \frac{A + \sqrt{D}}{B}$  квадратичная иррациональность. Тогда ее непрерывная дробь периодична.

*Доказательство.* Вначале предположим, что  $\alpha_0$  приведенная квадратичная иррациональность, то есть

$$\alpha_0 > 1, \quad a_0 \geq 1, \quad -1 < \hat{\alpha}_0 < 0.$$

Тогда из (5.3) следует, что  $\alpha_1 > 1$ . Далее, следуя равенству (5.24), получим

$$\frac{1}{\hat{\alpha}_1} = \hat{\alpha}_0 - a_0 < 0 - a_0 \leq -1,$$

следовательно,  $-1 < \hat{\alpha}_1 < 0$  и  $\alpha_1$  является приведенной квадратичной иррациональностью.

Продолжая далее, мы получим, что  $\alpha_2$  и все остальные полные частные  $\alpha_n = \frac{A_n + \sqrt{D}}{B_n}$  являются приведенными квадратичными иррациональностями. Из леммы 5.7 следует, что значения  $A_n, B_n$  неотрицательны, ограничены сверху и бесконечная последовательность пар  $A_n, B_n$  принимает значения на конечном множестве. Следовательно, найдется некоторый индекс  $n_0$  такой, что  $A_0 = A_{n_0}, B_0 = B_{n_0}$  и последовательность  $\alpha_n$  заиклится или, другими словами, периодична.

Для завершения доказательства теоремы нам осталось показать, что для любой квадратичной иррациональности  $\alpha_0$  найдется такой индекс  $n_0$ , что  $\alpha_{n_0}$  является приведенной квадратичной иррациональностью.

Вначале рассмотрим частный случай. Пусть

$$\alpha_0 = A_0 + \sqrt{D}$$

и  $\alpha_0$  не является приведенной. Тогда  $a_0 = A_0 + \lfloor \sqrt{D} \rfloor$  и равенство (5.24) позволяет записать неравенства

$$-1 < \hat{\alpha}_1 = \frac{1}{\hat{\alpha}_0 - a_0} = \frac{-1}{\sqrt{D} + \lfloor \sqrt{D} \rfloor} < 0.$$

Следовательно,  $\alpha_1$  приведенная квадратичная иррациональность.

Теперь перейдем к общему случаю. Рассмотрим равенство (5.25) и, учитывая равенство (5.12), полученное в ходе доказательства теоремы 5.1, при  $n \geq 1$ , получим

$$\begin{aligned} \hat{\alpha}_{n+1} &= -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n} = \\ &= -\frac{Q_{n-1}}{Q_n} \left( \frac{\hat{\alpha}_0 - \frac{P_{n-1}}{Q_{n-1}}}{\hat{\alpha}_0 - \frac{P_n}{Q_n}} \right) = -\frac{Q_{n-1}(1 + \omega_{n+1})}{Q_n}, \end{aligned} \quad (5.26)$$

где точное значение  $\omega_{n+1}$  определено равенством

$$\omega_{n+1} = \frac{\left( \frac{(-1)^{n-1}}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} - \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right)}{\hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})}}. \quad (5.27)$$

Равенство (5.26) позволяет сделать следующее заключение. Если величина  $\omega_{n+1}$  удовлетворяет неравенствам

$$-1 < \omega_{n+1} < \frac{Q_n}{Q_{n-1}} - 1, \quad (5.28)$$

то, при  $n \geq 1$ , из (5.26) вытекают неравенства  $-1 < \hat{\alpha}_{n+1} < 0$ . Следовательно,  $\alpha_{n+1}$  приведенная квадратичная иррациональность и, как мы доказали ранее, ее разложение в непрерывную дробь периодически. Следовательно, периодически разложение для  $\alpha_0$ .

Нам осталось показать, что найдется индекс  $n \geq 1$ , для которого выполнены неравенства (5.28). Рассмотрим равенство (5.27) более подробно и обозначим символом  $\delta_{n+1}$  числитель дроби, то есть

$$\delta_{n+1} = (-1)^{n-1} \left( \frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right).$$

Поскольку  $\alpha_n$  и  $Q_n$  положительные целые числа, то выполнено  $|\delta_{n+1}| < 1$ . Более того

$$\begin{aligned} |\delta_{n+1}| &= \frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \leq \\ &\leq \frac{1}{Q_{n-1}(a_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(a_{n+1} Q_n + Q_{n-1})} = \\ &= \frac{1}{Q_n Q_{n-1}} + \frac{1}{Q_{n+1} Q_n} = \frac{1}{Q_n} \left( \frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}} \right). \end{aligned} \quad (5.29)$$

Обозначим  $\gamma = \hat{\alpha}_0 - \alpha_0$  и рассмотрим знаменатель дроби (5.27), тогда

$$\begin{aligned} \left| \hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right| &\geq \\ &|\gamma| - \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \geq |\gamma| - \frac{1}{Q_{n+1} Q_n}. \end{aligned}$$

С учетом (5.29), мы получили следующее неравенство

$$\begin{aligned} |\omega_{n+1}| &\leq \frac{|\delta_{n+1}|}{|\gamma| - \frac{1}{Q_{n+1} Q_n}} \leq \\ &\left( \frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}} \right) \frac{Q_{n+1}}{Q_{n+1} Q_n |\gamma| - 1} = \\ &= \frac{Q_{n+1} + Q_{n-1}}{Q_{n+1} Q_n Q_{n-1} |\gamma| - Q_{n-1}}. \end{aligned}$$

Полученное неравенство позволяет нам сделать вывод о том, что всегда найдется индекс  $n$ , при котором будут выполнены ограничения на  $\omega_{n+1}$ , то есть неравенства (5.28). Если  $|\gamma|$  принимает большие значения, например  $|\gamma| > 1$ , то выполнение неравенств (5.28) очевидно. Более тонким является случай, когда значения  $|\gamma|$  близки к нулю.

Предположим, что  $|\gamma|$  ограничен снизу величиной

$$|\gamma| > \frac{3}{Q_n Q_{n-1}} = \frac{3Q_{n+1}}{Q_{n+1} Q_n Q_{n-1}} > \frac{Q_{n+1} + 2Q_{n-1}}{Q_{n+1} Q_n Q_{n-1}},$$

тогда выполнено  $|\omega_{n+1}| < 1$ .

В силу того, что  $Q_n$  образуют монотонно возрастающую последовательность, замечаем, что для сколь угодно малого значения  $\gamma = \hat{\alpha}_0 - \alpha_0$  найдется такой индекс  $n$ , что будет выполнено неравенство  $|\gamma| > \frac{3}{Q_n Q_{n-1}}$  и, следовательно,  $|\omega_{n+1}| < 1$ .  $\square$

Доказанная нами теорема позволяет получить оценку на величину индекса  $n$ , начиная с которого полные частные  $\alpha_n$  станут приведенными квадратичными иррациональностями.

**Следствие 1.** Пусть  $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$  квадратичная иррациональность, являющаяся корнем многочлена  $f(x) = ux^2 + vx + w$ ,  $u, v, w \in \mathbb{Z}$ , где  $u > 0$  и  $D = v^2 - 4uw$ . Тогда  $\alpha_n$  приведенная квадратичная иррациональность, если

$$n > \log_2 \left( \frac{6u}{\sqrt{D}} \right).$$

*Доказательство.* Вспомним, что

$$\gamma = \hat{\alpha}_0 - \alpha_0 = \pm \frac{2\sqrt{D}}{B_0} = \pm \frac{\sqrt{D}}{u},$$

тогда из условия леммы следуют неравенства

$$n > \log_2 \left( \frac{6u}{\sqrt{D}} \right) = \log_2 \left( \frac{6}{|\gamma|} \right) \quad \text{и} \quad 2^{n-1} > \frac{3}{|\gamma|}.$$

Из утверждения леммы 5.5 получаем

$$Q_n Q_{n-1} \geq 2^{n-1} > \frac{3}{|\gamma|} \quad \text{или} \quad |\gamma| > \frac{3}{Q_n Q_{n-1}}.$$

Таким образом,  $|\omega_{n+1}| < 1$  и следствие доказано.  $\square$

Теорема 5.2 позволяет говорить, что разложение любой квадратичной иррациональности периодически. Верно и обратное утверждение.

**Теорема 5.3.** Пусть последовательность полных частных  $\alpha_0 = \alpha$ ,  $\alpha_1, \alpha_2, \dots$  периодична. Тогда  $\alpha$  является квадратичной иррациональностью.

*Доказательство.* Воспользуемся (5.7) и запишем равенство

$$\alpha_n = \frac{P_{n-2} - \alpha_0 Q_{n-2}}{\alpha_0 Q_{n-1} - P_{n-1}},$$

выполненное для любого индекса  $n = 1, 2, \dots$

Из определения периодичности следует, что найдутся два индекса  $n$  и  $m$ , для которых будет выполнено равенство  $\alpha_n = \alpha_m$ . Тогда

$$\frac{P_{n-2} - \alpha_0 Q_{n-2}}{\alpha_0 Q_{n-1} - P_{n-1}} = \frac{P_{m-2} - \alpha_0 Q_{m-2}}{\alpha_0 Q_{m-1} - P_{m-1}},$$

откуда следует, что

$$\begin{aligned} & \alpha_0^2 (Q_{m-1} Q_{n-2} + Q_{m-2} Q_{n-1}) + \\ & \alpha_0 (Q_{m-1} P_{n-2} + P_{m-1} Q_{n-2} - P_{m-2} Q_{n-1} - Q_{m-2} P_{n-1}) + \\ & P_{m-2} P_{n-1} - P_{m-1} P_{n-2} = 0. \end{aligned}$$

Таким образом, величина  $\alpha_0$  является корнем квадратного трехчлена с целыми коэффициентами. Поскольку величины  $Q_n$  больше нуля, то старший коэффициент построенного трехчлена отличен от нуля, следовательно, величина  $\alpha_0$  является квадратичной иррациональностью.  $\square$

Нам осталось доказать последнюю теорему, которая позволяет связать между собой числители и знаменатели подходящих дробей и коэффициенты  $A_n, B_n$  разложения квадратичной иррациональности в непрерывную дробь.

**Теорема 5.4.** Пусть  $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$  действительная квадратичная иррациональность и  $\alpha_1, \alpha_2, \dots$  последовательность полных частных, удовлетворяющих равенству

$$\alpha_n = \frac{A_n + \sqrt{D}}{B_n}.$$

Тогда для всех индексов  $n = 1, 2, \dots$  числители  $P_n$  и знаменатели  $Q_n$  подходящих дробей для  $\alpha_0$  удовлетворяют равенству

$$(P_n B_0 - Q_n A_0)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}. \quad (5.30)$$

*Доказательство.* Согласно (5.7), для любого индекса  $n = 0, 1, \dots$ , мы можем записать равенство

$$\alpha_0 = \frac{\alpha_{n+1}P_n + P_{n-1}}{\alpha_{n+1}Q_n + Q_{n-1}}.$$

Вспоминая, что  $\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}}$ , получим равенство

$$\frac{A_0 + \sqrt{D}}{B_0} = \frac{P_n(A_{n+1} + \sqrt{D}) + B_{n+1}P_{n-1}}{Q_n(A_{n+1} + \sqrt{D}) + B_{n+1}Q_{n-1}},$$

которое равносильно

$$\begin{aligned} B_0(P_n(A_{n+1} + \sqrt{D}) + B_{n+1}P_{n-1}) &= \\ &= (A_0 + \sqrt{D})(Q_n(A_{n+1} + \sqrt{D}) + B_{n+1}Q_{n-1}). \end{aligned}$$

Раскрывая в последнем равенстве скобки и приводя слагаемые со множителем  $\sqrt{D}$ , получим равенство

$$\begin{aligned} B_0B_{n+1}P_{n-1} - A_0A_{n+1}Q_n - A_0B_{n+1}Q_{n-1} + B_0P_nA_{n+1} - Q_nD &= \\ &= (A_0Q_n + A_{n+1}Q_n + B_{n+1}Q_{n-1} - B_0P_n)\sqrt{D}. \end{aligned}$$

Применяя к последнему равенству рассуждения, аналогичные тем, что были применены к равенству (5.17), получим, что правая и левая части равенства равны нулю. Это позволяет из правой части равенства получить выражение для знаменателя  $Q_{n-1}$

$$Q_{n-1} = \frac{B_0P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}}, \quad (5.31)$$

а также из левой части равенства, для числителя  $P_{n-1}$

$$\begin{aligned} P_{n-1} &= \frac{A_0A_{n+1}Q_n + A_0B_{n+1}Q_{n-1} + Q_nD - B_0P_nA_{n+1}}{B_0B_{n+1}} = \\ &= \frac{Q_n(D - A_0^2) - B_0P_n(A_{n+1} - A_0)}{B_0B_{n+1}}. \end{aligned} \quad (5.32)$$

Теперь рассмотрим утверждение леммы 5.3 и равенство (5.8), в правой части которого индекс  $n$  заменен на индекс  $n - 1$ , а в левой  $(-1)^{n-1}$  на  $(-1)^{n+1}$

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}.$$

Подставляя в него полученные выше выражения (5.31), (5.32), запишем

$$P_n \frac{B_0 P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}} - Q_n \frac{Q_n(D - A_0^2) - B_0 P_n(A_{n+1} - A_0)}{B_0 B_{n+1}} = (-1)^{n+1}.$$

Домножая наше равенство на  $B_0 B_{n+1}$ , раскрывая скобки и сокращая подобные члены, получим окончательный результат

$$(P_n B_0 - Q_n A_0)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}.$$

□

В частном случае, когда  $\alpha_0 = \sqrt{N}$ , выражение (5.30) принимает вид

$$P_n^2 - Q_n^2 D = (-1)^{n+1} B_{n+1}, \quad (5.33)$$

поскольку  $A_0 = 0$  и  $B_0 = 1$ .

## 5.4 Иррациональности старших степеней

Выше, мы описали алгоритм разложения в непрерывную дробь действительного числа  $\alpha$ , являющегося корнем многочлена второй степени. Описанный алгоритм может быть обобщен и применен к разложению в непрерывную дробь корней многочленов произвольной степени.

**Определение 5.7.** Пусть задан многочлен  $f(x) = u_m x^m + u_{m-1} x^{m-1} + \dots + u_0$  с целыми коэффициентами, неприводимый над полем рациональных чисел. Если действительное число  $\alpha$  является корнем многочлена  $f(x)$ , то мы будем называть  $\alpha$  иррациональностью степени  $m$ .

Кроме того, для числа  $\alpha$  принято название – алгебраическое число.

Из неприводимости многочлена  $f(x)$  сразу следует, что число  $\alpha$  не является рациональным и раскладывается в бесконечную непрерывную дробь. Сам алгоритм разложения тесно связан со следующим преобразованием.

Пусть  $f_n(x) = u_m x^m + u_{m-1} x^{m-1} + \dots + u_0$  многочлен с целыми коэффициентами, неприводимый над полем рациональных чисел. Выберем произвольное целое значение  $a_n$  и определим многочлен

$$f_{n+1}(x) = x^m f_n \left( a_n + \frac{1}{x} \right). \quad (5.34)$$

Верна следующая лемма.



**Лемма 5.9.** Для многочлена  $f_{n+1}(x)$ , определенного равенством (5.34), выполнены следующие свойства.

1. Верно равенство  $f_{n+1}(x) = \sum_{k=0}^m \frac{f_n^{(k)}(a_n)}{k!} x^{m-k}$ .
2. Пусть  $e_1, \dots, e_s$  действительные корни многочлена  $f_n(x)$ , тогда действительные корни многочлена  $f_{n+1}(x)$  принимают вид  $\frac{1}{e_1 - a_n}, \dots, \frac{1}{e_s - a_n}$ .

*Доказательство.* В силу (5.34) для многочлена  $f_{n+1}(x)$  выполнено равенство

$$f_{n+1}(x) = x^m f_n \left( a_n + \frac{1}{x} \right) = \sum_{k=0}^m u_k x^{m-k} (a_n x + 1)^k, \quad (5.35)$$

в котором каждое слагаемое, согласно биному Ньютона (2.17), удовлетворяет

$$u_k x^{m-k} (a_n x + 1)^k = \sum_{j=0}^k u_k C_j^k a_n^j x^{m-k+j},$$

где  $C_j^k = \frac{k!}{j!(k-j)!}$ . Таким образом, каждое слагаемое в равенстве (5.35) содержит все степени  $x$  от  $m-k$  до  $m$ .

Перегруппировывая слагаемые при одинаковых степенях  $x$ , а также учитывая, что  $C_{i-k}^i = C_k^i$  получим, что для (5.35) верно равенство

$$\sum_{k=0}^m u_k x^{m-k} (a_n x + 1)^k = \sum_{k=0}^m \left( \sum_{i=k}^m u_i C_k^i a_n^{i-k} \right) x^{m-k}. \quad (5.36)$$

С другой стороны, согласно (3.13), для  $k$ -й производной многочлена выполнено равенство

$$f_n^{(k)}(x) = \sum_{i=k}^m u_i \cdot i(i-1) \cdots (i-k+1) \cdot x^{i-k} = k! \sum_{i=k}^m u_i C_k^i x^{i-k}.$$

Поставляя это равенство в (5.36), получим первое утверждение леммы.

Перейдем ко второму утверждению. Пусть  $e$  произвольный корень многочлена  $f_n(x)$ . Тогда для любого индекса  $i = 1, \dots, s$  верны равенства

$$0 = f_n(e_i) = f_n \left( a_n + \frac{1}{\gamma_i} \right) = \gamma_i^m f_n \left( a_n + \frac{1}{\gamma_i} \right) = f_{n+1}(\gamma_i),$$

где  $\gamma_i = \frac{1}{e_i - a_n}$  — корень многочлена  $f_{n+1}(x)$ . Лемма доказана.  $\square$

Теперь рассмотрим произвольную иррациональность  $\alpha$ , являющуюся корнем некоторого неприводимого многочлена  $f(x)$ , и определим последовательность полных частных  $\alpha_0 = \alpha, \alpha_1, \dots$ , вычисляемую при помощи равенства (5.1), тогда

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}.$$

Следовательно, если  $\alpha_n$  есть корень некоторого многочлена  $f_n(x)$ , то  $\alpha_{n+1}$ , согласно второму утверждению доказанной нами леммы, является корнем многочлена  $f_{n+1}(x)$ , определяемого равенством (5.34).

Мы получили, что для вычисления последовательности неполных частных  $a_0, a_1, \dots$  нам необходимо находить корни многочленов, преобразуемых из многочлена  $f_0(x)$  в соответствии с формулами из первого утверждения доказанной леммы.

**Пример 5.3.** Приведем пример и разложим в непрерывную дробь величину  $\alpha = \sqrt[3]{5} \sim 1.709$ , являющуюся корнем многочлена  $f_0(x) = x^3 - 5$ . Поскольку многочлен  $f_0(x)$  имеет только один действительный корень, то, согласно второму утверждению доказанной леммы, все многочлены  $f_1(x), f_2(x), \dots$  также будут иметь один действительный корень.

Поскольку  $[\alpha] = 1$ , то определим  $a_0 = 1$  и вычислим многочлен  $f_1(x)$ , корнем которого является величина  $\alpha_1$

$$f_1(x) = \sum_{k=0}^3 \frac{f_0^{(k)}(1)}{k!} x^{3-k} = -4x^3 + 3x^2 + 3x + 1.$$

Приближенное значение действительного корня многочлена  $f_1(x)$  равно 1.408, следовательно, мы можем определить  $a_1 = 1$  и многочлен

$$f_2(x) = 3x^3 - 3x^2 - 9x - 4,$$

корень которого близок к величине 2.448. Аналогично, определим  $a_2 = 2$  и многочлен

$$f_3(x) = -10x^3 + 15x^2 + 15x + 3,$$

корень которого близок к величине 2.232. Определим  $a_3 = 2$  и запишем равенство

$$\alpha = [1, 1, 2, 2, \alpha_4],$$

где неизвестная величина  $\alpha_4$  является корнем следующего многочлена  $f_4(x) = 13x^3 - 45x^2 - 45x - 10$ . Мы остановили наши вычисления, поскольку, в силу теоремы 5.3, полученное нами разложение величины  $\alpha$  не периодически.

Покажем, что для квадратичных иррациональностей описанный способ разложения в непрерывную дробь аналогичен доказанным ранее соотношениям (5.20). Пусть  $\alpha_n$  бóльший корень многочлена второй степени  $f_n(x) = u_n x^2 + v_n x + w_n$ , тогда верны равенства

$$\alpha_n = \frac{-v_n + \sqrt{v_n^2 - 4u_n w_n}}{2u_n} = \frac{A_n + \sqrt{D}}{B_n},$$

откуда вытекает  $A_n = -v_n$ ,  $B_n = 2u_n$ .

Заметим, что при преобразовании (5.1) бóльший корень многочлена  $f_n(x)$  переходит в меньший корень многочлена  $f_{n+1}(x)$  и наоборот. Следовательно,  $\alpha_{n+1}$  есть меньший корень многочлена

$$f_{n+1}(x) = (u_n a_n^2 + v_n a_n + w_n) x^2 + (2u_n a_n + v_n) x + u_n,$$

имеющий вид

$$\alpha_{n+1} = \frac{-2u_n a_n - v_n - \sqrt{D}}{2(u_n a_n^2 + v_n a_n + w_n)}, \quad (5.37)$$

поскольку дискриминант многочлена  $f_{n+1}(x)$  удовлетворяет равенству

$$(2u_n a_n + v_n)^2 - 4u_n (u_n a_n^2 + v_n a_n + w_n) = v_n^2 - 4u_n w_n = D.$$

Подставляя в (5.37) величины  $A_n$ ,  $B_n$ , домножая числитель и знаменатель дроби на  $-1$ , а также замечая, что  $2w_n = 2u_{n-1} = -B_{n-1}$ , получим равенство

$$\alpha_{n+1} = \frac{A_n - a_n B_n - \sqrt{D}}{a_n(2a_n B_n - 2A_n) - B_{n-1}} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}}$$

в котором величины  $A_{n+1}$ ,  $B_{n+1}$  удовлетворяют соотношениям из утверждения леммы 5.6.

## 5.5 Эквивалентность действительных чисел

Напомним следующее определение.

**Определение 5.8.** Два действительных числа  $\alpha$  и  $\gamma$  называются эквивалентными, если найдутся такие целые числа  $a, b, c, d$ , что

$$\gamma = \frac{a\alpha + b}{c\alpha + d}, \quad ad - bc = \pm 1. \quad (5.38)$$

Для обозначения эквивалентности действительных чисел  $\alpha$  и  $\gamma$  мы будем использовать запись  $\alpha \sim \gamma$ .

Если в равенстве (5.38) величина  $s$  принимает отрицательные значения, то, домножая числитель и знаменатель на  $-1$ , мы получим равенство, в котором  $s \geq 0$ . В этом разделе мы покажем, что аппарат непрерывных дробей позволяет решать задачу об эквивалентности двух произвольных действительных чисел.

Вначале отметим, что введённое нами отношение эквивалентности разбивает всё множество действительных чисел на классы эквивалентности. Действительно, верна следующая лемма.

**Лемма 5.10.** *Выполнены следующие утверждения.*

1. Число  $\alpha$  эквивалентно самому себе.
2. Если  $\gamma \sim \alpha$ , то выполнено и обратное свойство  $\alpha \sim \gamma$ .
3. Выполнено свойство транзитивности, то есть если выполнено  $\gamma \sim \alpha$  и  $\vartheta \sim \gamma$ , то выполнено и  $\vartheta \sim \alpha$ .
4. Выполнены частные случаи  $\alpha \sim -\alpha$ ,  $\alpha \sim \frac{1}{\alpha}$  и  $\alpha \sim \alpha + q$  для любого целого числа  $q$ .

*Доказательство.* Первое утверждение леммы, очевидно, выполнено при  $a = d = 1$  и  $b = c = 0$ . Далее, выражая из (5.38) величину  $\alpha$ , получим

$$\alpha = \frac{-d\gamma + b}{c\gamma - a} \quad \text{и} \quad (-d)(-a) - bc = \pm 1,$$

следовательно,  $\alpha \sim \gamma$ .

Для доказательства третьего утверждения будем считать, что

$$\gamma = \frac{a\alpha + b}{c\alpha + d}, \quad \vartheta = \frac{p\gamma + q}{s\gamma + t}, \quad ad - bc = \pm 1, \quad pt - sq = \pm 1.$$

Подставляя первое равенство во второе, получим

$$\vartheta = \frac{p(a\alpha + b) + q(c\alpha + d)}{s(a\alpha + b) + t(c\alpha + d)} = \frac{(ap + cq)\alpha + (bp + dq)}{(as + ct)\alpha + (bs + dt)}.$$

Поскольку

$$(ap + cq)(bs + dt) - (bp + dq)(as + ct) = (pt - sq)(ad - bc) = \pm 1,$$

то выполнено  $\vartheta \sim \alpha$ . Более того, из второго утверждения леммы следует, что  $\alpha \sim \vartheta$ .

Последнее утверждение следует из равенств

$$\begin{aligned}
-\alpha &= \frac{-1 \cdot \alpha + 0}{0 \cdot \alpha + 1}, & -1 \cdot 1 - 0 \cdot 0 &= -1, \\
\frac{1}{\alpha} &= \frac{0 \cdot \alpha + 1}{1 \cdot \alpha + 0}, & 0 \cdot 0 - 1 \cdot 1 &= -1, \\
\alpha + q &= \frac{1 \cdot \alpha + q}{0 \cdot \alpha + 1}, & 1 \cdot 1 - q \cdot 0 &= 1.
\end{aligned}$$

Лемма доказана.  $\square$

Теперь мы можем доказать следующую теорему.

**Теорема 5.5.** *Два действительных числа  $\alpha$  и  $\gamma$  эквивалентны тогда и только тогда, когда их разложения в непрерывные дроби, начиная с некоторого места, совпадают.*

*Доказательство.* В начале рассмотрим случай, когда разложения двух действительных чисел в непрерывную дробь совпадают. Тогда найдутся такие целые индексы  $n$  и  $m$ , что

$$\alpha = [a_0, a_1, \dots, \alpha_n], \quad \gamma = [c_0, c_1, \dots, \gamma_m] \quad \text{и} \quad \alpha_n = \gamma_m.$$

Воспользовавшись равенством (5.7) запишем

$$\alpha = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}},$$

При этом, согласно лемме 5.3, выполнены равенства

$$P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1} = \pm 1.$$

Следовательно, числа  $\alpha$  и  $\alpha_n$  эквивалентны. Аналогичными рассуждениями мы получаем, что эквиваленты числа  $\gamma$  и  $\gamma_m$ . Тогда

$$\alpha \sim \alpha_n = \gamma_m \sim \gamma.$$

Докажем обратное утверждение теоремы. Пусть для чисел  $\gamma$  и  $\alpha$  выполнено равенство (5.38). Покажем, что найдется последовательность действительных чисел  $\gamma_0 = \gamma, \gamma_1, \dots, \gamma_m = \alpha$  таких, что для всех  $n = 0, 1, \dots, m-1$  выполнено условие  $\gamma_n \sim \gamma_{n+1}$  и, кроме того, разложения чисел  $\gamma_n$  и  $\gamma_{n+1}$  в непрерывную дробь, начиная с некоторого места, совпадают. При этом, мы будем считать, что оба числа не являются рациональными, поскольку в противном случае их разложения конечны.

Начнем доказательство с рассмотрения простейших случаев эквивалентности, рассмотренных при доказательстве леммы 5.10.

1. Рассмотрим случай  $\gamma \sim \alpha + q$ . Разложим  $\alpha$  в непрерывную дробь  $\alpha = a_0 + \frac{1}{\alpha_1}$ , где  $\alpha_1 > 1$ . Следовательно,

$$\gamma = \alpha + q = a_0 + q + \frac{1}{\alpha_1} = [a_0 + q, \alpha_1].$$

Таким образом, разложения чисел  $\alpha$  и  $\gamma$  совпадают.

2. Рассмотрим случай  $\gamma \sim -\alpha$ . Пусть, как и ранее,  $\alpha = a_0 + \frac{1}{\alpha_1}$  и  $\alpha_1 > 1$ . В начале предположим, что  $\alpha_1 > 2$ . Тогда

$$\gamma = -a_0 - \frac{1}{\alpha_1} = -a_0 - 1 + \frac{1}{1 + \frac{1}{\alpha_1 - 1}} = [-a_0 - 1, 1, \alpha_1 - 1], \quad (5.39)$$

где величина  $\alpha_1 - 1 > 1$ . Согласно первому свойству, разложения чисел  $\alpha_1$  и  $\alpha_1 - 1$  совпадают, следовательно, совпадают разложения чисел  $\alpha$  и  $\gamma$ .

Обозначим  $\varrho = \frac{1}{\alpha_1 - 1}$  и будем считать, что  $1 < \alpha_1 < 2$ , тогда верно неравенство  $\varrho > 1$ . Более того, из (5.39) и равенства

$$\alpha = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{1 + \frac{1}{\varrho}} = [a_0, 1, \varrho]$$

можно сделать вывод, что разложения чисел  $\alpha$  и  $\gamma = [-a_0 - 1, 1 + \varrho]$  совпадают при  $1 < \alpha_1 < 2$ .

3. Рассмотрим случай  $\gamma \sim \frac{1}{\alpha}$ . Доказанное нами второе свойство позволяет рассматривать только случай  $\alpha > 0$ . Тогда, если  $\alpha > 1$ , то выполнено равенство  $\gamma = [0, \alpha]$  и разложения чисел  $\gamma$  и  $\alpha$  совпадают.

В случае  $1 > \alpha > 0$  мы получаем, что  $\alpha = \frac{1}{\gamma}$  и  $\gamma > 1$ , следовательно,  $\alpha = [0, \gamma]$  и разложения двух чисел опять совпадают.

Теперь рассмотрим общий случай. Пусть  $\gamma = \frac{a_0\alpha + b_0}{c_0\alpha + d_0}$  и выполнено равенство  $a_0d_0 - b_0c_0 = \pm 1$ . Определим  $\gamma_0 = \gamma$  и рассмотрим преобразование

$$\gamma_{n+1} = \frac{1}{\gamma_n - q_n}, \quad n = 0, 1, \dots$$

для некоторого целого числа  $q_n$ . Из рассмотренных нами частных случаев, а также четвертого утверждения леммы 5.10, следует, что  $\gamma_{n+1} \sim \gamma_n$

и их разложения в непрерывную дробь, начиная с некоторого места, совпадают.

Мы будем выбирать последовательность величин  $q_0, q_1, \dots$  следующим образом. Без ограничения общности мы можем считать, что  $c_n > 0$ , тогда определим величину  $q_n$  равенством

$$a_n = q_n c_n + r_n, \quad 0 \leq r_n < c_n.$$

Тогда

$$\gamma_{n+1} = \frac{1}{\gamma_n - q_n} = \frac{c_n \alpha + d_n}{(a_n - q_n c_n) \alpha + (b_n - q_n d_n)} = \frac{a_{n+1} \alpha + b_{n+1}}{c_{n+1} \alpha + d_{n+1}},$$

где

$$a_{n+1} = c_n, \quad b_{n+1} = d_n, \quad c_{n+1} = r_n, \quad d_{n+1} = b_n - q_n d_n$$

и выполнено условие

$$a_{n+1} d_{n+1} - c_{n+1} d_{n+1} = c_n (b_n - q_n d_n) - d_n (a_n - q_n c_n) = \pm 1. \quad (5.40)$$

Мы получили, что каждый элемент последовательности  $\gamma_0, \gamma_1, \dots$  выражается через число  $\alpha$  и при этом последовательность неотрицательных величин  $c_n$  убывает, так как  $c_{n+1} = r_n < c_n$ . Следовательно, найдется индекс  $m$  такой, что  $c_m = 0$ , тогда

$$\gamma_m = \frac{a_m \alpha + b_m}{0 \cdot \alpha + d_m}.$$

Учитывая равенство (5.40) мы получаем, что верно равенство  $a_m d_m = \pm 1$ , тогда  $\gamma_m = \pm(\alpha + b_m)$  для некоторого целого числа  $b_m$ . Из доказанных выше первого и второго частных случаев следует, что  $\gamma_m$  и  $\alpha$  эквивалентны и их разложения в непрерывную дробь, начиная с некоторого места, совпадают. Теорема доказана.  $\square$

Из доказательства теоремы явным образом следует метод проверки эквивалентности двух заданных действительных чисел. Приведем пример.

**Пример 5.4.** Покажем, что большие корни многочленов

$$f(x) = x^2 - 3x - 2 \quad \text{и} \quad h(x) = 2x^2 - 15x + 26$$

эквивалентны. Поскольку мы исследуем квадратичные иррациональности, то их разложения в непрерывную дробь периодичны. Это позволит нам вычислить все элементы последовательности полных частных для каждого из чисел, а потом сравнить найденные значения.

В начале найдем разложение  $\alpha = \frac{3+\sqrt{17}}{2}$  — большего корня многочлена  $f(x)$ , и сведем полученные результаты в следующую таблицу.

$n$	$\alpha_n$	$a_n$	$P_n$	$Q_n$
0	$\alpha_0 = \frac{3+\sqrt{17}}{2}$	3	$P_0 = 3$	$Q_0 = 1$
1	$\alpha_1 = \frac{3+\sqrt{17}}{4}$	1	$P_1 = 4$	$Q_0 = 1$
2	$\alpha_2 = \frac{1+\sqrt{17}}{4}$	1	$P_2 = 7$	$Q_0 = 2$
3	$\alpha_3 = \alpha_0$			

Отметим, что вместе с разложением в непрерывную дробь мы вычислили числители и знаменатели подходящих дробей. Эти величины будут использованы нами для определения соотношения между раскладываемыми числами.

Теперь разложим в непрерывную дробь  $\gamma = \frac{15+\sqrt{17}}{4}$  – бóльший корень многочлена  $h(x)$ . Легко видеть, что  $\lfloor \gamma \rfloor = 4$  и

$$\gamma_1 = \frac{1}{\gamma - 4} = \frac{1 + \sqrt{17}}{4} = \alpha_2.$$

Тогда, используя равенство (5.7) при  $n = 1$ , запишем равенство

$$\alpha = \frac{4\alpha_2 + 3}{\alpha_2 + 1} = \frac{4\left(\frac{1}{\gamma-4}\right) + 3}{\left(\frac{1}{\gamma-4}\right) + 1} = \frac{3\gamma - 8}{\gamma - 3}.$$

Поскольку верно равенство  $3 \cdot (-3) - (-8) \cdot 1 = -1$ , то мы доказали, что числа  $\alpha$  и  $\gamma$  эквивалентны, а также в явном виде предъявили соотношение, позволяющее выразить одно число через другое.

## 5.6 Наилучшие приближения

Мы завершим эту главу результатами, иллюстрирующими связь между непрерывными дробями и, так называемыми, наилучшими приближениями.

Рассмотрим задачу приближения действительного числа  $\alpha$  рациональной дробью  $\frac{P}{Q}$ . В теории вычислительных методов, традиционно, наибольший интерес представляет собой величина  $\varepsilon$ , представляющая собой оценку погрешности приближения, то есть  $\varepsilon > \left| \alpha - \frac{P}{Q} \right|$ . Если  $\alpha$  не является рациональным числом, то из теоремы 5.1 следует, что для любого значения  $\varepsilon$  найдется бесконечно много подходящих дробей, удовлетворяющих указанному неравенству. Однако, как следует из леммы



5.5, знаменатели этих дробей быстро растут и принимают сколь угодно большие значения.

Если же мы ограничим сверху величину знаменателя некоторой константой, зависящей от  $\varepsilon$ , то приближений к числу  $\alpha$  окажется конечное число, среди которых можно будет выделить одно, в некотором смысле, *наилучшее*. Дадим строгое определение.

**Определение 5.9.** Пусть  $\alpha$  действительное, отличное от нуля число. Рациональная дробь  $\frac{P}{Q}$  называется *наилучшим приближением к числу  $\alpha$* , если любой другой дроби  $\frac{A}{B} \neq \frac{P}{Q}$  такой, что  $1 \leq B \leq Q$ , выполнено неравенство

$$|B\alpha - A| > |Q\alpha - P|.$$

Наилучшее приближение есть несократимая дробь. Предположив обратное, получим  $P = uA$ ,  $Q = uB$  при  $u > 1$ , откуда вытекает неравенство  $|Q\alpha - P| = u|B\alpha - A| > |B\alpha - A|$ , противоречащее определению наилучшего приближения.

**Теорема 5.6.** Всякое наилучшее приближение к действительному числу  $\alpha$  есть подходящая дробь к нему. И наоборот, каждая подходящая дробь  $\frac{P_n}{Q_n}$  к числу  $\alpha$  при  $n \geq 1$  есть наилучшее приближение.

Прежде чем переходить к доказательству, заметим, что данное нами определение 5.9 эквивалентно тому, что система неравенств

$$\begin{cases} |x - \alpha y| \leq |P - \alpha Q|, \\ 0 < y \leq Q, \end{cases} \quad (5.41)$$

имеет единственное решение в целых числах  $x = P$ ,  $y = Q$ . Нам понадобится следующая лемма.

**Лемма 5.11.** Пусть  $\frac{P_n}{Q_n}$ ,  $\frac{P_{n+1}}{Q_{n+1}}$  две соседние подходящие дроби к числу  $\alpha$ , причем  $\frac{P_{n+1}}{Q_{n+1}} \neq \alpha$ . Тогда система неравенств

$$\begin{cases} |x - \alpha y| \leq |P_n - \alpha Q_n|, \\ 0 < y \leq Q_{n+1}, \end{cases} \quad (5.42)$$

имеет лишь два решения в целых числах, а именно  $x = P_n$ ,  $y = Q_n$  и  $x = P_{n+1}$ ,  $y = Q_{n+1}$ .

*Доказательство.* Пусть  $x, y$  целые числа, решения системы неравенств (5.42). Представим их в виде

$$\begin{aligned} x &= uP_n + vP_{n+1}, \\ y &= uQ_n + vQ_{n+1}, \end{aligned}$$

где  $u, v$  неизвестные значения. Выражая в явном виде неизвестные  $u, v$  и воспользовавшись равенством (5.8), получим

$$u = (-1)^n(yP_{n+1} - xQ_{n+1}), \quad v = (-1)^n(xQ_n - yP_n).$$

Следовательно, неизвестные  $u, v$  могут принимать только целые значения, поскольку  $P_n, Q_n, P_{n+1}, Q_{n+1}, x, y \in \mathbb{Z}$ .

Наборы  $u = 0, v = 1$  и  $u = 1, v = 0$  дают нам два решения неравенства (5.42), указанные в формулировке леммы. Покажем, что других решений не существует.

Предположим, что  $u$  и  $v$  имеют одинаковые знаки. Тогда из условия  $y > 0$  следует, что  $uQ_n + vQ_{n+1} > 0$  и  $u > 0, v > 0$ . Но тогда  $y \geq Q_n + Q_{n+1}$ , что противоречит второму неравенству в (5.42). Таким образом, нам осталось рассмотреть случай, когда  $u$  и  $v$  имеют разные знаки.

Из неравенств (5.10) и утверждения теоремы 5.1 получаем, что числа  $P_n - \alpha Q_n$  и  $P_{n+1} - \alpha Q_{n+1}$  тоже имеют разные знаки, поэтому выполнено неравенство

$$\begin{aligned} |x - \alpha y| &= |u(P_n - \alpha Q_n) + v(P_{n+1} - \alpha Q_{n+1})| = \\ &= |u||P_n - \alpha Q_n| + |v||P_{n+1} - \alpha Q_{n+1}| > |P_n - \alpha Q_n|, \end{aligned}$$

которое противоречит (5.42). Лемма доказана.  $\square$

*Перейдем к доказательству теоремы 5.6.* Пусть дробь  $\frac{P}{Q}$  является наилучшим приближением к числу  $\alpha$  и  $n$  максимальный индекс такой, что  $Q_n \leq Q$ . Предположим, что

$$|P - \alpha Q| < |P_n - \alpha Q_n|, \quad (5.43)$$

тогда, согласно утверждению леммы 5.11, дробь  $\frac{P}{Q}$  совпадает с одной из подходящих дробей  $\frac{P_n}{Q_n}$  или  $\frac{P_{n+1}}{Q_{n+1}}$ . Если (5.43) не выполнено, то  $|P - \alpha Q| \geq |P_n - \alpha Q_n|$  и, в силу того, что  $\frac{P}{Q}$  – наилучшее приближение, выполнено  $P = P_n, Q = Q_n$ . В обоих случаях первое утверждение теоремы выполнено.

Теперь докажем обратное утверждение и покажем, что для всех индексов  $n \geq 0$  каждая подходящая дробь  $\frac{P_{n+1}}{Q_{n+1}}$  является наилучшим приближением. Рассмотрим значения  $x, y$ , являющиеся решением системы сравнений

$$\begin{cases} |x - \alpha y| \leq |P_{n+1} - \alpha Q_{n+1}|, \\ 0 < y \leq Q_{n+1}. \end{cases} \quad (5.44)$$

Из неравенств (5.10) и утверждения теоремы 5.1 получаем, что выполнено  $|P_n - \alpha Q_n| > |P_{n+1} - \alpha Q_{n+1}|$ . Тогда из (5.44) следуют неравенства

$$\begin{cases} |x - \alpha y| \leq |P_n - \alpha Q_n|, \\ 0 < y \leq Q_{n+1}, \end{cases}$$

которым, согласно лемме 5.11, удовлетворяет не более двух решений, а именно пары  $P_n, Q_n$  и  $P_{n+1}$  и  $Q_{n+1}$ . Поскольку  $P_n, Q_n$  не удовлетворяет (5.44), то  $\frac{P_{n+1}}{Q_{n+1}}$  наилучшее приближение. Теорема доказана.  $\square$

Докажем еще одну теорему, которая будет использована нами позднее при обосновании алгоритмов факторизации целых чисел.

**Теорема 5.7.** *Если несократимая дробь  $\frac{P}{Q}$ , при  $Q > 0$ , удовлетворяет неравенству*

$$\left| \alpha - \frac{P}{Q} \right| < \frac{1}{2Q^2}, \quad (5.45)$$

*то она есть наилучшее приближение к  $\alpha$ .*

*Доказательство.* Предположим, что целые числа  $x = A$ ,  $y = B$  удовлетворяют неравенствам (5.41), то есть

$$\begin{cases} |A - \alpha B| \leq |P - \alpha Q|, \\ 0 < B \leq Q. \end{cases}$$

Тогда рассмотрим разность целых чисел  $AQ - BP$  и получим неравенство

$$\begin{aligned} |AQ - BP| &= |Q(A - \alpha B) - B(P - \alpha Q)| \leq \\ &\leq Q|A - \alpha B| + B|P - \alpha Q| \leq 2Q|P - \alpha Q| < 2Q^2 \left| \alpha - \frac{P}{Q} \right| < 1, \end{aligned}$$

из которого следует, что разность  $AQ - BP$  равна нулю или, что равносильно,  $AQ = BP$ . Поскольку дробь  $\frac{P}{Q}$  несократима, то числа  $P$  и  $Q$  взаимно просты и мы получаем, что  $Q|B$ . Поскольку  $B < Q$ , то получаем, что  $B = Q$ , откуда вытекает равенство  $A = P$ . Следовательно, система неравенств (5.41) имеет только одно решение. Теорема доказана.  $\square$

Заметим, что из утверждения теорем 5.6 и 5.7 следует, что всякая несократимая дробь  $\frac{P}{Q}$ , удовлетворяющая неравенству (5.45), является подходящей дробью к числу  $\alpha$ .

## ПРОСТЫЕ ЧИСЛА

Построение таблицы простых чисел - Вероятностные алгоритмы проверки на простоту - Тест Соловея-Штрассена - Тест Миллера-Рабина - Теорема Поклингтона и ее дополнения - Алгоритмы построения простых чисел - Числа Мерсенна и доказательство теоремы о бесконечности множества простых - Рекуррентные последовательности Люка - Теорема Моррисона - Рекурсивный алгоритм построения простого числа с известным разложением  $p - 1$  - Алгоритм построения сильно простого числа.

В криптографических приложениях простые числа играют основополагающую роль, являясь долговременными параметрами криптографических схем и подвергаясь атакам нарушителей. Время действия открытых параметров ограничено, что вынуждает разработчиков криптографических схем достаточно часто вырабатывать новые, не использовавшиеся ранее простые числа.

При выработке простых чисел, на них, как правило, накладываются дополнительные условия. Приведем пример: согласно первой редакции стандарта Российской Федерации на электронную цифровую подпись ГОСТ Р 34.10, необходимо построить два простых числа  $p, q$ , удовлетворяющих условиям

$$2^{1021} < p < 2^{1024}, \quad q^{254} < q < 2^{256}, \quad p \equiv 1 \pmod{q}.$$

Следующая редакция стандарта накладывает несколько другие условия на простые числа  $p, q$ :

$$2^{255} < p < 2^{256}, \quad 2^{254} < q < 2^{256}, \quad q \equiv 1 + \tau \pmod{p}, \quad p^t \not\equiv 1 \pmod{q},$$

для некоторых целых  $\tau$  и  $t$ , удовлетворяющих неравенствам  $|\tau| \leq 2\sqrt{p}$  и  $0 < t \leq 31$ .

При генерации простых чисел, как правило, возникает два вопроса.

1. Как построить простое число с заданными ограничениями на размер числа?
2. Как определить, является ли заданное целое число  $m$  простым или составным?

Данные вопросы тесно связаны между собой: как только у нас появляется критерий проверки простоты, мы сразу можем предложить алгоритм построения простого числа, основанный на данном критерии.

Кроме того, задача проверки простоты числа связана с задачей разложения на множители. Наиболее простой способ проверить, является ли число  $m$  составным или нет, это проверить утверждение леммы 1.6, то есть выяснить, существует ли у числа  $m$  простой делитель, не превосходящий величины  $\sqrt{m}$ . Если такого делителя нет, то число  $m$  является простым. Для перебора всех возможных делителей нам потребуется сделать около  $\sqrt{m}$  операций пробного деления числа  $m$ . При больших значениях числа  $m$  эта процедура становится не реализуемой на практике. Вместе с тем, пробное деление часто используется для проверки: есть ли у числа маленькие делители.

Приведем алгоритм построения таблицы всех простых чисел, ограниченных сверху некоторой величиной  $b$ . Подобные таблицы будут нами использованы как для реализации метода пробного деления, так и в некоторых алгоритмах разложения целых чисел на множители.

### Алгоритм 6.1 (Алгоритм построения таблицы простых чисел)

**Вход:** Целое число  $b > 0$ .

**Выход:** Таблица простых чисел  $p_0, \dots, p_n$  таких, что  $p_n < b$  и  $n$  размер таблицы простых чисел.

1. Присвоить начальным элементам массива значения

$$p_0 = 2, \quad p_1 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \quad p_6 = 13, \quad p_7 = 17.$$

2. Определить переменные  $n = 8, h = 5, s = 25$ .
3. Определить  $p_n = p_n + 2$  и  $k = 1$ .
4. **Если**  $p_n > b$ , **то** завершить алгоритм и вернуть значение  $n$ .
5. **Если**  $p_n > s$ , **то** определить  $s = s + h, h = h + 1, s = s + h$ .
6. **Пока**  $p_k \leq h$  **выполнить**

6.1. **Если**  $p_n \equiv 0 \pmod{p_k}$ , **то** вернуться на шаг 3.

**Иначе** вычислить  $k = k + 1$ .

7. Определить  $n = n + 1$  и вернуться на шаг 3.

□

Приведенный алгоритм перебирает нечетные числа и реализует для них циклическую проверку утверждения леммы 1.6. Для каждого числа  $p_n$  проверяется его делимость на маленькие, построенные ранее простые числа, не превосходящие величины  $\sqrt{p_n}$ . Поскольку вычисление квадратного корня из целого числа является достаточно медленной процедурой то, для ее оптимизации на 5-м шаге алгоритма мы выполняем итерационное вычисление значений  $s, h$  таких, что  $p_n < s = h^2$ .

Трудоёмкость алгоритма построения таблицы простых чисел может быть оценена сверху величиной  $\frac{b\sqrt{b}}{2}$  операций деления на простые числа,

не превосходящие величины  $\sqrt{b}$ . При этом, объем используемой в алгоритме памяти минимален и равен  $\pi(b)$  – количеству простых чисел, не превосходящих величины  $b$ , см. приложение В.

Методы построения таблиц простых чисел, имеющие меньшую трудоемкость, но использующие объем памяти сравнимый с величиной  $b$ , называются методами решета. Наиболее известным является решето Эратосфена.

Рассмотрим массив  $m$  всех целых чисел от единицы до  $b$ , то есть  $m[i] = i$  для всех  $i = 2, \dots, b$  и  $m[1] = 0$ . В начале, обнулим в данном массиве все числа, делящиеся на двойку, то есть  $m[2i] = 0$  для всех  $i = 1, \dots, \lfloor \frac{b}{2} \rfloor$ . Потом найдем в массиве минимальное число  $d$ , большее двойки и отличное от нуля, то есть  $d = 3$ . Обнулим все числа, делящиеся на тройку, то есть  $m[3i] = 0$  для всех  $i = 1, \dots, \lfloor \frac{b}{3} \rfloor$ .

Продолжим эту процедуру для всех чисел  $d \leq \sqrt{b}$ , обнуляя числа, кратные  $d$ , то есть  $m[di] = 0$ , тогда, согласно лемме 1.6, оставшиеся в массиве  $m$  отличные от нуля числа будут простыми.

Еще один вариант решета был предложен в 1934 году индийцем Сундарамой. Он основывается на следующей простой идее. Все четные числа, большие двойки и меньшие  $b$ , очевидно, не являются простыми. Нечетные числа имеют вид  $2k + 1$  для некоторого целого  $k$ , где  $k \leq \lfloor \frac{b-1}{2} \rfloor$ . Если нечетное число является составным, то оно имеет как минимум два нечетных делителя, то есть

$$2k + 1 = (2i + 1)(2j + 1) \quad \text{или} \quad k = 2ij + i + j.$$

Пусть  $2i + 1$  наименьший делитель числа  $2k + 1$ , тогда, согласно лемме 1.6, выполнено неравенство  $2i + 1 \leq \lfloor \sqrt{b} \rfloor$ , которое дает оценку сверху для возможных значений  $i$ , то есть  $1 \leq i \leq \lfloor \frac{\sqrt{b}-1}{2} \rfloor$ . Для величины  $j$ , с учетом оценки сверху для величины  $k$ , получаем  $i \leq j \leq \lfloor \frac{b-3}{6} \rfloor$ .

Алгоритм решета выглядит следующим образом. Как и ранее, рассмотрим массив  $m$  всех целых чисел от единицы до  $b$ , то есть  $m[i] = i$  для всех  $i = 2, \dots, b$  и  $m[1] = 0$ . Перебирая индексы  $i$  и  $j$  в указанных пределах, определим  $m[(2i + 1)(2j + 1)] = 0$ . Тогда оставшиеся в массиве отличные от нуля числа будут простыми.

## 6.1 Вероятностные тесты проверки простоты

Процедуры строгого доказательства простоты заданного нечетного числа  $m$  являются достаточно трудоемкими и могут требовать больших

вычислительных ресурсов. Гораздо эффективнее могут быть реализованы процедуры, которые проверяют, не является ли число  $m$  составным с некоторой вероятностью – так называемые «вероятностные тесты».

Тесты позволяют очень эффективно отбраковать составные числа, однако они не в состоянии строго доказать простоту числа, они лишь позволяют говорить, что число  $m$  не является составным с некоторой вероятностью.

Первая и наиболее очевидная идея построения подобного теста заключается в обращении малой теоремы Ферма, см. теорему 2.7. Действительно, если найдется целое, взаимно простое с  $m$  число  $a$  такое, что  $a^{m-1} \not\equiv 1 \pmod{m}$ , то из утверждения малой теоремы Ферма следует, что число  $m$  составное.

С другой стороны, если выполнено сравнение  $a^{m-1} \equiv 1 \pmod{m}$ , можно ли считать число  $m$  простым? Рассмотрим в качестве примера  $m = 2701$  и вычислим

$$2^{2700} \equiv 1 \pmod{2701}, \quad 3^{2700} \equiv 1 \pmod{2701}.$$

Однако, как легко заметить, выполнено равенство  $2701 = 37 \cdot 73$  и число 2701 является составным. Действительно, выбирая в качестве  $a = 5$ , получим

$$5^{2700} \equiv 2554 \not\equiv 1 \pmod{2701}.$$

Как мы видим, для составных чисел существуют как основания  $a$  для которых утверждение малой теоремы Ферма выполнено, так и те основания, для которых утверждение неверно. Этот факт позволяет предложить следующий тест проверки заданного числа  $m$  на простоту.

1. Выбрать случайным образом вычет  $a$ . Если выполнено условие  $\text{НОД}(a, m) > 1$ , то число  $m$  составное.
2. Если сравнение  $a^{m-1} \equiv 1 \pmod{m}$  не выполнено, то число  $m$  составное. В противном случае, вернуться к первому шагу.

Если число  $m$  простое, то, в силу малой теоремы Ферма, приведенный тест никогда не завершится. Поэтому на практике, для предотвращения заикливания, мы должны ограничить число возвращений некоторой величиной  $k$  и после выбора  $k$  случайных значений вычета  $a$  считать, что число  $m$  простое.

Если число  $m$  составное, то мы могли бы предположить, что, при достаточно большом значении величины  $k$ , найдется вычет, для которого условия малой теоремы Ферма будут не выполнены. Однако это предположение выполнено не для всех составных чисел.

В 1885 году немецкий математик Альвин Корсельт (Alwin Reinhold Korselt) показал, что существуют составные числа  $m$ , для которых малая теорема Ферма выполнена для всех вычетов  $a$ , взаимно простых с  $m$ .

**Теорема 6.1** (Критерий Корсельта). *Пусть  $m$  нечетное натуральное число. Сравнение*

$$a^{m-1} \equiv 1 \pmod{m} \quad (6.1)$$

*выполнено для всех вычетов  $a$ , взаимно-простых с  $m$ , тогда и только тогда, когда полнены следующие условия.*

1. Число  $m$  свободно от квадратов, то есть для любого простого делителя  $p$  числа  $m$  выполнено  $p^2 \nmid m$ .
2. Если  $m$  представимо в виде  $m = p_1 \cdots p_k$ , то для всех  $i = 1, \dots, k$  выполнено условие  $p_i - 1 \mid m - 1$ .

*Доказательство.* В начале предположим, что для числа  $m$  выполнены условия теоремы, и рассмотрим произвольный вычет  $a$  такой, что  $\text{НОД}(a, m) = 1$ . Для любого индекса  $i = 1, \dots, k$  выполнено сравнение

$$a^{m-1} \equiv \left( a^{(p_i-1)} \right)^{\frac{(m-1)}{(p_i-1)}} \equiv 1 \pmod{p_i},$$

следовательно, воспользовавшись китайской теоремой об остатках, см. следствие 2 на стр. 21, получаем необходимое нам сравнение (6.1)

$$a^{m-1} \equiv 1 \pmod{p_1 \cdots p_k = m}.$$

Теперь докажем утверждение теоремы в обратную сторону. Рассмотрим натуральное число  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  и предположим, что для него выполнено условие (6.1).

Согласно теореме 2.8, для любого индекса  $i = 1, \dots, k$  найдется вычет  $a_i$ , являющийся первообразным корнем по модулю  $p_i$ , а величина  $p_i - 1$  является наименьшей степенью  $x$ , для которой  $a_i^x \equiv 1 \pmod{p_i}$ . Поскольку  $m$  удовлетворяет условию теоремы, то для  $a_i$  выполнено сравнение  $a_i^{m-1} \equiv 1 \pmod{m} \equiv 1 \pmod{p_i}$ , из которого следует условие  $p_i - 1 \mid m - 1$  и, в силу произвольности индекса  $i$ , второе утверждение теоремы.

Для доказательства первого утверждения рассмотрим  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  и предположим, что найдется индекс  $i$  такой, что  $\alpha_i > 1$ . Согласно теореме 2.11 найдется вычет  $b_i$ , являющийся первообразным корнем по модулю  $p_i^{\alpha_i}$ . Тогда, используя рассуждения аналогичные приведенным выше,



получаем, что показатель числа  $b_i$  делит величину  $m - 1$ , то есть

$$\text{ord}_{p_i^{\alpha_i}} b_i = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i - 1) | m - 1.$$

Мы получаем, что простое число  $p_i$  делит как величину  $m$ , в силу определения, так и величину  $m - 1$ , по только что доказанному свойству. Такого, однако, быть не может, поскольку  $p_i > 2$ . Следовательно, наше предположение неверно. Теорема доказана.  $\square$

**Следствие 1.** Пусть нечетное целое число  $m = p_1 \cdots p_k$  удовлетворяет критерию Корселя, тогда  $k \geq 3$ .

*Доказательство.* Предположим обратное, тогда найдется удовлетворяющее критерию Корселя составное число  $m = pq$ , где  $p, q$  различные простые числа. Без ограничения общности будем считать, что  $p < q$ .

Запишем равенство  $m - 1 = pq - 1 = p(q - 1) + p - 1$ , из которого следует сравнение  $m - 1 \equiv p - 1 \pmod{q - 1}$ . Поскольку  $p$  нечетное простое, то  $p > 2$  и величина  $p - 1$  не сравнима с нулем по модулю  $q - 1$ . Следовательно,  $q - 1$  не делит величину  $m - 1$ , и мы получаем противоречие второму утверждению теоремы 6.1.  $\square$

К огромному сожалению, Корсельт не предъявил в явном виде ни одного числа, удовлетворяющего критерию. Впервые это сделал Роберт Кармайкл (Robert D. Carmichael). В период с 1910 года по 1912 год он нашел все числа, см. [19], не превосходящие 10000

$$\begin{aligned} 561 &= 3 \cdot 11 \cdot 17, \\ 1105 &= 5 \cdot 13 \cdot 17, \\ 1729 &= 7 \cdot 13 \cdot 19, \\ 2465 &= 5 \cdot 17 \cdot 29, \\ 2821 &= 7 \cdot 13 \cdot 31, \\ 6601 &= 7 \cdot 23 \cdot 41, \\ 8911 &= 7 \cdot 19 \cdot 67. \end{aligned}$$

В настоящее время числа, удовлетворяющие критерию Корселя, принято называть числами Кармайкла. Мы можем также привести числа Кармайкла, имеющие четыре или пять простых делителей

$$\begin{aligned} 41041 &= 7 \cdot 11 \cdot 13 \cdot 47, \\ 825265 &= 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73. \end{aligned}$$

Известно, что чисел Кармайкла бесконечно много, см. [15, 27], но встречаются они достаточно редко. Несмотря на это, описанный нами

ранее вероятностный тест на основе малой теоремы Ферма, не позволяет различать между собой простые числа и числа Кармайкла. Этот факт привел к появлению других тестов.

### 6.1.1 Тест Соловея-Штрассена

В 1977 году работе [51] Соловеем (Robert M. Solovay) и Штрассеном (Völker Strassen) был опубликован тест, основанный на свойствах символов Лежандра и Якоби. Докажем следующий результат, лежащий в основе теста.

**Теорема 6.2.** *Пусть  $m$  нечетное составное целое число. Тогда среди всех целых чисел  $a$  таких, что  $0 < a < m$ , не более половины будут удовлетворять следующим условиям.*

1.  $\text{НОД}(a, m) = 1$ .
2. Выполнено сравнение  $a^{\frac{m-1}{2}} \equiv \left(\frac{a}{m}\right) \pmod{m}$ , где символ  $\left(\frac{a}{m}\right)$  означает символ Якоби.

*Доказательство.* Вначале мы покажем, что найдется вычет  $a$  – целое, взаимно простое с  $m$  число,  $0 < a < m$  такое, что второе условие теоремы будет не выполнено, то есть  $a^{\frac{m-1}{2}} \not\equiv \left(\frac{a}{m}\right) \pmod{m}$ .

Пусть  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  разложение составного числа  $m$  на простые, нечетные сомножители. Для начала рассмотрим случай, когда найдется такой индекс  $i$ ,  $1 \leq i \leq k$  такой, что  $\alpha_i > 1$ . Без ограничения общности будем считать, что  $i = 1$ .

Определим целое число  $a$  равенством

$$a = 1 + \frac{m}{p_1}, \quad (6.2)$$

тогда  $a \equiv 1 \pmod{p_i}$  для всех индексов  $1 \leq i \leq k$ . Это позволяет нам записать равенство

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k} = 1.$$

Предположим, что для числа  $a$  выполнено сравнение  $a^{\frac{m-1}{2}} \equiv 1 \pmod{m}$ . Тогда, поскольку  $p_1^{\alpha_1} | m$ , получаем, что  $a^{\frac{m-1}{2}} \equiv 1 \pmod{p_1^{\alpha_1}}$ .

Обозначим символом  $d$  показатель числа  $a$  по модулю  $p_1^{\alpha_1}$ , то есть  $d$  минимальное целое такое, что  $a^d \equiv 1 \pmod{p_1^{\alpha_1}}$ . Используя утверждение леммы 2.4, получаем, что  $d | \frac{m-1}{2}$  и, следовательно,  $d | m - 1$ .

В силу (6.2) мы можем записать сравнение  $a \equiv 1 + kp_1^{\alpha_1-1} \pmod{p_1^{\alpha_1}}$  для некоторого целого числа  $k$  такого, что  $\text{НОД}(k, p_1) = 1$ . Используя формулу бинома Ньютона, см. (2.17), мы можем записать сравнение

$$1 \equiv a^d \equiv (1 + kp_1^{\alpha_1-1})^d \equiv 1 + kdp_1^{\alpha_1-1} \pmod{p_1^{\alpha_1}},$$

из которого следует, что  $kdp_1^{\alpha_1-1} \equiv 0 \pmod{p_1^{\alpha_1}}$  или, что равносильно,  $p_1 | kd$ . В силу взаимной простоты  $k$  и  $p_1$  получаем, что  $p_1 | d | m - 1$ .

Вспоминая, что нечетное простое  $p_1$  является делителем числа  $m$  и не может одновременно делить  $m - 1$  получаем, что наше предположение неверно и число  $a$ , определенное равенством (6.2), не удовлетворяет второму условию теоремы.

Теперь рассмотрим случай, когда составное число  $m$  раскладывается в произведение нечетных простых делителей в первой степени, то есть  $m = p_1 \cdots p_k$ . Определим целое число  $a$  как решение системы сравнений

$$\begin{cases} x \equiv s \pmod{p_1}, \\ x \equiv 1 \pmod{p_2}, \\ \quad \quad \quad \dots \\ x \equiv 1 \pmod{p_k}, \end{cases} \quad (6.3)$$

где  $s$  произвольный квадратичный невычет по модулю  $p_1$ . В силу определения, для числа  $a$  выполнено равенство

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right) = \left(\frac{s}{p_1}\right) = -1.$$

С другой стороны,  $a^{\frac{m-1}{2}} \equiv 1 \pmod{p_i}$  для всех индексов  $i$ ,  $2 \leq i \leq k$ . Следовательно, воспользовавшись китайской теоремой об остатках, см. теорему 2.3, получаем сравнение  $a^{\frac{m-1}{2}} \equiv 1 \pmod{p_2 \cdots p_k}$ .

Если же выполнено условие  $a^{\frac{m-1}{2}} \equiv \left(\frac{a}{m}\right) \equiv -1 \pmod{m}$ , то сразу получаем сравнение  $a^{\frac{m-1}{2}} \equiv -1 \pmod{p_2 \cdots p_k}$ , что противоречит выбору  $a$ . Таким образом, определенный системой сравнений (6.3) вычет  $a$  не удовлетворяет второму утверждению теоремы.

Покажем, что чисел, не удовлетворяющих условиям теоремы, достаточно много. Пусть  $w$  целое число, удовлетворяющее условиям теоремы. Рассмотрим вычет  $u \equiv aw \pmod{m}$ , где  $a$  вычет, построенный нами ранее, и предположим, что  $u$  также удовлетворяет условиям теоремы. Тогда выполнено сравнение

$$u^{\frac{m-1}{2}} \equiv \left(\frac{u}{m}\right) \pmod{m}.$$

С другой стороны, выполнены сравнения

$$u^{\frac{m-1}{2}} \equiv a^{\frac{m-1}{2}} w^{\frac{m-1}{2}},$$

$$\left(\frac{u}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{w}{m}\right) = \left(\frac{a}{m}\right) w^{\frac{m-1}{2}},$$

из которых следует, что вычет  $a$  удовлетворяет условиям теоремы. Это, в силу построения, неверно. Следовательно, мы получаем, что для каждого вычета  $w$ , удовлетворяющего условиям теоремы, найдется вычет  $u$ , который не удовлетворяет условиям теоремы. Таким образом, теорема доказана.  $\square$

Теперь вернемся к вопросу о простоте числа  $m$ . Если число  $m$  простое, то оба условия доказанной нами теоремы, в силу свойств символа Якоби, будут выполнены. В случае, если число  $m$  составное, то найдется такой вычет  $a$ , что одно из условий теоремы будет не выполнено. При этом мы доказали, что таких вычетов не менее, чем вычетов, для которых утверждение теоремы выполнено.

### Алгоритм 6.2 (Тест Соловея-Штрассена)

**Вход:** Целое число  $m$ .

**Выход:** Заключение о том, что число составное, либо заключение о том, что число не является составным с некоторой вероятностью.

1. Определить число итераций  $k = 20$ .
2. Вычислить случайное число  $a$ ,  $0 < a < m$ .
3. Если  $\text{НОД}(a, m) > 1$ , то закончить алгоритм с уведомлением, что число  $m$  составное.
4. Если  $a^{\frac{m-1}{2}} \not\equiv \left(\frac{a}{m}\right) \pmod{m}$ , то закончить алгоритм с уведомлением, что число  $m$  составное.
5. Вычислить  $k = k - 1$ .
6. Если  $k = 0$ , то закончить алгоритм с уведомлением, что число  $m$ , вероятно, простое.

Иначе вернуться на шаг 2.  $\square$

Заметим, что число итераций алгоритма  $k$  определяет вероятность принять составное число  $m$  за простое. Данная вероятность, очевидно, равняется  $\frac{1}{2^k}$ . Таким образом, если число  $m$  завершило тест с заключением, что оно, вероятно, простое, то оно является простым лишь с вероятностью  $1 - \frac{1}{2^k}$ .

При практической реализации алгоритма, для снижения его трудоемкости, выбирают числа  $a$  не из интервала  $0 < a < m$ , а из меньшего интервала  $0 < a < c$ , где константа  $c$  определяет максимально возможное значение натурального числа, помещающегося в одном регистре процессора.

### 6.1.2 Тест Миллера-Рабина

Следующий тест может быть реализован на ЭВМ более эффективно, чем тест Соловея-Штрассена. Детерминированная версия данного теста была предложена Гери Миллером (Gary L. Miller) в 1976 году [37]. Позднее, в 1980 году, Майкл Рабин (Michael O. Rabin) [46] предложил вероятностный алгоритм тестирования простоты и получил теоретическую оценку вероятности его успешного завершения.

Приведем результат Рабина, на котором основан тест проверки на простоту.

**Теорема 6.3** (Рабин, 1980). Пусть  $m$  нечетное составное число такое, что  $\text{НОД}(6, m) = 1$ . Определим целые числа  $n, q$  равенством  $m - 1 = 2^n q$  и будем говорить, что вычет  $a$  принадлежит множеству  $\mathcal{S} \subset \mathbb{Z}_m$ , если выполнено одно из двух условий.

1.  $a^q \equiv 1 \pmod{m}$ .
2.  $a^{2^k q} \equiv -1 \pmod{m}$  для некоторого целого индекса  $k$ ,  $0 \leq k < n$ .

Тогда мощность множества  $\mathcal{S}$  не превосходит  $\frac{m}{4}$ .

Заметим, что если число  $m$  является простым, то, согласно лемме 4.7, условия теоремы 6.3 выполнены для всех целых чисел  $a$  взаимно простых с  $m$ . Именно это различие между простыми и составными числами лежит в основе теста, предложенного Миллером и Рабином.

Мы проведем доказательство теоремы, следуя идеям статьи [4]. Начнем с доказательства вспомогательных результатов и определим множество  $\mathcal{A} \subset \mathbb{Z}_m$  вычетов  $a$ , удовлетворяющих одному из двух условий.

1.  $a^{m-1} \not\equiv 1 \pmod{m}$ .
2. Число  $a$  является первообразным корнем по модулю  $p$  – некоторого простого делителя числа  $m$  и выполнено условие  $a^z \not\equiv -1 \pmod{m}$  для любого целого  $z$ .

**Лемма 6.1.** Для любого элемента  $a \in \mathcal{A}$  и любого элемента  $s \in \mathcal{S}$  выполнено условие  $as \pmod{m} \notin \mathcal{S}$  или, на языке множеств, выполнено  $a\mathcal{S} \cap \mathcal{S} = \emptyset$ .

*Доказательство.* Вначале заметим, что поскольку выполнено равенство  $m - 1 = 2^n q$ , то для любого  $s \in \mathcal{S}$  выполнено  $s^{m-1} \equiv 1 \pmod{m}$ .

Теперь предположим, что  $a \in \mathcal{A}$  удовлетворяет первому условию, то есть  $a^{m-1} \not\equiv 1 \pmod{m}$ . Тогда, очевидно,

$$(as)^{m-1} \equiv a^{m-1}s^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m}$$

и вычет  $as$  не принадлежит множеству  $\mathcal{S}$ .

Второй случай, когда  $a^{m-1} \equiv 1 \pmod{m}$  и  $a^z \not\equiv -1 \pmod{m}$  для любого целого  $z$ , рассматривается несколько сложнее.

Предположим, что вычет  $as$  принадлежит множеству  $\mathcal{S}$  и рассмотрим четыре возможных варианта.

1.  $s^q \equiv 1 \pmod{m}$  и  $(as)^q \equiv 1 \pmod{m}$ .
2.  $s^q \equiv 1 \pmod{m}$  и  $(as)^{2^l q} \equiv -1 \pmod{m}$ ,  $0 \leq l < n$ .
3.  $s^{2^k q} \equiv -1 \pmod{m}$ ,  $0 \leq k < n$  и  $(as)^q \equiv 1 \pmod{m}$ .
4.  $s^{2^k q} \equiv -1 \pmod{m}$ ,  $0 \leq k < n$  и  $(as)^{2^l q} \equiv -1 \pmod{m}$ ,  $0 \leq l < n$ .

Для первого варианта сразу получаем, что  $a^q \equiv 1 \pmod{m}$ . Это не верно: в противном случае,  $a^q \equiv 1 \pmod{p}$ , поскольку  $p|m$  и  $p-1|q$ , поскольку  $a$  первообразный корень по модулю  $p$ . Последнее условие не выполнено в силу того, что  $p-1$  четно, а  $q$  нечетно.

Для второго варианта получаем  $-1 \equiv a^{2^l q}(s^q)^{2^l} \equiv a^{2^l q} \pmod{m}$ , что противоречит выбору  $a$ .

В третьем случае выразим из второго сравнения  $s^q \equiv a^{-q} \pmod{m}$ . Подставляя полученное выражение в первое сравнение, получим сравнение  $a^{-2^k q} \equiv -1 \pmod{m}$ , которое противоречит выбору  $a$ .

В последнем случае, если  $l > k$ , то, подставляя первое сравнение во второе, получим сравнение  $a^{2^k q} \equiv -1 \pmod{m}$ , которое противоречит выбору  $a$ . Если же  $l \leq k$ , выражая  $s^{2^l q} \equiv -a^{2^l q} \pmod{m}$  и подставляя это выражение в первое сравнение, получим сравнение

$$\left(-a^{2^l q}\right)^{2^{k-l}} \equiv -1 \pmod{m},$$

которое также противоречит выбору  $a$  при  $l < k$ . Оставшийся вариант, при  $k = l$ , приводит нас к сравнению  $a^{2^l q} \equiv 1 \pmod{m}$ . Тогда, поскольку  $p|m$ , получаем  $a^{2^l q} \equiv 1 \pmod{p}$ , а поскольку  $a$  первообразный корень по модулю  $p$ , то  $p-1|2^l q = 2^k q$ . Последнее равенство влечет за собой сравнение  $s^{p-1} \equiv s^{2^k q} \equiv 1 \pmod{p}$ , которое противоречит выбору  $s$ .

Таким образом, мы рассмотрели все возможные варианты и показали, что вычет  $as$  не принадлежит множеству  $\mathcal{S}$ . Лемма доказана.  $\square$

**Лемма 6.2.** Пусть  $a$  и  $b$  два различных элемента из  $\mathbb{Z}_m$ . Элемент  $a$  обратим по модулю  $m$ , а элемент  $b \in \mathcal{A}$ . Тогда множества  $a\mathcal{S}$  и  $b\mathcal{S}$  не пересекаются, если  $a^{-1}b \in \mathcal{A}$ .

*Доказательство.* Предположим, что  $s_1, s_2$  два элемента из множества  $\mathcal{S}$  такие, что  $as_1 \equiv bs_2 \pmod{m}$ . Поскольку  $a$  обратим, получаем, что  $s_1 \equiv a^{-1}bs_2 \pmod{m}$ ,  $s_1 \in \mathcal{S}$ . Из предыдущей леммы получаем, что это невозможно, если  $a^{-1}b \in \mathcal{A}$ . Лемма доказана.  $\square$

*Доказательство теоремы 6.3.* Путь доказательства теоремы зависит от разложения числа  $m$  на простые сомножители. Вначале предположим, что число  $m$  делится на степень простого числа, то есть найдется такое простое число  $p$ , что  $p^\alpha | m$  при некотором целом  $\alpha > 1$ .

Рассмотрим множество

$$\mathcal{G} = \left\{ 1 + k \frac{m}{p} \pmod{m}, \quad \text{для всех } 0 \leq k < p \right\}$$

и покажем, что оно образует мультипликативную группу порядка  $p$ , являющуюся подгруппой группы обратимых элементов  $\mathbb{Z}_m^*$ .

Легко видеть, что операция умножения не выводит за пределы группы  $\mathcal{G}$ . Действительно, в силу определения, выполнено равенство

$$\begin{aligned} \left( 1 + k \frac{m}{p} \right) \left( 1 + h \frac{m}{p} \right) &\equiv \\ &\equiv \left( 1 + (k + h) \frac{m}{p} + kh \frac{m^2}{p^2} \right) \equiv \left( 1 + l \frac{m}{p} \right) \pmod{m}, \end{aligned} \quad (6.4)$$

где  $l \equiv k + h \pmod{p}$ .

Элемент  $g = \left( 1 + k \frac{m}{p} \right) \in \mathcal{G}$  обратим по модулю  $m$ . В противном случае было бы выполнено условие  $\text{НОД}(g, m) = d > 1$  и  $d | 1$ . Более того, из равенства (6.4) следует, что обратным к элементу  $g = \left( 1 + k \frac{m}{p} \right)$  является элемент  $\left( 1 + h \frac{m}{p} \right)$ , у которого  $h \equiv -k \pmod{p}$ . Таким образом, мы показали, что множество  $\mathcal{G}$  образует мультипликативную группу обратимых по модулю  $m$  элементов.

Пусть  $g$  отличный от единицы элемент группы  $\mathcal{G}$ . Рассмотрим сравнение

$$g^{m-1} \equiv \left( 1 + k \frac{m}{p} \right)^{m-1} \pmod{m} \equiv 1 + k(m-1) \frac{m}{p} \pmod{m},$$

при некотором  $k$  таком, что  $0 < k < p$ . Поскольку  $p|m$  и  $p$  не делит  $(m-1)$ , то мы можем считать, что  $m$  не делит  $k(m-1)\frac{m}{p}$  и, следовательно,  $g^{m-1} \not\equiv 1 \pmod{m}$ .

Мы получили, что любой отличный от единицы элемент группы  $\mathcal{G}$  принадлежит множеству  $\mathcal{A}$ . Поскольку  $\mathcal{G}$  является группой, то мы получаем, что  $a^{-1}b \in \mathcal{G} \supset \mathcal{A}$  для любых двух отличных от единицы элементов  $a, b$  группы  $\mathcal{G}$ .

Воспользовавшись утверждением леммы 6.2, получим, что множества  $aS$  и  $bS$  не пересекаются для любых двух элементов  $a, b$  группы  $\mathcal{G}$ . Следовательно,

$$\mathbb{Z}_m \supseteq \left| \bigcup_{g \in \mathcal{G}} gS \right| = |\mathcal{G}| \cdot |S| = p|S|.$$

Вспоминая, что  $\text{НОД}(6, m) = 1$  получаем неравенство  $p \geq 5$  и условие

$$m = |\mathbb{Z}_m| > 4|S|,$$

которое завершает доказательство теоремы для составного числа  $m$ , делящегося, как минимум, на квадрат простого числа.

Теперь рассмотрим случай, когда составное число  $m$  не делится на квадрат простого числа, то есть  $m = p_1 \cdots p_k$ , где  $p_1, \dots, p_k$  различные простые числа,  $k \in \mathbb{N}$ . Без ограничения общности будем считать, что  $p_1 < \cdots < p_k$ .

Определим вычеты для каждого  $i = 1, \dots, k$  определим вычет  $c_i$  по модулю  $m$  как решение системы сравнений

$$\begin{cases} x \equiv a_i \pmod{p_i}, \\ x \equiv 1 \pmod{p_j}, \quad \text{для всех } j, j \neq i, \end{cases}$$

где  $a_i$  первообразный корень по модулю простого числа  $p_i$ .

Сделаем предположение о том, что найдется целое число  $z$  такое, что  $c_i^z \equiv -1 \pmod{m}$ . Поскольку  $p_j|m$ ,  $j \neq i$ , то должно быть выполнено сравнение  $c_i^z \equiv -1 \pmod{p_j}$ . Последнее сравнение никогда не выполнено, в силу построения числа  $c_i$ . Таким образом, все вычеты  $c_1, \dots, c_k \in \mathcal{A}$ . Более того, вычеты  $c_1, \dots, c_k$  обратимы и  $c_1^{-1}, \dots, c_k^{-1} \in \mathcal{A}$ .

Рассмотрим вычет  $d \equiv c_1 c_2 \pmod{m}$  и покажем, что  $d \in \mathcal{A}$ . При  $k \geq 3$  доказательство этого факта аналогично доказательству того, что  $c_i \in \mathcal{A}$ . Рассмотрим случай  $k = 2$ .

Пусть выполнено сравнение  $d^{m-1} \equiv 1 \pmod{m}$ , тогда выполнено  $a^{m-1} \equiv 1 \pmod{p_2}$ , поскольку  $p_2|m$ . Из последнего сравнения следует, что  $p_2 - 1|m - 1$ , см. третье утверждение леммы 2.4, поскольку, в силу построения,  $d \pmod{p_2}$  является первообразным корнем по модулю  $p_2$ .



Запишем равенство

$$m - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) - p_1 - 1, \quad \text{и} \quad p_1 - 1 < p_2 - 1,$$

из которого следует, что  $m - 1$  не может делиться на  $p_2 - 1$ . Из полученного противоречия следует, что  $d^{m-1} \not\equiv 1 \pmod{m}$ , то есть  $d \in \mathcal{A}$ .

Для завершения доказательства рассмотрим четыре множества  $S$ ,  $c_1 S$ ,  $c_2 S$ ,  $dS \subset \mathbb{Z}_m$ . В силу леммы 6.2 эти множества не пересекаются, следовательно,  $4|S| \leq |\mathbb{Z}_m|$ . Теорема доказана.  $\square$

Теорема Рабина в явном виде описывает множество вычетов (множество  $\mathcal{S}$ ), которое должно использоваться для проверки, является ли число  $m$  составным или нет. Опишем алгоритм, реализующий данный тест.

### Алгоритм 6.3 (Тест Миллера-Рабина)

**Вход:** Целое нечетное число  $m$  такое, что  $\text{НОД}(6, m) = 1$ .

**Выход:** Заключение о том, что число составное, либо заключение о том, что число не является составным с некоторой вероятностью.

1. Вычислить такие целые числа  $n, q$ , что  $m - 1 = 2^n q$  и  $q$  – нечетно.
2. Определить  $k = 20$  число попыток выбора случайного числа в теореме Рабина.
3. Вычислить  $k = k - 1$ . Если  $k = 0$ , то завершить алгоритм с заключением, что  $m$ , вероятно, простое число.
4. Выбрать случайный вычет  $a \in \mathbb{Z}_m$  и вычислить  $b \equiv a^q \pmod{m}$ .
5. Если  $b \equiv \pm 1 \pmod{m}$ , то вернуться на шаг 3. В противном случае, определить счетчик  $i = 0$ .
6. Пока  $i < n$  выполнить
  - 6.1. Вычислить  $b \equiv b^2 \pmod{m}$ .
  - 6.2. Если  $b \equiv -1 \pmod{m}$ , то вернуться на шаг 3. В противном случае вычислить  $i = i + 1$ .
7. Завершить алгоритм с заключением, что число  $m$  составное.  $\square$

Сделаем несколько замечаний к данному алгоритму. Как следует из теоремы Рабина, мы можем принять составное число  $m$  за простое с вероятностью  $\frac{1}{4}$ . В алгоритме мы реализуем  $k$  попыток проверки условий теоремы, следовательно, общая вероятность принять составное число за простое составляет  $\frac{1}{4^k}$ .

Мы выбираем число  $k$  достаточно случайно, исходя из эффективности реализации теста Миллера-Рабина. Вместе с тем необходимо заметить, что в детерминированном варианте данного теста Миллер, см. [37], предложил перебирать все значения  $a$  от двойки до величины  $\ln^2 m$ . Он доказал, что в этом случае, при выполнении расширенной гипотезы Римана, число  $m$  будет простым.

И еще, на четвертом шаге алгоритма мы можем выбирать случайный вычет  $a$  не из всего кольца  $\mathbb{Z}_m$ , а из некоторого малого множества, например  $1 < a < 2^w$ , где  $w$  определяет разрядность регистров процессора ЭВМ, выполняющей вычисления. Это не изменит общей вероятности, однако несколько снизит трудоемкость алгоритма при возведении в степень на четвертом шаге алгоритма.

При практических вычислениях число, проходящее тест Миллера-Рабина, предварительно тестируется на наличие маленьких делителей методом пробных делений. Поэтому, в силу выбора небольших значений  $a$ , мы не стали добавлять в четвертый шаг алгоритма проверку условия  $\text{НОД}(a, m) = 1$ .

## 6.2 $N - 1$ методы доказательства простоты

Теперь мы перейдем к рассмотрению методов, позволяющих получить строгое доказательство простоты числа. Именно подобный класс методов используется на практике при построении простых чисел, используемых в криптографических схемах.

Методы доказательства простоты целых чисел, использующие разложение числа  $m - 1$  на простые множители, были известны достаточно давно. Мы можем доказать хорошо известную теорему Э. Люка (Édouard Lucas) о простоте числа  $m$ , основанную на свойствах первообразных корней.

**Теорема 6.4** (Люка, 1876). Пусть  $m > 1$  нечетное целое число. Если найдется такое целое число  $a$ ,  $\text{НОД}(a, m) = 1$ , такое, что для любого простого делителя  $q$  числа  $m - 1$  выполнены сравнения

$$a^{m-1} \equiv 1 \pmod{m}, \quad a^{\frac{m-1}{q}} \not\equiv 1 \pmod{m},$$

то  $m$  – простое число.

*Доказательство.* Пусть существует целое число  $a$ , для которого выполнены условия теоремы. Тогда из утверждения теоремы 2.9 следует, что  $\text{ord}_m a = m - 1$  и  $a$  является первообразным корнем по модулю  $m$ . Следовательно,  $\varphi(m) = m - 1$ , а это возможно только в случае, когда  $m$  простое число.  $\square$

Основываясь на теореме Люка мы можем предложить простой тест проверки простоты нечетного числа  $m$ , если известно разложение  $m - 1$

на множители.

### Алгоритм 6.4 (Алгоритм Люка для доказательства простоты)

**Вход:** Целое число  $m$  такое, что  $m - 1 = \prod_{k=1}^n q_k^{\alpha_k}$ .

**Выход:** Заключение о том, является ли число  $m$  простым или составным.

1. Определить  $c = 20$  и  $k = 1$ .
2. Выбрать случайно элемент  $1 \leq a < m$ . Если  $\text{НОД}(a, m) > 1$ , то закончить алгоритм с уведомлением, что число  $m$  составное.
3. Вычислить  $c = c - 1$ . Если  $c = 0$ , то завершить алгоритм с уведомлением, что алгоритм не может дать однозначного ответа на вопрос, составное число или нет.
4. Пока  $k \leq n$  выполнить
  - 4.1. Если выполнено условие  $a^{m-1} \not\equiv 1 \pmod{m}$ , то закончить алгоритм с уведомлением, что число  $m$  составное.
  - 4.2. Если выполнено условие  $a^{\frac{m-1}{q_k}} \equiv 1 \pmod{m}$ , то вернуться на шаг 2.
  - 4.3. Вычислить  $k = k + 1$ .
5. Завершить алгоритм с уведомлением, что число  $m$  простое. □

Ситуация, когда нам полностью известно разложение числа  $m - 1$  на простые множители, возникает нечасто. Как правило, используемые нами методы разложения на множители позволяют получить лишь частичное разложение числа  $m - 1$  на множители. Это вынуждает нас использовать более тонкие результаты, чем теорема Люка.

Итак, мы хотим проверить на простоту нечетное целое число  $m > 0$ . Запишем  $m - 1$  в виде

$$m - 1 = fr, \quad \text{НОД}(f, r) = 1, \quad (6.5)$$

где  $f$  число с известным разложением на множители  $f = \prod_{k=1}^n q_k^{\alpha_k}$ , а  $r$  составное число с неизвестным разложением на множители. Заметим, что если число  $r$  простое, то мы получаем полное разложение числа  $m - 1$  на простые сомножители, что позволяет нам воспользоваться теоремой Люка для проверки простоты  $m$ .

Дополнительно мы будем считать, что каждый простой делитель  $q$  числа  $r$  удовлетворяет неравенству  $q > B$  для некоторого натурального числа  $B$ . В качестве границы  $B$ , на практике, можно выбрать величину

$$B = \max_k q_k,$$

то есть максимальное из простых чисел, входящих в разложение числа  $f$ . Впрочем, можно несколько увеличить эту границу, взяв в качестве величины  $B$  значение  $q_{k+1} - 1$ , где  $q_{k+1}$  следующее за максимальным  $q_k$  простое число.

Определим следующие условия.

1. Для каждого простого числа  $q_k$ ,  $k = 1, \dots, n$ , входящего в разложение числа  $f$ , найдется некоторое взаимно простое с  $m$  целое число  $a_k$  такое, что

$$a_k^{m-1} \equiv 1 \pmod{m} \quad \text{и} \quad \text{НОД} \left( a_k^{\frac{m-1}{q_k}} - 1, m \right) = 1. \quad (6.6)$$

2. Найдется некоторое взаимно простое с  $m$  целое число  $b$  такое, что

$$b^{m-1} \equiv 1 \pmod{m} \quad \text{и} \quad \text{НОД} \left( b^{\frac{m-1}{r}} - 1, m \right) = 1. \quad (6.7)$$

Выполнимость одного или двух указанных условий позволяет нам говорить о простоте числа  $m$ .

**Теорема 6.5** (Поклингтон, 1918). *Рассмотрим нечетное натуральное число  $m$ , удовлетворяющее условию (6.6). Пусть  $p$  произвольный простой делитель числа  $m$ , тогда*

$$p \equiv 1 \pmod{f}.$$

*Доказательство.* Пусть выполнены утверждения теоремы и  $p$  произвольный простой делитель числа  $m$ . Рассмотрим  $q_k$  некоторый простой делитель, входящий в разложение числа  $f$ , и обозначим символом  $t$  показатель числа  $a_k$  по модулю  $p$ .

Из первого утверждения теоремы следует, что  $a_k^{m-1} \equiv 1 \pmod{p}$ , тогда, согласно третьему утверждению леммы 2.4,  $t|m-1$ . Из второго утверждения теоремы получаем, что  $a_k^{\frac{m-1}{q_k}} \not\equiv 1 \pmod{p}$ , следовательно,  $t$  не делит  $\frac{m-1}{q_k}$ . Поскольку  $q_k^{\alpha_k} | m-1$ , то из полученных условий вытекает, что  $q_k^{\alpha_k} | t$ .

С другой стороны, согласно малой теореме Ферма, см. теорему 2.7, выполнено  $t|p-1$ . Таким образом, мы получаем, что  $q_k^{\alpha_k} | p-1$ , что равносильно,

$$p \equiv 1 \pmod{q_k^{\alpha_k}}.$$

В силу произвольного выбора индекса  $k$  мы получаем, что последнее сравнение выполнено для всех индексов  $k = 1, \dots, n$ . Следовательно, по китайской теореме об остатках, см. теорему 2.3, выполнено сравнение  $p \equiv 1 \pmod{f}$ , поскольку  $f = \prod_{k=1}^n q_k^{\alpha_k}$ . Теорема доказана.  $\square$

Доказанный нами результат был впоследствии использован Дерриком Лемером (Derrick Henry Lehmer) для доказательства простоты целых чисел. Следуя статье [53], приведем несколько полезных для наших целей результатов.

**Теорема 6.6** (Лемер, 1927). Пусть  $m > 0$  нечетное целое число. Если число  $m$  удовлетворяет условию теоремы 6.5 и  $f^2 \geq \sqrt{m}$ , то  $m$  - простое.

*Доказательство.* Если выполнены условия теоремы 6.5, то для любого простого делителя  $p$  числа  $m$  выполнено равенство  $p = 1 + kf$  при некотором  $k \in \mathbb{Z}$ . Следовательно, для любого простого делителя  $p$  выполнено неравенство  $p = 1 + kf \geq 1 + \sqrt{m} > \sqrt{m}$ , которое противоречит утверждению леммы 1.6. Полученное противоречие завершает доказательство.  $\square$

Приведем пример использования данной теоремы.

**Пример 6.1.** Рассмотрим число  $m = 156 \cdot 5^{202} + 1$ . Используя вычисления на ЭВМ, находим, что

$$13^m \equiv 1 \pmod{m} \quad \text{и} \quad \text{НОД}(13^{156 \cdot 5^{201}}, m) = 1,$$

следовательно, всякий простой делитель  $p$  числа  $m$  имеет вид  $p = 1 + k5^{202}$ . Поскольку  $5^{202} > \sqrt{m}$ , то число  $m$  простое.

Теперь покажем, как можно использовать для доказательства простоты введенное нами ранее условие (6.7).

**Теорема 6.7.** Пусть  $m$  нечетное натуральное число, для которого выполнено условие (6.7) и  $p$  произвольный простой делитель числа  $m$ , тогда

$$p \equiv 1 \pmod{q},$$

где  $q$  некоторый простой делитель числа  $r$ .

*Доказательство.* Пусть  $p|m$ . Обозначим символом  $t$  показатель элемента  $b$  по модулю простого числа  $p$ . Тогда из условия  $b^{m-1} \equiv 1 \pmod{m}$  следует, что  $b^{m-1} \equiv 1 \pmod{p}$  и  $t|m-1$ . Из второго условия теоремы  $\text{НОД}(b^{\frac{m-1}{r}}, m) = 1$  следует, что  $b^{\frac{m-1}{r}} \not\equiv 1 \pmod{p}$  и  $t$  не делит  $\frac{m-1}{r}$ . Суммируя оба вывода, получаем, что  $\text{НОД}(t, r) > 1$ , следовательно, найдется простой делитель  $q$  числа  $r$  такой, что  $q|t$ .

Поскольку  $t|p-1$  получаем, что  $q|p-1$  или, что равносильно,  $p \equiv 1 \pmod{q}$ . Теорема доказана.  $\square$

Скомбинировав утверждения двух последних теорем, можно получить следующее утверждение.

**Теорема 6.8.** Пусть  $m$  нечетное натуральное число, для которого выполнены условия (6.6) и (6.7). Пусть  $p$  произвольный простой делитель числа  $m$ , тогда

$$p \equiv 1 \pmod{fq},$$

где  $q$  некоторый простой делитель числа  $r$ . Кроме того, если выполнено неравенство

$$(1 + fB)^2 > m, \quad (6.8)$$

то  $m$  простое число.

Доказательство данной теоремы очевидным образом основывается на утверждениях предыдущих теорем, и мы оставляем его читателю в качестве упражнения.

При больших значениях числа  $m$  не всегда удастся получить значения  $f$  и  $B$ , удовлетворяющие неравенству (6.8). В этом случае можно воспользоваться утверждением следующей теоремы.

**Теорема 6.9.** Пусть  $m$  нечетное натуральное число, для которого выполнено условие (6.6) и неравенство  $f^3 > m > f^2$ . Определим целые, неотрицательные числа  $c_1, c_2$  равенствами

$$c_1 \equiv \frac{m-1}{f} \pmod{f} \quad \text{и} \quad c_2 = \frac{m - c_1 f - 1}{f^2},$$

то есть разложим число  $m$  по степеням  $f$ . Число  $m$  простое тогда и только тогда, когда многочлен  $f(x) = c_2 x^2 + c_1 x + 1 \in \mathbb{Z}[x]$  неприводим в кольце целых чисел.

*Доказательство.* Предположим, что число  $m$  составное и обозначим символом  $p_1$  его простой делитель. Поскольку  $m$  удовлетворяет условию (6.6), то из теоремы Поклингтона, см. теорему 6.5,  $p_1 = 1 + x_1 f$  для некоторого натурального  $x_1$ .

Обозначим символом  $p_2$  целое число, удовлетворяющее  $p_2 = \frac{m}{p_1}$ . Поскольку каждый простой делитель числа  $p_2$  также является и делителем числа  $m$ , то для  $p_2$  выполнено равенство  $p_2 = 1 + x_2 f$  для некоторого натурального  $x_2$ .

Легко видеть, что  $p_2 < f^2$ . В противном случае получаем противоречивое неравенство  $m = p_1 p_2 = (1 + x_1 f)(1 + x_2 f) > f p_2 > f^3 \geq m$ . Таким образом, выполнено  $f < p_2 < f^2$ . Аналогичным способом выведем, что  $f < p_1 < f^2$ . Из полученных неравенств следуют неравенства  $0 < x_1, x_2 < f$ .

Вспомним, что число  $m$  удовлетворяет равенству  $m = c_2 f^2 + c_1 f + 1$ , где значения  $c_1$  и  $c_2$  определены в условии теоремы, и запишем систему уравнений относительно неизвестных  $x_1, x_2$

$$\begin{cases} x_1 + x_2 = c_1, \\ x_1 x_2 = c_2. \end{cases}$$

Решение указанной системы в целых числах равносильно поиску целых корней многочлена  $f(x) = c_2 x^2 + c_1 x + 1 \in \mathbb{Z}[x]$ . Если система разрешима в целых числах, то мы находим разложения числа  $m$  на множители. Если система неразрешима, то число  $m$  простое. Теорема доказана.  $\square$

## 6.3 Числа Мерсенна

Сделаем отступление и рассмотрим небольшой класс целых чисел, исследования которого привели к появлению  $N + 1$  метода доказательства простоты. Сам метод мы рассмотрим далее, сейчас же остановим свое внимание на целых числах вида  $2^p - 1$ , где  $p$  простое число.

**Определение 6.1.** Мы будем называть целое число  $m$  совершенным, если оно равно сумме всех своих делителей, отличных от него самого.

Приведем примеры совершенных чисел.

$$\begin{aligned} 6 &= 1 + 2 + 3 &= 2(2^2 - 1), \\ 28 &= 1 + 2 + 4 + 7 + 14 &= 2^2(2^3 - 1), \\ 496 &= 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 &= 2^3(2^5 - 1). \end{aligned}$$

В общем случае, мы можем записать совершенное число в виде  $m = 2^{p-1} M_p$ , где  $M_p = 2^p - 1$ . Верна следующая лемма.

**Лемма 6.3.** Если  $M_p = 2^p - 1$  простое число, то число  $m = 2^{p-1} M_p$  совершенно.

*Доказательство.* Все делители числа  $m$ , включая само число, имеют вид

$$1, 2, 2^2, \dots, 2^{p-1}, M_p, 2M_p, \dots, 2^{p-1} M_p.$$

Суммируя все делители, получаем

$$(M_p + 1)(1 + 2 + \dots + 2^{p-1}) = (M_p + 1)S. \quad (6.9)$$

Для определения величины  $S$  запишем равенство

$$S = 2S - S = 2 + 2^2 + \dots + 2^p - 1 - 2 - 2^2 - \dots - 2^{p-1} = 2^p - 1 = M_p,$$

следовательно сумма (6.9) равна  $(M_p + 1)M_p = 2^p M_p$ . Вспоминая, что данная сумма содержит число  $m = 2^{p-1}M_p$  получаем равенство

$$2^p M_p - 2^{p-1} M_p = 2^{p-1} M_p = m,$$

которое завершает доказательство леммы.  $\square$

Из утверждения леммы следует, что каждое простое число  $M_p$  порождает совершенное число. Обратная связь менее тривиальна. Леонард Эйлер доказал, что если  $m$  четно и совершенно, то оно имеет рассмотренный нами вид  $2^{p-1}M_p$ . Результаты о нечетных совершенных числах неизвестны. Существует лишь гипотеза Эйлера о том, что нечетных совершенных чисел нет.

**Определение 6.2.** Число  $M_p = 2^p - 1$  называется числом Мерсенна, если оно простое.

Свое название простые числа вида  $2^p - 1$  получили по имени французского математика Марена Мерсенна (Marin Mersenne), который принимал активное участие в их изучении. Приведем примеры чисел Мерсенна.

$$\begin{aligned} M_2 &= 2^2 - 1 = 3, \\ M_3 &= 2^3 - 1 = 7, \\ M_5 &= 2^5 - 1 = 31, \\ M_7 &= 2^7 - 1 = 127, \\ M_{13} &= 2^{13} - 1 = 8191, \\ M_{17} &= 2^{17} - 1 = 131071, \\ M_{19} &= 2^{19} - 1 = 524882. \end{aligned}$$

Отметим, что простота последних двух чисел была доказана итальянцем Пьетро КATALДИ (Pietro Cataldi) уже к 1588 году, то есть еще до рождения Мерсенна.

**Лемма 6.4.** Если число  $M_p = 2^p - 1$  простое, то  $p$  простое число.

*Доказательство.* Предположим обратное, тогда  $p = ab$ , где  $a, b$  нетривиальные делители. Верно равенство

$$M_p = 2^{ab} - 1 = (2^a - 1) \left( 1 + 2^a + 2^{2a} + \dots + 2^{(b-1)a} \right).$$



Поскольку  $a > 1$ , то величина  $2^a - 1$  является нетривиальным делителем числа  $M_p$ . Полученное противоречие завершает доказательство леммы.  $\square$

Необходимо отметить, что обратное утверждение неверно. Действительно, при  $p = 11$  получаем, что число

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

является составным. Докажем еще один результат о специфичности чисел Мерсенна.

**Лемма 6.5.** Пусть  $a > 0$  целое число и число  $a^p - 1$  простое. Тогда, либо  $a = 2$ , либо  $p = 1$ .

*Доказательство.* Заметим, что из сравнения  $a - 1 \equiv 0 \pmod{a - 1}$  следует, сравнение  $a \equiv 1 \pmod{a - 1}$ . Возведем обе части сравнения в степень  $p$ , тогда  $a^p \equiv 1 \pmod{a - 1}$  или, что равносильно,  $a - 1 \mid a^p - 1$ .

Пусть  $a^p - 1$  простое число. Тогда из полученного условия следует выполнение одного из двух условий: либо  $a - 1 = \pm 1$ , либо  $p = 1$ . Поскольку из равенства  $a - 1 = -1$  следует, что  $a = 0$ , то мы получаем утверждение леммы.  $\square$

Мы можем получить информацию о делителях чисел вида  $2^p - 1$ . Докажем следующий результат.

**Лемма 6.6.** Пусть  $p$  нечетное простое число, тогда для любого нечетного простого делителя  $q$  числа  $2^p - 1$  выполнено сравнение

$$q \equiv 1 \pmod{2p}.$$

*Доказательство.* Предположим, что  $\text{НОД}(p, q - 1) = 1$ , воспользуемся расширенным алгоритмом Эвклида и найдем целые числа  $u$  и  $v$ , удовлетворяющие лемме Безу, см. лемму 2.2, т.е.

$$u(q - 1) + vp = 1. \quad (6.10)$$

Поскольку  $q$  является делителем числа  $2^p - 1$ , то  $2^p - 1 \equiv 0 \pmod{q}$  или  $2^p \equiv 1 \pmod{q}$ .

Используя полученное сравнение, равенство (6.10), а также малую теорему Ферма, получаем

$$2 \equiv 2^{u(q-1)+vp} \equiv (2^{q-1})^u (2^p)^v \equiv 1 \pmod{q},$$

то есть противоречие. Следовательно, наше предположение неверно и выполнено условие  $\text{НОД}(p, q - 1) > 1$ . Поскольку  $p$  простое число, то  $p|q - 1$  или  $q = 1 + kp$  для некоторого натурального числа  $k$ .

В условии леммы предполагается, что числа  $p$  и  $q$  нечетны, следовательно, четна величина  $k$ , т.е.  $q \equiv 1 \pmod{2p}$ . Лемма доказана.  $\square$

Утверждение леммы легко проиллюстрировать следующими примерами.

$$\begin{aligned} 2^{11} - 1 &= 2047 = 23 \cdot 89 = (1 + 2 \cdot 11)(1 + 2 \cdot 4 \cdot 11), \\ \left. \begin{aligned} M_5 &= 31 = 1 + 2 \cdot k \cdot 5, \text{ где } k = 5, \\ M_{13} &= 8191 = 1 + 2 \cdot k \cdot 13, \text{ где } k = 315, \end{aligned} \right\} \text{Простые.} \end{aligned}$$

Доказанная лемма позволяет получить еще одно доказательство теоремы Эвклида о бесконечности простых чисел, см. теорему 1.3.

**Теорема 6.10.** *Множество простых чисел бесконечно.*

*Доказательство.* Предположим обратное и обозначим  $p$  – максимальное из простых чисел. Из утверждения леммы 6.6 следует, что для любого нечетного простого делителя  $q$  числа  $2^p - 1$  выполнено равенство  $q = 1 + 2kp$  для некоторого натурального  $k$ .

Поскольку  $q = 1 + 2kp > p$ , то мы предъявили еще одно простое число, большее, чем  $p$ . Следовательно, наше предположение неверно.  $\square$

Желание найти как можно большее число Мерсенна привело к разработке методов доказательства простоты, использующих тот факт, что число  $M_p + 1 = 2^p$ , то есть является степенью двойки или, в более общем смысле, является произведением небольших простых чисел.

## 6.4 $N + 1$ метод доказательства простоты

Рассмотрим метод доказательства простоты числа  $m$ , использующий разложение  $m + 1$  на простые сомножители. Метод был разработан для поиска больших чисел Мерсенна, однако он применим и к произвольным числам, для которых разложение числа  $m + 1$  на простые сомножители не содержит больших делителей.

Прежде чем сформулировать и доказать необходимое утверждение, мы дадим некоторые определения.

**Определение 6.3.** *Рассмотрим многочлен  $f(x) = x^2 - ax + b$  с целыми коэффициентами такими, что  $\text{НОД}(a, b) = 1$  и дискриминант*

многочлена  $D = a^2 - 4b$  отличен от нуля. Обозначим

$$\alpha = \frac{a + \sqrt{D}}{2}, \quad \beta = \frac{a - \sqrt{D}}{2}, \quad \alpha > \beta,$$

корни многочлена  $f(x)$  и определим последовательности чисел  $U_n, V_n$  равенствами

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n, \quad n = 0, 1, \dots \quad (6.11)$$

Мы будем называть последовательности  $\{U_n\}, \{V_n\}$  рекуррентными последовательностями Люка.

Данное нами определение рекуррентных последовательностей Люка не задает, в явном виде, соотношения между элементами последовательности. Следующая лемма позволяет предъявить данные соотношения, а также выявить ряд полезных свойств рекуррентных последовательностей Люка.

**Лемма 6.7.** Пусть последовательности чисел  $\{U_n\}, \{V_n\}$  определены равенствами (6.11). Тогда верны следующие утверждения.

1. Для всех индексов  $n = 0, 1, \dots$  значения  $U_n, V_n$  являются целыми числами. Более того, выполнены рекуррентные соотношения

$$U_{n+1} = aU_n - bU_{n-1}, \quad V_{n+1} = aV_n - bV_{n-1}, \quad n = 1, 2, \dots \quad (6.12)$$

где  $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a$ .

2. Выполнены равенства

$$U_{2n} = U_n V_n, \quad V_{2n} = \frac{1}{2} (V_n^2 + D U_n^2). \quad (6.13)$$

3. Выполнены равенства

$$U_{n+1} = \frac{1}{2} (V_n + aU_n), \quad V_{n+1} = \frac{1}{2} (aV_n + D U_n). \quad (6.14)$$

4. Выполнены равенства

$$U_{k+l} = \frac{1}{2} (U_k V_l + U_l V_k), \quad V_{k+l} = \frac{1}{2} (V_k V_l + D U_k U_l). \quad (6.15)$$

5. Выполнено равенство  $4b^n = V_n^2 - D U_n^2$ .

6. Для любого индекса  $d$  такого, что  $d|n$ , выполнено  $U_d|U_n$ .

*Доказательство.* Прежде чем переходить к доказательству перечисленных утверждений, заметим, что для корней многочлена  $f(x)$ , в силу теоремы Виета, выполнены простые соотношения, которые будут использованы нами далее

$$\alpha + \beta = a, \quad \alpha\beta = b, \quad (\alpha - \beta)^2 = D. \quad (6.16)$$

Докажем первое утверждение леммы. Подставляя значения  $n = 0, 1$  в соотношения (6.11), получим равенства  $U_0 = 0, U_1 = 1$ , а также  $V_0 = 2, V_1 = a$ . Теперь, используя индуктивное предположение, докажем истинность соотношений (6.12). Учитывая (6.16), получаем равенства

$$\begin{aligned} aU_n - bU_{n-1} &= \frac{1}{\alpha - \beta} ((\alpha + \beta)(\alpha^n - \beta^n) - \alpha\beta(\alpha^{n-1} - \beta^{n-1})) = \\ &= \frac{1}{\alpha - \beta} (\alpha^{n+1} - \beta^{n+1}) = U_{n+1}, \end{aligned}$$

$$\begin{aligned} aV_n - bV_{n-1} &= (\alpha + \beta)(\alpha^n + \beta^n) - \alpha\beta(\alpha^{n+1} + \beta^{n+1}) = \\ &= \alpha^{n+1} + \beta^{n+1} = V_{n+1}. \end{aligned}$$

Из полученных равенств следует, что все элементы последовательностей  $\{U_n\}, \{V_n\}$  выражаются через целые коэффициенты  $a, b$  и начальные значения  $U_0, U_1$  и  $V_0, V_1$ , то есть являются целыми числами.

Доказательства остальных утверждений леммы проводятся аналогичным способом. Действительно, с учетом (6.16), получаем равенства

$$U_{2n} = \frac{1}{\alpha - \beta} (\alpha^{2n} - \beta^{2n}) = \frac{1}{\alpha - \beta} (\alpha^n - \beta^n)(\alpha^n + \beta^n) = U_n V_n,$$

$$V_n^2 + DU_n^2 = (\alpha^n + \beta^n)^2 + (\alpha^n - \beta^n)^2 = 2(\alpha^{2n} + \beta^{2n}) = 2V_{2n},$$

из которых следует второе утверждение леммы.

Третье утверждение леммы, при внимательном рассмотрении, оказывается частным случаем четвертого утверждения.

Четвертое утверждение леммы вытекает из равенств

$$\begin{aligned} U_k V_l + U_l V_k &= \frac{1}{\alpha - \beta} ((\alpha^l + \beta^l)(\alpha^k - \beta^k) + (\alpha^k + \beta^k)(\alpha^l - \beta^l)) = \\ &= \frac{2}{\alpha - \beta} (\alpha^{k+l} - \beta^{k+l}) = 2U_{k+l}. \end{aligned}$$

$$\begin{aligned} V_k V_l + D U_k U_l &= (\alpha^k + \beta^k) (\alpha^l + \beta^l) + (\alpha - \beta)^2 \frac{(\alpha^k - \beta^k)}{\alpha - \beta} \frac{(\alpha^l - \beta^l)}{\alpha - \beta} = \\ &= 2 (\alpha^{k+l} + \beta^{k+l}) = 2 V_{k+l}. \end{aligned}$$

Докажем пятое утверждение леммы. Для этого выразим  $\alpha^n, \beta^n$  через  $U_n, V_n$ . Поскольку выполнены равенства (6.11), то

$$2\alpha^n = V_n - (\alpha - \beta)U_n, \quad 2\beta^n = V_n + (\alpha - \beta)U_n,$$

тогда, с учетом (6.16), получаем равенства

$$4b^n = (2\alpha^n)(2\beta^n) = V_n^2 - (\alpha - \beta)^2 U_n^2 = V_n^2 - D U_n^2$$

и доказательство пятого утверждения леммы.

Доказательство последнего утверждения леммы проведем по индукции. Рассмотрим  $U_d$ , тогда из второго утверждения леммы следует равенство  $U_{2d} = U_d V_d$  и  $U_d | U_{2d}$ . Теперь предположим, что утверждение леммы выполнено для всех целых индексов  $d, 2d, 3d, \dots, (k-1)d$ . Покажем, что оно выполнено и для индекса  $kd$ .

Воспользовавшись четвертым утверждением леммы, запишем равенство

$$2U_{kd} = U_d V_{(k-1)d} + V_d U_{(k-1)d}.$$

Поскольку, по предположению индукции,  $U_d | U_{(k-1)d}$ , то правая часть приведенного равенства делится на  $U_d$  и  $U_d | U_{kd}$ . Лемма доказана.  $\square$

Приведем пример вычисления элементов рекуррентных последовательностей Люка.

**Пример 6.2.** Рассмотрим целые числа  $a = 3, b = 1$  и построим элементы рекуррентных последовательностей Люка для всех  $n = 0, 1, \dots, 11$ . Согласно первому утверждению леммы, выполнены равенства

$$\begin{aligned} (U_0, V_0) &= (0, 2), \\ (U_1, V_1) &= (1, 3). \end{aligned}$$

Далее, воспользовавшись рекуррентными соотношениями (6.12), вычисляем

$$\begin{aligned} (U_2, V_2) &= (3, 7), & (U_7, V_7) &= (377, 843), \\ (U_3, V_3) &= (8, 18), & (U_8, V_8) &= (987, 2207), \\ (U_4, V_4) &= (21, 47), & (U_9, V_9) &= (2584, 5778), \\ (U_5, V_5) &= (55, 123), & (U_{10}, V_{10}) &= (6765, 15127), \\ (U_6, V_6) &= (144, 322), & (U_{11}, V_{11}) &= (17711, 39603), \\ & & (U_{12}, V_{12}) &= (46368, 103682). \end{aligned}$$

Понятно, что при больших значениях индекса  $n$  вычислить пару  $U_n, V_n$ , наивно применяя соотношения (6.12), достаточно сложно. Мы можем предложить простой алгоритм, использующий соотношения (6.13) и (6.14), сложность которого оценивается величиной  $O(\log_2 n)$ . Это делает его пригодным для вычисления элементов последовательностей Люка с произвольно большим индексом.

Приводимый нами алгоритм вычисляет значение пары элементов  $U_{kn}, V_{kn}$  последовательности Люка для заданной начальной пары значений  $U_k, V_k$  и целочисленного индекса  $n > 1$ , представленного в двоичном представлении  $n = \sum_{i=0}^{r-1} n_i 2^i$ . Напомним, что, согласно (6.12), при  $k = 1$  начальная пара последовательности Люка имеет вид  $U_1 = 1, V_1 = a$ .

### Алгоритм 6.5 (Вычисление последовательностей Люка)

**Вход:** Целые числа  $a, b$  такие, что  $\text{НОД}(a, b) = 1$ , целочисленный индекс  $n > 1$ , представленный в двоичном представлении  $n = \sum_{i=0}^{r-1} n_i 2^i$  и пара начальных значений последовательности  $U_k, V_k$ .

**Выход:** Пара элементов  $U_{kn}, V_{kn}$  рекуррентных последовательностей Люка.

1. Присвоить начальные значения переменным  $s = 0, i = 0, D = a^2 - 4b$ .
2. **Пока**  $n_i = 0$  **выполнять**  $s = s + 1, i = i + 1$ .
3. Определить  $U = U_k, V = V_k$  и вычислить  $i = i + 1$ .
4. **Пока**  $i \leq r - 1$  **выполнить**

4.1. Используя равенства (6.13), вычислить

$$x = UV, \quad y = \frac{1}{2} (V^2 + DU^2), \quad U = x, \quad V = y.$$

4.2. **Если**  $n_i = 1$ , **то**, используя равенства (6.14), вычислить

$$x = \frac{1}{2} (V + aU), \quad y = \frac{1}{2} (aV + DU), \quad U = x, \quad V = y.$$

4.3. Вычислить  $i = i + 1$ .

5. **Пока**  $s > 0$  **выполнить**

5.1. Используя равенства (6.13), вычислить

$$x = UV, \quad y = \frac{1}{2} (V^2 + DU^2), \quad U = x, \quad V = y.$$

5.2. Вычислить  $s = s - 1$ .

6. Завершить алгоритм и вернуть пару значений  $U, V$ . □

Используя приведенный алгоритм, для вычисления пары  $(U_{12}, V_{12})$  из примера 6.2, нам потребуется вычислить лишь пары элементов  $(U_1, V_1), (U_2, V_2), (U_3, V_3), (U_6, V_6)$  и  $(U_{12}, V_{12})$ .

Теперь перейдем к доказательству результатов, которые потребуются для проверки простоты целых чисел.

**Лемма 6.8.** Пусть  $p$  нечетное простое,  $\{U_n\}$  рекуррентная последовательность Люка с параметрами  $a, b$  и  $b \not\equiv 0 \pmod{p}$ . Пусть  $d$  минимальное целое число такое, что  $U_d \equiv 0 \pmod{p}$ . Тогда  $U_n \equiv 0 \pmod{p}$  тогда и только тогда, когда  $d|n$ .

*Доказательство.* Если индекс  $d|n$  то, согласно последнему утверждению леммы 6.7,  $U_d|U_n$  и, очевидно,  $U_n \equiv 0 \pmod{p}$ .

Предположим обратное, пусть  $n = kd + r$  для некоторого целого  $r$  такого, что  $0 < r < d$ .

Воспользовавшись четвертым утверждением леммы 6.7 получаем равенство  $U_n = U_{kd}V_r + U_rV_{kd}$ . Поскольку из предыдущих рассуждений и условия леммы следуют сравнения  $U_n \equiv 0 \pmod{p}$  и  $U_{kd} \equiv 0 \pmod{p}$ , мы получаем  $U_rV_{kd} \equiv 0 \pmod{p}$ . Поскольку  $d$  выбрано минимальным, а  $r < d$ , то мы получаем, что  $V_{kd} \equiv 0 \pmod{p}$ .

Теперь воспользуемся пятым утверждением леммы 6.7 и получим сравнение

$$4b^{kd} = V_{kd}^2 - DU_{kd}^2 \equiv 0 \pmod{p}.$$

Поскольку  $p$  нечетно, то мы получаем, что  $p|b$ , а это противоречит условиям леммы, следовательно, при  $r > 0$  разложение  $n = kd + r$  невозможно. Лемма доказана.  $\square$

**Лемма 6.9.** Пусть  $p$  нечетное простое число, удовлетворяющее условиям предыдущей леммы. Более того,  $D = a^2 - 4b \not\equiv 0 \pmod{p}$ . Обозначим  $\Phi(p) = p - \left(\frac{D}{p}\right)$ , где  $\left(\frac{D}{p}\right)$  символ Лежандра. Тогда выполнено сравнение

$$U_{\Phi(p)} \equiv 0 \pmod{p}.$$

*Доказательство.* Напомним, что  $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ , где  $\alpha = \frac{a + \sqrt{D}}{2}$ ,  $\beta = \frac{a - \sqrt{D}}{2}$ .

Вычислим значение  $\alpha^p \pmod{p}$ . Для этого вычислим  $\left(\frac{a + \sqrt{D}}{2}\right)^p = \frac{1}{2^p}(A_p + B_p\sqrt{D})$  и приведем по модулю  $p$  значения  $A_p$  и  $B_p$ .

Таким образом, используя малую теорему Ферма и критерий Эйлера, получаем сравнение

$$\begin{aligned} \alpha^p &\equiv \frac{1}{2^p}(a + \sqrt{D})^p \equiv \frac{1}{2} \left( a + D^{\frac{p-1}{2}} \sqrt{D} \right) \equiv \\ &\equiv \frac{1}{2} \left( a + \left( \frac{D}{p} \right) \sqrt{D} \right) \pmod{p}. \end{aligned}$$

Аналогичными рассуждениями получаем сравнение

$$\beta^p \equiv \frac{1}{2} \left( a - \left( \frac{D}{p} \right) \sqrt{D} \right) \pmod{p}.$$

Мы можем переписать полученные сравнения в следующем виде

$$\begin{cases} \alpha^p \equiv \alpha \pmod{p}, & \beta^p \equiv \beta \pmod{p}, & \text{при } \left(\frac{D}{p}\right) = 1, \\ \alpha^p \equiv \beta \pmod{p}, & \beta^p \equiv \alpha \pmod{p}, & \text{при } \left(\frac{D}{p}\right) = -1. \end{cases}$$

Теперь вычислим значение  $U_{\Phi(p)}$ . При  $\left(\frac{D}{p}\right) = -1$  получаем  $\Phi(p) = p + 1$  и

$$U_{\Phi(p)} = \frac{1}{\alpha - \beta} (\alpha^{p+1} - \beta^{p+1}) \equiv \frac{1}{\alpha - \beta} (\beta\alpha - \alpha\beta) \equiv 0 \pmod{p}.$$

При  $\left(\frac{D}{p}\right) = 1$  получаем  $\Phi(p) = p - 1$  и

$$U_{\varphi(p)} = \frac{1}{\alpha - \beta} (\alpha^{p-1} - \beta^{p-1}) \equiv \frac{1}{\alpha - \beta} \left(\frac{\alpha}{\alpha} - \frac{\beta}{\beta}\right) \equiv 0 \pmod{p}.$$

Лемма доказана.  $\square$

Теперь сформулируем теорему, которая позволяет нам сделать вывод о строении простых делителей числа  $m$ , по известным делителям числа  $m + 1$ .

**Теорема 6.11** (Моррисон, 1975). Пусть  $m$  нечетное целое число. Представим  $m + 1$  в виде  $m + 1 = fr$ , где для числа  $f$  известно полное разложение на множители  $f = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ .

Пусть  $a, b$  произвольные целые числа такие, что  $\text{НОД}(a, b) = 1$ . Определим  $\{U_n\}$  последовательность Люка, зависящую от параметров  $a, b$ . Если для каждого делителя  $q_i$  числа  $f$  будут выполнены условия

1. Выполнено сравнение  $U_{m+1} \equiv 0 \pmod{m}$ .
2. Выполнено условие  $\text{НОД}\left(U_{\frac{m+1}{q_i}}, m\right) = 1, i = 1, \dots, s,$

то для каждого простого делителя  $p$  числа  $m$  такого, что  $\left(\frac{D}{p}\right) \neq 0$ , где  $D = a^2 - 4b$  и  $b \not\equiv 0 \pmod{p}$ , будет выполнено сравнение

$$p \equiv \left(\frac{D}{p}\right) \pmod{f}.$$

*Доказательство.* Пусть для простого делителя  $q_i$  числа  $f$  выполнено первое условие теоремы, тогда  $U_{m+1} \equiv 0 \pmod{m}$  и для любого простого делителя  $p$  числа  $m$  выполнено сравнение  $U_{m+1} \equiv 0 \pmod{p}$ . Пусть



$d$  минимальное целое число такое, что  $U_d \equiv 0 \pmod{p}$ , тогда, в силу леммы 6.8,  $d|m+1$ .

Из второго условия теоремы получаем, что  $U_{\frac{m+1}{q_i}} \not\equiv 0 \pmod{p}$ , следовательно,  $d \nmid \frac{m+1}{q_i}$ . Сравнивая два полученных утверждения получаем, что  $d|q_i^{\alpha_i}$ .

С другой стороны, согласно лемме 6.9 выполнено  $U_{\Phi(p)} \equiv 0 \pmod{p}$ . Воспользовавшись еще раз утверждением леммы 6.8, получаем условие  $d|\Phi(p)$ . Таким образом,  $d|\text{НОД}(q_i^{\alpha_i}, \Phi(p)) = q_i^{\alpha_i}$ . Последнее равенство выполнено в силу простоты  $q_i$ .

Мы получили, что  $q_i^{\alpha_i}|\Phi(p)$ , что равносильно  $\Phi(p) \equiv 0 \pmod{q_i^{\alpha_i}}$  или

$$p \equiv \left(\frac{D}{p}\right) \pmod{q_i^{\alpha_i}}.$$

Воспользовавшись китайской теоремой об остатках, мы получаем, что аналогичное сравнение выполнено и по модулю  $f$ . Теорема доказана.  $\square$

Эта теорема имеет очевидное следствие, которое позволяет сделать вывод о простоте числа  $m$ .

**Следствие 1.** Пусть для числа  $m$  выполнены утверждения теоремы 6.11 и выполнено неравенство  $(f-1)^2 > m$ . Тогда число  $m$  простое.

*Доказательство.* Предположим, что число  $m$  составное и, без ограничения общности, имеет два простых делителя  $p$  и  $q$ . Если для числа  $m$  выполнены условия теоремы 6.11, то  $p = \pm 1 + kf$ ,  $q = \pm 1 + lf$  для некоторых целых чисел  $k \geq 1$ ,  $l \geq 1$  и мы получаем, что  $m = pq > (f-1)^2 > m$ . Противоречие.  $\square$

Мы можем воспользоваться для доказательства простоты числа  $m$  приведенным следствием следующим образом. Пусть нам известно частичное разложение числа  $m+1 = fr$  на простые множители, где  $f = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ ,  $f^2 > m$ .

Выберем целые числа  $a, b$  такие, что выполнены условия

$$\text{НОД}(a, b) = 1, \quad \text{НОД}(m, b) = 1, \quad \text{НОД}(m, a^2 - 4b) = 1,$$

и проверим условия теоремы 6.11. Если они выполнены, то число  $m$  простое. Отметим, что нам достаточно вычислять элементы рекуррентной последовательности по модулю  $m$ , поскольку в этом случае необходимые нам свойства делимости сохраняются.

## 6.5 Алгоритмы построения простых чисел

Основываясь на изложенных выше идеях, приведем несколько алгоритмов построения простых чисел, которые используются при генерации параметров криптографических схем.

Мы начнем с описания простого алгоритма, который позволяет строить простые числа  $p$  с известным разложением  $p - 1$  на множители. Основная идея данного алгоритма заключается в поиске простых чисел в арифметических прогрессиях. Хорошо известен следующий результат.

**Теорема 6.12** (Дирихле, см. [3], гл. 3). *Пусть арифметическая прогрессия задана соотношением  $x_k = ak + b$ ,  $k = 0, 1, \dots$ , где параметры  $a, b$  натуральные, взаимно простые числа. Тогда среди чисел  $x_k$  бесконечно много простых.*

Как показывают практические вычисления, простые числа встречаются в арифметических прогрессиях достаточно часто. В комбинации с доказанными ранее результатами о простоте чисел, например, теоремами Поклингтона или Моррисона, мы получаем достаточно удобный инструмент для построения больших простых чисел.

### 6.5.1 Рекурсивный алгоритм построения простых по известному разложению $p - 1$

Многие математики предлагали различные варианты алгоритмов построения простых чисел, использующих поиск в арифметических прогрессиях. Среди отечественных ученых можно отметить Владимира Геннадьевича Антипкина и Юрия Валентиновича Нестеренко, среди зарубежных – Преду Михалеску (Preda Mihailescu), см. [36]. Все варианты, так или иначе, использовали для доказательства простоты числа  $p$  последовательность из трех шагов.

1. Проверку делимости числа  $p$  на маленькие простые числа,
2. Применение теста Миллера-Рабина, см. тест 6.3, для отбраковки составных чисел, имеющих большие простые делители,
3. Применение теоремы Лемера, см. теорему 6.6, для доказательства простоты числа  $p$ .

Мы опишем некоторый сводный вариант алгоритма, и будем искать простое число вида  $p = kq + 1$ , где  $q$  простое число, удовлетворяющее

неравенству  $q > \sqrt{p}$ , а  $k$  произвольное четное целое число. Мы будем считать, что нам заданы два натуральных числа  $A, B$  таких, что выполнено  $B > A + 1$ , и будем искать простое число  $p$ , удовлетворяющее неравенству

$$A < p < B. \quad (6.17)$$

Из неравенства (6.17) мы можем получить оценки на  $q$  и  $k$ . Действительно, поскольку  $q$  целое, удовлетворяющее неравенству  $q > \sqrt{p}$ , то из (6.17) следует оценка на  $q$  снизу

$$q \geq \left\lceil \sqrt{B} \right\rceil > \sqrt{p}.$$

Обозначим  $q_A = \left\lceil \sqrt{B} \right\rceil$  и ограничим простое число  $q$  сверху, то есть  $q_A \leq q \leq \alpha q_A$  для произвольного действительного числа  $\alpha > 1$ , тогда для  $k$  выполнены следующие оценки.

Если  $k < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$ , то выполнено

$$p = kq + 1 \leq k\alpha q_A + 1 < \alpha q_A \frac{B-1}{\alpha q_A} + 1 = B$$

и для  $p$  верна оценка сверху (6.17).

Аналогично, если  $k \geq \left\lceil \frac{A}{q_A} \right\rceil$ , то выполнено

$$p = kq + 1 > kq \geq kq_A \geq q_A \frac{A}{q_A} = A,$$

и для  $p$  верна оценка снизу (6.17). Исходя из того, что интервал для значений  $k$  не должен быть пустым, мы получаем оценку сверху на значение параметра  $\alpha$ . Действительно, из неравенства  $\left\lceil \frac{A}{q_A} \right\rceil < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$  получаем, что  $\alpha$  ограничено сверху величиной  $\frac{B-1}{A}$ , то есть принадлежит интервалу

$$1 < \alpha < \frac{B-1}{A}. \quad (6.18)$$

Указанный интервал не пуст, поскольку величина  $\frac{B-1}{A} > 1$  для всех натуральных значений  $A, B$  таких, что  $B > A + 1$ . В алгоритме мы будем использовать значение  $\alpha = \frac{B+A-1}{2A}$ , которое является серединой интервала (6.18).

Итак, мы будем искать простые числа в арифметической прогрессии  $p_k = kq + 1$ , перебирая все четные числа  $k$  в заданном интервале, последовательно увеличивая число  $k$  на двойку. Для отбраковки большей части

составных чисел мы будем использовать *пробное деление* на маленькие простые числа.

Для того чтобы оптимизировать данную процедуру, заметим следующий простой факт. Предположим, что мы разделили число  $p$  на маленькие простые числа  $d_1, \dots, d_n$  и нашли остатки от деления  $\delta_1, \dots, \delta_n$  такие, что  $p \equiv \delta_n \pmod{d_n}$ . Предположим, что найдется остаток  $\delta_i \equiv 0 \pmod{d_i}$ ,  $1 \leq i \leq n$ , тогда число  $p$  делится на  $d_i$  и является составным.

Для проверки следующего числа заметим, что  $p+2 \equiv \delta_i+2 \pmod{d_i}$  для всех  $i$ ,  $1 \leq i \leq n$ . Таким образом, мы можем найти остатки от деления следующего числа на маленькие простые без деления большого числа, а лишь изменяя остатки от деления предыдущего числа. На практике мы будем выбирать число  $n = 10$  и проверять делимость числа  $p$  на простые 3, 5, 7, 11, 13, 17, 19, 23, 29 и 31. Мы исключили из этого списка двойку, поскольку число  $p$  всегда нечетно.

Прежде чем приступить к описанию алгоритма, заметим, что нам потребуется таблица всех простых чисел, не превосходящих некоторой величины, скажем  $2^{16}$ . Построить эту таблицу можно, например, используя алгоритм 6.1.

### Алгоритм 6.6 (Алгоритм построения простого числа)

**Вход:** Натуральные числа  $A, B$  такие, что  $A+1 < B$ .

**Выход:** Простое число  $p$  такое, что  $2^A < p < 2^B$ .

1. Если  $B \leq 2^{16}$ , то выбрать случайным образом простое число  $p$  из таблицы простых чисел и завершить работу.
2. Определить переменные  $q_A = \lceil \sqrt{B} \rceil$ ,  $\alpha = \frac{B+A-1}{2A}$  и  $k_1 = \lceil \frac{A}{q_A} \rceil$ ,  $k_2 = \lfloor \frac{B-1}{q_A} \rfloor$ .
3. Определить  $k_n = k_2$ . Используя этот же алгоритм 6.6, построить простое число  $q$ , удовлетворяющее неравенствам  $q_A < q < \lfloor \alpha q_A \rfloor$ .
4. Выбрать случайное число  $k$  в интервале  $k_1 < k < k_n$ . Если  $k$  нечетно, то положить  $k = k - 1$ . Определить  $k_s = k_n$ ,  $k_n = k$  и целое число  $p = kq + 1$ .
5. Для простых чисел  $d_1 = 3, \dots, d_{10} = 31$  определить остатки  $\delta_1, \dots, \delta_{10}$  от деления числа  $p$  на простые  $d_1, \dots, d_{10}$ , то есть  $\delta_i \equiv p \pmod{d_i}$ ,  $1 \leq i \leq 10$ .
6. Вычислить  $k = k + 2$ ,  $p = p + 2q$  и  $\delta_i = \delta_i + 2 \pmod{d_i}$  для всех  $i$  таких, что  $1 \leq i \leq 10$ .
7. Если  $k > k_s$ , то вернуться на шаг 4.
8. Если найдется индекс  $i$ ,  $1 \leq i \leq 10$  и  $\delta_i = 0$ , то вернуться на шаг 6.
9. Применить к числу  $p$  тест Миллера-Рабина, см. тест 6.3. Если тест не пройден, то вернуться на шаг 6.
10. Определить значение счетчика  $c = 10$ .
11. Вычислить случайное целое число  $a$  и  $c = c - 1$ .
12. Если  $\text{НОД}(a^k - 1, p) = 1$  и  $a^{p-1} \equiv 1 \pmod{p}$ , то завершить алгоритм с уведомлением, что число  $p$  простое.
13. Если  $c = 0$ , то вернуться на шаг 6. Иначе, вернуться на шаг 11.

□

Как мы говорили выше, описанный алгоритм использует для доказательства простоты числа  $p$  утверждение теоремы Лемера, см. теорему 6.6. Вместе с тем, он может быть легко модифицирован таким образом, чтобы использовать утверждение теоремы 6.9.

Другой возможной модификацией данного алгоритма является использование теоремы Моррисона, см. теорему 6.11, и последовательностей Люка для доказательства простоты числа  $p$ . Детальную проработку этих модификаций мы оставляем читателю.

### 6.5.2 Алгоритм построения сильно простого числа

Во многих приложениях возникает необходимость строить простые числа с дополнительными условиями. Дадим следующее определение.

**Определение 6.4.** Мы будем называть нечетное простое число  $p$  *сильно простым*, если найдутся такие нечетные простые числа  $q$ ,  $s$  и  $r$  такие, что

$$p \equiv 1 \pmod{q}, \quad p \equiv -1 \pmod{s}, \quad q \equiv 1 \pmod{r}, \quad (6.19)$$

что равносильно равенствам

$$\begin{cases} p = kq + 1, \\ p = is - 1, \\ q = jr + 1, \end{cases}$$

для некоторых четных чисел  $i, j, k$ .

Поскольку предложенный нами ранее алгоритм 6.6 позволяет строить простые числа  $p$ , удовлетворяющие только первому и третьему из сравнений (6.19), то для построения строго простых чисел нам потребуется провести его некоторую модификацию.

В 1979 году Хью Вильямс (Hugh Williams) и Бренд Шмидт (Brend Schmid) в работе [55] предложили алгоритм, вариант которого мы приведем далее.

Предположим, что мы построили два простых числа  $r$ ,  $s$  и хотим построить оставшиеся два простых числа  $p$  и  $q$  так, чтобы выполнялись сравнения (6.19). Для этого зафиксируем целое число  $a \geq 1$ , определим наименьшее положительное целое число  $x$  такое, что  $x \equiv -\frac{(1+a)}{ar} \pmod{s}$ , и будем искать простое число  $q$  в арифметической прогрессии

$$q = (ks + x)r + 1, \quad k = 0, 1, \dots$$

Для поиска такого числа  $q$  можно организовать переборный алгоритм, аналогичный алгоритму 6.6. Тогда, если число  $p = 2aq + 1$  будет простым, мы найдем искомое строго простое число – это вытекает из сравнения

$$\begin{aligned} p = 2aq + 1 &= 2a((ks + x)r + 1) + 1 = \\ &= 2aksr + 2arx + (2a + 1) \equiv -1 \pmod{s}. \end{aligned}$$

Если  $r > \sqrt{q}$ , то мы можем воспользоваться теоремой Лемера для доказательства простоты как числа  $q$ , так и числа  $p$ .

Если  $a = 1$ , то простое число  $p$  удовлетворяет равенству  $p = 2q + 1$ . Простые числа  $p$  и  $q$ , удовлетворяющие этому равенству, называются *простыми-близнецами* и встречаются достаточно редко. Поэтому, при практических вычислениях, необходимо выбирать  $a$  достаточно большим.

Прежде чем приводить алгоритм построения сильно простого числа  $p$ , приведем оценки сверху и снизу на параметры, которые нам необходимо определить. Как и раньше, мы будем строить простое число  $p$ , удовлетворяющее неравенству

$$A < p < B, \quad \text{тогда} \quad q_A = \left\lceil \frac{A-1}{2a} \right\rceil \leq q = \frac{p-1}{2a} \leq \left\lfloor \frac{B-1}{2a} \right\rfloor = q_B,$$

для некоторых целых  $A, B$  таких, что  $B > A + 2a$ . Заметим, что для выполнения условий теоремы Лемера, при доказательстве простоты  $p$ , нам необходимо выполнение условия  $q > \sqrt{p}$ . Так мы получаем оценку на  $a$  сверху, а именно

$$\frac{B-1}{2\sqrt{A}} > \frac{p-1}{2q} = a.$$

Теперь, как и в предыдущем алгоритме, получим оценки на  $r$ . Для выполнимости условий теоремы Лемера и доказательства простоты  $q$ , положим

$$r \geq \lceil \sqrt{q_A} \rceil = r_A,$$

тогда  $\lfloor \alpha r_A \rfloor \geq r \geq r_A$  для некоторого действительного параметра  $\alpha > 1$ .

Если  $ks + x \leq \left\lfloor \frac{q_B-1}{\alpha r_A} \right\rfloor$ , тогда выполнена оценка сверху

$$q = (ks + x)r + 1 < \frac{q_B-1}{\alpha r_A} \alpha r_A + 1 \leq q_B.$$

Аналогично, если  $ks + x \geq \left\lceil \frac{q_A}{r_A} \right\rceil$ , то выполнена оценка снизу

$$q = (ks + x)r + 1 \geq \frac{q_A}{r_A} r_A + 1 > q_A.$$

Таким образом, мы получили ограничения сверху и снизу на размер перебираемого параметра  $k$

$$\left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor \geq (ks + x) \geq \left\lceil \frac{q_A}{r_A} \right\rceil. \quad (6.20)$$

Исходя из того, что перебираемый интервал не должен быть пустым, мы получим оценку сверху на параметр  $\alpha$ . Действительно, указанный интервал не пуст при  $\alpha < \frac{q_B - 1}{q_A} < \frac{B - 2a}{A}$ . При практических вычислениях мы будем использовать значение  $\alpha = \frac{q_B + q_A - 1}{2q_A}$ .

Исходя из неравенства (6.20), получаем оценки для  $k$

$$\left\lfloor \frac{q_B - 1}{\alpha s r_A} \right\rfloor - x \geq k \geq \left\lceil \frac{q_A}{s r_A} \right\rceil - x,$$

а также оценку на  $s$  сверху. Поскольку, в силу построения,  $s > x > 0$  и  $k \geq 1$ , то мы получаем неравенство

$$\frac{q_B - 1}{\alpha r_A} \geq \left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor \geq (k + 1)s > ks + x,$$

откуда следует неравенство  $s < \left\lfloor \frac{q_B - 1}{2\alpha r_A} \right\rfloor = s_A$ , которое мы будем использовать для верхней оценки  $s$ . Для нижней оценки будем использовать величину<sup>1</sup>  $\lceil \sqrt{s_A} \rceil$ .

### Алгоритм 6.7 (Алгоритм построения сильно простого числа)

**Вход:** Натуральные числа  $A, B$  такие, что  $A + 2 < B$ .

**Выход:** Сильно простое число  $p$  такое, что  $A < p < B$ .

1. Вычислить случайное натуральное число  $a$  такое, что  $1 \leq a \leq \left\lfloor \frac{B-1}{2\sqrt{A}} \right\rfloor$ .
2. Определить  $q_A = \left\lceil \frac{A-1}{2a} \right\rceil$ ,  $q_B = \left\lfloor \frac{B-1}{2a} \right\rfloor$ ,  $r_A = \lceil \sqrt{q_A} \rceil$ ,  $\alpha = \frac{q_B + q_A - 1}{2q_A}$  и  $s_A = \left\lfloor \frac{q_B - 1}{2\alpha r_A} \right\rfloor$ .
3. Используя алгоритм 6.6, вычислить простое число  $r$ , удовлетворяющее неравенствам  $r_A < r < \lfloor \alpha r_A \rfloor$ .
4. Используя алгоритм 6.6, вычислить простое число  $s$ , удовлетворяющее неравенствам  $\lceil \sqrt{s_A} \rceil < s < s_A$ .
5. Вычислить наименьшее положительное целое число  $x$ , удовлетворяющее сравнению  $x \equiv -\frac{(1+a)}{ar} \pmod{s}$ .
6. Определить  $k_2 = \left\lfloor \frac{q_B - 1}{\alpha s r_A} \right\rfloor - x$  и  $k_1 = \left\lceil \frac{q_A}{s r_A} \right\rceil - x$ .
7. Вычислить случайное число  $k$ ,  $k_1 \leq k \leq k_2$ .
8. Если  $x$  - четно и  $k$  - четно, то положить  $k = k + 1$  и перейти к шагу 10.
9. Если  $x$  - нечетно и  $k$  - нечетно, то положить  $k = k + 1$ .

<sup>1</sup>Нижняя граница для числа  $s$  определяется исходя из криптографических требований к конкретной системе защиты информации.

10. Определить  $q = (ks + x)r + 1$  и  $p = 2aq + 1$ .
11. Вычислить  $k = k + 2$ ,  $q = q + 2sr$  и  $p = p + 4asr$ .
12. Если  $k > k_2$ , то вернуться на шаг 3.
13. Применить к числу  $q$  тест Миллера-Рабина, см. тест 6.3. Если тест не пройден, то вернуться на шаг 11.
14. Применить к числу  $p$  тест Миллера-Рабина, см. тест 6.3. Если тест не пройден, то вернуться на шаг 11.
15. Определить значение счетчика  $n = 10$ .
16. Вычислить случайное целое число  $a$  и  $n = n - 1$ .
17. Если  $\text{НОД}(a^{ks+x} - 1, q) = 1$  и  $a^{q-1} \equiv 1 \pmod{q}$ , то перейти к шагу 19.
18. Если  $n = 0$ , то вернуться на шаг 11. Иначе, вернуться на шаг 16.
19. Определить значение счетчика  $n = 10$ .
20. Вычислить случайное целое число  $a$  и  $n = n - 1$ .
21. Если  $\text{НОД}(a^q - 1, p) = 1$  и  $a^{p-1} \equiv 1 \pmod{p}$ , то завершить алгоритм с уведомлением, что сильно простое число  $p$  построено.
22. Если  $n = 0$ , то вернуться на шаг 11. Иначе, вернуться на шаг 20. □

Приведенный алгоритм имеет высокую трудоемкость и при практической реализации на ЭВМ может занимать достаточно много времени. В 1984 году Джон Гордон (John Gordon) в работе [26] предложил другой способ построения сильно простых чисел. Он основан на следующей лемме.

**Лемма 6.10** (Гордон). *Простое число  $p > 2$  является сильно простым и удовлетворяет сравнениям (6.19), тогда и только тогда, когда  $p$  имеет вид  $p = u + 2kqs$ , для натурального  $k$  и*

$$u = \begin{cases} w, & \text{если } w - \text{нечетно,} \\ w + qs, & \text{если } w - \text{четно,} \end{cases}$$

где  $u \equiv s^{q-1} - q^{s-1} \pmod{qs}$ .

*Доказательство.* Пусть  $p = u + 2kqs$ , для некоторого натурального  $k$ , тогда, в силу малой теоремы Ферма,

$$p \equiv u \equiv -q^{s-1} \equiv -1 \pmod{s}, \quad \text{и} \quad p \equiv u \equiv s^{q-1} \equiv 1 \pmod{q},$$

и сравнения (6.19) выполнены, если простое число  $q$  имеет большой простой делитель  $r$ .

Пусть  $\pi$  сильно простое число, не удовлетворяющее условиям леммы. В силу сравнений (6.19)  $\pi - p \equiv 1 - 1 \equiv 0 \pmod{q}$  и  $\pi - p \equiv -1 - (-1) \equiv 0 \pmod{s}$ , следовательно,  $\pi \equiv p \pmod{qs}$ . Тогда  $\pi \equiv w \pmod{rs}$  и имеет вид  $\pi = u + 2kqs$  для некоторого натурального числа  $k$ . Лемма доказана. □



Предложенный Гордоном алгоритм основывался на данной лемме и состоял из следующей последовательности действий. Вначале необходимо построить простые числа  $q, s, r$ , например, с использованием алгоритма 6.6, изложенного нами ранее. Далее, число  $p$  необходимо искать в арифметической прогрессии  $p = u + 2kqs$ . Для отсева составных чисел можно использовать тест Миллера-Рабина. Для доказательства простоты необходимо использовать алгоритмы доказательства простоты чисел произвольного вида.

## ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ

Метод пробного деления - Метод Ферма - Метод Лемана - Метод Полларда - Метод Брента -  $p - 1$  метод Полларда -  $p + 1$  метод Вильямса - Оптимизация методов Полларда и Вильямса.

Рассмотрим элементарные методы разложения составного числа  $m$  на множители. Эти методы достаточно просты для изложения, но имеют высокую трудоемкость, что не позволяет их использовать для разложения чисел, используемых на практике. Тем не менее, излагаемые алгоритмы могут быть использованы в качестве составных частей в более сложных алгоритмах.

На протяжении всей главы мы будем считать, что  $m > 0$  нечетное, составное число. Вопрос о том, как определить: является ли число  $m$  составным или простым, мы рассматривали в предыдущей главе.

Напомним, что под задачей факторизации мы подразумеваем нахождение таких простых чисел  $p_1, \dots, p_k$ , что число  $m$  может быть единственным образом представлено в виде произведения

$$m = \prod_{i=1}^k p_i^{\alpha_i} = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

где  $\alpha_i$  натуральные числа. Такое представление, в силу основной теоремы арифметики, см. теорему 1.4, существует и единственно.

Для поиска всех простых делителей числа  $m$  нам необходимо найти два делителя числа  $m$ , быть может, и не простых, а потом применить процедуру поиска делителей к каждому из найденных делителей. Далее мы будем описывать алгоритмы предполагая, что нам достаточно найти два произвольных делителя числа  $m$ .

### 7.1 Метод пробного деления

Метод пробного деления является самым простым и очевидным алгоритмом поиска делителей числа  $m$ . Метод заключается в последовательном делении числа  $m$  на числа, не превосходящие величины  $\lceil \sqrt{m} \rceil$ . Такая оценка сверху верна в силу леммы 1.6, из которой следует, что любой простой делитель  $p$  числа  $m$  удовлетворяет неравенству  $p \leq \sqrt{m}$ .

С теоретической точки зрения, достаточно делить число  $m$  только на простые числа. Однако для этого необходимо иметь заранее подготовленную таблицу всех простых чисел от 2 до  $\lceil \sqrt{m} \rceil$  включительно. Данная

таблица может быть построена с помощью алгоритма 6.1, приведенного нами ранее. Однако при больших значениях числа  $m$  такая таблица занимала бы в ЭВМ слишком много памяти.

На практике вырабатывается таблица простых в небольшом диапазоне, например до  $2^{16}$ , и проверка проводится только для маленьких чисел. Поиск больших делителей выполняется другими алгоритмами.

## 7.2 Метод Ферма

Авторство метода, который мы излагаем далее, приписывается известному математику Пьеру Ферма (Pierre de Fermat). Он заметил, что составное число всегда может быть представлено в виде разности двух квадратов и предложил, основанный на этом наблюдении, простой способ поиска делителей.

Пусть  $m = pq$ , где  $p, q$  натуральные, не обязательно простые, делители числа  $m$ , и  $p > q$ . Тогда

$$m = x^2 - y^2, \quad \text{где} \quad x = \frac{p+q}{2}, \quad y = \frac{p-q}{2}. \quad (7.1)$$

Метод Ферма разложения на множители заключается в переборе всех возможных значений величины  $x$  и проверке: является ли число  $m - x^2$  полным квадратом. Если это условие выполнено, то делители  $p, q$  удовлетворяют равенствам  $p = x + y$ ,  $q = x - y$ .

### Алгоритм 7.1 (Алгоритм факторизации Ферма)

**Вход:** Целое составное число  $m > 0$ .

**Выход:** Натуральный делитель  $p > 1$  числа  $m$ .

1. Вычислить наименьшее целое число  $h$  такое, что  $h^2 \geq \sqrt{m}$ , то есть  $h = \lceil \sqrt{m} \rceil$ .
2. Если  $h^2 = m$ , то определить  $p = h$  и завершить алгоритм.
3. Определить  $x = h$ ,  $v = x^2 - m$  и счетчик  $k = 0$ .
4. Пока  $k > 0$  выполнить



4.1. Если величина  $v$  является полным квадратом, то определить  $y = \sqrt{v}$ ,  $p = x + y$  и закончить алгоритм.

4.2. Вычислить  $k = k + 1$ ,  $x = x + 1$  и  $v = v + 2h + 1$ .

□

Легко показать, что количество проверок числа  $v$  (количество повторений на четвертом шаге алгоритма) не превосходит величины  $y = \frac{p-q}{2}$ . Поскольку выполнено неравенство  $p > h > q$ , мы можем оценить величину  $k$  следующим образом. Согласно шагу 4.2 приведенного алгоритма, в

момент нахождения делителя выполнено равенство  $x = h + k$ , получаем

$$k = x - h = p - y - h < p - q - y = \frac{p - q}{2}.$$

Далее мы рассмотрим несколько вопросов, которые влияют на быстроедействие алгоритма Ферма при его практической реализации на ЭВМ.

### 7.2.1 Вычисление квадратного корня

На первом шаге, а также при проверке, является ли число  $v$  квадратом, необходимо вычислять квадратный корень из большого целого числа. Для реализации этой операции мы можем использовать арифметику большой точности для действительных чисел и вычислять действительный корень, например, с помощью алгоритма Ньютона. Эта достаточно медленная операция может быть заменена аналогичным алгоритмом, использующим вычисления только с целыми числами и вычисляющим такое целое число  $h$ , что  $h^2 \leq m < (h + 1)^2$ , то есть  $h = \lfloor \sqrt{m} \rfloor$ .

#### Алгоритм 7.2 (Вычисление целозначного квадратного корня)

**Вход:** Натуральное число  $m > 0$ .

**Выход:** Натуральное число  $h$ , удовлетворяющее неравенствам  $h^2 \leq m < (h + 1)^2$ .

1. Определить  $x = m$ .
2. Вычислить<sup>1</sup>  $y = \left\lfloor \frac{x + \lfloor \frac{m}{x} \rfloor}{2} \right\rfloor$ .
3. Если  $y < x$ , то положить  $x = y$  и вернуться на шаг 2. В противном случае, положить  $h = x$  и завершить алгоритм.  $\square$

Докажем, что приведенный алгоритм действительно находит целое число  $h$  такое, что  $h = \lfloor \sqrt{m} \rfloor$ . Для начала отметим, что для любого значения  $x > 0$  выполнено неравенство

$$\frac{x + \frac{m}{x}}{2} > \sqrt{m}, \quad \text{при } m > 0. \quad (7.2)$$

Действительно, из неравенства  $(x^2 - m)^2 > 0$  следует, что

$$x^4 - 2x^2m + m^2 > 0 \quad \text{или} \quad x^4 + 2x^2m + m^2 > 4x^2m,$$

тогда  $(x^2 + m)^2 > 4x^2m$  или  $x^2 + m > 2x\sqrt{m}$ . Последнее неравенство равносильно (7.2).

<sup>1</sup>При программировании на ЭВМ операцию деления на двойку целесообразно реализовывать как операцию сдвига.

Таким образом, мы получаем, что на каждом шаге алгоритма 7.2 для неизвестного  $x$  выполнено неравенство  $x \geq h$ . В силу условия на третьем шаге алгоритма мы получаем, что последовательность значений  $x$  убывает. Покажем, что алгоритм остановится только при выполнении условия  $x = h$ .

Предположим, что это не так. Тогда выполнены неравенства  $y \geq x$ ,  $x > h$  и

$$y - x = \left\lfloor \frac{x + \lfloor \frac{m}{x} \rfloor}{2} \right\rfloor - x = \left\lfloor \frac{\lfloor \frac{m}{x} \rfloor - x}{2} \right\rfloor = \left\lfloor \frac{m - x^2}{2x} \right\rfloor.$$

Поскольку  $x > h$  и  $x$  целое число, то  $x^2 > h^2 \geq m$ , следовательно,  $m - x^2 < 0$  и  $y - x < 0$ . Таким образом, мы получили противоречие нашему предположению  $y \geq x$ .

### 7.2.2 Как быстро проверить, что число является полным квадратом

Сделаем еще одно замечание, касающееся вопроса о проверке: является ли целое число  $v$ , вырабатываемое в алгоритме Ферма, полным квадратом. Для предварительного отсева, перед использованием алгоритма 7.2, можно воспользоваться следующим утверждением.

**Теорема 7.1.** *Целое число  $v > 0$  является полным квадратом тогда и только тогда, когда число  $v$  является квадратичным вычетом по модулю любого нечетного простого числа  $p$ .*

Прежде чем переходить к доказательству теоремы, нам потребуется следующая лемма.

**Лемма 7.1.** *Пусть  $q_1, \dots, q_r$  различные нечетные простые числа,  $\varepsilon_1, \dots, \varepsilon_r$  набор знаков, принимающих значения  $\pm 1$ . Тогда существует бесконечно много простых чисел  $p$  таких, что выполнены равенства*

$$\left( \frac{p}{q_1} \right) = \varepsilon_1, \dots, \left( \frac{p}{q_r} \right) = \varepsilon_r,$$

где  $\left( \frac{p}{q_i} \right)$  – символ Лежандра для всех  $i = 1, \dots, r$ .

*Доказательство.* Для любого индекса  $i = 1, \dots, r$  найдется некоторое натуральное число  $b_i$ ,  $0 < b_i < q_i$ , удовлетворяющее условию  $\left( \frac{b_i}{q_i} \right) = \varepsilon_i$ . Заметим, что в силу леммы 4.2, таких чисел будет ровно  $\frac{q_i-1}{2}$ .

Рассмотрим систему сравнений

$$\{x \equiv b_i \pmod{q_i} \quad i = 1, \dots, r. \quad (7.3)$$

Поскольку числа  $q_1, \dots, q_r$  взаимно просты, то используя китайскую теорему об остатках, см. теорему 2.3, получим, что существует целое число  $x_0$ , для которого система (7.3) эквивалентна сравнению

$$x \equiv x_0 \pmod{q_1 \cdots q_r}.$$

Воспользуемся утверждением теоремы Дирихле, см. теорему 6.12, из которого следует, что в арифметической последовательности

$$x_k = kq_1 \cdots q_r + x_0$$

найдется бесконечно много простых чисел  $p$ , удовлетворяющих сравнению  $p \equiv x_0 \pmod{q_1 \cdots q_r}$ .

Для каждого такого простого числа, используя свойства символа Лежандра, см. лемму 4.3, получаем равенства

$$\left(\frac{p}{q_i}\right) = \left(\frac{x_0}{q_i}\right) = \left(\frac{b_i}{q_i}\right) = \varepsilon_i, \quad i = 1, \dots, r,$$

из которых вытекает утверждение леммы. □

*Доказательство теоремы 7.1.* Если число  $v$  является полным квадратом, то утверждение теоремы очевидно, в силу определения квадратичного вычета. Теперь предположим, что число  $v$  не является полным квадратом и покажем, что в этом случае существует бесконечное число простых чисел  $p$ , для которых  $v$  не является квадратичным вычетом.

Прежде всего заметим, что если  $v = ab^2$ , то любого нечетного простого  $p$  выполнено равенство  $\left(\frac{v}{p}\right) = \left(\frac{a}{p}\right)$  и нам достаточно рассматривать числа  $v$ , которые раскладываются в произведение простых чисел в первой степени, то есть  $v = 2q_1 \cdots q_r$ , где  $q_1, \dots, q_r$  различные нечетные простые.

Зафиксируем некоторый набор знаков  $\varepsilon_1, \dots, \varepsilon_r$ , принимающих значения  $\pm 1$ , такой, что число значений  $-1$  в нем нечетное количество. Согласно доказанной нами лемме, найдется бесконечное множество простых чисел  $p$  таких, что  $p \equiv x_0 \pmod{q_1 \cdots q_r}$  и

$$\left(\frac{p}{q_i}\right) = \left(\frac{x_0}{q_i}\right) = \left(\frac{b_i}{q_i}\right) = \varepsilon_i, \quad i = 1, \dots, r.$$

Выберем из этого множества простые числа, удовлетворяющие условию  $p \equiv 1 \pmod{8}$ . Согласно теореме Дирихле, их также бесконечно много, поскольку они принадлежат арифметической прогрессии  $x_0 + k8q_1 \cdots q_r$ . Тогда числа  $\frac{p-1}{2}$  и  $\frac{p^2-1}{8}$  четные и выполнено равенство

$$\left(\frac{v}{p}\right) = \left(\frac{2}{p}\right) \prod_{i=1}^r \left(\frac{q_i}{p}\right) = (-1)^{\frac{p^2-1}{8}} \prod_{i=1}^r \left(\frac{p}{q_i}\right) (-1)^{\frac{p-1}{2} \frac{q_i-1}{2}} = \prod_{i=1}^r \varepsilon_i = -1,$$

то есть число  $v$  является квадратичным невычетом. Теорема доказана.  $\square$

Из утверждения теоремы следует, что мы можем реализовать следующую процедуру проверки чисел  $v$ . Вначале мы проверяем выполнение утверждения теоремы для некоторого заранее выбранного множества простых, а после, в случае если  $v$  окажется квадратичным вычетом по модулю этих простых, с помощью алгоритма 7.2 вычисляем целочисленный квадратный корень.

Заметим, что для проверки утверждения теоремы 7.1 необязательно вычислять символ Лежандра. Можно заранее для каждого простого числа  $p$  определить множество чисел на интервале  $1, \dots, p-1$ , являющихся квадратичными вычетами по модулю  $p$  и проверять, принадлежит ли  $v \pmod{p}$  этому множеству.

Можно оценить эффективность данной процедуры по отбраковке чисел, не являющихся полными квадратами. Докажем следующую теорему.

**Теорема 7.2.** Пусть  $v$  натуральное число, которое не является полным квадратом. Тогда не менее чем для половины нечетных простых чисел  $p$  будет выполнено условие  $\left(\frac{v}{p}\right) = -1$ .

*Доказательство.* Пусть, как и в предыдущей теореме, число  $v$  раскладывается в произведение  $v = 2q_1 \cdots q_r$ , где  $q_1, \dots, q_r$  различные нечетные простые. Пусть  $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$  знаки  $\pm 1$ , которые соответствуют символам Лежандра, то есть

$$\left(\frac{2}{p}\right) = \varepsilon_0, \quad \left(\frac{q_1}{p}\right) = \varepsilon_1, \quad \dots, \quad \left(\frac{q_r}{p}\right) = \varepsilon_r$$

для некоторого простого числа  $p$  и  $\left(\frac{v}{p}\right) = \prod_{i=0}^r \varepsilon_i$ .

Простые числа  $p$ , для которых выполнено условие  $\left(\frac{v}{p}\right) = -1$ , принадлежат бесконечной арифметической прогрессии  $\{x_0 + k8q_1 \cdots q_r\}$ , где

$k = 0, 1, \dots$ , для некоторого целого  $x_0$ , взаимно простого с  $8q_1 \cdots q_r$ . Количество таких прогрессий ограничено и равно

$$\varphi(8q_1 \cdots q_r) = 4 \prod_{i=1}^r (q_i - 1),$$

где  $\varphi(\cdot)$  – функция Эйлера.

Покажем, что число прогрессий, при которых значение символа Лежандра  $\left(\frac{v}{p}\right) = -1$  совпадает с числом прогрессий, при которых  $\left(\frac{v}{p}\right) = 1$ .

Значение величины  $x_0$ , как следует из доказательства предыдущей теоремы, определяется как решение системы сравнений

$$\begin{cases} x \equiv b_0 \pmod{8}, \\ x \equiv b_i \pmod{q_i}, \quad i = 1, \dots, r, \end{cases} \quad (7.4)$$

где величины  $b_i$  определяют знак символов Лежандра  $\left(\frac{2}{p}\right)$  и  $\left(\frac{q_i}{p}\right)$ , для  $i = 1, \dots, r$ . При этом ровно половина чисел из интервала  $0 < b_i < q_i$  соответствует знаку  $\varepsilon_i = 1$ , а другая половина – знаку  $\varepsilon_i = -1$ . Отметим, что  $b_i \neq 0$ , поскольку в этом случае решение системы (7.4) кратно  $q_i$  и не может являться простым числом.

Для случая двойки, аналогично, два значения 1, 7 соответствуют знаку  $\varepsilon_0 = 1$  и два значения 3, 5 – знаку  $\varepsilon_0 = -1$ . Таким образом, для любого набора знаков  $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$  ровно половина значений  $x_0$  таких, что  $0 < x_0 < 8q_1 \cdots q_r$ ,  $\text{НОД}(x_0, 8q_1 \cdots q_r) = 1$ , позволит нам определить последовательность простых чисел, для которой символ Лежандра  $\left(\frac{v}{p}\right) = -1$ . Соответственно, другая половина таких чисел даст нам последовательность, для которой символ Лежандра  $\left(\frac{v}{p}\right) = 1$ . Теорема доказана<sup>2</sup>.  $\square$

Из доказанной теоремы следует, что в случае, если число  $v$  не является полным квадратом, то вероятность его отбраковки составляет  $\frac{1}{2}$ . Более того, если мы получим, что символ Лежандра  $\left(\frac{v}{p}\right) = 1$  для  $k$  различных простых чисел, то вероятность того, что число  $v$  является полным квадратом близка к единице и равна  $1 - \frac{1}{2^k}$ .

<sup>2</sup>Собственно говоря, мы доказали более слабый результат о совпадении числа последовательностей, которые содержат простые числа, по модулю которых  $v$  является квадратичным вычетом или невычетом. С другой стороны, поскольку простые числа распределены в арифметических последовательностях равномерно, см. монографию [12, §7, гл.4], из этого следует утверждение теоремы.



## 7.3 Метод Лемана

В настоящее время алгоритм Шермана Лемана (R. Sherman Lehman) носит число исторический интерес и, как правило, не используется на практике. Вместе с тем, он был первым детерминированным алгоритмом факторизации целых чисел, имеющим оценку сложности меньшую, чем корневая от величины раскладываемого на множители числа. Впервые метод был описан в 1974 году в работе [32].

Метод Лемана развивает идеи, заложенные в алгоритме Ферма и ищет делители числа  $m$ , используя равенство

$$x^2 - y^2 = 4bt, \quad (7.5)$$

для некоторого целого числа  $b$ . Он основан на следующей теореме.

**Теорема 7.3.** Пусть  $m = pq$  составное число, являющееся произведением двух нечетных взаимно простых чисел, удовлетворяющих неравенствам  $\sqrt[3]{m} < p < q < \sqrt[3]{m^2}$ . Тогда найдутся натуральные числа  $x$ ,  $y$  и  $b \geq 1$ , удовлетворяющие следующим условиям.

1. Выполнено равенство  $x^2 - y^2 = 4bt$  при  $b < \sqrt[3]{m}$ .
2. Выполнено неравенство  $0 \leq x - \lfloor \sqrt{4bt} \rfloor < \frac{\sqrt[6]{m}}{4\sqrt{b}} + 1$ .

Вначале докажем следующую лемму.

**Лемма 7.2.** Пусть выполнены условия теоремы 7.3. Тогда найдутся натуральные числа  $r$ ,  $s$  такие, что

$$rs < \sqrt[3]{m} \quad \text{и} \quad |pr - qs| < \sqrt[3]{m}.$$

*Доказательство.* Для доказательства леммы разложим рациональное число  $\frac{q}{p}$  в непрерывную дробь. Символами  $\frac{P_n}{Q_n}$  мы будем обозначать подходящие дроби к  $\frac{q}{p}$ . В силу леммы 5.1 число подходящих дробей конечно и  $\frac{P_t}{Q_t} = \frac{q}{p}$  для некоторого индекса  $t$ .

Согласно определению подходящей дроби и ограничениям на числа  $p$ ,  $q$  получаем, что

$$P_0 = \left\lfloor \frac{q}{p} \right\rfloor < \frac{q}{p} < \frac{\sqrt[3]{m^2}}{\sqrt[3]{m}} = \sqrt[3]{m}, \quad Q_0 = 1,$$

то есть выполнено неравенство  $P_0Q_0 < \sqrt[3]{m}$ . С другой стороны,  $P_tQ_t = pq > p > \sqrt[3]{m}$ . Следовательно, найдется максимальный индекс  $n$  такой, что

$$P_nQ_n < \sqrt[3]{m}, \quad P_{n+1}Q_{n+1} > \sqrt[3]{m}, \quad 0 \leq n < t. \quad (7.6)$$

Определим в качестве исходных значений  $r = P_n$ ,  $s = Q_n$  и покажем, что они удовлетворяют утверждению леммы.

Первое неравенство очевидным образом выполняется в силу выбора значений  $r, s$ . Для доказательства второго неравенства рассмотрим два случая. Вначале предположим, что выполнено неравенство  $\frac{q}{p} \geq \frac{P_{n+1}}{Q_{n+1}}$ , которое может быть переписано в виде

$$\frac{p}{Q_{n+1}} \leq \frac{q}{P_{n+1}}. \quad (7.7)$$

Воспользовавшись равенством (5.13), получим, что

$$\left| \frac{q}{p} - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n Q_{n+1}}, \quad (7.8)$$

тогда, учитывая (7.6), (7.7) и (7.8), получим

$$\begin{aligned} |pr - qs| &= |pP_n - qQ_n| = pQ_n \left| \frac{q}{p} - \frac{P_n}{Q_n} \right| \leq \frac{p}{Q_{n+1}} = \\ &= \sqrt{\frac{p}{Q_{n+1}}} \sqrt{\frac{p}{Q_{n+1}}} \leq \sqrt{\frac{p}{Q_{n+1}}} \sqrt{\frac{q}{P_{n+1}}} = \sqrt{\frac{m}{P_{n+1}Q_{n+1}}} < \\ &< \frac{\sqrt{m}}{\sqrt[6]{m}} = \sqrt[3]{m}. \end{aligned}$$

Рассмотрим второй случай, при котором выполнены неравенства

$$\frac{P_{n+1}}{Q_{n+1}} > \frac{q}{p} > \frac{P_n}{Q_n}. \quad (7.9)$$

Тогда, переворачивая данное неравенство и учитывая утверждение леммы 5.3, получаем

$$\frac{Q_n}{P_n} - \frac{p}{q} < \frac{Q_n}{P_n} - \frac{Q_{n+1}}{P_{n+1}} = \frac{(-1)^{n+1}}{P_n P_{n+1}}. \quad (7.10)$$

Кроме того, из (7.9) следует неравенство  $pP_{n+1} > qQ_{n+1}$  или

$$\frac{p}{Q_{n+1}} > \frac{q}{P_{n+1}}. \quad (7.11)$$

Теперь, учитывая (7.6), (7.10) и (7.11), получим

$$\begin{aligned} |pr - qs| &= |pP_n - qQ_n| = qP_n \left| \frac{p}{q} - \frac{Q_n}{P_n} \right| < \frac{q}{P_{n+1}} = \\ &= \sqrt{\frac{q}{P_{n+1}}} \sqrt{\frac{q}{P_{n+1}}} < \sqrt{\frac{q}{P_{n+1}}} \sqrt{\frac{p}{Q_{n+1}}} = \sqrt{\frac{m}{P_{n+1}Q_{n+1}}} < \\ &< \frac{\sqrt{m}}{\sqrt[6]{m}} = \sqrt[3]{m}. \end{aligned}$$

Лемма доказана.  $\square$

*Доказательство теоремы 7.3.* Пусть  $p, q$  нечетные делители числа  $m$ . Определим числа  $x = pr + qs$  и  $y = pr - qs$ , где  $r, s$  удовлетворяют утверждению леммы 7.2, тогда выполнено равенство

$$x^2 - y^2 = (pr + qs)^2 - (pr - qs)^2 = 4rspq = 4bm,$$

где  $b = rs$ . В силу леммы 7.2, целое число  $b$  удовлетворяет неравенству  $b < \sqrt[3]{m}$ , а кроме того,  $y < \sqrt[3]{m}$ . Первое утверждение теоремы выполнено.

Для доказательства второго утверждения определим целое число  $k$  равенством

$$k = x - \lfloor \sqrt{4bm} \rfloor = pr + qs - \lfloor \sqrt{4bm} \rfloor$$

и покажем, что оно удовлетворяет заданному ограничению.

Вначале заметим, что поскольку  $x^2 = 4bm + y^2$ , то  $x \geq \sqrt{4bm}$  и величина  $k \geq 0$ . Далее, используя оценку сверху на величину  $y$ , получаем

$$\begin{aligned} (\sqrt[3]{m})^2 &> y^2 = x^2 - 4bm = \\ &= (pr + qs + \sqrt{4bm})(pr + qs - \sqrt{4bm}) \geq \\ &\geq 2\sqrt{4bm}(pr + qs - \sqrt{4bm}) \geq 2\sqrt{4bm}(k - 1). \end{aligned}$$

Тогда выполнено

$$k < \frac{(\sqrt[3]{m})^2}{2\sqrt{4bm}} + 1 = \frac{\sqrt[6]{m}}{4\sqrt{b}} + 1.$$

Теорема доказана. □

Используя утверждения доказанной нами теоремы, Леман предложил следующий алгоритм поиска делителей числа  $m$ .

### Алгоритм 7.3 (Алгоритм Лемана)

**Вход:** Натуральное нечетное число  $m$ .

**Выход:** Простое число  $p$  такое, что  $p|m$ , либо заключение о том, что число  $m$  простое.

**1. Для всех  $p$  от 2 до  $\lceil \sqrt[3]{m} \rceil$  выполнить**

**1.1. Если  $m \equiv 0 \pmod{p}$ , то вернуть  $p$  в качестве делителя числа  $m$  и завершить алгоритм.**

**2. Для всех  $b$  от 1 до  $\lfloor \sqrt[3]{m} \rfloor$  выполнить**

**2.1. Определить  $k = 0$  и  $D = \left\lfloor \frac{\sqrt[6]{m}}{4\sqrt{b}} \right\rfloor + 1$ .**

**2.2. Определить  $x = \lfloor \sqrt{4bm} \rfloor + k$  и  $v = x^2 - 4bm$ .**

**2.3. Если  $v$  является полным квадратом<sup>3</sup>, то определить**

$$p = \text{НОД}(m, x \pm \sqrt{v})$$

**и завершить алгоритм.**

---

<sup>3</sup>Очевидно, что проверку можно производить используя методы, описанные нами ранее в разделах 7.2.1 и 7.2.2.

**2.4.** Определить  $k = k + 1$ .

**2.5.** Если  $k \geq D$ , то вычислить новое значение  $d$ . В противном случае, вернуться на шаг 2.2.

**3.** Завершить алгоритм с уведомлением, что число  $m$  простое.  $\square$

Описанный нами алгоритм сперва проверяет, имеет ли число  $m$  простые делители, не превосходящие величины  $\lceil \sqrt[3]{m} \rceil$ , а потом устраивает перебор значений  $b$  и  $k$  для проверки выполнимости утверждений теоремы 7.3. В случае, если искомые значения  $x, y$  не найдены, мы получаем, что число  $m$  простое. Таким образом, приведенный алгоритм может рассматриваться как тест числа  $m$  на простоту. Алгоритм, очевидно, является детерминированным, поскольку однозначно дает ответ на вопрос, является ли число  $m$  составным или простым.

Оценим трудоемкость алгоритма 7.3. На первом шаге нам потребуется произвести  $\lceil \sqrt[3]{m} \rceil$  операций деления для поиска маленьких делителей числа  $m$ .

Трудоемкость второго шага оценивается в операциях тестирования числа  $v$ , определяемого на шаге 2.2, на то, является ли оно полным квадратом. Заметим, что для всех  $b > \frac{\sqrt[6]{m}}{4}$  выполняется только две проверки: для  $k = 0$  и  $k = 1$ . Тогда, трудоемкость второго этапа оценивается сверху величиной

$$\frac{\sqrt[6]{m}}{4} \sum_{b=1}^{\lfloor \sqrt[6]{m} \rfloor} \frac{1}{\sqrt{b}} + 2(\lceil \sqrt[3]{m} \rceil - \lfloor \sqrt[6]{m} \rfloor) < 3\lceil \sqrt[3]{m} \rceil.$$

Таким образом, трудоемкость всего алгоритма есть величина  $O(\sqrt[3]{m})$ .

## 7.4 Метод Полларда-Флойда

Описанные нами ранее алгоритмы факторизации носили детерминированный характер и позволяли после фиксированного числа шагов либо найти нетривиальные делители числа  $m$ , либо доказать, что число  $m$  простое.

Теперь мы перейдем к рассмотрению вероятностных алгоритмов, обладающих следующими свойствами. Во-первых, для алгоритма можно определить лишь среднее число шагов алгоритма, поскольку точное число шагов является случайной величиной и зависит от значений используемых в алгоритме псевдослучайных чисел. Во-вторых, если алгоритм не сможет определить делители числа  $m$ , то нельзя будет ничего сказать о том, является ли число  $m$  простым.

Мы начнем изложения с метода, предложенного Джоном Поллардом (John M. Pollard) в 1974 году в работе [42]. Метод основывается на свойствах случайных отображений конечного множества в себя. Подобные отображения мы подробно рассматриваем в приложении А.

Пусть, как и ранее,  $m$  нечетное составное число, которое мы хотим разложить на множители. Фиксируем произвольный многочлен с целыми коэффициентами, степени большей единицы, например, следуя Полларду,  $f(x) = x^2 + 1$ . Данный многочлен задает отображение кольца вычетов по модулю  $m$  в себя

$$f(x) \pmod{m} : \mathbb{Z}_m \rightarrow \mathbb{Z}_m.$$

Выберем произвольный элемент  $x_0$  кольца  $\mathbb{Z}_m$  и рассмотрим его орбиту, порожденную многочленом  $f(x)$ , то есть последовательность элементов кольца, определенных соотношением

$$x_{n+1} \equiv f(x_n) \pmod{m}, \quad n = 0, 1, \dots$$

Зафиксируем некоторый произвольный делитель  $p$  числа  $m$ . Рассмотрим последовательность  $\{a_n\}_{n=0}^{\infty}$ , элементы которой определяются сравнением  $a_n \equiv x_n \pmod{p}$  и принадлежат кольцу  $\mathbb{Z}_p$ . Поскольку число элементов кольца  $\mathbb{Z}_p$  конечно, то найдутся такие целые числа  $\tau$  и  $\lambda$ , что для всех индексов  $n \geq \lambda$  будет выполнено сравнение

$$a_n \equiv a_{n+\tau} \pmod{p}, \tag{7.12}$$

где величина  $\tau$  определяет длину цикла последовательности  $\{a_n\}_0^{\infty}$ , а величина  $\lambda$  – длину подхода к циклу.

Следовательно, для всех индексов  $n \geq \lambda$  будет выполнено сравнение  $x_n \equiv x_{n+\tau} \pmod{p}$ , то есть  $p \mid (x_{n+\tau} - x_n)$ . Последнее условие позволяет найти неизвестный делитель  $p$ , вычисляя  $\text{НОД}(m, x_{n+\tau} - x_n)$  для тех индексов  $n$ , при которых  $x_{n+\tau} \neq x_n$ .

Для поиска неизвестной величины  $\tau$  Поллард предложил использовать метод Флойда поиска циклов в последовательностях, который подробно рассматривается нами в приложении А, см. раздел А.2.1.

Заметим, что нам достаточно найти величину кратную  $\tau$ , поскольку  $x_n \equiv x_{n+\tau} \equiv x_{n+k\tau} \pmod{p}$  для любого  $k = 1, 2, \dots$ . Тогда, согласно Флойду, нам достаточно сравнивать элементы последовательности  $\{x_n\}_{n=0}^{\infty}$  с индексами  $n$  и  $2n$ , и проверять совпадение выполнимостью условия

$$\text{НОД}(m, x_n - x_{2n}) > 1.$$

Выполнение данного неравенства автоматически влечет за собой нахождение неизвестного делителя  $p$ . Отметим, что исходя из геометрических соображений, данный метод часто называют  $\rho$ -методом Полларда или методом Полларда-Флойда.

Суммируем приведенные выше рассуждения в виде алгоритма.

#### Алгоритм 7.4 ( $\rho$ -метод Полларда, метод Полларда-Флойда)

**Вход:** Целое составное число  $m$ .

**Выход:** Целое, быть может, составное число  $p$  такое, что  $p|m$ .

1. Зафиксировать некоторый многочлен второй степени  $f(x) \in \mathbb{Z}[x]$ , например,  $f(x) = x^2 + 1$ .
2. Выбрать случайный вычет  $x \in \mathbb{Z}_m$  и определить  $z = x$ ,  $p = 1$ .
3. Вычислить  $x \equiv f(x) \pmod{m}$ ,  $y \equiv f(z) \pmod{m}$ ,  $z \equiv f(y) \pmod{m}$ .
4. Вычислить  $p = \text{НОД}(m, z - x \pmod{m})$ .
5. Если  $p > 1$ , то завершить работу, в противном случае вернуться на шаг 3.  $\square$

Поскольку начальное значение последовательности  $\{x_n\}_{n=0}^\infty$  вырабатывается случайным образом, мы не можем получить точную оценку числа шагов, необходимых для разложения числа  $m$  на множители.

Предположим, что многочлен  $f(x)$  выбран случайно из множества всех возможных отображений кольца  $\mathbb{Z}_p$  в себя. Тогда, применяя теорему А.1, получим, что математическое ожидание длины цикла последовательности  $\{a_n\}_{n=0}^\infty$  есть величина, стремящаяся к  $\sqrt{\frac{\pi p}{8}} = O(\sqrt{p})$ . Последняя величина определяет оценку математического ожидания трудоемкости всего алгоритма, то есть для определения нетривиального делителя числа  $m$  нам потребуется, в среднем, вычислить  $O(\sqrt{p}) = O(\sqrt[4]{m})$  элементов последовательности  $\{x_n\}_{n=0}^\infty$ .

## 7.5 Метод Брента

Метод Брента является достаточно простой модификацией метода Полларда-Флойда, обладающей двумя принципиальными отличиями. Мы отметим эти отличия, сохранив обозначения предыдущего раздела.

Во-первых, для поиска совпадения элементов последовательности  $\{x_n\}_{n=0}^\infty$  используется метод, отличный от метода Флойда. В приложении А, см. раздел А.2.2, мы даем строгое обоснование этого метода.

Здесь же заметим, что Брент предложил искать совпадение элементов последовательности  $\{a_n\}_{n=0}^\infty$  путем проверки условия

$$x_n \equiv x_{2^k-1} \pmod{p},$$

для всех индексов  $n$  таких, что  $2^k \leq n < 2^{k+1}$ ,  $k = 0, 1, \dots$ . Как и ранее, проверка выполняется путем вычисления

$$\text{НОД}(m, x_n - x_{2^k-1}).$$

Во-вторых, метод факторизации реализуется в виде теста. Перед началом выполнения алгоритма фиксируется константа  $B$  – количество вычисляемых элементов последовательности. Как правило, из соображений эффективности реализации на ЭВМ, в качестве константы  $B$  выбирается некоторая степень двойки, т.е.  $B = 2^c$  для некоторого натурального  $c$ . Если по окончании  $B$  шагов нетривиальный делитель числа  $m$  не найден, то алгоритм завершает свою работу с уведомлением о неудаче.

### Алгоритм 7.5 (Алгоритм Брента)

**Вход:** Целое составное число  $m$  и натуральное число  $c \geq 1$ .

**Выход:** Либо целое, быть может, составное, число  $p$  такое, что  $p|m$ , либо заключение о том, что делитель не найден.

1. Зафиксировать многочлен  $f(x) \in \mathbb{Z}[x]$ , например,  $f(x) = x^2 + 1$ .
2. Выбрать случайный вычет  $x \in \mathbb{Z}_m$  и определить  $z = 0$ ,  $n = 0$  и  $k = 0$ ,  $t = 1$ .
3. Вычислить  $x \equiv f(x) \pmod{m}$ ,  $n = n + 1$ .
4. Если  $n = t$ , то определить  $z = x$  и  $k = k + 1$ ,  $t = 2t$ .
5. Если  $k > c$ , то завершить алгоритм с уведомлением о неудаче.  
Иначе вернуться на шаг 3.
6. Вычислить  $p = \text{НОД}(m, z - x)$ .
7. Если  $m > p > 1$ , то делитель найден и алгоритм завершает работу. В противном случае, вернуться на шаг 3. □

Трудоёмкость приведенного алгоритма фиксирована и составляет  $2^c$  операций вычисления элементов последовательности  $\{x_n\}_{n=0}^\infty$ . При этом, учитывая утверждение теоремы А.1 о длине цикла последовательности, можно ожидать, что алгоритм Брента сможет найти делитель  $p$ , не превосходящий величины  $O(B^2) = O(2^{2c})$ .

## 7.6 Методы факторизации чисел частного вида

Далее мы рассмотрим алгоритмы, которые позволяют эффективно раскладывать на множители числа  $m$  частного вида. В этих алгоритмах используются некоторые свойства числа  $m$ , которые существенно снижают трудоёмкость разложения на множители.

### 7.6.1 $p - 1$ метод Полларда

Один из первых подходов к разложению на множители чисел частного вида был предложен Джоном Поллардом в 1974 году работе [42]. Пусть  $m$  натуральное, нечетное, составное число, которое мы хотим разложить на множители и  $p$  некоторый простой делитель числа  $m$ .

Пусть  $a$  произвольное целое число, взаимно простое  $p$ . Зафиксируем целое число  $k$  такое, что  $p - 1 \mid k$ , тогда, согласно малой теореме Ферма, выполнено сравнение

$$a^k \equiv (a^{p-1})^{\frac{k}{p-1}} \equiv 1 \pmod{p},$$

откуда следует, что  $p \mid (a^k - 1)$ . Таким образом, задача определения неизвестного делителя  $p$  сводится к вычислению **НОД**  $(m, a^k - 1)$  и определению величины  $k$ .

Предположим, что нам *дополнительно* известно, что все простые делители числа  $p - 1$  не превосходят некоторой константы  $B$ , то есть

$$p - 1 = \prod_{i=1}^s p_i^{\alpha_i}, \quad \alpha_i \geq 1, \quad \alpha_i \in \mathbb{N}, \quad i = 1, \dots, s,$$

где  $p_i$  различные простые числа такие, что  $p_i < B$ . В этом случае, определим в качестве  $k$  произведение всех простых чисел, не превосходящих величины  $B$ ,

$$k = 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 5^{\gamma_3} \dots p_n^{\gamma_n}, \quad (7.13)$$

где величины  $\gamma_i$  удовлетворяют неравенствам

$$p_i^{\gamma_i - 1} < p \leq p_i^{\gamma_i},$$

то есть  $\gamma_i = \lceil \log_{p_i} p \rceil$ . Для данной величины  $k$ , очевидно, выполнено условие  $p - 1 \mid k$  и она может быть использована для поиска нетривиального делителя  $p$ .

На практике, при разложении числа  $m$  на множители, неизвестно ни точное значение величины  $B$ , ни размер простого делителя  $p$ . Поэтому описанная выше идея реализуется в виде следующего теста.

В начале, исходя из быстродействия вычислительного средства, реализующего тест, выбирается значение константы  $B$ . После строится число  $k$ , определяемое равенством (7.13). При этом величины  $\gamma_i$  полагаются равными единице практически для всех значений, кроме нескольких начальных простых чисел. Далее, несколько раз, случайным образом выбирается вычет  $a$  и вычисляется значение  $d = \text{НОД}(m, a^k - 1)$ . Если



величина  $d$  отлична от единицы, то нетривиальный делитель найден. Заметим, что нам достаточно для определения величины  $d$  вычислять значение  $a^k - 1$  по модулю числа  $m$ .

### Алгоритм 7.6 ( $p - 1$ алгоритм факторизации Полларда)

**Вход:** Целое составное число  $m$ , границы  $B$  и  $c \in \mathbb{N}$ .

**Выход:** Целое, быть может, составное, число  $p$  такое, что  $p|m$ .

1. Используя алгоритм 6.1, построить все простые числа  $p_1, p_2, \dots$ , не превосходящие величины  $B$  и определить величину  $k$ . Определить  $i = 0$ .
2. Вычислить  $i = i + 1$ , положить  $a = p_i$  (при  $i = 1$  значение параметра  $a$  должно равняться 2).
3. Если  $\text{НОД}(a, m) > 1$ , то завершить алгоритм с результатом  $p = a$ .
4. Вычислить  $d = \text{НОД}(m, a^k - 1 \pmod{m})$ .
5. Если  $m > d > 1$ , то завершить алгоритм с результатом  $p = d$ .
6. Если  $i < c$ , то вернуться на шаг 2. В противном случае, завершить алгоритм с уведомлением о неудаче. □

Поскольку мы определили величины  $\gamma_i$  меньшими, чем  $\lceil \log_{p_i} p \rceil$ , то могут найтись вычеты  $a$  такие, что их показатель по модулю  $p$  не будет делить  $k$ . В связи с этим, мы выполняем несколько проверок, число которых определяется параметром  $c$ . При практической реализации алгоритма величина  $c$  может принимать небольшие значения.

Как можно заметить,  $p - 1$  метод Полларда представляет собой аналог алгоритма пробного деления, изложенного нами ранее. Только в данном случае мы перебором ищем не делители числа  $m$ , а делители числа  $p - 1$ , собранные в виде произведения в число  $k$ . Немного позже мы опишем процедуры оптимизации алгоритма 7.6, в которых перебор делителей числа  $p - 1$  будет описан в явном виде.

#### 7.6.2 $p + 1$ метод Вильямса

Данный метод был предложен Хью Вильямсом (Hugh Williams) в 1982 году работе [54] и опирается на идеи, аналогичные  $p - 1$  методу Полларда. Пусть  $m$  нечетное составное число, которое мы хотим разложить на множители. Мы будем применять метод Вильямса в том случае, когда хотя бы один простой делитель  $p$  числа  $m$  имеет вид

$$p \pm 1 = \prod_i p_i^{\alpha_i}, \quad (7.14)$$

где  $p_i$  простые числа, не превосходящие некоторой границы  $B$ .

Ранее, в 6-й главе, мы ввели последовательности Люка. Напомним, что для двух целых взаимно простых чисел  $a, b$  рекуррентной

последовательностью Люка называется последовательность пар целых чисел  $U_n, V_n$ , определяемых равенствами (6.12)

$$U_{n+1} = aU_n - bU_{n-1}, \quad V_{n+1} = aV_n - bV_{n-1}, \quad n = 1, 2, \dots$$

где  $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a$ . Для эффективного вычисления значений пар  $U_n, V_n$ , можно использовать алгоритм 6.5, описанный нами ранее.

Пусть  $p$  нечетный, простой делитель числа  $m$ . Для заданной последовательности Люка, с параметрами  $a$  и  $b, b \not\equiv 0 \pmod{p}$ , определим  $\Phi(p) = p - \left(\frac{D}{p}\right)$ , где  $D$  удовлетворяет равенству  $D = a^2 - 4b$  и условию  $D \not\equiv 0 \pmod{p}$ . Согласно утверждению леммы 6.9 выполнено условие  $U_{\Phi(p)} \equiv 0 \pmod{p}$ .

Пусть  $k$  произвольное натуральное число такое, что  $\Phi(p) | k$ . Тогда из шестого утверждения леммы 6.7 следует, что  $U_{\Phi(p)} | U_k$ , откуда вытекает, что  $U_k \equiv 0 \pmod{p}$ .

Суммируя, мы получаем, что в случае выполнения условия  $\Phi(p) | k$ , искомый делитель числа  $m$  удовлетворяет условию

$$p | \text{НОД}(m, U_k). \quad (7.15)$$

Для поиска нетривиального делителя  $p$  числа  $m$  можно предложить следующий алгоритм, основывающийся на проверке условия (7.15). Он основан на выборе случайной пары чисел  $a, b$  и вычислении элемента последовательности Люка  $U_k$  при  $k$ , удовлетворяющем равенству

$$k = \prod_i p_i^{\alpha_i}, \quad \text{где } p_i \leq B. \quad (7.16)$$

Алгоритм Вильямса, так же как и  $p-1$  метод Полларда, является вероятностным и представляет собой тест. Если выполнено условие  $\Phi(p) | k$  или, что равносильно: либо  $p-1 | k$ , либо  $p+1 | k$ , то алгоритм сможет найти делитель числа  $m$ . В противном случае, алгоритм завершится с уведомлением о неудаче.

### Алгоритм 7.7 ( $p+1$ алгоритм факторизации Вильямса)

**Вход:** Целое составное число  $m$ , границы  $B$  и  $c \in \mathbb{N}$ .

**Выход:** Целое, быть может, составное, число  $p$  такое, что  $p | m$ .

1. Используя алгоритм 6.1, построить все простые числа, не превосходящие величины  $B$  и определить величину  $k = \prod_i p_i^{\alpha_i}$ , где  $p_i \leq B$ , при некоторых натуральных значениях<sup>4</sup> величин  $\alpha_i$ . Определить  $i = 0$ .

<sup>4</sup>Выбор натуральных значений  $\alpha_i$  может быть произведен аналогично  $p-1$  методу Полларда.

2. Вычислить  $i = i + 1$ , выбрать случайные, взаимно простые значения  $a, b$  и определить  $D = a^2 - 4b$ .
3. Если  $p = \text{НОД}(m, b) > 1$ , то завершить алгоритм.
4. Если  $p = \text{НОД}(m, D) > 1$ , то завершить алгоритм.
5. Используя алгоритм 6.5, вычислить элемент  $U_k$  последовательности Люка с параметрами  $a$  и  $b$ . При этом все вычисления величин можно проводить по модулю факторизуемого числа  $m$ .
6. Если  $p = \text{НОД}(m, U_k) > 1$ , то завершить алгоритм.
7. Если  $i < c$ , то вернуться на шаг 2. В противном случае, завершить алгоритм с уведомлением о неудаче.  $\square$

Как и в  $p - 1$  методе Полларда, нами введена граница  $c$ , которая задает количество перебираемых последовательностей Люка, для которых проверяется выполнение условия (7.15). При практической реализации алгоритма эта величина может принимать небольшие значения, например 10.

В заключение заметим, что метод Вильямса является расширением метода Полларда, поскольку он также применим для случая, когда для некоторого простого делителя  $p$  числа  $m$  значение  $p - 1$  раскладывается в произведение маленьких простых чисел. Однако вычисление последовательности Люка является более трудоемким, чем модульное возведение малого числа в степень  $k$ . В связи с этим, иногда, при практическом тестировании больших составных чисел метод Вильямса не используют, ограничиваясь более простым  $p - 1$  методом Полларда.

### 7.6.3 Второй этап: оптимизация алгоритмов Полларда и Вильямса

Предложенные нами выше алгоритмы Полларда и Вильямса могут быть оптимизированы путем добавления второго этапа. Предположим, что некоторого простого делителя  $p$  разложение (7.14) имеет вид

$$p \pm 1 = q \cdot \prod_{i=1}^s p_i^{\alpha_i}, \quad \text{где } p_i < B \text{ и } B < q. \quad (7.17)$$

То есть в разложение чисел  $p \pm 1$  входит один простой делитель, превосходящий заданную нами границу  $B$ . В этом случае, мы можем провести дополнительные вычисления для поиска величины  $q$  – второй этап указанных алгоритмов 7.6 и 7.7.

При поиске простого делителя  $q$  мы будем считать, что он ограничен сверху некоторой величиной  $B_1 > B$ . Перебирая все простые числа

$q_1, \dots, q_l$  на интервале  $B \leq q_1 < q_2 < \dots < q_l \leq B_1$ , мы можем проверить, для метода Полларда, выполнимость условия

$$\text{НОД}\left(m, (a^k)^{q_i} - 1 \pmod{m}\right) > 1, \quad i = 1, \dots, l,$$

где величина  $k$  определяется на первом этапе алгоритма. Если условие выполнено, то  $p - 1 \mid kq_i$  и мы найдем нетривиальный делитель числа  $m$ . Аналогично, для метода Вильямса, нам надо проверять выполнимость условия

$$\text{НОД}(m, U_{kq_i}) > 1, \quad i = 1, \dots, l.$$

В случае его выполнения, мы получаем, что  $\Phi(p) \mid kq_i$  и мы находим нетривиальный делитель числа  $m$ . Для вычисления  $U_{kq_i}$  можно использовать алгоритм 6.5 с начальными значениями  $U_k, V_k$ .

При больших значениях параметров  $B$  и  $B_1$  процедура перебора всех простых чисел на интервале  $[B, B_1]$  может являться достаточно трудоемкой. Поэтому мы приведем несколько способов, позволяющих оптимизировать перебор простых чисел.

## Разностная схема

Для упрощения процедуры перебора, Поллард предложил использовать тот факт, что разности между двумя соседними простыми числами, принадлежащими интервалу  $[B, B_1]$ , принимают небольшие значения.

Пусть  $q_1, \dots, q_l$  все простые числа в интервале от  $B$  до  $B_1$ . Определим разности

$$r_{i+1} = q_{i+1} - q_i \quad \text{для всех } i = 1, \dots, l - 1.$$

Обозначим  $b \equiv a^k \pmod{m}$ , тогда вычисление вычетов  $(a^k)^{q_i} \equiv b^{q_i} \pmod{m}$  в алгоритме Полларда может быть реализовано последовательно, то есть

$$b^{q_{i+1}} \equiv b^{q_i + r_i} \equiv b^{q_i} b^{r_i} \pmod{m}.$$

Величины  $b^{r_i} \pmod{m}$  могут быть вычислены перед выполнением второго этапа алгоритма и сохранены в памяти ЭВМ.

Эта же идея применима и для алгоритма Вильямса. Воспользовавшись соотношениями (6.15), мы можем записать равенства

$$U_{kq_{i+1}} = \frac{1}{2} (U_{kq_i} V_{kr_i} + U_{kr_i} V_{kq_i}), \quad V_{kq_{i+1}} = \frac{1}{2} (V_{kq_i} V_{kr_i} + DU_{kq_i} U_{kr_i}),$$

которые позволяют выразить пару  $U_{kq_{i+1}}, V_{kq_{i+1}}$  через пары  $U_{kq_i}, V_{kq_i}$  и  $U_{kr_i}, V_{kr_i}$ . Величины  $U_{kr_i}, V_{kr_i}$  также могут быть вычислены и сохранены

в памяти ЭВМ перед началом выполнения второго этапа. Мы не приводим в явном виде реализацию второго этапа для алгоритмов Полларда и Вильямса, оставляя ее в качестве упражнения читателю.

### Метод согласования

Опишем другой метод перебора всех простых чисел  $q_1, \dots, q_l$  в интервале от  $B$  до  $B_1$ . Отметим, что в русскоязычной литературе данный метод принято называть *методом согласования*, в то время как в англоязычной литературе используется понятие improved standard continuation (усложненное стандартное продолжение).

Определим натуральное число  $h = \lceil \sqrt{B_1} \rceil$ , тогда любое простое число  $q$  из интервала  $B \leq q \leq B_1$  может быть представлено в виде

$$q = uh + v, \quad \text{где } u, v \in \mathbb{N}, \quad \left\lfloor \frac{B}{h} \right\rfloor \leq u < h, \quad v < h. \quad (7.18)$$

Применим полученное равенство к алгоритму Полларда. Пусть выполнено условие  $p - 1 \mid kq$ , тогда  $(a^k)^q \equiv 1 \pmod{p}$ , что равносильно,

$$(a^k)^q (a^k)^{-v} \equiv (a^{kh})^u \pmod{p} \quad \text{или} \quad (a^k)^{-v} - (a^{kh})^u \equiv 0 \pmod{p}.$$

Последнее сравнение позволяет нам найти нетривиальный делитель числа  $m$ , путем вычисления

$$\text{НОД}(m, d^v - (b^h)^u \pmod{m}), \quad \text{где } b \equiv a^k, \quad d \equiv b^{-1} \pmod{m},$$

при некоторых натуральных  $u, v$ .

Реализация второго этапа алгоритма может выглядеть следующим образом. Вначале вычисляются значения  $(b^h)^u \pmod{m}$  для всех  $u$ , удовлетворяющих неравенствам (7.18). Вычисленные значения сохраняются в памяти ЭВМ. После этого для всех  $v = 1, 2, \dots, h$  вычисляются значения вычетов  $d^v \pmod{m}$  и проверяется условие

$$1 < \text{НОД}(m, d^v - (b^h)^u \pmod{m}) < m.$$

Если оно выполнено, то нетривиальный делитель числа  $m$  найден.

Соотношение (7.18) может быть использовано и при реализации метода Вильямса. Действительно, следуя (7.15), мы используем тот факт, что  $p \mid \text{НОД}(m, U_{kq})$ , для некоторого простого  $q$ , удовлетворяющего равенству (7.18).

Воспользовавшись равенствами (6.15), мы можем записать

$$2U_{kq} = (U_{khu}V_{kv} + U_{kv}V_{khu}).$$

Таким образом, мы можем предварительно вычислить значения  $U_{khu}$ ,  $V_{khu}$ , для всех  $u$  удовлетворяющих неравенствам (7.18), и сохранить их в памяти ЭВМ. После этого для всех  $v = 1, 2, \dots, h$  вычисляются значения элементов последовательности Люка  $U_{kv}$ ,  $V_{kv}$  и проверяется условие

$$m > \text{НОД}(m, U_{khu}V_{kv} + U_{kv}V_{khu}) > 1.$$

Если оно выполнено, то нетривиальный делитель числа  $m$  найден. Заметим, что поскольку  $m$  нечетно, то мы уменьшаем вычисления и заменяем величину  $U_{kq}$  величиной  $2U_{kq}$ .

Для снижения множества перебираемых значений можно использовать следующую идею. Выберем параметр  $h$  в равенстве (7.18) равным не  $h = \lceil \sqrt{B_1} \rceil$ , а наименьшим целым числом, большим, чем  $\lceil \sqrt{B_1} \rceil$  и кратным<sup>5</sup>  $2 \cdot 3 \cdot 5 \cdot 7 = 210$ . При этом интервал для величины  $u$  принимает вид  $\lfloor \frac{B}{h} \rfloor \leq u \leq \lceil \frac{B_1}{h} \rceil$ . Поскольку число  $q = uh + v$  должно быть простым, то параметр  $v$  не может принимать значения кратные 2, 3, 5 и 7.

Перебор таких значений  $v$  может быть организован аналогично методу решета, примененного нами в алгоритме 6.6. Положим  $v = 1$  и  $\delta_3 = \delta_5 = \delta_7 = 1$ . Мы будем прибавлять к  $v$  двойку, поскольку значение  $v$  должно быть нечетно. При каждом увеличении  $v$  на двойку мы вычисляем  $\delta_p = \delta_p + 2 \pmod{p}$ , при  $p = 3, 5, 7$ . Если все  $\delta_p$  отличны от нуля, то значение  $v$  может быть использовано. В противном случае вычисляется следующее значение.

## Поиск пар простых чисел

Следующая идея, развивающая метод согласования, была предложена Питером Монтогмери (Peter Montgomery) в статье [38]. Пусть, как и в методе согласования, нам задано целое число  $h$  – большее, чем  $\lceil \sqrt{B_1} \rceil$  и кратное 210.

Простое число  $q$  из интервала  $B \leq q \leq B_1$ , которое нам необходимо определить, может быть представлено в виде (7.18). Кроме того, мы можем определить парное ему число  $q_1$ , удовлетворяющее равенствам

$$q = uh + v, \quad q_1 = uh - v, \quad \left\lfloor \frac{B}{h} \right\rfloor \leq u \leq \left\lceil \frac{B_1}{h} \right\rceil, \quad v < h. \quad (7.19)$$

Пусть выполнено условие  $p - 1 \mid kq$  и  $(a^k)^q \equiv 1 \pmod{p}$ . Обозначим,

<sup>5</sup>Достаточно очевидно, что при реализации алгоритма мы можем использовать и другие значения, например,  $30 = 2 \cdot 3 \cdot 5$  или  $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ .

как и ранее  $b \equiv a^k \pmod{m}$ , тогда

$$\begin{aligned} b^{(uh)^2} - b^{v^2} &\equiv b^{v^2} \left( b^{(uh)^2 - v^2} - 1 \right) \equiv b^{v^2} \left( b^{(uh-v)(uh+v)} - 1 \right) \equiv \\ &\equiv b^{v^2} ((b^q)^{q_1} - 1) \equiv 0 \pmod{p}. \end{aligned} \quad (7.20)$$

Таким образом, сравнение (7.20) позволяет нам найти нетривиальный делитель числа  $m$  путем проверки условия

$$m > \text{НОД} \left( m, b^{(uh)^2} - b^{v^2} \pmod{m} \right) > 1. \quad (7.21)$$

Второй этап реализуется следующим образом. Вначале, по заданной таблице простых чисел, строится множество пар  $u, v$ , удовлетворяющих условиям (7.19). При этом для некоторых простых чисел парные к ним не будут простыми, тем не менее, такие пары мы также будем использовать. Поскольку процесс построения не зависит от числа  $m$ , раскладываемого на множители, то он может быть выполнен предварительно.

Далее, перебирая все пары из построенного множества, мы проверяем выполнимость условия (7.21): сперва мы фиксируем значение  $u$  и перебираем все допустимые значения  $v$ . После чего переходим к следующему значению  $u$ .

Для уменьшения трудоемкости вычисления величин  $b^{(hu)^2} \pmod{m}$  для всех  $u$ , последовательно пробегающих интервал  $\left\lfloor \frac{B}{h} \right\rfloor \leq u \leq \left\lceil \frac{B_1}{h} \right\rceil$ , можно воспользоваться следующим сравнением

$$b^{(h(u+1))^2} \equiv b^{(hu)^2} \cdot (b^{hu})^2 \cdot b^h \pmod{m},$$

основываясь на котором, мы можем вычислить следующее значение с использованием предыдущего, одного возведения в квадрат и одного модульного умножения.

Отметим, что в силу сложности соотношения (7.20), подход, основанный на переборе пар простых чисел, практически не применим при реализации метода Вильямса, и используется только для оптимизации  $p - 1$  метода Полларда.

## Поиск циклов в последовательностях

Последний подход, так же как и изложенный ранее метод факторизации Полларда-Флойда, основан на свойствах случайных отображений конечного множества в себя. Пусть, как и ранее, на первом этапе алгоритма Полларда мы вычислили элемент  $b \equiv a^k \pmod{m}$  и хотим найти простое число  $q$  такое, что  $B \leq q \leq B_1$  и  $b^k \equiv 1 \pmod{p}$ .

Рассмотрим псевдослучайную последовательность элементов

$$b_{i+1} \equiv b_i^{s_i} \pmod{m}, \quad s_i \equiv b_i \pmod{M}, \quad i = 0, 1, \dots,$$

где  $b_0 = b$ , а  $M$  некоторая маленькая константа, например 16.

Если мы рассмотрим каждый элемент этой последовательности по модулю некоторого простого числа  $p$ , являющегося делителем числа  $m$ , то данная последовательность заиклится. Для поиска цикла мы можем использовать метод Флойда, то есть искать пару значений

$$b_i \equiv b_{2i} \pmod{p} \quad (7.22)$$

для некоторого индекса  $i$ . Последнее сравнение равносильно тому, что

$$p \mid \text{НОД}(m, b_i - b_{2i} \pmod{m}). \quad (7.23)$$

Поскольку нам неизвестно точное значение простого числа  $q$ , то мы не можем определить мощность множества  $\{b, b^2, \dots, b^q \equiv 1 \pmod{p}\}$ . Поэтому мы будем проверять выполнение условия (7.23) для всех индексов  $i$  от 1 до  $\lceil \sqrt{B_1} \rceil$ . Такая оценка сверху очевидным образом следует из свойств псевдослучайных последовательностей. Более детально алгоритмы поиска циклов в последовательностях рассматриваются нами в приложении А.

Данный подход может быть достаточно просто перенесен на алгоритм Вильямса. Определим множество  $U_{kB}, U_{k(B+1)}, \dots, U_{kB_1}$  элементов последовательности Люка, которому принадлежит элемент  $U_{kq}$  для некоторого простого числа  $q$  такого, что  $B \leq q \leq B_1$  и  $p \mid \text{НОД}(m, U_{kq})$ .

Мы будем искать совпадение двух элементов на введенном множестве, при этом, величина  $B_1 - B$  задает мощность нашего множества.

Элементами нашей последовательности будут пары  $(U, V)$  элементов последовательности Люка. Начальный элемент последовательности имеет вид  $(U_k, V_k)$ . Тогда остальные элементы последовательности определяются по следующему правилу

$$s = B + (U_i \pmod{(B_1 - B)}), \quad U_{i+1} = U_{ks}, \quad V_{i+1} = V_{ks}.$$

Мы выбираем значение степени  $s$  таким образом, чтобы оно удовлетворяло неравенству  $B \leq s < B_1$ . В этом случае условие (7.23) принимает вид

$$p \mid \text{НОД}(m, U_i - U_{2i} \pmod{m}), \quad (7.24)$$

для некоторого индекса  $i$ , которое может быть проверено для всех индексов, не превосходящих  $\lceil \sqrt{B_1} \rceil$ .



### 7.6.4 Метод Женга

В 2001 году в статье [56] Женьксиань Женг (Zhenxiang Zhang) опубликовал алгоритм, который позволяет, при некоторых дополнительных условиях, эффективно раскладывать на множители составные числа, являющиеся произведением двух простых делителей. Для описания алгоритма и его модификаций нам потребуется следующая лемма.

**Лемма 7.3.** *Рассмотрим составное число  $m$ , являющееся произведением двух нечетных простых чисел  $p$  и  $q$ , для которых выполнено неравенство  $p < q$ , а также найдутся целые числа  $r, s$ , удовлетворяющие равенству  $q = s(p - 1) - r$  при  $0 < r \leq \frac{p-3}{2}$ .*

*Рассмотрим множество  $M$ , содержащее в себе все взаимно простые с  $m$  вычеты  $a$  такие, что  $a^{m+r} \equiv 1 \pmod{m}$ . Тогда выполнены следующие условия.*

1. *Мощность множества  $M$  не превосходит величины  $\frac{\varphi(m)}{2}$ .*
2. *Для любого натурального числа  $b$ , взаимно простого с  $m$ , и не принадлежащего множеству  $M$  выполнено условие*

$$p = \text{НОД}(m, b^{m+r} - 1 \pmod{m}). \quad (7.25)$$

*Доказательство.* Множество  $M$  образовано вычетами кольца  $\mathbb{Z}_m$ , являющимися корнями многочлена  $x^{m+r} - 1$ . Согласно теореме 3.4, эти вычеты удовлетворяют системе сравнений

$$\begin{cases} (x^{m+r} - 1) \equiv 0 \pmod{p}, \\ (x^{m+r} - 1) \equiv 0 \pmod{q}. \end{cases} \quad (7.26)$$

Количество вычетов по модулю  $p$ , удовлетворяющих первому сравнению данной системы равно  $p - 1$ . Действительно

$$\text{НОД}(m + r, p - 1) = \text{НОД}(s(p - 1), p - 1) = p - 1,$$

следовательно, каждое решение сравнения  $x^{m+r} - 1 \equiv 0 \pmod{p}$  удовлетворяет сравнению  $x^{p-1} \equiv 1 \pmod{p}$ . Последнее сравнение, согласно малой теореме Ферма, выполнено для всех вычетов  $x$ , взаимно простых с  $p$ .

Число решений второго сравнения системы (7.26) не превосходит величины  $\frac{q-1}{2}$ . Действительно, обозначим  $d = \text{НОД}(m + r, q - 1)$ . Тогда,

согласно теореме 2.10, сравнение  $x^{m+r} - 1 \equiv 0 \pmod{q}$  имеет не более  $d$  решений по модулю  $q$ . С другой стороны

$$\begin{aligned} d &= \text{НОД}(m+r, q-1) = \text{НОД}(s(p-1), s(p-1) - (r+1)) = \\ &= \text{НОД}(s(p-1), r+1) < r+1 \leq \frac{p-1}{2} < \frac{q-1}{2}. \end{aligned}$$

Таким образом, число решений системы (7.26) и, соответственно, мощность множества  $M$ , оценивается величиной

$$\text{НОД}(m-r, p-1) \text{НОД}(m-r, q-1) < \frac{(p-1)(q-1)}{2} = \frac{\varphi(m)}{2}.$$

Первое утверждение леммы доказано.

Для доказательства второго утверждения рассмотрим взаимно простой с  $m$  вычет  $b$ , не принадлежащий множеству  $M$ . Тогда выполнено сравнение  $b^{m+r} \not\equiv 1 \pmod{m}$ . С другой стороны, используя малую теорему Ферма, см. теорему 2.7, получаем

$$b^{m+r} \equiv (b^p)^qb^r \equiv b^qb^r \equiv b^{s(p-1)-r}b^r \equiv b^{-r}b^r \equiv 1 \pmod{p}.$$

Таким образом,  $p \mid (b^{m+r} - 1) \pmod{m}$ . Последнее утверждение завершает доказательство леммы.  $\square$

Метод разложения числа  $m$  на множители, основанный на доказанной нами лемме, выглядит следующим образом. Выберем случайный вычет  $b$ . Если он не взаимно прост с  $m$ , мы получаем нетривиальный делитель. В противном случае, с вероятностью, большей  $\frac{1}{2}$  будет выполнено условие  $\text{НОД}(m, b^{m+r} - 1 \pmod{m}) = p$  при некотором значении  $r$ . Перебирая все значения  $r$ , удовлетворяющие неравенству  $0 < r \leq \frac{p-3}{2}$ , мы находим делитель числа  $m$ . Трудоемкость данного алгоритма есть величина  $O(r)$ , что, в общем случае, сравнимо с  $O(p) \sim O(\sqrt{m})$ . Однако при малых значениях величины  $r$  алгоритм может быстро привести к разложению числа  $m$  на множители.

Для оптимизации предложенного метода мы можем его совместить с изложенным ранее  $p-1$  методом Полларда, см. раздел 7.6.1. Более того, мы будем рассматривать его как еще один вариант второго этапа метода Полларда, см. раздел 7.6.3.

Пусть  $k = \prod_i p_i^{\alpha_i}$  – произведение маленьких простых чисел  $p_i$ , не превосходящих некоторой заранее заданной границы  $B$ . Пусть выполнены условия

$$p-1 = ud, \quad k = ut, \quad d, u, t \in \mathbb{N}, \quad (7.27)$$

то есть величина  $p - 1$  раскладывается в произведение маленьких простых чисел, входящих в разложение числа  $k$  и некоторого натурального числа  $d$ , каждый простой делитель которого превышает величину  $B$ , то есть  $\mathbf{НОД}(d, k) = 1$ . Подобная ситуация возникает на втором этапе  $p - 1$ -метода Полларда.

Рассмотрим для наибольшего делителя  $q$  числа  $m$  два представления

$$q = s(p - 1) - r, \quad q = ld - z, \quad 0 < r \leq \frac{p-3}{2}, \quad 0 \leq z < d. \quad (7.28)$$

Теперь мы можем записать сравнение

$$\begin{aligned} (a^k)^m &\equiv (a)^{kq} \equiv a^{kld}(a^k)^{-z} \equiv a^{utld}(a^k)^{-z} \equiv \\ &\equiv (a^{p-1})^{lt}(a^k)^{-z} \equiv (a^k)^{-z} \pmod{p}, \end{aligned}$$

из которого следует  $(a^k)^{m+z} \equiv 1 \pmod{p}$ . Согласно доказанной ранее лемме, с вероятностью  $\frac{1}{2}$  выполнено условие  $(a^k)^{m+z} \not\equiv 1 \pmod{m}$  и мы получаем утверждение, аналогичное (7.25), а именно

$$p = \mathbf{НОД}(m, (a^k)^{m+z} - 1 \pmod{m}). \quad (7.29)$$

Полученное равенство существенно снижает границу для перебора значений  $z$ , поскольку  $0 \leq z < d$ . Однако она все равно остается достаточно высокой, поскольку  $d > B$ .

Надо заметить, что алгоритм Женга должен рассматриваться как частный случай  $p - 1$ -метода Полларда. Действительно, на втором этапе мы пытаемся найти простое число  $d$ , для которого выполнено сравнение  $(a^k)^d \equiv 1 \pmod{p}$  и  $p - 1 = d \cdot \mathbf{НОД}(p - 1, k)$ .

В случае выполнимости условия  $(a^k)^{m+z} \equiv 1 \pmod{p}$  получаем, что должно быть выполнено условие  $d \mid m + z$ . Это действительно так, поскольку из (7.28) следует равенство

$$m + z = p(ld - z) + z = dlp - (p - 1)z = d(lp - uz).$$

Обозначим  $\xi = \mathbf{НОД}(l, u) = \mathbf{НОД}(l, \frac{p-1}{d})$ , тогда  $m + z \equiv 0 \pmod{\xi}$ , что позволяет существенно снизить перебор возможных значений  $z$  и ограничиться только неотрицательными величинами  $z$ , удовлетворяющими сравнению  $z \equiv -m \pmod{\xi}$ . На практике величина  $\xi$  нам неизвестна, однако если она невелика, то есть величина  $l$  имеет маленькие простые делители, мы можем искать возможные значения неизвестной  $z$  в арифметических прогрессиях

$$z \equiv -m \pmod{\xi}, \quad \xi = 2, 3, 5, \dots$$

## ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ II

**Основная лемма - Решето Крайчика - Метод непрерывных дробей - Метод Моррисона-Брилхарда - Линейное решето Шрёппеля - Метод квадратичного решета и его модификации.**

В этой главе мы рассмотрим более эффективные методы разложения целого, составного нечетного числа  $m$  на множители. Описываемый нами класс методов имеет субэкспоненциальную оценку трудоемкости. На протяжении всей главы будем считать, что число  $m$  не содержит маленьких простых делителей и имеет общий вид, не позволяющий успешно применять алгоритмы, описанные ранее.

Докажем лемму, утверждения которой используются во всех алгоритмах настоящей главы. Лемма является обобщением равенств используемых в алгоритмах Ферма и Лемана.

**Лемма 8.1** (Лемма о факторизации). Пусть  $m$  нечетное составное число и  $x, y$  вычеты по модулю  $m$  такие, что  $x \not\equiv \pm y \pmod{m}$  и

$$x^2 \equiv y^2 \pmod{m}, \quad (8.1)$$

тогда будет выполнено условие  $1 < \text{НОД}(x - y, m) < m$ .

*Доказательство.* Согласно основной теореме арифметики, представим  $m$  в виде  $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ , где  $p_1, \dots, p_n$  различные нечетные простые числа,  $\alpha_1, \dots, \alpha_n$  натуральные числа. Тогда сравнение (8.1) позволяет нам записать равенство

$$(x - y)(x + y) = kp_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

для некоторого целого числа  $k$ .

Предположим, что выполнено условие  $\text{НОД}(x - y, m) = 1$ . Тогда, согласно лемме 1.4, выполнено  $p_i^{\alpha_i} \mid x + y$  для любого индекса  $i = 1, \dots, n$ . Следовательно,  $m \mid (x + y)$ , что равносильно сравнению  $x \equiv -y \pmod{m}$ . Последнее сравнение противоречит условию леммы.

Теперь предположим, что выполнено условие  $\text{НОД}(x - y, m) = m$ . Аналогичными рассуждениями получаем, что  $m \mid (x - y)$ , то есть сравнение  $x \equiv y \pmod{m}$  и противоречие условиям леммы. Таким образом, величина  $\text{НОД}(x - y, m)$  не превосходит  $m$  и не равна 1 или  $m$ . Лемма доказана.  $\square$

Согласно доказанной лемме для разложения числа  $m$  на множители достаточно найти пару вычетов  $x, y$ , удовлетворяющих условиям леммы. Легко заметить, что рассмотренные ранее равенства (7.1), (7.5) и (??) являются частным случаем сравнения (8.1).

## 8.1 Метод Крайчика

Еще в докомпьютерную эпоху, в 1926 году в монографии [31] Морис Крайчик<sup>1</sup> предложил последовательность действий, позволяющую для заданного составного числа  $m$  найти пару  $x, y$ , удовлетворяющую сравнению (8.1), и разложить число  $m$  на множители.

1. Вычислить некоторое множество пар целых чисел  $u, v$ , удовлетворяющих сравнению  $u \equiv v \pmod{m}$ .
2. Определить полное или частичное разложение чисел  $u, v$  на множители для каждой пары  $u, v$ .
3. С помощью известного разложения на множители выбрать те пары  $u, v$ , произведение которых позволит получить сравнение (8.1).
4. Разложить число  $m$  на множители.

В своей работе Крайчик не предъявил конкретный алгоритм поиска пар чисел  $u, v$  и алгоритмический способ составления из найденных соотношений сравнения (8.1). Тем не менее, Крайчик заметил, что в случае, когда одно из чисел является полным квадратом, то есть выполнено сравнение  $u^2 \equiv v \pmod{m}$ , получить сравнение (8.1) несколько проще.

**Пример 8.1.** Приведем пример и, используя метод Крайчика, разложим составное число  $m = 1081$  на множители. Рассмотрим равенства

$$\begin{aligned}1081 - 81 &= 1000, \\1081 - 960 &= 121, \\1081 - 720 &= 361, \\1089 - 1081 &= 8, \\1156 - 1081 &= 75.\end{aligned}$$

---

<sup>1</sup>Крайчик, Морис Борисович, родился в Минске 21 апреля 1882 г., еще до революции уехал в Бельгию, где учился и работал в университете города Льеж. Автор книг по теории чисел. Умер в Брюсселе 19 августа 1957.

Раскладывая на множители в приведенных равенствах слагаемые, отличные от 1081, мы можем записать следующие сравнения

$$\begin{aligned}
 -3^4 &\equiv 2^3 \cdot 5^3 \pmod{1081} \\
 -2^6 \cdot 3 \cdot 5 &\equiv 11^2 \pmod{1081} \\
 -2^4 \cdot 3^2 \cdot 5 &\equiv 19^2 \pmod{1081} \\
 3^2 \cdot 11^2 &\equiv 2^3 \pmod{1081} \\
 2^2 \cdot 17^2 &\equiv 3 \cdot 5^2 \pmod{1081}.
 \end{aligned} \tag{8.2}$$

Можно заметить, что правая или левая часть каждого из сравнений в (8.2), согласно замечанию Крайчика, является полным квадратом.

Перемножая первое, третье и четвертое сравнения из (8.2), получим

$$(-1)^2 \cdot 3^4 \cdot 2^4 \cdot 3^2 \cdot 5 \cdot 3^2 \cdot 11^2 \equiv 2^3 \cdot 5^3 \cdot 19^2 \cdot 2^3 \pmod{1081}$$

или, сокращая на  $2^4 \cdot 5$ ,

$$3^8 \cdot 11^2 \equiv 2^2 \cdot 5^2 \cdot 19^2 \pmod{1081}.$$

Последнее сравнение равносильно  $891^2 \equiv 190^2 \pmod{1081}$ . Мы получили сравнение вида (8.1), но оно не может быть использовано для разложения числа 1081 на множители. Действительно, поскольку выполнено равенство  $891 + 190 = 1081$ , то есть  $891 \equiv -190 \pmod{1081}$ , мы получаем противоречие с условием леммы 8.1.

Попробуем перемножить первое, второе, четвертое и пятое сравнения из (8.2). Получим

$$(-1)^2 \cdot 3^4 \cdot 2^6 \cdot 3 \cdot 5 \cdot 3^2 \cdot 11^2 \cdot 2^2 \cdot 17^2 \equiv 2^3 \cdot 5^3 \cdot 11^2 \cdot 2^3 \cdot 3 \cdot 5^2 \pmod{1081}$$

или, сокращая на  $2^6 \cdot 3 \cdot 5 \cdot 11^2$ ,

$$2^2 \cdot 3^6 \cdot 17^2 \equiv 5^4 \pmod{1081}.$$

Последнее сравнение равносильно  $918^2 \equiv 25^2 \pmod{1081}$ . Вычислим  $918 - 25 = 893$  и найдем **НОД**(893, 1081) = 47. Величина 47 является делителем числа 1081. Другим делителем числа 1081, как легко проверить, является число 23.

## 8.2 Метод непрерывных дробей

Как мы видели ранее, метод Крайчика сводит задачу разложения числа  $m$  на множители к построению некоторого количества сравнений  $u^2 \equiv v \pmod{m}$  и разложению на множители чисел  $v$ .

В общем случае величина  $v$  является величиной такого же порядка, как и  $m$ . Поэтому наивное применение метода Крайчика может привести к многократному разложению на множители чисел, сравнимых по величине с  $m$ .

Используя соотношения, возникающие при разложении квадратичных иррациональностей в непрерывные дроби, в 1931 году в работе [33] Лемер и Пауэрс (D.H. Lehmer & R.E. Powers) предложили два варианта генерации указанных сравнений. Оба варианта обладают тем свойством, что величины  $v$ , которые необходимо раскладывать на множители, не превосходят  $2\sqrt{m}$ .

Пусть  $f(x) = ax^2 + bx + c$  многочлен второй степени с целыми коэффициентами, дискриминант которого  $D = b^2 - 4ac$  не является полным квадратом и удовлетворяет неравенству  $D > 0$ . Дополнительно будем предполагать, что величина  $D \equiv 0 \pmod{m}$ .

Следуя разделу 5.3, определим квадратичную иррациональность  $\alpha_0$  – корень многочлена  $f(x)$ , удовлетворяющий неравенству  $\alpha_0 > 1$ , и разложим  $\alpha_0$  в непрерывную дробь

$$\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\alpha_n}}}},$$

где  $a_n = \lfloor \alpha_n \rfloor$  и  $\alpha_n = \frac{A_n + \sqrt{D}}{B_n}$ ,  $n = 0, 1, \dots$ , а коэффициенты  $A_n, B_n$  удовлетворяют рекуррентным соотношениям (5.20)

$$\begin{aligned} A_{n+1} &= a_n B_n - A_n, \\ B_{n+1} &= a_n (A_n - A_{n+1}) + B_{n-1}, \end{aligned}$$

где  $B_{-1} = -\frac{cB_0}{a}$ .

### 8.2.1 Первый вариант

Согласно доказанной нами ранее лемме 5.6, для коэффициентов  $A_n, B_n$  выполнено равенство (5.22)

$$-B_n B_{n+1} = A_{n+1}^2 - D.$$

Поскольку  $D \equiv 0 \pmod{m}$ , то мы можем записать сравнение

$$A_{n+1}^2 \equiv -B_n B_{n+1} \pmod{m}, \quad n = 0, 1, \dots \quad (8.3)$$

Полученное сравнение имеет вид  $u^2 \equiv v \pmod{m}$ , предложенный Крайчиком, и может быть использовано для факторизации числа  $m$ . При этом величина  $v$  является произведением двух натуральных чисел, каждое из которых не превосходит  $2\sqrt{D}$ .

Согласно следствию 1 к теореме 5.2, найдется индекс  $n_0$  такой, что для всех индексов  $n \geq n_0$ , квадратичная иррациональность  $\alpha_n$  будет приведенной, см. определение на стр. 94. Тогда, согласно лемме 5.7, для величин  $A_n, B_n$  будут выполнены неравенства

$$0 < A_n < \sqrt{D}, \quad 0 < B_n < 2\sqrt{D}. \quad (8.4)$$

Вычисляя последовательно полные частные  $\alpha_1, \alpha_2, \dots$  мы будем получать сравнения (8.3) для  $n = 0, 1, \dots$ . Раскладывая величины  $B_n$  на множители и комбинируя полученные сравнения аналогично тому, как это делалось в методе Крайчика, мы можем получить искомое сравнение  $x^2 \equiv y^2 \pmod{m}$ .

**Пример 8.2.** Проиллюстрируем изложенный метод и разложим на множители число  $m = 1081$ .

Выберем многочлен  $f(x) = 11x^2 + 5x - 24$ , дискриминант которого  $D = 25 + 4 \cdot 11 \cdot 24 = 1081$ , следовательно,  $D > 0$  и  $D \equiv 0 \pmod{1081}$ .

Определим в качестве квадратичной иррациональности  $\alpha_0$  положительный корень многочлена  $f(x)$ , то есть  $\alpha_0 = \frac{-5 + \sqrt{1081}}{22}$ . Получаем  $a_0 = \lfloor \alpha_0 \rfloor = 1$  и  $A_0 = -5, B_0 = 22$ .

Воспользовавшись равенством (5.1), запишем

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{27 + \sqrt{1081}}{16}, \quad a_1 = \lfloor \alpha_1 \rfloor = 3,$$

то есть  $A_1 = 27, B_1 = 16$ . Продолжая вычисления, находим

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{21 + \sqrt{1081}}{40}, \quad a_2 = 1, \quad A_2 = 21, \quad B_2 = 40,$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{19 + \sqrt{1081}}{18}, \quad a_3 = 2, \quad A_3 = 19, \quad B_3 = 18,$$

$$\alpha_4 = \frac{1}{\alpha_3 - a_3} = \frac{17 + \sqrt{1081}}{44}, \quad a_4 = 1, \quad A_4 = 17, \quad B_4 = 44.$$

Теперь запишем сравнения (8.3) для  $n = 0, 1, 2, 3$ .

$$\begin{aligned} -2^5 \cdot 11 &\equiv 3^6 \pmod{1081}, \\ -2^7 \cdot 5 &\equiv 3^2 \cdot 7^2 \pmod{1081}, \\ -2^4 \cdot 3^3 \cdot 5 &\equiv 19^2 \pmod{1081}, \\ -2^3 \cdot 3^2 \cdot 11 &\equiv 17^2 \pmod{1081}. \end{aligned} \quad (8.5)$$



Перемножая первое и четвертое сравнения, получим

$$(-1)^2 \cdot 2^5 \cdot 11 \cdot 2^3 \cdot 3^2 \cdot 11 \equiv 3^6 \cdot 17^2 \pmod{1081}$$

или, приводя подобные множители и сокращая на  $3^2$ ,

$$2^8 \cdot 11^2 \equiv 3^4 \cdot 17^2 \pmod{1081} \quad \text{или} \quad 176^2 \equiv 153^2 \pmod{1081}.$$

Мы получили сравнение вида (8.1), используя которое можно найти делитель числа 1081. Действительно,  $\text{НОД}(176 - 153, 1081) = 23$ . Легко проверить, что второй делитель числа 1081 равен 47.

## 8.2.2 Второй вариант

Второй вариант, предложенный Лемером и Пауэрсом, заключался в следующем. Пусть, как и ранее,  $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$  – квадратичная иррациональность, раскладываемая в непрерывную дробь, и  $\alpha_1, \alpha_2, \dots, \alpha_n, \dots$  последовательность полных частных.

Рассмотрим последовательность подходящих дробей  $\frac{P_n}{Q_n}$  к  $\alpha_0$  для всех индексов  $n = 0, 1, \dots$ . Напомним, что числители и знаменатели этих дробей удовлетворяют рекуррентным соотношениям (5.6)

$$\begin{aligned} P_{n+1} &= a_{n+1}P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1}Q_n + Q_{n-1}, \end{aligned}$$

где  $a_n = \lfloor \alpha_n \rfloor$  и  $P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1$ . Более того, согласно теореме 5.4, верно равенство (5.30)

$$(P_n B_0 - Q_n A_0)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1},$$

связывающее коэффициенты  $A_n, B_n$  полных частных и числители и знаменатели  $P_n, Q_n$  подходящих дробей.

Поскольку мы предположили, что  $D \equiv 0 \pmod{m}$ , то из последнего равенства вытекает сравнение

$$(P_n B_0 - Q_n A_0)^2 \equiv (-1)^{n+1} B_0 B_{n+1} \pmod{m}. \quad (8.6)$$

Данное сравнение имеет вид  $u^2 \equiv v \pmod{m}$ , предложенный Крайчиком, и может быть использовано для факторизации числа  $m$  так же, как и в первом варианте алгоритма.

Разложение квадратичной иррациональности в непрерывную дробь периодически, см. теорему 5.2. Поэтому количество соотношений, которые можно получить с помощью данного метода, ограничено, и их может оказаться недостаточно для набора соотношений и построения сравнения (8.1).

В той же работе [33] Лемер и Пауэрс показали, что оба варианта алгоритма эквивалентны: если один вариант алгоритма найдет решение, то и второй вариант также найдет решение. Как показывают практические эксперименты, при больших значениях  $m$  оба варианта алгоритма всегда находят разложение числа  $m$  на множители.

### 8.2.3 Метод Моррисона и Бриллхарта

В начале 70-х годов прошлого столетия, см. статью [39], Майкл Моррисон и Джон Бриллхарт (Michael A. Morrison & John Brillhart) предложили простую модификацию второго варианта алгоритма Лемера и Пауэрса. Они реализовали свой алгоритм на ЭВМ и применили его к факторизации седьмого числа Ферма  $F_7 = 2^{2^7} + 1$ .

Основное отличие реализованного Моррисоном и Бриллхартом алгоритма от первоначального варианта заключалось в введении процедуры алгоритмического построения сравнения  $x^2 \equiv y^2 \pmod{m}$  по заданному множеству сравнений вида  $u^2 \equiv v \pmod{m}$ . Для реализации этой процедуры потребовалось введение понятия «факторная база».

Напомним, что величина  $D$  является дискриминантом многочлена  $f(x)$  второй степени, корень которого раскладывается в непрерывную дробь. Поскольку  $D \equiv 0 \pmod{m}$ , то для дискриминанта выполнено равенство  $D = km$  при некотором натуральном числе  $k$ .

**Определение 8.1.** *Зафиксируем натуральное число  $B > 2$ . Мы будем называть множество  $\mathcal{B}_B$  факторной базой, если оно содержит целые числа  $-1, 2$ , а также нечетные простые числа  $p$ , удовлетворяющие следующим условиям.*

1. *Для величины  $p$  выполнено неравенство  $p \leq B$ .*
2. *Выполнено равенство  $\left(\frac{D}{p}\right) = 1$ , то есть число  $D$  является квадратичным вычетом по модулю  $p$ .*

Пусть в ходе выполнения первого или второго варианта алгоритма найдено сравнение вида  $u^2 \equiv v \pmod{D}$ . Факторная база  $\mathcal{B}_B$  представляет собой множество возможных делителей числа  $v$ , не превосходящих заданной величины  $B$ .

Обозначим символом  $p$  произвольный простой делитель числа  $v$ , тогда из сравнения  $u^2 \equiv v \pmod{D}$  следует сравнение  $D \equiv u^2 \pmod{p}$ . Таким образом, величина  $D$  является квадратичным вычетом по модулю любого простого числа, делящего  $v$ . Это объясняет второе условие в введенном нами определении факторной базы.

Параметр  $B$  влияет как на размер факторной базы, так и на общее количество вычисляемых сравнений. Оптимальное значение величины  $B$  мы получим позднее при исследовании анализа трудоемкости данного метода.

Опишем способ, который предложили Моррисон и Бриллхарт для построения сравнения  $x^2 \equiv y^2 \pmod{m}$  по множеству сравнений вида  $u^2 \equiv v \pmod{m}$ , вырабатываемых в ходе выполнения алгоритма. Каждому найденному сравнению, в котором

$$v = (-1)^{\gamma_0} \prod_{i=1}^{s-1} p_i^{\gamma_i}, \quad p_i \in \mathcal{B}_B, \quad \gamma_i \in \mathbb{N}, \quad (8.7)$$

и величина  $s$  определяет количество элементов в факторной базе, сопоставим вектора

$$\bar{\gamma} = (\gamma_0, \dots, \gamma_{s-1}), \quad (8.8)$$

$$\bar{e} = (e_0, e_1, \dots, e_{s-1}), \quad \text{где } e_i \equiv \gamma_i \pmod{2}. \quad (8.9)$$

Вектор  $\bar{e}$  содержит нули и единицы, то есть степени простых, входящих в разложение  $v$ , взятые по модулю 2. Нулям соответствуют простые в четной степени, то есть квадраты, единицам – простые, которые не образуют квадрат.

Предположим, что мы нашли  $r$  сравнений

$$u_i^2 \equiv v_i \pmod{m}, \quad i = 0, \dots, r-1, \quad (8.10)$$

правые части которых удовлетворяют равенству (8.7). Каждому сравнению будут соответствовать свои вектора  $\bar{\gamma}_i$  и  $\bar{e}_i$  вида (8.9).

Образуем из векторов  $\bar{e}_i$  прямоугольную матрицу  $E$  размера  $(r \times s)$ , где  $r$  количество строк матрицы, а  $s$  количество столбцов. Элементами матрицы являются нули и единицы – каждая строка матрицы соответствует одному из найденных сравнений (8.10). Аналогично, из векторов  $\bar{\gamma}_i$  образуем матрицу  $\Gamma$ .

Применим алгоритм исключения Гаусса над полем из двух элементов  $\mathbb{F}_2$  и приведем матрицу  $E$  к треугольному виду. Если  $r > s$ , то количество строк больше, чем количество столбцов, и, согласно [6], ранг матрицы

не превосходит  $s$ . Следовательно, найдется как минимум одна линейно зависимая строка, состоящая из одних нулевых элементов. Именно эта строка будет соответствовать сравнению, в котором правая часть будет полным квадратом.

Одновременно с изменением матрицы  $E$  мы будем модифицировать матрицу  $\Gamma$  и найденные нами сравнения таким образом, чтобы при получении нулевой строки, соответствующее ей сравнение имело искомый вид  $x^2 \equiv y^2 \pmod{m}$ .

### Алгоритм 8.1 (Алгоритм гауссового исключения)

**Вход:** Матрицы  $E = (e_{i,j})$  и  $\Gamma = (\gamma_{i,j})$  размера  $r \times s$  при  $r > s$ , а также сравнения (8.10), заданные в виде двух векторов  $(u_0^2, \dots, u_{r-1}^2)$  и  $(v_0, \dots, v_{r-1})$ .

**Выход:** Сравнение вида  $x^2 \equiv y^2 \pmod{m}$ .

**1. Для всех  $i$  от 0 до  $s - 1$  выполнить**

**1.1.** Перебирая  $j = 0, 1, \dots$ , найти номер строки  $u$  которой в  $i$ -м столбце стоит единица. Если такая строка не найдена, перейти к следующему значению индекса  $i$ .

**1.2. Для всех  $l$  от  $j + 1$  до  $r - 1$  выполнить**

**1.2.1** Если у  $l$ -й строки в  $i$ -м столбце есть единица, то вычислить

$$\begin{aligned} (e_{l,0}, \dots, e_{l,s-1}) &= (e_{j,0} + e_{l,0} \pmod{2}, \dots, e_{j,s-1} + e_{l,s-1} \pmod{2}) \\ u_l^2 &= u_l^2 \cdot u_j^2 \pmod{m}, \quad v_l = v_l \cdot v_j \pmod{m}, \\ (\gamma_{l,0}, \dots, \gamma_{l,s-1}) &= (\gamma_{i,0} + \gamma_{l,0}, \dots, \gamma_{i,s-1} + \gamma_{l,s-1}). \end{aligned}$$

**2. Для всех  $i$  от 0 до  $r - 1$  выполнить**

**2.1.** Если  $i$ -я строка состоит из одних нулей, то сравнение  $u_i^2 \equiv v_i \pmod{m}$  является искомым сравнением, поскольку  $v_i \equiv y^2 \pmod{m}$  для  $y$ , удовлетворяющего сравнению

$$y \equiv \prod_{j=1}^{s-1} p_j^{\frac{\gamma_{i,j}}{2}} \pmod{m}, \quad p_j \in \mathcal{B}_B.$$

□

Приведенный нами алгоритм гауссового исключения хорошо известен, см., например, монографию [6]. Его трудоемкость оценивается величиной  $O(s^3)$  операций побитового сложения и умножения вычетов по модулю  $m$  на шаге 1.2.1 приведенного алгоритма.

## 8.2.4 Как выбрать множитель $k$

Еще Крайчик в [31] заметил, что для генерации промежуточных соотношений можно использовать множитель  $k$ , отличный от единицы. При

этом для различных значений  $k$  множество простых, входящих в факторную базу, может быть различно. Однако Крайчик не предложил способ выбора величины  $k$ .

Метод для выбора оптимального значения величины  $k$  впервые предложил Рихард Шрёппель (Richard Schroepel) в конце 70-х годов прошлого столетия. Результаты Шрёппеля были опубликованы без строгого обоснования в 1981 году Дональдом Кнудом (Donald E. Knuth) во втором издании его монографии «Искусство программирования», см. [30, Гл.4 п.5].

Зафиксируем параметр  $B$  – оценку сверху для нечетных простых чисел, входящих в факторную базу  $\mathcal{B}_B$ . Тот факт, что при разных значениях  $k$  множество простых чисел, для которых выполнено равенство  $\left(\frac{D}{p}\right) = 1$  при  $D = km$ , различно, существенно влияет на выбор параметра  $k$ .

Допустим, что мы нашли сравнение  $u^2 \equiv v \pmod{D}$  и абсолютное значение правой части не превосходит  $2\sqrt{D}$ . Мы всегда можем записать равенство

$$|v| = t \cdot \prod_{i=1}^{s-1} p_i^{\gamma_i}, \quad \gamma_i \geq 0, \quad p_i \in \mathcal{B}_B, \quad (8.11)$$

где  $t$  равно единице, либо раскладывается в произведение простых чисел, больших чем  $B$ . Мы будем выбирать параметр  $k$  таким образом, чтобы, в среднем, максимизировать произведение  $\prod_{i=1}^{s-1} p_i^{\gamma_i}$  и минимизировать величину  $t$ .

Определим степень, в которой простое число  $p$ , в среднем, входит в разложение (8.11). Рассмотрим множество всех целых чисел, не превосходящих  $2\sqrt{D}$ , и предположим, что величины  $v$  распределены равномерно на указанном интервале. Зафиксируем простое число  $p$ , принадлежащее факторной базе  $\mathcal{B}_B$ , и дополнительно будем считать, что  $p$  не делит множитель  $k$ .

Хорошо известно, что количество чисел, делящихся на  $p$  и принадлежащих указанному интервалу, не более  $\frac{2\sqrt{D}}{p}$ , количество делящихся на  $p^2$  – не более  $\frac{2\sqrt{D}}{p^2}$  и так далее. Используя это, получим, что среди всех чисел, не превосходящих  $2\sqrt{D}$ , найдется ровно  $N_1$  чисел, которые в точности<sup>2</sup> делятся на  $p$ , где

$$N_1 = 2\sqrt{D} \left( \frac{1}{p} - \frac{1}{p^2} - \frac{1}{p^3} - \dots - \frac{1}{p^{n-1}} \right)$$

<sup>2</sup>Напомним, что число  $v$  в точности делится на  $p$ , если  $p$  делит  $v$ , а  $p^2$  уже не делит  $v$ .

для некоторого натурального  $n$  такого, что  $p^n > 2\sqrt{D}$ . Обобщая, мы можем записать, что мощность множества чисел, не превосходящих величины  $2\sqrt{D}$  и в точности делящихся на  $p^i$ , составляет

$$N_i = 2\sqrt{D} \left( \frac{1}{p^i} - \sum_{j=i+1}^{n-1} \frac{1}{p^j} \right), \quad i = 1, \dots, n-2, \quad (8.12)$$

и  $N_{n-1} = \frac{1}{p^{n-1}}$ . Следовательно, мы можем определить долю вхождения простого числа  $p$ , в среднем, в разложение числа  $v \in [1, 2\sqrt{D})$ , равенством

$$p^{\beta_p} = p^{\frac{1}{2\sqrt{D}}(N_1 + 2N_2 + \dots + (n-1)N_{n-1})}.$$

Суммируя значения сумм (8.12) с соответствующими множителями, получим выражение для  $\beta_p$

$$\beta_p = \sum_{i=1}^{n-1} a_i \frac{1}{p^i}, \quad \text{где} \quad a_i = i - \frac{i(i-1)}{2},$$

то есть, мы получаем равенство

$$\beta_p = \frac{1}{p} + \frac{1}{p^2} - \frac{2}{p^4} - \frac{5}{p^5} - \dots \quad (8.13)$$

Таким образом, мы будем считать, что простое число  $p$  входит в разложение целого числа  $v \in [1, 2\sqrt{D})$ , в среднем, в степени  $\beta_p$ , определяемой равенством (8.13). Вернемся к равенству (8.11) и запишем его в виде

$$\ln |v| = \ln t + \sum_{i=1}^{s-1} \beta_{p_i} \ln p_i.$$

Тогда максимум произведения  $\prod_{i=1}^{s-1} p_i^{\beta_i}$  достигается, в среднем, при максимуме суммы  $\sum_{i=1}^{s-1} \beta_{p_i} \ln p_i$ .

Теперь рассмотрим случай, когда простое число  $p$  в точности делит  $k$ . В этом случае выполнено равенство  $\left(\frac{km}{p}\right) = 0$  и простое не входит в факторную базу. Предположим, что мы нашли сравнение вида  $u^2 \equiv v \pmod{km}$ , в котором правая часть делится на  $p$ , то есть найдется такое натуральное число  $e > 0$ , что  $p^e | v$ . В этом случае мы получаем сравнение

$$pu_1^2 \equiv p^{e-1}v_1 \pmod{k_1m}, \quad (8.14)$$

где  $u = u_1p$ ,  $v = v_1p^e$  и  $k = k_1p$ . Если значение  $e > 1$  и четно, то сравнение (8.14) равносильно сравнению  $u_1^2 p^{2-e} \equiv v_1 \pmod{m}$ , снова имеющему вид  $u^2 \equiv v \pmod{m}$ . Если значение  $e$  нечетно, то сравнение (8.14)

равносильно сравнению

$$u_1^2 p^{1-e} \equiv v_1 p^{-1} \pmod{m},$$

в котором слева стоит полный квадрат, а правая часть содержит множитель  $p^{-1} \pmod{m}$ . Следовательно, если величина  $p^{-1} \pmod{m}$  раскладывается в произведение элементов факторной базы, то есть представляется в виде (8.7), то простое число  $p$  также должно быть учтено. Множество таких чисел мы будем обозначать символом  $\Delta$ . Случай, когда величина  $k$  делится на степени простых чисел, мы рассматривать не будем.

Определим функцию  $\tau(k, m, B)$

$$\tau(k, m, B) = \sum_{i=1}^{s-1} \beta_{p_i} \ln p_i, \quad p_i \in \mathcal{B}_B \cup \Delta,$$

где коэффициенты  $\beta_{p_i}$  определены равенством (8.13). Мы будем выбирать множитель  $k$ , удовлетворяющий следующим условиям.

1. Поскольку факторная база всегда содержит двойку, то множитель  $k$  должен быть нечетным.
2. Множитель  $k$  не должен делиться на степень простого числа, большую единицы.
3. Множитель  $k$  должен максимизировать значение функции

$$k = \max_k \tau(k, m, B).$$

Добавим, что количество слагаемых в (8.13) может зависеть от величины числа  $m$  и определяется точностью различения значений функции  $\tau(k, m, B)$  для различных значений  $k$ . Например, в работе [50] Роберт Сильвермен (Robert D. Silverman) использовал значение  $\beta_p = \frac{1}{p}$ . В той же работе функция  $\tau(k, m, B)$  получила название «функция Кнута-Шрёппеля».

### 8.2.5 Как выбрать квадратичную иррациональность

Пусть нам задано нечетное составное число  $m$ , не имеющее маленьких простых делителей. Нам необходимо определить величину  $\alpha_0 > 1$ , которая будет раскладываться в непрерывную дробь. Величина  $\alpha_0$  является

корнем многочлена второй степени  $f(x) = ax^2 + bx + c$ , дискриминант которого должен быть положителен и удовлетворять сравнению  $D \equiv 0 \pmod{m}$ .

Для начала заметим, что равенство  $D = b^2 - 4ac$  влечет за собой сравнение  $D \equiv b^2 \pmod{4}$ . Это сравнение разрешимо относительно  $b$  только в том случае, когда  $D \equiv 0, 1 \pmod{4}$ . Следовательно, при фиксированных значениях  $m$  и  $k$  дискриминант многочлена  $f(x)$  должен удовлетворять равенствам

$$b^2 - 4ac = D = \begin{cases} km, & \text{если } k \equiv m \pmod{4}, \\ 4km, & \text{иначе.} \end{cases}$$

Заметим, что для введенной ранее функции Кнута-Шрёппеля выполнено равенство  $\tau(k, m, B) = \tau(4k, m, B)$ , из которого следует, что умножение на четверку не изменяет свойство оптимальности выбранного параметра  $k$ .

Легко проверить, что выполнение условия  $k \equiv m \pmod{4}$  влечет за собой сравнение  $D \equiv 1 \pmod{4}$ . Действительно, поскольку  $m$  нечетно, то  $m \equiv 2\delta + 1 \pmod{4}$  для некоторого значения  $\delta \in \{0, 1\}$ . Поскольку  $k \equiv m \pmod{4}$ , то получаем сравнение

$$D = km \equiv (2\delta + 1)^2 \equiv 4\delta^2 + 4\delta + 1 \equiv 1 \pmod{4}.$$

Окончательно, мы заключаем

$$\begin{aligned} D &\equiv 1 \pmod{4}, & \text{при } k &\equiv m \pmod{4}, \\ D &\equiv 0 \pmod{4}, & \text{при } k &\not\equiv m \pmod{4}, \end{aligned}$$

Наиболее простой способ – определить многочлен  $f(x)$  равенством  $f(x) = x^2 - km$ , при этом положительный корень многочлена имеет вид  $\alpha_0 = \sqrt{km}$ . Именно такие значения использовались как в алгоритме Лемера и Пауэrsa, так и в алгоритме Моррисона и Брилхарта.

Другим способом является выбор некоторого произвольного многочлена  $f(x) = ax^2 + bx + c$ , при  $a > 1$ , положительный корень которого будет раскладываться в непрерывную дробь.

В качестве параметра  $a$  выберем произвольное нечетное простое число из факторной базы и рассмотрим два случая.

1. Пусть выполнено сравнение  $D \equiv 1 \pmod{4}$  или, что равносильно,  $km = D = b^2 - 4ac$ . В силу выбора параметра  $a$ , величина  $D$  является квадратичным вычетом по модулю  $a$ , следовательно, можно воспользоваться алгоритмом Тонелли-Шенкса, см. алгоритм 4.2,



и найти два значения величины  $b$ , удовлетворяющей сравнению  $b^2 \equiv D \pmod{a}$ .

Выберем из двух найденных значений нечетное, тогда выполнено сравнение  $b^2 \equiv D \pmod{4a}$ . Таким образом, мы можем определить параметр  $c$  равенством  $c = \frac{b^2 - km}{4a}$ . Для того чтобы гарантировать неравенство

$$\alpha_0 = \frac{-b + \sqrt{D}}{2a} > 1,$$

нам достаточно выполнения условия  $\sqrt{km} > 2a + b$ . Поскольку  $b < a$ , то мы можем наложить более жесткое условие  $0 < a < \frac{\sqrt{km}}{3}$ .

2. Если выполнено сравнение  $D \equiv 0 \pmod{4}$ , то  $4km = b^2 - 4ac$ . Следовательно, величина  $b$  четна. Определим  $b = 2b_1$ , где  $b_1$  произвольное решение сравнения  $b_1^2 \equiv D \pmod{a}$ . Как и ранее, величина  $b_1$  может быть найдена с использованием алгоритма Тонелли-Шенкса. Мы получаем, что величина  $c$  должна удовлетворять равенству  $c = \frac{b_1^2 - km}{a}$ . Для того чтобы гарантировать неравенство

$$\alpha_0 = \frac{-b + \sqrt{D}}{2a} = \frac{-b_1 + \sqrt{km}}{a} > 1,$$

достаточно выполнения условия  $\sqrt{km} > a + b_1$  или более жесткого неравенства  $0 < a < \frac{\sqrt{km}}{2}$ .

## 8.2.6 Асимптотическая оценка сложности

Кратко суммируем вышеизложенное: метод непрерывных дробей развивает идеи, предложенные Крайчиком, и состоит из следующей последовательности шагов.

### Алгоритм 8.2 (Факторизация с помощью непрерывных дробей)

**Вход:** Целое составное число  $m > 0$ .

**Выход:** Натуральный делитель  $p > 1$  числа  $m$ .

1. Выбрать значение  $B > 0$  и, воспользовавшись функцией Кнута-Шрёпеля, определить множитель  $k$  и факторную базу  $\mathcal{B}_B$ .
2. Построить многочлен второй степени  $f(x) \in \mathbb{Z}[x]$ , положительный корень которого  $\alpha_0$  удовлетворяет неравенству  $\alpha_0 > 1$ .
3. Разложить  $\alpha_0$  в непрерывную дробь и, используя сравнения (8.3) или (8.6), получить множество сравнений вида  $u^2 \equiv v \pmod{D}$ , где  $D = km$ .

4. Среди найденных сравнений отобрать те, для которых величина  $v$  может быть представлена в виде (8.7)

$$v = (-1)^{\gamma_0} \prod_{i=1}^{s-1} p_i^{\gamma_i}, \quad p_i \in \mathcal{B}_B, \quad \gamma_i \in \mathbb{N}.$$

При разложении на множители чисел  $v$  можно использовать пробное деление. Более эффективным является применение алгоритмов Брента,  $p - 1$  метода Полларда или  $p + 1$  метода Вильямса. Еще более эффективный способ заключается в использовании алгоритмов решета, которые мы опишем в следующих разделах.

5. Согласно описанию раздела 8.2.3, построить матрицы  $E$  и  $G$ . Применяя алгоритм 8.1 гауссового исключения, построить сравнение  $x^2 \equiv y^2 \pmod{D}$ .
6. Используя лемму 8.1, найти нетривиальный делитель числа  $m$ , то есть определить  $p = \text{НОД}(D, x - y)$ .  $\square$

Прежде чем оценить трудоемкость данного алгоритма, приведем пример, иллюстрирующий его некоторые шаги.

**Пример 8.3.** Разложим на множители целое число  $m = 63819221$ . Выберем значение параметра  $k = 1$  и определим  $D = km = 63819221$ . Определим параметр  $B = 15$  и рассмотрим факторную базу

$$\mathcal{B}_{15} = \{-1, 2, 5, 7, 11\}.$$

Построим многочлен  $f(x) = ax^2 + bx + c$ , корень которого будет раскладываться в непрерывную дробь. Выберем  $a = 5$  – наименьшее нечетное простое число, входящее в факторную базу. Поскольку выполнено сравнение  $63819221 \equiv 1 \pmod{5}$ , то мы можем определить параметры  $b = 1$  и  $c = \frac{1-63819221}{5} = -3190961$ . Выбирая наибольший корень построенного многочлена  $f(x) = 5x^2 + x - 3190961$  получим, что квадратичная иррациональность  $\alpha$  принимает вид

$$\alpha = \frac{-1 + \sqrt{63819221}}{10}.$$

Теперь разложим построенное число  $\alpha$  непрерывную дробь и вычислим, с использованием равенств (5.20), последовательность коэффициентов  $A_n, B_n$ , где  $A_0 = -1, B_0 = 10$ . Для каждого индекса  $n$  попробуем разложить величину  $B_n$  в произведение элементов факторной базы и получим несколько значений

$$\begin{aligned} B_{37} &= 686 &= 2 \cdot 7^3 \\ B_{41} &= 350 &= 2 \cdot 5^2 \cdot 7 \\ B_{45} &= 8750 &= 2 \cdot 5^4 \cdot 7 \\ B_{51} &= 3850 &= 2 \cdot 5^2 \cdot 7 \cdot 11. \end{aligned}$$

Воспользуемся соотношениями (5.6) и вычислим подходящие дроби к  $\alpha$  с индексами, меньшими чем найденные, на единицу. При этом, мы будем вычислять значения числителей и знаменателей по модулю величины  $D$ , то есть

$n$	$P_n \pmod{D}$	$Q_n \pmod{D}$
36	52685695	37880572
40	21881617	35689443
44	4921880	62241323
50	47792522	39029725

Воспользуемся сравнением (8.6) и составим несколько соотношений, в которых левая часть является квадратом, а правая раскладывается в произведение элементов факторной базы. Поскольку  $B_0 = 2 \cdot 5$ , получаем

$$\begin{aligned} \text{при } n = 36 : \quad 54183754^2 &\equiv -6860 &= -2^2 \cdot 5 \cdot 7^3 \\ \text{при } n = 40 : \quad 63047950^2 &\equiv -3500 &= -2^2 \cdot 5^3 \cdot 7 \\ \text{при } n = 44 : \quad 47640902^2 &\equiv -87500 &= -2^2 \cdot 5^5 \cdot 7 \\ \text{при } n = 50 : \quad 6401177^2 &\equiv -38500 &= -2^2 \cdot 5^3 \cdot 7 \cdot 11. \end{aligned}$$

Составим матрицы  $\Gamma$  и  $E$

$$\Gamma = \begin{pmatrix} 1 & 2 & 1 & 3 & 0 \\ 1 & 2 & 3 & 1 & 0 \\ 1 & 2 & 5 & 1 & 0 \\ 1 & 2 & 3 & 1 & 1 \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

и приведем матрицу  $E$  к диагональному виду. Легко видеть, что в матрице  $E$  вторая и третья строка совпадают с первой. Поэтому, прибавляя первую строку ко всем строкам, получим следующие матрицы

$$\Gamma = \begin{pmatrix} 1 & 2 & 1 & 3 & 0 \\ 2 & 4 & 4 & 4 & 0 \\ 2 & 4 & 6 & 4 & 0 \\ 2 & 4 & 4 & 4 & 1 \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Матрица  $E$  имеет диагональный вид и несколько строк, полностью состоящих из нулей. Каждая такая строка может дать нам нетривиальное разложение число  $m$  на множители.

Второй строке матрицы  $E$  соответствует сравнение

$$(54183754 \cdot 63047950)^2 \equiv (-1)^2 \cdot 2^4 \cdot 5^4 \cdot 7^4 \cdot 11^0 = 4900^2 \pmod{63819221},$$

откуда

$$\text{НОД}(63819221, 63259991 - 4900) = 8059,$$

то есть нетривиальный делитель числа  $m = 63819221$  найден и равен 8059. Аналогично, третьей строке матрицы  $E$  соответствует сравнение

$$(54183754 \cdot 47640902)^2 \equiv (-1)^2 \cdot 2^4 \cdot 5^6 \cdot 7^4 \cdot 11^0 = 24500^2 \pmod{63819221}.$$

При этом, выполнено

$$54183754 \cdot 47640902 \equiv 63794721 \equiv -24500 \pmod{63819221},$$

откуда следует, что найденное соотношение не удовлетворяет условиям леммы 8.1 и не может быть использовано для нахождения нетривиального делителя числа 63819221.

---

Изложенный нами метод состоит из большого числа шагов

### 8.3 Метод линейного решета

В конце 70-х годов прошлого столетия Рихард Шрёппель (Richard Schroepel) предложил свой собственный метод генерации соотношений вида  $u^2 \equiv v \pmod{m}$ . Впоследствии этот метод получил название метода линейного решета. Поскольку Шрёппель не опубликовал свои результаты, мы излагаем его метод согласно статье [44].

Обозначим, как и ранее,  $h = \lfloor \sqrt{m} \rfloor$ . Зафиксируем действительное число  $\varepsilon$ , удовлетворяющее неравенствам  $0 < \varepsilon < \frac{1}{2}$ , и зафиксируем интервал  $\mathcal{I} = \{-m^\varepsilon, m^\varepsilon\}$ . Рассмотрим две функции двух целочисленных переменных  $a, b$ , определенных на интервале  $\mathcal{I}$  равенствами

$$s(a, b) = (h + a)(h + b) - m, \quad t(a, b) = (h + a)(h + b), \quad a, b \in \mathbb{Z} \cap \mathcal{I}.$$

Поскольку  $t(a, b) \equiv s(a, b) \pmod{m}$ , то Шрёппель предложил использовать значения введенных функций  $s(a, b)$  и  $t(a, b)$  для построения необходимых соотношений. Зафиксируем некоторую границу  $B > 0$  и рассмотрим факторную базу  $\mathcal{B}_B$ , в которую входят все простые числа, не превосходящие  $B$ , а также целое число  $-1$ .

Рассмотрим сравнение

$$\prod_{i,j} t(a_i, b_j) \equiv \prod_{i,j} s(a_i, b_j) \pmod{m}. \quad (8.15)$$

Левая часть сравнения (8.15) будет полным квадратом, если каждая из величин  $a_i, b_j$  входит в произведение четное число раз. Предположим,

что правая часть в сравнении (8.15) может быть представлена в виде произведения

$$\prod_{i,j} s(a_i, b_j) = (-1)_0^\gamma \Delta \prod_{p_i} p_i^{\gamma_i},$$

где  $p_i$  простые числа, принадлежащие факторной базе  $\mathcal{B}_B$ , а  $\Delta$  целое число, являющееся полным квадратом. В этом случае сравнение (8.15) представляет собой сравнение вида  $u^2 \equiv v \pmod{m}$  с известным разложением  $v$  на множители из факторной базы. Если таких сравнений будет найдено больше, чем элементов факторной базы, то алгоритм гауссового исключения позволит построить необходимое для разложения числа  $m$  сравнение  $x^2 \equiv y^2 \pmod{m}$ .

Относительно разложения величин  $s(a, b)$  на множители Шрёппель заметил следующее. Во-первых, они принимают достаточно небольшие значения. Действительно, поскольку выполнено неравенство  $m^\varepsilon < h$ , верна оценка

$$|s(x, y)| = |h^2 + h(x + y) + xy - m| < 2hm^\varepsilon + m^{2\varepsilon} < 3hm^\varepsilon.$$

Во-вторых, существует эффективный способ поиска значений  $a, b$ , при которых величины  $s(a, b)$  раскладываются в произведение элементов факторной базы. Этот способ называется методом решета.

Пусть простое число  $p \in \mathcal{B}_B$  делит значение величины  $s(a, b)$  при некоторых  $a$ . Тогда из равенства

$$\begin{aligned} s(a + kp, b + lp) &= (h + a + kp)(h + b + lp) - m = \\ &= (h + a)(h + b) - m + kp(h + b) + (h + a + kp)lp = \\ &= s(a, b) + p(k(h + b) + l(h + a + kp)) \end{aligned}$$

следует, что  $p | s(a + kp, b + lp)$  для произвольных целых значений  $k, l$ . Таким образом, проверка делимости на простое число  $p$  величины  $s(a, b)$  для произвольных  $a, b \in \mathcal{I}$  сводится к проверке делимости на  $p$  величины  $s(a \pmod{p}, b \pmod{p})$ . Последние величины могут быть сохранены в памяти ЭВМ при небольших значениях  $B$ .

Автору не известен случай практической реализации метода линейного решета на ЭВМ. Причиной этому стали отсутствие алгоритмического способа построения сравнений (8.15) с известным разложением левой части в произведение множителей из факторной базы, необходимость использования большого объема памяти, а также скорое появление более эффективного метода квадратичного решета.

## 8.4 Метод квадратичного решета

В 1981 году Карл Померанс (Carl Pomerance) предложил алгоритм, который в настоящее время называется алгоритмом квадратичного решета (quadratic sieve algorithm). Померанс предложил упростить метод линейного решета Шрёппеля и рассмотреть вместо функции двух переменных  $s(a, b)$  многочлен от одной переменной  $x$

$$s(x, x) = f(x) = (h + x)^2 - m.$$

Легко видеть, что для любого значения целочисленной переменной  $x$  выполнено сравнение

$$(h + x)^2 \equiv f(x) \pmod{m}, \quad (8.16)$$

то есть сравнение Крайчика вида  $u^2 \equiv v \pmod{m}$ , которое может быть использовано для построения сравнения (8.1).

Аналогично методу Моррисона-Брилхарт, см. раздел 8.2.3, заметим следующий факт. Пусть для некоторого целого  $x$  найдется нечетное простое число  $p$  такое, что  $p \mid f(x)$ , то есть  $f(x) = (h + x)^2 - m = kp$  для некоторого натурального числа  $k$ . Последнее равенство равносильно сравнению  $(h + x)^2 \equiv m \pmod{p}$ . Следовательно, если нечетное простое число  $p$  делит правую часть в сравнении (8.16), то  $m$  является квадратичным вычетом по модулю  $p$  и для символа Лежандра  $\left(\frac{m}{p}\right)$  выполнено равенство  $\left(\frac{m}{p}\right) = 1$ .

Зафиксируем факторную базу  $\mathcal{B}_B$  – множество, содержащее числа  $-1$ ,  $2$  и некоторое количество нечетных простых чисел, удовлетворяющих двум условиям.

1. Каждое нечетное простое число  $p \in \mathcal{B}_B$  не превосходит величины  $B$ , то есть  $p \leq B$ .
2. Число  $m$  должно являться квадратичным вычетом по модулю каждого нечетного простого числа  $p \in \mathcal{B}_B$ , то есть  $\left(\frac{m}{p}\right) = 1$ .

Факторная база определяет множество возможных делителей правой части сравнения (8.16). Покажем, как предложенный Шрёппелем алгоритм решета может быть использован для поиска значений многочлена  $f(x)$ , удовлетворяющих равенству (8.7)

$$f(x) = (-1)^{\gamma_0} \prod_{i=1}^{s-1} p_i^{\gamma_i}, \quad p_i \in \mathcal{B}_B, \quad \gamma_i \in \mathbb{N}.$$

Зафиксируем некоторый интервал  $\mathcal{I}$  и будем считать, что переменная  $x$  пробегает множество всех целых чисел, принадлежащих интервалу  $\mathcal{I}$ . Обозначим символом  $\delta$  количество таких целых чисел. Мы будем искать среди  $\delta$  значений многочлена  $f(x)$  те значения, для которых выполнено равенство (8.7) при  $x \in \mathcal{I}$ .

Алгоритм основывается на следующем свойстве. Пусть нечетное простое число  $p$  делит значение многочлена  $f(x)$ , то есть  $f(x) \equiv 0 \pmod{p}$ . Тогда для любого целого значения  $k$  выполнено сравнение

$$\begin{aligned} f(x + kp) &= (h + x + kp)^2 - m = (h + x)^2 + 2kp(h + x) + k^2p^2 - m = \\ &= f(x) + p(2k(h + x) + pk^2) \equiv 0 \pmod{p}. \end{aligned}$$

Таким образом, если в точке  $x$  значение многочлена  $f(x)$  делится на простое число  $p$ , то во всех точках вида  $x + kp$  значение  $f(x + kp)$  также делится на  $p$ .

Рассмотрим массив  $T$ , состоящий из  $\delta$  действительных значений, и выполним следующую последовательность действий.

1. Инициализируем все элементы массива нулем.
2. Воспользуемся алгоритмом Тонелли-Шенкса, см. раздел 4.3, и для каждого простого числа  $p \in \mathcal{B}_B$  найдем величины  $x_1, x_2$ , удовлетворяющие сравнению  $f(x) \equiv 0 \pmod{p}$ . Поскольку  $p$  принадлежит факторной базе, то, в силу теоремы 4.2, искомое сравнение действительно будет иметь два различных решения.
3. Для всех возможных значений целочисленного индекса  $k$ , такого, что  $x_i + kp \in \mathcal{I}$ , при  $i = 1, 2$ , определим новое значение элементов массива

$$T[x_i + kp] = T[x_i + kp] + \ln p, \quad x_i + kp \in \mathcal{I}, \quad i = 1, 2.$$

4. После того как будут перебраны все простые числа из факторной базы, найдем те элементы массива  $T$ , для которых значения величин  $T[x]$  будут достаточно близкими к величине  $\ln |f(x)|$ .
5. Для каждого из таких элементов разложим величину  $f(x)$  на простые множители и проверим выполнимость равенства (8.7).

Из равенства (8.7) следует, что

$$\ln |f(x)| = \sum_{i=1}^{s-1} \gamma_i \ln p_i. \quad (8.17)$$

Поэтому предложенный метод позволяет накапливать значения  $\ln p_i$  в ячейках массива и находить те элементы, в которых правая часть равенства (8.17) близка к величине  $|f(x)|$ .

Легко видеть, что описанный нами метод может быть модифицирован таким образом, чтобы учитывать факт делимости значений многочлена  $f(x)$  на отличные от единицы степени простых  $p \in \mathcal{B}_B$ . Так, зная значения  $x_1, x_2$ , при которых выполнено сравнение  $f(x) \equiv 0 \pmod{p}$ , легко найти значения, при которых будет выполнено сравнение  $f(x) \equiv 0 \pmod{p^\alpha}$  для целого  $\alpha > 1$ . Мы предлагаем читателю воспользоваться результатами раздела 3.5 и самостоятельно модифицировать предложенную последовательность действий.

Описанный нами метод решета существенно снижает трудоемкость поиска соотношений (8.16), в которых правая часть удовлетворяет равенству (8.7): без использования решета мы должны раскладывать на множители все  $\delta$  значений многочлена  $f(x)$  при  $x \in \mathcal{I}$ . В случае применения решета мы раскладываем на множители лишь те значения многочлена  $f(x)$ , которые заведомо имеют маленькие простые делители; таких значений существенно меньше  $\delta$ .

#### 8.4.1 MPQS — метод нескольких многочленов

Неприятная особенность алгоритма Померанса заключается в определении длины интервала  $\mathcal{I}$ . Если интервал слишком большой, то значения многочлена  $f(x)$  становятся очень большими (существенно больше, чем в алгоритме непрерывных дробей) и недостаточно часто раскладываются в произведение элементов факторной базы. С другой стороны, если интервал  $\mathcal{I}$  слишком мал, то количество найденных соотношений (8.16) может оказаться недостаточным.

Наиболее очевидным решением данной проблемы является использование в алгоритме решета не одного многочлена  $f(x)$ , а нескольких многочленов, выбранных случайным образом. Кроме того, целесообразно фиксировать длину интервала  $\mathcal{I}$  так, чтобы значения многочленов на данном интервале не превышали некоторой величины, например, такой же, как в методе непрерывных дробей.

Эти идеи были высказаны, независимо, Питером Монтгомери (Peter Montgomery), а также Джеймсом Девисом (James A. Davis) и Дианой Холдридж (Diane B. Holdridge), реализовавшими алгоритм квадратичного решета на практике, см. работу [22]. В 1987 году вышла статья Роберта Сильвермена (Robert D. Silverman), см. [50], в которой был предложен эффективный алгоритм построения многочленов. В настоящее вре-



мя алгоритм Сильвермена называют алгоритмом квадратичного решета с несколькими многочленами (MPQS – multiple polynomial quadratic sieve).

Рассмотрим многочлен  $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$  с положительным старшим коэффициентом  $a > 0$ . Будем считать, что для дискриминанта данного многочлена выполнено сравнение  $D = b^2 - 4ac \equiv 0 \pmod{m}$ , то есть выполнено равенство  $D = km$  при некотором натуральном  $k$ . Используя рассуждения, аналогичные приведенным в начале раздела 8.2.5, будем считать, что дискриминант многочлена  $f(x)$  и параметр  $k$  связаны равенствами

$$b^2 - 4ac = D = \begin{cases} km, & \text{если } k \equiv m \pmod{4}, \\ 4km, & \text{иначе.} \end{cases}$$

Воспользовавшись утверждением теоремы 4.2, мы можем записать сравнение

$$f(x) \equiv a(x - e)^2 \pmod{m}, \quad \text{где } e \equiv -\frac{b}{2a} \pmod{m},$$

или

$$af(x) \equiv (ax + b)^2 \pmod{m}, \quad (8.18)$$

последнее сравнение является сравнением Крайчика. Легко видеть, что предложенный Померансом многочлен  $f(x) = (x + h)^2 - m$  является частным случаем рассматриваемого класса многочленов.

Поскольку выполнено условие  $a > 0$ , то многочлен  $f(x)$  имеет минимум, который достигается в точке  $x = -\frac{b}{2a}$ . Выберем эту точку в качестве середины интервала  $\mathcal{I}$ , на котором рассматриваются значения многочлена  $f(x)$ , и определим его длину  $\delta$  таким образом, чтобы абсолютные значения многочлена  $f(x)$  в точке минимума и на границах интервала совпадали. Тогда выполнены равенства

$$\left| f\left(-\frac{b}{2a}\right) \right| = f\left(-\frac{b}{2a} - \frac{\delta}{2}\right) = f\left(-\frac{b}{2a} + \frac{\delta}{2}\right). \quad (8.19)$$

Поскольку  $f\left(-\frac{b}{2a}\right) = -\frac{D}{4a}$ , а  $f\left(-\frac{b}{2a} - \frac{\delta}{2}\right) = f\left(-\frac{b}{2a} + \frac{\delta}{2}\right) = -\frac{D}{4a} + \frac{a\delta^2}{4}$ , то из условия (8.19) следует равенство

$$a\delta = \sqrt{2D}. \quad (8.20)$$

Полученное равенство связывает между собой старший коэффициент многочлена  $f(x)$  и длину интервала  $\mathcal{I}$ , на котором проходит поиск значений, удовлетворяющих равенству (8.7). Стоит отметить, что из (8.20)

следует, что на всем интервале  $\mathcal{I}$  выполнена оценка

$$|f(x)| \leq \frac{\delta}{4\sqrt{2}} \sqrt{D}. \quad (8.21)$$

Заметим, что при  $\delta > 8\sqrt{2}$  эта оценка хуже, чем у метода непрерывных дробей, см. (8.4).

Поскольку величины  $a, \delta$  являются положительными целыми числами, то при практических вычислениях равенство (8.20) не может быть достигнуто. Поэтому величина  $\delta$  фиксируется, а равенство (8.20) заменяется неравенством  $a \leq \left\lfloor \frac{\sqrt{2D}}{\delta} \right\rfloor$ .

Зафиксируем значения параметров  $D$  и  $\delta$  и опишем процедуру выбора коэффициентов многочлена  $f(x)$ . Вначале выберем нечетное простое число  $d$  такое, что  $\left(\frac{D}{d}\right) = 1$  и  $d \leq \left\lfloor \sqrt{\frac{\sqrt{2D}}{\delta}} \right\rfloor$ .

Мы определим параметр  $a$  равенством  $a = d^2$ , тогда из (8.18) следует сравнение

$$f(x) \equiv \left( \frac{ax + b}{d} \right)^2 \pmod{m}.$$

Мы снова получили сравнение Крайчика, в котором левая часть удовлетворяет неравенству (8.21).

Из равенств  $b^2 - 4ac = D$  и  $a = d^2$  следует сравнение

$$D \equiv b^2 \pmod{4d^2},$$

которое мы будем использовать для определения коэффициента  $b$ .

Воспользуемся утверждениями теорем 3.4, 3.5 и определим величину  $b \pmod{d^2}$ . Поскольку мы выбрали нечетное простое число  $d$  таким образом, что выполнено равенство  $\left(\frac{D}{d}\right) = 1$ , то  $D$  является квадратичным вычетом по модулю  $d$ .

Воспользовавшись алгоритмом Тонелли-Шенкса, см. алгоритм 4.2, найдем величины  $b_i$ , удовлетворяющие сравнению  $x^2 \equiv D \pmod{d}$ . Теперь, воспользовавшись сравнением 3.18 при  $f(x) = x^2 - D$ , определим параметр  $b$  равенством

$$b = b_i + td, \quad \text{где} \quad t \equiv \frac{D - b_i^2}{2db_1} \pmod{d}, \quad i \in \{1, 2\}. \quad (8.22)$$

Поскольку величина  $D$  удовлетворяет сравнениям  $D \equiv 0, 1 \pmod{4}$ , а величина  $b$  должна удовлетворять сравнению  $b^2 \equiv D \pmod{4}$ , мы получаем, что выбор индекса  $i$  в равенстве (8.22) должен производиться

таким образом, чтобы  $b$  было четным, если  $D \equiv 0 \pmod{4}$ , и нечетным – в противном случае.

Напоследок заметим, что свободный член  $c$  многочлена  $f(x)$  определяется исходя из равенства  $c = \frac{b^2 - D}{4d^2}$ .

## ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ

Основные свойства индексов - метод согласования - логарифмирование в группе составного порядка - метод Поллига-Хеллмана - метод Полларда - метод Госпера - субэкспоненциальный метод логарифмирования - решение систем линейных сравнений - вывод асимптотической оценки трудоемкости.

Рассмотрим методы решения задачи дискретного логарифмирования в мультипликативной группе конечного поля  $\mathbb{F}_p$ .

**Определение 9.1.** Пусть заданы простое число  $p$  и вычет  $a$ , показатель которого по модулю  $p$  равен  $m$ , то есть  $\text{ord}_p a = m$  и  $m | p - 1$ . Пусть задан вычет  $b$ , удовлетворяющий сравнению

$$a^x \equiv b \pmod{p}. \quad (9.1)$$

Задача определения вычета  $x \pmod{m}$  называется задачей вычисления индекса элемента  $b$  по основанию  $a$ . В криптографической литературе задача вычисления индекса получила синонимичное название: «задача дискретного логарифмирования».

Для вычета  $x$ , удовлетворяющего сравнению (9.1), принято использовать обозначение

$$x \equiv \text{ind}_a b \pmod{m} \quad \text{или} \quad x \equiv \log_a b \pmod{m} \quad (9.2)$$

и называть его индекс или дискретный логарифм  $b$  по основанию  $a$ .

Из данного выше определения и утверждения леммы 2.4 вытекает, что сравнение (9.1) разрешимо только в том случае, когда вычет  $b$  принадлежит множеству

$$\mathcal{A} = \{1, a, a^2, \dots, a^{q-1}\} \subset \mathbb{F}_p^*,$$

то есть является элементом циклической группы, порожденной элементом  $a$ . Мы будем также говорить, что в этом случае вычет  $b$  принадлежит множеству возможных степеней вычета  $a$  по модулю  $p$ .

Прежде чем описывать методы решения задачи дискретного логарифмирования, мы опишем основные свойства индексов.

**Лемма 9.1.** Пусть задано простое число  $p$  и вычет  $a$ , показатель которого по модулю  $p$  равен  $m$ , то есть  $\text{ord}_p a = m$ . Пусть задан вычет  $b$ , принадлежащий множеству возможных степеней вычета  $a$  по модулю  $p$ . Тогда выполнены следующие утверждения.

1. Выполнено сравнение  $\log_a a \equiv 1 \pmod{m}$ .

2. Пусть для вычета  $b$  выполнено равенство

$$b \equiv b_1^{\alpha_1} \cdots b_n^{\alpha_n} \pmod{p},$$

где  $\alpha_1, \dots, \alpha_n$  произвольные натуральные числа, а вычеты  $b_1, \dots, b_n$  принадлежат множеству  $\mathcal{A}$  возможных степеней вычета  $a$ . Тогда

$$\log_a b \equiv \alpha_1 \log_a b_1 + \cdots + \alpha_n \log_a b_n \pmod{m}.$$

3. Выполнено сравнение  $\log_a b^n \equiv n \log_a b \pmod{m}$ .

4. Пусть для вычетов  $b, c, d \in \mathcal{A}$  выполнено  $d \equiv \frac{b}{c} \pmod{p}$ . Тогда

$$\log_a d = \log_a b - \log_a c \pmod{m}.$$

*Доказательство.* Первое утверждение леммы выполнено по определению. Для доказательства второго утверждения рассмотрим случай, когда  $b \equiv b_1 b_2 \pmod{p}$ . Поскольку вычеты  $b_1$  и  $b_2$  принадлежат множеству возможных степеней вычета  $a$ , то найдутся такие вычеты  $x, y$ , что

$$\begin{aligned} a^x &\equiv b_1 \pmod{p}, & a^y &\equiv b_2 \pmod{p} & \text{или} \\ x &\equiv \log_a b_1 \pmod{m}, & y &\equiv \log_a b_2 \pmod{m}. \end{aligned}$$

Перемножая вычеты  $b_1$  и  $b_2$ , мы получим  $b \equiv b_1 b_2 \equiv a^x \cdot a^y \equiv a^{x+y} \pmod{p}$ . Следовательно, выполнено сравнение

$$\log_a b \equiv \log_a b_1 b_2 \equiv x + y \equiv \log_a b_1 + \log_a b_2 \pmod{m}.$$

Обобщая это сравнение на случай  $b \equiv b_1^{\alpha_1} \cdots b_n^{\alpha_n} \pmod{p}$ , мы получим второе утверждение леммы. Легко видеть, что третье и четвертое утверждения леммы являются следствиями из второго утверждения.  $\square$

**Пример 9.1.** Особо стоит обратить внимание на тот факт, что в условии леммы 9.1 требуется принадлежность вычетов  $b_1, \dots, b_n$  циклической подгруппе, порожденной вычетом  $a$ . Приведем пример, в котором нарушение этого условия приводит к опровержению утверждения леммы.

Рассмотрим уравнение

$$27^x \equiv 520 \pmod{547}$$

и заметим, что  $\text{ord}_{547} 27 = 14$ , то есть, вычет 27 не является первообразным корнем и порождает мультипликативную группу

$$\mathcal{A} = \langle 27 \rangle = \{27, 182, 538, 304, 3, 81, 546, 520, 365, 9, 243, 544, 466, 1\},$$

состоящую из 14 элементов. Легко видеть, что решение нашего уравнения существует и  $x = 8$ .

С другой стороны, выполнено равенство  $520 = 2^3 \cdot 5 \cdot 13$ . Применяя для нахождения неизвестного  $x$  утверждение леммы 9.1, мы должны записать сравнение

$$\log_{27} 520 \equiv 3 \log_{27} 2 + \log_{27} 5 + \log_{27} 13 \pmod{14}. \quad (9.3)$$

Поскольку вычеты 2, 5 и 13 не принадлежат группе  $\mathcal{A}$ , то индексы  $\log_{27} 2$ ,  $\log_{27} 5$  и  $\log_{27} 13$  не существуют, следовательно, правая часть сравнения (9.3) не существует. Таким образом, получено противоречие со вторым утверждением леммы 9.1.

## 9.1 Метод согласования

Долгое время эффективный алгоритм решения задачи дискретного логарифмирования не был известен и при вычислениях использовались заранее подготовленные таблицы индексов. Пример такой таблицы можно найти, например, в монографии [1, стр. 372].

В 1962 году советским математиком Александром Осиповичем Гельфондом был предложен метод, см. [9, гл.6, п.3], который позволил вычислять индексы достаточно эффективно при небольших значениях  $p$ . В русскоязычной литературе этот метод получил название «метода согласования».

Независимо, в 1971 году Даниэль Шенкс (Daniel Shanks), см. [49], предложил аналогичный метод решения задачи дискретного логарифмирования, получивший название «метода больших и малых шагов» (baby steps and giant steps). В настоящее время в литературе используются оба названия метода.

Итак, рассмотрим сравнение (9.1). Если вычет  $b \equiv 1 \pmod{p}$ , то, очевидно, выполнено сравнение  $x \equiv 0 \pmod{m}$  и наша задача решена.

Во всех остальных случаях определим целое число  $h = \lceil \sqrt{m} \rceil$ . Поскольку мы ищем величину  $x$ , для которой  $0 < x < m$ , мы можем воспользоваться утверждением леммы 1.1 и определить такие целые значения  $u$ ,  $v$ , что

$$x = hu - v, \quad 0 < u \leq h, \quad 0 \leq v < h. \quad (9.4)$$

Выполнено сравнение

$$b \equiv a^x \equiv (a^h)^u a^{-v} \pmod{p}, \quad \text{или} \quad ba^v \equiv (a^h)^u \pmod{p},$$

из которого следует, что значения  $u, v$  могут быть найдены перебором в указанных границах, после чего может быть определена величина  $x$ .

Мы организуем перебор следующим образом. Для всех возможных значений  $v = 0, 1, \dots, h-1$  вычислим вычеты  $ba^v \pmod{p}$  и сохраним их в памяти. Далее, вычисляя  $(a^h)^u$  для всех  $u = 1, \dots, h$  будем сравнивать полученные значения со значениями, сохраненными в памяти. Как только будет найдено равенство, мы определим неизвестные  $u, v$ , а следом, используя (9.4), и величину  $x$ .

**Пример 9.2.** Рассмотрим следующую задачу. Необходимо найти  $x$ , удовлетворяющее сравнению  $3^x \equiv 148 \pmod{181}$ , если известно, что выполнено условие  $\text{ord}_{181} 3 = 45$ .

Поскольку показатель величины 3 по модулю 181 равен 45. Следовательно, мы можем определить величину  $h = \lceil \sqrt{45} \rceil = 7$ . Составим таблицу возможных значений величины  $ba^v \pmod{p}$ ,  $v = 0, 1, \dots, 6$  для значений  $a = 3, b = 148$ .

$v$	0	1	2	3	4	5	6
$ba^v$	148	82	65	14	42	126	16

Теперь составим таблицу значений  $(a^h)^u$  при  $a = 3, h = 7$  и  $u = 1, 2, \dots, 7$ .

$u$	1	2	3	4	5	6	7
$(a^h)^u$	15	44	117	126	80	114	81

Легко заметить, что в обеих таблицах содержится одно и то же значение 126. Используя этот факт, мы можем записать сравнение

$$148 \cdot 3^5 \equiv 126 \equiv (3^7)^4 \pmod{181},$$

следовательно,  $u = 4, v = 5$  и мы получаем, что  $x = 7 \cdot 4 - 5 = 23$ . Проверяя, получим сравнение  $3^{23} \equiv 148 \pmod{181}$ .

Укажем некоторые аспекты реализации на ЭВМ метода согласования и одновременно оценим его трудоемкость. На первом шаге мы составляем таблицу, содержащую  $h$  значений – величины  $ba^v \pmod{p}$  для

всех  $v = 0, \dots, h-1$ . Каждый элемент таблицы представляет собой пару значений  $(v, ba^v)$ , которые сортируются при вставке в таблицу по возрастанию величины вычета  $ba^v$ . Сортировка производится для оптимизации процедуры поиска значений на втором шаге алгоритма.

Для создания таблицы нам потребуется  $h$  операций умножения вычетов по модулю  $p$ . Кроме того, мы будем выполнять операцию вставки пар значений  $(v, ba^v)$  в таблицу.

Хорошо известно, см. [2, гл.2], что трудоемкость процедуры вставки элемента в отсортированный массив оценивается величиной<sup>1</sup>  $\log_2 n$  операций сравнения элементов таблицы, где  $n$  число элементов массива. Следовательно, при создании таблицы нам потребуется

$$\log_2 1 + \log_2 2 + \log_2 3 + \dots + \log_2 h = \log_2 h! < \log_2 h^h = h \log_2 h$$

операций сравнения вычетов по модулю  $p$ . При этом на практике операция сравнения выполняется существенно быстрее операции умножения.

На втором шаге алгоритма нам необходимо вычислить не более  $h$  вычетов  $a^{hu}$  при  $u = 0, \dots, h-1$ . Это потребует не более  $h$  операций умножения вычетов по модулю  $p$ . Следовательно, трудоемкость метода согласования не более  $2h \log_2 h$  операций с вычетами по модулю  $p$ .

Как правило, трудоемкостью операций сравнения вычетов пренебрегают. В этом случае трудоемкость метода согласования составляет  $2h$  операций с вычетами по модулю  $p$  или  $O(\sqrt{m})$ . При этом объем памяти, необходимой для хранения таблицы промежуточных значений, также составляет  $O(\sqrt{m})$ .

## 9.2 Логарифмирование в подгруппе составного порядка

В методе согласования информация о том, является ли число  $m$  простым или составным, не существенна. Однако, если мы хотим снизить трудоемкость решения задачи дискретного логарифмирования, информация о разложимости показателя элемента  $a$  является важной.

Зафиксируем некоторое натуральное число  $n > 1$  и рассмотрим задачу дискретного логарифмирования

$$a^x \equiv b \pmod{p}, \quad \text{ord}_p a = m = q^n,$$

<sup>1</sup>Здесь используется традиционная логарифмическая функция, а не функция, определенная равенствами (9.2).



дополнительно считая, что показатель элемента  $a$  по модулю  $p$  есть степень некоторого простого числа  $q$ .

Мы можем свести исходную задачу логарифмирования к решению  $n$  задач в подгруппе порядка  $q$  и снизить трудоемкость решения задачи с величины  $O(\sqrt{q^n})$  до величины  $O(n\sqrt{q})$ . Впервые метод сведения был опубликован Стефаном Полигом (Stephen Pohlig) и Мартином Хеллманом (Martin Hellman) в 1978 году в статье [41].

Мы будем искать целое значение  $x$ , удовлетворяющее неравенствам  $0 < x < q^n$  и представимое в виде

$$x = x_0 + x_1q + \dots + x_{n-1}q^{n-1}, \quad (9.5)$$

где  $0 \leq x_i < q$  для всех  $i = 0, 1, \dots, n-1$ . В начале мы последовательно определим неизвестные коэффициенты  $x_0, \dots, x_{n-1}$ , а после, используя равенство (9.5), определим искомую величину  $x$ .

Обозначим  $\alpha \equiv a^{q^{n-1}} \pmod{p}$ . Легко проверить, что  $\text{ord}_p \alpha = q$ , а кроме того,

$$\begin{aligned} \alpha^x &\equiv \alpha^{x_0} \alpha^{x_1q} \dots \alpha^{x_{n-1}q^{n-1}} \equiv \\ &\equiv \alpha^{x_0} (\alpha^q)^{x_1} (\alpha^q)^{x_2q} \dots (\alpha^q)^{x_{n-1}q^{n-2}} \equiv \alpha^{x_0} \pmod{p}. \end{aligned}$$

С другой стороны,

$$\alpha^x \equiv (a^{q^{n-1}})^x \equiv (a^x)^{q^{n-1}} \equiv b^{q^{n-1}} \pmod{p},$$

и мы получаем, что  $x_0$  есть решение задачи дискретного логарифмирования

$$\alpha^{x_0} \equiv b_0 \pmod{p}, \quad (9.6)$$

где  $\alpha \equiv a^{q^{n-1}} \pmod{p}$ ,  $\text{ord}_p \alpha = q$  и  $b_0 \equiv b^{q^{n-1}} \pmod{p}$ .

Используя схожие рассуждения, мы можем найти остальные неизвестные коэффициенты  $x_1, \dots, x_{n-1}$ . Для этого определим последовательность вычетов

$$a_i \equiv a^{q^{n-i-1}} \pmod{p}, \quad i = 0, 1, \dots, n-1.$$

Легко видеть, что  $a_0 \equiv \alpha \pmod{p}$ ,  $a_{n-1} \equiv a \pmod{p}$ , а также выполнены сравнения

$$a_i^{q^j} \equiv a^{q^{n-i-1}q^j} \equiv a^{q^{n-i+j-1}} \equiv a_{i-j} \pmod{p}, \quad (9.7)$$

при  $j < i$  и  $a_i^{q^j} \equiv 1 \pmod{p}$  при  $j > i$ .

Вывод формулы для определения величины  $x_i$  проведем по индукции. Предположим, что для всех индексов, меньших чем  $i$ , искомые величины

найжены. Тогда, учитывая сравнение (9.7) и тот факт, что  $\text{ord}_p a_0 = q$ , получаем

$$a_i^x \equiv a_i^{x_0} a_i^{x_1 q} \cdots a_i^{x_{n-1} q^{n-1}} \equiv a_i^{x_0} a_{i-1}^{x_1} \cdots a_0^{x_i} \pmod{p}. \quad (9.8)$$

С другой стороны, выполнено сравнение

$$a_i^x \equiv (a^{q^{n-i-1}})^x \equiv (a^x)^{q^{n-i-1}} \equiv b^{q^{n-i-1}} \pmod{p}.$$

Обозначим  $b_i \equiv b^{q^{n-i-1}} \pmod{p}$  и запишем сравнение (9.8) в виде

$$a_0^{x_i} \equiv b_i a_i^{-x_0} a_{i-1}^{-x_1} \cdots a_1^{-x_{i-1}} \pmod{p}.$$

Поскольку  $a_0 \equiv \alpha \pmod{p}$ , мы получили, что величина  $x_i$  есть решение задачи дискретного логарифмирования

$$\alpha^{x_i} \equiv \beta_i \pmod{p}, \quad \text{где} \quad \beta_i \equiv b_i (a_i^{x_0} a_{i-1}^{x_1} \cdots a_1^{x_{i-1}})^{-1} \pmod{p}, \quad (9.9)$$

для всех  $i = 0, 1, \dots, n-1$ . Суммируя изложенное, предложим следующий алгоритм.

### Алгоритм 9.1 (Алгоритм Полига-Хеллмана)

**Вход:** Простое число  $p$  и вычеты  $a, b$ , удовлетворяющие сравнению  $a^x \equiv b \pmod{p}$ . Кроме того, выполнено равенство  $\text{ord}_p a = q^n$  для некоторого простого  $q$  и натурального  $n > 1$ .

**Выход:** Дискретный логарифм  $x \equiv \log_a b \pmod{q^n}$ .

1. Определить  $a_{n-1} = a, b_{n-1} = b$ .
2. Для всех  $i$  от 1 до  $n-1$  выполнить
  - 2.1. Определить  $a_{n-i-1} \equiv a_{n-i}^q \pmod{p}$  и  $b_{n-i-1} \equiv b_{n-i}^q \pmod{p}$ .
3. Для всех  $i$  от 0 до  $n-1$  выполнить
  - 3.1. Если  $i > 0$ , то определить  $\gamma \equiv a_i^{x_0} a_{i-1}^{x_1} \cdots a_1^{x_{i-1}} \pmod{p}$ .  
Иначе определить  $\gamma = 1$ .
  - 3.2. Определить  $\beta_i \equiv b_i \gamma^{-1} \pmod{p}$ .
  - 3.3. Используя, например, метод согласования, найти дискретный логарифм  $x_i$ , удовлетворяющий сравнению  $a_0^{x_i} \equiv \beta_i \pmod{p}$ .
4. Определить  $x = x_0 + x_1 q + \cdots + x_{n-1} q^{n-1}$ . □

Приведенный алгоритм требует около  $3n$  ячеек памяти для хранения промежуточных значений. Оценим его трудоемкость. Для вычисления значений  $a_i, b_i$  на втором шаге алгоритма нам потребуется не более  $2n$  операций умножения вычетов по модулю  $p$ .

На третьем шаге мы в цикле вычисляем значение вычета  $\gamma$  – не более  $n \log_2 q$  операций умножения, значение вычета  $b$  – около  $\log_2 p$  операций

деления вычетов, см. раздел 2.1, а также находим дискретный логарифм  $x_i$ . Трудоемкость последнего действия зависит от метода дискретного логарифмирования и для метода согласования составляет  $O(\sqrt{q})$ .

Трудоемкость последнего, четвертого шага алгоритма не превосходит  $n^2 \log_2 q$  операций умножения. Суммируя, получаем, что трудоемкость алгоритма 9.1 есть величина  $O(n^2 \log_2 q + n\sqrt{q})$ .

Теперь мы можем рассмотреть задачу дискретного логарифмирования

$$a^x \equiv b \pmod{p}, \quad \text{ord}_p a = m, \quad (9.10)$$

в случае, когда нам известно полное разложение показателя элемента  $a$  на простые сомножители, то есть  $m = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ , где  $q_i$  различные простые, а  $\alpha_i$  некоторые натуральные числа.

Фиксируем некоторый индекс  $i$ ,  $1 \leq i \leq n$ , и определим вычет  $c_i$  сравнением  $c_i \equiv a^{\frac{m}{q_i^{\alpha_i}}} \pmod{p}$ . Поскольку  $\text{ord}_p a = m$ , то для вычета  $c_i$  выполнено условие  $\text{ord}_p c_i = q_i^{\alpha_i}$ .

С другой стороны, возводя в сравнении (9.10) правую и левую часть в степень  $\frac{m}{q_i^{\alpha_i}}$ , получим сравнение

$$c_i^x \equiv b^{\frac{m}{q_i^{\alpha_i}}} \pmod{m}. \quad (9.11)$$

Поскольку показатель элемента  $c_i$  равен  $q_i^{\alpha_i}$ , то мы можем воспользоваться алгоритмом 9.1 и найти величину  $x_i$ , сравнимую с  $x$  по модулю  $q_i^{\alpha_i}$ . Проведенные нами рассуждения верны для любого индекса  $i$ , следовательно, мы можем для каждого  $i$  найти величину  $x_i$ , а после воспользоваться китайской теоремой об остатках и найти величину  $x$ .

Таким образом, неизвестное  $x$  удовлетворяет системе сравнений

$$\begin{cases} x \equiv x_1 \pmod{q_1^{\alpha_1}}, \\ \dots \\ x \equiv x_n \pmod{q_n^{\alpha_n}}, \end{cases}$$

где дискретные логарифмы  $x_i$  удовлетворяют сравнениям (9.11). Следует добавить, что метод решения сравнения (9.10) для случая, когда показатель элемента  $a$  есть составное число, был впервые найден Василием Ильичом Нечаевым в 1965 году, см. [9, гл.6, п.3].

**Пример 9.3.** Рассмотрим еще раз задачу из примера 9.2 и найдем  $x$ , удовлетворяющий сравнению  $3^x \equiv 148 \pmod{181}$ . Поскольку нам известно, что  $\text{ord}_{181} 3 = 45 = 3^2 \cdot 5$ , мы будем искать  $x$  как решение системы сравнений

$$\begin{cases} x \equiv x_1 \pmod{5}, \\ x \equiv x_2 \pmod{3^2}, \end{cases}$$

где  $x_1$  и  $x_2$  удовлетворяют сравнениям

$$135^x \equiv 42 \pmod{181}, \quad 62^x \equiv 65 \pmod{181}.$$

Первое сравнение получено путем возведения правой и левой частей исходного сравнения в степень  $3^2$ , второе сравнение – путем возведения в степень 5.

Решим первое сравнение. Поскольку  $\text{ord}_{181} 135 = \frac{45}{9} = 5$  мы можем в явном виде выписать всё множество возможных степеней вычета 135 по модулю 181.

$i$	1	2	3	4	5
$135^i$	135	125	42	59	1

Из таблицы сразу следует необходимое значение.

Для решения второго сравнения  $63^x \equiv 65 \pmod{181}$  воспользуемся алгоритмом 9.1. В нашем случае значения параметров алгоритма равны  $n = 2$  и  $q = 3$ , поэтому мы будем искать неизвестное  $x$  в виде  $x = x_0 + 3x_1$ .

Определим константы

$$\begin{aligned} a_0 &\equiv 132 \pmod{181}, & a_1 &\equiv 62 \pmod{181}, \\ b_0 &\equiv 48 \pmod{181}, & b_1 &\equiv 65 \pmod{181}. \end{aligned}$$

Величина  $x_0$  является решением сравнения  $132^x \equiv 48 \pmod{181}$ . Поскольку  $\text{ord}_{181} 132 = 3$ , то  $132^2 \equiv 48 \pmod{181}$ ,  $132^3 \equiv 1 \pmod{181}$  и мы можем сразу определить  $x_0 = 2$ .

Прежде чем вычислять  $x_1$ , определим величину  $\beta_1$ , удовлетворяющую сравнению

$$\beta_1 \equiv 65 \cdot (62^2)^{-1} \equiv 132 \pmod{181}.$$

Мы получили, что величина  $x_1$  является решением сравнения  $132^x \equiv 132 \pmod{181}$ , откуда сразу вытекает равенство  $x_1 = 1$  и тот факт, что решение второго сравнения равно 5.

Возвратимся к исходному сравнению  $3^x \equiv 148 \pmod{181}$  и найдем неизвестное  $x$  из системы сравнений

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 5 \pmod{3^2}. \end{cases}$$

Воспользовавшись алгоритмом Гарнера, см. алгоритм 2.3, получим ответ  $x = 23$ .

## 9.3 Вероятностные методы

Снова рассмотрим сравнение

$$a^x \equiv b \pmod{p}, \quad \text{ord}_p a = m. \quad (9.12)$$

Как мы показали в предыдущем разделе, решение задачи дискретного логарифмирования сводится к рассмотрению одного или нескольких случаев, при которых показатель  $m$  элемента  $a$  является простым числом.

Мы привели метод согласования, который позволяет найти дискретный логарифм в этом случае. Однако при больших значениях  $m$  требование наличия объема памяти порядка  $\sqrt{m}$ , делает метод согласования неприменимым на практике. Способ обойти это требование был впервые предложен в 1978 году Джоном Поллардом (John Pollard) в статье [43].

### 9.3.1 Метод Полларда-Флойда

Используя идеи, схожие с теми, на которых основан метод факторизации, см. раздел 7.4, Поллард предложил алгоритм, базирующийся на свойстве случайных отображений заикливаться при действии на конечных множествах.

Для обнаружения заикливаний Поллард предложил использовать тест Роберта Флойда (Robert W Floyd), см. [29, п.3.1, задача 6b]. В современной литературе метод дискретного логарифмирования Полларда-Флойда часто называют  $\rho$ -методом Полларда.

Зафиксируем натуральное число  $s \geq 3$ . Рассмотрим конечное множество возможных степеней вычета  $a$

$$\mathcal{A} = \{1, a, \dots, a^{m-1}\},$$

состоящее из  $m$  элементов, и разделим его на  $s$  непересекающихся интервалов  $\mathcal{I}_0, \mathcal{I}_1, \dots, \mathcal{I}_{s-1}$  таким образом, что  $\mathcal{A} = \cup_{i=0}^{s-1} \mathcal{I}_i$ . Способ деления, например, может быть следующим: мы будем говорить, что элемент  $z \in \mathcal{A}$  принадлежит интервалу  $\mathcal{I}_i$ , если  $z \equiv i \pmod{s}$ .

Для всех значений  $i = 0, 1, \dots, s-1$  зафиксируем произвольные постоянные  $\alpha_i, \beta_i \in \mathbb{Z}_m$ , однозначно связанные с интервалом  $\mathcal{I}_i$ , и определим отображение множества  $\mathcal{A}$  в себя

$$f(z) : \mathcal{A} \rightarrow \mathcal{A},$$

$$f(z) \equiv za^{\alpha_i}b^{\beta_i} \pmod{p}, \quad \text{если } z \in \mathcal{I}_i,$$

где вычеты  $a, b$  определены сравнением (9.12).

Легко показать, что функция  $f(z)$  определена корректно для любого набора величин  $\alpha_n, \beta_n$ . Если  $z \in \mathcal{A}$ , то найдется такой вычет  $\gamma$  по модулю  $m$ , что  $z \equiv a^\gamma \pmod{p}$ . Тогда, учитывая равенство (9.12), получаем  $f(z) \equiv a^\gamma a^{\alpha_i} a^{x\beta_i} \equiv a^{\gamma+\alpha_i+x\beta_i} \pmod{p}$  для некоторого индекса  $n$  и  $f(z) \in \mathcal{A}$ .

Выберем случайный вычет  $k_0 \pmod{m}$  и определим элемент  $z_0 \in \mathcal{A}$  сравнением  $z_0 \equiv a^{k_0} \pmod{p}$ . Рассмотрим последовательность элементов  $z_0, z_1, \dots$ , определяемую соотношением

$$z_{n+1} = f(z_n), \quad n = 0, 1, \dots \quad (9.13)$$

Из определения функции  $f$  следует, что

$$z_{n+1} \equiv z_n a^{\alpha_i+x\beta_i} \pmod{p}, \quad z_n \in \mathcal{I}_i \pmod{s},$$

следовательно, каждый элемент последовательности  $z_0, z_1, \dots$  может быть представлен в виде

$$z_{n+1} \equiv z_n a^{\alpha_i+x\beta_i} \equiv a^{A_{n+1}+xB_{n+1}} \pmod{p},$$

где  $A_{n+1}, B_{n+1}$  определяются равенствами

$$A_{n+1} = \alpha_i + A_n, \quad B_{n+1} = \beta_i + B_n, \quad A_0 = k_0, \quad B_0 = 0, \quad (9.14)$$

то есть являются суммами соответствующих коэффициентов  $\alpha_i$  и  $\beta_i$ , определяемых функцией  $f(z)$ .

Поскольку множество  $\mathcal{A}$  конечно, то последовательность  $z_0, z_1, \dots$  заиклится и найдутся такие два индекса  $n, r$ , что  $z_n \equiv z_r \pmod{p}$  или

$$a^{A_n+xB_n} \equiv a^{A_r+xB_r} \pmod{p}.$$

Последнее сравнение позволяет нам выразить неизвестное  $x$ . Действительно, выполнено

$$A_n + xB_n \equiv A_r + xB_r \pmod{m} \quad \text{или} \quad x \equiv \frac{A_n - A_r}{B_r - B_n} \pmod{m}.$$

Для обнаружения сравнения  $z_n \equiv z_r \pmod{p}$  Поллард предложил использовать метод Флойда определения циклов в последовательностях, то есть проверять, выполнено ли сравнение

$$z_n \equiv z_{2n} \pmod{p},$$

для всех индексов  $n$ .

### Алгоритм 9.2 (Алгоритм Полларда-Флойда)

**Вход:** Простое число  $p$ , вычеты  $a, b$ , удовлетворяющие сравнению  $a^x \equiv b \pmod{p}$ , где  $\text{ord}_p a = m$ , а также параметр  $s \geq 3$  и отображение  $f(x)$ , задаваемое наборами вычетов  $\alpha_0, \dots, \alpha_{s-1}, \beta_0, \dots, \beta_{s-1}$ .

**Выход:** Дискретный логарифм  $x \equiv \log_a b \pmod{m}$ .

1. Выбрать случайное  $k_0$  такое, что  $0 < k_0 < m$  и определить  $z \equiv a^{k_0} \pmod{p}$ .
2. Определить начальные значения  $A_z = A_y = k_0, B_z = B_y = 0$ .
3. Вычислить  $z = f(z), i \equiv z \pmod{s}$  и определить

$$A_z \equiv A_z + \alpha_i \pmod{m}, \quad B_z \equiv B_z + \beta_i \pmod{m}.$$

4. Вычислить  $t = f(z), y = f(t)$  и  $i \equiv t \pmod{s}, j \equiv y \pmod{s}$ . Определить

$$A_y \equiv A_y + \alpha_i + \alpha_j \pmod{m}, \quad B_y \equiv B_y + \beta_i + \beta_j \pmod{m}.$$

5. Если  $z \not\equiv y \pmod{p}$ , то вернуться на шаг 3.
6. Если  $A_z = A_y$  или  $B_z = B_y$ , то вернуться на шаг 3.
7. Определить  $x$  сравнением  $x \equiv \frac{A_z - A_y}{B_y - B_z} \pmod{m}$ . □

Данный алгоритм носит вероятностный характер, поскольку момент заикливания последовательности  $z_0, z_1, \dots$  зависит как от выбора начального элемента  $z_0$ , так и от коэффициентов  $\alpha_0, \dots, \alpha_{s-1}, \beta_0, \dots, \beta_{s-1}$ .

Если отображение  $f(z)$  ведет себя как случайное, то мы можем ожидать, что для обнаружения момента заикливания нам потребуется вычислить  $O(\sqrt{m})$  элементов последовательности. Случайность отображения  $f(z)$  достигается за счет выбора большого значения параметра  $s$ .

Поллард предложил выбирать  $s = 3$ . Позднейшие эксперименты показали, см. [8], что величина  $s$  зависит от величины  $m$  и должна принимать большие значения, например,  $s = 500$ .

Метод Полларда-Флойда выполняет сравнимое с методом согласования количество операций, но использует лишь ограниченное количество ячеек памяти. Это позволяет реализовывать метод Полларда-Флойда на ЭВМ при больших значениях  $m$ .

### 9.3.2 Метод Госпера

Алгоритм Флойда поиска циклов в последовательностях является простым, но не самым оптимальным. Для задачи дискретного логарифмирования наиболее эффективным<sup>2</sup> методом является алгоритм, предложенный Биллом Госпером (Ralph William Gosper, Jr.).

<sup>2</sup>Обзор методов поиска длин циклов в последовательностях и их криптографических приложений может быть найден в статье [8].

В алгоритме Госпера для поиска двух совпадающих элементов последовательности (9.13)

$$z_{n+1} = f(z_n), \quad n = 0, 1, \dots$$

производится сравнение элемента  $z_n$  с элементами некоторого множества  $M(n)$ .

Для начала напомним, что функция  $\nu_2(z)$  возвращает наибольшую степень двойки, делящую величину  $z$ . Теперь, фиксируем значение  $n > 0$  и поместим в множество  $M(n)$  элементы  $z_{n_0}, z_{n_1}, \dots$  последовательности (9.13), с условием

$$n_k = \max_{r < n} \{r | \nu_2(r+1) = k\}, \quad (9.15)$$

для всех возможных значений  $k = 0, 1, \dots$ . Из определения следует, что множество  $M(n)$  конечно, содержит не более  $\lfloor \log_2 n \rfloor + 1$  чисел и отличается от множества  $M(n+1)$  лишь одним элементом.

**Теорема 9.1** (Госпер, см. [8]). *Пусть заданы параметры  $\lambda$  и  $\tau$ , определяющие длину подхода к циклу и длину цикла последовательности (9.13). Тогда найдутся натуральные индексы  $r$  и  $n = r + \tau$  такие, что*

1. *элемент  $z_r$  принадлежит множеству  $M(n)$  и выполнено равенство  $z_n = z_r$ ,*
2.  $\lambda + \tau \leq n < \lambda + 2\tau$ .

Утверждение теоремы в явном виде задает нам множество  $M(n)$ , в котором содержится элемент  $a_r$  такой, что  $a_r = a_n$ . Более того, теорема позволяет получить оценку сверху на максимальное число элементов последовательности (9.13), которые необходимо вычислить для нахождения указанного равенства.

Мы строим множество  $M(n)$  следующим образом: разобьем последовательность (9.13) на несколько подпоследовательностей так, что первая подпоследовательность содержит все элементы с индексами  $i$  такими, что  $i+1$  нечетно, вторая — элементы индексами  $i$  такими, что  $i+1$  делится в точности на двойку, третья — элементы с индексами  $i$  такими, что  $i+1$  делится в точности на четверку и т.д. Тогда в множество  $M(n)$  входит по одному элементу из каждой подпоследовательности с максимальным индексом, не превосходящим  $n$ . Например, для  $n = 16$  множество  $M(16)$  имеет вид

$$M(16) = \{a_{14}, a_{13}, a_{11}, a_7, a_{15}\}.$$



Мы будем хранить множество  $M(n)$  в массиве  $T$

$$T = T_0, T_1, \dots, T_{\lfloor \log_2 n \rfloor + 1}.$$

Каждый элемент  $T_i$  представляет собой структуру, хранящую элемент множества  $\mathcal{A}$ , а также два элемента  $A, B$ , определенные равенствами (9.14) и являющиеся суммами соответствующих коэффициентов  $\alpha_i$  и  $\beta_i$ . Мы будем обозначать эти данные, соответственно,  $T_i[z]$ ,  $T_i[A]$  и  $T_i[B]$ .

### Алгоритм 9.3 (Алгоритм Госпера)

**Вход:** Простое число  $p$ , вычеты  $a, b$ , удовлетворяющие сравнению  $a^x \equiv b \pmod{p}$ , где  $\text{ord}_p a = m$ , а также параметр  $s \geq 3$  и отображение  $f(x)$ , задаваемое наборами вычетов  $\alpha_0, \dots, \alpha_{s-1}, \beta_0, \dots, \beta_{s-1}$ .

**Выход:** Дискретный логарифм  $x \equiv \log_a b \pmod{m}$ .

1. Выбрать случайное  $k_0$  такое, что  $0 < k_0 < m$  и определить  $z \equiv a^{k_0} \pmod{p}$ , а также  $n = 0, t = 1, A = k_0, B = 0$  и  $T_0[z] = x, T_0[A] = k_0, T_0[B] = 0$ .
2. Вычислить  $z = f(z)$  и  $A \equiv A + \alpha_i \pmod{m}, B \equiv B + \beta_i \pmod{m}$ , для величины  $i$ , удовлетворяющей сравнению  $i \equiv z \pmod{s}$ .
3. Для всех  $i$  от 0 до  $t - 1$  выполнить
  - 3.1. Если  $z = T_i[z]$ , то вычислить  $x \equiv \frac{A - T_i[A]}{T_i[B] - B} \pmod{m}$  и завершить алгоритм.
4. Определить  $n = n + 1$  и  $k = \nu_2(n)$ .
5. Если  $k = t$ , то вычислить  $t = t + 1$ .
6. Определить  $T_k[z] = z, T_k[A] = A, T_k[B] = B$  и вернуться на шаг 2. □

Как следует из утверждения теоремы А.3, приведенный алгоритм затратит на нахождение неизвестной величины  $z$  не более двух периодов последовательности  $z_0, z_1, \dots$ . Однако асимптотическая оценка метода Госпера совпадает с оценкой метода Полларда-Флойда и составляет  $O(\sqrt{m})$ .

## 9.4 Субэкспоненциальный метод

Описанные нами ранее алгоритмы позволяли находить решение задачи дискретного логарифмирования

$$a^x \equiv b \pmod{p}, \quad \text{ord}_p a = m$$

с экспоненциальной сложностью, составляющей величину  $O(\sqrt{m})$ .

Далее мы опишем метод, позволяющий находить неизвестное  $x$  существенно быстрее, а именно, с субэкспоненциальной сложностью от величины  $p$ . Везде далее мы будем подразумевать, что вычет  $a$  является первообразным корнем и порождает все множество  $\mathbb{F}_p^*$  отличных от нуля вычетов по модулю  $p$ .

### 9.4.1 Идеология Крайчика

Излагаемый нами метод был впервые применен<sup>3</sup> в 1926 году Морисом Крайчиком для построения таблиц индексов. Следуя его монографии [31], приведем пример построения начальных значений таблицы индексов для простого числа  $p = 9649$  и первообразного корня  $a = 7$ .

Для начала найдем индексы первых трех простых чисел. Введем обозначения

$$x = \log_7 2, \quad y = \log_7 3, \quad z = \log_7 5$$

и рассмотрим сравнение

$$9600 \equiv -49 \equiv (-1)7^2 \pmod{9649}. \quad (9.16)$$

Запишем величину  $-1 \pmod{9649}$  в виде степени 7. Из малой теоремы Ферма вытекает сравнение  $7^{9648} \equiv 1 \pmod{9649}$ . Следовательно, выполнено одно из сравнений

$$7^{\frac{9648}{2}} \equiv 1 \pmod{9649}, \quad 7^{\frac{9648}{2}} \equiv -1 \pmod{9649}.$$

Поскольку 7 является первообразным корнем, то первое сравнение не может быть выполнено, следовательно, выполнено второе сравнение и

$$-1 \equiv 7^{\frac{9648}{2}} \equiv 7^{4824} \pmod{9649}.$$

Теперь, раскладывая величину 9600 на простые множители, используя утверждение леммы 9.1 и полученное нами выражение для  $-1$ , перепишем сравнение (9.16) в виде

$$2^7 \cdot 3 \cdot 5^2 \equiv 7^{4826} \pmod{9649}.$$

Переходя к индексам, получаем уравнение относительно неизвестных  $x$ ,  $y$  и  $z$

$$7x + y + 2z \equiv 4826 \pmod{9648}. \quad (9.17)$$

Аналогично, рассматривая второе сравнение

$$9604 \equiv -45 \pmod{9649},$$

и замечая, что  $9604 = 2^2 \cdot 7^4$  и  $45 = 3^2 \cdot 5$ , переходим к индексам и получаем уравнение

$$4 + 2x \equiv 4824 + 2y + z \pmod{9648} \quad \text{или} \quad 2x - 2y - z \equiv 4820 \pmod{9648}. \quad (9.18)$$

---

<sup>3</sup>Автор не берет на себя смелости заявить, что именно Крайчику принадлежит авторство метода. Вместе с тем, автору не известны более ранние публикации данного метода.

Воспользовавшись сравнением  $7^{18} \equiv 7500 \pmod{9649}$  и равенством  $7500 = 2^2 \cdot 3 \cdot 5^4$ , получаем последнее уравнение

$$18 \equiv 2x + y + 4z \pmod{9648}. \quad (9.19)$$

Сравнения (9.17), (9.18) и (9.19) дают нам систему уравнений

$$\begin{cases} 7x + y + 2z \equiv 4826 \pmod{9648}, \\ 2x - 2y - z \equiv 4820 \pmod{9648}, \\ 2x + y + 4z \equiv 18 \pmod{9648}. \end{cases}$$

Уничтожая из первого и третьего сравнений переменную  $z$ , получаем систему

$$\begin{cases} 11x - 3y \equiv 4818 \pmod{9648}, \\ 12x + y \equiv 9634 \pmod{9648}. \end{cases}$$

Теперь, выражая  $y \equiv 9634 - 12x \pmod{9648}$ , получаем сравнение  $47x \equiv 4776 \pmod{9648}$ , следовательно,

$$x = \log_7 2 = 1128, \quad y = \log_7 3 = 5746, \quad \text{и} \quad z = \log_7 5 = 5240. \quad (9.20)$$

Мы нашли индексы маленьких простых чисел 2, 3, 5 и 7. Для построения всей таблицы индексов нам достаточно вычислить индексы только для простых чисел. В силу леммы 9.1 остальные значения могут быть выражены через индексы простых чисел.

Мы не будем вычислять всю таблицу, а найдем только одно значение, например,  $\log_7 43$  — решение сравнения  $7^x \equiv 43 \pmod{9649}$ . Для поиска неизвестного значения рассмотрим сравнение

$$7^{10} \equiv 774 \pmod{9649}.$$

Воспользуемся разложением на простые множители  $774 = 2 \cdot 3^2 \cdot 43$  и запишем полученное сравнение для индексов

$$10 \equiv \log_7 2 + 2 \log_7 3 + \log_7 43 \pmod{9648}.$$

Используя найденные ранее значения (9.20), получим необходимое нам значение

$$\log_7 43 \equiv 10 - 1128 - 2 \cdot 5746 \equiv 6866 \pmod{9648}.$$

Резюмируя изложенный пример, заметим: предложенный Крайчиком метод состоял из двух этапов. Вначале вычислялись индексы маленьких простых чисел, а потом через найденные значения выражались все остальные индексы. И хотя Крайчик не указал алгоритм в явном виде, его метод был известен и неоднократно использовался при вычислениях таблиц индексов, см., например, [52].

### 9.4.2 Алгоритм Адлемана

Предложенный Крайчиком метод оформился в алгоритм, пригодный к реализации на ЭВМ, только в 1979 году, когда независимо друг от друга вышли работы Ральфа Меркля (Ralph C. Merkle) [35] и Леонарда Адлемана (Leonard Adleman) [14]. В настоящее время предложенный в этих работах алгоритм принято называть по фамилии второго автора.

Пусть задана пара вычетов  $a$  и  $b$ , удовлетворяющих сравнению

$$a^x \equiv b \pmod{p},$$

а кроме того, вычет  $a$  является первообразным корнем по модулю  $p$ .

Вначале выберем натуральное число  $B > 0$  и сформируем факторную базу

$$\mathcal{B}_B = \{p_1, p_2, \dots, p_s\},$$

множество всех простых чисел, не превосходящих  $B$ . Точное значение параметра  $B$  мы определим несколько позже, при выводе оценки трудоемкости алгоритма.

Далее вычислим соотношения, необходимые для отыскания индексов простых чисел  $p_1, \dots, p_s$ , принадлежащих факторной базе. Для получения одного соотношения необходимо выполнить следующие шаги.

1. Вычислить случайное целое число  $k$ , удовлетворяющее неравенству  $0 < k < p$ , и определить абсолютно-наименьший вычет  $w$ , удовлетворяющий сравнению

$$a^k \equiv w \pmod{p}, \quad -\frac{p-1}{2} \leq w \leq \frac{p-1}{2}.$$

2. Разложить вычет  $w$  в произведение простых чисел, принадлежащих факторной базе

$$w = (-1)^{\gamma_0} p_1^{\gamma_1} \cdots p_s^{\gamma_s}, \quad p_1, \dots, p_s \in \mathcal{B}_B, \quad (9.21)$$

где величины  $\gamma_0, \gamma_1, \dots, \gamma_s$  являются некоторыми натуральными числами. Если разложение (9.21) невозможно, то вернуться к первому шагу и выбрать новое значение  $k$ .

3. Поскольку  $a$  первообразный корень, то  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ . Воспользовавшись этим фактом, а также полученным разложением (9.21), записать сравнение

$$a^k \equiv (-1)^{\gamma_0} p_1^{\gamma_1} \cdots p_s^{\gamma_s} \pmod{p}$$

или, переходя к индексам,

$$k \equiv \frac{\gamma_0(p-1)}{2} + \gamma_1 \log_a p_1 + \dots + \gamma_s \log_a p_s \pmod{p-1}. \quad (9.22)$$

Полученное сравнение является одним соотношением, относительно неизвестных  $\log_a p_1, \dots, \log_a p_s$ .

После того, как указанным способом будет найдено не менее чем  $s$  соотношений, необходимо решить полученную систему сравнений в кольце вычетов по модулю  $p-1$ . Для решения полученной системы можно использовать алгоритм, который мы опишем ниже в разделе 9.4.3. Найденные решения системы сравнений будут являться значениями индексов для простых чисел  $p_1, \dots, p_s$ , принадлежащих факторной базе.

На последнем шаге алгоритма мы находим неизвестное значение  $x = \log_a b$ . Для этого необходимо выбрать целое число  $l$ , удовлетворяющее неравенству  $0 < l < p$ , такое, что

$$ba^l \equiv w \pmod{p} \quad \text{и} \quad w = (-1)^{\gamma_0} p_1^{\gamma_1} \dots p_s^{\gamma_s}, \quad p_1, \dots, p_s \in \mathcal{B}_B.$$

Тогда, переходя к индексам, получаем сравнение

$$\log_a b + l \equiv \frac{\gamma_0(p-1)}{2} + \gamma_1 \log_a p_1 + \dots + \gamma_s \log_a p_s \pmod{p-1},$$

из которого выражается неизвестная величина  $\log_a b$ .

Нам остается добавить, что описанный метод может быть применен для решения задачи дискретного логарифмирования в случае, когда  $a$  не является первообразным корнем по модулю  $p$

$$a^x \equiv b \pmod{p}, \quad \text{ord}_p a = m|p-1.$$

В этом случае, согласно теореме 2.8, найдется вычет  $c$ , являющийся первообразным корнем по модулю  $p$ . Для вычисления вычета  $c$  можно использовать алгоритм 2.4.

Воспользовавшись описанным выше методом, можно найти неизвестные индексы  $u, v$  такие, что

$$c^u \equiv a \pmod{p}, \quad c^v \equiv b \pmod{p}.$$

Тогда неизвестное  $x$  удовлетворяет сравнению  $ux \equiv v \pmod{m}$ .

### 9.4.3 Решение систем линейных сравнений

Рассмотрим более подробно вопрос решения систем линейных сравнений, возникающих при вычислениях индексов. Предположим, что нам задана система из  $t$  сравнений, где  $t \geq s$

$$\begin{cases} \gamma_{11}x_1 + \gamma_{12}x_2 + \cdots + \gamma_{1s}x_s \equiv \gamma_{1s+1} \pmod{p-1}, \\ \cdots \\ \gamma_{t1}x_1 + \gamma_{t2}x_2 + \cdots + \gamma_{ts}x_s \equiv \gamma_{ts+1} \pmod{p-1}, \end{cases} \quad (9.23)$$

относительно неизвестных  $x_1, \dots, x_s$ . При этом, неизвестные представляют собой искомые индексы  $\log_a p_1, \dots, \log_a p_s$ , а каждое сравнение системы представляет собой соотношение вида (9.22).

Опишем метод, который может рассматриваться как аналог метода Гаусса для решения систем линейных уравнений в кольцах. Нам требуется следующая лемма.

**Лемма 9.2.** Пусть  $\gamma_1, \gamma_2$  вычета кольца  $\mathbb{Z}$ . Тогда найдутся целые числа  $a, b, c, d$  такие, что  $ad - bc = 1$  и выполнено матричное равенство

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} z \\ 0 \end{pmatrix}, \quad z = \text{НОД}(\gamma_1, \gamma_2).$$

*Доказательство.* Нам достаточно предъявить значения величин  $a, b, c, d$  и проверить выполнимость утверждений леммы. Воспользуемся утверждением леммы Безу, см. лемму 2.2, и определим целые числа  $a, b$  равенством

$$a\gamma_1 + b\gamma_2 = z, \quad z = \text{НОД}(\gamma_1, \gamma_2),$$

а величины  $c, d$  равенствами

$$c = -\frac{\gamma_2}{z}, \quad d = \frac{\gamma_1}{z}.$$

Тогда выполнены равенства

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = \frac{1}{z}(a\gamma_1 + b\gamma_2) = 1$$

и  $c\gamma_1 + d\gamma_2 = \frac{1}{z}(\gamma_2\gamma_1 - \gamma_1\gamma_2) = 0$ , из которых следует утверждение леммы.  $\square$

Вернемся к системе сравнений (9.23) и рассмотрим матрицу

$$\Gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1s} & \gamma_{1s+1} \\ & & \cdots & & \\ \gamma_{t1} & \gamma_{t2} & \cdots & \gamma_{ts} & \gamma_{ts+1} \end{pmatrix},$$

составленную из коэффициентов и свободных членов системы (9.23). Мы будем также записывать матрицу  $\Gamma$  в виде столбца строк

$$\Gamma = \begin{pmatrix} \bar{\gamma}_1 \\ \bar{\gamma}_2 \\ \dots \\ \bar{\gamma}_t \end{pmatrix}, \quad \bar{\gamma}_i = (\gamma_{i1}, \gamma_{i2}, \dots, \gamma_{is+1}).$$

Фиксируем два индекса  $i, j$  и для матрицы  $\Gamma$  определим преобразование  $F_{ij}(\Gamma, a, b, c, d)$ , зависящее от четырех параметров  $a, b, c$  и  $d$

$$\Gamma = \begin{pmatrix} \bar{\gamma}_1 \\ \dots \\ \bar{\gamma}_i \\ \dots \\ \bar{\gamma}_j \\ \dots \\ \bar{\gamma}_t \end{pmatrix} \rightarrow \begin{pmatrix} \bar{\gamma}_1 \\ \dots \\ a\bar{\gamma}_i + b\bar{\gamma}_j \\ \dots \\ c\bar{\gamma}_i + d\bar{\gamma}_j \\ \dots \\ \bar{\gamma}_t \end{pmatrix},$$

где

$$a\bar{\gamma}_i + b\bar{\gamma}_j = (a\gamma_{i1} + b\gamma_{j1} \pmod{p-1}, \dots, a\gamma_{is} + b\gamma_{js} \pmod{p-1}).$$

Если  $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$ , то преобразование  $F_{ij}$  обратимо в кольце  $\mathbb{Z}_{p-1}$  и не изменяет множество решений системы сравнений (9.23). Из доказательства леммы 9.2 вытекает способ построения таких квадратных матриц.

Теперь можно привести алгоритм, который последовательно применяет введенное нами преобразование  $F_{ij}$  и приводит матрицу  $\Gamma$  к верхнетреугольному виду.

#### Алгоритм 9.4 (Алгоритм гауссового исключения)

**Вход:** Матрица  $\Gamma$ , соответствующая системе сравнений (9.23).

**Выход:** Матрица  $\Gamma$ , приведенная к верхнетреугольному виду.

**1. Для всех  $i$  от 1 до  $s-1$  выполнить**

**1.1. Для всех  $j$  от  $i+1$  до  $t-1$  выполнить**

1.1.1 Если одновременно  $\gamma_{ii} \equiv 0 \pmod{p-1}$  и  $\gamma_{ji} \equiv 0 \pmod{p-1}$ , то перейти к следующему значению  $j$ .

1.1.2 Вычислить целые числа  $a, b, c$  и  $d$ , удовлетворяющие условиям леммы 9.2, для вычетов  $\gamma_{ii}$  и  $\gamma_{ji}$ .

1.1.3 Применить к матрице  $\Gamma$  преобразование  $F_{ij}(\Gamma, a, b, c, d)$ .

□

В ходе выполнения внутреннего цикла обнуляются все элементы матрицы  $\Gamma$ , расположенные в  $i$ -м столбце ниже  $i$ -го элемента, то есть элементы  $\gamma_{i+1,i}, \gamma_{i+2,i}, \dots, \gamma_{ti}$ . Если выполнено  $\gamma_{ii} \equiv 0 \pmod{p-1}$ , то в ходе применения преобразования  $F_{ij}$  величина  $\gamma_{ii}$  будет заменена на первую отличную от нуля величину  $\gamma_{ji}$   $i < j < t$ .

После приведения матрица  $\Gamma$  примет вид

$$\Gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1s-1} & \gamma_{1s} & \gamma_{1,s+1} \\ 0 & \gamma_{22} & \cdots & \gamma_{2s-1} & \gamma_{2s} & \gamma_{2,s+1} \\ & & \cdots & & & \\ 0 & 0 & & 0 & \gamma_{rs} & \gamma_{r,s+1} \\ 0 & 0 & \cdots & 0 & 0 & \gamma_{r+1,s+1} \\ & & \cdots & & & \\ 0 & 0 & \cdots & 0 & 0 & \gamma_{t,s+1} \end{pmatrix}.$$

Величина  $r$ , удовлетворяющая неравенству  $1 < r \leq s$ , определяет ранг системы (9.23). Для того чтобы найти решение задачи дискретного логарифмирования, должно выполняться равенство  $r = s$ . В противном случае  $s - r$  неизвестных могут принимать произвольные значения в кольце  $\mathbb{Z}_{p-1}$ , что не позволяет однозначно определить величины  $\log_a p_1, \dots, \log_a p_s$ .

Далее, если хотя бы одна из величин  $\gamma_{r+1,s+1}, \dots, \gamma_{t,s+1}$  отлична от нуля, то система несовместна и решение не существует. При решении задачи дискретного логарифмирования неизвестные значения существуют, поэтому система (9.23) должна являться совместной.

Таким образом, при выполнении условий  $r = s$  и  $\gamma_{r+1,s+1} \equiv \dots \equiv \gamma_{t,s+1} \equiv 0 \pmod{p-1}$  решение системы может быть найдено путем применения обратного хода, то есть из системы сравнений

$$\begin{cases} x_s & \equiv \gamma_{s,s}^{-1} \gamma_{s,s+1} \pmod{p-1}, \\ x_{s-1} & \equiv \gamma_{s-1,s-1}^{-1} (\gamma_{s-1,s+1} - \gamma_{s-1,s} x_s) \pmod{p-1}, \\ & \dots \\ x_1 & \equiv \gamma_{1,1}^{-1} (\gamma_{1,s+1} - \gamma_{1,s} x_s - \dots - \gamma_{1,2} x_2) \pmod{p-1}. \end{cases} \quad (9.24)$$

В общем случае, согласно теореме 2.1, число решений системы (9.24) не превосходит величины

$$\text{НОД}(\gamma_{s,s}, p-1) \cdot \text{НОД}(\gamma_{s-1,s-1}, p-1) \cdots \text{НОД}(\gamma_{1,1}, p-1).$$

При решении задачи дискретного логарифмирования, в силу единственности решения, должен существовать только один набор значений  $x_1, \dots, x_s$ , удовлетворяющих системе (9.24).



Оценим трудоемкость алгоритма 9.4, предполагая, для упрощения выкладок, что  $t = s$ . Оценим трудоемкость применения одного преобразования  $F_{ij}$ , зависящего от элементов  $\gamma_{ii}$  и  $\gamma_{ji}$  матрицы  $\Gamma$ . Вначале, для вычисления коэффициентов  $a$  и  $b$ , нам необходимо применить расширенный алгоритм Эвклида. Согласно теореме 1.2, его трудоемкость не превосходит  $3 \log_2 p$  операций деления целых чисел с остатком; при этом целые числа не превосходят  $p$ .

Далее, для преобразования  $i$ -й и  $j$ -й строк матрицы  $\Gamma$  необходимо выполнить  $4(s - i + 1)$  операций умножения вычетов в кольце  $\mathbb{Z}_{p-1}$ . Получаем, что для одного применения преобразования  $F_{ij}$  необходимо выполнить  $3 \log_2 p + 4(s - i + 1)$  операций с вычетами кольца  $\mathbb{Z}_{p-1}$ .

Для обнуления всех элементов, расположенных в  $i$ -м столбце ниже  $i$ -го элемента потребуется  $(s - i)(3 \log_2 p + 4(s - i + 1))$  операций. Учитывая, что индекс  $i$  пробегает все значения от 1 до  $s - 1$ , получаем итоговую трудоемкость алгоритма

$$\begin{aligned} \sum_{i=1}^{s-1} (s - i)(3 \log_2 p + 4(s - i + 1)) &= \\ &= (3 \log_2 p + 4) \sum_{k=1}^{s-1} k + 4 \sum_{k=1}^{s-1} k^2 = O(hs^2), \end{aligned}$$

где  $h = \max\{\log_2 p, s\}$ .

**Пример 9.4.** Для иллюстрации приведенного алгоритма решим систему сравнений из раздела 9.4.1.

$$\begin{cases} 7x + y + 2z \equiv 4826 \pmod{9648}, \\ 2x - 2y - z \equiv 4820 \pmod{9648}, \\ 2x + y + 4z \equiv 18 \pmod{9648}. \end{cases}$$

Соответствующая данной системе матрица, с приведенными по модулю 9648 коэффициентами<sup>4</sup>, будет иметь вид

$$\Gamma = \begin{pmatrix} 7 & 1 & 2 & 4826 \\ 2 & 9646 & 9647 & 4820 \\ 2 & 1 & 4 & 18 \end{pmatrix}.$$

Сперва последовательно применим описанное выше преобразование к первому столбцу и обнулим в нем все элементы, за исключением первого.

<sup>4</sup> Для человеческого восприятия было бы комфортнее использовать отрицательные значения коэффициентов с минимальной абсолютной величиной. Однако в памяти ЭВМ, как правило, используется беззнаковое представление вычетов.

Поскольку для элементов 7 и 2 первого столбца выполнено равенство  $1 \cdot 7 - 3 \cdot 2 = 1$ , то определим параметры  $a = 1$ ,  $b = -3$ ,  $c = -2$  и  $d = 7$ . Тогда матрица преобразуется следующим образом.

$$\begin{pmatrix} 7 & 1 & 2 & 4826 \\ 2 & 9646 & 9647 & 4820 \\ 2 & 1 & 4 & 18 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 7 & 5 & 14 \\ 0 & 9632 & 9637 & 4792 \\ 2 & 1 & 4 & 18 \end{pmatrix}.$$

Аналогично, рассматривая элементы из первой и третьей строк первого столбца, получим равенство  $3 \cdot 1 - 1 \cdot 2 = 1$  и определим параметры  $a = 3$ ,  $b = -1$ ,  $c = -2$  и  $d = 1$ . Преобразование матрицы выглядит следующим образом.

$$\begin{pmatrix} 1 & 7 & 5 & 14 \\ 0 & 9632 & 9637 & 4792 \\ 2 & 1 & 4 & 18 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 20 & 11 & 24 \\ 0 & 9632 & 9637 & 4792 \\ 0 & 9635 & 9642 & 9638 \end{pmatrix}.$$

Теперь применим еще один раз наше преобразование и обнулим элемент, стоящий во втором столбце в третьей строке. Применяя лемму Безу к элементам 9632 и 9635, находим равенство

$$-3212 \cdot 9632 + 3211 \cdot 9635 = 1,$$

следовательно,  $a = -3212$ ,  $b = 3211$ ,  $c = -9635$  и  $d = 9632$ . Тогда преобразование матрицы имеет вид

$$\begin{pmatrix} 1 & 20 & 11 & 24 \\ 0 & 9632 & 9637 & 4792 \\ 0 & 9635 & 9642 & 9638 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 20 & 11 & 24 \\ 0 & 1 & 6418 & 3138 \\ 0 & 0 & 9601 & 4568 \end{pmatrix}.$$

Мы привели матрицу к верхнетреугольному виду и теперь можем найти значения неизвестных  $x$ ,  $y$  и  $z$  из системы сравнений

$$\begin{cases} x + 20y + 11z \equiv 24 & (\text{mod } 9648), \\ y + 6418z \equiv 3138 & (\text{mod } 9648), \\ 9601z \equiv 4568 & (\text{mod } 9648). \end{cases}$$

Третье сравнение дает нам  $z \equiv 5953 \cdot 4568 \equiv 5240 \pmod{9648}$ , второе  $y \equiv 3138 - 6418 \cdot 5240 \equiv 5746 \pmod{9648}$ , а первое сравнение позволяет найти  $x \equiv 24 - 20 \cdot 5746 - 11 \cdot 5240 \equiv 1128 \pmod{9648}$ .

### 9.4.4 Асимптотическая оценка метода

Нам осталось оценить трудоемкость алгоритма, описанного в разделе 9.4.2 и в явном виде определить значение параметра  $s$ , определяющего мощность факторной базы  $\mathcal{B}_B$ . Поскольку алгоритм носит вероятностный характер, мы не можем точно определить его трудоемкость. Вместо этого мы получим асимптотическую оценку, то есть оценку, которая верна при  $p \rightarrow \infty$ .

Для оценки числа операций, необходимых для поиска одного соотношения вида (9.22), нам потребуется следующий результат. Обозначим символом  $\psi(x, y)$  количество натуральных чисел  $n \leq x$ , у которых наибольший простой делитель не превосходит  $y$ .

**Теорема 9.2** (см. [45, §2]). Пусть  $0 < \varepsilon < \frac{1}{2}$  некоторая действительная константа. Если выполнены неравенства

$$\ln^\varepsilon x < \ln y < \ln^{1-\varepsilon} x,$$

то при  $x \rightarrow \infty$  выполнено  $\psi(x, y) = x e^{-u \ln u + o(u \ln u)}$ , где  $u = \frac{\ln x}{\ln y}$ .

Зафиксируем произвольное действительное число  $\alpha > 0$  и определим параметр  $B$  равенством  $B = e^{\alpha \sqrt{\ln p \ln \ln p}}$ . Выберем случайное равновероятное число  $k$ ,  $0 \leq k < p-1$  и определим  $w \equiv a^k \pmod{p}$ .

Согласно утверждению теоремы В.3, вероятность того, что выполнено равенство (9.21), то есть все делители числа  $w$  не превосходят величины  $B$ , оценивается величиной  $\frac{\psi(p, B)}{p}$ . Следовательно, для нахождения одного соотношения (9.22) необходимо выработать  $\frac{p}{\psi(p, B)}$  случайных чисел. Обозначим  $u = \frac{\ln p}{\ln B}$ , тогда

$$u = \frac{\ln p}{\alpha \sqrt{\ln p \ln \ln p}} = \frac{\sqrt{\ln p}}{2\sqrt{\ln \ln p}}, \quad \ln u = \frac{\ln \ln p}{2} - \ln \alpha - \frac{\ln \ln \ln p}{2},$$

и мы получаем, что

$$\frac{p}{\psi(p, B)} = e^{u \ln u} = e^{\frac{1}{2\alpha} \sqrt{\ln p \ln \ln p} - o(\sqrt{\ln p \ln \ln p})},$$

при  $p \rightarrow \infty$ .

Для каждого случайного  $k$  нам надо проверить существует ли для вычета  $w$  разложение (9.21), то есть разделить  $w$  на все простые числа  $p_1, \dots, p_s$ . Поскольку нам надо найти не менее  $s$  соотношений, то получаем, что суммарная трудоемкость построения матрицы  $\Gamma$ , образованной соотношениями вида (9.22), составляет

$$O\left(s^2 e^{\frac{1}{2\alpha} \sqrt{\ln p \ln \ln p}}\right)$$

операций с вычетами, не превосходящими  $p$ . Величина  $s$  представляет собой количество простых чисел, не превосходящих  $B$ . Для упрощения расчетов мы будем считать, что величина  $s$  имеет тот же порядок, что и  $B$ , то есть  $s = O(B)$ .

Как мы показали ранее, трудоемкость решения системы сравнений составляет  $O(s^3)$  операций. Таким образом, мы получаем, что для нахождения индексов маленьких простых чисел, принадлежащих факторной базе  $\mathcal{B}_B$ , составляет

$$O\left(e^{\left(2\alpha + \frac{1}{2\alpha}\right)\sqrt{\ln p \ln \ln p}}\right) + O\left(e^{3\alpha\sqrt{\ln p \ln \ln p}}\right).$$

Для того чтобы оба слагаемых приняли одинаковый порядок, нам надо минимизировать величину функции  $\max\left\{3\alpha, 2\alpha + \frac{1}{2\alpha}\right\}$  при  $\alpha > 0$ . Легко видеть, что экстремум функции  $2\alpha + \frac{1}{2\alpha}$  находится в точке  $\alpha = \frac{1}{2}$  и этот экстремум – минимум. Поскольку функция  $3\alpha$  монотонно возрастает, получаем, что искомый минимум достигается в точке  $\alpha = \frac{1}{2}$ .

Таким образом, трудоемкость вычисления индексов маленьких простых составляет

$$O\left(e^{\frac{3}{2}\sqrt{\ln p \ln \ln p}}\right) = L\left(\frac{1}{2}, \frac{3}{2}, p\right),$$

при  $B = e^{\frac{1}{2}\sqrt{\ln p \ln \ln p}}$  и  $s = O(B)$ .

Читателю остается, в качестве упражнения, показать, что трудоемкость определения неизвестного  $x \equiv \log_a b \pmod{m}$  не превосходит полученной нами величины.

## 9.5 Двучленные сравнения

В заключение главы рассмотрим еще одну задачу, тесно связанную с задачей дискретного логарифмирования. Пусть  $p$  нечетное простое число, а  $n$  и  $b$  целые числа. Необходимо найти вычет  $x$ , удовлетворяющий сравнению

$$x^n \equiv b \pmod{p}. \quad (9.25)$$

Ранее, в 4-й лекции, мы рассматривали частный случай данного уравнения для случая  $n = 2$ . Теперь рассмотрим обобщение.

**Определение 9.2.** Целое число  $b$  называется  $n$ -степенным вычетом или вычетом степени  $n$ , если сравнение (9.25) разрешимо. В противном случае число  $b$  называется  $n$ -степенным невычетом.

При  $n = 2, 3, 4$  применяются также термины квадратичный, кубический и биквадратичный вычет или невычет.

Ответ на вопрос о том, является ли число  $b$  вычетом или невычетом, существенно зависит от величины  $n$ . Рассмотрим случай, когда  $\text{НОД}(n, p-1) = 1$ . С помощью расширенного алгоритма Эвклида вычислим вычет  $u$ , удовлетворяющий сравнению  $un \equiv 1 \pmod{p-1}$ , и определим неизвестное  $x$  сравнением  $x \equiv b^u \pmod{p}$ . Легко видеть, что найденное значение удовлетворяет сравнению (9.25). Действительно,

$$x^n \equiv b^{un} \equiv b \pmod{p}. \quad (9.26)$$

В общем случае верна следующая теорема.

**Теорема 9.3.** Пусть  $p$  нечетное простое число,  $n$  целое число и  $d = \text{НОД}(n, p-1)$ . Обозначим символом  $q$  показатель числа  $b$  по модулю  $p$ . Тогда сравнение (9.25)

$$x^n \equiv b \pmod{p}$$

разрешимо тогда и только тогда, когда  $q \mid \frac{p-1}{d}$ .

В случае, когда сравнение разрешимо имеется ровно  $d$  не сравнимых по модулю  $p$  решений.

*Доказательство.* В начале определим величины  $s$  и  $e$  равенствами

$$p-1 = ds, \quad n = de$$

и предположим, что сравнение (9.25) разрешимо. Тогда найдется вычет  $x$  для которого, в силу малой теоремы Ферма, будет выполнено сравнение

$$b^s \equiv x^{ns} \equiv (x^{ds})^e \equiv 1 \pmod{p}.$$

Из полученного сравнения и третьего утверждения леммы 2.4 следует, что условие  $q \mid s = \frac{p-1}{d}$  является необходимым.

Теперь покажем, что этого условия достаточно для существования  $d$  не сравнимых между собой по модулю  $p$  вычетов, удовлетворяющих сравнению (9.25). Мы дадим доказательство, позволяющее предъявить решения в явном виде.

Согласно теореме 2.8 найдется некоторый вычет  $g$ , являющийся первообразным корнем по модулю  $p$ . Для его построения можно воспользоваться алгоритмом 2.4.

Поскольку, в силу леммы 2.4, показатель вычета  $b$  делит величину  $\varphi(p) = p-1$ , то найдется некоторое целое число  $h$ , удовлетворяющее равенству  $p-1 = hq$ . Определим вычет  $a$  сравнением  $a \equiv g^h \pmod{p}$ .

Используя первое утверждение леммы 2.5 получаем, что показатели вычетов  $a$  и  $b$  совпадают. Тогда, согласно утверждению теоремы 2.10 выполнено сравнение

$$a^z \equiv b \pmod{p} \quad (9.27)$$

для некоторого натурального  $z$  такого, что  $\text{НОД}(z, q) = 1$ . Для нахождения величины  $z$  можно воспользоваться любым алгоритмом дискретного логарифмирования, описанным в настоящей лекции.

Заметим, что выполнены условия

$$p - 1 = ds, \quad p - 1 = hq \quad \text{и} \quad q|s.$$

Таким образом, мы можем сделать вывод, что  $d|h$ , то есть для некоторого  $l$  выполнено равенство  $h = dl$ . Теперь рассмотрим уравнение

$$yn \equiv zh \pmod{p - 1}.$$

относительно неизвестной величины  $y$ . Согласно утверждению теоремы 2.1, указанное сравнение разрешимо, поскольку  $d = \text{НОД}(n, p - 1) | zh$ . Имеется ровно  $d$  решений

$$y = t + ks, \quad t \equiv zle^{-1} \pmod{s}, \quad k = 0, 1, \dots, d - 1. \quad (9.28)$$

Определим искомые неизвестные сравнением

$$x \equiv g^y \pmod{p} \quad (9.29)$$

для всех возможных значений  $y$ , определенных равенством (9.28). Легко видеть, что величины (9.29) удовлетворяют сравнению (9.25). Действительно,

$$x^n \equiv g^{ny} \equiv g^{zh} \equiv a^z \equiv b \pmod{p}.$$

Теорема доказана. □

В ходе доказательства теоремы мы предъявили последовательность шагов, которая позволяет в явном виде предъявить все решения сравнения (9.25). Однако, для этого нам необходимо вычислять произвольный первообразный корень по модулю  $p$ , а также решать задачу дискретного логарифмирования в циклической группе, порожденной элементом показателя  $s$ . При больших значениях величины  $s$  это может быть достаточно трудоемким.

С другой стороны, как видно из примера приведенного перед формулировкой теоремы, для некоторых значений  $n$  существует полиномиальный от величины  $p$  алгоритм поиска решений сравнения (9.25). Обобщим наш пример и докажем следующий результат.

**Следствие 1.** Пусть показатель элемента  $b$  по модулю нечетного простого числа  $p$  равен  $q$ . Если для некоторого натурального  $n$  выполнены условия

$$\text{НОД}(n, q) = 1 \quad \text{и} \quad q|s,$$

где  $d = \text{НОД}(n, p-1)$ ,  $s = \frac{p-1}{d}$ , то сравнение (9.25) разрешимо и имеет ровно  $d$  несовместных между собой решений.

Определим величину  $u$  сравнением  $un \equiv 1 \pmod{q}$ , а вычет  $s$  — сравнением  $s \equiv g^s \pmod{p}$ , где  $g$  произвольный первообразный корень по модулю  $p$ . В этом случае, решения сравнения (9.25) удовлетворяют

$$x \equiv b^u c^k \pmod{p}, \quad k = 0, \dots, d-1.$$

*Доказательство.* Разрешимость сравнения (9.25) и существование  $d$  различных решений, очевидно, следуют из утверждения теоремы 9.3.

Поскольку  $g$  является первообразным корнем по модулю  $p$ , то, согласно первому утверждению леммы 2.5, показатель вычета  $s$  равен  $\frac{p-1}{s} = d$ . Следовательно, учитывая первое утверждение леммы 2.4, получаем, что все вычеты

$$1, c, c^2, \dots, c^{d-1},$$

несовместны между собой по модулю  $p$  и удовлетворяют условию

$$(c^k)^d \equiv (g^{\frac{p-1}{d}})^{kd} \equiv 1^k \equiv 1 \pmod{p}.$$

Таким образом, учитывая, что показатель вычета  $b$  по модулю  $p$  равен  $q$ , получаем

$$x^n \equiv b^{un} (c^k)^{de} \equiv b \pmod{p}, \quad k = 0, \dots, d-1,$$

где величина  $e$  удовлетворяет равенству  $n = de$ . □

## СХЕМЫ АСИММЕТРИЧНОГО ШИФРОВАНИЯ

Схема шифрования RSA - Определение параметров схемы RSA - Алгоритм Винера и методы компрометации схемы RSA - Схема шифрования RSA-OAEP - Схема шифрования Рабина - Эквивалентность задач факторизации и вычисления квадратного корня - Схема шифрования ЭльГамала.

В этой лекции мы кратко остановимся на простейших криптографических приложениях, которые используют методы теории чисел – мы рассмотрим вопросы шифрования передаваемых по каналам связи сообщений. Традиционно считается, что начало исследованиям в этой области криптографии положил доклад Уайтфилда Диффи (Whitfield Diffie) и Мартина Хеллмана (Martin Hellman), сделанный в июне 1976 года [23].

В декабре 1997 года в сети Internet была опубликована посмертная статья Джеймса Эллиса<sup>1</sup> (James H. Ellis), согласно которой аналогичные результаты были получены несколькими годами ранее. Исследования были начаты еще в шестидесятых годах, проводились в британском агентстве правительственной связи и, очевидно, были засекречены.

Мы начнем наше изложение с описания схем шифрования информации и будем считать, что абонент Б отправляет абоненту А некоторое сообщение  $\xi$ . Для шифрования сообщения используется некоторый ключ — открытый ключ получателя информации (абонента А), доступный любому желающему отправить сообщение. Для расшифрования сообщения используется секретный ключ, известный только одному получателю сообщения. При этом существует математическая зависимость между открытым и секретными ключами, которая используется для эффективной реализации алгоритма расшифрования.

Использование двух различных, связанных между собой ключей и привело к названию *асимметричная схема шифрования*. В англоязычной литературе обычно используется другой термин — схема шифрования с открытым ключом (*public-key cryptosystem*), вытекающий из существования открытого, известного всем ключа.

---

<sup>1</sup> Джеймс Эллис (1927-1997) — британский инженер и криптограф, в шестидесятые-семидесятые годы работал на правительство своей страны. Возглавлял исследования в области асимметричной криптографии или «шифровании без секрета» (non-secret encryption). Краткий исторический очерк, написанный Эллисом, можно найти в сети Internet [24].



## 11.1 Схема шифрования RSA. Теория

Согласно статье Эллиса, первый вариант данной схемы был разработан сотрудником британской спецслужбы GCHQ<sup>2</sup> Клиффордом Коксом (Clifford Cocks) в ноябре 1973 года [20].

Для зашифрования сообщения  $\xi$  необходимо определить модуль схемы — нечетное составное число  $m$ , являющееся произведением двух простых чисел  $p$  и  $q$  таких, что

$$\text{НОД}(p, q - 1) = \text{НОД}(q, p - 1) = 1.$$

Число  $m$  является известным и является открытым ключом получателя сообщения, числа  $p$  и  $q$  являются секретными, секретным ключом получателя сообщения, и используются для расшифрования сообщения.

Сообщение  $\xi$  представляется<sup>3</sup> в виде целого числа  $1 < s < m$  и зашифровывается путем вычисления

$$c \equiv s^m \pmod{m}.$$

Вычет  $c$  является шифртекстом и передается по открытым каналам связи получателю сообщения.

Для расшифрования сообщения  $c$  Кокс предложил следующую последовательность действий. В начале вычисляются вычеты  $c_p$  и  $c_q$ , удовлетворяющие сравнениям

$$\begin{aligned} c_p &\equiv c^{z_q} \pmod{p}, & \text{где } z_q &\equiv q^{-1} \pmod{p-1}, \\ c_q &\equiv c^{z_p} \pmod{q}, & \text{где } z_p &\equiv p^{-1} \pmod{q-1}. \end{aligned}$$

Отметим, что вычеты  $c_p$ ,  $c_q$  удовлетворяют сравнениям  $c_p \equiv s \pmod{p}$ ,  $c_q \equiv s \pmod{q}$ . Действительно, учитывая малую теорему Ферма, теорема 2.7 и сравнение  $qz_q \equiv 1 \pmod{p-1}$  получаем, что для вычета  $c_p$  выполнены сравнения

$$c_p \equiv c^{z_q} \equiv s^{pqz_q} \equiv s^p \equiv s \pmod{p}.$$

<sup>2</sup>Government Communication Headquarters - Центр правительственной связи Великобритании, был создан в 1946 году и стал наследником правительственной школы кодов и шифров, созданной для радиоспионажа еще в 1919 году. Центр прославился тем, что именно его специалисты во время второй мировой войны смогли взломать немецкую шифровальную машину «Энигма».

<sup>3</sup>Как правило, в памяти ЭВМ сообщение  $\xi$  представляется в виде последовательности байт  $b_0, b_1, \dots$ , где  $b_k$  целые числа такие, что  $0 \leq b_k < 256$ . В этом случае представление сообщения  $\xi$  в виде числа  $s$  может быть произведено следующим образом  $s = \sum_{k=0} b_k 256^k$ .

Аналогичные сравнения выполнены и для вычета  $c_q$ . Далее, используя китайскую теорему об остатках, теорема 2.3, находим вычет  $s$ , удовлетворяющий системе сравнений

$$\begin{cases} s \equiv c_p \pmod{p}, \\ s \equiv c_q \pmod{q}. \end{cases}$$

Для системы двух сравнений мы можем в явном виде предъявить значение  $s$  в виде

$$s = c_p qv + c_q pu,$$

где целые числа  $u, v$  удовлетворяют равенству  $pu + qv = 1$  и могут быть найдены с помощью расширенного алгоритма Эвклида, см. алгоритм 2.1.

Отметим, что способ предложенный Коксом обладает рядом особенностей. Во первых значения вычетов  $z_p, z_q$ , а также чисел  $u, v$ , могут быть подсчитаны заранее, до получения сообщения  $s$ . Во вторых, при вычислении вычетов  $c_p, c_q$  используется возведение вычета в степень не более чем  $\max\{p, q\}$ , что являлось немаловажным при ручных вычислениях.

Естественным обобщением схемы Кокса является общеизвестная схема RSA, предложенная в 1977 году и опубликованная лишь годом позже в статье [47].

Схема RSA названа по первым буквам фамилий ее авторов - Рона Райвеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Эйдлемана (Leonard Adleman). В несколько модифицированном виде схема RSA активно применяется для шифрования данных в сети Internet и включена в различные международные и национальные стандарты в области информационной безопасности, среди которых можно отметить стандарты IEEE P1363 [?] и PKCS#1 [?].

Как и в схеме Кокса, необходимо определить модуль схемы — целое составное число  $m$ , являющееся произведением двух простых чисел  $p$  и  $q$ , а также секретный ключ  $d$  и открытый ключ  $e$  получателя сообщения, удовлетворяющие сравнению

$$ed \equiv 1 \pmod{\varphi(m)}, \quad 1 < e < \varphi(m), \quad 1 < d < \varphi(m), \quad (11.1)$$

где  $\varphi(m)$  функция Эйлера, определенная равенством (2.12) и удовлетворяющая  $\varphi(m) = (p-1)(q-1)$ .

Сообщение  $\xi$  представляется в виде целого числа  $1 < s < m$  и зашифровывается путем вычисления

$$c \equiv s^e \pmod{m}.$$

Вычет  $c$  является шифртекстом и передается по открытым каналам связи получателю сообщения.

Для расшифрования сообщения  $s$  необходимо вычислить

$$s \equiv c^d \pmod{m}.$$

Последнее сравнение выполнено, поскольку из сравнения (11.1) и теоремы Эйлера, см. теорему 2.6, следует  $c^d \equiv s^{ed} \equiv s^{1 \pmod{\varphi(m)}} \equiv s \pmod{m}$ .

Легко видеть, что схема Кокса является частным случаем схема RSA при  $e \equiv m \pmod{\varphi(m)}$ . Способ расшифрования сообщений в схеме RSA, очевидно, может быть применен и для расшифрования сообщений в схеме Кокса.

Стойкость криптосхемы RSA основывается на трудоемкости решения задачи разложения числа  $m$  на два простых множителя. Как мы показали в предыдущих лекциях, решение этой задачи при больших значениях  $m$  является сложным. Вместе с тем, в схеме RSA присутствуют дополнительные параметры, а именно, секретный и открытый ключи  $d$  и  $e$ , а также собственно сообщение  $s$ , которое зашифровывается и передается по каналам связи. В некоторых случаях удастся использовать эту дополнительную информацию для компрометации схемы. Прежде чем привести несколько примеров, сведем все параметры в одну таблицу.

Известные значения	Неизвестные значения
$m, e, c$	$d, p, q, \varphi(m), s$

### 11.1.1 Факторизация при известном значении $\varphi(m)$

Наиболее простой задачей является определение простых делителей числа  $m$  по известным значениям  $m$  и  $\varphi(m)$ .

Поскольку выполнено  $\varphi(m) = (p-1)(q-1) = m - (p+q) + 1$ , то мы можем рассмотреть систему уравнений относительно неизвестных целых чисел  $p$  и  $q$

$$\begin{cases} p + q = m + 1 - \varphi(m), \\ pq = m \end{cases} \quad (11.2)$$

Согласно теореме Виета получаем, что искомые значения  $p$  и  $q$  являются корнями трехчлена  $f(x) = x^2 - x(m - \varphi(m) + 1) + m$ . Следовательно, знание значения  $\varphi(m)$  сразу приводит нас к разложению числа  $m$  на множители.

### 11.1.2 Факторизация при известном значении $d$

Легко показать, что знание секретного ключа  $d$  схемы RSA также приводит к разложению модуля схемы  $m$  на простые множители. Преж-

де чем привести вероятностный, полиномиальный алгоритм, который находит разложение числа  $m$  на множители, нам потребуется следующая лемма.

**Лемма 11.1.** Пусть  $m$  нечетное, составное число, раскладывающееся в произведение двух простых чисел  $p$  и  $q$ . Представим  $\varphi(m)$  в виде  $\varphi(m) = 2^n t$ . Обозначим символом  $\mathcal{S}$  множество вычетов  $a \in \mathbb{Z}_m$  таких, что  $\text{НОД}(a, m) = 1$  и выполнено одно из двух условий

1.  $a^t \equiv 1 \pmod{m}$ ,
2.  $a^{2^k t} \equiv -1 \pmod{m}$  для некоторого целого  $k$ ,  $0 \leq k \leq n$ ,

тогда мощность множества  $\mathcal{H}$  не превосходит  $\frac{\varphi(m)}{2}$ .

Заметим, что ранее мы рассматривали схожее утверждение, теорема Рабина 6.3, в которой использовалось разложение числа  $m - 1$ .

*Доказательство леммы 11.1.* Из определения функции Эйлера следует, что вычетов  $a$ , взаимно простых с  $m$ , ровно  $\varphi(m)$ , то есть мощность множества  $\mathcal{H}$  не превосходит  $\varphi(m)$ .

Далее, рассмотрим равенства  $p - 1 = 2^{d_p} t_p$ ,  $q - 1 = 2^{d_q} t_q$  и обозначим  $d = \min\{d_p, d_q\}$ . Согласно теореме 3.4, сравнение  $a^t \equiv 1 \pmod{m}$  равносильно системе сравнений

$$\begin{cases} a^t \equiv 1 \pmod{p}, \\ a^t \equiv 1 \pmod{q}, \end{cases} \quad (11.3)$$

число решений которой равно  $\text{НОД}(t, p - 1) \text{НОД}(t, q - 1)$ . Поскольку  $t$  нечетно, мы получаем оценку

$$\begin{aligned} \text{НОД}(t, p - 1) \text{НОД}(t, q - 1) &= \text{НОД}(t, t_p) \text{НОД}(t, t_q) \leq \\ &\leq t_p t_q \leq \frac{p - 1}{2^d} \frac{q - 1}{2^d} = \frac{\varphi(m)}{4^d} = T. \end{aligned}$$

Точно так же можно заметить, что сравнение  $a^{2^k t} \equiv -1 \pmod{m}$  равносильно системе сравнений

$$\begin{cases} a^{2^k t} \equiv -1 \pmod{p}, \\ a^{2^k t} \equiv -1 \pmod{q}, \end{cases} \quad (11.4)$$

для числа решений которой верна оценка

$$\begin{aligned} \text{НОД}(2^k t, p - 1) \text{НОД}(2^k t, q - 1) &= \\ &= 2^k \text{НОД}(t, t_p) \text{НОД}(t, t_q) \leq 4^k T. \end{aligned}$$

Прежде чем подсчитать общее число решений систем (11.3) и (11.4) покажем, что выполнено неравенство  $k < d$ . Поскольку числа  $t, t_p, t_q$  нечетны, то из равенства

$$\varphi(m) = 2^n t = (p-1)(q-1) = 2^{d_p} 2^{d_q} t_p t_q$$

получаем, что  $t_p = \frac{p-1}{2^{d_p}} t$  и  $t = x \frac{p-1}{2^d}$  для некоторого четного, либо равного единице натурального числа  $x$ . Тогда, рассматривая первое сравнение в (11.4) получаем сравнение

$$a^{2^k t} \equiv a^{2^k x \frac{p-1}{2^d}} \equiv (a^{p-1})^{x 2^{k-d}} \equiv -1 \pmod{p},$$

которое, в силу малой теоремы Ферма, разрешимо только при  $k < d$ . Аналогичное условие выполнено и для второго сравнения в (11.4).

Теперь просуммируем число решений систем (11.3) и (11.4), то есть вычетов  $a$ , удовлетворяющих одному из условий леммы. Воспользовавшись равенством  $\sum_{k=0}^n x^k = \frac{1-x^{n+1}}{1-x}$ , получим оценку

$$T + \sum_{k=0}^{d-1} 4^k T = T \left( 1 + \sum_{k=0}^{d-1} 4^k \right) = T \left( 1 + \frac{4^d - 1}{3} \right) \leq T \frac{4^d}{2} = \frac{\varphi(m)}{2},$$

которая завершает доказательство леммы.  $\square$

Утверждение доказанной леммы позволяет нам построить простой алгоритм факторизации числа  $m$ , основанный на следующей идее. Пусть  $a$  вычет, который не удовлетворяет условиям леммы, то есть

$$a^t \not\equiv 1 \pmod{m} \quad \text{и} \quad a^{2^k t} \not\equiv 1 \pmod{m}.$$

Пусть  $k$ ,  $0 \leq k < n$ , максимальное из всех возможных значений, то есть  $a^{2^{k+1}t} \equiv 1 \pmod{m}$ . Такое  $k$  всегда найдется, поскольку, в силу теоремы Эйлера, выполнено сравнение  $2^{2^n t} \equiv 2^{\varphi(m)} \equiv 1$ .

Обозначим  $u \equiv a^{2^k t} \pmod{m}$  и  $v \equiv a^{2^{k+1}t} \pmod{m}$ . Тогда

$$u \not\equiv \pm 1 \pmod{m} \quad \text{и} \quad v \equiv u^2 \equiv 1 \pmod{m}.$$

Таким образом, мы получаем сравнения

$$u^2 \equiv 1 \pmod{m} \quad \text{или} \quad (u-1)(u+1) \equiv 0 \pmod{m},$$

которые позволяют найти делитель числа  $m$ , поскольку либо  $p|(u-1)$ , либо  $q|(u+1)$ . Соберем высказанные выше рассуждения и приведем алгоритм разложения числа  $m$  на множители.

### Алгоритм 11.1 (Факторизация модуля схемы RSA)

**Вход:** Целое, составное число  $m$  — модуль схемы RSA и значения секретного  $d$  и открытого  $e$  ключей схемы RSA.

**Выход:** Простой делитель  $p$  числа  $m$ .

1. Определить  $w = ed - 1$  и представить  $w = 2^nt$ .
2. Выбрать случайное значение  $b$ ,  $0 < b < m$ .
3. Если  $p = \text{НОД}(b, m) > 1$ , то завершить алгоритм.
4. Вычислить  $v \equiv b^t \pmod{m}$ . Если выполнено  $v \equiv 1 \pmod{m}$ , то вернуться на шаг 2. В противном случае определить  $k = 0$ .
5. Пока  $k < n$  выполнить
  - 5.1. Если  $v \equiv -1 \pmod{m}$ , то вернуться на шаг 2.
  - 5.2. Вычислить  $u = v$ ,  $v \equiv u^2 \pmod{m}$ ,  $k = k + 1$ .
  - 5.3. Если  $v \equiv 1 \pmod{m}$ , то перейти к шагу 7.
6. Вернуться на шаг 2.
7. Вычислить  $p = \text{НОД}(u - 1, m)$ .
8. Если  $p > 1$ , то, закончить алгоритм. В противном случае вернуться к шагу 2. □

Ключи схемы RSA удовлетворяют сравнению  $ed \equiv 1 \pmod{m}$ , следовательно на первом шаге алгоритма выполнено равенство  $w = s\varphi(m)$  для некоторого натурального  $s$ . Таким образом вычет  $b$  вычисляемый случайным образом на втором шаге алгоритма удовлетворяет сравнению  $b \equiv a^s \pmod{m}$ , где вычет  $a$  удовлетворяет условиям леммы 11.1.

Согласно утверждению данной леммы, с вероятностью  $\frac{1}{2}$  данный вычет даст нам разложение числа  $m$  на простые сомножители. С увеличением числа выработанных на втором шаге алгоритма вычетов  $b$  вероятность разложения числа  $m$  на множители стремится к единице.

### 11.1.3 Атака Винера на секретный ключ

В 1990 году Майкл Винер (Michael Wiener) в статье [?] предложил полиномиальный от величины  $m$  алгоритм определения секретного ключа  $d$  схемы RSA в случае, если величина  $d$  не достаточно велика. В основе метода лежит следующее утверждение.

**Лемма 11.2.** Пусть  $m = pq$  модуль схемы RSA такой, что простые числа  $p, q$  удовлетворяют неравенству  $p < q < 2p$ . Пусть  $e, d$  открытый и секретный ключи схемы такие, что  $d < \frac{\sqrt[4]{m}}{\sqrt{6}}$ . Тогда дробь  $\frac{k}{d}$  является наилучшим приближением к величине  $\frac{e}{m}$ , где величина  $k$  определяется равенством  $ed = 1 + k\varphi(m)$ .

*Доказательство.* Для доказательства леммы нам потребуется оценить разность

$$\begin{aligned} km - ed &= k(m - \varphi(m)) - 1 = k(pq - (p-1)(q-1)) - 1 = \\ &= k(p+q) - (k+1) < k(p+q). \end{aligned} \quad (11.5)$$

Последнее неравенство выполнено в силу того, что все числа, участвующие в (11.5), положительны.

Поскольку, в силу построения параметров схемы, выполнено неравенство  $e < \varphi(m)$ , то из неравенства  $ed = 1 + k\varphi(m) > k\varphi(m)$  следует, что выполнено неравенство  $d > k$ . Теперь, учитывая неравенства  $p < q < 2q$  и (11.5), получаем

$$\left| \frac{e}{m} - \frac{k}{d} \right| = \frac{|ed - km|}{dm} < \frac{k(p+q)}{dm} < \frac{3kp}{dm} < \frac{3k\sqrt{m}}{dm} = \frac{3k}{d\sqrt{m}} < \frac{3}{\sqrt{m}}.$$

Теперь, вспоминая ограничение на  $d$ , получаем неравенство

$$\left| \frac{e}{m} - \frac{k}{d} \right| < \frac{1}{2d^2}$$

из которого, с учетом теоремы 5.7, следует утверждение леммы.  $\square$

Воспользовавшись утверждением данной леммы и теоремой 5.6, Винер предложил искать пары значений  $k, d$  среди подходящих дробей к дроби  $\frac{e}{m}$ .

Для поиска неизвестного значения  $d$  необходимо выбрать случайный вычет  $s$ , взаимно простой с  $m$ , и вычислить шифртекст  $c \equiv s^e \pmod{m}$ . После чего, используя соотношения (5.6), вычислять подходящие дроби  $\frac{P_n}{Q_n}$ ,  $n = 1, 2, \dots$  до тех пор, пока для некоторой пары открытого и шифрованного текста  $s, c$  не будет выполнено сравнение  $c^{Q_n} \equiv s \pmod{m}$ .

Для определения значения  $d$  также можно воспользоваться и другим тестом. Определить число  $\varphi = \frac{eQ_n - 1}{P_n}$ . Если число  $z$  целое, то необходимо проверить, имеет ли система уравнений (11.2) целочисленные решения  $p$  и  $q$ . Если да, то  $d = Q_n$ , а кроме того, мы получаем разложение числа  $m$  на простые множители.

Оценить число шагов данного алгоритма просто. Из утверждения леммы 5.5 следует, что неравенство  $d = Q_n \geq 2^{\lceil \frac{n-1}{2} \rceil}$ , которое дает нам оценку на  $n$

$$n \leq 2 \left\lceil \frac{n-1}{2} \right\rceil < 2 \log_2 d < 2 \log_2 \left( \frac{\sqrt[4]{m}}{\sqrt{6}} \right) < \frac{\log_2 m}{2}.$$

Далее мы рассмотрим еще несколько методов, позволяющих либо дешифровать передаваемое сообщение  $s$ , либо получить дополнительную информацию о секретных ключах криптосхемы RSA.

### 11.1.4 Случай использования общего модуля

В работе [?] была описана следующая уязвимость. Предположим, что два абонента используют один и тот же модуль  $m$  схемы шифрования RSA, но обладают разными парами открытых и секретных ключей —  $e_1, d_1$  первый абонент и, соответственно,  $e_2, d_2$  второй абонент,

$$e_1 d_1 \equiv 1 \pmod{\varphi(m)}, \quad e_2 d_2 \equiv 1 \pmod{\varphi(m)}.$$

При этом мы будем дополнительно считать, что  $\text{НОД}(e_1, e_2) = 1$ .

Нарушитель может дешифровать сообщение  $s$ , если оно зашифровано дважды — на ключе  $e_1$  и на ключе  $e_2$ . Действительно, пусть нарушителю известны значения

$$t_1 \equiv s^{e_1} \pmod{m} \quad \text{и} \quad t_2 \equiv s^{e_2} \pmod{m}.$$

Тогда, используя расширенный алгоритм Эвклида, алгоритм 2.1, нарушитель вычисляет значения  $u, v$  такие, что

$$ue_1 + ve_2 = 1.$$

Тогда выполнено сравнение

$$s \equiv s^{ue_1 + ve_2} \equiv t_1^u t_2^v \pmod{m},$$

из которого значение открытого текста выражается в явном виде через значения вычетов  $t_1, t_2$  и целых чисел  $u, v$ .

Более того, если два абонента используют один и тот же модуль  $m$ , то каждый из них может определить секретный ключ другого абонента, без разложения числа  $m$  на множители.

Опишем действия второго абонента, которому известны значения  $e_2, d_2$ , но неизвестно значение  $\varphi(m)$ .

Обозначим символом  $w = e_2 d_2 - 1$ , тогда выполнено  $w = k\varphi(m)$  при некотором целом значении  $k$ . Определим

$$h = \text{НОД}(w, e_1) \quad \text{и} \quad z = \frac{e_1}{h}, \quad t = \frac{w}{h}, \quad \text{НОД}(t, e_1) = 1.$$

Тогда выполнено равенство

$$k\varphi(m) = th \quad \text{или} \quad zk\varphi(m) = te_1.$$

Поскольку  $\text{НОД}(e_1, \varphi(m)) = 1$  то, воспользовавшись леммой 1.4 получаем, что

$$\varphi(m) | t \quad \text{или} \quad \varphi(m) = k_1 t,$$



при некотором целом значении  $k_1$ .

Используя расширенный алгоритм Эвклида, алгоритм 2.1, найдем такие целые значения  $u, v$ , что

$$ut + ve_1 = 1,$$

тогда выполнено  $ve_1 \equiv 1 \pmod{t}$  и  $ve_1 \equiv 1 \pmod{\varphi(m)}$ . Следовательно, мы получаем, что  $v$  является искомым значением  $d_1$ .

Изложенные выше соображения привели к тому, что на практике значение открытого ключа  $e$  фиксируется единственным образом для всех абонентов, но каждый абонент сети использует собственное значение модуля  $m$  и секретного ключа  $d$ .

В некоторых криптографических стандартах величину  $e$  предписывается выбирать равной 3 или 65537. В этом случае  $e$  мало и содержит всего две единицы в разложении по степеням двойки. Данное свойство позволяет эффективно реализовать процесс модульного возведения в степень — процесс зашифрования.

### 11.1.5 Случай использования малой экспоненты

Несмотря на высказанные выше соображения, использование малой экспоненты может оказаться опасным. Приведем простой пример.

Определим параметр  $b$  равенством  $b = \lfloor \sqrt[e]{m} \rfloor$ , где  $e$  открытый ключ получателя сообщения. Тогда сообщение  $s$ , удовлетворяющее неравенству  $1 \leq s \leq b$ , может быть определено из соответствующего ему зашифрованного текста  $c$  путем вычисления целозначного корня, то есть  $s = \sqrt[e]{c}$ . Это верно, поскольку  $s^e < m$ .

При небольших значениях  $e$ , например при  $e = 3$ , множество значений  $s$ , удовлетворяющих неравенству  $1 < s \leq b$  становится достаточно большим.

В работе [?] было предложено обобщение данной атаки, которое может быть применено для произвольного значения открытого ключа  $e$ , общего для всех участников обмена зашифрованными сообщениями.

Рассмотрим ситуацию когда одно и тоже сообщение  $s$  направляется нескольким, скажем  $n$ , участникам. В этом случае, нарушитель, перехватывающий зашифрованные сообщения, может составить систему сравнений

$$\begin{cases} s^e \equiv c_1 \pmod{m_1}, \\ \dots \\ s^e \equiv c_n \pmod{m_n}, \end{cases}$$

Используя китайскую теорему об остатках, см. теорему 2.3, нарушитель может вычислить значение  $d \equiv a^e \pmod{\prod_{k=1}^n m_k}$ . В силу того, что  $c_i < m_i$ , мы получим  $s^e < (\min_{i=1, \dots, n} \{m_i\})^e$ , следовательно, при больших значениях  $n$ ,  $n \geq e$ , выполнено неравенство  $(\min_{i=1, \dots, n} \{m_i\})^e < d$  и нарушитель определяет открытый текст  $s$  вычисляя значение  $s = \sqrt[e]{d}$ .

### 11.1.6 Метод итерационного шифрования

Метод итерационного шифрования является методом бесключевого чтения, то есть таким методом, для реализации которого знание секретного ключа не необходимо.

Предположим, что показатель числа  $e$  по модулю  $\varphi(m)$  не велик, то есть целое число  $n$  такое, что

$$e^n \equiv 1 \pmod{\varphi(m)},$$

принимает не очень большое значение, скажем  $n \sim O(\log_2 m)$ .

Тогда нарушитель, имея в своем распоряжении шифртекст  $c$ , может вычислить последовательность вычетов

$$c_{k+1} \equiv c_k^e \pmod{m}, \quad c_0 = c, \quad k = 0, \dots$$

Как только будет выполнено сравнение  $c_k \equiv c \pmod{m}$ , нарушитель сможет определить открытый текст равенством  $s \equiv c_{k-1} \pmod{m}$ .

Легко видеть, что искомый индекс найдется всегда, поскольку

$$c_n \equiv c^{e^n} \equiv c^{1+n\varphi(m)} \equiv c \pmod{m},$$

для некоторого целого  $k$ . При небольших значениях  $n$  данный метод дешифрования эффективен, поскольку его трудоемкость, как легко видеть, составляет  $O(n \log_2 e)$ .

### 11.1.7 Фиксированные точки

Дадим следующее определение.

**Определение 11.1.** Пусть  $m = pq$  модуль схемы RSA, величины  $e, d$  определяют, соответственно, открытый и секретный ключи схемы. Рассмотрим вычет  $s$ , взаимно простой с  $m$ . Мы будем вычет  $s$  фиксированной точкой схемы RSA, если

$$s^e \equiv s \pmod{m}. \quad (11.6)$$

**Лемма 11.3.** *Количество фиксированных точек схемы RSA равно*

$$\text{НОД}(p-1, e-1) \cdot \text{НОД}(q-1, e-1).$$

*Доказательство.* Если нам известно разложение числа  $m$  на простые сомножители, то мы можем в явном виде предъявить все фиксированные точки. Действительно, обозначим  $r = \text{НОД}(p-1, e-1)$ . Поскольку числа  $p-1$  и  $e-1$  четные, то выполнено неравенство  $r \geq 2$ .

Согласно теореме 2.10 найдется вычет  $a$  такой, что  $\text{ord}_p a = r$ . Легко видеть, что для любого вычета  $a_i \equiv a^i \pmod{p}$ ,  $i = 0, \dots, r-1$  выполнено

$$(a_i)^e \equiv a^i (a^i)^{e-1} \equiv (a^i) (a^r)^{i \frac{e-1}{r}} \equiv a_i \pmod{p}.$$

Аналогично, обозначая  $l = \text{НОД}(q-1, e-1)$ , найдем вычет  $b$  такой, что  $\text{ord}_q b = l$ , и определим множество вычетов  $b_j \equiv b^j \pmod{q}$ , где  $j = 0, \dots, l-1$ . Для каждого вычета  $b_j$  выполнено  $(b_j)^e \equiv b_j \pmod{q}$ . Тогда, согласно теореме 3.4, фиксированными точками  $s_{ij}$  будут являться решения систем сравнений

$$\begin{cases} s_{ij} \equiv a_i \pmod{p}, \\ s_{ij} \equiv b_j \pmod{q}, \end{cases} \quad (11.7)$$

для всех  $i = 0, \dots, r-1$  и  $j = 0, \dots, l-1$ . Число предъявленных нами точек, очевидно, равно  $rl = \text{НОД}(p-1, e-1) \cdot \text{НОД}(q-1, e-1)$ .

Покажем, что не существует других фиксированных точек, отличных от предъявленных нами. Пусть  $s$  произвольная фиксированная точка, тогда  $\text{НОД}(p, s) = 1$  и из (11.6) следует сравнение  $s^e \equiv s \pmod{p}$  или  $s^{e-1} \equiv 1 \pmod{p}$ .

Обозначим  $t = \text{ord}_p s$ . Тогда,  $t|e-1$  и, в силу определения показателя,  $t|p-1$ . Следовательно мы получаем, что  $t|\text{НОД}(p-1, e-1) = r$ .

Согласно второму следствию к теореме 2.10, см. стр. 33, вычет  $s$  имеет вид  $a_i \equiv a^i \pmod{p}$  для некоторого натурального  $i$ ,  $1 \leq i < r$ , где  $a$  построенный ранее вычет, показатель которого равен  $r$ .

Аналогично, мы получаем, что  $s \equiv b_j \equiv b^j \pmod{q}$  для некоторого индекса  $j$ . То есть, вычет  $s$  является решением системы сравнений (11.7). Лемма доказана.  $\square$

Следует отметить, что в литературе часто встречается другое утверждение о величине  $\omega$ , см. (Ризель) и (Харин, Берник), а именно

$$\omega = (1 + \text{НОД}(p-1, e-1)) (1 + \text{НОД}(q-1, e-1)).$$

Читателю, в качестве упражнения, предлагается доказать, что это равенство выполнено в случае, если мы рассматриваем все вычеты  $s = 0, 1, \dots, m-1$ , а не только взаимно простые с  $m$ .

### 11.1.8 Случай большого общего делителя

Определим величину  $w$  равенством

$$w = \text{НОД}(p-1, q-1)$$

и будем считать, что значение  $w$  велико и известно нарушителю. В этом случае можно предложить достаточно простой способ вычисления значения функции Эйлера  $\varphi(m)$ . Прежде чем переходить к описанию данного способа заметим, что всегда выполнено условие  $2|w$ , поскольку числа  $p-1$  и  $q-1$  четные.

**Лемма 11.4.** Пусть  $m = pq$  — составное число, раскладывающееся в произведение двух простых чисел. Тогда для любого взаимно простого с  $m$  вычета  $a$ ,  $0 < a < m$ , выполнено

$$\text{ord}_m a \mid \text{НОК}(p-1, q-1).$$

*Доказательство.* Доказательство данной леммы достаточно просто следует из определения показателя числа  $a$  по модулю  $m$ , см. определение 2.7, теоремы Эйлера, см. теорему 2.5, и определения наибольшего общего кратного двух чисел, см. определение 2.10.

Пусть  $r$  некоторое простое число и  $\alpha$  максимальное натуральное число такое, что  $r^\alpha \mid \varphi(m) = (p-1)(q-1)$ . Тогда  $r^\alpha \mid \text{НОК}(p-1, q-1)$ . Следовательно, в силу теоремы Эйлера

$$\text{ord}_m a \mid \varphi(m), \quad \text{ord}_m a \mid \text{НОК}(p-1, q-1).$$

Лемма доказана. □

Заметим, что введенного нами ранее значения  $w$  выполнено равенство

$$\varphi(m) = (p-1)(q-1) = w \text{НОК}(p-1, q-1). \quad (11.8)$$

Определим величины  $v_k$  равенством

$$v_k = d + k \text{НОК}(p-1, q-1), \quad k = 0, 1, \dots, w-1.$$

Тогда для любого значения  $v_k$ , в силу леммы 11.4, выполнено

$$c^{v_k} \equiv c^d \left( c^{\text{НОК}(p-1, q-1)} \right)^k \equiv c^d \equiv s \pmod{m}.$$

Таким образом мы получаем, что существует  $w$  значений  $v_k$ , которые могут быть использованы для расшифрования сообщения  $s$ . В криптографии принято называть такие значения «эквивалентными ключами».

Отметим, что поскольку  $2|w$ , то схема шифрования RSA всегда имеет два эквивалентных секретных ключа.

Теперь вернемся к вопросу об определении значения  $\varphi(m)$ . В силу определения  $w$  получаем, что  $\varphi(m) = w^2x$ . Следовательно

$$x = \frac{\varphi(m)}{w^2} < \frac{m}{w^2}.$$

Обозначим  $h = \frac{[\sqrt{m}]}{w}$  и представим неизвестное значение  $x$  в виде  $\alpha h + \beta$ , где  $0 \leq \alpha, \beta < h$ . Неизвестные значения  $\alpha, \beta$  могут быть найдены методом согласования, аналогично тому, как это было предложено Гельфондом для решения задачи дискретного логарифмирования.

Поскольку выполнено равенство

$$w^2x = \varphi(m) = w \text{НОК}(p-1, q-1),$$

то  $xw = \text{НОК}(p-1, q-1)$  и, в силу леммы 11.4, получаем сравнения

$$s^{xw} \equiv 1 \pmod{m}, \quad \text{или} \quad (s^{wh})^\alpha \equiv (s^{-w})^\beta \pmod{m},$$

которые используются в методе согласования. Сложность поиска значений  $\alpha, \beta$  оценивается величиной порядка  $O\left(\frac{[\sqrt{m}]}{w}\right)$  и существенно зависит от величины параметра  $w$ .

На практике нарушителю неизвестно значение  $w$ . Вместе с тем, это значение известно разработчику параметров схемы RSA, который вырабатывает значения  $m, e, d$  и предоставляет их конечному пользователю. Таким образом может быть реализована «закладка», то есть ситуация при которой разработчик параметров, зная значение величины  $w$ , может выступать в качестве нарушителя и дешифровывать передаваемые сообщения. В свою очередь, пользователь всегда может проверить факт наличия такой закладки, используя алгоритм факторизации, изложенный нами в разделе 11.1.2.

### 11.1.9 Случай алгебраической зависимости открытых текстов

Для дешифрования сообщений в схеме RSA может быть использован факт существования алгебраической зависимости между открытыми текстами.

Предположим, что нарушителю известны два шифртекста  $c_1$  и  $c_2$  такие, что для соответствующих им открытых текстов  $s_1$  и  $s_2$  выполнено соотношение

$$s_2 \equiv \alpha s_1 + \beta \pmod{m},$$

при некоторых, известных нарушителю значениях  $\alpha, \beta$ . В начале нарушитель определяет многочлен

$$f(x) = x^e - c_1, \quad f(x) \in \mathbb{Z}_m[x].$$

Как легко видеть открытый текст  $s_1$  является корнем многочлена  $f(x)$ . Далее, для многочлена

$$g(x) = (\alpha x + \beta)^e - c_2, \quad f(x) \in \mathbb{Z}_m[x]$$

значение  $s_1$  также является корнем, следовательно, многочлен  $h(x) = \text{НОД}(f(x), g(x))$  нетривиален и имеет степень, большую либо равную единицы.

Предположим, что многочлен  $h(x)$  имеет второй корень, скажем  $s_3$ , отличный от  $s_1$ . Тогда  $s_3$  является и корнем многочлена  $f(x)$ , следовательно,

$$s_3^e \equiv c_1 \equiv s_1^e \pmod{m},$$

что равносильно

$$b^e \equiv 1 \pmod{m}, \quad \text{при} \quad b \equiv s_1 s_3^{-1} \pmod{m}.$$

Поскольку  $e < \varphi(m)$ , то из последнего неравенства и теоремы Эйлера, см. теорему 2.6, следует, что  $e | \varphi(m)$ , а это невозможно, поскольку  $\text{НОД}(e, \varphi(m)) = 1$ . Таким образом многочлен  $h(x) = (x - s_1)$ , что позволяет нарушителю найти значение  $s_1$ , а после, и значение  $s_2$ .

Аналогичный подход верен и для случая, когда сообщение  $s_2$  удовлетворяет соотношению

$$\begin{aligned} s_2 &\equiv u_0 + u_1 s_1 + \dots + u_n s_1^n \pmod{m}, \\ s_2 &\equiv u(s_1), \quad u(x) \in \mathbb{Z}_m[x], \quad \deg u(x) = n. \end{aligned}$$

В этом случае, многочлен  $g(x)$  определяется равенством  $g(x) = u(x)^e - c_2$ .

### 11.1.10 Свойство мультипликативности и контроль целостности

Для двух произвольных открытых текстов  $s_1$  и  $s_2$  в схеме RSA верно следующее сравнение

$$(s_1 s_2)^e \equiv s_1^e s_2^e \equiv c_1 c_2 \pmod{m},$$

то есть шифртекст произведения двух открытых текстов является произведением двух соответствующих шифртекстов. Данное свойство называется свойством мультипликативности. Рассмотрим простую атаку, которая иллюстрирует использование данного свойства схемы RSA.

Пусть  $c \equiv s^e \pmod{m}$  шифртекст, соответствующий открытому тексту  $s$ . Нарушитель вычисляет случайное значение  $k$ , взаимно простое с  $m$ , и заменяет сообщение  $s$  на сообщение  $v \equiv ck^e \pmod{m}$ . Получатель сообщения расшифровывает модифицированное сообщение и вычисляет значение

$$u \equiv v^d \equiv c^d k^{ed} \equiv sk \pmod{m},$$

которое представляется ему истинным сообщением, хотя на самом деле оно изменено нарушителем. Если у нарушителя появляется возможность узнать сообщение  $u$ , то он сразу вычисляет исходное сообщение  $s$ , используя сравнение  $s \equiv uk^{-1} \pmod{m}$ . Данную атаку на сообщение  $s$  принято называть *атакой с адаптивным выбором шифртекста*.

Для предотвращения подобного рода подмен и модификаций, в практических приложениях к каждому сообщению добавляется так называемый *код целостности сообщения*, который позволяет эффективно проверить, было ли сообщение изменено в момент передачи по каналам связи.

### 11.1.11 Семантическая стойкость

В заключение мы приведем еще одно свойство схемы RSA, которое влияет на ее стойкость. Мы будем говорить, что схема шифрования RSA является семантически стойкой, если для любых значений открытого текста  $s$ , шифртекста  $c$  и также секретного и открытого ключей  $d$ ,  $e$  схемы RSA, не существует полиномиального алгоритма, позволяющего с вероятностью большей  $\frac{1}{2}$ , отделить открытый текст  $s$  от случайного двоичного вектора той же длины, по известным открытым параметрам  $c$  и  $m$ .

Для схемы RSA условие семантической стойкости не выполняется. Так как  $\text{НОД}(e, \varphi(m)) = 1$  и  $\varphi(m) = (p-1)(q-1)$ , то  $e$  нечетно. Тогда для любого шифртекста  $c$  выполнено равенство

$$\left(\frac{c}{m}\right) = \left(\frac{s^e}{m}\right) = \left(\frac{s}{m}\right),$$

где символ  $\left(\frac{\cdot}{\cdot}\right)$  обозначает символ Якоби, см. раздел 4.2. Из приведенного равенства следует, что в силу значения символа Якоби  $\left(\frac{c}{m}\right)$ , около половины случайных открытых текстов могут быть отбракованы и удалены из перечня возможных значений открытого текста  $s$ .

## 11.2 Схема шифрования RSA. Практика

Существование столь большого числа методов, позволяющих так или иначе скомпрометировать схему RSA привело к тому, что в настоящее время схема шифрования существенно усложнилась по сравнению с тем, что мы описали ранее. Появились стандартные требования к генерации модуля  $m$  и пары ключей  $e$ ,  $d$  схемы RSA, а также изменился процесс преобразования сообщения  $\xi$  в целое число  $s$ , подвергаемое зашифрованию.

Суммируя описанные нами как в предыдущих, так в настоящей лекции методы приведем требования к построению  $m$  модуля схемы RSA.

1. Модуль  $m = pq$  должен быть целым числом, являющимся произведением двух простых чисел  $p$ ,  $q$  и удовлетворяющим условию  $\log_2 m \in \{2^{10}, 2^{11}, 2^{12}, \dots\}$ . Столь большие размеры числа  $m$  делают затруднительным применение методов факторизации целых чисел общего вида, таких как метод квадратичного решета.
2. Числа  $p$ ,  $q$  должны удовлетворять неравенствам

$$\log_2 p > 2^7, \quad \log_2 q > 2^7.$$

Как правило, простые числа  $p$ ,  $q$  выбирают величинами одного порядка  $\sqrt{m}$ . Подобное ограничение затрудняет применение методов разложения на множители, основанных на поиске маленьких простых делителей, например методов Брента, см. раздел 7.5, или Ленстры.

3. Числа  $p \pm 1$  и  $q \pm 1$  должны иметь большие простые делители, то есть

$$\begin{aligned} p &= a_1 p_1 + 1, & p &= a_2 p_2 - 1, \\ q &= b_1 q_1 + 1, & q &= b_2 q_2 - 1, \end{aligned}$$

где  $p_1$ ,  $p_2$ ,  $q_1$ ,  $q_2$  простые числа удовлетворяющие неравенствам

$$\log_2 p_i > 2^7, \quad \log_2 q_i > 2^7, \quad i = 1, 2.$$

Подобное ограничение затрудняет применение методов разложения на множители частного вида, таких как методы Полларда, раздел 7.6.1, и Вильямса, раздел 7.6.2.

**Необходимо добавить условия из алгоритма 7.6.4**



4. Числа  $p_1 - 1$ ,  $q_1 - 1$  должны иметь большие простые делители, то есть

$$p_1 = c_1 p_2 + 1, \quad q_1 = d_1 q_2 + 1.$$

5. Величина  $w = \text{НОД}(p - 1, q - 1)$  должна удовлетворять неравенству  $\log_2 w < 64$ . Подобное ограничение существенно снижает число эквивалентных ключей схем RSA, см. раздел 11.1.8.
6. Величина  $|p - q|$  должна удовлетворять неравенству  $\log_2 |p - q| > 2^7$ . Данное ограничение делает невозможным факторизацию модуля схемы RSA методом Ферма, см. раздел 7.1.
7. Величина  $p - q$  должна иметь большой простой делитель  $r$ , удовлетворяющий неравенству  $\log_2 r > 2^7$ .
8. Величина  $\frac{p}{q}$  не должна быть близкой к отношению двух небольших целых чисел, то есть неравенство  $|pr - qs| < \sqrt[3]{m}$  не должно быть разрешимо ни для каких целых  $r, s$  удовлетворяющих неравенствам  $\log_2 r < 2^6$ ,  $\log_2 s < 2^6$ . Данное ограничение делает невозможным факторизацию модуля схемы RSA методом Лемана, см. раздел 7.3.
9. Как правило, открытый ключ  $e$  должен быть равен  $2^{16} + 1 = 65537$ . Простые числа  $p, q$  должны удовлетворять условию

$$\log_2(\text{ord}_{\varphi(m)} e) > 2^7.$$

Подобное ограничение делает затруднительными атаки на основе итерационного шифрования, см. раздел , см. раздел 11.1.6.

10. Модуль схемы  $m$  не должен иметь вид  $m = a^n \pm c$  для значений  $c$ , удовлетворяющих неравенству  $\log_2 c < 2^6$ . Другими словами, для указанного диапазона значений  $c$ , величина  $\sqrt[n]{m} \pm c$  не должна быть целым числом для всех  $n = 2, 3, \dots, \log_2 m$ . Подобное ограничение делает затруднительным применение частных случаев метода решета числового поля для факторизации модуля  $m$ .

Помимо требований, накладываемых на модуль схемы RSA, в современных стандартах изменен способ выработки целого числа  $s$  из сообщения  $\xi$ . Приведем описание двух вариантов схемы шифрования RSA в том виде, в каком они изложены в действующем в настоящее время стандарте PKCS №1 [?].

### 11.2.1 RSAES: схема с добавлением случайного вектора

Данная схема является простой модификации теоретической схемы, изложенной нами ранее в разделе 11.1. Она включена в стандарт для совместимости со старыми версиями и, на момент написания этой лекции, уже не рекомендовалась к реализации в новых приложениях. На вход алгоритма шифрования подаются

- Модуль схемы шифрования  $m$  такой, что  $\lceil \log_2 m \rceil = 8n$ , то есть любой вычет по модулю  $m$  может быть представлен в виде последовательности длиной не более  $n$  байт.
- Открытый ключ  $e$  получателя сообщения, целое число, удовлетворяющее условиям  $\text{НОД}(e, \varphi(m)) = 1$  и  $e < \varphi(m)$ . Как правило, используется фиксированное значение  $e = 65537$ .
- Сообщение  $\xi$ , представленное в виде последовательности байт  $\xi_0, \xi_1, \dots, \xi_{k-1}$ , где величина  $k$  удовлетворяет неравенству  $k \leq n - 11$ .

#### Алгоритм 11.2 (Алгоритм зашифрования в схеме RSAES)

1. Вычислить случайную последовательность байт  $\alpha_0, \dots, \alpha_{n-k-3}$ .
2. Определить двоичный вектор  $(s_0, \dots, s_{n-1})$  длины  $n$  байт
 
$$(s_0, \dots, s_{n-1}) = (0x00 || 0x02 || \alpha_0 || \alpha_1 || \dots || \alpha_{n-k-3} || 0x00 || \xi_0 || \dots || \xi_{k-1})$$
3. Определить целое число  $s = \sum_{i=0}^{n-1} s_i (256)^i$
4. Определить вычет  $c \equiv s^e \pmod{m}$  и представить его в виде  $c = (c_0, \dots, c_{n-1})$ , где  $c_i$  коэффициенты разложения вычета  $c$ , то есть  $c = \sum_{i=0}^{n-1} c_i (256)^i$ .
5. Определить в качестве шифртекста, соответствующего открытому тексту  $\xi$ , последовательность байт  $(c_0, \dots, c_{n-1})$ .  $\square$

Как видно из приведенного алгоритма, схема шифрования RSAES отличается от теоретической схемы добавлением в сообщение псевдослучайного вектора  $\alpha = (\alpha_0, \dots, \alpha_{n-k-3})$ . Длина данного вектора не менее восьми байт (64 бит). Это сделано для того, чтобы не допустить возможность появления алгебраических зависимостей между различными сообщениями и предотвращения атаки, описанной нами в разделе 11.1.9.

В качестве кода целостности, то есть информации подтверждающей то, что сообщение было не изменено в ходе передачи по каналам связи, выступают два фиксированных байта  $0x00, 0x02$ , расположенных в начале сообщения и значение которых не зависит от передаваемого сообщения. На взгляд разработчиков схемы это было явно не достаточно, что привело к появлению следующей модификации схемы.

### 11.2.2 RSA-OAEP: оптимальная асимметричная схема шифрования

В 1994 году Белларе (Mihir Bellare) и Рогавей (Phillip Rogaway) опубликовали статью [?] в которой предложили способ «оптимального асимметричного шифрования», то есть способ защиты от целого класса атак, основанных на адаптивном подборе шифртекстов, в частности, от атаки описанной нами ранее в разделе 11.1.10. В последствие, этот способ был стандартизован и включен в стандарт PKCS №1 [?].

Для того, чтобы описать данный способ, нам потребуется напомнить понятие «бесключевой функции хеширования».

**Определение 11.2.** Пусть функция  $h$  задает отображение множества сообщения произвольной длины в сообщения фиксированной длины  $n$ , то есть  $f : \mathbb{V}_\infty \rightarrow \mathbb{V}_n$ . Функция  $h$  является сжимающим отображением и может иметь несколько прообразов  $\xi_1, \xi_2, \dots$ , для которых результат действия функции  $h$  совпадает, то есть

$$h(\xi_1) = h(\xi_2) = \dots$$

Мы будем называть функцию  $h$  бесключевой функцией хеширования, если выполнены следующие условия.

1. Для заданного значения  $a$  функции  $h$  задача вычисления какого-либо сообщения  $\xi$  такого, что  $h(\xi) = a$  является трудноразрешимой. Такая задача называется задачей построения прообраза функции хеширования.
2. Задача построения двух произвольных сообщений  $\xi_1$  и  $\xi_2$  таких, что  $h(\xi_1) = h(\xi_2)$  является трудноразрешимой. Такая задача называется задачей построения коллизии для функции хеширования.

Результат действия функции хеширования  $h$  над заданным сообщением  $\xi$  мы будем называть хеш-кодом сообщения  $\xi$ .

Фактически, функция хеширования позволяет присвоить каждому сообщению его хеш-код, то есть практически уникальный идентификатор, обладающий тем свойством, что при его фиксированном значении очень трудно подобрать другое, ложное сообщение с тем же значением хеш-кода.

В настоящее время разработано и стандартизировано много различных функций хеширования. В качестве примера можно привести функцию, регламентированную государственным стандартом Российской Федерации ГОСТ Р 34.11-94 [?].

В случае, если сообщение будет случайным или преднамеренным образом изменено во время передачи по каналам связи, то и хеш-код сообщения также должен измениться, что позволяет отследить факт искажения передаваемой информации.

В общем случае, алгоритм зашифрования сообщения  $\xi$  в схеме, предложенной Белларе и Рогавеем, заключается в вычислении сообщения

$$c = f(\xi \oplus g(r) || r \oplus h(\xi \oplus g(r))), \quad (11.9)$$

где  $\oplus$  операция побитового сложения (операция сложения двоичных векторов по модулю 2),  $r$  некоторое псевдо-случайное значение, например случайный вектор, функция  $g$  это генератор псевдо-случайной последовательности, инициированный значением  $r$ , а функция  $f$  — это функция зашифрования полученного сообщения.

К исходному сообщению добавляется случайный вектор  $r$ , который используется не только для противодействия атакам, основанным на алгебраических соотношениях между открытыми текстами, но и для маскирования исходного сообщения. Это позволяет получать при зашифровании одного и того же открытого сообщения получать различные зашифрованные сообщения.

Применительно к схеме RSA процедура зашифрования сообщения  $\xi$ , предложенная Белларе и Рогавеем, была несколько модифицирована разработчиками схемы и представлена следующим образом. На вход алгоритма шифрования подаются перечисленные ниже параметры.

- Модуль схемы шифрования  $m$  такой, что  $\lceil \log_2 m \rceil = 8n$ , то есть любой вычет по модулю  $m$  может быть представлен в виде последовательности длиной не более  $n$  байт.
- Открытый ключ  $e$  получателя сообщения, целое число, удовлетворяющее условиям  $\text{НОД}(e, \varphi(m)) = 1$  и  $e < \varphi(m)$ . Как правило, используется фиксированное значение  $e = 65537$ .
- Бесключевая функция хеширования  $h$ , вырабатывающая для произвольного сообщения хеш-код длиной  $l$  байт.

- Генератор<sup>4</sup> псевдослучайной последовательности  $g(x, y)$ , который, по заданной входной последовательности байт  $x$ , вырабатывает выходную последовательность байт длины  $y$  байт.
- Сообщение  $\xi$ , представленное в виде последовательности байт  $\xi_0, \xi_1, \dots, \xi_{k-1}$ , где  $k \leq n - 2(l + 1)$ .
- На вход алгоритма зашифрования может подаваться произвольная метка  $L$  — произвольная строка, идентифицирующая сообщение и передаваемая по каналам связи в незашифрованном виде. Допускается зашифрование сообщения  $\xi$  без задания метки, в этом случае считается, что вектор  $L$  состоит из одних нулей и его длина совпадает с длиной хеш-кода используемой функции хеширования.

### Алгоритм 11.3 (Алгоритм зашифрования в схеме RSA-OAEP)

1. Определить  $x = n - k - 2(l + 1)$ , вычислить случайную последовательность байт  $\alpha_0, \dots, \alpha_{x-1}$  и определить вектор  $(a_0, \dots, a_{k+l+x})$  равенством

$$(a_0, \dots, a_{k+l+x}) = (h(L) || \alpha_0 || \dots || \alpha_{x-1} || 0x01 || \xi_0 || \dots || \xi_{k-1})$$

2. Выработать случайную последовательность байт  $r_0, \dots, r_{l-1}$  и наложить на вектор  $(a_0, \dots, a_{k+l+x})$  маску, выработанную с помощью генератора  $g$ , то есть

$$(a_0, \dots, a_{k+l+x}) = (a_0 \oplus \zeta_0, \dots, a_{k+l+x} \oplus \zeta_{k+l+x}),$$

где  $(\zeta_0, \dots, \zeta_{k+l+x}) = g(r_0, \dots, r_{l-1}, k + l + x)$ .

3. Определить вектор  $(b_0, \dots, b_{l-1})$  равенством

$$(b_0, \dots, b_{l-1}) = (\alpha_0 \oplus \zeta_0, \dots, \alpha_{l-1} \oplus \zeta_{l-1}),$$

где  $(\zeta_0, \dots, \zeta_{k+l+x}) = g(a_0, \dots, a_{k+l+x}, l)$ .

4. Определить двоичный вектор  $(s_0, \dots, s_{n-1})$  длины  $n$  байт

$$(s_0, \dots, s_{n-1}) = (0x00 || b_0 || \dots || b_{l-1} || a_0 || \dots || a_{k+l+x})$$

5. Определить целое число  $s = \sum_{i=0}^{n-1} s_i (256)^i$ .
6. Определить вычет  $c \equiv s^e \pmod{m}$  и представить его в виде  $c = (c_0, \dots, c_{n-1})$ , где  $c_i$  коэффициенты разложения вычета  $c$ , то есть  $c = \sum_{i=0}^{n-1} c_i (256)^i$ .
7. Определить в качестве шифртекста, соответствующего открытому тексту  $\xi$ , последовательность байт  $(c_0, \dots, c_{n-1})$ .  $\square$

Как видно из приведенного алгоритма, исходное сообщение дополняется случайными данными и перед зашифрованием представляется в виде двух половинок, меньшая из которых является хеш-кодом большей,

<sup>4</sup>В стандарте PKCS №1 данная функция называется функцией генерации масок – MGF (Mask generation function).

то есть кодом целостности. Такая структура позволяет, после расширения сообщения, проверить код целостности и удостовериться в том, что сообщение не было изменено.

Для полноты картины приведем также и алгоритм расшифрования сообщения в схеме RSA-OAEP, на вход которого должны подаваться все те же, перечисленные ранее параметры, за некоторым исключением.

- Вместо открытого ключа должно быть задан секретный ключ  $d$ , удовлетворяющий сравнению  $ed \equiv 1 \pmod{\varphi(m)}$ .
- Вместо открытого текста  $\xi$  подается зашифрованное сообщение, представленное в виде двоичного вектора  $(c_0, \dots, c_{n-1})$ .

### Алгоритм 11.4 (Алгоритм расшифрования в схеме RSA-OAEP)

1. Определить целое число  $c = \sum_{i=0}^{n-1} c_i(256)^i$ .
2. Определить вычет  $s$  сравнением  $s \equiv c^d \pmod{m}$  и представить его в виде вектора  $s = (s_0, \dots, s_{n-1})$ , координаты которого определены равенством  $s = \sum_{i=0}^{n-1} s_i(256)^i$ .
3. Если  $s_0 \neq 0x00$ , то завершить алгоритм с уведомлением о том, что сообщение искажено.
4. Определить вектор  $(r_0, \dots, r_{l-1})$  равенством

$$(r_0, \dots, r_{l-1}) = (s_1 \oplus \zeta_0, \dots, s_l \oplus \zeta_{l-1}),$$

где  $(\zeta_0, \dots, \zeta_{l-1}) = g(s_{l+1}, \dots, s_{n-1}, l)$ .

5. Определить вектор  $(a_0, \dots, a_{k+l+x})$  равенством

$$(a_0, \dots, a_{k+l+x}) = (s_{l+1} \oplus \zeta_0, \dots, s_{n-1} \oplus \zeta_{k+l+x},$$

где  $(\zeta_0, \dots, \zeta_{k+l+x}) = g(r_0, \dots, r_{l-1}, k + l + x)$ .

6. Если  $(a_0, \dots, a_{l-1}) \neq h(L)$ , то завершить алгоритм с уведомлением о том, что сообщение искажено.
7. Если  $a_{l+x} \neq 0x01$ , то завершить алгоритм с уведомлением о том, что сообщение искажено.
8. Определить вектор  $a_{l+x+1}, \dots, a_{k+l+x}$  в качестве открытого текста. □

Как видно из приведенного нами описания, реальные криптографические схемы основываются не только на трудноразрешимых теоретико-числовых задачах, но и содержат дополнительные меры защиты, предотвращающие возможность проведения атак, не связанных напрямую с решением математических задач. В современных криптографических схемах используются достаточно сложные комбинации различных преобразований, каждое из которых не позволяет реализовать нарушителю ту или иную атаку на алгоритм шифрования.

## 11.3 Схема шифрования Рабина

Схема шифрования RSA является самой известной, но не единственной схемой, криптографическая стойкость которой основывается на задаче факторизации целых чисел. В 1979 году Микаэль Рабин (Michael Rabin) предложил следующую схему шифрования [?].

Пусть  $m = pq > 0$  нечетное составное число, являющееся произведением двух простых чисел  $p$  и  $q$ . Данное число является открытым ключом абонента, который хочет получать сообщения. Секретным ключом являются значения простых чисел  $p$  и  $q$ .

Процесс зашифрования сообщения выглядит следующим образом. Пусть сообщение  $s$  удовлетворяет неравенствам  $1 < s < m - 1$  и выполнено условие  $\text{НОД}(s, m) = 1$ . Тогда для зашифрования сообщения  $s$  необходимо вычислить

$$c \equiv s^2 \pmod{m}.$$

Процесс расшифрования сообщения, то есть определения числа  $s$  по заданным значениям  $c$  и  $m$ , выглядит следующим образом. Получатель сообщения, абонент которому известно разложение числа  $m$  на множители, вычисляет значения  $x_p, x_q$  такие, что

$$x_p^2 \equiv c \pmod{p}, \quad x_q^2 \equiv c \pmod{q}.$$

В предыдущих лекциях мы подробно рассмотрели алгоритм Тонелли-Шенкса вычисления квадратного корня по модулю простого числа, алгоритм 4.2. Для упрощения вычислений при генерации числа  $m$  рекомендуется выбирать  $p \equiv q \equiv 3 \pmod{4}$ . В этом случае задача вычисления квадратного корня, как мы показали ранее, сводится к модульному возведению в степень, то есть

$$x_p \equiv c^{\frac{p+1}{4}} \pmod{p}, \quad x_q \equiv c^{\frac{q+1}{4}} \pmod{q}.$$

Найденные значения  $x_p, x_q$  используются для вычисления множества, состоящего из четырех значений  $s_1, s_2, s_3, s_4$  таких, что  $s_i^2 \equiv c \pmod{m}$ . Это можно сделать, например, с помощью китайской теоремы об остатках, теорема 2.3.

Другой подход заключается в следующем. Используя расширенный алгоритм Эвклида, алгоритм 2.1, вычислим  $u, v$  такие, что

$$up + vq = 1,$$

и определим

$$\begin{aligned} s_1 &\equiv upx_q + vqx_p \pmod{m}, \\ s_2 &= m - s_1, \\ s_3 &\equiv upx_q - vqx_p \pmod{m}, \\ s_4 &= m - s_3. \end{aligned}$$

Заметим, что вычисление значений  $u$  и  $v$  можно произвести заранее, например, сразу после генерации простых чисел  $p$  и  $q$ .

Подобный подход избавляет нас от необходимости решать четыре различных системы сравнений. Получателю остается сделать выбор какое же из четырех полученных им значений было ему отправлено.

Существование нескольких вариантов расшифрованного сообщения, среди которых необходимо выбирать истинное, сильно снижает привлекательность практического использования схемы шифрования Рабина. Для выбора истинного значения к сообщению необходимо добавить код целостности, проверка которого позволяет как выбрать истинное значение открытого текста из четырех вариантов, так и защититься от атак, основанных на изменении целостности передаваемого сообщения.

### 11.3.1 Об эквивалентности задач факторизации и вычисления квадратного корня

Легко видеть, что существование быстрого алгоритма факторизации числа  $m$  приводит к быстрому вычислению квадратного корня по модулю  $m$ . В статье [?] Рабин показал, что верно и обратное утверждение.

**Теорема 11.1.** Пусть  $m = pq$  нечетное составное число с неизвестным разложением на множители. Задача факторизации числа  $m$  может быть сведена к задаче поиска хотя бы одного решения сравнения  $x^2 \equiv a \pmod{m}$ .

*Доказательство.* Рассмотрим сравнение

$$x^2 \equiv k^2 \pmod{m}. \quad (11.10)$$

Пусть  $k \equiv u \pmod{p}$  и  $k \equiv v \pmod{q}$ , тогда решение  $x$  сравнения (11.10) удовлетворяет одному из четырех сравнений

$$\begin{aligned} \begin{cases} x \equiv u \pmod{p}, \\ x \equiv -v \pmod{q}, \end{cases} & \begin{cases} x \equiv -u \pmod{p}, \\ x \equiv v \pmod{q}, \end{cases} \\ & \begin{cases} x \equiv u \pmod{p}, \\ x \equiv v \pmod{q}, \end{cases} \begin{cases} x \equiv -u \pmod{p}, \\ x \equiv -v \pmod{q}. \end{cases} \end{aligned} \quad (11.11)$$



Теперь предположим, что у нас есть алгоритм, который находит неизвестное значение  $x$ , удовлетворяющее сравнению  $x^2 \equiv a \pmod{m}$ . Выберем случайное целое число  $k$ ,  $1 < k < m-1$ . Если выполнено неравенство  $\text{НОД}(k, m) = d > 1$ , то мы нашли нетривиальный делитель числа  $m$ .

В противном случае, определим  $a \equiv k^2 \pmod{m}$  и, используя наш алгоритм, вычислим  $x$  такой, что  $x^2 \equiv a \equiv k^2 \pmod{m}$ . Если  $x$  удовлетворяет второй или третьей системе из (11.11), то мы получим, что

$$\text{НОД}(x + k, m) > 1.$$

В случае остальных двух систем, мы получим либо  $\text{НОД}(x + k, m) = 1$ , либо  $\text{НОД}(x + k, m) = m$ . Следовательно, при однократном выборе числа  $k$  вероятность найти нетривиальный делитель числа  $m$  не менее  $\frac{1}{2}$ . При увеличении числа попыток вероятность стремится к единице.  $\square$

Предложенный нами алгоритм сведения является вероятностным, и при заданном значении вероятности, его трудоемкость может быть оценена полиномом от  $\log_2 m$ .

## 11.4 Схема шифрования Эль-Гамала

## СЛУЧАЙНЫЕ ОТОБРАЖЕНИЯ

**Орбиты элементов - циклы и подходы - теорема о математическом ожидании длин циклов и подходов - алгоритмы Флойда, Брента, Госпера и Ниваша для поиска длин циклов в последовательностях.**

В этом приложении мы приведем несколько формальных определений и опишем свойства случайных отображений конечного множества в себя. Мы опишем несколько алгоритмов поиска длин циклов в последовательностях, которые используются нами при реализации и исследовании сложности алгоритмов факторизации целых чисел и вычисления дискретного логарифма.

### А.1 Орбиты элементов

Рассмотрим произвольное конечное множество  $\mathcal{M}$ , состоящее из  $m$  элементов, и дадим несколько определений.

**Определение А.1.** Мы будем обозначать символом  $\mathcal{F}_m$  множество всех функций, отображающих элементы множества  $\mathcal{M}$  в себя

$$\mathcal{F}_m = \{f : \mathcal{M} \rightarrow \mathcal{M}\}.$$

Отметим, что любую функцию  $f \in \mathcal{F}_m$  можно определить аналитически или задать таблицей

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{m-1} \\ f(a_0) & f(a_1) & \dots & f(a_{m-1}) \end{pmatrix}$$

Мы допускаем возможность возникновения у функции  $f$  коллизии, то есть существования двух элементов  $a, b \in \mathcal{M}$  таких, что  $f(a) = f(b)$  при  $a \neq b$ .

Зафиксируем некоторое отображение  $f \in \mathcal{F}_m$ , выберем элемент  $a$  из множества  $\mathcal{M}$  и рассмотрим последовательность элементов  $\{a_n\}_{n=0}$ , определяемую равенствами

$$a_0 = a, \quad a_{n+1} = f(a_n), \quad n = 0, 1, \dots \quad (\text{А.1})$$

**Определение А.2.** Пусть  $a$  некоторый элемент из  $\mathcal{M}$  и  $f \in \mathcal{F}_m$  некоторое фиксированное отображение. Орбитой элемента  $a$  называется последовательность  $\{a_n\}_{n=0}$ , определяемая равенством (А.1).

Сформулируем важное наблюдение. В силу того, что множество  $\mathcal{M}$  конечно, орбита каждого элемента  $a$  заиклится, то есть найдется индекс  $\lambda$  такой, что для всех индексов  $n \geq \lambda$  будет выполнено равенство

$$a_n = a_{n+\tau}, \quad (\text{A.2})$$

при некоторой натуральной величине  $\tau$ .

**Определение А.3.** Мы будем называть элементы  $a_0, a_1, \dots, a_{\lambda-1}$  *подходом к циклу*, значение  $\lambda$  — *длиной подхода*, наименьшее из всех возможных значений  $\tau$ , удовлетворяющих равенству (A.2) — *длиной цикла* последовательности  $\{a_n\}_{n=0}$  или, другими словами, орбиты элемента  $a$ .

**Пример А.1.** Поясним введенные выше определения. Рассмотрим в качестве множества  $\mathcal{M}$  кольцо вычетов  $\mathbb{Z}_{11}$  и зафиксируем отображение  $f$ , задаваемое таблицей

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 4 & 10 & 2 & 5 & 1 & 1 & 8 & 5 & 3 & 9 \end{pmatrix}$$

Тогда орбита элемента  $a = 0$  будет иметь следующий вид

$$\begin{aligned} a_0 &= 0, \\ a_1 &= f(0) = 6, \\ a_2 &= f(6) = 1, \\ a_3 &= f(1) = 4, \\ a_4 &= f(4) = 5, \\ a_5 &= f(5) = 1, \\ a_6 &= f(1) = 4, \quad \dots \end{aligned}$$

Схематично, орбиту элемента  $a = 0$  можно нарисовать следующим образом

$$\underbrace{0 \rightarrow 6}_{\text{подход}} \rightarrow \underbrace{1 \rightarrow 4 \rightarrow 5}_{\text{цикл}} \rightarrow \dots$$

В нашем примере длина подхода  $\lambda = 2$ , а длина цикла  $\tau = 3$ . Кроме того заметим, что элемент  $a = 0$  не является результатом действия функции  $f$  и может появиться только в одном месте орбиты — в ее начале.

**Определение А.4.** Пусть  $f \in \mathcal{F}_m$  некоторое фиксированное отображение множества  $\mathcal{M}$  в себя. Элемент  $a \in \mathcal{M}$  называется *терминальным*, если не существует элемента  $b \in \mathcal{M}$  такого, что  $a = f(b)$ .

*Элементы, не являющиеся терминальными, естественно назвать образами на множестве  $\mathcal{M}$ .*

Согласно данному определению, в рассматриваемом нами примере элементы 0 и 7 являются терминальными. Остальные элементы — образами множества  $\mathbb{Z}_{11}$ .

Поскольку мы допускаем, что отображение  $f \in \mathcal{F}_m$  может реализовывать коллизии на множестве  $\mathcal{M}$ , мы должны допустить возможность того, что один цикл может иметь несколько подходов. Действительно, легко заметить, что орбита элемента  $a = 7$  имеет вид

$$\underbrace{7 \rightarrow 8}_{\text{подход}} \rightarrow \underbrace{5 \rightarrow 1 \rightarrow 4}_{\text{цикл}} \rightarrow \dots$$

и сходится к тому же циклу, что и орбита элемента  $a = 0$ .

**Определение А.5.** Пусть  $f \in \mathcal{F}_m$  некоторое фиксированное отображение множества  $\mathcal{M}$  в себя. Мы будем называть областью связности или, другими словами, связной компонентой множества  $\mathcal{M}$ , цикл и множество его подходов.

Легко видеть, что в примере А.1 отображение  $f$  разбивает множество  $\mathbb{Z}_{11}$  на две связные компоненты. Одна состоит из рассмотренного ранее цикла и двух его подходов, вторая — из цикла длины 4 без подходов

$$\underbrace{2 \rightarrow 10 \rightarrow 9 \rightarrow 3}_{\text{цикл}} \rightarrow \dots$$

Сформулируем утверждение, описывающее асимптотический характер поведения введенных нами параметров при условии, что мощность множества  $\mathcal{M}$ , на котором действует случайное отображение, стремится к бесконечности.

**Теорема А.1** (см. [5]). Пусть  $f \in \mathcal{F}_m$  некоторое отображение, являющееся реализацией случайной величины, равномерно распределенной на множестве  $\mathcal{F}_m$ . Выполнены следующие утверждения.

1. Обозначим символом  $M(f, m)$  математическое ожидание числа областей связности, на которые разбивается множество  $\mathcal{M}$ , тогда

$$\lim_{m \rightarrow \infty} \frac{M(f, m)}{\frac{1}{2} \ln m} = 1.$$

2. Обозначим символом  $T(f, m)$  математическое ожидание числа терминальных элементов множества  $\mathcal{M}$ , тогда

$$\lim_{m \rightarrow \infty} \frac{T(f, m)}{\frac{m}{e}} = 1, \quad \text{где} \quad e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n$$

основание натурального логарифма.

3. Обозначим символом  $S(f, m)$  математическое ожидание числа образов множества  $\mathcal{M}$ , то есть элементов, не являющихся терминальными, тогда

$$\lim_{m \rightarrow \infty} \frac{S(f, m)}{\left(\frac{e-1}{e}\right) m} = 1.$$

4. Обозначим символом  $\tau(f, m)$  математическое ожидание длины цикла произвольной орбиты множества  $\mathcal{M}$ , тогда

$$\lim_{m \rightarrow \infty} \frac{\tau(f, m)}{\sqrt{\frac{\pi m}{8}}} = 1.$$

5. Обозначим символом  $\lambda(f, m)$  математическое ожидание длины подхода к циклу произвольной орбиты множества  $\mathcal{M}$ , тогда

$$\lim_{m \rightarrow \infty} \frac{\lambda(f, m)}{\sqrt{\frac{\pi m}{8}}} = 1.$$

Проведем эксперимент и применим утверждения теоремы к определенному в примере А.1 отображению  $f$ . Легко видеть, что изучаемые нами параметры принимают следующие значения.

1. Согласно утверждению теоремы, математическое ожидание числа компонент связности должно принимать значение  $M = \frac{\ln 11}{2} = 1.19$ . Точное значение равно двум.
2. Математическое ожидание числа терминальных элементов  $T = \frac{11}{e} = 4.04$ . Точное значение равно двум.
3. Математическое ожидание длины цикла и длины подхода к циклу равно  $\sqrt{\frac{11\pi}{8}} = 2.08$ . Точное значение длин подходов равно двум, а средняя длина цикла равна трем с половиной.

Приведенный пример показывает, что утверждения теоремы носят асимптотический характер и при малых значениях  $m$  могут не выполняться.

## А.2 Поиск длин циклов в последовательностях

Теперь мы зафиксируем некоторое отображение  $f : \mathcal{M} \rightarrow \mathcal{M}$  множества  $\mathcal{M}$  в себя, произвольный элемент  $a_0 \in \mathcal{M}$ , его орбиту  $\{a_n\}_0^\infty$  и рассмотрим задачу определения длины цикла, то есть задачу вычисления величины  $\tau$  такой, что

$$a_n = a_{n+\tau}$$

для всех индексов  $n \geq \lambda$ , при неизвестном значении величины  $\lambda \geq 0$ .

В настоящее время известно несколько алгоритмов решения данной задачи. Первый и самый известный алгоритм был предложен в 1968 году Робертом Флойдом (Robert W Floyd), см. [30, п.3.1, задача 6b]. Годом позже Дональдом Кнутом (Donald Knuth) был опубликован, см. [30, п.3.1, задача 7b], алгоритм Ричарда Брента (Richard P. Brent).

Однако наиболее эффективный способ решения поставленной задачи заключается в использовании алгоритма, предложенного в 1972 году Биллом Госпером (Ralph William Gosper, Jr.), см. [16, п.132].

Несмотря на свою эффективность, алгоритм Госпера не является хорошо известным. Единственное его описание на русском языке может быть найдено в переводной книге Генри Уоррена (Henry S. Warren, Jr.) [13, п.5.4]. Возможно в силу простоты алгоритма, Госпер не дал его строгого математического обоснования. Оно опубликовано автором, см. [8], только в 2010 году.

Стоит также отметить еще два алгоритма. Первый, был предложен Робертом Седжвиком (Robert Sedgewick) и Томасом Сжимански (Thomas Szymansky) в 1981 году, оценки времени его работы опубликованы в статье [48]. Алгоритм Седжвика-Сжимански обладает наименьшей трудоемкостью среди всех известных алгоритмов поиска длин циклов в последовательностях. Вместе с тем, алгоритм использует столь большой объем памяти для хранения промежуточных элементов последовательности, что делает его неприменимым для применения на практике.

Второй алгоритм предложен Габриэлом Нивашем (Gabriel Nivasch) в 2004 году, см. [40], и основан на очень красивой идее поиска минимального элемента, лежащего внутри цикла. Алгоритм имеет сравнимую с методом Госпера трудоемкость и объем используемой памяти. Однако, данный алгоритм может быть использован только для тех множеств  $\mathcal{M}$ , на которых можно ввести отношение упорядоченности элементов.

### А.2.1 Алгоритм Флойда

Алгоритм Флойда является самым простым и хорошо известным. Он основан на выполнении следующего условия: если выполнено равенство

$$a_n = a_{2n}, \quad (\text{A.3})$$

то величина  $\tau$  делит  $n$ . Для вычисления числа, кратного  $\tau$ , можно использовать следующий алгоритм.

#### Алгоритм А.1 (Алгоритм Флойда)

**Вход:** Отображение  $f : \mathcal{M} \rightarrow \mathcal{M}$  и начальный элемент  $a_0$ .

**Выход:** Значение длины цикла  $\tau$ .

1. Определить начальные значения:  $a \leftarrow a_0$  и  $b \leftarrow f(a)$ .
2. **Пока** положить  $a \neq b$  **выполнять**  $a = f(a)$ ,  $c = f(b)$  и  $b = f(c)$ .
3. Определить  $b = f(a)$  и  $\tau = 1$ .
4. **Пока**  $a \neq b$  **выполнять**  $b = f(b)$  и  $\tau = \tau + 1$ . □

Второй шаг алгоритма выполняется до тех пор, пока не будет найдено равенство (A.3), при этом точное значение индекса  $n$  не вычисляется. Поскольку задача поиска всех делителей числа  $n$ , как мы видели в главах 7-8, является весьма трудоемкой, то, на четвертом шаге алгоритма, мы вычисляем точное значение  $\tau$  непосредственным перебором.

Легко видеть, что минимально возможное значение индекса  $n$ , при котором выполняется равенство  $a_n = a_{2n}$ , равно  $\tau \left\lceil \frac{\lambda}{\tau} \right\rceil$ . Таким образом трудоемкость алгоритма Флойда равна  $\tau \left( 3 \left\lceil \frac{\lambda}{\tau} \right\rceil + 1 \right)$  операций вычисления функции  $f$ .

### А.2.2 Алгоритм Брента

Прежде чем описывать алгоритм вычисления длины цикла последовательности (A.1), мы докажем теорему, утверждения которой служат его обоснованием. При доказательстве теоремы мы будем следовать идеям, высказанным в монографии [21, п.8.2.2]. Определим функцию целочисленного аргумента

$$l(n) = 2^{\lfloor \log_2 n \rfloor}, \quad n = 1, 2, \dots,$$

которая возвращает максимальное целое число, являющееся степенью двойки и не превосходящее числа  $n$ . Из определения функции  $l(n)$  следует, что  $l(n) \leq n < 2l(n)$ . Определим параметр  $k$  равенством

$$k = \lceil \log_2 \max\{\lambda + 1, \tau\} \rceil,$$

где  $\tau$  означает длину цикла, а  $\lambda$  длину подхода к циклу в последовательности, порожденной элементом  $a_0$ . Из определения параметра  $k$  следуют неравенства  $\tau \leq 2^k$  и  $\lambda \leq 2^k - 1$ . Определим индекс  $n_0$  равенством

$$n_0 = 2^k + \tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \quad (\text{A.4})$$

**Теорема А.2.** *Выполнены следующие утверждения*

1. Верны неравенства  $2^k \leq n_0 < 2^{k+1}$ ,
2. Для индекса  $n_0$  выполнено равенство  $a_{n_0} = a_{l(n_0)-1}$ ,
3. Выполнено  $\frac{3}{2}l(n_0) \leq n_0 < 2l(n_0)$ .

*Доказательство.* Начнем с доказательства первого утверждения теоремы. Поскольку длина цикла  $\tau$  является целым числом, то  $\tau \geq 1$ . Поскольку неравенство  $\left\lceil \frac{l(\lambda)+1}{\tau} \right\rceil \geq 1$  выполнено по определению, то неравенство  $2^k \leq n_0$  очевидно. Для оценки сверху заметим, что нам достаточно показать, что

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil \leq 2^k,$$

тогда  $n_0 \leq 2 \cdot 2^k - 1 < 2^{k+1}$ .

1. В начале рассмотрим случай, когда  $\tau > l(\lambda)$ . Тогда выполнено  $\tau \geq l(\lambda) + 1$  и  $\frac{l(\lambda)+1}{\tau} \leq 1$ . Следовательно

$$\left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil = 1 \quad \text{и} \quad \tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil = \tau \leq 2^k.$$

Последнее неравенство выполнено в силу выбора параметра  $k$ .

2. Рассмотрим второй случай  $\tau \leq l(\lambda)$ . Тогда выполнено

$$\left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil = \frac{l(\lambda) + 1 + \delta}{\tau} \leq \frac{l(\lambda) + \tau}{\tau} \leq \frac{2l(\lambda)}{\tau},$$

при некотором натуральном  $\delta < \tau$ . Полученное неравенство позволяет записать<sup>1</sup>

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil \leq 2l(\lambda) = 2^{\lceil \log_2 \lambda \rceil + 1} = 2^{\lceil \log_2 (\lambda + 1) \rceil} \leq 2^k.$$

---

<sup>1</sup>Мы пользуемся равенством  $\lceil \log_2 \lambda \rceil + 1 = \lceil \log_2 (\lambda + 1) \rceil$ , которое выполнено при натуральных значениях  $\lambda$ .



Мы получили, что для обоих случаев выполнено необходимое неравенство, таким образом первое утверждение теоремы доказано.

Для доказательства второго утверждения теоремы заметим, что из первого утверждения следует

$$k \leq \log_2 n_0 < k + 1 \quad \text{и} \quad l(n_0) = 2^k.$$

Тогда разность  $n_0 - (l(n_0) - 1) = \tau \left\lceil \frac{l(n_0)+1}{\tau} \right\rceil$  кратна длине цикла  $\tau$ , то есть равенство  $a_{n_0} = a_{l(n_0)-1}$  действительно имеет место.

Нам осталось доказать последнее утверждение теоремы. Оценка сверху тривиально вытекает из определения функции  $l(n)$ . Для получения нижней оценки заметим справедливость неравенств

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \geq \tau - 1 = 2^{\log_2 \tau} - 1 \geq 2^{\lceil \log_2 \tau \rceil - 1} \quad (\text{A.5})$$

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \geq l(\lambda) = 2^{\lceil \log_2 \lambda + 1 \rceil - 1}. \quad (\text{A.6})$$

Следовательно, выполнено неравенство  $\tau \left\lceil \frac{l(\lambda)+1}{\tau} \right\rceil - 1 \geq 2^{k-1}$ , откуда следует

$$n_0 = 2^k + \tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \geq 2^k + 2^{k-1} = \frac{3l(n_0)}{2}$$

и доказательство последнего утверждения теоремы.  $\square$

Доказанная нами теорема в явном виде задает значение индекса  $n_0$  которое необходимо вычислить для определения длины цикла. К сожалению, на практике, нам неизвестно значение  $n_0$ .

Основываясь на утверждениях доказанной теоремы, Brent предложил следующую идею: для поиска значения, кратного величине  $\tau$ , нам необходимо воспользоваться тем фактом, что  $a_{n_0} = a_{2^k-1}$  при некотором натуральном значении  $k$  таком, что  $3 \cdot 2^{k-1} \leq n_0 < 2^{k+1}$ .

## Алгоритм А.2 (Алгоритм Брента)

**Вход:** Отображение  $f : \mathcal{M} \rightarrow \mathcal{M}$  и начальный элемент  $a_0$ .

**Выход:** Значение длины цикла  $\tau$ .

1. Определить начальные значения:  $c = a_0$ ,  $a = f(a_0)$ ,  $n = 1$  и  $t = 1$ .
2. Если  $a = c$ , то вернуть значение  $\tau = 1$  и завершить алгоритм.
3. Если  $n = t$ , то положить  $c = a$  и вычислить  $t = 2t$ .
4. Определить  $a = f(a)$  и вычислить  $n = n + 1$ .
5. Если  $n \geq 3t/4$ , то проверить выполняется, ли равенство  $a = c$ . Если нет, то вернуться на шаг 3.

6. Определить  $\tau = 1$  и  $a = f(c)$ .

7. Пока  $a \neq c$  выполнять  $a = f(a)$  и  $\tau = \tau + 1$ . □

Алгоритм Брента, как и алгоритм Флойда, не позволяет в явном виде определить значение длины цикла  $\tau$ . На пятом шаге приведенного алгоритма мы находим совпадение  $a_{n_0} = a_{2^k-1}$  для некоторого натурального числа  $k$ . Последние два шага приведенного алгоритма позволяют определить значение  $\tau$  в явном виде. Как и ранее, мы не вычисляем значение  $n_0 + 1 - 2^k$ , кратное величине  $\tau$ , а находим искомую величину простым перебором.

Для оценки трудоемкости алгоритма Брента заметим, что из третьего утверждения теоремы А.2 и определения величины  $k$  следует оценка снизу

$$n_0 \geq \frac{3l(n_0)}{2} = \frac{3}{2} \cdot 2^k \geq \frac{3}{2} \max\{\lambda + 1, \tau\},$$

для числа шагов, необходимых для поиска совпадения на пятом шаге алгоритма. Таким образом, общая трудоемкость алгоритма Брента составит не менее  $\tau + \frac{3}{2} \max\{\lambda + 1, \tau\}$  операций вычисления функции  $f$ .

### А.2.3 Алгоритм Госпера

В алгоритме Госпера для поиска двух совпадающих элементов последовательности (А.1)

$$a_{n+1} = f(a_n), \quad n = 0, 1, \dots$$

производится сравнение  $a_n$  с элементами некоторого множества  $M(n)$ . Фиксируем значение  $n > 0$  и поместим в множество  $M(n)$  элементы  $a_{n_0}, a_{n_1}, \dots$  последовательности (А.1), с условием

$$n_k = \max_{r < n} \{r \mid \nu_2(r + 1) = k\}, \quad (\text{А.7})$$

для всех возможных значений  $k = 0, 1, \dots$ . Напомним, что функция  $\nu_2(r + 1)$  возвращает наибольшую степень двойки, делящую величину  $r + 1$ . Из определения следует, что множество  $M(n)$  конечно, содержит не более  $\lfloor \log_2 n \rfloor + 1$  чисел и отличается от множества  $M(n + 1)$  лишь одним элементом.

**Теорема А.3.** Пусть заданы параметры  $\lambda$  и  $\tau$ , определяющие длину подхода к циклу и длину цикла последовательности (А.1). Тогда найдутся натуральные индексы  $r$  и  $n = r + \tau$  такие, что

1. элемент  $a_r$  принадлежит множеству  $M(n)$  и выполнено равенство  $a_n = a_r$ ,
2.  $\lambda + \tau \leq n < \lambda + 2\tau$ .

*Доказательство.* Определим в качестве параметра  $k$  целое число, удовлетворяющее неравенствам  $2^k \leq \tau < 2^{k+1}$  и рассмотрим целые числа

$$r = 2^k \left\lceil \frac{\lambda + 1}{2^k} \right\rceil - 1 \quad \text{и} \quad n = r + \tau.$$

Очевидно, что  $r < n$  для любого целого  $\tau \geq 1$ . Представим  $\left\lceil \frac{\lambda+1}{2^k} \right\rceil = 2^l s$ , где  $l \geq 0$  целое число и  $s = 2h + 1$  нечетное целое число. Тогда  $r$  имеет вид

$$r = 2^{k+l} s - 1 = 2^{k+l} (2h + 1) - 1 = 2^{k+l} - 1 + h 2^{k+l+1}, \quad (\text{A.8})$$

то есть  $r \equiv 2^{k+l} - 1 \pmod{2^{k+l+1}}$  и мы получаем, что  $\nu_2(r + 1) = k + l$ . Поскольку выполнено неравенство

$$r + 2^{k+l+1} \geq r + 2^{k+1} > r + \tau = n$$

мы получаем, что индекс  $r$  принадлежит множеству  $M(n)$ . Учитывая, что  $\tau$  есть период последовательности (A.1), то  $a_r = a_{r+\tau} = a_n$ . Первое утверждение теоремы доказано.

Для доказательства второго утверждения теоремы получим оценки снизу и сверху на величину  $r$ . Воспользовавшись неравенством

$$x \leq \lceil x \rceil < x + 1,$$

выполненным для любого действительного  $x > 0$ , получим

$$\begin{aligned} \lambda = 2^k \left( \frac{\lambda + 1}{2^k} \right) - 1 &\leq 2^k \left\lceil \frac{\lambda + 1}{2^k} \right\rceil - 1 = r \\ &< 2^k \left( \frac{\lambda + 1}{2^k} + 1 \right) - 1 = \lambda + 2^k \leq \lambda + \tau, \end{aligned}$$

то есть неравенство  $\lambda \leq r < \lambda + \tau$ , из которого следует утверждение теоремы.  $\square$

Утверждение теоремы в явном виде задает нам множество  $M(n)$  в котором содержится элемент  $a_r$  такой, что  $a_r = a_n$ . Более того, теорема позволяет получить оценку сверху на максимальное число элементов последовательности (A.1), которые необходимо вычислить для нахождения указанного равенства.

Мы можем построить множество  $M(n)$  следующим образом. Разобьем исходную последовательность (А.1) на несколько подпоследовательностей таким образом, что первая подпоследовательность содержит все элементы с индексами  $i$  такими, что  $i + 1$  нечетно, вторая — элементы индексами  $i$  такими, что  $i + 1$  делится в точности на двойку, третья — элементы с индексами  $i$  такими, что  $i + 1$  делится в точности на четверку и так далее.

Тогда в множество  $M(n)$  входит по одному элементу из каждой подпоследовательности с максимальным индексом, не превосходящим  $n$ . Например, для  $n = 16$  множество  $M(16)$  имеет вид

$$M(16) = \{a_{14}, a_{13}, a_{11}, a_7, a_{15}\}.$$

Мы храним множество  $M(n)$  в массиве  $T$ , содержащем элементы из каждой подпоследовательности с максимальным индексом. Элемент  $T[0]$  содержит элемент первой подпоследовательности,  $T[1]$  — элемент второй подпоследовательности и так далее.

### Алгоритм А.3 (Алгоритм Госпера)

**Вход:** Отображение  $f : \mathcal{M} \rightarrow \mathcal{M}$  и начальный элемент  $a_0$ .

**Выход:** Значение длины цикла  $\tau$ .

1. Определить начальные значения:  $a = a_0$ ,  $n = 1$ ,  $t = 1$  и  $T[0] = a_0$ .
2. Вычислить  $a = f(a)$ .
3. Для всех  $k$  от 0 до  $t - 1$  выполнить
  - 3.1. Если  $T[k] = a$ , то положить  $\tau = n - 2^k \left(1 + \left\lfloor \frac{n - 2^k + 1}{2^k} \right\rfloor\right) + 1$  и завершить алгоритм.
4. Вычислить  $n = n + 1$  и  $k = \text{ntz}(n)$ .
5. Если  $k = t$ , то вычислить  $t = t + 1$ .
6. Определить  $T[k] = a$  и вернуться на шаг 2. □

Неизвестное нам значение  $\tau$  мы определяем на четвертом шаге алгоритма. Из (А.7) и (А.8) следует, что при завершении работы алгоритма величина  $h = \left\lfloor \frac{n - (2^k - 1)}{2^{k+1}} \right\rfloor$ , величина  $r = 2^k - 1 + h2^{k+1}$ . Поскольку  $\tau = n - r$ , то мы получаем равенство, приведенное выше.

### А.2.4 Алгоритм Ниваша

Алгоритм Ниваша основан на следующей очень простой идее. Пусть на множестве  $\mathcal{M}$  задано отношение упорядоченности, то есть для любых двух элементов  $a, b \in \mathcal{M}$  определена функция  $h : \mathcal{M} \rightarrow \{-1, 0, 1\}$  такая,

что

$$h(a, b) = \begin{cases} -1, & \text{если } a < b, \\ 0, & \text{если } a = b, \\ 1, & \text{если } a > b. \end{cases}$$

В этом случае, в цикле последовательности (A.1) может быть определен наименьший элемент  $a_l$  такой, что  $h(a_l, a_n) = -1$  для всех индексов  $n = \lambda, \dots, \lambda + \tau - 1$  при  $n \neq l$ . Идея Ниваша заключается в том, что минимальный элемент может быть определен при первом проходе цикла, тогда на втором проходе цикла будет найдено совпадение.

Для реализации поиска минимального элемента нам потребуется массив  $T$ , элементами которого будут являться пары  $(a_n, n)$  содержащие значение элемента последовательности и его индекс. Мы будем обозначать символом  $T[i].a$  значение элемента последовательности, содержащееся в  $i$ -й ячейке массива, аналогично  $T[i].n$  будет означать индекс сохраненного в ячейке элемента последовательности.

#### Алгоритм А.4 (Алгоритм Ниваша)

**Вход:** Отображение  $f : \mathcal{M} \rightarrow \mathcal{M}$  и начальный элемент  $a_0$ .

**Выход:** Значение длины цикла  $\tau$ .

1. Определить значения  $a = a_0$ ,  $n = 0$ ,  $k = 1$  и  $T[0] = (a_0, 0)$ .
2. Определить  $a = f(a)$ ,  $n = n + 1$  и  $i = k$ .
3. **Пока** ( $i \geq 0$  и  $h(a, T[i].a) = -1$ ) **выполнять**  $i = i - 1$ .
4. **Если**  $h(a, T[i].a) = 0$ , **то** определить  $\tau = n - T[i].n$  и завершить алгоритм.
5. **Если**  $h(a, T[i].a) = 1$ , **то** определить новое значение  $T[i+1].a = a$ ,  $T[i+1].n = n$  и  $k = i + 2$ .
6. Вернуться на шаг 2. □

Легко видеть, что количество вычислений функции  $f$  в приведенном алгоритме не превышает величины  $\lambda + 2\tau$ , то есть длины подхода и двух циклов последовательности (A.1). Массив  $T$  реализует собой стек, в котором хранятся элементы последовательности, отсортированные по возрастанию. Каждый новый вырабатываемый элемент  $a$  помещается в стек. Если в нем есть элементы, большие чем  $a$ , то они удаляются.

Если предположить, что элементы последовательности (A.1) являются реализацией некоторой случайной, равномерно распределенной на множестве  $\mathcal{M}$  величины, то, как показано в [29, п.1.2.10], с ростом индекса  $n$  размер стека растет как величина порядка  $O(\log_2 n)$ . Таким образом, мы можем считать, что величина стека в алгоритме Ниваша составляет  $\lceil \log_2(\lambda + 2\tau) \rceil$  элементов, каждый из которых хранит элемент последовательности (A.1) и его индекс.

Для сравнения, сведем в одну таблицу различные характеристики описанных нами выше алгоритмов. Во второй колонке мы приводим

оценку трудоемкости алгоритма, измеряемую в количестве вычислений функции  $f$ . В третьей колонке содержится количество ячеек памяти, необходимых для вычисления длины цикла  $\tau$ .

<i>Алгоритм</i>	<i>Трудоемкость</i>	<i>Объем памяти</i>
Флойд	$\tau \left( 3 \left\lceil \frac{\lambda}{\tau} \right\rceil + 1 \right)$	3
Брент	не менее $\tau + \frac{3}{2} \max\{\lambda + 1, \tau\}$	4
Госпер	не более $\lambda + 2\tau$	$\lceil \log_2 m \rceil + 4$
Ниваш	не более $\lambda + 2\tau$	$2\lceil \log_2(\lambda + 2\tau) \rceil$

Рассмотрение вопроса о трудоемкости приведенных в таблице алгоритмов в зависимости от мощности  $m$  множества  $\mathcal{M}$ , сводится к определению значений математического ожидания  $E_m(\lambda, f)$  и  $E_m(\tau, f)$  для величин  $\lambda$  и  $\tau$ , соответственно, при случайном выборе отображения  $f$ . Хорошо известно, см. например [5, п.5.3], что

$$\lim_{m \rightarrow \infty} \frac{E_m(\lambda, f)}{\sqrt{m}} = \lim_{m \rightarrow \infty} \frac{E_m(\tau, f)}{\sqrt{m}} = \sqrt{\frac{\pi}{8}}. \quad (\text{A.9})$$

Таким образом, асимптотическая оценка у всех приведенных алгоритмов одинакова и составляет  $O(\sqrt{m})$ .

## АНАЛИТИЧЕСКИЕ РЕЗУЛЬТАТЫ

В этом приложении мы кратко сформулируем известные результаты из аналитической теории чисел, относящиеся к оценкам количества простых чисел и количества простых делителей с заданными ограничениями. Мы не приводим строгих доказательств, поскольку это явно выходит за рамки нашей тематики. Вместе с тем, излагаемые утверждения и теоремы используются нами как при обосновании трудоемкости, так и при выборе параметров изложенных ранее алгоритмов.

### В.1 Количественные оценки простых чисел

Пусть  $x > 0$  некоторое натуральное число. Обозначим символом  $\pi(x)$  количество простых чисел, не превосходящих числа  $x$ . Вычисление точного значения функции  $\pi(x)$  равносильно построению всех простых чисел на интервале  $[1, x]$  и представляет собой сложную вычислительную задачу, см. алгоритм 6.1. На практике, как правило, используются приближенные значения функции.

Впервые достаточно точные оценки значения функции  $\pi(x)$  были установлены Пафнутием Львовичем Чебышовым в 1850 году.

**Теорема В.1** (доказательство см. в [7, гл. 2]). *Для всех  $x \geq 6$  верны неравенства*

$$a \frac{x}{\ln x} \leq \pi(x) \leq b \frac{x}{\ln x},$$

где  $a = \frac{\ln 2}{2} = 0,346\dots$ ,  $b = 5 \ln 2 = 3,465\dots$

Заметим, что Чебышовым были получены более точные значения параметров  $a = 0,921\dots$ ,  $b = 1,105\dots$ , но при достаточно больших значениях  $x$ . Асимптотическая форма данного утверждения выглядит следующим образом.

**Теорема В.2** (доказательство см. в [12, гл. 3]). *Выполнено равенство*

$$\lim_{x \rightarrow \infty} \pi(x) \left( \frac{x}{\ln x} \right)^{-1} = 1.$$

Приведем точные значения и приближенные оценки функции  $\pi(x)$  для некоторых значений вида  $x = 10^n$  при  $n = 1, \dots, 10$ .

$n$	$\pi(10^n)$	автор	$x/\ln x$
1	4	—	4,342...
2	25	L. Pisano (1202)	21,714...
3	168	F. van Schooten (1657)	144,765...
4	1229	F. van Schooten (1657)	1085,74...
5	9592	T. Brancker (1668)	8685.89...
6	78498	A. Felkel (1785)	72382.41...
7	664579	J. P. Kulik (1867)	620420.68...
8	5761455	Meissel (1871)	5428681.02...
9	50847534	Meissel (1886)	48254942.43...
10	455052511	D. Lehmer (1959)	434294481.903...

Как видно из таблицы, константы, полученные Чебышевым, верны, начиная с  $x = 10^5$ .

## В.2 Количественные оценки чисел с маленькими простыми делителями

При исследовании трудоемкости алгоритмов факторизации и дискретного логарифмирования часто возникает необходимость в оценке количества целых чисел не превосходящих некоторой величины, и имеющих небольшие простые делители.

Обозначим символом  $\psi(x, y)$  количество натуральных чисел  $n \leq x$ , у которых наибольший простой делитель не превосходит  $y$ . Для небольших значений  $x$  значение функции  $\psi(x, y)$  может быть вычисленно в явном виде, например,  $\psi(125, 5) = 36$ , поскольку только числа

2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32,  
36, 40, 45, 48, 50, 54, 60, 64, 72, 75, 80, 81, 90, 96, 100, 108, 120, 125

делятся на простые, меньшие либо равные 5.

При больших значениях  $x$  получение точного значения величины  $\psi(x, y)$  является сложной вычислительной задачей. Одна из первых оценок функции  $\psi(x, y)$  была получена де Брюином (N.G. de Bruijn) в работе [18].

**Лемма В.1** (де Брюин). *Для любого целого  $k \geq 1$  выполнено неравенство  $\psi(y^k, y) \geq C_k^{\pi(y)+k}$ , где  $C_k^n = \frac{n!}{k!(n-k)!}$ , а функция  $\pi(y)$  определяет количество простых, не превосходящих  $y$ .*



Применим утверждение леммы к значению функции  $\psi(125, 5)$ . Поскольку  $125 = 5^3$  и  $\pi(5) = 3$ , то

$$36 = \psi(125, 5) \geq C_3^{3+3} = 20.$$

Таким образом, утверждение леммы выполнено, однако оценка величины  $\psi(x, y)$  оказывается достаточно грубой.

Асимптотическое поведение функции  $\psi(x, y)$  исследовано в работе [45]. Доказан следующий результат.

**Теорема В.3** ([45, §2]). Пусть  $0 < \varepsilon < \frac{1}{2}$  некоторая действительная константа. Если выполнены неравенства

$$\ln^\varepsilon x < \ln y < \ln^{1-\varepsilon} x,$$

то при  $x \rightarrow \infty$  выполнено  $\psi(x, y) = xe^{-u \ln u + o(u \ln u)}$ , где  $u = \frac{\ln x}{\ln y}$ .

# ЛИТЕРАТУРА

- [1] *Бухштаб А.А.* Теория чисел. – М.:Просвещение. – 1966. – 384 с.
- [2] *Вирт Н.* Алгоритмы и структуры данных. – М.:Мир. – 1989. – 360 с.
- [3] *Галочкин А.И., Нестеренко Ю.В. и Шидловский А.Б.* Введение в теорию чисел. – М.:Изд-во Московского Университета. – 1984. – 152 с.
- [4] *Гаишков С.Б.* Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // Дискретная математика. – №. 4. – Vol. 10. – 1998. – с. 35-38.
- [5] *Колчин В.Ф.* Случайные графы. – 2-е изд. – М.:ФИЗМАТЛИТ, 2004. – 206 с.
- [6] *Кострикин А.И.* Введение в алгебру. – М.:Наука. – 1977. – 495 с.
- [7] *Нестеренко Ю.В.* Теория чисел. – М.:Академия. – 2008. – 272 с.
- [8] *Нестеренко А.Ю.* Алгоритмы поиска длин циклов в последовательностях и их приложения // Фундаментальная и прикладная математика. – №. 6. – Т. 16. – 2010. – с. 109-122.
- [9] *Нечаев В.И.* Элементы криптографии (Основы теории защиты информации). – М.:Высш.шк. – 1999. – 109 с.
- [10] *Сушкевич А.К.* Теория чисел. Элементарный курс. – Харьков:Изд-во Харьковского университета. – 1954. – 204 с.
- [11] *Ноден П. и Китте К.* Алгебраическая алгоритмика с упражнениями и решениями. – М.:Мир. – 1999. – 720 с.
- [12] *Прахар К.* Распределение простых чисел. – М.:Мир. – 1967. – 512 с.
- [13] *Уоррен Г.С.* Алгоритмические трюки для программистов. – М.:Вильямс. – 2003. – 288 с.
- [14] *Adleman L.* A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography // Proc. 20-th Annual IEEE Symposium on Foundations of Computer Science. – 1979. – pp. 55-60.
- [15] *Alford R., Granville A. and Pomerance C.* There are infinitely many Carmichael numbers // Annals of Mathematics. – Vol. 140. – 1994. – pp. 703-722.
- [16] *Beeler M., Gosper R.W., Schroepfel R.* HACMEM - MIT Artificial Intelligence Laboratory AIM 239. – February 1972. – 106 p.
- [17] *Brent R.P.* An Improved Monte-Carlo Factorization Algorithm // BIT. – Vol. 20. – 1980. – pp. 176-184.

- 
- [18] *de Bruijn N.G.* On the number of positive integers  $\leq x$  and free of prime factors  $> y$ . II // *Indag. Math.* — Vol. 28. — 1966. — pp. 239-247.
  - [19] *Carmichael R.D.* The Theory Of Numbers. — New York: J. Willey & Sons. — 1914. — 95 p.
  - [20] *Cocks C.* A Note on Non-Secret Encryption, CESG Report, 20 November 1973.
  - [21] *Cohen H.*, A Course in Computational Algebraic Number Theory, 3rd Edition. — Springer — 1996. — 545 p.
  - [22] *Davis J.A. and Holdridge D.B.*, Factorization Using the Quadratic Sieve Algorithm // Sandia National Laboratories. — Albuquerque, New Mexico. — 1983.
  - [23] *Diffie W., Hellman M.* Multiuser Cryptographic Techniques, 1976 National Computer Conference, New York City, 7-10 June 1976.
  - [24] *Ellis J.* The Story Of Non-Secret Encryption, 1987.  
<http://web.archive.org/web/20030610193721/http://jya.com/ellisdoc.htm>
  - [25] *Garner H.* The Residue Number System // *IRE Transactions on Electronic Computers.* — №. 2. — Vol. 8. — 1959. — pp. 140-147.
  - [26] *Gordon J.* Strong RSA keys // *Electronic Letters.* — №. 12. — Vol. 20. — June 1984. — pp. 514-516.
  - [27] *Granville A.* Primality testing and Carmichael numbers // *Notices of the American Mathematical Society.* — Vol. 39. — 1992. — pp. 696-700.
  - [28] *Hecke E.* Vorlesungen über die Theorie der algebraischen Zahlen. — Leipzig: Akademische Verlagsgesellschaft M.B.H. — 1923. — В русском переводе: Гекке Э. Лекции по теории алгебраических чисел. — М.: ГИТТЛ, 1940. — 260 с.
  - [29] *Knuth D.E.*, Fundamental Algorithms. Volume 1 of The Art of Computer Programming. — Addison-Wesley Professional. — 1969.
  - [30] *Knuth D.E.*, Seminumerical Algorithms. Volume 2 of The Art of Computer Programming. — Addison-Wesley Professional. — 1969.
  - [31] *Kraitchik M.* Théorie des Nombres. Tome I et II. — Paris: Gauthier-Villars. — 1926.
  - [32] *Lehman R.S.* Factoring Large Integers // *Mathematics Of Computation.* — №. 126. — Vol. 28. — 1974. — pp. 637-646.
  - [33] *Lehmer D.H. and Powers R.E.* On Factoring Large Numbers // *Bulletin Of the American Mathematical Society.* — №. 9. — Vol. 37. — 1931. — pp. 770-776.
  - [34] *McKee J.* Speeding Fermat's Factoring Algorithm // *Mathematics Of Computation.* — №. 228. — Vol. 68. — 1999. — pp. 1729-1737.

- 
- [35] *Merkle R.C.* Secrecy, Authentication and Public Key Systems // PhD. Thesis / Electrical Engineering. – June 1979. – P. 182.
  - [36] *Mihailescu P.* Fast Generation Of Provable Primes Using Search In Arithmetic Progressions // Advances in Cryptology – CRYPTO '94. – Vol. 839 Of Lecture Notes Of Computer Science. – Springer. – 1994. – pp. 282-293.
  - [37] *Miller G.L.* Riemann's Hypothesis and Tests for Primality // Journal of Computer and System Sciences. – №. 3. – Vol. 13. – 1976. – pp. 300-317.
  - [38] *Montgomery P.L.* Speeding The Pollard and Elliptic Curve Methods of Factorization // Mathematics Of Computation. – № 177. – Vol. 48. – 1987. – pp. 243-267.
  - [39] *Morrison M.A. and Brillhart J.* A Method of Factoring and the Factorization of  $F_7$  // Mathematics Of Computation. – №. 129. – Vol. 29. – 1975. – pp. 183-205.
  - [40] *Nivash G.*, Cycle Detecting Using a Stack // Journal Information Processing Letters – Volume 90 – Issue 3 – 2004.
  - [41] *Pohlig S.C. and Hellman M.E.* An Improved Algorithm for Computing Logarithms Over  $GF(p)$  and its Cryptographic Significance // IEEE Transactions Information Theory. – Vol. 24. – 1978. – pp. 106-110.
  - [42] *Pollard J.M.* Theorems on Factorization And Primality Testing // Proceedings of the Cambridge Philosophical Society. – №. 3. – Vol. 76. – 1974. – pp. 521-528.
  - [43] *Pollard J.M.* Monte Carlo methods for index computation  $(\text{mod } p)$  // Mathematics Of Computation. – №. 143. – Vol. 32. – 1978. – pp. 918-924.
  - [44] *Pomerance C.* The Quadratic Sieve Factoring Algorithm // Advances in Cryptology. Eurocrypt '84. – Vol. 209 Of Lecture Notes Of Computer Science. – Springer. – 1985. – pp. 169-182.
  - [45] *Pomerance C.* Two Methods in Elementary Analytic Number Theory // Number Theory and Applications / Ed. R.A. Molin. – 1989. – pp. 135-161.
  - [46] *Rabin M.O.* Probabilistic Algorithm for Testing Primality // Journal of Number Theory. – №. 1. – Vol. 12. – 1980. – pp. 128-138.
  - [47] *Rivest R.L., Shamir A. and Adleman L.* A Method For Obtaining Digital Signatures And Public-Key Cryptosystems// Comm. Of ACM, v.21, No. 2, pp. 120-126, 1978.
  - [48] *Sedgewick R., Szymansky T.G., Yao A.C.*, The Complexity of Finding Cycles In Periodic Functions // Siam Journal Of Computing – Vol.11 – №. 2 – 1982. – 376-390pp.
  - [49] *Shanks D.* Class Number, a Theory of Factorization and Genera // Proceedings Of Symposium Pure Mathematics. – Vol. 20. – AMS:Providence, R. I. – 1971. – pp. 415-440.

- 
- [50] *Silverman R.D.*, The Multiple Polynomial Quadratic Sieve // Mathematics Of Computation. – №. 177. – Vol. 48. – 1987. – pp. 329-339.
  - [51] *Solovay R. and Strassen V.* A Fast Monte-Carlo Test for Primality // SIAM Journal on Computing. – №. 1. – Vol. 6. – 1977. – pp. 84-85.
  - [52] *Western A.E. and Miller J.C.P.* Tables of Indices and Primitive Roots. – Vol. 9 of Royal Society Mathematical Tables. – Cambridge University Press. – 1968. – P. 384.
  - [53] *Williams H.C.* Primality Testing On A Computer // Ars Combinatoria. – Vol. 5. – 1978. – pp. 127-185.
  - [54] *Williams H.C.* A  $p + 1$  Method of Factoring // Mathematics Of Computation. – №. 159. – Vol. 39. – 1982. – pp. 225-234.
  - [55] *Williams H.C. and Schmid B.* Some remarks cocerning the MIT public-key cryptosystem // BIT. – Vol. 19. – 1979. – pp. 525-538.
  - [56] *Zhang Z.* Using Lucas Sequences to Factor Large Integers Near Group Orders // Fibonacci Quarterly. – №. 3. – Vol. 39. – 2001. – pp. 228-237.

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

## А

алгоритм

бинарный НОД, 12

вычисления

всех корней многочлена, 84

квадратного корня, 156

обратного элемента, 20, 28, 89

первообразного корня, 37

последовательности Люка, 142

символа Якоби, 71

случайного корня многочлена, 82

Гарнера, 26

гауссового исключения, 188

для колец, 223

деления многочленов, 46

дискретного логарифмирования

$\varrho$ -метод Полларда, 213

Госпера, 217

Полига-Хеллмана, 210

Полларда-Флойда, 215

доказательства простоты

Лемана, 163

Люка, 131

подъема решения, 57

поиска длин циклов

Брента, 265

Госпера, 268

Ниваша, 269

Флойда, 263

построения

простого числа, 148

сильно простого числа, 151

таблицы простых чисел, 117

решения

системы сравнений, 24

Тонелли-Шенкса, 77

факторизации

$\varrho$ -метод Полларда, 166

$p - 1$  Полларда, 169

Брента, 167

Вильямса, 170

Лемана, 163

по известным значениям  $d$  и  $e$ , 237

Полларда-Флойда, 166, 175

с помощью непрерывных дробей,

182, 193

Ферма, 155

Эвклида, 10, 86

для многочленов, 48

расширенный, 20

атака

Винера, 238

с адаптивным выбором

шифртекста, 247

## Б

бином Ньютона, 38

## В

вычет

абсолютно-наименьший, 17

квадратичный, 60

наименьший

неотрицательный, 17

## Г

гипотеза

Эйлера, 136

группа

мультипликативная, 41

обратимых элементов, 40, 43

циклическая, 41

## Д

делитель

наибольший общий (НОД), 8

многочленов, 47

дискриминант

иррациональности

квадратичной, 93

длина

подхода к циклу, 165, 259

цикла, 165, 259

дробь

непрерывная, 86

подходящая, 87

цепная, 86

## З

задача

вычисления индекса, 204  
 дискретного логарифмирования, 204  
 определения длины цикла, 262  
 построения коллизии, 251  
 построения прообраза, 251  
 факторизации, 16, 154  
 закон  
   взаимности  
     квадратичный, 62  
 значение  
   многочлена, 44

## И

индекс, 204  
 иррациональность  
   действительная, 87  
   квадратичная, 93  
     приведенная, 97  
     сопряженная, 94

## К

квадрат  
   полный, 93  
 код целостности сообщения, 247  
 коллизия, 251, 258  
 корень  
   квадратный  
     по модулю простого числа, 59  
   многочлена, 52  
   первообразный, 30  
 кратное  
   наименьшее  
     общее (НОК), 32  
 кратность  
   корня, 52  
 критерий  
   Корсельта, 120  
   Эйлера, 61

## Л

лемма  
   Безу, 20  
   для  $n$  переменных, 22  
   для многочленов, 49  
   Гаусса, 63  
   Гордона, 152  
   о факторизации, 180  
 логарифм  
   дискретный, 204

## М

метод  
   больших и малых шагов, 206  
   Крайчика, 181  
   решета, 197, 199  
   согласования, 173, 206  
   Флойда, 165, 176  
 многочлен, 43  
   линейный, 44  
   неприводимый, 45  
   нормированный, 44  
   приведенный, 44  
   унитарный, 44

## Н

наилучшее приближение, 113  
 невычет  
   квадратичный, 60  
 нуль  
   многочлена, 52

## О

область связности, 260  
 образ элемента, 260  
 орбита  
   элемента, 258  
 остаток от деления, 46

## П

период, 259  
 подход  
   к циклу, 259  
 подъем решения, 56  
 показатель  
   числа, 29  
 поле  
   конечное, 40  
 порядок  
   элемента, 30  
 последовательность  
   рекуррентная  
     Люка, 139, 169  
     Фибоначи, 11  
 производная  
   многочлена, 53

## Р

решето  
   линейное, 196

Сундарамы, 118  
Эратосфена, 118

## С

свойство  
    мультипликативности, 247  
связная компонента, 260  
символ  
    Лежандра, 60  
    Якоби, 68  
система вычетов  
    абсолютно-наименьших  
        полная, 18  
    полная, 17  
    приведенная, 26  
степень  
    многочлена, 44  
стойкость  
    семантическая, 247  
схема шифрования  
    RSA, 233, 248  
        вариант RSAES, 250  
        вариант RSA-OAEP, 251  
    Рабина, 255  
    Эль-Гамала, 257

## Т

теорема  
    арифметики основная, 15  
        для многочленов, 51  
    Виета, 95, 235  
    Дирихле, 146  
    китайская  
        об остатках, 23  
    Ламе, 11  
    Лемана, 161  
    Лемера, 133  
    Люка, 130  
    Моррисона, 144  
    о первообразном корне  
        по модулю  $p$ , 31  
        по модулю  $p^\alpha$ , 38  
    о полном квадрате, 157  
    Поклингтона, 132  
    Рабина, 125  
    Ферма, 28  
    Чебышева, 271  
    Эвклида, 14, 138  
    Эйлера, 28

тест

Миллера-Рабина, 129  
Соловея-Штрассена, 124

## Ф

факторная база, 186, 220  
функция  
    Кнута-Шрёппеля, 191  
    хеширования  
        бесключевая, 251  
    Эйлера, 26, 234

## Ц

целая часть, 85

## Ч

частное от деления, 46  
частные  
    неполные, 86  
    полные, 86  
число  
    алгебраическое, 104  
    взаимно простое, 8  
    Кармайкла, 121  
    Мерсенна, 136  
    простое, 13  
        близнец, 150  
    совершенное, 135  
    составное, 14  
    Ферма  
        седьмое, 186  
    эквивалентное, 107

## Э

элемент  
    обратимый, 40, 43  
    примитивный, 30  
    терминальный, 259