А.Ю. Нестеренко

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Москва 2012

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
Московский государственный институт
электроники и математики
(технический университет)

А.Ю. Нестеренко

Теоретико-числовые методы в криптографии

Рекомендовано Редакционно-издательским советом института
в качестве учебного пособия

Москва 2012

УДК 511

Рецензенты: докт. физ. - мат. наук, проф. В.Г. Данилов, зав. кафедрой математического анализа МТУСИ;
докт. физ. - мат. наук, проф. В.Г. Чирский, зав. кафедрой теории чисел математического факультета МПГУ.

Нестеренко А.Ю.
Теоретико-числовые методы в криптографии: учебное пособие. Моск. гос. ин-т. электроники и математики. 2012, 224 с.
ISBN 978-5-94506-320-4

Изложен курс алгоритмической теории чисел с приложениями. Основное внимание уделено вопросам строгого обоснования, эффективной реализации и анализа трудоемкости алгоритмов, используемых в криптографических приложениях.

Рассматриваются вопросы решения некоторых диофантовых уравнений, вопросы решения сравнений произвольных степеней по простому и составному модулям, а также методы доказательства простоты и построения больших простых чисел, методы решения задач дискретного логарифмирования и разложения больших целых чисел на множители.

Предназначено студентам старших курсов МИЭМ, обучающимся по специальности «Компьютерная безопасность».

ISBN 978-5-94506-320-4 УДК 511

Оглавление

Введение

Настоящее учебное пособие содержит в себе изложение вопросов элементарной алгоритмической теории чисел. Мы приводим строгое обоснование большого числа теоретико-числовых алгоритмов, возникающих при реализации, построении параметров и исследовании целого класса криптографических схем и протоколов. Также мы уделяем большое внимание вопросам эффективной реализации алгоритмов на современных вычислительных средствах.

Изложение начинается с основ – теории деления в кольцах челых чисел и многочленов, теории полиномиальных сравнений, теории цепных дробей, а заканчивается – изложением алгоритмов построения больших простых чисел, алгоритмов решения задач разложения больших целых чисел на множители и дискретного логарифмирования.

Прежде чем начинать изложение, нам необходимо формализовать понятие сложности алгоритма – некоторой счетной последовательности действий. Мы будем измерять сложность алгоритма некоторой величиной, позволяющей охарактеризовать алгоритм с точки зрения его практической применимости. Чем меньше данная величина, тем больше целесообразность применения данного алгоритма.

Определение 1. *Под сложностью алгоритма мы будем подразумевать количество выполняемых в ходе алгоритма операций над элементами некоторого конечного множества. Для сложности алгоритма мы также будем использовать синоним — трудоемкость алгоритма.*

Из нашего определения сразу следует, что понятие сложности не однозначно и зависит от выбора конечного множества, над которым производятся вычисления. Существует два подхода при выборе множества операндов — первый основывается на фиксации некоторого математического объекта, например, группы или кольца. Второй подход основывается на фиксации длины регистров вычислительного средства, которое будет реализовывать данный алгоритм. Первый подход более прост, универсален и принят в математических исследованиях, второй подход привязан к вычислительному средству, более точен и позволяет оценить сложность алгоритма в тактах работы вычислительного средства. Мы будем использовать первый подход, оставляя детальный анализ разработчикам программного обеспечения.

В обоих случаях рассматривается некоторый параметр n, характеризующий множество, элементами которого оперирует алгоритм. Сложность алгоритма представляется в виде функции от n.

Пусть $n > 0$ — произвольная целая или действительная переменная. Напомним, что символом $O\left(f(n)\right)$ обозначается функция такая, что

$$\lim_{n\to\infty} \frac{O\left(f(n)\right)}{f(n)} = c,$$

где $c > 0$ некоторая константа. Рассмотрим функцию

$$L(x, z, n) = e^{z(\log n)^x (\log\log n)^{1-x}}, \tag{1}$$

действительных переменных x и z, где $0 \leqslant x \leqslant 1$, $z \geqslant 0$ и $n > 0$ целая или действительная переменная.

Определение 2. *Пусть $f(n)$ — функция, задающая сложность алгоритма, функция $L(x, z, n)$ определена равенством (1), значения x, z фиксированы и $n \to \infty$. Мы будем использовать следующую терминологию.*

1. *Функция $f(n)$ называется полиномиальной, если*

$$f(n) = O\left(L(0, z, n)\right) = O\left(\log^z n\right) \quad \textit{при} \quad z > 0.$$

2. *Функция $f(n)$ называется экспоненциальной, если*

$$f(n) = O\left(L(1, z, n)\right) = O\left(n^z\right) \quad \textit{при} \quad z > 0.$$

3. *Функция $f(n)$ называется субэкспоненциальной, если*

$$f(n) = O\left(L(x, z, n)\right) \quad \textit{при} \quad 0 < x < 1, \quad z \neq 0.$$

Рассмотрим также частные случаи.

4. *Если $f(n) = O\left(1\right)$ или, что равносильно, $z = 0$ при любом значении x, то $f(n)$ называется константой.*

5. *Если $f(n) = O\left(n\right)$ экспоненциальна при $z = 1$, то $f(n)$ называется сложностью тотального перебора.*

Как видно из данного определения, субэкспоненциальная функция занимает промежуточное положение между полиномиальной и эспоненциальной функциями. Действительно при фиксированных значениях z и $n > 1$ получаем

$$(\log n)^z = e^{z \log\log n} = L(0, z, n) = \lim_{x \to 0} L(x, z, n) \leqslant$$
$$L(x, z, n) \leqslant \lim_{x \to 1} L(x, z, n) = L(1, z, n) = e^{z \log n} = n^z.$$

Здесь мы неявно используем тот факт, что при фиксированных значениях z, n функция $L(x, z, n)$ является монотонно неубывающей функцией.

Отметим одну особенность, возникающую при решении криптографических задач. Все рассматриваемые нами задачи обязательно имеют решение, поиск которого может быть сведен к перебору всех элементов некоторого конечного множества, характеризуемого целочисленным параметром n. Следовательно, максимальная сложность решения подобной задачи определяется сложностью тотального перебора, то есть $O(n)$.

Однако в используемых на практике приложениях значение параметра n настолько велико, что применение тотального перебора не позволяет найти решение за приемлемое время, даже с использованием максимально производительных вычислительных средств. В связи с этим, наша задача сводится к поиску алгоритмов, имеющих сложность, меньшую сложности тотального перебора.

Отметим, что существование полиномиального, то есть быстрого алгоритма решения рассматриваемых нами задач является, скорее, приятным исключением, чем правилом. Задач, имеющих полиномиальные алгоритмы решения, крайне не много, большинство из них мы перечисляем ниже:

- вычисление наибольшего общего делителя;
- возведение элемента группы в целочисленную степень;
- нахождение корня многочлена по модулю простого числа;
- доказательство простоты целого числа;
- построение простого числа.

Для остальных задач, рассматриваемых нами, достижимый минимум сложности – существование субэкспоненциального алгоритма.

Теперь рассмотрим еще один способ классификации алгоритмов. Традиционно принято подразделять все алгоритмы на *детерминированные* и *вероятностные*. Для детерминированного алгоритма оценка сложности вычисляется однозначно, в то время как для вероятностного алгоритма оценка сложности вычисляется при некоторых предположениях, которые могут существенно влиять на получаемые результаты. Приведем некоторые примеры и поясним вышесказанное.

Определение 3. *Алгоритм называется детерминированным, если после фиксированного числа шагов (операций над элементами конечного множества) результат работы данного алгоритма всегда является решением поставленной задачи.*

Отметим, что слово «всегда» в приведенном определении является существенно важным.

Определение 4. *Мы будем называть алгоритм вероятностным, если выполнено одно из следующих утверждений*

- *результат работы алгоритма является решением поставленной задачи с некоторой вероятностью,*
- *оценка числа шагов алгоритма является случайной величиной; если для этой величины можно определить математическое ожидание, то именно оно и называется оценкой сложности алгоритма,*
- *алгоритм заканчивает свою работу с некоторой вероятностью.*

Собственно один и тот же алгоритм может рассматриваться и как детерминированный, и как вероятностный, в зависимости от нашего толкования этого термина, либо от попытки минимизировать его сложность.

Рассмотрим следующий пример. Пусть у нас имеется урна, в которой находится n шаров – один красный и $n-1$ черных шаров. Мы можем вытаскивать из урны шары, не возвращая их на место. Наша задача вытащить красный шар.

Если мы подряд вытащим из урны все n шаров, то среди них обязательно окажется красный шар, следовательно, мы получаем детерминированный алгоритм. Сложность этого алгоритма равна n вынимания шара из урны.

Теперь опишем вариант решения той же задачи с помощью вероятностного алгоритма, удовлетворяющего первому утверждению нашего определения.

Зафиксируем число попыток вытащить шар из урны и обозначим его символом k. В этом случае вероятность успешного завершения алгоритма, или другими словами, вероятность того, что мы не вытащим k черных шаров подряд, будет равна $\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{n-k+1} \sim \frac{k}{n}$ при небольших значениях k.

Таким образом, если мы хотим иметь полиномиальный алгоритм, то выберем $k = \log n$, при этом вероятность его успешного завершения мала и равна $\frac{\log n}{n}$. Очевидно, что при $k = n$ мы получим описанные ранее детерминированный алгоритм, поскольку вероятность его успешного завершения равна единице.

Зафиксируем вероятность успешного завершения алгоритма и обозначим ее символом p, $0 < p \leqslant 1$, тогда среднее число шагов, необходимых для успешного завершения алгоритма, равно pn. Таким образом, фиксация вероятности успеха приводит к определению трудоемкости алгоритма. Если мы положим вероятность равной единице, то мы, очевидно, получим, что среднее число шагов алгоритма (вытаскиваний шара из урны) равно n. Это второй вариант вероятностного алгоритма в нашем определении.

Третий вариант алгоритма в нашем определении может быть получен, если мы будем возвращать вынутые черные шары обратно в урну. В этом случае существует вероятность, что мы так и не вытащим красный шар, то есть не завершим выполнение алгоритма.

Суммируя изложенное, заметим, что мы могли бы изначально определить понятие сложности алгоритма, как функцию двух аргументов — количества выполненных им шагов и вероятности успешного завершения алгоритма. Однако такой подход к исследованию трудоемкости не является общепринятым. В дальнейшем, если это не оговорено особо, мы будем оценивать сложность вероятностных алгоритмов в предположении, что вероятность их успешного завершения не менее $\frac{1}{2}$.

Глава 1

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

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

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*

$$b = aq + r, \quad 0 \leqslant r < |a|. \tag{1.1}$$

Доказательство. Без ограничения общности будем считать, что $a > 0$. Тогда найдется наибольшее целое число q такое, что $aq \leqslant b$ и $b < a(q+1)$. Обозначая $r = b - aq$, получим неравенство $0 \leqslant r < a$ 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 сдедует, что $|r_1 - r| < a$. Таким образом, $r_1 - r = 0$ и $r_1 = r$, $q_1 = q$. Лемма доказана. □

Определение 1.2. *Пусть a, b целые числа. Мы будем называть целое число r, $0 \leqslant r < |a|$, 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 $\mathbf{НОД}(a,\ b)$.

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 $\mathbf{НОД}(a,\ b) > 0$.

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. $\mathbf{НОД}(a,\ b) = \mathbf{НОД}(b,\ a)$,
2. $\mathbf{НОД}(-a,\ b) = \mathbf{НОД}(a,\ b)$,
3. $\mathbf{НОД}(a,\ a) = \mathbf{НОД}(a,\ 0) = |a|$,
4. $\mathbf{НОД}(ac,\ bc) = |c| \cdot \mathbf{НОД}(a,\ b)$,
5. *Если* $\mathbf{НОД}(a,\ c) = 1$, *то* $\mathbf{НОД}(a,\ cb) = \mathbf{НОД}(a,\ b)$,
6. $\mathbf{НОД}(a,\ b) = \mathbf{НОД}(a \pm b,\ a)$,
7. $\mathbf{НОД}(a,\ b) = \mathbf{НОД}(a,\ r)$, *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 $0 \leqslant r < |a|$. Обозначим $d = \mathbf{НОД}(a,\ b)$, 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, $d_1 | \mathbf{НОД}(a,\ b) = d$ и $d_1 \leqslant d$.

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 $d_2 | \mathbf{НОД}(a,\ b) = d$ и $d_2 \leqslant d$. □

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. Используя шестое утверждение, можно получить простейший алгоритм вычисления наибольшего делителя, который использует только операцию вычитания натуральных чисел.

1.2 Алгоритм Эвклида

Основываясь на седьмом утверждении леммы 1.2, мы 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 $r_{-1}, r_0, \ldots, r_{n+1}$ и $q_1, \ldots, q_{n+1}$ равенствами (1.2). Тогда найдется такое натуральное число n, что $r_{n+1} = 0$ и*

$$r_n = \mathbf{НОД}\,(a,\ b)\,.$$

Доказательство. В силу леммы 1.1 для всех $n = 0,\ 1,\ \ldots$ выполнено равенство $0 \leqslant r_{n+1} < r_n$. Следовательно, члены последовательности r_{-1}, $r_0, \ldots$ 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

$$\mathbf{НОД}\,(a,\ b) = \mathbf{НОД}\,(r_1,\ a) = \ldots = \mathbf{НОД}\,(r_n,\ 0) = r_n$$

и утверждение теоремы. □

Вычисление последовательности остатков $r_{-1}, r_0, \ldots, r_{n+1}$ 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: $\mathbf{НОД}\,(a,\ b)$ – 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 $q = \left\lfloor \dfrac{r_{-1}}{r_0} \right\rfloor$.
   - **2.2.** Определить $r = r_{-1} - qr_0$ и присвоить $r_{-1} = r_0$, $r_0 = r$.
3. Определить $\mathbf{НОД}\,(a,\ b) = r_{-1}$. □

Следующая теорема позволяет оценить число шагов алгоритма Эвклида.

Теорема 1.2 (Ламе[1], 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 вычислимая константа.*

Для доказательства этой теоремы нам потребуется сделать небольшое отступление.

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

$$\begin{aligned} &A_0 = 0, \quad A_1 = 1, \\ &A_{n+1} = A_n + A_{n-1}, \quad \textit{при} \quad n = 1,\ 2,\ \ldots \end{aligned} \tag{1.3}$$

последовательностью Фибоначи .

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

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

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

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

□

Доказательство теоремы Ламе. Вначале мы докажем неравенство

$$r_{k-1} \geqslant A_{n+1-k}, \quad \text{при} \quad k = 0,\ 1,\ \ldots,\ n, \tag{1.4}$$

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

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

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

[1]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

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

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

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

которое завершает доказательство теоремы. □

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 $c = 2c$, $x = \dfrac{x}{2}$ и $y = \dfrac{y}{2}$.

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** $(a,\ b) = cx$. □

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 $k \geqslant 0$, такую, что $c|a, c|b$ и **НОД** $(a,\ b) = c \cdot$ **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* **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 **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 **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 **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. □

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,

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

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

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

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. □

Легко доказать следующую простую лемму.

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

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

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 $p_1,\ \ldots,\ p_n$.

Рассмотрим целое число $N = p_1 \cdots p_n + 1$. Число N не делится нацело ни на одно простое число $p_1,\ \ldots,\ p_n$, 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 $p_1,\ \ldots,\ p_n$. Таким образом, мы нашли еще одно простое число, что противоречит нашему предположению. □

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

$$n = p_1 \cdots p_k. \tag{1.5}$$

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

$$p_1 \cdots p_k = q_1 \cdots q_s. \tag{1.6}$$

Будем считать, что $s \geqslant k$. 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 $q_j \cdots q_s$, $2 \leqslant j \leqslant s$, 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 $p_{s+1}, \ldots, p_k$ больше единицы, то последнее равенство невозможно и мы получаем, что $k = s$ и разложения в равенстве (1.6) совпадают. □

Перемножая в равенстве (1.5) одинаковые сомножители получим

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

где p_i различные простые числа, а α_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.

Глава 2

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 $m|(a-b)$ 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 $0 \leqslant x < m$, 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. $-\dfrac{m}{2} < x \leqslant \dfrac{m}{2}$ *при четном m;*

2. $-\dfrac{m-1}{2} \leqslant x \leqslant \dfrac{m-1}{2}$ *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

$$ax \equiv b \pmod{m}. \tag{2.1}$$

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* $\mathbf{НОД}(a,\ m) = 1$;
2. $N = d$, *если* $\mathbf{НОД}(a,\ m) = d$ *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* $\mathbf{НОД}(c,\ m) = 1$, *то* $ac \equiv bc \pmod{m}$,
2. *Пусть* $\mathbf{НОД}(a,\ b) = d$ *и* $d|m$, *тогда* $\dfrac{a}{d} \equiv \dfrac{b}{d} \pmod{\dfrac{m}{d}}$,
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 $\mathbf{НОД}(a,\ m) = 1$ и существуют два решения x, x_1 сравнения (2.1), тогда $ax \equiv ax_1 \equiv b \pmod m$ или, что равносильно, $ax = b + km$, $ax_1 = b + k_1 m$ 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 $\mathbf{НОД}(a,\ m) = d$, 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 $a_1 x \equiv b_1 \pmod{m_1}$, число решений которого, согласно первому утверждению теоремы, равно одному.

Пусть x_1 решение сравнения $a_1 x \equiv b_1 \pmod{m_1}$, тогда найдется целое число l такое, что $a_1 x_1 = b_1 + m_1 l$. Обозначим $x = x_1 + m_1 k$, где k произвольное целое число, тогда из равенства

$$ax = da_1(x_1 + m_1 k) = db_1 + dm_1 l + dm_1 k = b + m(l + k)$$

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. □

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

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

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

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

$$a_1 z \equiv b_1 \pmod{m_1},$$

где

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

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

$$z + km_1, \quad k = 0,\ \ldots,\ d - 1. \tag{2.3}$$

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

$$a(z + km_1) = d(a_1 z + ka_1 m_1) = d(b_1 + lm_1 + ka_1 m_1) = \\ = db_1 + (l + ka_1)m \equiv b \pmod{m}.$$

при некотором натуральном l.

Так или иначе, но решение сравнения (2.1) сводится к решению сравнения $az \equiv 1 \pmod{m}$, где $\mathbf{НОД}(a,\ m) = 1$. Верно следующее утверждение, авторство которого приписывается французскому математику [1] Этьену Безу (Étienne Bézout).

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

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

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

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

Вместо доказательства леммы, мы приведем алгоритм поиска коэффициентов z, w в соотношении (2.4) и докажем его корректность. Для нас является важным, что из леммы Безу вытекает разрешимость сравнения (2.2).

Для вычисления чисел z, w, удовлетворяющих равенству (2.4), можно воспользоваться следующим алгоритмом, который принято называть расширенным алгоритмом Эвклида.

Алгоритм 2.1 (Расширенный алгоритм Эвклида)

Вход: целые числа a, m такие, что $m > a > 0$.
Выход: целые числа z, w такие, что $az + bw = \mathbf{НОД}(a,\ b)$.

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**
  2.1. Определить $q = \left\lfloor \dfrac{r_{-1}}{r_0} \right\rfloor$.
  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 $\mathbf{НОД}(a,\ m) = r_{-1}$, $z = z_{-1}$, $w = w_{-1}$. □

[1] 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.

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*

$$az + mw = \mathbf{НОД}\,(a,\ m)\,.$$

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

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

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

$$az_k + mw_k = r_k, \quad k = -1, 0, \ldots, n, \tag{2.5}$$

где

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

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

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

Поскольку $r_n = \mathbf{НОД}\,(a,\ b)$, 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 $z \equiv a^{-1} \pmod m$.

2.2 Китайская теорема об остатках

Перейдем к рассмотрению систем сравнений и рассмотрим систему

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

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 $m_1, \ldots, m_k$ целые, взаимно простые числа, произведение которых равно $M = \prod_{j=1}^{k} m_j$. Тогда любого набора целых чисел $a_1, \ldots, a_k$ решение системы сравнений*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \ldots \\ x \equiv a_k \pmod{m_k}, \end{cases} \tag{2.7}$$

единственно по модулю M и удовлетворяет сравнению

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

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

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

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 $i = 1, \ldots, k$, или

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

при некоторых целых значениях $c_1, \ldots, c_k$. Поскольку все числа $m_1, \ldots, m_k$ 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. □

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

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

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. □

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

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

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

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. □

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, $m_1, \ldots, m_k$ и $a_1, \ldots, a_k$, удовлетворяющие теореме 2.3.
Выход: вычет x, $0 \leqslant x < M$ – решение системы сравнений (2.7).

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

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

$$0 \leqslant a_i bc < AM, \quad \text{где} \quad A = \max_{i=1,\ldots,k} a_i.$$

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 $a_1, \ldots, a_k$. Он основывается на следующей теореме.

Теорема 2.4. *Пусть $m_1, \ldots, m_k$ 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 $x_1, \ldots, x_k$, что $x_i < m_i$ для всех $i = 1, \ldots, k$ и*

$$x = x_1 + x_2 m_1 + x_3 m_1 m_2 + \ldots + x_k m_1 \cdots m_{k-1}. \tag{2.9}$$

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

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

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

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

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

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

где величина b_i^{-1} определяется из сравнения $b_i b_i^{-1} \equiv 1 \pmod{m_i}$. Поскольку $\mathbf{НОД}(b_i, m_i) = 1$, 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 $i = 1, \ldots, k$.

Изучая равенство (2.9), заметим, что для всех индексов $i = 1, \ldots, k$ 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 $i = 1, \ldots, k$. 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. □

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 [9]. Добавим, что в англоязычной и переводной литературе этот алгоритм, применительно к произвольному значению k, носит имя американского математика Харви Гарнера (Harvey L. Garner), см. [17].

Алгоритм 2.3 (Алгоритм Гарнера)

Вход: целые числа k, $m_1, \ldots, m_k$ и $a_1, \ldots, a_k$, удовлетворяющие теореме 2.3.
Выход: x, $0 \leqslant x < M$ – решение системы сравнений (2.7).

1. Определить $i = 2$, $b = 1$, $s = a_1 \pmod{m_1}$.
2. **Пока** $i \leqslant k$ **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. □

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

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

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*

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

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 $0,\ 1,\ \ldots,\ p-1$ взаимно простых с p ровно $p-1$ в силу условия $\mathbf{НОД}\,(0,\ p) = p$ (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, $0 \leqslant z < p^\alpha$, выполнено либо равенство $\mathbf{НОД}\,(z,\ p^\alpha) = 1$, либо условие $p \mid \mathbf{НОД}\,(z,\ p^\alpha)$. Поскольку среди чисел 0, 1, …, $p^\alpha - 1$ 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 α один из вычетов по модулю a, а β, 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 α не взаимно просто с a, $\mathbf{НОД}\,(\alpha,\ a) > 1$ или β не взаимно просто с b, $\mathbf{НОД}\,(\beta,\ b) > 1$, то мы сразу получаем, что $\mathbf{НОД}\,(\gamma,\ ab) > 1$. И наоборот, $\mathbf{НОД}\,(\gamma,\ ab) = 1$ только тогда, когда α и β 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. □

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* **НОД**$(a,\ m) = 1$*. Тогда*

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

Доказательство. Рассмотрим приведенную систему вычетов по модулю m

$$1,\ \ldots,\ m-1,$$

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

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

Сокращая на множитель, стоящий в правой части сравнения, получим утверждение теоремы. □

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

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

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*

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

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

Лемма 2.3. *Пусть $a, m > 0$ целые числа такие, что $\mathbf{НОД}(a,\ m) = 1$, и показатель числа a по модулю m равен q. Тогда выполнены следующие условия*

1. *Числа $1,\ a,\ a^2,\ \ldots,\ a^{q-1}$ 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, $0 \leqslant k < l < q$, 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 $0 \leqslant r_1 < q$ и $l = l_1 q + r_2$, где $0 \leqslant r_2 < q$.

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

$$a^{r_1} \equiv \left(a_1^k\right)^q a^{r_1} \equiv \left(a_1^l\right)^q a^{r_2} \equiv a^{r_2} \pmod m.$$

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 $q|s$. □

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* $\operatorname{ord}_m a = \varphi(m)$.

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* $\mathbf{НОД}(a,\ p) = 1$. *Тогда порядком числа a по модулю p называется показатель числа a по модулю p, то есть минимальное из чисел q таких, что $a^q \equiv 1 \pmod p$*

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

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 $\alpha \geqslant 1$.

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 2.4. *Пусть a, b целые числа, p простое число.*

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

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 2.3, 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

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

Используя второе утверждение леммы 2.3, получим, что $tx \equiv y \pmod y$ или $tx = yc$ при некотором целом c. Поскольку $\mathbf{НОД}(x,\ y) = 1$, 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 2.3 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*

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

Данное определение может быть обобщено на несколько целых чисел

$$\mathbf{HOK}\,(a_1,\ \ldots,\ a_k) = \min\{m \in \mathbb{N} :\ a_1|m,\ \ldots,\ a_k|m\}.$$

Лемма 2.5. *Верны следующие утверждения:*

1. *Любое общее кратное нескольких чисел $a_1,\ \ldots,\ a_k$ делится на их наименьшее общее кратное.*

2. *Наименьшее общее кратное взаимно простых чисел $a_1,\ \ldots,\ a_k$ равно их произведению, то есть $\mathbf{HOK}\,(a_1,\ \ldots,\ a_k) = \prod_{i=1}^{k} a_k$.*

3. *Если число b делится на каждое из попарно взаимно простых чисел $a_1,\ \ldots,\ a_k$, то оно делится и на их произведение.*

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

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

где q, r некоторые натуральные числа. В силу определения общего делителя, находим, что $r = s - mq$ делится на каждое из чисел $a_1,\ \ldots,\ a_k$ 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 $\mathbf{HOK}(a_1, \ldots, a_k)$, 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, $i = 2, \ldots, k$.

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

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

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 $\{t_1, \ldots, t_k\}$ множество различных показателей, которым принадлежат числа $1, 2, \ldots, p-1$. Определим $\tau = \mathbf{HOK}(t_1, \ldots, t_k)$ 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, $1 \leqslant i \leqslant k$, 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 2.4 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 τ число b_i такое, что $\operatorname{ord}_p b_i = q_i^{\alpha_i}$ для всех $i = 1, \ldots, r$.

Тогда, согласно второму утверждению леммы 2.4, показатель элемента $b \equiv b_1 \cdots b_r \pmod{p}$ равен τ. Из третьего утверждения леммы 2.3, получаем $\tau | \varphi(p) = p - 1$.

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

Теперь мы знаем, что для нечетного простого числа p обязательно найдется первообразный корень. Протестировать, является ли заданное

число a первообразным корнем по модулю целого числа m, позволяет следующая теорема.

Теорема 2.9. *Пусть $a, m > 0$ целые взаимно простые числа. Известно разложение числа $\varphi(m)$ на простые сомножители $\varphi(m) = \prod_{i=1}^{r} q_i^{\alpha_i}$, где $q_1, \ldots, q_r$ различные простые числа, а $\alpha_1, \ldots, \alpha_r$ натуральные числа. Число a является первообразным корнем по модулю m тогда и только тогда, когда выполнены условия*

$$a^{\frac{\varphi(m)}{q_1}} \not\equiv 1 \pmod{m}, \quad \cdots, \quad a^{\frac{\varphi(m)}{q_r}} \not\equiv 1 \pmod{m}.$$

Доказательство. Если a первообразный корень по модулю m, то в силу определения первообразного корня, для любого $c | \operatorname{ord}_m a = \varphi(m)$ выполнено $a^{\frac{\operatorname{ord} a}{c}} \not\equiv 1 \pmod{m}$, следовательно, выполнено и утверждение теоремы.

Обратно, пусть для числа a выполнены условия теоремы и его показатель равен t. Тогда, из третьего утверждения леммы 2.3 следует, что найдется некоторое натуральное число c такое, что $ct = \varphi(m)$. Если $c = 1$, то показатель элемента a равен $\varphi(m)$, 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 $\varphi(m) = qut$ для некоторого целого числа u и выполнено сравнение

$$a^{\frac{\varphi(m)}{q}} \equiv \left(a^t\right)^u \equiv 1 \pmod{m},$$

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

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

$$a^n \pmod{p} \quad \textit{для всех} \quad 1 \leqslant n \leqslant q-1, \quad \mathbf{НОД}(n,\ q) = 1, \qquad (2.14)$$

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 2.4, 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 2.3, получаем, что $q|nl$. Поскольку для индекса n выполнено условие $\mathbf{НОД}\,(n,\ q)=1$, 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

$$x^q - 1 \equiv 0 \pmod p. \tag{2.15}$$

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

С другой стороны, согласно теореме 3.3[2], 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

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

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 $n = 1,\ \ldots, q$, только элементы множества (2.14) имеют показатель, равный q.

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

[2]Теорема 3.3 говорит о максимально возможном числе корней многочлена, её доказательство не зависит от материала, изложенного в данной главе.

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. □

Согласно доказанной нами теореме, количество вычетов, чей показатель равен q по модулю p, оценивается величиной $\varphi(q)$. В частности, количество первообразных корней по модулю p равно $\varphi(p-1)$.

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 $\operatorname{ord}_p a = p-1$.

1. Выбрать случайно элемент a, удовлетворяющий неравенству $1 \leqslant a < p$.
2. Определить $i = 1$.
3. **Пока** $i \leqslant k$ **выполнить**
   - **3.1.** Если $a^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$, то вернуться на шаг 1.
4. Вернуть значение a. □

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 π близко к единице, следовательно, вероятность того, что случайный вычет a окажется первообразным корнем, достаточно велика.

2.4.2 Существование первообразных корней по модулю p^α

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

$$(a+p)^n = \sum_{k=0}^{n} C_k^n a^{n-k} p^k, \quad \text{где} \quad C_k^n = \frac{n!}{k!(n-k)!} \tag{2.16}$$

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

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

Поскольку $\mathbf{НОД}(a,\ p) = 1$, 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

$$a^{p-1} = 1 + hp \tag{2.17}$$

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

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

для произвольного значения $\alpha \geqslant 2$.

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 2.3, $p-1|s$. 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 $m = p,\ p^2,\ \ldots, p^{\alpha-1}$ вычет a, удовлетворяющий условию теоремы, является первообразным корнем. Обозначим s показатель вычета a по модулю p^α, тогда $a^s \equiv 1 \pmod{p^\alpha} \equiv 1 \pmod{p^{\alpha-1}}$, следовательно, $\varphi\left(p^{\alpha-1}\right) = p^{\alpha-2}(p-1)|s$.

С другой стороны, в силу леммы 2.3, $s|\varphi\left(p^\alpha\right) = p^{\alpha-1}(p-1)$. Мы снова получили, что величина s может принимать только два значения, а именно, либо $s = \varphi\left(p^{\alpha-1}\right)$, либо $\varphi\left(p^\alpha\right)$.

Предположим, что показатель s удовлетворяет первому равенству, то есть выполнено сравнение $a^{\varphi\left(p^{\alpha-1}\right)} \equiv 1 \pmod{p^\alpha}$. Тогда, учитывая (2.17), получаем

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

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

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 2.1. 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 сравения

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

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

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

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 $\mathbb{F}_p^*$

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

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

$$\mathbb{F}_p^* =< a >= \{a,\ a^2 \pmod p,\ \ldots,\ a^{p-1} \pmod p\},$$

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 [5, §3, гл.4].

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.

Глава 3

Многочлены

Определение элементарных операций - Алгоримы 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 $\mathbb{F}_p$

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

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 ε кольца $\mathbb{U}$ обратимым, если он является делителем единицы, то есть для него найдется некоторый элемент ε^{-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 ε 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 $n \geqslant 0$ целое число. Многочленом $a(x)$ от одной переменной x мы будем называть сумму*

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

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

При некотором фиксированном значении $x \in \mathbb{U}$ значением 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 $a(x) = x^x + a_{n-1}x^{n-1} + \cdots + a_0$, старший коэффициент которого равен единице, называется унитарным*[1].

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 $m \geqslant n$. Определим их сумму равенством

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

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

Определим произведение многочленов равенством

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

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

[1]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 $\deg a(x) \leqslant \deg b(x)$.

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 $k = 0, \ldots, n$.

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. *Если 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. [5, 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

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

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

$$a(x)\left(q(x) - q_1(x)\right) = \left(r_1(x) - r(x)\right). \tag{3.3}$$

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

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

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). □

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* $\mathbf{НОД}\,(a(x),\ b(x)) = 1$, *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. $\mathbf{НОД}\,(a(x),\ b(x)) = \mathbf{НОД}\,(b(x),\ a(x))$.
2. $\mathbf{НОД}\,(a(x),\ a(x)) = \mathbf{НОД}\,(a(x),\ 0) = a_n^{-1}a(x)$, *где a_n старший коэффициент многочлена $a(x)$.*
3. $\mathbf{НОД}\,(a(x),\ b(x)) = \mathbf{НОД}\,(a(x),\ r(x))$, *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 $\deg b(x) \geqslant \deg a(x) > 0$.
Выход: $\mathbf{НОД}\,(a(x),\ b(x))$ – 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 $\mathbf{НОД}\,(a(x),\ b(x)) = u_n^{-1}u(x)$, 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*

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

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 [20], 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

$$d(x) = a(x)u_1(x) + m(x)v_1(x) \tag{3.5}$$

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

$$r(x) = m(x) - q(x)\big(a(x)u_1(x) + m(x)v_1(x)\big) = \\ - a(x)q(x)u_1(x) + m(x)\big(1 - q(x)v_1(x)\big),$$

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 $d(x) = d_1(x)$. □

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

$$f(x)t(x) = g(x)h(x). \tag{3.6}$$

Пусть многочлен $f(x)$ не делит многочлен $g(x)$. Тогда, в силу неприводимости многочлена $f(x)$, выполнено $\mathbf{НОД}\,(f(x),\ g(x)) = 1$ 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. □

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*

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

где $c \in \mathbb{U}$, а $f_1(x), \ldots, f_k(x)$ различные унитарные неприводимые многочлены, $\alpha_1, \ldots, \alpha_k$ 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)

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

Поскольку все многочлены $f_1(x), \ldots, f_k(x)$ и $h_1(x), \ldots, h_s(x)$ унитарны, мы получаем, что значения c и d совпадают. Без ограничения общности будем считать, что $s \geqslant k$ 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 $k = s$, $\alpha_i = \beta_i$, $i = 1, \ldots, k$, откуда вытекает утверждение теоремы. □

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. □

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 α, 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 $e_1, \ldots, e_s \in \mathbb{U}$ корни многочлена $f(x)$. Тогда из теоремы 3.2 следует, что найдутся натуральные числа $\alpha_1, \ldots, \alpha_s \geqslant 1$ такие, что

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

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

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

из которого следует утверждение теоремы. □

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

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

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

$$f(x+c) + g(x+c) \equiv f(x) + cf'(x) + g(x) + cg'(x) \equiv \\ (f(x) + g(x)) + c\,(f'(x) + g'(x)) \pmod{c^2}.$$

Аналогично, доказательство второго утверждения следует из определения производной и соотношения

$$f(x+c)g(x+c) \equiv (f(x) + cf'(x))(g(x) + cg'(x)) \equiv \\ f(x)g(x) + c\,(f'(x)g(x) + f(x)g'(x)) \pmod{c^2}.$$

□

Обобщая утверждения леммы, мы получаем равенства

$$(f_1(x) + \dots + f_k(x))' = f_1'(x) + \dots + f_k'(x), \tag{3.10}$$

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

Из (3.11) получаем равенство

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

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

$$f'(x) = \left(\sum_{k=0}^{n} a_k x^k\right)' = \sum_{k=1}^{n} k a_k x^{k-1} = \\ = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k = n a_n x^{n-1} + \cdots + 2a_2 x + a_1, \tag{3.13}$$

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

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

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*

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

и системе сравнений

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

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 $i = 1, \ldots, k$, 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 $i = 1, \ldots, k$, то есть $f(e)$ является общим кратным чисел $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$. Согласно лемме 2.5 наименьшее кратное чисел $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ 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 $a_1, \ldots, a_k$ 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 $i = 1, \ldots, k$. 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 $a_1, \ldots, a_k$ 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 $a_1, \ldots, a_k$. Это доказывает, что других решений, отличных от построенных, сравнение (3.15) не имеет. □

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 α.

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 $\alpha \geqslant 1$ 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 α, и обозначим e_α 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

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

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^α, следовательно, сокращая полученное равенство на p^α, получаем сравнение

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

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

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^α. 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

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

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

$$f'(x) \equiv \gamma(x-e)^{\gamma-1}u(x) + (x-e)^\gamma u'(x) \equiv \\ \equiv (x-e)^{\gamma-1}\left(\gamma u(x) + u'(x)\right) \pmod p,$$

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

Доказательство. Очевидно, что при $\alpha \leqslant \beta$ 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. □

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_α 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** $k \leqslant \alpha$ **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.

Глава 4

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

$$x^2 \equiv a \pmod{p}. \tag{4.1}$$

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 $\mathbf{НОД}(a,\ p) = 1$ 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 $\mathbf{НОД}(2,\ p) = \mathbf{НОД}(x_1,\ p) = 1$ и $x_1 \neq 0$. □

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 $1,\ 2,\ \ldots,\ p-1$ содержится равное число квадратичных вычетов и квадратичных невычетов по модулю p.*

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

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

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

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

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

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

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: $1,\ 2,\ \ldots,\ p-1$ найдется ровно $\dfrac{p-1}{2}$ квадратичных вычетов. Остальные – квадратичные невычеты. □

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

$$zz = kp, \tag{4.3}$$

при некотором целом k.

Поскольку p простое число, то $\mathbf{НОД}(z,\ p) = 1$ 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. □

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, $\mathbf{НОД}\,(a,\ p) = 1$, выполнено одно из сравнений

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

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{4.5}$$

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 $\dfrac{p-1}{2}$ 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

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

□

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 [9]. Это третье доказательство квадратичного закона взаимности из шести, данных Гауссом, последняя его часть принадлежит Кронекеру. Нам потребуется еще одна лемма.

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

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

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

Доказательство. Обозначим символами

$$a_1,\ a_2,\ \ldots,\ a_\lambda,\ -b_1,\ -b_2,\ \ldots,\ -b_\mu, \tag{4.6}$$

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

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

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

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

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

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

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

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

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. □

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

$$\begin{cases} a = q_1 p + r_1, \\ 2a = q_2 p + r_2, \\ \ldots \\ \frac{p-1}{2} a = q_{\frac{p-1}{2}} p + r_{\frac{p-1}{2}}, \end{cases} \tag{4.8}$$

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

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

следовательно, можно записать равенство

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

Сложим почленно все равенства в (4.8) и, учитывая равенство[1]

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

получим

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

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

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

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

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

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, $1 \leqslant k \leqslant \dfrac{p-1}{2}$, определяемых равенствами (4.8), равны нулю. Это, очевидно, следует из того, что все числа вида ka при всех $1 \leqslant k \leqslant \dfrac{p-1}{2}$ не превосходят величины p. Таким образом,

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

[1]Мы используем равенство $1 + 2 + \ldots + m = \frac{m(m+1)}{2}$, 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 $q_k = \left\lfloor \dfrac{ka}{p} \right\rfloor$ и $\mu \equiv \sum\limits_{k=1}^{\frac{p-1}{2}} \left\lfloor \dfrac{ka}{p} \right\rfloor$, 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

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

Для этого рассмотрим выражение

$$\frac{s}{a} - \frac{k}{p}, \quad \text{где} \quad 1 \leqslant k \leqslant \frac{p-1}{2}, \quad 1 \leqslant s \leqslant \frac{a-1}{2}. \tag{4.11}$$

Учитывая пределы для переменных k и s, получим, что разность (4.11) может принимать $\dfrac{1}{4}(p-1)(a-1)$ отличных от нуля значений. Подсчитаем количество положительных и отрицательных значений.

Пусть $\frac{s}{a} - \frac{k}{p} > 0$, то есть $k < \frac{sp}{a}$. Тогда, при фиксированном значении s переменная k может принимать значения $1,\ 2,\ \ldots, \left\lfloor \frac{sp}{a} \right\rfloor$. Поскольку s принимает все значения, не превосходящие $\frac{a-1}{2}$, получим, что существует всего $\sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor$ положительных значений разности (4.11).

Пусть $\frac{s}{a} - \frac{k}{p} < 0$, то есть $s < \frac{ka}{p}$. Аналогичными рассуждениями получаем, что существует $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$ отрицательных значений разности (4.11). Тогда, из мощностных соображений, получаем равенство

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

которое завершает доказательство леммы. □

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, α_i целые неотрицательные числа, k натуральное и $1 \leqslant i \leqslant k$.

Рассмотрим целое число a и определим символ Якоби равенством

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

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 $b \equiv a$

$(\mathrm{mod}\ m)$ 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

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

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

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

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 $a = b^2 c$ и $\mathbf{НОД}\,(a,\ m) = 1$, то

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

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

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r} \left(\frac{q_j}{p_i}\right) =$$

$$(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r} \frac{q_j-1}{2}\cdot\frac{p_i-1}{2}} \prod_{j=1}^{s}\prod_{i=1}^{r} \left(\frac{p_i}{q_j}\right) =$$

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

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

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

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.

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

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 $x = \dfrac{x}{2}$ 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

$$x^2 \equiv 4a^2 (4a)^{\frac{p-5}{4}} \equiv a (4a)^{1+\frac{p-5}{4}} \equiv a 2^{\frac{p-1}{2}} a^{\frac{p-1}{4}} \pmod p. \tag{4.12}$$

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 некорого целого k. Тогда, возвращаясь к (4.12), 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* $\mathbf{НОД}(a,\ p) = 1$. *Тогда*

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

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

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

$$a^{p-1} - 1 \equiv a^{2^n q} - 1 \equiv \left(a^{2^{n-1} q} - 1\right)\left(a^{2^{n-1} q} + 1\right) \equiv 0 \pmod{p}. \quad (4.13)$$

Тогда, в силу леммы 1.4, либо правая скобка, либо левая скобка в сравнении (4.13) 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 (4.13) 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 $k = n - 2, \ldots, 1$ не будет выполнено утверждение леммы, придем к сравнению

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

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

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

$$w^2 a^q \equiv 1 \pmod{p}, \tag{4.14}$$

тогда решение сравнения (4.1) примет вид $x \equiv w a^{\frac{q+1}{2}} \pmod{p}$. 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 $\operatorname{ord}_p z = 2^n$.*

2. *Обозначим $z_k \equiv z^{2^k} \pmod{p}$, тогда $z_k \equiv z_{k-1}^2 \pmod{\ }$ и $\operatorname{ord}_p z_k = 2^{n-k}$.*

3. *Пусть u, v вычеты такие, что $\operatorname{ord}_p u = \operatorname{ord}_p v = 2^{k+1}$, тогда выполнено условие $\operatorname{ord}_p(uv) | 2^k$.*

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 $\operatorname{ord}_p z = 2^n$, 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 2.4 следует, что

$$\operatorname{ord}_p z_k = \operatorname{ord}_p z^{2^k} = \frac{\operatorname{ord}_p z}{2^k} = 2^{n-k},$$

то есть второе утверждение леммы.

Рассмотрим третье утверждение леммы. Поскольку $\operatorname{ord}_p u = \operatorname{ord}_p v = 2^{k+1}$, 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 2.3, получим $\operatorname{ord}_p(uv) | 2^k$. Лемма доказана. □

Введенные нами в утверждении леммы вычеты z_k будут использованы для построения вычета w такого, что выполнено сравнение (4.14)

$$w^2 a^q \equiv 1 \pmod p.$$

При этом заметим, что выполнение данного сравнения равносильно выполнению равенства $\operatorname{ord}_p(w^2 a^q) = 1$. Напомним, что в силу леммы 4.7, найдется такой индекс k, $0 \leqslant k < n$, что $a^{2^k q} \equiv -1 \pmod p$, следовательно, $\operatorname{ord}_p a^q = 2^{k+1}$.

Определим конечную последовательность $u_1, u_1, \ldots, u_{r+1}$ сравнениями

$$\begin{aligned} &u_1 \equiv a^q \pmod p, \\ &u_2 \equiv z_{l_1} u_1 \pmod p, \\ &\cdots \\ &u_{r+1} \equiv z_{l_r} u_r \pmod p, \end{aligned}$$

где индексы l_j выбираются из условия $\operatorname{ord}_p u_j = \operatorname{ord}_p z_{l_j}$, $j = 1, \ldots, r$, а вычеты z_{j_j} определяются вторым утверждением леммы 4.8.

Из третьего утверждения леммы 4.8 следует, что

$$\operatorname{ord}_p u_j \mid \operatorname{ord}_p u_{j-1}, \quad \text{при} \quad j = 2, \ldots, r,$$

и выполнена цепочка неравенств

$$\operatorname{ord}_p u_1 > \operatorname{ord}_p u_2 > \cdots > \operatorname{ord}_p u_{r+1} = 1$$

для некоторого значения $r \geqslant 1$. 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 (4.14)

$$z_{l_1} \cdots z_{l_r} \cdot a^q \equiv \left(z_{l_1-1} \cdots z_{l_r-1}\right)^2 a^q \equiv w^2 a^q \equiv 1 \pmod p$$

и мы можем определить неизвестное x сравнением

$$x \equiv \left(z_{l_1-1} \cdots z_{l_r-1}\right) \cdot a^{\frac{q+1}{2}} \pmod p.$$

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

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{4.15}$$

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 (4.15) не имеет решений,*
2. *если $D \equiv 0 \pmod{p}$, то сравнение (4.15) имеет единственное решение $e \equiv -\dfrac{b}{2a} \pmod{p}$,*
3. *если $\left(\frac{D}{p}\right) = 1$, то сравнение (4.15) 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 (4.15) эквивалентна разрешимости сравнения

$$z^2 \equiv D \pmod{p}, \quad \text{где} \quad z \equiv 2ax + b \pmod{p}.$$

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. □

Мы доказали результат о разрешимости сравнения (4.15) по модулю простого числа p в зависимости от величины дискриминанта D. Теперь получим обратное утверждение – о разрешимости сравнения (4.15) 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, α_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 $\alpha_2 \geqslant 1$. 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

$$\frac{(p_1-1)}{2}\frac{(q-1)}{2} - \frac{(p-1)}{2}\frac{(q-1)}{2} = (q-1)\frac{(p_1-p)}{4} \equiv 0 \pmod 2.$$

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

$$\left(\frac{D}{p_1}\right) = \left(\frac{-1}{p_1}\right)^{\alpha_1} \left(\frac{2}{p_1}\right)^{\alpha_2} \prod_{i=3}^{k} \left(\frac{q_i}{p_1}\right)^{\alpha_i} =$$

$$= \left(\frac{-1}{p}\right)^{\alpha_1} \left(\frac{2}{p}\right)^{\alpha_2} \prod_{i=3}^{k} \left(\frac{q_i}{p}\right)^{\alpha_i} = \left(\frac{D}{p}\right).$$

Теорема доказана. □

Утверждение доказанной теоремы позволяет в явном виде определить множество всех простых чисел, при которых разрешимо сравнение (4.15) 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 $e = 0, 1 \ldots, p-1$ 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*

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-p+1) = \prod_{k=0}^{p-1}(x-k) \pmod{p}. \quad (4.16)$$

Доказательство. Согласно малой теореме Ферма, см. теорему 2.7, для каждого целого числа e, $0 \leqslant e < p$, 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 (4.16). Лемма доказана. □

Лемма 4.10. *Пусть $f(x)$ произвольный многочлен из $\mathbb{F}_p[x]$. Определим многочлен $h(x)$*

$$h(x) = \mathbf{НОД}\,(x^p - x,\ \ f(x))\,.$$

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 $e_1, \ldots, e_k$ 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,

$$h(x) = \mathbf{НОД}\,(x^p - x,\ \ f(x)) = (x - e_1) \cdots (x - e_r) \in \mathbb{F}_p[x].$$

Последнее равенство завершает доказательство леммы. □

Согласно утверждению последней леммы, мы можем свести задачу определения корней многочлена $f(x)$ к определению корней многочлена $h(x)$, раскладывающего в произведение линейных множителей, такого, что $\deg h(x) \leqslant \deg f(x)$.

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 линеен, 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 $h(x) \equiv \prod_{k=1}^{r}(x - e_k) \pmod p$, раскладывающийся на линейные множители в $\mathbb{F}_p[x]$ с неизвестными значениями $e_1, \ldots, e_r$.
Выход: Корень многочлена – одно из значений $e_1, \ldots, e_r$.

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 $d(x) \in \mathbb{F}_p[x]$
$$d(x) = \textbf{НОД}\left(h(x),\ (x-c)^{\frac{p-1}{2}} - 1\right).$$
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 $d(x) = \textbf{НОД}\left(h(x),\ (x-c)^{\frac{p-1}{2}} - 1\right)$ 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 $\mathcal{D}$

$$\mathcal{D} = \{c \in \mathbb{F}_p : \quad (e_1 - c)^{\frac{p-1}{2}} \not\equiv (e_2 - c)^{\frac{p-1}{2}} \pmod p\}.$$

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 γ_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 $\gamma_1, \ldots, \gamma_{\frac{p-1}{2}}$. Следовательно, степень многочлена $d(x) = \mathbf{НОД}\,(h(x),\ v(x))$ 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

$$|\mathcal{D}| \geqslant p - \frac{p-3}{2} = \frac{p+3}{2}.$$

Таким образом выбирая случайное значение c в интервале $0, \ldots, p-1$, мы с вероятностью $\frac{p+3}{2p} > \frac{1}{2}$ выберем значение, принадлежащее множеству $\mathcal{D}$. Из этого следует второе утверждение леммы. □

Из утверждений доказанной леммы следует, что в среднем нам потребуется две попытки выбора значения c 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 c 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 $e_1, \ldots, e_r$, $\alpha_1, \ldots, \alpha_r$ 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 $e_1, \ldots, e_r$, $\alpha_1, \ldots, \alpha_r$ 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 $h(x) = \mathbf{НОД}(x^p - x,\ f(x))$.
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, α в список корней и их кратностей и перейти на шаг 3. □

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.

Глава 5

Непрерывные дроби

Определение непрерывной дроби - Понятие подходящей дроби - Теорема о наилучшем приближении - Квадратичные иррациональности и их свойства - Подходящие дроби и наилучшие приближения.

Рассмотрим непрерывные дроби действительных чисел.

Определение 5.1. *Пусть α действительное число. Мы будем называть целой частью α, которую мы обозначаем символом $\lfloor\alpha\rfloor$, наибольшее целое число, меньшее, либо равное α. В частном случае: целая часть целого числа совпадает с ним.*

Отметим, что α может быть как отрицательным, так и положительным числом. Например $\lfloor\sqrt{13}\rfloor = 3$, в то время как $\lfloor-\sqrt{13}\rfloor = -4$. В любом случае выполнено неравенство $\lfloor\alpha\rfloor \leqslant \alpha$.

Пусть α_0 действительное число и $\alpha_0 \neq 0$. Определим последовательность действительных чисел $\alpha_1,\ \alpha_2,\ \ldots$ следующим реккурентным соотношением

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \quad \text{где} \quad a_n = \lfloor\alpha_n\rfloor. \tag{5.1}$$

В случае, если α_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 $\alpha_n = a_n + \dfrac{1}{\alpha_{n+1}}$, мы можем выразить число α_0 в виде

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}} = \cdots$$

или, в общем виде,

$$\alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{\alpha_n}}}}, \tag{5.2}$$

для произвольного индекса n.

Для упрощенной записи равенства (5.2) мы будем использовать обозначение $\alpha_0 = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$.

Определение 5.2. *Пусть $\alpha_0 \neq 0$ действительное число. Мы будем называть представление (5.2)*

$$\alpha_0 = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{\alpha_n}}}},$$

$n = 1,\ 2,\ \ldots$ непрерывной или цепной дробью числа α_0. Элементы последовательности $a_0,\ a_1,\ \ldots$ мы будем называть неполными частными, а элементы последовательности $\alpha_1,\ \alpha_2,\ \ldots$ полными частными.

Заметим, что из соотношения (5.1) и неравенства $\lfloor \alpha \rfloor \leqslant \alpha$ вытекает выполнимость следующих неравенств

$$0 \leqslant \alpha_n - \lfloor \alpha_n \rfloor < 1 \quad \text{и} \quad \alpha_n > 1, \quad a_n \geqslant 1 \quad \text{при} \quad n \geqslant 1. \tag{5.3}$$

5.1 Конечные непрерывные дроби

Остановимся на частном случае, когда последовательность полных частных $\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_n$ конечна. Верна следующая лемма.

Лемма 5.1. *Пусть $\alpha_0 \neq 0$ действительное число. Последовательность полных частных $\alpha_1,\ \alpha_2,\ \ldots$, определяемая соотношениями (5.1), обрывается тогда и только тогда, когда α_0 рациональное число.*

Доказательство. Если последовательность конечна, то найдется индекс n, такой что α_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 α_0 является рациональным числом.

Если α_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

$$p = a_0 q + r_1, \quad \text{где} \quad 0 \leqslant r_1 < q.$$

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

$$q = a_1 r_1 + r_2, \quad \text{где} \quad 0 \leqslant r_2 < r_1,$$

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

$$\begin{aligned} &r_{-1} = p,\ r_0 = q, \\ &r_{n-1} = a_n r_n + r_{n+1}, \quad 0 \leqslant r_{n+1} < r_n. \end{aligned} \tag{5.4}$$

Последовательность $r_0,\ r_1, \ldots$ 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. □

Из утверждения доказанной нами леммы следует, что рассматриваемая последовательность $\alpha_1,\ \alpha_2,\ \ldots$ бесконечна, если α_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

$$\frac{P_n}{Q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} = [a_0, a_1, \ldots, a_{n-1}, a_n]. \tag{5.5}$$

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 α_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 α_0 выполнены следующие рекуррентные соотношения*

$$\begin{aligned} P_{n+1} &= a_{n+1} P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1} Q_n + Q_{n-1}, \end{aligned} \tag{5.6}$$

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

$$\frac{P_n}{Q_n} = [a_0, a_1, \ldots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}}.$$

Тогда утверждение леммы следует из следующего равенства

$$\begin{aligned}\frac{P_{n+1}}{Q_{n+1}} &= [a_0, a_1, \ldots, a_n, a_{n+1}] = \\ &= \left[a_0, a_1, \ldots, a_n + \frac{1}{a_{n+1}}\right] = \frac{\left(a_n + \dfrac{1}{a_{n+1}}\right) P_{n-1} + P_{n-2}}{\left(a_n + \dfrac{1}{a_{n+1}}\right) Q_{n-1} + Q_{n-2}} = \\ &= \frac{a_{n+1}\left(a_n P_{n-1} + P_{n-2}\right) + P_{n-1}}{a_{n+1}\left(a_n Q_{n-1} + Q_{n-2}\right) + Q_{n-1}} = \frac{a_{n+1} P_n + P_{n-1}}{a_{n+1} Q_n + Q_{n-1}}.\end{aligned}$$

□

Основываясь на доказательстве леммы 5.2, легко заметить, что из равенства

$$[a_0, \ldots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}},$$

следует равенство

$$\alpha_0 = [a_0, \ldots, \alpha_{n+1}] = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}. \tag{5.7}$$

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 α является как рациональным, так и иррациональным.

Лемма 5.3. *При всех индексах $n = 0, 1, \ldots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение*

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^n. \tag{5.8}$$

Доказательство. Используя равенства (5.6), получим следующие равенства

$$\begin{aligned} P_{n+1}Q_n - Q_{n+1}P_n &= (a_{n+1}P_n + P_{n-1})Q_n - (a_{n+1}Q_n + Q_{n-1})P_n = \\ &= -(P_nQ_{n-1} - Q_nP_{n-1}) = (-1)^2(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) = \cdots \\ &= (-1)^k(P_{n-k+1}Q_{n-k} - Q_{n-k+1}P_{n-k}), \end{aligned}$$

для любого $k = 1,\ 2,\ \ldots$.

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. □

Заметим, что из равенства (5.8) следует, что подходящая дробь $\frac{P_n}{Q_n}$ несократима. Если предположить обратное, то найдется целое число d_n такое, что $\mathbf{НОД}(P_n,\ Q_n) = d_n > 1$ и $d_n|(-1)^{n+1}$. Последнее условие невыполнимо.

Лемма 5.4. *При всех индексах $n = 0, 1, \ldots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение*

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(-1)^{n+1}. \tag{5.9}$$

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

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(P_nQ_{n-1} - Q_nP_{n-1}) = a_{n+1}(-1)^{n-1}.$$

□

Две последние леммы позволяют нам 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

$$\cdots \frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}} > \cdots > \frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}} > \cdots \tag{5.10}$$

из которой следует, что последовательность подходящих дробей сходится и имеет предел. Чему равен этот предел данной определяет теорема 5.1, к доказательству которой мы скоро приступим.

Лемма 5.5. *Для всех индексов $n = 1,\ 2,\ \ldots$ знаменатели Q_n подходящих дробей удовлетворяют неравенству $Q_{n+1} > 2^{\lceil \frac{n}{2} \rceil}$ или, что равносильно*

$$\begin{cases} Q_{n+1} \geqslant 2^{\frac{n}{2}}, & \text{при четном } n, \\ Q_{n+1} \geqslant 2^{\frac{n+1}{2}}, & \text{при нечетном } n. \end{cases} \tag{5.11}$$

Доказательство. Из соотношений (5.3) и (5.6) следует неравенство

$$Q_{n+1} = a_{n+1}Q_n + Q_{n-1} \geqslant Q_n + Q_{n-1} \geqslant 2Q_{n-1} + Q_{n-2} \geqslant 2Q_{n-1},$$

из которого следует утверждение леммы – при нечетном n выполнено неравенство $Q_{n+1} \geqslant 2^{\frac{n+1}{2}} Q_0 = 2^{\frac{n+1}{2}}$, а при четном n – выполнено неравенство $Q_{n+1} \geqslant 2^{\frac{n}{2}} Q_1 \geqslant 2^{\frac{n}{2}}$. □

Теперь мы можем доказать теорему о приближении числа α_0 последовательностью подходящих дробей.

Теорема 5.1. *Пусть $\alpha_0 \neq 0$ действительное число. Тогда последовательность подходящих дробей сходится к α_0, то есть выполнено условие*

$$\alpha_0 = \lim_{n\to\infty} \frac{P_n}{Q_n}.$$

Доказательство. Сначала мы покажем, что последовательность подходящих дробей сходится. Действительно, из леммы 5.3 получаем равенство

$$\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n Q_{n+1}} \left| P_{n+1}Q_n - Q_{n+1}P_n \right| = \frac{1}{Q_n Q_{n+1}}.$$

Из этого равенства и из утверждения леммы 5.5 следует, что последовательность подходящих дробей сходится, то есть

$$\lim_{n\to\infty} \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = 0.$$

Нам осталось выяснить чему равен предел последовательности подходящих дробей. Учитывая равенство (5.7) и утверждение леммы 5.3, получим следующее равенство

$$\alpha_0 - \frac{P_n}{Q_n} = \frac{1}{Q_n}\left(\alpha_0 Q_n - P_n\right) = \\ = \frac{1}{Q_n}\left(Q_n \frac{\alpha_{n+1}P_n + P_{n-1}}{\alpha_{n+1}Q_n + Q_{n-1}} - P_n\right) = \\ = \frac{1}{Q_n}\left(\frac{Q_n P_{n-1} - P_n Q_{n-1}}{\alpha_{n+1}Q_n + Q_{n-1}}\right) = \frac{(-1)^n}{Q_n\left(\alpha_{n+1}Q_n + Q_{n-1}\right)}. \quad (5.12)$$

Вспоминая, что α_n и Q_n положительны при всех $n \geqslant 1$, получаем неравенство

$$\left|\alpha_0 - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n\left(\alpha_{n+1}Q_n + Q_{n-1}\right)} \leqslant \\ \frac{1}{Q_n\left(a_{n+1}Q_n + Q_{n-1}\right)} = \frac{1}{Q_{n+1}Q_n}, \quad (5.13)$$

из которого вытекает утверждение теоремы. □

Из доказанной нами теоремы следует, что мы можем приблизить действительное число α_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. Отойдем 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

$$\alpha_0 = \sqrt{29} \sim 5.3851648, \quad a_0 = \lfloor\sqrt{29}\rfloor = 5, \quad P_0 = 5, Q_0 = 1,$$
$$\alpha_1 = \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{(\sqrt{29} - 5)(\sqrt{29} + 5)} = \frac{\sqrt{29} + 5}{4},$$
$$a_1 = \lfloor\alpha_1\rfloor = \left\lfloor\frac{\sqrt{29} + 5}{4}\right\rfloor = 2, \quad P_1 = 11, \quad Q_1 = 2, \quad \frac{P_1}{Q_1} = 5.5,$$

аналогично мы получим следующие равенства

$$\alpha_2 = \frac{1}{\frac{\sqrt{29}+5}{4} - 2} = \frac{\sqrt{29}+3}{5}, \quad a_2 = 1, \quad \frac{P_2}{Q_2} = \frac{16}{3} = 5.333333,$$
$$\alpha_3 = \frac{1}{\frac{\sqrt{29}+3}{5} - 1} = \frac{\sqrt{29}+2}{5}, \quad a_3 = 1, \quad \frac{P_3}{Q_3} = \frac{27}{5} = 5.4,$$
$$\alpha_4 = \frac{1}{\frac{\sqrt{29}+2}{5} - 1} = \frac{\sqrt{29}+3}{4}, \quad a_4 = 2, \quad \frac{P_4}{Q_4} = \frac{70}{13} = 5.3846154,$$
$$\alpha_5 = \frac{1}{\frac{\sqrt{29}+3}{4} - 2} = \sqrt{29}+5, \quad a_5 = 10, \quad \frac{P_5}{Q_5} = \frac{727}{135} = 5.3851852,$$
$$\alpha_6 = \frac{1}{\sqrt{29}-5} = \frac{\sqrt{29}+5}{4}, \quad a_6 = 2, \quad \frac{P_6}{Q_6} = \frac{1524}{283} = 5.385159,$$
$$\alpha_7 = \frac{1}{\frac{\sqrt{29}+5}{4} - 2} = \frac{\sqrt{29}+3}{5}, \quad a_7 = 1, \quad \frac{P_7}{Q_7} = \frac{2251}{418} = 5.3851675.$$

Мы остановим наши вычисления и заметим, что выполнены равенства

$$\alpha_6 = \alpha_1, \quad \alpha_7 = \alpha_2, \ \ldots,$$

то есть наша последовательность полных частных зациклилась и имеет период равный 5. Мы можем записать непрерывную дробь для $\alpha_0 = \sqrt{29}$ в виде

$$\sqrt{29} = [5; 2, 1, 1, 2, 10, 2, 1, 1, 2, 10, \ldots]$$

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 α_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 α 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 α 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 α.

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 $\alpha = \dfrac{5 + \sqrt{109}}{2}$.

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

$$\begin{cases} A = -v, B = 2u, & \text{либо} \\ A = v, B = -2u, \end{cases} \tag{5.15}$$

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

$$A = \mp v, B = \pm u. \tag{5.16}$$

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 $\alpha = \dfrac{C + \sqrt{D}}{E}$. Тогда выполнено равенство

$$E(A + \sqrt{D}) = B(C + \sqrt{D}),$$

откуда

$$EA - BC = (B - E)\sqrt{D}. \tag{5.17}$$

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* $\alpha = \dfrac{A+\sqrt{D}}{B}$ *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 α.

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 α 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 $\alpha_0 = \dfrac{A_0+\sqrt{D}}{B_0}$, являющуюся корнем многочлена $f(x) = ux^2 + vx + w$, в непрерывную дробь.

Для полного частного α_1 выполнено равенство

$$\begin{aligned} \alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\dfrac{A_0+\sqrt{D}}{B_0} - a_0} = \frac{B_0}{(A_0 - a_0B_0) + \sqrt{D}} = \\ = \frac{B_0\,(A_0 - a_0B_0) - B_0\sqrt{D}}{(A_0 - a_0B_0)^2 - D}. \end{aligned} \quad (5.19)$$

Обозначим символом $\hat{\alpha}_0 = \dfrac{A_0-\sqrt{D}}{B_0}$ 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

$$\alpha_1 = \frac{(a_0B_0 - A_0) + \sqrt{D}}{2a_0A_0 - a_0^2B_0 + B_{-1}} = \frac{A_1 + \sqrt{D}}{B_1},$$

где

$$A_1 = a_0B_0 - A_0,$$
$$B_1 = a_0(2A_0 - a_0B_0) + B_{-1} = a_0(A_0 - A_1) + B_{-1}.$$

Мы получили, что полное частное α_1 имеет такой же вид, как α_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* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *квадратичная иррациональность, являющаяся корнем многочлена* $f(x) = ux^2 + vx + w$, $D = v^2 - 4uw$, *и* $\alpha_0,\ \alpha_1,\ \ldots, \alpha_n, \ldots$ *последовательность полных частных.*

Тогда для каждого полного частного α_{n+1} *выполнено равенство*

$$\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}},$$

где

$$\begin{aligned} A_{n+1} &= a_nB_n - A_n, \\ B_{n+1} &= a_n(A_n - A_{n+1}) + B_{n-1}, \end{aligned} \tag{5.20}$$

при $B_{-1} = -\frac{wB_0}{u}$, *а также выполнено равенство*

$$-B_nB_{n+1} = \left(A_{n+1}^2 - D\right).$$

Доказательство. Мы проведем доказательство по индукции. Выполнимость утверждений леммы для α_1 мы проверили выше. Предположим, что для всех индексов $1, \ldots, n$ утверждение леммы выполнено, тогда, аналогично (5.19), получаем

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{B_n}{(A_n - a_nB_n) + \sqrt{D}} = \\ = \frac{-B_n\left(A_{n+1} + \sqrt{D}\right)}{A_{n+1}^2 - D}, \tag{5.21}$$

где $A_{n+1} = (a_nB_n - A_n)$.

Покажем, что $B_n | \left(A_{n+1}^2 - D\right)$. В силу предположения индукции выполнено $B_n | \left(A_n^2 - D\right)$. 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 $B_n | \left(A_{n+1}^2 - D\right)$. Обозначим $B_{n+1} = \dfrac{A_{n+1}^2 - D}{-B_n}$, тогда

$$-B_n B_{n+1} = \left(A_{n+1}^2 - D\right). \tag{5.22}$$

Подставляя (5.22) в (5.21), получим приведенное в утверждении леммы равенство $\alpha_{n+1} = \dfrac{A_{n+1} + \sqrt{D}}{B_{n+1}}$. Нам осталось получить рекуррентную формулу для B_{n+1}.

Из (5.21), с учетом изменения индексов в равенстве (5.22), получаем

$$\begin{aligned} B_{n+1} = \frac{A_{n+1}^2 - D}{-B_n} &= \frac{(a_n B_n - A_n)^2 - D}{-B_n} = \\ &= \frac{-B_n(2a_n A_n - a_n^2 B_n) + A_n^2 - D}{-B_n} = \\ &= a_n\left(2A_n - a_n B_n\right) + B_{n-1} = a_n(A_n - A_{n+1}) + B_{n-1}. \end{aligned}$$

□

Доказанная лемма определяет соотношения (5.20), которые используются для эффективного разложения квадратичной иррациональности в непрерывную дробь.

В рассмотренном нами ранее на стр. 93 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 α – квадратичная иррациональность и $\hat{\alpha}$, сопряженная с α. Тогда α называется приведенной квадратичной иррациональностью, если*

$$\alpha > 1 \quad и \quad -1 < \hat{\alpha} < 0. \tag{5.23}$$

Лемма 5.7. *Пусть $\alpha = \dfrac{A + \sqrt{D}}{B}$ приведенная квадратичная иррациональность. Тогда*

$$\begin{aligned} &0 < A < \sqrt{D}, \\ &0 < B < 2\sqrt{D}. \end{aligned}$$

Доказательство. Пусть α удовлетворяет условию леммы, тогда из неравенств (5.23) вытекают следующие утверждения.

1. Так как $\alpha - \hat{\alpha} = \dfrac{2\sqrt{D}}{B} > 0$ и $\sqrt{D} > 0$, то выполнено $B > 0$.

2. Так как $\alpha - \hat{\alpha} = \dfrac{2\sqrt{D}}{B} > 1$, то выполнено $2\sqrt{D} > B$.

3. Так как $\alpha + \hat{\alpha} = \dfrac{2A}{B} > 0$ и $B > 0$, то выполнено $A > 0$.

4. Так как $\hat{\alpha} = \dfrac{A - \sqrt{D}}{B} < 0$ и $B > 0$, то выполнено неравенство $A < \sqrt{D}$ и лемма доказана.

□

Лемма 5.8. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *квадратичная иррациональность и* $\hat{\alpha}_1, \hat{\alpha}_2, \ldots$ *сопряженные полных частных ее разложения в непрерывную дробь. Тогда выполнены следующие утверждения.*

1. *Для всех* $n \geqslant 0$ *верно равенство*

$$\hat{\alpha}_{n+1} = \frac{1}{\hat{\alpha}_n - a_n}. \tag{5.24}$$

2. *Значение* $\hat{\alpha}_{n+1}$ *удовлетворяет равенству*

$$\hat{\alpha}_{n+1} = -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n}. \tag{5.25}$$

Доказательство. Учитывая (5.22), первое утверждение леммы получаем из равенства

$$\frac{1}{\hat{\alpha}_n - a_n} = \frac{B_n}{(A_n - a_n B_n) - \sqrt{D}} = \\ = \frac{B_n\left(-A_{n+1} + \sqrt{D}\right)}{A_{n+1}^2 - D} = \frac{-A_{n+1} + \sqrt{D}}{-B_{n+1}} = \hat{\alpha}_{n+1}.$$

Докажем второе утверждение леммы. Используя первое утверждение леммы, разложим $\hat{\alpha}_0$ в непрерывную дробь

$$\hat{\alpha}_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{\hat{\alpha}_{n+1}}}}}.$$

Таким образом, последовательность подходящих дробей для $\hat{\alpha}_0$ совпадает с последовательностью подходящих дробей $\frac{P_n}{Q_n}$ для α_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* $\alpha = \dfrac{A + \sqrt{D}}{B}$ *квадратичная иррациональность. Тогда ее непрерывная дробь периодична.*

Доказательство. Вначале предположим, что α_0 приведенная квадратичная иррациональность, то есть

$$\alpha_0 > 1, \quad a_0 \geqslant 1, \quad -1 < \hat{\alpha}_0 < 0.$$

Тогда из (5.3) следует, что $\alpha_1 > 1$. Далее, следуя равенству (5.24), получим

$$\frac{1}{\hat{\alpha}_1} = \hat{\alpha}_0 - a_0 < 0 - a_0 \leqslant -1,$$

следовательно, $-1 < \hat{\alpha}_1 < 0$ и α_1 является приведенной квадратичной иррациональностью.

Продолжая далее, мы получим, что α_2 и все остальные полные частные $\alpha_n = \dfrac{A_n + \sqrt{D}}{B_n}$ 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 α_n зациклится или, другими словами, периодична.

Для завершения доказательства теоремы нам осталось показать, что для любой квадратичной иррациональности α_0 найдется такой индекс n_0, что α_{n_0} является приведенной квадратичной иррациональностью.

Вначале рассмотрим частный случай. Пусть

$$\alpha_0 = A_0 + \sqrt{D}$$

и α_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, α_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 $n \geqslant 1$, получим

$$\hat{\alpha}_{n+1} = -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n} = \\ = -\frac{Q_{n-1}}{Q_n}\left(\frac{\hat{\alpha}_0 - \frac{P_{n-1}}{Q_{n-1}}}{\hat{\alpha}_0 - \frac{P_n}{Q_n}}\right) = -\frac{Q_{n-1}(1+\omega_{n+1})}{Q_n}, \quad (5.26)$$

где точное значение ω_{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 ω_{n+1} удовлетворяет неравенствам

$$-1 < \omega_{n+1} < \frac{Q_n}{Q_{n-1}} - 1, \quad (5.28)$$

то, при $n \geqslant 1$, из (5.26) вытекают неравенства $-1 < \hat{\alpha}_{n+1} < 0$. Следовательно, α_{n+1} приведенная квадратичная иррациональность и, как мы доказали ранее, ее разложение в непрерывную дробь периодично. Следовательно, периодично разложение для α_0.

Нам осталось показать, что найдется индекс $n \geqslant 1$, для которого выполнены неравенства (5.28). Рассмотрим равенство (5.27) более подробно и обозначим символом δ_{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 α_n и Q_n положительные целые числа, то выполнено $|\delta_{n+1}| < 1$. Более того

$$|\delta_{n+1}| = \frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})} \leqslant$$
$$\leqslant \frac{1}{Q_{n-1}(a_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(a_{n+1}Q_n + Q_{n-1})} =$$
$$\frac{1}{Q_n Q_{n-1}} + \frac{1}{Q_{n+1}Q_n} = \frac{1}{Q_n}\left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}}\right). \quad (5.29)$$

Обозначим $\gamma = \hat{\alpha}_0 - \alpha_0$ и рассмотрим знаменатель дроби (5.27), тогда

$$\left|\hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})}\right| \geqslant$$
$$|\gamma| - \frac{1}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})} \geqslant |\gamma| - \frac{1}{Q_{n+1}Q_n}.$$

С учетом (5.29), мы получили следующее неравенство

$$|\omega_{n+1}| \leqslant \frac{|\delta_{n+1}|}{|\gamma| - \dfrac{1}{Q_{n+1}Q_n}} \leqslant$$
$$\left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}}\right)\frac{Q_{n+1}}{Q_{n+1}Q_n|\gamma| - 1} =$$
$$= \frac{Q_{n+1} + Q_{n-1}}{Q_{n+1}Q_nQ_{n-1}|\gamma| - Q_{n-1}}.$$

Полученное неравенство позволяет нам сделать вывод о том, что всегда найдется индекс n, при котором будут выполнены ограничения на ω_{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

$$|\gamma| > \frac{3}{Q_nQ_{n-1}} = \frac{3Q_{n+1}}{Q_{n+1}Q_nQ_{n-1}} > \frac{Q_{n+1} + 2Q_{n-1}}{Q_{n+1}Q_nQ_{n-1}},$$

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 $|\gamma| > \frac{3}{Q_nQ_{n-1}}$ и, следовательно, $|\omega_{n+1}| < 1$. □

Доказанная нами теорема позволяет получить оценку на величину индекса n, начиная с которого полные частные α_n станут приведенными квадратичными иррациональностями.

Следствие 1. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *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* α_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

$$Q_n Q_{n-1} \geqslant 2^{n-1} > \frac{3}{|\gamma|} \quad \text{или} \quad |\gamma| > \frac{3}{Q_n Q_{n-1}}.$$

Таким образом, $|\omega_{n+1}| < 1$ и следствие доказано. □

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 5.3. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *действительная квадратичная иррациональность и* α_1, α_2, … *последовательность полных частных, удовлетворяющих равенству*

$$\alpha_n = \frac{A_n + \sqrt{D}}{B_n}.$$

Тогда для всех индексов $n = 1, 2, \ldots$ *числители* P_n *и знаменатели* Q_n *подходящих дробей для* α_0 *удовлетворяют равенству*

$$\left(P_n B_0 - Q_n A_0 \right)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}. \tag{5.30}$$

Доказательство. Согласно (5.7), для любого индекса $n = 0, 1, \ldots$, 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 $\alpha_{n+1} = \dfrac{A_{n+1} + \sqrt{D}}{B_{n+1}}$, 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

$$B_0\big(P_n(A_{n+1} + \sqrt{D}) + B_{n+1}P_{n-1}\big) = \\ = \big(A_0 + \sqrt{D}\big)\big(Q_n(A_{n+1} + \sqrt{D}) + B_{n+1}Q_{n-1}\big).$$

Раскрывая в последнем равенстве скобки и приводя слогаемые со множителем $\sqrt{D}$, получим равенство

$$B_0B_{n+1}P_{n-1} - A_0A_{n+1}Q_n - A_0B_{n+1}Q_{n-1} + B_0P_nA_{n+1} - Q_nD = \\ = \big(A_0Q_n + A_{n+1}Q_n + B_{n+1}Q_{n-1} - B_0P_n\big)\sqrt{D}.$$

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}

$$Q_{n-1} = \frac{B_0P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}}, \tag{5.31}$$

а также из левой части равенства, для числителя P_{n-1}

$$P_{n-1} = \frac{A_0A_{n+1}Q_n + A_0B_{n+1}Q_{n-1} + Q_nD - B_0P_nA_{n+1}}{B_0B_{n+1}} = \\ = \frac{Q_n(D - A_0^2) - B_0P_n(A_{n+1} - A_0)}{B_0B_{n+1}}. \tag{5.32}$$

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

$$P_n\frac{B_0P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}} - \\ - Q_n\frac{Q_n(D - A_0^2) - B_0P_n(A_{n+1} - A_0)}{B_0B_{n+1}} = (-1)^{n+1}.$$

Домножая наше равенство на B_0B_{n+1}, раскрывая скобки и сокращая подобные члены, получим окончательный результат

$$\big(P_nB_0 - Q_nA_0\big)^2 - Q_n^2D = (-1)^{n+1}B_0B_{n+1}.$$

□

В частном случае, когда $\alpha_0 = \sqrt{N}$, выражение (5.30) принимает вид

$$P_n^2 - Q_n^2D = (-1)^{n+1}B_{n+1}, \tag{5.33}$$

поскольку $A_0 = 0$ и $B_0 = 1$.

5.4 Наилучшие приближения

В некоторых методах анализа криптографических схем нам потребуется понятие «наилучшего приближения». Поэтому мы завершим эту главу результатами, связывающими понятия о непрерывных дробях и наилучших приближениях. При изложении мы следуем монографии [6].

Определение 5.7. *Пусть α действительное, отличное от нуля число. Рациональная дробь $\frac{P}{Q}$ называется наилучшим приближением к числу α, если любой другой дроби $\frac{A}{B} \neq \frac{P}{Q}$ такой, что $1 \leqslant B \leqslant Q$, 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 5.4. *Всякое наилучшее приближение к действительному числу α есть подходящая дробь к нему. И наоборот, каждая подходящая дробь $\frac{P_n}{Q_n}$ к числу α при $n \geqslant 1$ есть наилучшее приближение.*

Прежде чем переходить к доказательству, заметим, что данное нами определение 5.7 эквивалентно тому, что система неравенств

$$\begin{cases} |x - \alpha y| \leqslant |P - \alpha Q|, \\ 0 < y \leqslant Q, \end{cases} \tag{5.34}$$

имеет единственное решение в целых числах $x = P$, $y = Q$. Нам понадобится следующая лемма.

Лемма 5.9. *Пусть $\frac{P_n}{Q_n}$, $\frac{P_{n+1}}{Q_{n+1}}$ две соседние подходящие дроби к числу α, причем $\frac{P_{n+1}}{Q_{n+1}} \neq \alpha$. Тогда система неравенств*

$$\begin{cases} |x - \alpha y| \leqslant |P_n - \alpha Q_n|, \\ 0 < y \leqslant Q_{n+1}, \end{cases} \tag{5.35}$$

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 (5.35). 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 (5.35), 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 $y \geqslant Q_n + Q_{n+1}$, что противоречит второму неравенству в (5.35). 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 (5.35). Лемма доказана. □

Перейдем к доказательству теоремы 5.4. Пусть дробь $\frac{P}{Q}$ является наилучшим приближением к числу α и n максимальный индекс такой, что $Q_n \leqslant Q$. Предположим, что

$$|P - \alpha Q| < |P_n - \alpha Q_n|, \tag{5.36}$$

тогда, согласно утверждению леммы 5.9, дробь $\frac{P}{Q}$ совпадает с одной из подходящих дробей $\frac{P_n}{Q_n}$ или $\frac{P_{n+1}}{Q_{n+1}}$. Если (5.36) не выполнено, то $|P-\alpha Q| \geqslant |P_n - \alpha Q_n|$ 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 $n \geqslant 0$ каждая подходящая дробь $\frac{P_{n+1}}{Q_{n+1}}$ является наилучшим приближением. Рассмотрим значения x, y, являющиеся решением системы сравнений

$$\begin{cases} |x - \alpha y| \leqslant |P_{n+1} - \alpha Q_{n+1}|, \\ 0 < y \leqslant Q_{n+1}. \end{cases} \tag{5.37}$$

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 (5.37) следуют неравенства

$$\begin{cases} |x - \alpha y| \leqslant |P_n - \alpha Q_n|, \\ 0 < y \leqslant Q_{n+1}, \end{cases}$$

которым, согласно лемме 5.9, 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 (5.37), то $\frac{P_{n+1}}{Q_{n+1}}$ наилучшее приближение. Теорема доказана. □

Докажем еще одну теорему, которая будет использована нами позднее при обосновании алгоритмов факторизации целых чисел.

Теорема 5.5. *Если несократимая дробь $\frac{P}{Q}$, при $Q > 0$, удовлетворяет неравенству*

$$\left|\alpha - \frac{P}{Q}\right| < \frac{1}{2Q^2}, \tag{5.38}$$

то она есть наилучшее приближение к α.

Доказательство. Предположим, что целые числа $x = A$, $y = B$ удовлетворяют неравенствам (5.34), то есть

$$\begin{cases} |A - \alpha B| \leqslant |P - \alpha Q|, \\ 0 < B \leqslant Q. \end{cases}$$

Тогда рассмотрим разность целых чисел $AQ-BP$ и получим неравенство

$$|AQ - BP| = |Q(A - \alpha B) - B(P - \alpha Q)| \leqslant$$
$$\leqslant Q|A - \alpha B| + B|P - \alpha Q| \leqslant 2Q|P - \alpha Q| < qQ^2 \left|\alpha - \frac{P}{Q}\right| < 1,$$

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 (5.34) имеет только одно решение. Теорема доказана. □

Заметим, что из утверждения теорем 5.4 и 5.5 следует, что всякая несократимая дробь $\frac{P}{Q}$, удовлетворяющая неравенству (5.38), является подходящей дробью к числу α.

Глава 6

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 - Реккурентные 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 важную роль, являясь долговременными параметрами криптографических схем и подвергаясь атакам нарушителей в первую очередь. 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 34.10-94, 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:

$$2^{255} < p < 2^{256}, \quad 2^{254} < q < 2^{256}, \quad q \equiv 1 + t \pmod{p},$$

для некоторого целого t, удовлетворяющего неравенству $|t| \leqslant 2\sqrt{p}$. 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 $p_0, \ldots, p_n$ 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** $p_k \leqslant h$ **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 проверятся 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 $p_n < s = h^2$.

Трудоемкость алгоритма построения таблицы простых чисел может быть оценена сверху величиной $\frac{b\sqrt{b}}{2}$ операций деления на простые числа, не превосходящие величины $\sqrt{b}$.

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 $\mathbf{НОД}(a,\ m) > 1$, 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

зацикливания, 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*

$$a^{m-1} \equiv 1 \pmod{m} \tag{6.1}$$

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 $i = 1, \ldots, k$ выполнено условие $p_i - 1 | m - 1$.*

Доказательство. В начале предположим, что для числа m выполнены условия теоремы, и рассмотрим произвольный вычет a такой, что $\mathbf{НОД}(a,\ m) = 1$. Для любого индекса $i = 1,\ \ldots,\ k$ 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. 27), 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 $i = 1,\ \ldots,\ k$ 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

$p_i - 1 | m - 1$ 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

$$\operatorname{ord}_{p_i^{\alpha_i}} b_i = \varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i - 1}(p_i - 1) | m - 1.$$

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. □

Следствие 1. *Пусть нечетное целое число $m = p_1 \cdots p_k$ удовлетворяет критерию Корсельта, тогда $k \geqslant 3$.*

Доказательство. Предположим обратное, тогда найдется удовлетворяющее критерию Кормельта 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. □

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. [15], 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 Корсельта, принято называть числами Кармайкла. Мы можем также привести чис-

ла Кармайкла, имеющие четыре или пять простых делителей

$$41041 = 7 \cdot 11 \cdot 13 \cdot 47,$$
$$825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73.$$

Известно, что чисел Кармайкла бесконечно много, см. [13, 19], 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 [40] 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. $\mathbf{НОД}(a,\ m) = 1$.
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, $1 \leqslant i \leqslant k$ такой, что $\alpha_i > 1$. Без ограничения общности будем считать, что $i = 1$.

Определим целое число a равенством

$$a = 1 + \frac{m}{p_1}, \tag{6.2}$$

тогда $a \equiv 1 \pmod{p_i}$ для всех индексов $1 \leqslant i \leqslant k$. 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 2.3, 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 $\mathbf{НОД}(k,\ p_1) = 1$. Используя формулу бинома Ньютона, см. (2.16), мы можем записать сравнение

$$1 \equiv a^d \equiv \left(1 + kp_1^{\alpha_1 - 1}\right)^d \equiv 1 + kdp_1^{\alpha_1 - 1} \pmod{p_1^{\alpha_1}},$$

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

$$\begin{cases} x \equiv s \pmod{p_1}, \\ x \equiv 1 \pmod{p_2}, \\ \qquad\qquad \cdots \\ x \equiv 1 \pmod{p_k}, \end{cases} \tag{6.3}$$

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, $2 \leqslant i \leqslant k$. 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

$$u^{\frac{m-1}{2}} \equiv a^{\frac{m-1}{2}} w^{\frac{m-1}{2}},$$
$$\left(\tfrac{u}{m}\right) = \left(\tfrac{a}{m}\right)\left(\tfrac{w}{m}\right) = \left(\tfrac{a}{m}\right) w^{\frac{m-1}{2}},$$

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. □

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 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. □

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 [29]. Позднее, в 1980 году, Майкл Рабин (Michael O. Rabin) [37] 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* $\mathbf{НОД}(6,\ m) = 1$. *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, $0 \leqslant k < n$.

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 $a\mathcal{S} \cap \mathcal{S} = \varnothing$.*

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 $(as)^{2^l q} \equiv -1 \pmod m$, $0 \leqslant l < n$.
3. $s^{2^k q} \equiv -1 \pmod m$, $0 \leqslant k < n$ и $(as)^q \equiv 1 \pmod m$.
4. $s^{2^k q} \equiv -1 \pmod m$, $0 \leqslant k < n$ и $(as)^{2^l q} \equiv -1 \pmod m$, $0 \leqslant l < n$.

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 $l \leqslant k$, 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. □

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. □

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

$$\mathcal{G} = \left\{ 1 + k\frac{m}{p} \pmod{m}, \quad \text{для всех } 0 \leqslant k < p \right\}$$

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

$$\left(1 + k\frac{m}{p}\right)\left(1 + h\frac{m}{p}\right) \equiv \left(1 + (k+h)\frac{m}{p} + kh\frac{m^2}{p^2}\right) \equiv \left(1 + l\frac{m}{p}\right) \pmod{m}, \quad (6.4)$$

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 $\mathbf{НОД}(g,\ m) = d > 1$ 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,

$$\mathbb{Z}_m \supseteq \left|\bigcup_{g\in\mathcal{G}} gS\right| = |G| \cdot |S| = p|S|.$$

Вспоминая, что $\mathbf{НОД}(6,\ m) = 1$ получаем неравенство $p \geqslant 5$ 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 $p_1,\ \ldots, p_k$ различные простые числа, $k \in \mathbb{N}$. Без ограничения общности будем считать, что $p_1 < \cdots < p_k$.

Определим вычеты для каждого $i = 1,\ \ldots, k$ определим вычет c_i по модулю m как решение системы сравнений

$$\begin{cases} x \equiv a_i \pmod{p_i}, \\ x \equiv 1 \pmod{p_j}, \quad \text{для всех} \quad j,\ j \neq i, \end{cases}$$

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 $c_1,\ \ldots,\ c_k \in \mathcal{A}$. Более того, вычеты $c_1,\ \ldots,\ c_k$ обратимы и $c_1^{-1},\ \ldots,\ c_k^{-1} \in \mathcal{A}$.

Рассмотрим вычет $d \equiv c_1 c_2 \pmod m$ и покажем, что $d \in \mathcal{A}$. При $k \geqslant 3$ 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 2.3, 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, $4|S| \leqslant |\mathbb{Z}_m|$. Теорема доказана. □

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 **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. □

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. [29], 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 $\mathbf{НОД}\,(a,\ m) = 1$.

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, $\mathbf{НОД}\,(a,\ m) = 1$, 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 $\operatorname{ord}_m a = m-1$ и a является первообразным корнем по модулю m. Следовательно, $\varphi(m) = m-1$, а это возможно только в случае, когда m простое число. □

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 $1 \leqslant a < m$. Если $\mathbf{НОД}(a,\ m) > 1$, 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** $k \leqslant n$ **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

$$m-1 = fr, \quad \mathbf{НОД}(f,\ r) = 1, \tag{6.5}$$

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, $k = 1, \ldots, n$, входящего в разложение числа f, найдется некоторое взаимно простое с m целое число a_k такое, что

$$a_k^{m-1} \equiv 1 \pmod{m} \quad \text{и} \quad \textbf{НОД}\left(a_k^{\frac{m-1}{q_k}} - 1,\ m\right) = 1. \tag{6.6}$$

2. Найдется некоторое взаимно простое с m целое число b такое, что

$$b^{m-1} \equiv 1 \pmod{m} \quad \text{и} \quad \textbf{НОД}\left(b^{\frac{m-1}{r}} - 1,\ m\right) = 1. \tag{6.7}$$

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 2.3, $t | m-1$. 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 $k = 1, \ldots, n$. 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. □

Доказанный нами результат был впоследствии использован Деррик ком Лемером (Derrick Henry Lehmer) для доказательства простоты целых чисел. Следуя статье [42], приведем несколько полезных для наших целей результатов.

Теорема 6.6 (Лемер, следствие теоремы Поклингтона, 1927)**.** *Пусть нечетное целое число $m > 0$. Если число m удовлетворяет условию теоремы 6.5 и $f^2 \geqslant \sqrt{m}$, 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 $p = 1 + kf \geqslant 1 + \sqrt{m} > \sqrt{m}$, которое противоречит утверждению леммы 1.6. Полученное противоречие завершает доказательство. □

Приведем пример использования данной теоремы.

Пример 6.1. Рассмотрим число $m = 156 \cdot 5^{202} + 1$. Используя вычисления на ЭВМ, находим, что

$$13^m \equiv 1 \pmod{m} \quad \text{и} \quad \textbf{НОД}\left(13^{156 \cdot 5^{201}},\ m\right) = 1,$$

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 $\mathbf{НОД}\left(b^{\frac{m-1}{r}},\ m\right) = 1$ 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 $\mathbf{НОД}(t,\ r) > 1$, 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. □

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

$$(1+fB)^2 > m, \tag{6.8}$$

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 удается 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*

$$c_1 \equiv \frac{m-1}{f} \pmod{f} \quad и \quad c_2 = \frac{m - c_1 f - 1}{f^2},$$

то есть разложим число m по степеням f. Число m простое тогда и только тогда, когда многочлен $f(x) = c_2x^2 + c_1x + 1 \in \mathbb{Z}[x]$ 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 $m = p_1 p_2 = (1 + x_1 f)(1 + x_2 f) > f p_2 > f^3 \geqslant m$. Таким образом, выполнено $f < p_2 < f^2$. Аналогичным способом выводим, 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. □

6.3 $N+1$ метод доказательства простоты

Рассмотрим метод доказательства простоты числа m, использующий разложение $m+1$ на простые сомножители. Прежде чем сформулировать и доказать необходимое утверждение, мы дадим некоторые определения.

Определение 6.1. *Рассмотрим многочлен $f(x) = x^2 - ax + b$ с целыми коэффициентами такими, что* $\mathbf{НОД}(a,\ b) = 1$ *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

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n, \quad n = 0, 1\ \ldots. \tag{6.9}$$

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 6.3. *Пусть последовательности чисел* $\{U_n\}, \{V_n\}$ *определены равенствами (6.9). Тогда верны следующие утверждения.*

1. *Для всех индексов* $n = 0, 1 \ \ldots$ *значения* U_n, V_n *являются целыми числами. Более того, выполнены рекуррентные соотношения*

$$U_{n+1} = aU_n - bU_{n-1}, \quad V_{n+1} = aV_n - bV_{n-1}, \quad n = 1, 2, \ \ldots \tag{6.10}$$

   где $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = a$.

2. *Выполнены равенства*

$$U_{2n} = U_n V_n, \quad V_{2n} = \frac{1}{2}\left(V_n^2 + DU_n^2\right). \tag{6.11}$$

3. *Выполнены равенства*

$$U_{n+1} = \frac{1}{2}\left(V_n + aU_n\right), \quad V_{n+1} = \frac{1}{2}\left(aV_n + DU_n\right). \tag{6.12}$$

4. *Выполнены равенства*

$$U_{k+l} = \frac{1}{2}(U_k V_l + U_l V_k), \quad V_{k+l} = \frac{1}{2}(V_k V_l + DU_k U_l). \tag{6.13}$$

5. *Выполнено равенство* $4b^n = V_n^2 - DU_n^2$.

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

$$\alpha + \beta = a, \quad \alpha\beta = b, \quad (\alpha - \beta)^2 = D. \tag{6.14}$$

Докажем первое утверждение леммы. Подставляя значения $n = 0, 1$ в соотношения (6.9), получим равенства $U_0 = 0$, $U_1 = 1$, а также $V_0 = 2$, $V_1 = a$. Теперь, используя индуктивное предположение, докажем истинность соотношений (6.10). Учитывая (6.14), получаем равенства

$$aU_n - bU_{n-1} = \frac{1}{\alpha-\beta}\left((\alpha+\beta)(\alpha^n-\beta^n) - \alpha\beta(\alpha^{n-1}-\beta^{n-1})\right) = \\ = \frac{1}{\alpha-\beta}\left(\alpha^{n+1}-\beta^{n+1}\right) = U_{n+1},$$

$$aV_n - bV_{n-1} = (\alpha+\beta)\left(\alpha^n+\beta^n\right) - \alpha\beta\left(\alpha^{n+1}+\beta^{n+1}\right) = \\ = \alpha^{n+1}+\beta^{n+1} = V_{n+1}.$$

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 (6.14), получаем равенства

$$U_{2n} = \frac{1}{\alpha-\beta}\left(\alpha^{2n}-\beta^{2n}\right) = \frac{1}{\alpha-\beta}\left(\alpha^n-\beta^n\right)\left(\alpha^n+\beta^n\right) = U_nV_n,$$

$$V_n^2 + DU_n^2 = \left(\alpha^n+\beta^n\right)^2 + \left(\alpha^n-\beta^n\right)^2 = 2\left(\alpha^{2n}+\beta^{2n}\right) = 2V_{2n},$$

из которых следует второе утверждение леммы.

Третье утверждение леммы, при внимательном рассмотрении, оказывается частным случаем четвертого утверждения.

Четвертое утверждение леммы вытекает из равенств

$$U_kV_l + U_lV_k = \frac{1}{\alpha-\beta}\left((\alpha^l+\beta^l)(\alpha^k-\beta^k) + (\alpha^k+\beta^k)(\alpha^l-\beta^l)\right) = \\ = \frac{2}{\alpha-\beta}\left(\alpha^{k+l}-\beta^{k+l}\right) = 2U_{k+l}.$$

$$V_kV_l + DU_kU_l = \left(\alpha^k+\beta^k\right)\left(\alpha^l+\beta^l\right) + (\alpha-\beta)^2\frac{\left(\alpha^k-\beta^k\right)}{\alpha-\beta}\frac{\left(\alpha^l-\beta^l\right)}{\alpha-\beta} = \\ = 2\left(\alpha^{k+l}+\beta^{k+l}\right) = 2V_{k+l}.$$

Докажем пятое утверждение леммы. Для этого выразим α^n, β^n через U_n, V_n. Поскольку выполнены равенства (6.9), то

$$2\alpha^n = V_n - (\alpha - \beta)U_n, \quad 2\beta^n = V_n + (\alpha - \beta)U_n,$$

тогда, с учетом (6.14), получаем равенства

$$4b^n = (2\alpha^n)(2\beta^n) = V_n^2 - (\alpha - \beta)^2 U_n^2 = V_n^2 - DU_n^2$$

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 $d, 2d, 3d, \ldots, (k-1)d$. 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. □

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 $n = 0, 1, \ldots 11$. Согласно первому утверждению леммы, выполнены равенства

$$(U_0, V_0) = (0, 2),$$
$$(U_1, V_1) = (1, 3).$$

Далее, воспользовавшись рекуррентными соотношениями (6.10), вычисляем

$$(U_2, V_2) = (3, 7), \qquad (U_7, V_7) = (377, 843),$$
$$(U_3, V_3) = (8, 18), \qquad (U_8, V_8) = (987, 2207),$$
$$(U_4, V_4) = (21, 47), \qquad (U_9, V_9) = (2584, 5778),$$
$$(U_5, V_5) = (55, 123), \qquad (U_{10}, V_{10}) = (6765, 15127),$$
$$(U_6, V_6) = (144, 322), \qquad (U_{11}, V_{11}) = (17711, 39603),$$
$$(U_{12}, V_{12}) = (46368, 103682).$$

Понятно, что при больших значениях индекса n вычислить пару U_n, V_n, наивно применяя соотношения (6.10), достаточно сложно. Мы можем предложить простой алгоритм, использующий соотношения (6.11)

и (6.12), 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 (6.10), 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 $\mathbf{НОД}(a,\ b) = 1$, 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** $i \leqslant r - 1$ **выполнить**

4.1. Используя равенства (6.11), вычислить

$$x = UV, \quad y = \frac{1}{2}\left(V^2 + DU^2\right), \quad U = x, \quad V = y.$$

4.2. **Если** $n_i = 1$, **то**, используя равенства (6.12), вычислить

$$x = \frac{1}{2}\left(V + aU\right), \quad y = \frac{1}{2}\left(aV + DU\right), \quad U = x, \quad V = y.$$

4.3. Вычислить $i = i + 1$.

5. **Пока** $s > 0$ **выполнить**

5.1. Используя равенства (6.11), вычислить

$$x = UV, \quad y = \frac{1}{2}\left(V^2 + DU^2\right), \quad U = x, \quad V = y.$$

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 6.4. *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 6.3, $U_d|U_n$ 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 6.3 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 6.3 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. □

Лемма 6.5. *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

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

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

$$\begin{cases} \alpha^p \equiv \alpha \pmod{p}, \quad \beta^p \equiv \beta \pmod{p}, \quad \text{при} \quad \left(\frac{D}{p}\right) = 1, \\ \alpha^p \equiv \beta \pmod{p}, \quad \beta^p \equiv \alpha \pmod{p}, \quad \text{при} \quad \left(\frac{D}{p}\right) = -1. \end{cases}$$

Теперь вычислим значение $U_{\Phi(p)}$. При $\left(\frac{D}{p}\right) = -1$ получаем $\Phi(p) = p+1$ и

$$U_{\Phi(p)} = \frac{1}{\alpha-\beta}\left(\alpha^{p+1} - \beta^{p+1}\right) \equiv \frac{1}{\alpha-\beta}(\beta\alpha - \alpha\beta) \equiv 0 \pmod{p}.$$

При $\left(\frac{D}{p}\right) = 1$ получаем $\Phi(p) = p-1$ и

$$U_{\varphi(p)} = \frac{1}{\alpha-\beta}\left(\alpha^{p-1} - \beta^{p-1}\right) \equiv \frac{1}{\alpha-\beta}\left(\frac{\alpha}{\alpha} - \frac{\beta}{\beta}\right) \equiv 0 \pmod{p}.$$

Лемма доказана. □

Теперь сформулируем теорему, которая позволяет нам сделать вывод о строении простых делителей числа m, по известным делителям числа $m+1$.

Теорема 6.10 (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 **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* **НОД**$\left(U_{\frac{m+1}{q_i}},\ m\right) = 1$, $i = 1, \ldots, s$,

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 6.4, $d | m+1$.

Из второго условия теоремы получаем, что $U_{\frac{m+1}{q_i}} \not\equiv 0 \pmod{p}$, следовательно, $d \not| \frac{m+1}{q_i}$. Сравнивая два полученных утверждения получаем, что $d | q_i^{\alpha_i}$.

С другой стороны, согласно лемме 6.5 выполнено $U_{\Phi(p)} \equiv 0 \pmod{p}$. Воспользовавшись еще раз утверждением леммы 6.4, получаем условие $d|\Phi(p)$. Таким образом, $d|\,\mathbf{НОД}\,(q_i^{\alpha_i},\ \Phi(p)) = q_i^{\alpha_i}$. 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. □

Эта теорема имеет очевидное следствие, которое позволяет сделать вывод о простоте числа m.

Следствие 1. *Пусть для числа m выполнены утверждения теоремы 6.10 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 6.10, то $p = \pm 1 + kf$, $q = \pm 1 + lf$ для некоторых целых чисел $k \geqslant 1$, $l \geqslant 1$ и мы получаем, что $m = pq > (f-1)^2 > m$. Противоречие. □

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

$$\mathbf{НОД}\,(a,\ b) = 1, \quad \mathbf{НОД}\,(m,\ b) = 1, \quad \mathbf{НОД}\left(m,\ a^2 - 4b\right) = 1,$$

и проверим условия теоремы 6.10. 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.

6.4 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 6.11 (Дирихле, см. [3], гл. 3)**.** *Пусть арифметическая прогрессия задана соотношением $x_k = ak + b$, $k = 0,\ 1,\ \ldots$, 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.

6.4.1 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. [28]. 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

$$A < p < B. \tag{6.15}$$

Из неравенства (6.15) мы можем получить оценки на q и k. Действительно, поскольку q целое, удовлетворяющее неравенству $q > \sqrt{p}$, то из (6.15) следует оценка на q снизу

$$q \geqslant \left\lceil \sqrt{B} \right\rceil > \sqrt{p}.$$

Обозначим $q_A = \left\lceil \sqrt{B} \right\rceil$ и ограничим простое число q сверху, то есть $q_A \leqslant q \leqslant \alpha q_A$ 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

$$p = kq + 1 \leqslant k\alpha q_A + 1 < \alpha q_A \frac{B-1}{\alpha q_A} + 1 = B$$

и для p верна оценка сверху (6.15).

Аналогично, если $k \geqslant \left\lceil \frac{A}{q_A} \right\rceil$, то выполнено

$$p = kq + 1 > kq \geqslant kq_A \geqslant q_A \frac{A}{q_A} = A,$$

и для p верна оценка снизу (6.15). Исходя из того, что интервал для значений k не должен быть пустым, мы получаем оценку сверху на значение параметра α. Действительно, из неравенства $\left\lceil \frac{A}{q_A} \right\rceil < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$ получаем, что α ограничено сверху величиной $\frac{B-1}{A}$, то есть принадлежит интервалу

$$1 < \alpha < \frac{B-1}{A}. \tag{6.16}$$

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 (6.16).

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 $d_1, \ldots, d_n$ и нашли остатки от деления $\delta_1, \ldots, \delta_n$

такие, что $p \equiv \delta_n \pmod{d_n}$. Предположим, что найдется остаток $\delta_i \equiv 0 \pmod{d_i}$, $1 \leqslant i \leqslant n$, 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, $1 \leqslant i \leqslant n$. 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 приступать 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** $B \leqslant 2^{16}$, **то** выбрать случайным образом простое число p из таблицы простых чисел и завершить работу.
2. Определить переменные $q_A = \left\lceil \sqrt{B} \right\rceil$, $\alpha = \frac{B+A-1}{2A}$ и $k_1 = \left\lceil \frac{A}{q_A} \right\rceil$, $k_2 = \left\lfloor \frac{B-1}{q_A} \right\rfloor$.
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 $d_1 = 3, \ \ldots, \ d_{10} = 31$ определить остатки $\delta_1, \ \ldots, \ \delta_{10}$ от деления числа p на простые $d_1, \ \ldots, \ d_{10}$, то есть $\delta_i \equiv p \pmod{d_i}$, $1 \leqslant i \leqslant 10$.
6. Вычислить $k = k + 2$, $p = p + 2q$ и $\delta_i = \delta_i + 2 \pmod{d_i}$ для всех i таких, что $1 \leqslant i \leqslant 10$.
7. **Если** $k > k_s$, **то** вернуться на шаг 4.
8. **Если** найдется индекс i, $1 \leqslant i \leqslant 10$ 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 НОД** $\left(a^k - 1, \ p\right) = 1$ 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 6.10, и последовательностей Люка для доказательства простоты числа p. Детальную проработку этих модификаций мы оставляем читателю.

6.4.2 Алгоритм построения сильно простого числа

Во многих приложениях возникает необходимость строить простые числа с дополнительными условиями. Дадим следующее определение.

Определение 6.2. *Мы будем называть нечетное простое число p сильно простым, если найдутся такие нечетные простые числа q, s и r такие, что*

$$p \equiv 1 \pmod{q}, \quad p \equiv -1 \pmod{s}, \quad q \equiv 1 \pmod{r}, \tag{6.17}$$

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 (6.17), 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 [44] 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 (6.17). Для этого зафиксируем целое число $a \geqslant 1$, 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

$$q = (ks + x)r + 1, \quad k = 0,\ 1,\ \ldots$$

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

$$p = 2aq + 1 = 2a((ks + x)r + 1) + 1 = \\ = 2aksr + 2arx + (2a + 1) \equiv -1 \pmod{s}.$$

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

$$A < p < B, \quad \text{тогда} \quad q_A = \left\lceil \frac{A-1}{2a} \right\rceil \leqslant q = \frac{p-1}{2a} \leqslant \left\lfloor \frac{B-1}{2a} \right\rfloor = q_B,$$

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

$$r \geqslant \lceil \sqrt{q_A} \rceil = r_A,$$

тогда $\lfloor \alpha r_A \rfloor \geqslant r \geqslant r_A$ для некоторого действительного параметра $\alpha > 1$.

Если $ks + x \leqslant \left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor$, тогда выполнена оценка сверху

$$q = (ks + x)r + 1 < \frac{q_B - 1}{\alpha r_A} \alpha r_A + 1 \leqslant q_B.$$

Аналогично, если $ks + x \geqslant \left\lceil \frac{q_A}{r_A} \right\rceil$, то выполнена оценка снизу

$$q = (ks + x)r + 1 \geqslant \frac{q_A}{r_A} r_A + 1 > q_A.$$

Таким образом, мы получили ограничения сверху и снизу на размер перебираемого параметра k

$$\left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor \geqslant (ks + x) \geqslant \left\lceil \frac{q_A}{r_A} \right\rceil. \tag{6.18}$$

Исходя из того, что перебираемый интервал не должен быть пустым, мы получим оценку сверху на параметр α. 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 (6.18), получаем оценки для k

$$\left\lfloor \frac{q_B-1}{\alpha s r_A} \right\rfloor - x \geqslant k \geqslant \left\lceil \frac{q_A}{s r_A} \right\rceil - x,$$

а также оценку на s сверху. Поскольку, в силу построения, $s > x > 0$ и $k \geqslant 1$, то мы получаем неравенство

$$\frac{q_B-1}{\alpha r_A} \geqslant \left\lfloor \frac{q_B-1}{\alpha r_A} \right\rfloor \geqslant (k+1)s > ks + x,$$

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[1] $\lceil \sqrt{s_A} \rceil$.

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 $1 \leqslant a \leqslant \left\lfloor \frac{B-1}{2\sqrt{A}} \right\rfloor$.
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, $k_1 \leqslant k \leqslant k_2$.
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 $k = k + 1$.
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.

[1] Нижняя граница для числа s определяется исходя из криптографических требований к конкретной системе защиты информации.

15. Определить значение счетчика $n = 10$.
16. Вычислить случайное целое число a и $n = n - 1$.
17. **Если НОД** $\left(a^{ks+x} - 1,\ q\right) = 1$ и $a^{q-1} \equiv 1 \pmod{q}$, **то** перейти у 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 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 [18] предложил другой способ построения сильно простых чисел. Он основан на следующей лемме.

Лемма 6.6 (Гордон). *Простое число $p > 2$ является сильно простым и удовлетворяет сравнениям (6.17), тогда и только тогда, когда p имеет вид $p = u + 2kqs$, для натурального k и*

$$u = \begin{cases} w, & \text{если} \quad w - \text{нечетно}, \\ w + qs, & \text{если} \quad w - \text{четно}, \end{cases}$$

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 (6.17) выполнены, если простое число q имеет большой простой делитель r.

Пусть π сильно простое число, не удовлетворяющее условиям леммы. В силу сравнений (6.17) $\pi - p \equiv 1 - 1 \equiv 0 \pmod{q}$ 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.

Глава 7

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 - Метод Женга - Метод Макки.

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 $p_1, \ldots, p_k$, 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 α_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 $p \leqslant \sqrt{m}$.

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

$$m = x^2 - y^2, \quad \text{где} \quad x = \frac{p+q}{2}, \quad y = \frac{p-q}{2}. \tag{7.1}$$

Метод разложения на множители Ферма 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 $h^2 \geqslant \sqrt{m}$, 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 быстродействие 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 $h^2 \leqslant m < (h+1)^2$, 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 $h^2 \leqslant m < (h+1)^2$.

1. Определить $x = m$.
2. Вычислить[1] $y = \left\lfloor \frac{x + \lfloor \frac{m}{x} \rfloor}{2} \right\rfloor$.
3. **Если** y $<$ x , **то** положить $x = y$ и вернуться на шаг 2. В противном случае, положить $h = x$ и завершить алгоритм. □

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

$$\frac{x + \frac{m}{x}}{2} > \sqrt{m}, \quad \text{при} \quad m > 0. \tag{7.2}$$

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).

[1] 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 $x \geqslant h$. 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 $y \geqslant x$, $x > h$ 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 $x^2 > h^2 \geqslant m$, следовательно, $m - x^2 < 0$ и $y - x < 0$. Таким образом, мы получили противоречие нашему предположению $y \geqslant x$.

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 $q_1, \ldots, q_r$ различные нечетные простые числа, ε_1, $\ldots$, ε_r набор знаков, принимающих значения ± 1. Тогда существует бесконечно много простых чисел p таких, что выполнены равенства*

$$\left(\frac{p}{q_1}\right) = \varepsilon_1, \ldots, \left(\frac{p}{q_r}\right) = \varepsilon_r,$$

где $\left(\frac{p}{q_i}\right)$ – символ Лежандра для всех $i = 1, \ldots, r$.

Доказательство. Для любого индекса $i = 1, \ldots, r$ 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

$$\{x \equiv b_i \pmod{q_i} \quad i = 1, \ \ldots, \ r. \tag{7.3}$$

Поскольку числа $q_1, \ \ldots, \ q_r$ 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 6.11, 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

$$\left(\frac{p}{q_i}\right) = \left(\frac{x_0}{q_i}\right) = \left(\frac{b_i}{q_i}\right) = \varepsilon_i, \quad i = 1, \ \ldots, \ r,$$

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 $q_1, \ \ldots, q_r$ различные нечетные простые.

Зафиксируем некоторый набор знаков $\varepsilon_1, \ \ldots, \varepsilon_r$, принимающих значения ± 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

$$\left(\frac{p}{q_i}\right) = \left(\frac{x_0}{q_i}\right) = \left(\frac{b_i}{q_i}\right) = \varepsilon_i, \quad i = 1, \ \ldots, \ r.$$

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. □

Из утверждения теоремы следует, что мы можем реализовать следующую процедуру проверки чисел v. Вначале мы проверяем выполнимость 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 $1, \ldots, p-1$, 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 $q_1, \ldots, q_r$ различные нечетные простые. Пусть $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r$ знаки ± 1, которые соответствуют символам Лежандра, то есть

$$\left(\frac{2}{p}\right) = \varepsilon_0, \ \left(\frac{q_1}{p}\right) = \varepsilon_1, \ \ldots, \ \left(\frac{q_r}{p}\right) = \varepsilon_r$$

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

$k = 0,\ 1\ \ldots$, для некоторого целого x_0, взаимно простого с $8q_1 \cdots q_r$. Количество таких прогрессий ограниченно 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

$$\begin{cases} x \equiv b_0 \pmod 8, \\ x \equiv b_i \pmod{q_i}, \quad i = 1,\ \ldots,\ r, \end{cases} \tag{7.4}$$

где величины b_i определяют знак символов Лежандра $\left(\frac{2}{p}\right)$ и $\left(\frac{q_i}{p}\right)$, для $i = 1,\ \ldots,\ r$. 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 $\varepsilon_0, \varepsilon_1,\ \ldots,\ \varepsilon_r$ ровно половина значений x_0 таких, что $0 < x_0 < 8q_1 \cdots q_r$, $\mathbf{НОД}(x_0,\ 8q_1 \cdots q_r) = 1$, 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[2]. □

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 $1 - \frac{1}{2^k}$.

[2]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 [11, §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 [24].

Метод Лемана развивает идеи, заложенные в алгоритме Ферма и ищет делители числа m, используя равенство

$$x^2 - y^2 = 4bm, \tag{7.5}$$

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 $b \geqslant 1$, удовлетворяющие следующим условиям.*

1. *Выполнено равенство $x^2 - y^2 = 4bm$ при $b < \sqrt[3]{m}$.*
2. *Выполнено неравенство $0 \leqslant x - \lfloor\sqrt{4bm}\rfloor < \frac{\sqrt[6]{m}}{4\sqrt{b}} + 1$.*

Вначале докажем следующую лемму.

Лемма 7.2. *Пусть выполнены условия теоремы 7.3. Тогда найдутся натуральные числа r, s такие, что*

$$rs < \sqrt[3]{m} \quad и \quad |pr - qs| < \sqrt[3]{m}.$$

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 $P_0 Q_0 < \sqrt[3]{m}$. С другой стороны, $P_t Q_t = pq > p > \sqrt[3]{m}$. Следовательно, найдется максимальный индекс n такой, что

$$P_n Q_n < \sqrt[3]{m}, \quad P_{n+1} Q_{n+1} > \sqrt[3]{m}, \quad 0 \leqslant n < t. \tag{7.6}$$

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 $\frac{q}{p} \geqslant \frac{P_{n+1}}{Q_{n+1}}$, которое может быть переписано в виде

$$\frac{p}{Q_{n+1}} \leqslant \frac{q}{P_{n+1}}. \tag{7.7}$$

Воспользовавшись равенством (5.13), получим, что

$$\left|\frac{q}{p} - \frac{P_n}{Q_n}\right| \leqslant \frac{1}{Q_n Q_{n+1}}, \tag{7.8}$$

тогда, учитывая (7.6), (7.7) и (7.8), получим

$$|pr - qs| = |pP_n - qQ_n| = pQ_n\left|\frac{q}{p} - \frac{P_n}{Q_n}\right| \leqslant \frac{p}{Q_{n+1}} =$$
$$= \sqrt{\frac{p}{Q_{n+1}}}\sqrt{\frac{p}{Q_{n+1}}} \leqslant \sqrt{\frac{p}{Q_{n+1}}}\sqrt{\frac{q}{P_{n+1}}} = \sqrt{\frac{m}{P_{n+1}Q_{n+1}}} <$$
$$< \frac{\sqrt{m}}{\sqrt[6]{m}} = \sqrt[3]{m}.$$

Рассмотрим второй случай, при котором выполнены неравенства

$$\frac{P_{n+1}}{Q_{n+1}} > \frac{q}{p} > \frac{P_n}{Q_n}. \tag{7.9}$$

Тогда, переворачивая данное неравенство и учитывая утверждение леммы 5.3, получаем

$$\frac{Q_n}{P_n} - \frac{p}{q} < \frac{Q_n}{P_n} - \frac{Q_{n+1}}{P_{n+1}} = \frac{(-1)^{n+1}}{P_n P_{n+1}}. \tag{7.10}$$

Кроме того, из (7.9) следует неравенство $pP_{n+1} > qQ_{n+1}$ или

$$\frac{p}{Q_{n+1}} > \frac{q}{P_{n+1}}. \tag{7.11}$$

Теперь, учитывая (7.6), (7.10) и (7.11), получим

$$|pr - qs| = |pP_n - qQ_n| = qP_n\left|\frac{p}{q} - \frac{Q_n}{P_n}\right| < \frac{q}{P_{n+1}} =$$
$$= \sqrt{\frac{q}{P_{n+1}}}\sqrt{\frac{q}{P_{n+1}}} < \sqrt{\frac{q}{P_{n+1}}}\sqrt{\frac{p}{Q_{n+1}}} = \sqrt{\frac{m}{P_{n+1}Q_{n+1}}} <$$
$$< \frac{\sqrt{m}}{\sqrt[6]{m}} = \sqrt[3]{m}.$$

Лемма доказана. □

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 $x \geqslant \sqrt{4bm}$ и величина $k \geqslant 0$. Далее, используя оценку сверху на величину y, получаем

$$\begin{aligned}\left(\sqrt[3]{m}\right)^2 > y^2 = x^2 - 4bm = \\ = (pr + qs + \sqrt{4bm})(pr + qs - \sqrt{4bm}) \geqslant \\ \geqslant 2\sqrt{4bm}(pr + qs - \sqrt{4bm}) \geqslant 2\sqrt{4bm}(k - 1).\end{aligned}$$

Тогда выполнено

$$k < \frac{\left(\sqrt[3]{m}\right)^2}{2\sqrt{4bm}} + 1 = \frac{\sqrt[6]{m}}{4\sqrt{b}} + 1.$$

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[3], **то** определить
   $$p = \textbf{НОД}\left(m,\ \ x \pm \sqrt{v}\right)$$
   и завершить алгоритм.

[3]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** $k \geqslant D$, **то** вычислить новое значение d. В противном случае, вернуться на шаг 2.2.

3. Завершить алгоритм с уведомлением, что число m простое. □

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 $O\left(\sqrt[3]{m}\right)$.

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, точное число шагов является случайной величиной и зависит от используемых в алгоритме генераторов 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 [33]. Метод основывается на свойствах случайных отображений конечного множества в себя.

Пусть, как и ранее, m нечетное составное число, которое мы хотим разложить на множители. Фиксируем некоторый многочлен $f(x) \in \mathbb{Z}[x]$ с целыми коэффициентами, степени большей единицы. В свой работе Поллард предложил выбрать многочлен вида $f(x) = x^2 + 1$. Данный многочлен задает отображение кольца вычетов по модулю m в себя

$$f(x) \pmod m : \quad \mathbb{Z}_m \to \mathbb{Z}_m.$$

Выберем произвольный элемент x_0 кольца $\mathbb{Z}_m$ и рассмотрим его орбиту, порожденную многочленом $f(x)$, то есть последовательность элементов кольца, определенных соотношением

$$x_{n+1} = f(x_n) \pmod m, \quad n = 0,\ 1,\ \ldots.$$

Поскольку число элементов кольца $\mathbb{Z}_m$ конечно, то найдутся такие целые индексы τ и λ, что для всех индексов $n \geqslant \lambda$ будет выполнено сравнение

$$x_n \equiv x_{n+\tau} \pmod m. \tag{7.12}$$

Величина τ называется периодом (длиной цикла) последовательности $\{x_n\}_0^\infty$, а величина λ – длиной подхода к периоду.

Пусть p произвольный простой делитель числа m, тогда из сравнения (7.12) следует, что $x_n \equiv x_{n+\tau} \pmod p$ и многочлен $f(x)$ порождает последовательность вычетов кольца $\mathbb{Z}_p$, которая зациклится, то есть найдутся такие индексы $j > i$, что

$$x_j \equiv x_i \pmod p. \tag{7.13}$$

Последнее сравнение позволяет нам найти нетривиальный делитель числа m. Действительно, из (7.13) получаем, что $\mathbf{НОД}(m,\ x_j - x_i) = p$, если $x_j \neq x_i$. Таким образом, метод Полларда сводится к поиску таких индексов i, j, для которых выполнено сравнение (7.13).

Для поиска необходимых индексов i, j Поллард предложил использовать метод Флойда (Robert W Floyd) поиска циклов в последовательностях, а именно, вычислять две последовательности $\{x_n\}_0^\infty$ и $\{x_{2n}\}_0^\infty$ и находить простой делитель p проверкой условия

$$\mathbf{НОД}(m,\ z) > 1, \quad \text{где} \quad z \equiv (x_{2n} - x_n) \pmod m.$$

Искомый делитель будет найден в том случае, когда период последовательности $\{x_n \pmod p\}_0^\infty$ будет делить значение индекса n.

Исходя из геометрических соображений, данный метод часто называют ϱ-методом Полларда или методом Полларда-Флойда. Мы суммируем приведенные выше рассуждения в виде алгоритма.

Алгоритм 7.4 (ϱ-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 $p = \mathbf{НОД}(m,\ z - x \pmod m)$.
5. **Если** $p > 1$, **то** завершить работу, в противном случае вернуться на шаг 3. □

Оценка числа шагов данного алгоритма следует из оценки длины периода последовательности $\{x_n \pmod p\}_0^\infty$, и, в среднем, составит величину порядка $O(\sqrt{p}) \sim O(\sqrt[4]{m})$.

7.5 Метод Брента

Метод Полларда-Флойда выполняет вычисления до тех пор, пока не будет найден нетривиальный делитель числа m, при этом оценка среднего числа шагов алгоритма зависит от размера делителя p. В 1980 году в работе [14] Ричард Брент (Richard P. Brent) предложил использовать этот факт для реализации теста, который позволяет определить, есть ли у составного числа m небольшие простые делители.

Метод Брента является достаточно простой модификацией метода Полларда-Флойда и вычисляет лишь конечное число элементов последовательности

$$x_{n+1} = f(x_n) \pmod m, \quad n = 0,\ 1,\ \ldots.$$

для некоторого полинома $f(x) \in \mathbb{Z}[x]$

$$f(x) \pmod m : \quad \mathbb{Z}_m \to \mathbb{Z}_m.$$

Брент предложил искать совпадение элементов последовательности $\{x_n \pmod p\}_0$ путем проверки условия

$$x_n \equiv x_{2^k-1} \pmod p,$$

для всех индексов n таких, что $2^k \leqslant n < 2^{k+1}$, $k = 0,\ 1,\ \ldots$. Как и ранее, проверка выполняется путем вычисления

$$\mathbf{НОД}(m,\ z), \quad \text{где} \quad z \equiv x_n - x_{2^k-1} \pmod m.$$

Алгоритм 7.5 (Алгоритм Брента)

Вход: Целое составное число m и натуральное число $c \geqslant 1$.
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 $p = \mathbf{НОД}(m,\ z - x)$.
7. **Если** $m > p > 1$, **то** делитель найден и алгоритм завершает работу. В противном случае, вернуться на шаг 3. □

Параметр c определяет трудоемкость алгоритма – количество его шагов не превышает величины $B = 2^c$. Тогда можно ожидать, что алгоритм Брента сможет найти делитель p, не превосходящий величины $O(B^2)$.

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 трудоемкость разложения на множители.

7.6 $p-1$ метод Полларда

Один из первых подходов к разложению на множители чисел частного вида был предложен Джоном Поллардом в 1974 году работе [33]. Пусть m натуральное, нечетное, составное число, которое мы хотим разложить на множители и p некоторый простой делитель числа m, то есть $p|m$.

Пусть a натуральное число, тогда, согласно третьему утверждению леммы 2.3, $\operatorname{ord}_p a$ – показатель a по модулю p делит число $p-1$, то есть $\operatorname{ord}_p a|(p-1)$. Согласно малой теореме Ферма, см. теорему 2.7, выполнено сравнение $a^{p-1} \equiv 1 \pmod{p}$. Таким образом, для любого натурального k такого, что $\operatorname{ord}_p a|(p-1)|k$ выполнено

$$a^k \equiv \left(a^{\operatorname{ord}_p a}\right)^t \equiv 1 \pmod{p}, \quad \text{при} \quad k = t \operatorname{ord}_p a,$$

что равносильно $a^k - 1 \equiv 0 \pmod{p}$. Последнее условие позволяет заключить, что

$$p|\, \mathbf{НОД}\left(m,\ a^k - 1 \pmod{m}\right). \tag{7.14}$$

Для выбора числа k Поллардом была предложена следующая идея. Из основной теоремы арифметики, см. теорему 1.4, следует, что для числа $p-1$ существует разложение на простые множители

$$p-1=\prod_{i=1}^{s} p_i^{\alpha_i}, \quad s\in\mathbb{N},$$

где $p_1=2$, а остальные p_i нечетны и не превосходят некоторой величины b_p. Легко видеть, что $b_p\leqslant\frac{p-1}{2}$.

Выберем в качестве k произведение всех маленьких простых чисел

$$k=\prod_i p_i^{\alpha_i}, \quad \text{где} \quad p_i\leqslant B=\max_{p|m}\{b_p\}, \tag{7.15}$$

а величины α_i принимают достаточно большие значения. В этом случае выполнено $p-1|k$ и делитель p может быть найден из условия (7.14).

При разложении числа m на множители, нам неизвестно точное значение величины B. Исходя из тривиальной оценки сверху на величину b_p, можно считать, что $B\sim\sqrt[4]{m}$. Однако в этом случае величина B принимает очень большое значение и вычисление значения $a^k-1 \pmod m$ становится более трудоемким, чем поиск делителей числа m пробным делением.

На практике величина B выбирается почти произвольным образом, в зависимости от быстродействия вычислительного средства, реализующего алгоритм, например, $B=10^6$.

Собственно алгоритм факторизации реализуется в виде теста — если для некоторого делителя p числа m, при k удовлетворяющем (7.15), выполнено условие (7.14), то делитель будет найден. В противном случае, алгоритм завершит свою работу с уведомлением о неудаче.

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, не превосходящие величины B и определить величину $k=\prod_i p_i^{\alpha_i}$, где $p_i\leqslant B$, при некоторых натуральных значениях[4] величин α_i. Определить $i=0$.
2. Вычислить $i=i+1$, положить $a=p_i$ (при $i=1$ значение параметра a должно равняться 2).
3. **Если НОД** $(a,\ m)>1$, **то** завершить алгоритм с результатом $p=a$.

[4]На практике для нескольких маленьких простых, например 2, ..., 31, величины α_i принимают значения не превосходящие 10, для всех остальных простых – значения α_i равны единице.

4. Вычислить $p = \mathbf{НОД}\left(m,\ a^k - 1 \pmod m\right)$.
5. **Если** $m > p > 1$, **то** завершить алгоритм.
6. **Если** $i < c$, **то** вернуться на шаг 2. В противном случае, завершить алгоритм с уведомлением о неудаче. □

Введенная нами в алгоритме граница c задает количество перебираемых чисел a, для которых проверяется выполнение условия (7.14). При практической реализации алгоритма эта величина может принимать небольшие значения, например 10.

Как можно заметить, $p-1$ метод Поллада представляет собой аналог алгоритма пробного деления, изложенного нами ранее. Только в методе Полларда мы ищем перебором 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 предъявлен в явном виде.

7.7 $p+1$ метод Вильямса

Данный метод был предложен Хью Вильямсом (Hugh Williams) в 1982 году работе [43] 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

$$p \pm 1 = \prod_i p_i^{\alpha_i}, \tag{7.16}$$

где p_i маленькие простые числа. Другими словами, как и в методе Полларда, найдется небольшое натуральное число B, например $B = 10^6$. При этом все p_i, определяемые равенством (7.16), удовлетворяют условию $p_i < B$.

Ранее, в 6-й главе, мы ввели последовательности Люка. Напомним, что для двух целых взаимно простых чисел чисел a, b рекуррентной последовательностью Люка называется последовательность пар целых чисел U_n, V_n, определяемых равенствами (6.10)

$$U_{n+1} = aU_n - bU_{n-1}, \quad V_{n+1} = aV_n - bV_{n-1}, \quad n = 1, 2, \ \ldots$$

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 6.5 выполнено условие $U_{\Phi(p)} \equiv 0 \pmod{p}$.

Пусть k произвольное натуральное число такое, что $\Phi(p)|k$. Тогда из шестого утверждения леммы 6.3 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

$$p|\,\mathbf{НОД}\,(m,\ U_k)\,. \tag{7.17}$$

Для поиска нетривиального делителя p числа m можно предложить следующий алгоритм, основывающийся на проверке условия (7.17). Он основан на выборе случайной пары числе a, b и вычислении элемента последовательности Люка U_k при k, удовлетворяющем равенству

$$k = \prod_i p_i^{\alpha_i}, \quad \text{где} \quad p_i \leqslant B. \tag{7.18}$$

Алгоритм Вильямса 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 $p_i \leqslant B$, при некоторых натуральных значениях[5] величин α_i. Определить $i = 0$.
2. Вычислить $i = i + 1$, выбрать случайные, взаимно простые значения a, b и определить $D = a^2 - 4b$.
3. **Если** $p = \mathbf{НОД}\,(m,\ b) > 1$, **то** завершить алгоритм.
4. **Если** $p = \mathbf{НОД}\,(m,\ D) > 1$, **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** $p = \mathbf{НОД}\,(m,\ U_k) > 1$, **то** завершить алгоритм.

[5]Выбор натуральных значений α_i может быть произведен, аналогично $p-1$ методу Полларда, см. сноску на 156-й странице.

7. **Если** $i < c$, **то** вернуться на шаг 2. В противном случае, завершить алгоритм с уведомлением о неудаче. □

Как и в $p-1$ методе Полларда, нами введена граница c, которая задает количество перебираемых последовательностей Люка, для которых проверяется выполнение условия (7.17). 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 Вилльямса не используют, ограничиваясь более простым $p-1$ методом Полларда.

7.8 Второй этап: оптимизация алгоритмов Полларда и Вильямса

Предложенные нами ранее алгоритмы Полларда, алгоритм 7.6, и Вильямса, алгоритм 7.7, могут быть оптимизированы путем добавления второго этапа. Предположим, что некоторого простого делителя p разложение (7.16) имеет вид

$$p \pm 1 = q \cdot \prod_{i=1}^{s} p_i^{\alpha_i}, \quad \text{где} \quad p_i < B \quad \text{и} \quad B < q. \tag{7.19}$$

То есть в разложение чисел $p\pm1$ входит один простой делитель, превосходящий заданную нами границу B. В этом случае, мы можем реализовать второй этап указанных алгоритмов 7.6 и 7.7, который выполняется после пятого и шестого шага, соответственно.

При поиске простого делителя q мы будем считать, что он ограничен сверху некоторой величиной B_1, например, $B_1 = 10^8$. Перебирая все простые числа $q_1, \ \ldots, \ q_l$ на интервале $B \leqslant q_1 < q_2 < \cdots < q_l \leqslant B_1$, мы можем проверить, для метода Полларда, выполнимость условия

$$\mathbf{НОД}\left(m, \ \left(a^k\right)^{q_i} - 1 \pmod m\right) > 1,$$

где величина k определяется на первом этапе алгоритма. Если условие выполнено, то $p-1 | kq_i$ и мы найдем нетривиальный делитель числа m.

Аналогично, для метода Вильямса, нам надо проверять выполнимость условия

$$\mathbf{НОД}\,(m,\ U_{kq_i}) > 1.$$

В случае его выполнения, мы получаем, что $\Phi(p)|kq_i$ 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.

7.8.1 Разностная схема

Для снижения трудоемкости процедуры перебора, Полларда предложил использовать тот факт, что разности между двумя соседними простыми числами, принадлежащими интервалу $[B, B_1]$, принимают небольшие значения.

Пусть $q_1,\ \ldots,\ q_l$ все простые числа в интервале от B до B_1. Определим разности

$$r_{i+1} = q_{i+1} - q_i \quad \text{для всех} \quad i = 1,\ \ldots,\ l-1.$$

Обозначим $b \equiv a^k \pmod m$, тогда вычисление вычетов $\left(a^k\right)^{q_i} \equiv b^{q_i} \pmod m$ 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 (6.13), мы можем записать равенства

$$U_{kq_{i+1}} = \frac{1}{2}\left(U_{kq_i}V_{kr_i} + U_{kr_i}V_{kq_i}\right), \quad V_{kq_{i+1}} = \frac{1}{2}\left(V_{kq_i}V_{kr_i} + DU_{kq_i}U_{kr_i}\right),$$

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.

7.8.2 Метод согласования

Опишем другой подход к перебору всех простых чисел $q_1,\ \ldots,\ q_l$ в интервале от B до B_1. Этот подход основан на методе согласования[6].

Определим натуральное число $h = \lceil \sqrt{B_1} \rceil$, тогда любое простое число q из интервала $B \leqslant q \leqslant B_1$ может быть представлено в виде

$$q = uh + v, \quad \text{где} \quad u, v \in \mathbb{N}, \quad \left\lfloor \frac{B}{h} \right\rfloor \leqslant u < h, \quad v < h. \tag{7.20}$$

Применим полученное равенство к алгоритму Полларда. Пусть выполнено условие $p - 1 | kq$, 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

$$\textbf{НОД}\left(m,\ d^v - (b^h)^u \pmod m\right), \quad \text{где} \quad b \equiv a^k, d \equiv b^{-1} \pmod m,$$

при некоторых натуральных u, v.

Реализация второго этапа алгоритма может выглядеть следующим образом. Вначале вычисляются значения $\left(b^h\right)^u \pmod m$ для всех u, удовлетворяющих неравенствам (7.20). Вычисленные значения сохраняются в памяти ЭВМ. После этого для всех $v = 1,\ 2,\ \ldots,\ h$ вычисляются значения вычетов $d^v \pmod m$ и проверяется условие

$$1 < \textbf{НОД}\left(m,\ d^v - (b^h)^u \pmod m\right) < m.$$

Если оно выполнено, то нетривиальный делитель числа m найден.

Соотношение (7.20) может быть использовано и при реализации метода Вильямса. Действительно, следуя (7.17), мы используем тот факт, что $p | \textbf{НОД}\,(m,\ U_{kq})$, для некоторого простого q, удовлетворяющего равенству (7.20).

Воспользовавшись равенствами (6.13), мы можем записать

$$2U_{kq} = \left(U_{khu} V_{kv} + U_{kv} V_{khu}\right).$$

Таким образом, мы можем предварительно вычислить значения U_{khu}, V_{khu}, для всех u удовлетворяющих неравенствам (7.20), и сохранить их в

[6] В англоязычных публикациях этот метод, применительно к $p-1$ методу Полларда, принято называть «усложненным стандартным продолжением» – improved standard continuation.

памяти ЭВМ. После этого для всех $v = 1,\ 2,\ \ldots,\ h$ вычисляются значения элементов последовательности Люка U_{kv}, V_{kv} и проверяется условие

$$m > \mathbf{НОД}\,(m,\ U_{khu}V_{kv} + U_{kv}V_{khu}) > 1.$$

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 (7.20) равным не $h = \lceil\sqrt{B_1}\rceil$, а ближайшим к $\lceil\sqrt{B_1}\rceil$ целым числом, кратным[7] $2{\cdot}3{\cdot}5{\cdot}7 = 210$. При этом интервал для величины u принимает вид $\left\lfloor\frac{B}{h}\right\rfloor \leqslant u \leqslant \left\lceil\frac{B_1}{h}\right\rceil$. 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 δ_p отличны от нуля, то значение v может быть использовано. В противном случае вычисляется следующее значение.

7.8.3 Поиск пар простых чисел

Следующая идея, развивающая метод согласования, была предложена Питером Монтгомери (Peter Montgomery) в статье [30]. Пусть, как и в методе согласования, нам задано целое число h – ближайшее к $\lceil\sqrt{B_1}\rceil$ и кратное 210.

Простое число q из интервала $B \leqslant q \leqslant B_1$, которое нам необходимо определить, может быть представлено в виде (7.20). Кроме того, мы можем определить парное ему число q_1, удовлетворяющее равенствам

$$q = uh + v, \quad q_1 = uh - v, \quad \left\lfloor\frac{B}{h}\right\rfloor \leqslant u \leqslant \left\lceil\frac{B_1}{h}\right\rceil, \quad v < h. \tag{7.21}$$

Пусть выполнено условие $p - 1 | kq$ и $(a^k)^q \equiv 1 \pmod p$. Обозначим, как и ранее $b \equiv a^k \pmod m$, тогда

$$b^{(uh)^2} - b^{v^2} \equiv b^{v^2}\left(b^{(uh)^2 - v^2} - 1\right) \equiv b^{v^2}\left(b^{(uh-v)(uh+v)} - 1\right) \equiv$$
$$\equiv b^{v^2}\left((b^q)^{q_1} - 1\right) \equiv 0 \pmod p. \tag{7.22}$$

[7] Достаточно очевидно, что при реализации алгоритма мы можем использовать и другие значения, например, $30 = 2 \cdot 3 \cdot 5$ или $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

Таким образом, сравнение (7.22) позволяет нам найти нетривиальный делитель числа m путем проверки условия

$$m > \mathbf{НОД}\left(m,\ b^{(uh)^2} - b^{v^2} \pmod m\right) > 1. \tag{7.23}$$

Второй этап реализуется следующим образом. Вначале, по заданной таблице простых чисел, строится множество пар u, v, удовлетворяющих условиям (7.21). 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 (7.23): сперва мы фиксируем значение u и перебираем все допустимые значения v. После чего переходим к следующему значений u.

Для уменьшения трудоемкости вычисления величин $b^{(hu)^2} \pmod m$ для всех u, последовательно пробегающих интервал $\left\lfloor \frac{B}{h} \right\rfloor \leqslant u \leqslant \left\lceil \frac{B_1}{h} \right\rceil$, можно воспользоваться следующим сравнением

$$b^{(h(u+1))^2} \equiv b^{(hu)^2} \cdot \left(b^{hu}\right)^2 \cdot b^h \pmod m,$$

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 (7.22), подход, основанный на переборе пар простых чисел, практически не применим при реализации метода Вильямса, и используется только для оптимизации $p-1$ метода Полларда.

7.8.4 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 $B \leqslant q \leqslant B_1$ и $b^k \equiv 1 \pmod p$.

Рассмотрим псевдослучайную последовательность элементов

$$b_{i+1} \equiv b_i^{s_i} \pmod m, \quad s_i \equiv b_i \pmod M, \quad i = 0,\ 1,\ \ldots,$$

где $b_0 = b$, а M некоторая маленькая константа, например 16.

Если мы рассмотрим каждый элемент этой последовательности по модулю некоторого простого числа p, являющего делителем числа m, то данная последовательность зациклится. Для поиска цикла мы можем использовать метод Флойда, то есть искать пару значений

$$b_i \equiv b_{2i} \pmod{p} \tag{7.24}$$

для некоторого индекса i. Последнее сравнение равносильно тому, что

$$p | \mathbf{НОД}(m,\ b_i - b_{2i} \pmod{m}). \tag{7.25}$$

Поскольку нам неизвестно точное значение простого числа q, то мы не можем определить мощность множества $\{b,\ b^2,\ \ldots,\ b^q \equiv 1 \pmod{p}\}$. Поэтому мы будем проверять выполнение условия (7.25) для всех индексов i от 1 до $\lceil\sqrt{B_1}\rceil$. Такая оценка сверху очевидным образом следует из свойств псевдослучайных последовательностей.

Данный подход может быть достаточно просто перенесен на алгоритм Вильямса. Определим множество $U_{kB},\ U_{k(B+1)},\ \ldots,\ U_{kB_1}$ элементов последовательности Люка, которому принадлежит элемент U_{kq} для некоторого простого числа q такого, что $B \leqslant q \leqslant B_1$ и $p | \mathbf{НОД}(m,\ U_{kq})$.

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 $B \leqslant s < B_1$. В этом случае условие (7.25) принимает вид

$$p | \mathbf{НОД}(m,\ U_i - U_{2i} \pmod{m}), \tag{7.26}$$

для некоторого индекса i, которое может быть проверено для всех индексов, не превосходящих $\lceil\sqrt{B_1}\rceil$.

7.9 Метод Женга

В 2001 году в статье [45] Женьксианъ Женг (Zhenxiang Zhang) опубликовал алгоритм, который позволяет, при некоторых дополнительных условиях, эффективно раскладывать на множители составные числа, используемые в схеме RSA. 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 $0 < r \leqslant \frac{p-3}{2}$.*

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*

$$p = \mathbf{НОД}\left(m,\ b^{m+r} - 1 \pmod m\right). \tag{7.27}$$

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

$$\begin{cases} (x^{m+r} - 1) \equiv 0 \pmod p, \\ (x^{m+r} - 1) \equiv 0 \pmod q. \end{cases} \tag{7.28}$$

Количество решений первого сравнения приведенной системы, согласно теореме 2.10, равно

$$\mathbf{НОД}\,(m + r,\ p - 1) = \mathbf{НОД}\,(s(p-1),\ p - 1) = p - 1.$$

Учитывая, что $q - 1 = s(p-1) - (r+1)$ получаем,

$$\begin{aligned} \mathbf{НОД}\,(m + r,\ q - 1) &= \mathbf{НОД}\,(s(p-1),\ s(p-1) - (r+1)) = \\ &= \mathbf{НОД}\,(s(p-1),\ r+1) < r + 1 \leqslant \frac{p-1}{2} < \frac{q-1}{2}. \end{aligned}$$

Таким образом, число решений системы (7.28) и, соответственно, мощность множества M, оценивается величиной

$$\mathbf{НОД}\,(m - r,\ p - 1)\,\mathbf{НОД}\,(m - r,\ q - 1) < \frac{(p-1)(q-1)}{2} = \frac{\varphi(m)}{2}.$$

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

$$b^{m+r} \equiv (b^p)^q b^r \equiv b^q b^r \equiv b^{s(p-1)-r} b^r \equiv b^{-r} b^r \equiv 1 \pmod p.$$

Таким образом, $p \mid (b^{m+r} - 1) \pmod m$. Последнее утверждение завершает доказательство леммы. □

Метод применения данной леммы для разложения числа m на множители 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 $\mathbf{НОД}(m,\ b^{m+r} - 1 \pmod m) = p$ при некотором значении r. Для его поиска необходимо перебрать все значения, удовлетворяющие неравенству $0 < r \leqslant \frac{p-3}{2}$.

В общем случае, мы получаем трудоемкость сравнимую с трудоемкостью тотального перебора. Однако при малых значениях величины r алгоритм может 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. Более того, мы будем рассматривать его как еще один вариант второго этапа метода Полларда, см. раздел 7.8.

Пусть $k = \prod_i p_i^{\alpha_i}$ – произведение маленьких простых чисел p_i, не превосходящих некоторой заранее заданной границы B. Пусть выполнены условия

$$p - 1 = ud, \quad k = ut, \quad d, u, t \in \mathbb{N}, \tag{7.29}$$

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

$$q = s(p-1) - r, \quad q = ld - z, \quad 0 < r \leqslant \frac{p-3}{2}, \quad 0 \leqslant z < d. \tag{7.30}$$

Теперь мы можем записать сравнение

$$(a^k)^m \equiv (a)^{kq} \equiv a^{kld}(a^k)^{-z} \equiv a^{utld}(a^k)^{-z} \equiv$$
$$\equiv (a^{p-1})^{lt}(a^k)^{-z} \equiv (a^k)^{-z} \pmod p,$$

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 (7.27), а именно

$$p = \mathbf{НОД}\left(m,\ (a^k)^{m+z} - 1 \pmod{m}\right). \tag{7.31}$$

Полученное равенство существенно снижает границу для перебора значений z, поскольку $0 \leqslant z < d$. 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 $d|m+z$. Это действительно так, поскольку из (7.30) следует равенство

$$m + z = p(ld - z) + z = dlp - (p-1)z = d(lp - uz).$$

Обозначим $\xi = \mathbf{НОД}\,(l,\ u) = \mathbf{НОД}\left(l,\ \frac{p-1}{d}\right)$, 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 ξ нам неизвестна, однако если она невелика, то есть величина l имеет маленькие простые делители, мы можем искать возможные значения неизвестной z в арифметических прогрессиях

$$z \equiv -m \pmod{\xi}, \quad \xi = 2,\ 3,\ 5,\ \ldots.$$

7.10 Метод Макки

В 1999 году в работе [26] Джеймс Макки (James McKee) доказал следующий результат.

Лемма 7.4 (Лемма Макки)**.** *Пусть m нечетное составное число, для которого выполнено $m = pq$ и $2\sqrt[4]{m} < p < q$. Определим $h = \lfloor \sqrt{m} \rfloor$ и выберем произвольное натуральное число $c \geqslant 1$. Тогда найдется c наборов натуральных чисел k, x, y, v, удовлетворяющих условиям*

$$x^2 - y^2 = mv^2, \quad \textit{где} \quad x = hv + k, \tag{7.32}$$

а также выполнены следующие условия.

1. *Величина v четна и удовлетворяет неравенствам*

$$2 \leqslant v \leqslant \sqrt[4]{m} + 2(c-1).$$

2. *Выполнено неравенство $|y| < c^2\sqrt{m}$.*

3. *Выполнены неравенства $0 < kv < c^4\sqrt{m}$.*

4. *Выполнено условие $1 < \mathbf{НОД}\,(x+y,\ m) < m$.*

Доказательство. Пусть ξ произвольное целое, отличное от нуля число. Определим значения x, y и v равенствами

$$x = q + \xi^2 p, \quad y = q - \xi^2 p, \quad v = 2\xi, \tag{7.33}$$

тогда для k выполнено $k = x - hv = q + \xi^2 p - 2h\xi$, а также выполнено равенство (7.32). Действительно,

$$x^2 - y^2 = (q + \xi^2 p)^2 - (q - \xi^2 p)^2 = 4\xi^2 pq = mv^2.$$

Таким образом, равенство (7.32) выполнено для любого целого ξ и величин x, y и v, определенных равенствами (7.33).

Поскольку значения x, y не зависят от знака ξ, мы ограничимся только положительными значениями ξ и покажем, что найдется c значений ξ, для которых выполнены утверждения леммы.

Рассмотрим величину $r = \left\lfloor \sqrt{\frac{q}{p}} \right\rfloor$ и определим величины ξ равенствами

$$\xi = r + i, \quad \text{для} \quad i = 0,\ 1,\ \ldots,\ c-1. \tag{7.34}$$

Поскольку выполнены ограничения $2\sqrt[4]{m} < p < q$, то мы получаем неравенство

$$1 \leqslant r \leqslant \sqrt{\frac{q}{p}} < \sqrt{\frac{m^{\frac{3}{4}}}{4m^{\frac{1}{4}}}} = \frac{\sqrt[4]{m}}{2}, \tag{7.35}$$

из которого вытекает оценка $2 \leqslant v = 2\xi < \sqrt[4]{m} + 2(c-1)$ и первое утверждение леммы.

Получим оценки для величины y, которая может принимать как положительные, так и отрицательные значения. Действительно, учитывая (7.34) и (7.35), получаем, что при $i = 0$ выполнено неравенство $\xi^2 \leqslant \frac{q}{p}$ и $y = q - \xi^2 p \geqslant 0$. В остальных случаях, при $i > 0$, получаем $\xi^2 > \frac{q}{p}$ и $y = q - \xi^2 p < 0$. В обоих случаях выполнено неравенство

$$y = q - \xi^2 p \geqslant q - p\left(\sqrt{\frac{q}{p}} + i\right)^2 = -\left(2i\sqrt{m} + pi^2\right).$$

Следовательно, учитывая интервал возможных значений для i, получаем неравенство

$$|y| \leqslant 2i\sqrt{m} + pi^2 < \sqrt{m}(1 + 2i + i^2) \leqslant c^2\sqrt{m},$$

из которого следует второе утверждение леммы.

Для доказательства третьего утверждения леммы заметим, что

$$k = x - hv = q + \xi^2 p - 2h\xi = \left(\sqrt{q} - \xi\sqrt{p}\right)^2 + 2\xi(\sqrt{m} - h) > 0. \quad (7.36)$$

Последнее неравенство верно, поскольку ξ положительно и $\sqrt{m} \geqslant h$, следовательно, k является суммой двух положительных величин.

Предположим, что $k \leqslant v$ тогда, учитывая первое утверждение леммы, получаем

$$kv \leqslant v^2 \leqslant \left(\sqrt[4]{m} + 2(c-1)\right)^2 < c^4\sqrt{m}.$$

Запишем равенство (7.32) в виде

$$mv^2 + y^2 = x^2 = (k + hv)^2 = k^2 + 2hkv + h^2v^2 \quad (7.37)$$

и рассмотрим случай $k > v$. Поскольку $h + \frac{k^2}{v^2} > h + 1 > m$, то выполнено неравенство $hv^2 + k^2 > mv^2$. Тогда, из (7.37), следует неравенство

$$kv = \frac{1}{2h}\left(y^2 + mv^2 - h^2v^2 - k^2\right) < \frac{y^2}{2h} < c^4\sqrt{m},$$

которое завершает доказательство третьего утверждения леммы.

Последнее утверждение леммы следует из равенств (7.33). Поскольку $x + y = 2q$ и m нечетно, получаем равенство $q = \mathbf{НОД}(x + y,\ m)$, которое позволяет нам найти нетривиальный делитель числа m. □

Утверждение доказанной леммы может быть использовано для разложения числа m на множители с помощью алгоритма, аналогичного алгоритмам Ферма или Лемана. В качестве упражнения читателю предлагается разработать данный алгоритм и показать, что его трудоемкость не меньше, чем у метода Лемана.

Для уменьшения трудоемкости перебора можно воспользоваться равенством (7.36). Обозначим

$$\lambda = \sqrt{q} - \xi\sqrt{p}, \quad \mu = \sqrt{\frac{q}{p}},$$

тогда

$$\sqrt{p} = \frac{\lambda}{\mu - \xi}, \quad \sqrt{q} = \frac{\lambda\mu}{\mu - \xi}, \quad \sqrt{m} = \frac{\lambda^2\mu}{(\mu - \xi)^2}.$$

Последнее равенство позволяет нам записать $\lambda^2 = \frac{(\mu-\xi)^2}{\mu}\sqrt{m}$. Тогда, из (7.36), получаем выражение

$$k = \frac{(\mu-\xi)^2}{\mu}\sqrt{m} + 2\xi(\sqrt{m} - h),$$

где $\xi = \lfloor\mu\rfloor + i$, $i = 0, 1\ \ldots, c-1$. Мы получили точное значение величины k в зависимости от величины μ и, тем самым, определили область перебора возможных значений k. К сожалению, на практике точное значение величины μ бывает известно не всегда.

В своей работе [26] Макки предложил отличный от описанного выше способ поиска величин k и v, основанный на вычислении наилучших приближений для рациональных чисел. Запишем равенство (7.32) в виде

$$y^2 = x^2 - mv^2 = (hv + k)^2 - mv^2 \tag{7.38}$$

для натуральных чисел k, v, удовлетворяющих условиям леммы 7.4.

Пусть $z \leqslant y$ – некоторый делитель числа y такой, что выполнены неравенства $z > v$ и $z^2 \geqslant 2kv$.

Предположим, что v делит z, тогда $v|y$, кроме того, из равенства $x^2 = y^2 + mv^2$ следует, что $v|x$. Используя обозначения, введенные при доказательстве леммы 7.4, запишем $v = 2\xi$, тогда $2\xi = v|(x + y) = 2q$, следовательно, $\xi|q$ и $\xi|m$. Мы получили, что величина ξ является делителем числа m и $\xi \leqslant \frac{\sqrt[4]{m}}{2} + (c - 1)$. С другой стороны, число m не имеет делителей, меньших, чем $2\sqrt[4]{m}$. Таким образом, при $c \leqslant \frac{3}{2}\sqrt[4]{m}$ величина v не делит z.

Далее из равенства (7.38) получаем, что $z^2|(hv+k)^2-mv^2$. Последнее условие равносильно сравнению

$$(hv + k)^2 \equiv mv^2 \pmod{z^2}.$$

Поскольку $\mathbf{НОД}(v,\ z) = 1$, то последнее сравнение равносильно

$$\left(h + \frac{k}{v}\right)^2 \equiv m \pmod{z^2}.$$

Мы получили, что числа k, v, удовлетворяющие равенству (7.38), связаны соотношением $k = k_0 v - lz^2$, где величина l является целым числом, удовлетворяющим неравенству $l > 0$, а k_0 является решением сравнения $(h + x)^2 \equiv m \pmod{z^2}$.

Предположим, что $l = 0$, тогда $k = k_0 v$ и величина v делит k. Таким образом, из равенства (7.38) следует, что $v|y$. Аналогично предыдущим

рассуждениям получаем, что $v|x$ и $\xi = \frac{v}{2}$ делит m, то есть противоречие условию леммы 7.4. Далее предположим, что выполнено неравенство $l < 0$, тогда

$$k = k_0 v - lz^2 = k_0 v + |l|z^2 \geqslant |l|z^2 \geqslant 2|l|kv \geqslant 4|l|k \quad \text{или} \quad |l| \leqslant \frac{1}{4}.$$

Поскольку l целое число, то последнее неравенство влечет за собой равенство $l = 0$, которое противоречит нашему предположению. Получаем

$$k = k_0 v - lz^2, \quad l > 0.$$

Поскольку $z^2 > 2kv$, то выполнено неравенство $\frac{1}{2v} > \frac{k}{z^2}$. Учитывая, что $k = k_0 v - lz^2 > 0$, получаем

$$\frac{1}{2v^2} > \frac{k}{z^2 v} = \frac{k_0 v - lz^2}{z^2 v} = \frac{k_0}{z^2} - \frac{l}{v} > 0.$$

Таким образом, согласно теореме 5.5, дробь $\frac{l}{v}$ является наилучшим приближением к величине $\frac{k_0}{z^2}$.

Воспользовавшись утверждением теоремы 5.4 мы получим, что дробь $\frac{l}{v}$ является подходящей дробью и может быть вычислена при помощи соотношений (5.6).

Алгоритм, предложенный Макки, состоял из следующей последовательности действий.

1. Фиксировать значение величины c, например, $c = \lceil \log_2 m \rceil$.

2. Выбрать случайное, простое число z, удовлетворяющее условиям $2c^2 \sqrt[4]{m} < z < c\sqrt{m}$ и $\left(\frac{m}{z}\right) = 1$.

3. Используя алгоритм Тонелли-Шенкса, алгоритм 4.2, и подъем решения, см. теорему 3.5, вычислить вычет k_0, который удовлетворяет сравнению $(h + x)^2 \equiv m \pmod{z^2}$.

4. Используя соотношения (5.6), вычислить все подходящие дроби $\frac{P_n}{Q_n}$ к величине $\frac{k_0}{z^2}$.

5. Для каждой дроби определить

$$v = Q_n, \quad k = k_0 v - P_n z^2, \quad x = hv + k, \quad t = x^2 - mv^2.$$

6. Если t является полным квадратом, вычислить $y = \sqrt{t}$ и определить q – делитель числа m равенством $q = \mathbf{НОД}(m,\ x + y)$.

7. Если для всех подходящих дробей делитель q не найден, то выбрать новое значение величины z.

Глава 8

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 эффективное методы разложения целого, составного нечетного числа m на множители. Описываемый нами класс методов имеет субъэкспоненциальную 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*

$$x^2 \equiv y^2 \pmod m, \tag{8.1}$$

тогда будет выполнено условие $1 < \mathbf{НОД}(x-y,\ m) < m$.

Доказательство. Согласно основной теореме арифметики, представим m в виде $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, где $p_1, \ldots, p_n$ различные нечетные простые числа, $\alpha_1,\ \ldots, \alpha_n$ 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 $\mathbf{НОД}(x-y,\ m) = 1$. Тогда, согласно лемме 1.4, выполнено $p_i^{\alpha_i} | x+y$ для любого индекса $i = 1,\ \ldots,\ n$. Следовательно, $m|(x+y)$, что равносильно сравнению $x \equiv -y \pmod m$. Последнее сравнение противоречит условию леммы.

Теперь предположим, что выполнено условие $\mathbf{НОД}(x-y,\ m) = m$. Аналогичными рассуждениями получаем, что $m|(x-y)$, то есть сравнение $x \equiv y \pmod m$ и противоречие условиям леммы. Таким образом, величина $\mathbf{НОД}(x-y,\ m)$ не превосходит m и не равна 1 или m. Лемма доказана. □

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 (7.32) являются частным случаем сравнения (8.1).

8.1 Метод Крайчика

Еще в докомпьютерную эпоху, в 1926 году в монографии [23] Морис Крайчик[1] 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

$$\begin{aligned} 1081 - 81 &= 1000, \\ 1081 - 960 &= 121, \\ 1081 - 720 &= 361, \\ 1089 - 1081 &= 8, \\ 1156 - 1081 &= 75. \end{aligned}$$

[1]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 $\mathbf{НОД}(893,\ 1081) = 47$. 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 [25] 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 α_0 – корень многочлена $f(x)$, удовлетворяющий неравенству $\alpha_0 > 1$, и разложим α_0 в непрерывную дробь

$$\alpha_0 = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{\alpha_n}}}},$$

где $a_n = \lfloor \alpha_n \rfloor$ и $\alpha_n = \dfrac{A_n + \sqrt{D}}{B_n}$, $n = 0,\ 1,\ \ldots$, 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

$$A_{n+1}^2 \equiv -B_n B_{n+1} \pmod{m}, \quad n = 0,\ 1,\ \ldots. \tag{8.3}$$

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 $n \geqslant n_0$, квадратичная иррациональность α_n будет приведенной, см. определение на стр. 98. Тогда, согласно лемме 5.7, для величин A_n, B_n будут выполнены неравенства

$$0 < A_n < \sqrt{D}, \quad 0 < B_n < 2\sqrt{D}. \tag{8.4}$$

Вычисляя последовательно полные частные $\alpha_1,\ \alpha_2,\ \ldots$ мы будем получать сравнения (8.3) для $n = 0,\ 1,\ \ldots$. 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 α_0 положительный корень многочлена $f(x)$, то есть $\alpha_0 = \dfrac{-5 + \sqrt{1081}}{22}$. 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

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{21 + \sqrt{1081}}{40},\ a_2 = 1,\ A_2 = 21,\ B_2 = 40,$$
$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{19 + \sqrt{1081}}{18},\ a_3 = 2,\ A_3 = 19,\ B_3 = 18,$$
$$\alpha_4 = \frac{1}{\alpha_3 - a_3} = \frac{17 + \sqrt{1081}}{44},\ a_4 = 1,\ A_4 = 17,\ B_4 = 44.$$

Теперь запишем сравнения (8.3) для $n = 0,\ 1,\ 2,\ 3$.

$$\begin{aligned} -2^5 \cdot 11 &\equiv 3^6 \pmod{1081}, \\ -2^7 \cdot 5 &\equiv 3^2 \cdot 7^2 \pmod{1081}, \\ -2^4 \cdot 3^3 \cdot 5 &\equiv 19^2 \pmod{1081}, \\ -2^3 \cdot 3^2 \cdot 11 &\equiv 17^2 \pmod{1081}. \end{aligned} \tag{8.5}$$

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, $\mathbf{НОД}\,(176 - 153,\ 1081) = 23$. 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, $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ – квадратичная иррациональность, раскладываемая в непрерывную дробь, и $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n,\ \ldots$ последовательность полных частных.

Рассмотрим последовательность подходящих дробей $\dfrac{P_n}{Q_n}$ к α_0 для всех индексов $n = 0,\ 1,\ \ldots$. 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 5.3, верно равенство (5.30)

$$\left(P_nB_0 - Q_nA_0\right)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1},$$

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

$$\left(P_nB_0 - Q_nA_0\right)^2 \equiv (-1)^{n+1} B_0 B_{n+1} \pmod{m}. \tag{8.6}$$

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 периодично, см. теорему 5.2. Поэтому количество соотношений, которые можно получить с помощью данного метода, ограниченно, и их может оказаться недостаточно для набора соотношений и построения сравнения (8.1).

В той же работе [25] Лемер и Пауерс 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 [31], Майкл Моррисон и Джон Бриллхарт (Michael A. Morrison & John Brillhart) предложили свой алгоритм, являющийся модификацией 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 $p \leqslant B$.*
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 при проведении анализа трудоемкости метода Моррисона-Бриллхарта.

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

$$v = (-1)^{\gamma_0} \prod_{i=1}^{s-1} p_i^{\gamma_i}, \quad p_i \in \mathcal{B}_B, \quad \gamma_i \in \mathbb{N}, \tag{8.7}$$

и величина s определяет количество элементов в факторной базе, сопоставим вектора

$$\overline{\gamma} = (\gamma_0,\ \ldots,\ \gamma_{s-1}), \tag{8.8}$$

$$\overline{e} = (e_0,\ e_1,\ \ldots,\ e_{s-1}), \quad \text{где} \quad e_i \equiv \gamma_i \pmod{2}. \tag{8.9}$$

Вектор $\overline{e}$ 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

$$u_i^2 \equiv v_i \pmod{m}, \quad i = 0,\ \ldots,\ r-1, \tag{8.10}$$

правые части которых удовлетворяют равенству (8.7). Каждому сравнению будут соответствовать свои вектора $\overline{\gamma}_i$ и $\overline{e}_i$ вида (8.9).

Образуем из векторов $\overline{e}_i$ 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 $\overline{\gamma}_i$ образуем матрицу Г.

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 [5], 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.

Поскольку мы будем модифицировать матрицу Γ и найденные нами сравнения одновременно с изменением матрицы E, то при получении нулевой строки, соответствующее ей сравнение будет иметь искомый вид $x^2 \equiv y^2 \pmod{m}$.

Алгоритм 8.1 (Алгоритм гауссового исключения)

Вход: Матрицы $\mathrm{E} = (e_{i,j})$ и $\Gamma = (\gamma_{i,j})$ размера $r \times s$ при $r > s$, а также сравнения (8.10), заданные в виде двух векторов $\left(u_0^2,\ \ldots,\ u_{r-1}^2\right)$ и $(v_0,\ \ldots,\ v_{r-1})$.
Выход: Сравнение вида $x^2 \equiv y^2 \pmod{m}$.

1. **Для всех** i **от** 0 **до** $s-1$ **выполнить**

   1.1. Перебирая $j = 0,\ 1, \ldots$, найти номер строки у 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

$$(e_{l,0},\ \ldots,\ e_{l,s-1}) = (e_{j,0} + e_{l,0} \pmod 2,\ \ldots,\ e_{j,s-1} + e_{l,s-1} \pmod 2)$$
$$u_l^2 = u_l^2 \cdot u_j^2 \pmod m, \quad v_l = v_l \cdot v_j \pmod m,$$
$$(\gamma_{l,0},\ \ldots,\ \gamma_{l,s-1}) = (\gamma_{i,0} + \gamma_{l,0},\ \ldots,\ \gamma_{i,s-1} + \gamma_{l,s-1}).$$

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

$$y \equiv \prod_{j=1}^{s-1} p_j^{\frac{\gamma_{i,j}}{2}} \pmod m, \quad p_j \in \mathcal{B}_B.$$

□

Прежде чем рассмотреть пример, полностью иллюстрирующий алгоритм разложения на множители, нам необходимо определить способ выбора величины k, определяющей значение дискриминанта $D = km$.

8.2.4 Как выбрать множитель k

Еще Крайчик в [23] 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 Schroeppel) в конце 70-х годов прошлого столетия. Результаты Шрёппеля были опубликованы в 1981 году Дональдом Кнутом (Donald E. Knuth) во втором издании его монографии «Искусство программирования», см. [22, 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.

Пусть мы нашли сравнение $u^2 \equiv v \pmod{D}$ и абсолютное значение правой части не превосходит $2\sqrt{D}$. Мы всегда можем записать равенство

$$|v| = t \cdot \prod_{i=1}^{s-1} p_i^{\gamma_i}, \quad \gamma_i \geqslant 0, \quad p_i \in \mathcal{B}_B, \tag{8.11}$$

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[2] делятся на p, где

$$N_1 = 2\sqrt{D}\left(\frac{1}{p} - \frac{1}{p^2} - \frac{1}{p^3} - \cdots - \frac{1}{p^{n-1}}\right)$$

для некоторого натурального n такого, что $p^n > 2\sqrt{D}$. Обобщая, мы можем записать, что мощность множества чисел, не превосходящих ве-

[2]Напомним, что число v в точности делится на p, если p делит v, а p^2 уже не делит v.

личины $2\sqrt{D}$ и в точности делящихся на p^i, составляет

$$N_i = 2\sqrt{D}\left(\frac{1}{p^i} - \sum_{j=i+1}^{n-1}\frac{1}{p^j}\right), \quad i = 1,\ \ldots, n-2, \tag{8.12}$$

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

$$p^{\beta_p} = p^{\frac{1}{2\sqrt{D}}(N_1+2N_2+\cdots+(n-1)N_{n-1})}.$$

Суммируя значения сумм (8.12) с соответствующими множителями, получим выражение для β_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

$$\beta_p = \frac{1}{p} + \frac{1}{p^2} - \frac{2}{p^4} - \frac{5}{p^5} - \cdots. \tag{8.13}$$

Таким образом, мы будем считать, что простое число p входит в разложение целого числа $v \in [1, 2\sqrt{D})$, в среднем, в степени β_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

$$pu_1^2 \equiv p^{e-1}v_1 \pmod{k_1 m}, \tag{8.14}$$

где $u = u_1 p$, $v = v_1 p^e$ и $k = k_1 p$. 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 Δ. Случаи, 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 β_{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 [39] 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 α_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

$$b^2 - 4ac = D = \begin{cases} km, & \text{если} \quad k \equiv m \pmod 4, \\ 4km, & \text{иначе.} \end{cases}$$

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 $D = km \equiv (2\delta + 1)^2 \equiv 4\delta^2 + 4\delta + 1 \equiv 1 \pmod 4$.

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 Пауэрса, так и в алгоритме Моррисона и Брилхарта.

Мы рассмотрим общий случай и, для начала, построим многочлен $f(x) = x^2 + bx + c$ со старшим коэффициентом равным единице. Если выполнено условие $D \equiv 1 \pmod 4$ или, что равносильно, $D = km$, то выберем в качестве параметра b любое нечетное число, удовлетворяющее неравенству $b < \sqrt{km} - 2$. Тогда $b^2 \equiv D \equiv 1 \pmod 4$ и мы можем определить величину $c = \frac{b^2 - D}{4}$. В силу ограничения сверху на величину b мы получаем, что корень $\alpha_0 = \frac{-b + \sqrt{km}}{2}$ положителен и $\alpha_0 > 1$.

Если выполнено условие $D \equiv 0 \pmod 4$, то определим $b = 2b_1$, где b_1 любое целое число, удовлетворяющее неравенству $b_1 < \sqrt{km} - 1$. Параметр c определим равенством $c = b_1^2 - km$. Тогда выполнено

$$\alpha_0 = \frac{-b + \sqrt{4km}}{2} = -b_1 + \sqrt{km} > 1. \tag{8.15}$$

Отметим, что непрерывная дробь квадратичной иррациональности (8.15) отличается от непрерывной дроби квадратичной иррациональности $\sqrt{km}$ только в значении неполного частного a_0.

Теперь построим многочлен произвольного вида $f(x) = ax^2 + bx + c$. В качестве параметра a выберем произвольное нечетное простое число из факторной базы. Так же как и ранее, рассмотрим два случая.

Если выполнено сравнение $D \equiv 1 \pmod 4$ или, что равносильно, $km = D = b^2 - 4ac$. Рассмотрим сравнение $km \equiv b^2 \pmod a$, которое, в силу выбора параметра a, будет разрешимо относительно неизвестного b. Используя алгоритм Тонелли-Шенкса, см. алгоритм 4.2, мы можем найти два возможных значения величины b. Выбирая нечетное значение, получим, что найденное значение b удовлетворяет сравнению $D \equiv b^2 \pmod{4a}$. Следовательно, мы можем определить величину 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 $\sqrt{km} > 2a + b$. Последнее неравенство может быть заменено более жестким условием $0 < a < \frac{\sqrt{km}}{3}$.

Если выполнено сравнение $D \equiv 0 \pmod 4$, то $4km = D = b^2 - 4ac$. Будем считать, что величина $b = 2b_1$, тогда, в силу выбора параметра a, сравнение $km \equiv b_1^2 \pmod a$ разрешимо относительно неизвестного b_1. Используя алгоритм Тонелли-Шенкса, мы можем найти два значения величины b_1, каждое из которых позволит определить $c = \frac{b_1^2-km}{a}$. 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 Заключение

Кратко суммируем вышеизложенное: метод непрерывных дробей развивает идеи, предложенные Крайчиком, и состоит из следующей последовательности шагов.

1. Выбрать значение $B > 0$ и, воспользовавшись функцией Кнута-Шрёппеля, определить множитель k и факторную базу $\mathcal{B}_B$.

2. Построить многочлен второй степени $f(x) \in \mathbb{Z}[x]$, положительный корень которого α_0 удовлетворяет неравенству $\alpha_0 > 1$.

3. Разложить α_0 в непрерывную дробь и, используя сравнения (8.3) или (8.6), получить множество сравнений вида $u^2 \equiv v \pmod m$.

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 можно использовать, например, алгоритмы, изложенные в предыдущей главе.

5. Согласно описанию раздела 8.2.3, построить матрицы E и Г. Применяя алгоритм гауссового исключения, алгоритм 8.1, построить сравнение $x^2 \equiv y^2 \pmod{m}$.

6. Используя утверждение леммы 8.1, найти нетривиальный делитель числа m.

Предложенная последовательность шагов является общей схемой, которой в дальнейшем придерживалось большинство алгоритмов разложения на множители. Основное различие заключалось в процедуре генерации соотношений $u^2 \equiv v \pmod{m}$.

Проверка разложимости правой части на простые сомножители, принадлежащие факторной базе $\mathcal{B}_B$, может проводиться различными способами, например, простым делением. Более эффективным является применение алгоритмов Брента, $p-1$ метода Полларда или $p+1$ метода Вильямса. Однако самый эффективный способ заключается в использовании алгоритмов решета, которые мы опишем в следующих разделах.

8.3 Метод линейного решета

В конце 70-х годов прошлого столетия Рихард Шрёппель (Richard Schroeppel) 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 [35].

Обозначим, как и ранее, $h = \lfloor \sqrt{m} \rfloor$. Зафиксируем действительное число ε, 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

$$\prod_{i,j} t(a_i, b_j) \equiv \prod_{i,j} s(a_i, b_j) \pmod{m}. \tag{8.16}$$

Левая часть сравнения (8.16) будет полным квадратом, если каждая из величин a_i, b_j входит в произведение четное число раз. Предположим, что правая часть в сравнении (8.16) 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 Δ целое число, являющееся полным квадратом. В этом случае сравнение (8.16) 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

$$\begin{aligned} s(a + kp, b + lp) &= (h + a + kp)(h + b + lp) - m = \\ &(h + a)(h + b) - m + kp(h + b) + (h + a + kp)lp = \\ &s(a, b) + p\big(k(h + b) + l(h + a + kp)\big) \end{aligned}$$

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 (8.16) 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

$$(h+x)^2 \equiv f(x) \pmod{m}, \tag{8.17}$$

то есть сравнение Крайчика вида $u^2 \equiv v \pmod{m}$, которое может быть использовано для построения сравнения (8.1).

Аналогично методу Моррисона-Брилхарта, см. раздел 8.2.3, заметим следующий факт. Пусть для некоторого целого x найдется нечетное простое число p такое, что $p|f(x)$, 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 (8.17), 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 $p \leqslant B$.

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 (8.17). 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 δ количество таких целых чисел. Мы будем искать среди δ 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

$$f(x + kp) = (h + x + kp)^2 - m = (h + x)^2 + 2kp(h + x) + k^2p^2 - m = \\ = f(x) + p\big(2k(h + x) + pk^2\big) \equiv 0 \pmod{p}.$$

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 δ 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

$$\ln|f(x)| = \sum_{i=1}^{s-1} \gamma_i \ln p_i. \tag{8.18}$$

Поэтому предложенный метод позволяет накапливать значения $\ln p_i$ в ячейках массива и находить те элементы, в которых правая часть равенства (8.18) 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 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 (8.17), в которых правая часть удовлетворяет равенству (8.7): без использования решета мы должны раскладывать на множители все δ 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 δ.

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 (8.17) 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. Holdrige), реализовавшими алгоритм квадратичного решета на практике, см. работу [16]. В 1987 году вышла статья Роберта Сильвермена (Robert D. Silverman), см. [39], в которой был предложен эффективный алгоритм построения многочленов. В настоящее время 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

$$b^2 - 4ac = D = \begin{cases} km, & \text{если} \quad k \equiv m \pmod 4, \\ 4km, & \text{иначе.} \end{cases}$$

Воспользовавшись утверждением теоремы 4.2, мы можем записать сравнение

$$f(x) \equiv a(x-e)^2 \pmod{m}, \quad \text{где} \quad e \equiv -\frac{b}{2a} \pmod{m},$$

или

$$af(x) \equiv (ax+b)^2 \pmod{m}, \tag{8.19}$$

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 δ таким образом, чтобы абсолютные значения многочлена $f(x)$ в точке минимума и на границах интервала совпадали. Тогда выполнены равенства

$$\left| f\left(-\frac{b}{2a}\right) \right| = f\left(-\frac{b}{2a} - \frac{\delta}{2}\right) = f\left(-\frac{b}{2a} + \frac{\delta}{2}\right). \tag{8.20}$$

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 (8.20) следует равенство

$$a\delta = \sqrt{2D}. \tag{8.21}$$

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 (8.21) следует, что на всем интервале $\mathcal{I}$ выполнена оценка

$$|f(x)| \leqslant \frac{\delta}{4\sqrt{2}}\sqrt{D}. \tag{8.22}$$

Заметим, что при $\delta > 8\sqrt{2}$ эта оценка хуже, чем у метода непрерывных дробей, см. (8.4).

Поскольку величины a, δ являются положительными целыми числами, то при практических вычислениях равенство (8.21) не может быть достигнуто. Поэтому величина δ фиксируется, а равенство (8.21) заменяется неравенством $a \leqslant \left\lfloor \frac{\sqrt{2D}}{\delta} \right\rfloor$.

Зафиксируем значения параметров D и δ и опишем процедуру выбора коэффициентов многочлена $f(x)$. Вначале выберем нечетное простое число d такое, что $\left(\frac{D}{d}\right) = 1$ и $d \leqslant \left\lfloor \sqrt{\frac{\sqrt{2D}}{\delta}} \right\rfloor$.

Мы определим параметр a равенством $a = d^2$, тогда из (8.19) 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 (8.22).

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

$$b = b_i + td, \quad \text{где} \quad t \equiv \frac{D - b_1^2}{2db_1} \pmod{d}, \quad i \in \{1, 2\}. \tag{8.23}$$

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 (8.23) 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 $c = \frac{b^2 - D}{4d^2}$.

Глава 9

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 $\operatorname{ord}_p a = m$ и $m|p-1$. Пусть задан вычет b, удовлетворяющий сравнению*

$$a^x \equiv b \pmod{p}. \tag{9.1}$$

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

$$x \equiv \operatorname{ind}_a b \pmod{m} \quad \textit{или} \quad x \equiv \log_a b \pmod{m} \tag{9.2}$$

и называть его индекс или дискретный логарифм b по основанию a.

Из данного выше определения и утверждения леммы 2.3 вытекает, что сравнение (9.1) разрешимо только в том случае, когда вычет b принадлежит множеству

$$\mathcal{A} = \{1,\ a,\ a^2,\ \ldots,\ a^{q-1}\} \subset \mathbb{F}_p^*,$$

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 $\operatorname{ord}_p a = m$. 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 $\alpha_1, \ldots, \alpha_n$ *произвольные натуральные числа, а вычеты* $b_1, \ldots, b_n$ *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 принадлеждат множеству возможных степеней вычета a, то найдутся такие вычеты x, y, что

$$a^x \equiv b_1 \pmod p, \quad a^y \equiv b_2 \pmod p \quad \text{или}$$
$$x \equiv \log_a b_1 \pmod m, \quad y \equiv \log_a b_2 \pmod m.$$

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. □

Пример 9.1. Особо стоит обратить внимание на тот факт, что в условии леммы 9.1 требуется принадлежность вычетов $b_1, \ldots, b_n$ 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 $\mathrm{ord}_{547}\,27 = 14$, то есть, вычет 27 не является первообразным корнем и порождает мультипликативную группу

$$\mathcal{A} =< 27 >= \{27, 182, 538, 304, 3, 81, 546, 520, 365, 9, 243, 544, 466, 1\},$$

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

$$\log_{27} 520 \equiv 3\log_{27} 2 + \log_{27} 5 + \log_{27} 13 \pmod{14}. \tag{9.3}$$

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 Осиповичом Гельфондом был предложен метод, см. [8, 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. [38], 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

$$x = hu - v, \quad 0 < u \leqslant h, \quad 0 \leqslant v < h. \tag{9.4}$$

Выполнено сравнение

$$b \equiv a^x \equiv \left(a^h\right)^u a^{-v} \pmod{p}, \quad \text{или} \quad ba^v \equiv \left(a^h\right)^u \pmod{p},$$

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 $v = 0,\ 1,\ \ldots,\ h-1$ вычислим вычеты $ba^v \pmod{p}$ и сохраним их в памяти. Далее, вычисляя $\left(a^h\right)^u$ для всех $u = 1,\ \ldots,\ h$ 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 $\operatorname{ord}_{181} 3 = 45$.

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 $ba^v \pmod{p}$, $v = 0,\ 1,\ \ldots, 6$ 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 $u = 1,\ 2,\ \ldots, 7$.

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 $v = 0, \ldots, h-1$. 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[1] $\log_2 n$ операций сравнения элементов таблицы, где n число элементов массива. Следовательно, при создании таблицы нам потребуется

$$\log_2 1 + \log_2 2 + \log_2 3 + \cdots + \log_2 h = \log_2 h! < \log_2 h^h = h \log_2 h$$

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 $u = 0, \ldots, h-1$. 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

$$a^x \equiv b \pmod p, \quad \operatorname{ord}_p a = m = q^n,$$

[1]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 $O\left(\sqrt{q^n}\right)$ 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 [32].

Мы будем искать целое значение x, удовлетворяющее неравенствам $0 < x < q^n$ и представимое в виде

$$x = x_0 + x_1 q + \cdots + x_{n-1} q^{n-1}, \tag{9.5}$$

где $0 \leqslant x_i < q$ для всех $i = 0,\ 1,\ \ldots, n-1$. В начале мы последовательно определим неизвестные коэффициенты $x_0,\ \ldots,\ x_{n-1}$, а после, используя равенство (9.5), определим искомую величину x.

Обозначим $\alpha \equiv a^{q^{n-1}} \pmod p$. Легко проверить, что $\operatorname{ord}_p \alpha = q$, а кроме того,

$$\alpha^x \equiv \alpha^{x_0}\alpha^{x_1 q}\cdots\alpha^{x_{n-1}q^{n-1}} \equiv$$
$$\equiv \alpha^{x_0}(\alpha^q)^{x_1}(\alpha^q)^{x_2 q}\cdots(\alpha^q)^{x_{n-1}q^{n-2}} \equiv \alpha^{x_0} \pmod p.$$

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

$$\alpha^{x_0} \equiv b_0 \pmod p, \tag{9.6}$$

где $\alpha \equiv a^{q^{n-1}} \pmod p$, $\operatorname{ord}_p \alpha = q$ и $b_0 \equiv b^{q^{n-1}} \pmod p$.

Используя схожие рассуждения, мы можем найти остальные неизвестные коэффициенты $x_1,\ \ldots,\ x_{n-1}$. Для этого определим последовательность вычетов

$$a_i \equiv a^{q^{n-i-1}} \pmod p, \quad i = 0,\ 1,\ \ldots, n-1.$$

Легко видеть, что $a_0 \equiv \alpha \pmod p$, $a_{n-1} \equiv a \pmod p$, а также выполнены сравнения

$$a_i^{q^j} \equiv a^{q^{n-i-1}q^j} \equiv a^{q^{n-i+j-1}} \equiv a_{i-j} \pmod p, \tag{9.7}$$

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

найдены. Тогда, учитывая сравнение (9.7) и тот факт, что $\operatorname{ord}_p a_0 = q$, получаем

$$a_i^x \equiv a_i^{x_0} a_i^{x_1 q} \cdots a_i^{x_{n-1} q^{n-1}} \equiv a_i^{x_0} a_{i-1}^{x_1} \cdots a_0^{x_i} \pmod{p}. \tag{9.8}$$

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

$$\alpha^{x_i} \equiv \beta_i \pmod{p}, \quad \text{где} \quad \beta_i \equiv b_i \left(a_i^{x_0} a_{i-1}^{x_1} \cdots a_1^{x_{i-1}}\right)^{-1} \pmod{p}, \tag{9.9}$$

для всех $i = 0,\ 1, \ldots,\ n-1$. 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 $\operatorname{ord}_p a = q^n$ 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 γ – 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 $O\left(n^2 \log_2 q + n\sqrt{q}\right)$.

Теперь мы можем рассмотреть задачу дискретного логарифмирования

$$a^x \equiv b \pmod{p}, \quad \operatorname{ord}_p a = m, \tag{9.10}$$

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 α_i некоторые натуральные числа.

Фиксируем некоторый индекс i, $1 \leqslant i \leqslant n$, и определим вычет c_i сравнением $c_i \equiv a^{\frac{m}{q_i^{\alpha_i}}} \pmod{p}$. Поскольку $\operatorname{ord}_p a = m$, то для вычета c_i выполнено условие $\operatorname{ord}_p c_i = q_i^{\alpha_i}$.

С другой стороны, возводя в сравнении (9.10) правую и левую часть в степень $\frac{m}{q_i^{\alpha_i}}$, получим сравнение

$$c_i^x \equiv b^{\frac{m}{q_i^{\alpha_i}}} \pmod{m}. \tag{9.11}$$

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 кажого 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. [8, 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 $\operatorname{ord}_{181} 3 = 45 = 3^2 \cdot 5$, 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 удволетворяют 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 $\operatorname{ord}_{181} 135 = \frac{45}{9} = 5$ 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

$$a_0 \equiv 132 \pmod{181}, \quad a_1 \equiv 62 \pmod{181},$$
$$b_0 \equiv 48 \pmod{181}, \quad b_1 \equiv 65 \pmod{181}.$$

Величина x_0 является решением сравнения $132^x \equiv 48 \pmod{181}$. Поскольку $\operatorname{ord}_{181} 132 = 3$, 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 β_1, удовлетворяющую сравнению

$$\beta_1 \equiv 65 \cdot \left(62^2\right)^{-1} \equiv 132 \pmod{181}.$$

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

$$a^x \equiv b \pmod{p}, \quad \operatorname{ord}_p a = m. \tag{9.12}$$

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 [34].

9.3.1 Метод Полларда-Флойда

Используя идеи, схожие с теми, на которых основан метод факторизации, см. раздел 7.4, Полларда предложил алгоритм, базирующийся на свойстве случайных отображений зацикливаться при действии на конечных множествах.

Для обнаружения зацикливаний Полларда предложил использовать тест Роберта Флойда (Robert W Floyd), см. [21, п.3.1, задача 6b]. В современной литературе метод дискретного логарифмирования Полларда-Флойда часто называют ϱ-методом Полларда.

Зафиксируем натуральное число $s \geqslant 3$. Рассмотрим конечное множество возможных степеней вычета a

$$\mathcal{A} = \{1,\ a,\ \ldots,\ a^{m-1}\},$$

состоящее из m элементов, и разделим его на s непересекающихся интервалов $\mathcal{I}_0,\ \mathcal{I}_1.\ \ldots,\ \mathcal{I}_{s-1}$ 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 $i = 0,\ 1,\ \ldots,\ s-1$ 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

$$f(z):\ \mathcal{A} \to \mathcal{A},$$
$$f(z) \equiv z a^{\alpha_i} b^{\beta_i} \pmod{p}, \quad \text{если} \quad z \in \mathcal{I}_i,$$

где вычеты a, b определены сравнением (9.12).

Легко показать, что функция $f(z)$ определена корректно для любого набора величин α_n, β_n. Если $z \in \mathcal{A}$, то найдется такой вычет γ 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 $z_0,\ z_1,\ \ldots$, определяемую соотношением

$$z_{n+1} = f(z_n), \quad n = 0,\ 1,\ \ldots. \tag{9.13}$$

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 $z_0,\ z_1,\ \ldots$ 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

$$A_{n+1} = \alpha_i + A_n, \quad B_{n+1} = \beta_i + B_n, \quad A_0 = k_0, \quad B_0 = 0, \tag{9.14}$$

то есть являются суммами соответствующих коэффициентов α_i и β_i, определяемых функцией $f(z)$.

Поскольку множество $\mathcal{A}$ конечно, то последовательность $z_0,\ z_1,\ \ldots$ зациклится 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 $\operatorname{ord}_p a = m$, а также параметр $s \geqslant 3$ и отображение $f(x)$, задаваемое наборами вычетов $\alpha_0, \ldots, \alpha_{s-1}, \beta_0, \ldots, \beta_{s-1}$.
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
$$A_z \equiv A_z + \alpha_i \pmod m, \quad B_z \equiv B_z + \beta_n \pmod m.$$
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 зацикливания последовательности $z_0, z_1, \ldots$ зависит как от выбора начального элемента z_0, так и от коэффициентов $\alpha_0, \ldots, \alpha_{s-1}, \beta_0, \ldots, \beta_{s-1}$.

Если отображение $f(z)$ ведет себя как случайное, то мы можем ожидать, что для обнаружения момента зацикливания нам потребуется вычислить $O(\sqrt{m})$ элементов последовательности. Случайность отображения $f(z)$ достигается за счет выбора большого значения параметра s.

Порллард предложил выбирать $s = 3$. Позднейшие эксперименты показали, см. [7], 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[2] методом является алгоритм, предложенный Биллом Госпером (Ralph William Gosper, Jr.).

[2]Обзор методов поиска длин циклов в последовательностях и их криптографических приложений может быть найден в статье [7].

В алгоритме Госпера для поиска двух совпадающих элементов последовательности (9.13)

$$z_{n+1} = f(z_n), \quad n = 0,\ 1,\ \ldots$$

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 $z_{n_0},\ z_{n_1},\ \ldots$ последовательности (9.13), с условием

$$n_k = \max_{r<n}\{r|\nu_2(r+1) = k\}, \tag{9.15}$$

для всех возможных значений $k = 0,\ 1,\ \ldots$. 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. [7]). *Пусть заданы параметры λ и τ, 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. *$\lambda + \tau \leqslant n < \lambda + 2\tau$.*

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

$$T = T_0,\ T_1,\ \ldots, T_{\lfloor \log_2 n \rfloor + 1}.$$

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 α_i и β_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 $\operatorname{ord}_p a = m$, а также параметр $s \geqslant 3$ и отображение $f(x)$, задаваемое наборами вычетов $\alpha_0,\ \ldots, \alpha_{s-1}$, $\beta_0,\ \ldots,\ \beta_{s-1}$.
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 $A \equiv A + \alpha_i \pmod m$, $B = B + \beta_i \pmod m$, 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 9.1, приведенный алгоритм затратит на нахождение неизвестной величины z не более двух периодов последовательности $z_0, z_1,\ \ldots$. Однако ассимптотическая 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

$$a^x \equiv b \pmod p, \quad \operatorname{ord}_p a = m$$

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[3] в 1926 году Морисом Крайчиком для построения таблиц индексов. Следуя его монографии [23], приведем пример построения начальных значений таблицы индексов для простого числа $p = 9649$ и первообразного корня $a = 7$.

Для начала найдем индексы первых четырех простых чисел. Из определения следует равенство $\log_7 7 = 1$; для остальных величин введем обозначения

$$x = \log_7 2, \quad y = \log_7 3, \quad z = \log_7 5$$

и рассмотрим сравнение

$$9600 \equiv -49 \equiv (-1)7^2 \pmod{9649}. \tag{9.16}$$

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

$$7x + y + 2z \equiv 4826 \pmod{9648}. \tag{9.17}$$

Аналогично, рассматривая второе сравнение

$$9604 \equiv -45 \pmod{9649},$$

раскладывая величины 9604 и 45 на множители и переходя к индексам, получаем уравнение

$$4 + 2x \equiv 4824 + 2y + z \pmod{9648} \quad \text{или}$$
$$2x - 2y - z \equiv 4820 \pmod{9648}. \tag{9.18}$$

[3] 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

$$18 \equiv 2x + y + 4z \pmod{9648}. \tag{9.19}$$

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,

$$x = \log_7 2 = 1128, \quad y = \log_7 3 = 5746, \quad \text{и} \quad z = \log_7 5 = 5240. \tag{9.20}$$

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, [41].

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) [27] и Леонарда Адлемана (Leonard Adleman) [12]. 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

$$\mathcal{B}_B = \{p_1,\ p_2,\ \ldots,\ p_s\},$$

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 $p_1, \ldots,\ p_s$, 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

$$a^k \equiv w \pmod{p}, \quad -\frac{p-1}{2} \leqslant w \leqslant \frac{p-1}{2}.$$

2. Разложить вычет w в произведение простых чисел, принадлежащих факторной базе

$$w = (-1)^{\gamma_0} p_1^{\gamma_1} \cdots p_s^{\gamma_s}, \quad p_1,\ \ldots, p_s \in \mathcal{B}_B, \tag{9.21}$$

   где величины $\gamma_0,\ \gamma_1,\ \ldots,\ \gamma_s$ 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,

$$k \equiv \frac{\gamma_0(p-1)}{2} + \gamma_1 \log_a p_1 + \cdots + \gamma_s \log_a p_s \pmod{p-1}. \quad (9.22)$$

Полученное сравнение является одним соотношением, относительно неизвестных $\log_a p_1,\ \ldots,\ \log_a p_s$.

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 $p_1,\ \ldots,\ p_s$, 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

$$ba^l \equiv w \pmod{p} \quad \text{и} \quad w = (-1)^{\gamma_0} p_1^{\gamma_1} \cdots p_s^{\gamma_s}, \quad p_1,\ \ldots, p_s \in \mathcal{B}_B.$$

Тогда, переходя к индексам, получаем сравнение

$$\log_a b + l \equiv \frac{\gamma_0(p-1)}{2} + \gamma_1 \log_a p_1 + \cdots + \gamma_s \log_a p_s \pmod{p-1},$$

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

$$a^x \equiv b \pmod{p}, \quad \operatorname{ord}_p a = m | p-1.$$

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 $t \geqslant s$

$$\begin{cases} \gamma_{11}x_1 + \gamma_{12}x_2 + \cdots + \gamma_{1s}x_s \equiv \gamma_{1s+1} \pmod{p-1}, \\ \cdots \\ \gamma_{t1}x_1 + \gamma_{t2}x_2 + \cdots + \gamma_{ts}x_s \equiv \gamma_{ts+1} \pmod{p-1}, \end{cases} \tag{9.23}$$

относительно неизвестных $x_1, \ \ldots, \ x_s$. При этом, неизвестные представляют собой искомые индексы $\log_a p_1, \ \ldots, \ \log_a p_s$, 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 потребуется следующая лемма.

Лемма 9.2. *Пусть m натуральное число и γ_1, γ_2 вычета кольца $\mathbb{Z}_{p-1}$, одновременно не сравнимых с нулем. Тогда найдутся целые числа a, b, c, d такие, что $ad - dc = 1$ и выполнено матричное равенство*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} z \\ 0 \end{pmatrix}, \quad z = \mathbf{НОД}\,(\gamma_1, \ \gamma_2)\,.$$

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

$$a\gamma_1 + b\gamma_2 = z, \quad z = \mathbf{НОД}\,(\gamma_1, \ \gamma_2)\,,$$

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. □

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 Γ в виде столбца строк

$$\Gamma = \begin{pmatrix} \overline{\gamma}_1 \\ \overline{\gamma}_2 \\ \dots \\ \overline{\gamma}_t \end{pmatrix}, \quad \overline{\gamma}_i = (\gamma_{i1},\ \gamma_{i2},\ \dots,\ \gamma_{is+1}).$$

Фиксируем два индекса i, j и для матрицы Γ определим преобразование $F_{ij}(\Gamma, a, b, c, d)$, зависящее от четырех параметров a, b, c и d

$$\Gamma = \begin{pmatrix} \overline{\gamma}_1 \\ \dots \\ \overline{\gamma}_i \\ \dots \\ \overline{\gamma}_j \\ \dots \\ \overline{\gamma}_t \end{pmatrix} \to \begin{pmatrix} \overline{\gamma}_1 \\ \dots \\ a\overline{\gamma}_i + b\overline{\gamma}_j \\ \dots \\ c\overline{\gamma}_i + d\overline{\gamma}_j \\ \dots \\ \overline{\gamma}_t \end{pmatrix},$$

где

$$a\overline{\gamma}_i + b\overline{\gamma}_j = (a\gamma_{i1} + b\gamma_{j1} \pmod{p-1},\ \dots,\ a\gamma_{is} + b\gamma_{js} \pmod{p-1}).$$

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 Γ к верхнетреугольному виду.

Алгоритм 9.4 (Алгоритм гауссового исключения)

Вход: Матрица Γ, соответствующая системе сравнений (9.23).
Выход: Матрица Γ, 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 лемму 9.2, для вычетов γ_{ii} и γ_{ji}.

1.1.3 Применить к матрице Γ преобразование $F_{ij}(\Gamma, a, b, c, d)$.

□

В ходе выполнения внутреннего цикла обнуляются все элементы матрицы Γ, расположенные в i-м столбце ниже i-го элемента, то есть элементы $\gamma_{i+1,i},\ \gamma_{i+2,i},\ \ldots,\ \gamma_{ti}$. Если выполнено $\gamma_{ii} \equiv 0 \pmod{p-1}$, то в ходе применения преобразования F_{ij} величина γ_{ii} будет заменена на первую отличную от нуля величину $\gamma_{ji}\ i < j < t$.

После приведения матрица Γ 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 $1 < r \leqslant s$, 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 $\log_a p_1,\ \ldots,\ \log_a p_s$.

Далее, если хотя бы одна из величин $\gamma_{r+1,s+1},\ \ldots,\ \gamma_{t,s+1}$ 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 $\gamma_{r+1,s+1} \equiv \ldots \equiv \gamma_{t,s+1} \equiv 0 \pmod{p-1}$ решение системы может быть найдено путем применения обратного хода, то есть из системы сравнений

$$\begin{cases} x_s & \equiv & \gamma_{s,s}^{-1}\gamma_{s,s+1} \pmod{p-1}, \\ x_{s-1} & \equiv & \gamma_{s-1,s-1}^{-1}\left(\gamma_{s-1,s+1} - \gamma_{s-1,s}x_s\right) \pmod{p-1}, \\ & \ldots & \\ x_1 & \equiv & \gamma_{1,1}^{-1}\left(\gamma_{1,s+1} - \gamma_{1,s}x_s - \ldots - \gamma_{1,2}x_2\right) \pmod{p-1}. \end{cases} \tag{9.24}$$

В общем случае, согласно теореме 2.1, число решений системы (9.24) не превосходит величины

$$\mathbf{НОД}\left(\gamma_{s,s},\ p-1\right) \cdot \mathbf{НОД}\left(\gamma_{s-1,s-1},\ p-1\right) \cdots \mathbf{НОД}\left(\gamma_{1,1},\ p-1\right).$$

При решении задачи дискретного логарифмирования, в силу единственности решения, должен существовать только один набор значений x_1, $\ldots$, 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 элеметов γ_{ii} и γ_{ji} матрицы Γ. 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 Γ 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

$$\sum_{i=1}^{s-1}(s-i)(3\log_2 p + 4(s-i+1)) = \\ = (3\log_2 p + 4)\sum_{k=1}^{s-1} k + 4\sum_{k=1}^{s-1} k^2 = O(hs^2),$$

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[4], 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.

[4] 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.

$$\begin{pmatrix} 7 & 1 & 2 & 4826 \\ 2 & 9646 & 9647 & 4820 \\ 2 & 1 & 4 & 18 \end{pmatrix} \to \begin{pmatrix} 1 & 7 & 5 & 14 \\ 0 & 9632 & 9637 & 4792 \\ 2 & 1 & 4 & 18 \end{pmatrix}.$$

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.

$$\begin{pmatrix} 1 & 7 & 5 & 14 \\ 0 & 9632 & 9637 & 4792 \\ 2 & 1 & 4 & 18 \end{pmatrix} \to \begin{pmatrix} 1 & 20 & 11 & 24 \\ 0 & 9632 & 9637 & 4792 \\ 0 & 9635 & 9642 & 9638 \end{pmatrix}.$$

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

$$\begin{pmatrix} 1 & 20 & 11 & 24 \\ 0 & 9632 & 9637 & 4792 \\ 0 & 9635 & 9642 & 9638 \end{pmatrix} \to \begin{pmatrix} 1 & 20 & 11 & 24 \\ 0 & 1 & 6418 & 3138 \\ 0 & 0 & 9601 & 4568 \end{pmatrix}.$$

Мы привели матрицу к верхнетреугольному виду и теперь можем найти значения неизвестных x, y и z из системы сравнений

$$\begin{cases} x + 20y + 11z \equiv 24 \pmod{9648}, \\ y + 6418z \equiv 3138 \pmod{9648}, \\ 9601z \equiv 4568 \pmod{9648}. \end{cases}$$

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 $p \to \infty$.

Для оценки числа операций, необходимых для поиска одного соотношения вида (9.22), нам потребуется следующий результат. Обозначим символом $\psi(x, y)$ количество натуральных чисел $n \leqslant x$, у которых наибольший простой делитель не превосходит y.

Теорема 9.2 (см. [36, §2]). *Пусть $0 < \varepsilon < \frac{1}{2}$ некоторая действительная константа. Если выполнены неравенства*

$$\ln^{\varepsilon} x < \ln y < \ln^{1-\varepsilon} x,$$

то при $x \to \infty$ выполнено $\psi(x, y) = xe^{-u \ln u + o(u \ln u)}$, где $u = \dfrac{\ln x}{\ln y}$.

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, $0 \leqslant k < p - 1$ и определим $w \equiv a^k \pmod p$.

Согласно утверждению теоремы 9.2, 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 $p \to \infty$.

Для каждого случайного k нам надо проверить существует ли для вычета w разложение (9.21), то есть разделить w на все простые числа $p_1, \ldots, p_s$. Поскольу нам надо найти не менее s соотношений, то получаем, что суммарная трудоемкость построения матрицы Γ, 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 3α 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.

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] *Гашков С.Б.* Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // Дискретная математика. – №. 4. – Vol. 10. – 1998. – с. 35-38.

[5] *Кострикин А.И.* Введение в алгебру. – М.:Наука. – 1977. – 495 с.

[6] *Нестеренко Ю.В.* Теория чисел. – М.:Академия. – 2008. – 272 с.

[7] *Нестеренко А.Ю.* Алгоритмы поиска длин циклов в последовательностях и их приложения // Фундаментальная и прикладная математика. – №. 6. – Т. 16. – 2010. – с. 109-122.

[8] *Нечаев В.И.* Элементы криптографии (Основы теории защиты информации). – М.:Высш.шк. – 1999. – 109 с.

[9] *Сушкевич А.К.* Теория чисел. Элементарный курс. – Харьков:Изд-во Харьковского университета. – 1954. – 204 с.

[10] *Ноден П. и Китте К.* Алгебраическая алгоритмика с упражнениями и решениями. – М.Мир. – 1999. – 720 с.

[11] *Прахар К.* Распределение простых чисел. – М.:Мир. – 1967. – 512 с.

[12] *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.

[13] *Alford R., Granville A. and Pomerance C.* There are infinitely many Carmichael numbers // Annals of Mathematics. – Vol. 140. – 1994. – pp. 703-722.

[14] *Brent R.P.* An Improved Monte-Carlo Factorization Algorithm // BIT. – Vol. 20. – 1980. – pp. 176-184.

[15] *Carmichael R.D.* The Theory Of Numbers. – New York:J. Willey & Sons. – 1914. – 95 p.

[16] *Davis J.A. and Holdridge D.B.*, Factorization Using the Quadratic Sieve Algorithm // Sandia National Laboratories. – Albuquerque, New Mexico. – 1983.

[17] *Garner H.* The Residue Number System // IRE Transactions on Electronic Computers. – №. 2. – Vol. 8. – 1959. – pp. 140-147.

[18] *Gordon J.* Strong RSA keys // Electronic Letters. – №. 12. – Vol. 20. – June 1984. – pp. 514-516.

[19] *Granville A.* Primality testing and Carmichael numbers // Notices of the American Mathematical Society. – Vol. 39. – 1992. – pp. 696-700.

[20] *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.

[21] *Knuth D.E.*, Fundamental Algorithms. Volume 1 of The Art of Computer Programming. – Addison-Wesley Professional. – 1969.

[22] *Knuth D.E.*, Seminumerical Algorithms. Volume 2 of The Art of Computer Programming. – Addison-Wesley Professional. – 1969.

[23] *Kraitchik M.* Théorie des Nombres. Tome I et II. – Paris:Gauthier-Villars. – 1926.

[24] *Lehman R.S.* Factoring Large Integers // Mathematics Of Computation. – №. 126. – Vol. 28. – 1974. – pp. 637-646.

[25] *Lehmer D.H. and Powers R.E.* On Factoring Large Numbers // Bulletin Of the American Mathematical Society. – №. 9. – Vol. 37. – 1931. – pp. 770-776.

[26] *McKee J.* Speeding Fermat's Factoring Algorithm // Mathematics Of Computation. – №. 228. – Vol. 68. – 1999. – pp. 1729-1737.

[27] *Merkle R.C.* Secrecy, Authentication and Public Key Systems // PhD. Thesis / Electrical Engineering. – June 1979. – P. 182.

[28] *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.

[29] *Miller G.L.* Riemann's Hypothesis and Tests for Primality // Journal of Computer and System Sciences. – №. 3. – Vol. 13. – 1976. – pp. 300-317.

[30] *Montgomery P.L.* Speeding The Pollard and Elliptic Curve Methods of Factorization // Mathematics Of Computation. – № 177. – Vol. 48. – 1987. – pp. 243-267.

[31] *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.

[32] *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.

[33] *Pollard J.M.* Theorems on Factorization And Primality Testing // Proceedings of the Cambridge Philosophical Society. – №. 3. – Vol. 76. – 1974. – pp. 521-528.

[34] *Pollard J.M.* Monte Carlo methods for index computation $\pmod p$ // Mathematics Of Computation. – №. 143. – Vol. 32. – 1978. – pp. 918-924.

[35] *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.

[36] *Pomerance C.* Two Methods in Elementary Analytic Number Theory // Number Theory and Applications / Ed. R.A. Molin. – 1989. – pp. 135-161.

[37] *Rabin M.O.* Probabilistic Algorithm for Testing Primality // Journal of Number Theory. – №. 1. – Vol. 12. – 1980. – pp. 128-138.

[38] *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.

[39] *Silverman R.D.*, The Multiple Polinomial Quadratic Sieve Mathematics Of Computation. – №. 177. – Vol. 48. – 1987. – pp. 329-339.

[40] *Solovay R. and Strassen V.* A Fast Monte-Carlo Test for Primality // SIAM Journal on Computing. – №. 1. – Vol. 6. – 1977. – pp. 84-85.

[41] *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.

[42] *Williams H.C.* Primality Testing On A Computer // Ars Combinatoria. – Vol. 5. – 1978. – pp. 127-185.

[43] *Williams H.C.* A $p + 1$ Method of Factoring // Mathematics Of Computation. – №. 159. – Vol. 39. – 1982. – pp. 225-234.

[44] *Williams H.C. and Schmid B.* Some remarks cocerning the MIT public-key cryptosystem // BIT. – Vol. 19. – 1979. – pp. 525-538.

[45] *Zhang Z.* Using Lucas Sequences to Factor Large Integers Near Group Orders // Fibonacci Quarterly. – №. 3. – Vol. 39. – 2001. – pp. 228-237.

НЕСТЕРЕНКО Алексей Юрьевич

Теоретико-числовые методы в криптографии
Учебное пособие

Редактор С.П. Клышинская
Технический редактор О.Г. Завьялова

Подписано в печать 26.03.12 Формат 60x84/16.
Бумага офсетная. Печать — ризография.
Усл. печ. л. Уч.-изд. л. Тираж 125 экз.
Заказ Бесплатно. Изд. № 26.
Московский государственный институт электроники и математики.
109208 Москва, пер. Б. Трехсвятительский, 3/12.
Отдел оперативной полиграфии Московского государственного института электроники и математики.
113054 Москва, ул. М. Пионерская, 12.