ТЕОРЕТИКО–ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

О.Н. Герман, Ю.В. Нестеренко

Оглавление

Введение

Теория чисел стала широко применяться в криптографии примерно 30 лет назад. Это было вызвано необходимостью обмена большими массивами конфиденциальной информации (не только государственной и военной, но и банковской, экономической, медицинской, юридической и т.п.), а также возможностью такого обмена, в связи с появлением доступных и эффективных компьютерных средств обработки этой информации. Любая информация может быть закодирована последовательностью чисел. Например, букве “а” можно сопоставить число 1, букве “б” — число 2 и так далее, букве “я” — число 32. Можно сопоставить числа пробелам, точке, другим знакам препинания. После этого процессы зашифрования и расшифрования информации представятся как некоторые алгоритмы, перерабатывающие одни массивы целых чисел в другие.

Криптографические потребности стимулировали исследования в некоторых областях теории чисел, стали источником постановки новых фундаментальных проблем. Стойкость криптографических алгоритмов напрямую зависит от невозможности найти быстрые алгоритмы для решения некоторых задач, другими словами, от того, что некоторые задачи теории чисел сложны в вычислительном отношении.

Сложность алгоритмов теории чисел обычно измеряют количеством арифметических операций (сложений, вычитаний, умножений и делений с остатком), необходимых для выполнения всех действий, предписанных алгоритмом. Впрочем, это определение не учитывает величины чисел, участвующих в вычислениях. Ясно, что перемно-

жить два стозначных числа значительно сложнее, чем два однозначных, хотя и в том, и в другом случае выполняется лишь одна арифметическая операция. Поэтому иногда учитывают еще и величину чисел, сводя дело к так называемым битовым операциям, т.е. оценивая количество необходимых операций с цифрами 0 и 1 в двоичной записи чисел (битовая сложность). Это зависит от рассматриваемой задачи, от целей автора и т.д.

На первый взгляд кажется странным, что операции умножения и деления приравниваются по сложности к операциям сложения и вычитания. Житейский опыт подсказывает, что умножать числа значительно сложнее, чем складывать их. В действительности же, вычисления можно организовать так, что на умножение или деление больших чисел понадобится не намного больше битовых операций, чем на сложение. В главе 2 описывается алгоритм Шенхаге - Штрассена, основанный на так называемом быстром преобразовании Фурье. Он требует $O(n \ln n \ln \ln n)$ битовых операций для умножения двух n-разрядных двоичных чисел. Таким же количеством битовых операций можно обойтись при выполнении деления с остатком двух двоичных чисел, записываемых не более, чем n цифрами. Для сравнения отметим, что сложение n-разрядных двоичных чисел требует $O(n)$ битовых операций. Говоря в этой книге о сложности алгоритмов, мы будем иметь в виду количество арифметических операций, необходимых для их выполнения.

Быстрыми алгоритмами обычно называют те, сложность которых оценивается величиной $O(L^c)$, где L количество битов, необходимых для записи всей информации, подаваемой на вход алгоритма, а c — некоторая абсолютная постоянная. Подобные алгоритмы называют также полиномиальными (количество операций оценивается полиномом от длины входа задачи). Так, например, алгоритм вычисления наибольшего общего делителя двух целых чисел a и b требует $O(\ln N)$ арифметических операций, где $N = \min(\mid a \mid, \mid b \mid)$, и потому он полиномиален.

Для многих задач алгоритмы полиномиальной сложности не из-

вестны. Сложной, например, является следующая фундаментальная задача.

Пример. *Дано простое число p. Для заданных чисел $a, b \in \mathbb{Z}$ требуется решить сравнение*

$$a^x \equiv b \pmod{p}. \tag{1}$$

Эта задача носит название дискретного логарифмирования. Как известно, мультипликативная группа $(\mathbb{Z}/p\mathbb{Z})^*$ циклична. Если a — ее образующая, то сравнение (1) при $p \nmid b$ всегда разрешимо. Однако нахождение решения при большом p является весьма трудоемкой в вычислительном отношении задачей. Не случайно в конце практически всех учебников по элементарной теории чисел приводятся таблицы индексов — так традиционно назывались дискретные логарифмы. Лучшие из известных алгоритмов дискретного логарифмирования, использующие вычисления в полях алгебраических чисел, требуют $O(\exp(c(\ln p)^{1/3}(\ln\ln p)^{2/3}))$ арифметических операций. Впрочем, эта оценка условна, ибо опирается на ряд недоказанных гипотез теории чисел.

В области действительных чисел имеется специальное основание $e = 2,71828\ldots$, позволяющее достаточно быстро вычислять логарифмы с произвольной точностью. Например, это можно сделать с помощью быстро сходящегося при $|\, x \,| < 1$ ряда

$$\ln\frac{1+x}{1-x} = 2\left(x + \frac{x^3}{3} + \frac{x^5}{5} + \ldots\right).$$

Логарифмы по произвольному основанию a могут быть вычислены с помощью тождества

$$\log_a b = \frac{\ln b}{\ln a}.$$

Последняя формула справедлива и в случае дискретных логарифмов, однако нет основания, по которому логарифмы вычислялись бы столь же быстро, как натуральные в поле действительных чисел.

Следующая задача также важна в криптографических приложениях и является сложной.

Пример. *Дано составное натуральное число N. Требуется разложить его на нетривиальные множители.*

Еще Ферма предложил алгоритм разложения чисел на множители. Различные видоизменения его были предложены Эйлером, Гауссом, Лежандром и другими классиками теории чисел. Современные алгоритмы используют вычисления в полях алгебраических чисел, эллиптические кривые и разнообразные технические конструкции. Наилучшая из известных оценок сложности разложения числа N на множители имеет такой же вид, как и оценка сложности дискретного логарифмирования, и так же носит условный характер.

Настоящая книга представляет собой учебник по алгоритмической теории чисел, ориентированный на вопросы, связанные с различными криптографическими применениями. В первой главе дается обзор некоторых результатов теории чисел, в основном элементарных, нужных для последующих глав. Здесь изложение ограничивается определениями, формулировками утверждений и разбором примеров. Вторая глава содержит описание ряда быстрых алгоритмов теории чисел. Обсуждаются детерминированные, условные и вероятностные алгоритмы. В последнем разделе этой главы рассказывается о дискретном преобразовании Фурье и его использовании для построения быстрых алгоритмов умножения и деления целых чисел. Последующие четыре главы рассматривают вопросы факторизации многочленов над конечными полями, проверки чисел на простоту и построения больших простых чисел, факторизации целых чисел, дискретного логарифмирования. Седьмая глава содержит описание так называемого LLL-алгоритма, с помощью которого можно находить короткие векторы в заданной решетке и, в частности, решать задачи построения совместных диофантовых приближений чисел. В последней главе обсуждаются важные для криптографии система шифрования информации RSA, приложения задачи дискретного логарифмирования, цифровая подпись.

Эта книга написана на основе курса по алгоритмической теории чисел, читавшегося авторами в течение ряда лет на механико–

математическом факультете МГУ. Авторы благодарны А.В. Устинову и А.Ю. Нестеренко за ряд полезных замечаний.

Глава 1

Элементы теории чисел

Числа

$$1, 2, 3, \ldots, 100, 101, \ldots$$

называются натуральными. Для обозначения множества натуральных чисел используется символ $\mathbb{N}$. Если к ним добавить отрицательные числа и ноль, получится множество целых чисел. Оно обозначается символом $\mathbb{Z}$. Рассматривая отношения целых чисел с ненулевыми знаменателями, можно определить множество рациональных чисел $\mathbb{Q}$. В свою очередь рациональные числа составляют подмножество совокупности действительных чисел $\mathbb{R}$.

Эта глава представляет собой обзор необходимых в дальнейшем сведений из теории чисел.

1.1 Делимость целых чисел. Алгоритм Евклида.

Говорят, что целое число a делится на целое число $b \neq 0$, если найдется целое число c, удовлетворяющее равенству

$$a = b \cdot c.$$

Если целое число a делится на целое число b, то b называется *делителем*, a называется *делимым*, а для обозначения этого отношения используется символ $b|a$. Если целое число a не делится на b, используется обозначение $b \nmid a$.

Для любых целого числа a и натурального b существуют единственным образом определенные целые числа q, r, удовлетворяющие условиям

$$a = bq + r, \qquad 0 \leqslant r < b.$$

Определенные так числа r и q называются, соответственно, *остатком от деления* числа a на b и *неполным частным* при делении a на b. В случае $r = 0$ слово "неполное" в названии q опускают.

Множество всех делителей целого отличного от нуля числа a конечно. Действительно, если $d|a$, то, согласно определению делимости выполняется неравенство $|d| \leqslant |a|$.

Общим делителем целых чисел $a_1, a_2, \ldots, a_n$ называется любое целое d с условием $d|a_1, d|a_2, \ldots, d|a_n$. Если среди чисел $a_1, a_2, \ldots, a_n$ есть не равное нулю, то множество общих делителей этих чисел конечно. Оно всегда содержит ± 1 и потому не пусто. Говоря в дальнейшем об общих делителях мы, даже если это не оговаривается особо, всегда будем подразумевать, что в соответствующем наборе $a_1, a_2, \ldots, a_n$ содержится хотя бы одно не равное нулю число.

Определение 1.1. *Наибольшим общим делителем совокупности целых чисел называется наибольшее положительное число, делящее каждое из этих чисел.*

Целые числа называются взаимно простыми, если их наибольший общий делитель равен 1.

Наибольший общий делитель чисел $a_1, a_2, \ldots, a_n$ обозначается символом $\mathbf{НОД}(a_1, \ldots, a_n)$ или просто $(a_1, \ldots, a_n)$.

Можно доказать, что *наибольший общий делитель нескольких чисел делится на любой их общий делитель*. Кроме того справедливо равенство

$$((a_1, \ldots, a_{n-1}), a_n) = (a_1, \ldots, a_n). \tag{1.1}$$

Равенство (1.1) сводит задачу вычисления наибольшего общего делителя нескольких чисел к такой же задаче для двух чисел.

Пусть $a \geqslant b$ — натуральные числа, требуется найти (a, b) — их наибольший общий делитель. Задача эта, конечно, может быть решена путем перебора всех натуральных чисел d от 1 до b и проверки условий $d|a, d|b$. Однако этот путь требует очень большого объёма вычислений. Известный в Древней Греции алгоритм, называемый алгоритмом Евклида, достаточно быстро находит наибольший общий делитель и при этом не разлагает числа на множители.

Пусть r — остаток от деления числа a на b, т.е. $a = bq+r$, $0 \leqslant r < b$. По свойствам делимости каждый общий делитель чисел b и r делит число $bq + r = a$ и, значит, принадлежит множеству общих делителей чисел b и a. Точно так же, каждый общий делитель чисел a и b делит число $a - bq = r$, так что принадлежит множеству общих делителей чисел b и r. Отсюда следует совпадение наибольших общих делителей пар чисел a, b и b, r, т.е. равенство

$$(a, b) = (b, r). \tag{1.2}$$

Это равенство позволяет при нахождении наибольшего общего делителя заменить пару чисел a, b другой парой b, r. Заметим, что $r < b$, т.е. одно из двух чисел, участвующих в алгоритме уменьшилось. Повторяя несколько раз деление с остатком и заменяя каждый раз пару целых чисел новой мы будем каждый раз уменьшать одно из двух чисел, участвующих в работе алгоритма. Ясно, что в какой-то момент одно из чисел станет равным 0 и наибольший общий делитель будет равен второму из чисел.

Рассмотрим алгоритм немного подробнее. Положим $r_0 = a$, $r_1 = b$ и обозначим через $r_2, \ldots, r_n$ — последующие делители в алгоритме

Евклида. Тогда получаются следующие равенства

$$\begin{aligned} a =& r_0 = bq_1 + r_2, && 0 \leqslant r_2 < b, \\ b =& r_1 = r_2q_2 + r_3, && 0 \leqslant r_3 < r_2, \\ & r_2 = r_3q_3 + r_4, && 0 \leqslant r_4 < r_3, \\ & \ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots \\ & r_{n-2} = r_{n-1}q_{n-1} + r_n, && 0 \leqslant r_n < r_{n-1}, \\ & r_{n-1} = r_nq_n. \end{aligned} \tag{1.3}$$

Алгоритм останавливается, когда деление произойдет без остатка. В приведенном выше тексте последний остаток $r_{n+1} = 0$. В соответствии с равенством (1.2) находим

$$(a, b) = (b, r_2) = (r_2, r_3) = (r_3, r_4) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Таким образом, наибольший общий делитель равен последнему делителю (он же последний ненулевой остаток) в алгоритме Евклида.

Пример. *Найти наибольший общий делитель чисел* 3009 *и* 894.

Пользуясь алгоритмом Евклида, находим

$$\begin{aligned} 3009 &= 894 \cdot 3 + 327, & 894 &= 327 \cdot 3 + 240, \\ 327 &= 240 \cdot 1 + 87, & 240 &= 87 \cdot 2 + 66, \\ 87 &= 66 \cdot 1 + 21, & 66 &= 21 \cdot 21 + 3, \\ 21 &= 3 \cdot 7. \end{aligned}$$

Последний ненулевой остаток равен 3, поэтому $(3009, 894) = 3$.

Алгоритм Евклида может быть использован для нахождения решений в целых числах x, y уравнения

$$ax + by = c, \tag{1.4}$$

где a, b, c — целые числа.

Теорема 1.1. *Уравнение (1.4) разрешимо в целых числах* x, y *тогда и только тогда, когда* $(a, b)|c$.

Доказательство. Предположим, что целые числа x_0, y_0 составляют решение уравнения (1.4). Так как $(a,b)|a$ и $(a,b)|b$, из свойств делимости следует, что $(a,b)|ax_0+by_0=c$. Необходимость условия $(a,b)|c$ для разрешимости уравнения (1.4) доказана.

Для доказательства достаточности рассмотрим еще раз равенства (1.3). Первое из них даёт $r_2 = a - bq_1$. Подставляя это выражение во второе равенство, находим

$$r_3 = b - r_2q_2 = b(1+q_1q_2) - aq_2.$$

Далее, из третьего —

$$r_4 = r_2 - r_3q_3 = a(1+q_2q_3) - b(q_1+q_3+q_1q_2q_3).$$

Продолжая эти вычисления, можно найти представление $r_n = au+bv$ с некоторыми целыми u, v. Но это равенство означает, что уравнение $ax+by=(a,b)$ имеет решение $x=u, y=v$. А поскольку $(a,b)|c$, решениями уравнения (1.4) будут целые числа $x_0 = \frac{cu}{(a,b)}$, $y_0 = \frac{cv}{(a,b)}$. □

Можно доказать, что в случае разрешимости уравнения (1.4) множество его решений бесконечно, и все они имеют вид

$$x = x_0 + \frac{b}{(a,b)}t, \qquad y = y_0 - \frac{a}{(a,b)}t, \tag{1.5}$$

где пара чисел x_0, y_0 есть какое-либо фиксированное решение, а t — произвольное целое число.

1.2 Простые числа, основная теорема арифметики

Натуральное число $N > 1$ называется *составным*, если его можно представить в виде произведения двух меньших натуральных чисел. Если такое представление невозможно, число N называется *простым*. Например, числа 1111111 и 11111111111 составные. Это следует из равенств

$$1111111 = 239 \cdot 4649, \qquad 11111111111 = 21649 \cdot 513239.$$

Все сомножители в этих равенствах — простые числа.

Существует метод, позволяющий сравнительно легко определить список всех простых чисел, до заданной границы N. Этот метод носит название *решето Эратосфена*[1].

Решето Эратосфена [Этот алгоритм находит список всех простых чисел $p_1 < p_2 < \dots$ до заданной границы N].

1. Выпишем все целые числа $2, 3, 4, 5, \dots, N-1, N$. *Положим* $p_1 = 2$ *и начиная с* $4 = p_1^2$ *будем вычеркивать числа, двигаясь с шагом* 2. *(Заметим, что все числа, вычеркнутые на этом шаге алгоритма — четны, т.е. делятся на* 2.*)*

2. Пусть $k \geqslant 2$ *и уже определены числа* $p_1, \dots, p_{k-1}$. *Обозначим через* p_k *первое невычеркнутое число, следующее за* p_{k-1}. *Если* $p_k^2 > N$, *обозначаем через* $p_{k+1}, p_{k+2}, \dots$ *все оставшиеся невычеркнутыми числа, следующие за* p_k *в порядке возрастания; на этом алгоритм завершает свою работу.*

3. Если $p_k^2 \leqslant N$, *вычеркиваем числа, начиная с* p_k^2 *и двигаясь до* N *с шагом* p_k. *Вычеркнутые ранее числа, также принимаются в учет, но не вычеркиваются еще раз. По завершении этой процедуры алгоритм увеличивает индекс* k *на единицу и переходит в шаг 2.*

Легко видеть, что в процессе работы решета Эратосфена вычеркиваются только составные, а все простые числа остаются невычеркнутыми. Можно доказать, что все оставшиеся невычеркнутыми по окончании работы алгоритма числа просты.

Простые числа составляют довольно большую часть натурального ряда. С помощью решета Эратосфена, вычеркнув среди целых чисел $2, \dots, 100$ все числа, делящиеся на 2, 3, 5, 7, можно определить список всех простых чисел $p \leqslant 100$. Он состоит из 25 простых чисел

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$
$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

[1] Эратосфен (276-196г. до нашей эры) — древнегреческий математик, географ и астроном.

Более сложный алгоритм позволил найти, что среди первых 10^{16} натуральных имеется 279238341033925 простых чисел. Наибольшие из известных в настоящее время простых чисел имеют вид

$$2^{24036583}-1, \quad 2^{25964951}-1, \quad 2^{30402457}-1, \quad 2^{32582657}-1.$$

Большее из них записывается 9808358 цифрами. Оно было найдено в сентябре 2006г. Следить за достижениями в этой области можно в Интернете по адресу http://primes.utm.edu/largest.html .

Утверждение о существовании сколь угодно больших простых чисел, или, что то же самое, о бесконечности множества простых чисел называется теоремой Евклида[2].

Теорема 1.2. *Множество простых чисел бесконечно.*

Теорема 1.3 (Основная теорема арифметики)**.** *Каждое целое число, большее единицы, раскладывается в произведение простых чисел и притом единственным способом, если не учитывать порядок сомножителей.*

Теорема утверждает, что два произведения простых чисел могут быть равны друг другу лишь в случае, если они имеют одинаковые сомножители и, возможно, отличаются порядком их следования.

Среди простых сомножителей, присутствующих в разложении $n = p_1 \cdots p_r$ могут быть и одинаковые. Например, $25 = 5 \cdot 5 = 5^2$. Их можно объединить вместе, воспользовавшись операцией возведения в степень. Кроме того, простые сомножители можно упорядочить по величине. В результате получается разложение

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \qquad p_1 < p_2 < \ldots < p_k.$$

Такое представление числа называется *каноническим разложением* на простые сомножители. Например, каноническое разложение числа 2520 имеет вид $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

[2]Теорема о простых числах содержится в IX книге "Начал" Евклида. По некоторым косвенным данным предполагается, что он жил в Александрии в III веке до нашей эры.

Набор различных простых чисел, а также набор показателей степени α_j определяются по числу n единственным способом. Для *кратности вхождения* простого числа p в каноническое разложение числа n будет использоваться обозначение $\nu_p(n)$. Если n не делится на простое p, будем считать $\nu_p(n) = 0$. Например,

$$\nu_2(2520) = 3, \qquad \nu_3(2520) = 2, \qquad \nu_{11}(2520) = 0.$$

Для любых двух целых чисел a, b и простого числа p выполняется равенство

$$\nu_p(ab) = \nu_p(a) + \nu_p(b). \tag{1.6}$$

Отсюда, в частности следует, что *целое число n делится на число d в том и только том случае, если для любого простого числа p выполняются неравенства*

$$\nu_p(d) \leqslant \nu_p(n). \tag{1.7}$$

Разложение на простые сомножители больших чисел — очень трудоемкая задача, в главе 5 мы обсудим некоторые алгоритмы ее решения.

Обозначим символом $\pi(x)$ количество простых чисел p, с условием $p \leqslant x$. Выше с помощью решета Эратосфена установлено, что $\pi(100) = 25$. Ясно, что с ростом x функция $\pi(x)$ возрастает. Теорема 1.3 равносильна утверждению $\pi(x) \to \infty$ при $x \to \infty$.

Впервые достаточно точные границы изменения функции $\pi(x)$ были установлены в 1850г. П.Л. Чебышевым[3].

Теорема 1.4. *При всех достаточно больших x справедливы неравенства*

$$a\frac{x}{\ln x} \leqslant \pi(x) \leqslant b\frac{x}{\ln x}, \tag{1.8}$$

где $a = 0,921\ldots$, $b = 1,105\ldots$.

В настоящее время известны намного более точные неравенства

$$\frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4}, \qquad x \geqslant 55.$$

[3]Русский математик Пафнутий Львович Чебышев, 1821–1894

1.3 Функция Эйлера и ее свойства

Для каждого целого числа $n \geqslant 1$ обозначим символом $\varphi(n)$ количество натуральных чисел, не превосходящих n и взаимно простых с n. Другими словами $\varphi(n)$ есть количество целых чисел k, удовлетворяющих условиям

$$1 \leqslant k \leqslant n, \qquad (k, n) = 1.$$

Так определенную функцию натурального аргумента n называют функцией Эйлера.

В частности, имеем $\varphi(1) = 1$. Для каждого простого числа p имеем $\varphi(p) = p - 1$, а также

$$\varphi(p^r) = p^r - p^{r-1} = p^r \cdot (1 - p^{-1})$$

при любом натуральном r. Свойства функции Эйлера описываются следующей теоремой.

Теорема 1.5. *1. Для любого натурального $n \geqslant 2$ выполняется равенство*

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

2. Функция Эйлера мультипликативна, т.е. для любых двух натуральных взаимно простых чисел a и b имеем

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

3. Для любого натурального n выполняется равенство

$$\sum_{d|n} \varphi(d) = n.$$

1.4 Сравнения

Пусть $m \geqslant 1$ целое число. Два целых числа a и b называются *сравнимыми по модулю m*, если $m|(a - b)$, т.е. если их разность делится на m. Число m называется *модулем* сравнения.

Отношение сравнимости обозначается символом $a \equiv b \pmod{m}$ и обладает следующими легко проверяемыми свойствами.

1. $a \equiv a \pmod{m}$ *для любого целого* a.
2. *Если* $a \equiv b \pmod{m}$, *то* $b \equiv a \pmod{m}$.
3. *Если* $a \equiv b \pmod{m}$ *и* $b \equiv c \pmod{m}$, *то* $a \equiv c \pmod{m}$.
4. *Если* $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, *то*

$$\begin{aligned} a + c &\equiv b + d \pmod{m}, \\ a - c &\equiv b - d \pmod{m}, \\ a \cdot c &\equiv b \cdot d \pmod{m}, \end{aligned}$$

   т.е. сравнения по одному и тому же модулю можно почленно складывать вычитать и умножать.

Из свойства 4 следует также, что к любой из частей сравнения можно прибавить любое целое число, обе части сравнения можно умножить на одно и то же целое число и возвести в одну и ту же натуральную степень. В результате получатся верные сравнения.

В частности, отсюда следует, что если $a \equiv b \pmod{m}$ и $P(x)$ — произвольный многочлен с целыми коэффициентами, то

$$P(a) \equiv P(b) \pmod{m}.$$

Подобное свойство выполняется и для многочленов от нескольких переменных.

Отметим еще несколько свойств сравнений.

5. *Если* $ab \equiv ac \pmod{m}$ *и* $(a, m) = 1$, *то* $b \equiv c \pmod{m}$.
6. *Обе части сравнения и модуль можно умножить на любое отличное от нуля число, т.е. из сравнения* $a \equiv b \pmod{m}$ *при* $d \neq 0$ *следует* $ad \equiv bd \pmod{md}$.

7. *Обе части сравнения и модуль можно разделить на их общий множитель, т.е. из сравнения* $ad \equiv bd \pmod{md}$ *при* $d \neq 0$ *следует* $a \equiv b \pmod{m}$.

8. *Если* $a \equiv b \pmod{m}$, *то* $(a, m) = (b, m)$.

9. *Если* $a \equiv b \pmod{m}$ *и* $d|m$, *то* $a \equiv b \pmod{d}$.

10. *Если сравнение* $a \equiv b$ *имеет место по нескольким модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.*

Свойства сравнений 1–3 означают, что всё множество целых чисел разбивается в объединение непересекающихся подмножеств, состоящих из чисел, попарно сравнимых между собой. Эти подмножества называются *классами вычетов* по модулю m. Элементы каждого из подмножеств называются вычетами этого класса. Класс вычетов, содержащий целое число a будет обозначаться $\overline{a}$. Таким образом, $\overline{a} = \overline{b}$, если и только если $a \equiv b \pmod{m}$. Например, класс вычетов $\overline{0}$ состоит из всех чисел, делящихся на m.

Существует ровно m классов вычетов по модулю m. Каждый из них содержит единственное целое число r из промежутка $0 \leqslant r < m$, называемое *наименьшим неотрицательным вычетом класса*. На множестве классов вычетов по модулю m можно ввести операции сложения, вычитания и умножения по правилам

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} - \overline{b} = \overline{a - b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}. \tag{1.9}$$

Свойство 4 сравнений показывает, что так определенные операции не зависят от выбора представителей классов a и b и действительно являются операциями между классами вычетов. Множество классов вычетов по модулю m с так определенными операциями является коммутативным кольцом — кольцом классов вычетов по модулю m. Оно обозначается $\mathbb{Z}/m\mathbb{Z}$. В этом кольце, вообще говоря, могут быть делители нуля. Например, при $m = 6$ имеем $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$.

Если a — целое число, взаимно простое с модулем m, то найдется целое число b, удовлетворяющее сравнению

$$ab \equiv 1 \pmod{m}. \tag{1.10}$$

Тогда $\overline{a}\overline{b} = \overline{ab} = \overline{1}$ и класс вычетов $\overline{a}$ обратим. Если же $(a, m) > 1$, то, как легко видеть, класс вычетов $\overline{a}$ есть делитель нуля в кольце $\in \mathbb{Z}/m\mathbb{Z}$ и потому обратимым быть не может. Итак, класс вычетов $\overline{a}$ обратим, если и только если $(a, m) = 1$.

По свойству 8 сравнений, если некоторый класс вычетов содержит число a, взаимно простое с модулем, то все вычеты этого класса будут взаимно простыми с модулем. Поэтому среди всех классов вычетов выделяются классы, состоящие из элементов, взаимно простых с модулем. Эти классы имеют вид $\overline{k}$ для $0 \leqslant k < m$ и $(k, m) = 1$. Количество таких чисел k равно $\varphi(m)$, т.е. задаётся функцией Эйлера.

Теорема 1.6. *Множество классов вычетов по модулю m с операциями, определенными равенствами (1.10), образует кольцо с единицей. Группа обратимых элементов этого кольца состоит из $\varphi(m)$ классов, содержащих числа, взаимно простые с модулем.*

В частности, если модуль $m = p$ есть простое число, т.е. $\varphi(m) = p - 1$, то каждый класс вычетов, отличный от $\overline{0}$ имеет обратный в кольце $\mathbb{Z}/p\mathbb{Z}$. Кольцо классов вычетов по простому модулю есть поле. Оно обозначается символами $GF(p)$ или F_p.

Следующее утверждение было доказано в 1760г. Л. Эйлером и носит его имя.

Теорема 1.7. *Для каждого целого числа a, взаимно простого с модулем m, выполняется сравнение*

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

Наименьшее натуральное число d с условием $a^d \equiv 1 \pmod{m}$ называется *показателем числа a* по модулю m. Натуральное число k

удовлетворяет сравнению $a^k \equiv 1 \pmod{m}$ в том и только том случае, когда $d|k$. В частности, $d|\varphi(m)$.

Рассмотрим частный случай теоремы Эйлера, в котором $m = p$ есть простое число. Тогда $\varphi(p) = p - 1$ и получается утверждение, называемое малой теоремой Ферма.

Теорема 1.8. *Если целое число a не делится на простое число p, то*

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

Из этой теоремы следует, что при любом целом a число $a^p - a = a(a^{p-1} - 1)$ делится на p.

1.5 Сравнения с одним неизвестным

Пусть даны целое число $m \geqslant 2$ и многочлен $f(x) = a_n x^n + \ldots + a_1 x + a_0$ с целыми коэффициентами. Говорят, что целое число u удовлетворяет сравнению

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \tag{1.11}$$

если $f(u) \equiv 0 \pmod{m}$. Множество, состоящее из всех целых чисел, удовлетворяющих (1.11), если оно не пусто, представляется в виде объединения нескольких непересекающихся классов вычетов по модулю m. Каждый класс вычетов, состоящий из чисел, удовлетворяющих (1.11), называется *решением сравнения* (1.11), а количество таких классов вычетов, называется *числом решений* этого сравнения. Число решений сравнения (1.11) есть число решений уравнения $f(x) = 0$ в кольце $\mathbb{Z}/m\mathbb{Z}$. При этом коэффициенты многочлена $f(x)$ заменяются их классами вычетов в кольце $\mathbb{Z}/m\mathbb{Z}$.

Согласно малой теореме Ферма каждое целое число удовлетворяет сравнению $x^p - x \equiv 0 \pmod{p}$ при простом p. Поэтому каждый класс вычетов кольца $\mathbb{Z}/p\mathbb{Z}$ есть решение этого сравнения, а число его решений равно p.

Если коэффициент при старшей степени x в (1.11) не делится на m, т.е. $m \nmid a_n$, то говорят, что *степень сравнения* (1.11) равна n.

Каждое сравнение первой степени может быть переписано в виде

$$ax \equiv b \pmod{m}, \qquad m \nmid a. \tag{1.12}$$

Основной результат о таких сравнениях есть

Теорема 1.9. *Сравнение (1.12) разрешимо если и только если, b делится на наибольший общий делитель (a, m). Количество решений в этом случае равно (a, m).*

При решении некоторых задач возникает потребность найти целые числа x, удовлетворяющие одновременно нескольким сравнениям. Как и в случае уравнений при этом говорят, что требуется решить систему сравнений.

Рассмотрим системы сравнений специального вида

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \qquad \cdots\cdots\cdots\cdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \tag{1.13}$$

где $m_i > 0$, a_i — заданные целые числа. Следующее утверждение было известно в Китае примерно 2 тысячелетия назад. В настоящее время оно носит название “китайская теорема об остатках”.

Теорема 1.10. *Если $m_1, \ldots, m_k$ попарно взаимно просты, то система сравнений (1.13) разрешима и имеет единственное решение по модулю $M = m_1 \cdots m_k$.*

Определим целые числа M_i, b_i соотношениями

$$M_i = \frac{M}{m_i}, \quad M_i b_i \equiv a_i \pmod{m_i}, \quad 1 \leqslant i \leqslant k,$$

и положим

$$x_0 = M_1 b_1 + \ldots + M_k b_k. \tag{1.14}$$

Множество целых чисел, удовлетворяющих системе (1.13), составляет класс вычетов $x \equiv x_0 \pmod{M}$.

Заметим, что числа b_i определяются не единственным способом. При использовании теоремы 1.10 для решения систем сравнений, следует выбирать те из них, которые дают по возможности меньшие значения x_0.

Далее рассмотрим сравнения вида

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}, \qquad p \nmid a_n, \tag{1.15}$$

где p — простое число. Следующее утверждение, доказанное Лагранжем в 1768г., носит его имя.

Теорема 1.11. *Сравнение (1.15) имеет не более n решений.*

Заметим, что для составного модуля, даже при $n = 1$, утверждение теоремы может нарушаться, см., например, теорему 1.9.

При решении полиномиальных сравнений часто используются следующие два утверждения.

Теорема 1.12. *Для каждого простого числа p справедливо сравнение*

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-p+1) \pmod{p}, \tag{1.16}$$

т.е. коэффициенты при одинаковых степенях переменной x в левой и правой частях (1.16) сравнимы между собой по модулю p.

Теорема 1.13. *Пусть*

$$f(x) = (x^p - x)g(x) + r(x), \qquad r(x) \in \mathbb{Z}[x], \quad \deg r(x) < p.$$

Тогда множества целых чисел, удовлетворяющих сравнениям

$$f(x) \equiv 0 \pmod{p} \qquad \text{и} \qquad r(x) \equiv 0 \pmod{p},$$

совпадают. Другими словами, каждое сравнение (1.15) можно заменить равносильным ему сравнением степени не превосходящей $p-1$.

Иногда степень сравнения можно еще уменьшить, не изменяя при этом множества решений. Для описания этого способа удобно воспользоваться тем, что кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$ по простому модулю p является полем. Для краткости мы будем обозначать его символом F_p. Из теоремы 1.12 получаем, что в кольце $F_p[x]$ выполняется равенство $x^p - x = x(x-1)\cdots(x-p+1)$. С формальной точки зрения в этом равенстве вместо чисел $1, 2, \ldots, p-1$ должны были бы стоять классы вычетов $\overline{1}, \overline{2}, \ldots, \overline{p-1}$, но для краткости записи мы черточки не ставим.

При любом простом p в кольце многочленов $F_p[x]$, выполняя деление с остатком, можно вычислять наибольший общий делитель двух многочленов. Этот алгоритм подобен алгоритму Евклида для целых чисел и носит то же название. Наибольший общий делитель многочленов $f(x)$ и $g(x)$ в кольце $F_p[x]$ определен не единственным способом, а с точностью до ненулевого множителя из поля коэффициентов. Как и для целых чисел, будем обозначать его символом $(f(x), g(x))$. При этом будем считать, что многочлен $(f(x), g(x))$ *унитарен*, т.е. его коэффициент при старшей степени x равен 1.

Следующее утверждение позволяет, не нарушая равносильности, понизить степень сравнения больше, чем теорема 1.13.

Теорема 1.14. *Пусть $f(x)$ и $d(x)$ — многочлены с целыми коэффициентами, причем, если рассматривать их как многочлены из кольца $F_p[x]$, то $d(x)$ есть наибольший общий делитель $f(x)$ и $x^p - x$. Тогда множества решений сравнений*

$$f(x) \equiv 0 \pmod{p}, \qquad \text{и} \qquad d(x) \equiv 0 \pmod{p} \tag{1.17}$$

одинаковы.

Конечно, кратности решений уравнений (1.17) могут различаться.

Для выяснения вопроса о разрешимости сравнения второй степени по простому модулю можно использовать так называемые символы Лежандра и Якоби, см. §2.2.

Кольцо $F_p[x]$ имеет много общего с кольцом целых чисел $\mathbb{Z}$. В нем не только выполняется алгоритм Евклида для нахождения наибольшего общего делителя двух многочленов. Например, можно ввести понятие сравнимости многочленов по модулю $m(x) \in F_p[x]$, полагая два многочлена $f(x), g(x) \in F_p[x]$ сравнимыми, если разность $f(x) - g(x)$ делится на $m(x)$. Это свойство можно обозначать символом $f(x) \equiv g(x) \pmod{m(x)}$. Для таких сравнений выполняются свойства, подобные свойствам сравнений из параграфа 1.4.

Аналогию между кольцами $\mathbb{Z}$ и $F_p[x]$ можно продолжить, объединив сравнимые между собой многочлены в классы вычетов, определив на этих классах операции сложения, вычитания, умножения, и рассмотрев кольцо $F_p[x]/(m(x))$ классов вычетов многочленов по модулю $m(x)$. Каждый класс вычетов содержит единственный элемент вида $c_0 + c_1 x + \ldots + c_{d-1} x^{d-1}$, где $d = \deg m(x)$ и $c_j \in F_p$. Так что кольцо классов вычетов конечно и состоит, как легко видеть, из $q = p^d$ элементов. Если многочлен $m(x)$ неприводим, то каждый ненулевой элемент кольца вычетов $F_p[x]/(m(x))$ обратим, и это кольцо есть поле, обозначаемое F_q, где $q = p^d$ и $d = \deg m(x)$. Каждый элемент $\alpha \in F_q$ удовлетворяет равенству $\alpha^q - \alpha = 0$.

Вернемся к кольцу $\mathbb{Z}$ и рассмотрим случай, когда модуль сравнения есть степень простого числа p, т.е. $m = p^k, k \geqslant 2$. Если $f(x)$ — многочлен с целыми коэффициентами и целое число a удовлетворяет сравнению $f(x) \equiv 0 \pmod{p^k}$, то $p^k | f(a)$. Но тогда $p | f(a)$, так что a удовлетворяет сравнению $f(x) \equiv 0 \pmod{p}$. Отсюда можно сделать два заключения.

1. *Если сравнение* $f(x) \equiv 0 \pmod{p}$ *не имеет решений, то ни при каком* $k \geqslant 2$ *сравнение* $f(x) \equiv 0 \pmod{p^k}$ *также не имеет решений.*

2. *Для каждого числа* a*, удовлетворяющего сравнению* $f(x) \equiv 0 \pmod{p^k}$ *найдется решение сравнения* $f(x) \equiv 0 \pmod{p}$*, сравнимое с* a *по модулю* p*.*

Таким образом решение сравнений по модулю, равному степени простого числа p, сводится, во-первых, к выяснению разрешимости сравнения по простому модулю p, и, в случае разрешимости, поис-

ку решений по простому модулю. А во-вторых, к поиску решений сравнения по модулю p^k, сравнимых с фиксированным решением по простому модулю.

Первый шаг будет обсуждаться в главе 3. Второй шаг основан на следующем утверждении.

Теорема 1.15. *Пусть $f(x)$ — многочлен с целыми коэффициентами и x_1 — целое число, удовлетворяющее условиям*

$$f(x_1) \equiv 0 \pmod{p}, \qquad f'(x_1) \not\equiv 0 \pmod{p}.$$

Тогда при любом $k \geqslant 1$ существует единственное решение сравнения $f(x) \equiv 0 \pmod{p^k}$, содержащееся в классе вычетов, состоящем из чисел x, удовлетворяющих сравнению $x \equiv x_1 \pmod{p}$.

Под производной многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0$ в формулировке теоремы понимается многочлен

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1$$

Рассмотрим сравнения вида

$$x^n \equiv a \pmod{p^\alpha}, \tag{1.18}$$

где p — простое нечетное число и α — натуральное. Будем также предполагать, что a — целое число, взаимно простое с p. Следующая теорема дает критерий разрешимости сравнения (1.18).

Теорема 1.16. *В указанных выше условиях сравнение (1.18) разрешимо тогда и только тогда, когда при $d = (n, \varphi(p^\alpha))$ выполняется*

$$a^{\frac{\varphi(p^\alpha)}{d}} \equiv 1 \pmod{p^\alpha}, \tag{1.19}$$

В случае разрешимости сравнение (1.18) имеет в точности d решений.

Решение сравнений по произвольному составному модулю сводится к решению сравнений по модулю, равному степени простого числа.

Теорема 1.17. *Пусть $f(x)$ — многочлен с целыми коэффициентами и $m_1 > 1, \ldots, m_k > 1$ — попарно взаимно простые числа. Множества целых чисел, удовлетворяющих сравнению*

$$f(x) \equiv 0 \pmod{m_1 \cdots m_k} \tag{1.20}$$

и системе сравнений

$$f(x) \equiv 0 \pmod{m_1}, \quad \ldots, \quad f(x) \equiv 0 \pmod{m_k} \tag{1.21}$$

совпадают. Если при любом натуральном m символ $T(m)$ обозначает количество решений сравнения $f(x) \equiv 0 \pmod{m}$, то

$$T(m_1 \cdots m_k) = T(m_1) \cdots T(m_k).$$

Пусть $m = p_1^{r_1} \cdots p_k^{r_k}$ — разложение в произведение различных простых чисел. Найдя числа $a_1, \ldots, a_k$, удовлетворяющие сравнениям $f(x) \equiv 0 \pmod{m_j}$ при $m_j = p_j^{r_j}$, $1 \leqslant j \leqslant k$, и выбрав x_0 с помощью равенства (1.14), мы найдем некоторое решение $x_0 \pmod{m}$ сравнения (1.20). Более того, так будут найдены все решения, если каждое из чисел $a_1, \ldots, a_k$ независимо будет пробегать все решения своего сравнения (1.21).

1.6 Первообразные корни и индексы.

При любом натуральном $m \geqslant 2$ группа обратимых элементов кольца $\mathbb{Z}/m\mathbb{Z}$ состоит из $\varphi(m)$ классов, элементы которых взаимно просты с модулем m. Мы будем обозначать эту группу символом $(\mathbb{Z}/m\mathbb{Z})^*$. В настоящем параграфе изучается ее структура.

Пусть a — целое число, взаимно простое с модулем m. Напомним, что наименьшее натуральное число d с условием $a^d \equiv 1 \pmod{m}$ называется показателем числа a по модулю m. На языке теории групп можно сказать, что показатель числа a по модулю m равен порядку элемента $\overline{a}$ в мультипликативной группе $(\mathbb{Z}/m\mathbb{Z})^*$. Заметим, что порядок этой группы равен $\varphi(m)$.

Определение 1.2. *Целое число a, взаимно простое с модулем m, называется первообразным корнем по модулю m, если его показатель равен $\varphi(m)$.*

Первообразный корень по модулю m существует лишь в случае, когда $(\mathbb{Z}/m\mathbb{Z})^*$ — циклическая группа. В 1801 году К.Ф. Гаусс опубликовал два доказательства следующей теоремы.

Теорема 1.18. *Для каждого простого нечетного числа p существуют первообразные корни по модулю p. Количество не сравнимых друг с другом по модулю p первообразных корней равно $\varphi(p-1)$.*

Для нахождения первообразных корней можно пользоваться следующим утверждением.

Теорема 1.19. *Целое число c, не делящееся на простое нечетное p, будет первообразным корнем по модулю p в том и только том случае, если для любого простого числа q, делящего $p-1$, выполняется*

$$c^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}.$$

Если известны все простые делители числа $p-1$, то проверка условий теоремы 1.19 выполняется достаточно быстро с помощью алгоритма, изложенного в параграфе 2.3. Множество первообразных корней при заданном p достаточно велико, поэтому выбирая числа c случайным образом на промежутке $0 < c < p$, можно с большой вероятностью попасть на первообразный корень и доказать это с помощью теоремы 1.19.

Теорема 1.20. *Пусть α — натуральное число, p — простое нечетное и g — первообразный корень по модулю p.*

1. Если

$$p^2 \nmid g^{p-1} - 1, \tag{1.22}$$

то g — первообразный корень по модулю p^α. По крайней мере одно из чисел g или $g+p$ удовлетворяет условию (1.22).

2. Если g нечетно и есть первообразный корень по модулю p^α, то g будет также первообразным корнем по модулю $2p^\alpha$.

Из этой теоремы следует существование первообразных корней по модулям p^α и $2p^\alpha$ при любом простом нечетном p и любом натуральном α. Действительно, если g — первообразный корень по модулю p, то этим свойством будет обладать и число $g+p$. Согласно первому утверждению теоремы 1.20 по крайней мере одно из чисел g, $g+p$ будет первообразным корнем по модулю p^α. Это доказывает существование первообразных корней по модулю p^α. Если g — первообразный корень по модулю p^α, то таким же свойством будет обладать и число $g+p^\alpha$. Но одно из этих двух чисел нечетно. Оно по второму утверждению теоремы 1.20 и будет первообразным корнем по модулю $2p^\alpha$.

Приведенное рассуждение описывает и способ нахождения первообразных корней.

Первообразные корни существуют лишь в случаях, указанных в теореме 1.20, да еще при $m=2$ и $m=4$.

Рассмотрим случаи $m=p^k$ или $m=2p^k$, где p — простое нечетное число и $k\geqslant 1$, в которых, по доказанному, существует первообразный корень. Пусть g — первообразный корень по модулю m. Тогда для любого целого взаимно простого с m числа a существует единственное целое γ, удовлетворяющее условиям

$$a\equiv g^\gamma \pmod m, \qquad 0\leqslant\gamma<\varphi(m).$$

Это число называется *индексом числа* a по основанию g при модуле m и обозначается символом $\operatorname{ind}_g a$ или $\operatorname{ind} a$, если указание на первообразный корень, относительно которого определяется индекс, не существенно. Итак, имеем

$$a\equiv g^{\operatorname{ind}_g a} \pmod m, \qquad 0\leqslant\operatorname{ind}_g a<\varphi(m). \tag{1.23}$$

Свойства индексов описывает следующее утверждение.

Теорема 1.21. *Пусть $m=p^k$ или $m=2p^k$. Тогда*
1) $\operatorname{ind}_g ab\equiv\operatorname{ind}_g a+\operatorname{ind}_g b \pmod{\varphi(m)}$;
2) если a,b — первообразные корни по модулю m, то для любого числа

c, взаимно простого с m, выполняется сравнение

$$\operatorname{ind}_b c \equiv \operatorname{ind}_a c \cdot \operatorname{ind}_b a \pmod{\varphi(m)},$$

причем $(\operatorname{ind}_b a, \varphi(m)) = 1$.

Эта теорема показывает, что свойства индексов напоминают свойства обычных логарифмов от действительных чисел. Поэтому иногда в современной литературе индексы называют дискретными логарифмами, а процесс их нахождения — дискретным логарифмированием. Соответственно вместо $\operatorname{ind}_g a$ при этом используется обозначение $\operatorname{Log}_g a$. Алгоритмам вычисления дискретных логарифмов будет посвящена глава 6.

Перейдем теперь к общему случаю. Пусть $m > 1$ — целое число и

$$m = 2^{\alpha} p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

— разложение в произведение степеней различных простых чисел. Обозначим

$$d = \begin{cases} 1, & \text{если } \alpha \leqslant 1, \\ 2, & \text{если } \alpha \geqslant 2, \end{cases} \qquad d_0 = \begin{cases} 1, & \text{если } \alpha \leqslant 1, \\ 2^{\alpha-2}, & \text{если } \alpha \geqslant 2, \end{cases}$$

$$d_i = \varphi(p_i^{\alpha_i}), \quad i = 1, \dots, r.$$

Заметим, что

$$d \cdot d_0 \cdot d_1 \cdots d_r = 2^{\alpha-1} \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) = \varphi(m) \tag{1.24}$$

при любом $\alpha \geqslant 0$.

Для каждого $i, 1 \leqslant i \leqslant r$, фиксируем некоторый первообразный корень g_i по модулю $p_i^{\alpha_i}$.

Определим также с помощью китайской теоремы об остатках целые числа c_{-1}, c_0 сравнениями

$$\begin{aligned} c_{-1} &\equiv -1 (\bmod 2^{\alpha}), & c_{-1} &\equiv 1 (\bmod p_k^{\alpha_k}), \quad 1 \leqslant k \leqslant r, \\ c_0 &\equiv 5 (\bmod 2^{\alpha}), & c_0 &\equiv 1 (\bmod p_k^{\alpha_k}), \quad 1 \leqslant k \leqslant r, \end{aligned}$$

и c_j для каждого $j = 1, \ldots, r$ сравнениями

$$c_j \equiv g_j (\mathrm{mod}\, p_j^{\alpha_j}), \quad c_j \equiv 1 (\mathrm{mod}\, 2^{\alpha}), \quad c_j \equiv 1 (\mathrm{mod}\, p_k^{\alpha_k}),$$
$$1 \leqslant k \leqslant r, \qquad k \neq j.$$

Из определения чисел $c_{-1}, c_0, \ldots, c_r$ следует, что их показатели равны соответственно $d_{-1}, d_0, \ldots, d_r$.

Теорема 1.22. *Для каждого взаимно простого с m целого числа a существует единственный набор чисел $k_{-1}, k_0, \ldots, k_r$, удовлетворяющих условиям*

$$a \equiv c_{-1}^{k_{-1}} c_0^{k_0} c_1^{k_1} \cdots c_r^{k_r} \pmod{m}, \tag{1.25}$$

$$0 \leqslant k_{-1} < d, \quad 0 \leqslant k_0 < d_0, \quad \ldots, \quad 0 \leqslant k_r < d_r,$$

другими словами, мультипликативная группа $(\mathbb{Z}/m\mathbb{Z})^*$ есть прямое произведение своих циклических подгрупп, порожденных классами вычетов, содержащими числа $c_{-1}, c_0, \ldots, c_r$.

1.7 Цепные дроби

Иногда приходится заменять действительные числа их приближенными значениями. Часто при этом хочется обеспечить необходимую точность, выбирая рациональное приближение по возможности с меньшим знаменателем. Описываемый в этом параграфе алгоритм цепных дробей позволяет находить в некотором смысле наилучшие приближения действительных чисел рациональными.

Пусть α — действительное число. Положим $\alpha_0 = \alpha$ и определим последовательности целых чисел a_k и действительных чисел α_k равенствами

$$a_k = [\alpha_k], \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \qquad k \geqslant 0, \tag{1.26}$$

проводя вычисления, пока это возможно, т.е. до тех пор, пока знаменатель дроби в (1.26) отличен от нуля.

Если α — рациональное число, то последовательность α_k конечна. Для иррациональных чисел эта последовательность всегда бесконечна. Последовательность целых чисел $a_0, a_1, \ldots$ называется *цепной* или *непрерывной* дробью числа α. Такое название связано с легко проверяемым равенством

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k + \cfrac{1}{\alpha_{k+1}}}}}.$$

Для цепной дроби используется обозначение $[a_0; a_1, a_2, \ldots]$. Можно доказать, что для любой бесконечной последовательности целых чисел $a_0, \quad a_1 \geqslant 1, \quad a_2 \geqslant 1, \quad a_3 \geqslant 1, \quad \ldots$ существует единственное число α, цепная дробь которого равна $[a_0; a_1, a_2, \ldots]$. Поэтому пишут $\alpha = [a_0; a_1, a_2, \ldots]$. Каждому рациональному числу также соответствует единственная цепная дробь $[a_0; a_1, a_2, \ldots, a_m]$ с дополнительным условием $a_m > 1$.

Числа a_j называются *неполными частными*, а числа α_j *остатками* цепной дроби числа α. Названия мотивируются равенствами (1.3), из которых следует, что $\frac{a}{b} = [q_1; q_2, \ldots, q_n]$.

Рациональные числа

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k}}}$$

называются *подходящими дробями* числа α. Числители P_k и знаменатели Q_k несократимых представлений подходящих дробей легко мо-

гут быть вычислены с помощью рекуррентных формул

$$\begin{cases} P_k = a_k P_{k-1} + P_{k-2}, & P_{-1} = 1, \quad P_0 = a_0, \\ Q_k = a_k Q_{k-1} + Q_{k-2}, & Q_{-1} = 0, \quad Q_0 = 1. \end{cases} \tag{1.27}$$

При любом $k \geqslant 0$ справедливы неравенства

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k Q_{k+1}}. \tag{1.28}$$

Согласно (1.27), последовательность знаменателей Q_k быстро возрастает с ростом номера k. Поэтому из неравенства (1.28) следует, что подходящие дроби хорошо приближают число α. Эти числа являются в некотором смысле наилучшими, см. главу 7, рациональными приближениями к α.

Формулы (1.26) и (1.27) позволяют вычислять цепную дробь заданного числа и его подходящие дроби. Для этого есть и другой способ. Можно доказать, что a_{k+1} есть наибольшее натуральное число r, для которого дроби $\frac{P_k}{Q_k}$ и

$$\frac{P_{k,r}}{Q_{k,r}} = \frac{rP_k + P_{k-1}}{rQ_k + Q_{k-1}}$$

лежат по разные стороны от числа α. Это свойство позволяет вычислять неполные частные a_{k+1} при $k \geqslant 1$ и с помощью (1.27) находить подходящие дроби. Впрочем, первый способ используется чаще.

Пример. Разложение в цепную дробь числа π имеет вид

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, \ldots] \ . \tag{1.29}$$

Соответствующие подходящие дроби равны

$$3, \quad \frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}, \quad \frac{103993}{33102}, \ldots \ . \tag{1.30}$$

Например,

$$\pi - \frac{355}{113} = -2,6676\ldots \cdot 10^{-7}.$$

Можно доказать, что при всех $n \geqslant 0$ справедливы равенства

$$Q_n P_{n-1} - P_n Q_{n-1} = (-1)^n. \tag{1.31}$$

Из них, в частности, следует, что P_n и Q_n взаимно просты, а дробь $\frac{P_n}{Q_n}$ несократима. Для рационального числа $\frac{a}{b} = [a_0; a_1, \ldots, a_m]$ имеем $\frac{a}{b} = \frac{P_m}{Q_m}$.

Равенство (1.31) позволяет решать диофантовы уравнения вида $ax - by = 1$ при взаимно простых a и b. Если $b > 0$ и $\frac{a}{b} = \frac{P_m}{Q_m}$, причем m нечетно, то $b = Q_m, a = P_m$ и с $x = Q_{m-1}, y = P_{m-1}$ имеем

$$ax - by = P_m Q_{m-1} - Q_m P_{m-1} = (-1)^{m-1} = 1.$$

Зная одно частное решение $x = Q_{m-1}, y = P_{m-1}$ можно найти все решения так, как это объясняется в (1.5).

Рассмотрим следующий

Пример. Решить диофантово уравнение

$$1003x + 298y = 1.$$

Рациональное число $\frac{1003}{298}$ имеет два разложения в цепную дробь $\frac{1003}{298} = [3; 2, 1, 2, 1, 3, 7] = [3; 2, 1, 2, 1, 3, 6, 1]$. Второе из них имеет нечетную длину $m = 7$. Подходящие дроби второго разложения находятся по правилу (1.27)

$$3, \quad \frac{7}{2}, \quad \frac{10}{3}, \quad \frac{27}{8}, \quad \frac{37}{11}, \quad \frac{138}{41}, \quad \frac{865}{257}, \quad \frac{1003}{298}.$$

В соответствии с указанным правилом находим $1003 \cdot 257 - 298 \cdot 865 = 1$. Значит, данное уравнение имеет решение $x = 257, y = -865$, а общее его решение имеет вид $x = 257 + 298k = -41 + 298(k+1), y = -865 - 1003k = 138 - 1003(k+1), k \in \mathbb{Z}$. Оно же может быть записано в виде $x = -41 + 298\ell, y = 138 - 1003\ell$, $\ell \in \mathbb{Z}$. Здесь использована замена $\ell = k + 1$.

Теорема 1.23. *Пусть $[a_0; a_1, a_2, \ldots]$ — конечная или бесконечная цепная дробь с целыми неполными частными, причем $a_n \geqslant 1$ при*

$n \geqslant 1$. Тогда имеют место следующие утверждения.
1. Последовательность подходящих дробей с четными номерами возрастает, последовательность подходящих дробей с нечетными номерами убывает, любая подходящая дробь нечетного порядка больше любой подходящей дроби четного порядка и число α, соответствующее данной непрерывной дроби, лежит между ними;
2. Если цепная дробь бесконечна, то

$$\alpha = \lim_{n\to\infty} \frac{P_n}{Q_n},$$

причем α — иррациональное число;
3. При всех $k \geqslant 0$ справедливы равенства

$$\alpha = \frac{\alpha_{k+1}P_k + P_{k-1}}{\alpha_{k+1}Q_k + Q_{k-1}}, \tag{1.32}$$

$$Q_k\alpha - P_k = \frac{(-1)^k}{\alpha_{k+1}Q_k + Q_{k-1}}. \tag{1.33}$$

$$a_{k+1} = \left[-\frac{Q_{k-1}\alpha - P_{k-1}}{Q_k\alpha - P_k} \right], \qquad a_0 = [\alpha]. \tag{1.34}$$

Пример. С помощью формул (1.27) и (1.34) находим разложение числа π в цепную дробь (1.29) и последовательность подходящих дро-

бей (1.30). Напомним, что $P_{-1} = 1, Q_{-1} = 0$.

$$\begin{aligned}
\alpha &= \pi, & a_0 &= [\pi] = 3,\\
P_0 &= 3, & Q_0 &= 1,\\
\alpha_1 &= \frac{1}{\pi - 3}, & a_1 &= [\alpha_1] = 7,\\
P_1 &= 7 \cdot 3 + 1 = 22, & Q_1 &= 7 \cdot 1 + 0 = 7,\\
\alpha_2 &= \frac{\pi - 3}{22 - 7\pi}, & a_2 &= [\alpha_2] = 15,\\
P_2 &= 15 \cdot 22 + 3 = 333, & Q_2 &= 15 \cdot 7 + 1 = 106,\\
\alpha_3 &= \frac{22 - 7\pi}{106\pi - 333}, & a_3 &= [\alpha_3] = 1,\\
P_3 &= 1 \cdot 333 + 22 = 355, & Q_3 &= 1 \cdot 106 + 7 = 113,\\
&\ldots\ldots & &\ldots\ldots
\end{aligned}$$

Пример. Найдем непрерывную дробь числа $\frac{1+\sqrt{17}}{2}$ и первые пять его подходящих дробей. В соответствии с формулами (1.26) получаем

$$\begin{aligned}
\alpha_0 &= \frac{1+\sqrt{17}}{2}, & a_0 &= [\alpha_0] = 2,\\
\alpha_1 &= \frac{1}{\alpha_0 - 2} = \frac{2}{\sqrt{17} - 3} = \frac{\sqrt{17}+3}{4}, & a_1 &= [\alpha_1] = 1,\\
\alpha_2 &= \frac{1}{\alpha_1 - 1} = \frac{4}{\sqrt{17} - 1} = \frac{\sqrt{17}+1}{4}, & a_2 &= [\alpha_2] = 1,\\
\alpha_3 &= \frac{1}{\alpha_2 - 1} = \frac{4}{\sqrt{17} - 3} = \frac{\sqrt{17}+3}{2}, & a_3 &= [\alpha_3] = 1,\\
\alpha_4 &= \frac{1}{\alpha_3 - 3} = \frac{2}{\sqrt{17} - 3} = \frac{\sqrt{17}+3}{4} = \alpha_1, & a_4 &= [\alpha_4] = 1.
\end{aligned}$$

В формулах (1.26) каждое число α_{n+1} однозначно определяется по числу α_n. Поэтому совпадение $\alpha_4 = \alpha_1$ означает, что будут выполнены равенства $\alpha_5 = \alpha_2$, $\alpha_6 = \alpha_3$ и так далее, т.е. последовательность a_n в

данном случае будет периодической. Имеем

$$\frac{1+\sqrt{17}}{2} = [2; 1, 1, 3, 1, 1, 3, 1, 1, 3, \ldots] = [2; \overline{1, 1, 3}].$$

Цепная дробь числа $\frac{1+\sqrt{17}}{2}$ состоит из повторяющихся блоков $1, 1, 3$.

Равенства (1.27) могут быть переписаны в матричном виде

$$\begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}.$$

Это позволяет организовать вычисление подходящих дробей, начиная с $n = 1$, следующим образом:

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}, \quad \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 23 & 18 \\ 9 & 7 \end{pmatrix}, \ldots$$

В результате находим следующие приближения

$$\frac{2}{1}, \quad \frac{3}{1}, \quad \frac{5}{2}, \quad \frac{18}{7}, \quad \frac{23}{9}, \quad \frac{41}{16}, \quad \frac{146}{57}, \ \ldots$$

Заметим, что

$$\frac{1+\sqrt{17}}{2} - \frac{41}{16} = -0.000947187\ldots.$$

Цепная дробь $[a_0; a_1, a_2, \ldots]$ называется *периодической*, если последовательность a_n, начиная с некоторого места, периодична, т.е. для некоторого целого k при всех достаточно больших n выполняется равенство $a_{n+k} = a_n$. Периодические дроби будут обозначаться

$$[\ a_0; a_1, \ldots, a_h, \overline{a_{h+1}, \ldots, a_{h+k}}\ ],$$

где $a_{h+1}, \ldots, a_{h+k}$ — период. Свойство периодичности характерно для цепных дробей так называемых действительных квадратичных иррациональностей. Число α называется *квадратичной иррациональностью*, если оно не рационально и есть корень квадратного трехчлена

$f(x) = ax^2 + bx + c$ с целыми коэффициентами a, b, c. Число $\frac{1+\sqrt{17}}{2}$ есть квадратичная иррациональность, ведь оно — корень многочлена $x^2 - x - 4$.

Теорема 1.24. *Пусть α — действительное иррациональное число. Цепная дробь α периодична тогда и только тогда, когда α — квадратичная иррациональность.*

Тот факт, что периодическим цепным дробям соответствуют квадратичные иррациональности был обнаружен Эйлером. Спустя 30 лет Лагранж доказал обратное утверждение.

1.8 p-адические числа

Так называемые p-адические числа, представляющие собой удобный язык для обсуждения различных свойств сравнений, выполняющихся по большой степени простого числа.

На поле рациональных чисел $\mathbb{Q}$ определено обычное абсолютное значение $|\ \ |$. Пополнением $\mathbb{Q}$ относительно этого абсолютного значения является поле действительных чисел $\mathbb{R}$.

Пусть p — простое число. Для каждого целого a будем обозначать символом $\nu_p(a)$ кратность, с которой p входит в разложение a на простые сомножители. Если $r = \frac{a}{b}$, $a, b \in \mathbb{Z}$, положим $\nu_p(r) = \nu_p(a) - \nu_p(b)$. Эта величина не зависит от представления r в виде отношения двух чисел. Будем также считать по определению $\nu_p(0) = +\infty$.

Для любых двух чисел $r_1, r_2 \in \mathbb{Q}$, $r_i \neq 0$, имеем

$$\nu_p(r_1 \cdot r_2) = \nu_p(r_1) + \nu_p(r_2), \qquad \nu_p(r_1 + r_2) \geqslant \min(\nu_p(r_1)\,,\ \nu_p(r_2)).$$

Определим теперь для любого рационального числа r его p-адическую абсолютную величину равенством

$$|r|_p = \begin{cases} p^{-\nu_p(r)}, & \text{если } r \neq 0; \\ 0, & \text{если } r = 0. \end{cases}$$

Так определенная абсолютная величина обладает свойствами:

1. $|r_1 \cdot r_2|_p = |r_1|_p \cdot |r_2|_p$,
2. $|r_1 + r_2|_p \leqslant \max(|r_1|_p,\ |r_2|_p)$,
3. $|r|_p = 0 \Leftrightarrow r = 0$.

В частности, при любом натуральном n выполняется неравенство

$$| n |_p = | \underbrace{1 + \ldots + 1}_{n} | \leqslant 1.$$

Значит, для p-адического абсолютного значения нарушается аксиома Архимеда. Такие абсолютные значения называются неархимедовыми.

Пополнение поля $\mathbb{Q}$ относительно p-адического абсолютного значения называется полем p-адических чисел. Оно обозначается символом $\mathbb{Q}_p$. Элементами поля $\mathbb{Q}_p$ являются классы эквивалентных последовательностей Коши, состоящих из рациональных чисел. Две последовательности Коши $\{a_n\}$ и $\{b_n\}$, состоящие из рациональных чисел, эквивалентны, если $|a_n - b_n|_p \to 0$ при $n \to \infty$.

Примеры. 1. Последовательность $x_n = 5^n$ стремится к нулю в поле 5-адических чисел $\mathbb{Q}_5$.

2. Пусть $p = 3$ и $x_n = 1 + 3 + \ldots + 3^n$. Так как $x_n = \frac{3^{n+1}-1}{2}$, то $\left| x_n + \frac{1}{2} \right|_p = 3^{-n-1}$ и $x_n \to -\frac{1}{2}$. Иначе говоря, ряд $1 + 3 + 3^2 + \ldots$ сходится в поле $\mathbb{Q}_3$. Его сумма равна $-\frac{1}{2}$.

3. Каждое рациональное число $\frac{a}{b}$ с целыми a, b, порождает последовательность Коши $x_n = \frac{a}{b}$. Класс эквивалентности этой последовательности, естественно, отождествить с числом $\frac{a}{b}$ и считать, что $\mathbb{Q} \subset \mathbb{Q}_p$.

4. Последовательность $x_n \in \mathbb{Q}_p$ есть последовательность Коши в $\mathbb{Q}_p$ если и только если $\lim\limits_{n\to\infty} (x_{n+1} - x_n) = 0$.

5. Ряд $\sum\limits_{n=1}^{\infty} a_n$, $a_n \in \mathbb{Q}_p$, сходится в $\mathbb{Q}_p$ в том и только том случае,

когда $\lim\limits_{n\to\infty} a_n = 0$. Так

$$1 + p + p^2 + \ldots = \frac{1}{1-p}$$

в поле $\mathbb{Q}_p$. Причина столь простого, по сравнению с действительным случаем, признака сходимости кроется в том, что p-адическое абсолютное значение неархимедово.

6. Пусть $\dfrac{a}{b}$ — рациональное число $a, b \in \mathbb{Z}$, $b > 0$, $p \nmid b$. Из последнего условия согласно малой теореме Ферма находим $p^{\varphi(b)} \equiv 1 \pmod{b}$. Определим целое число c равенством $p^{\varphi(b)} - 1 = bc$ а также целые числа A и B условиями

$$ac = A\left(p^{\varphi(b)} - 1\right) - B, \qquad 0 \leqslant B < p^{\varphi(b)} - 1.$$

Тогда

$$\frac{a}{b} = \frac{ac}{p^{\varphi(b)} - 1} = A + \frac{B}{1 - p^{\varphi(b)}} = A + \sum_{k=0}^{\infty} B \cdot p^{k\varphi(b)}.$$

Если

$$B = b_0 + b_1 p + \cdots + b_{r-1} p^{r-1}, \qquad r = \varphi(b), \quad 0 \leqslant b_j < p,$$

то

$$\frac{a}{b} = A + \left(\overline{b_0, b_1, \ldots, b_{r-1}} \right).$$

Целое число A можно прибавить к бесконечной сумме в последнем равенстве, перенося и прибавляя единицы в разрядах так же, как это делается в случае бесконечных десятичных дробей.

Таким образом, каждое рациональное число $\dfrac{a}{b}$ с условиями $b > 0, p \nmid b$ представимо в виде бесконечной суммы в $\mathbb{Q}_p$ с целыми периодически повторяющимися, начиная с некоторого места, коэффициентами $b_j, 0 \leqslant b_j < p$. Например,

$$-1 = \frac{p-1}{1-p} = \sum_{k=0}^{\infty} (p-1)p^k \in \mathbb{Q}_p.$$

Любое рациональное число может быть записано в виде $p^k \cdot \dfrac{a}{b}$, где a, b целые, $b > 0$ и $p \nmid b, p \nmid a$. Оно также представимо в виде $p^k \cdot \big(a_0, a_1, \ldots, a_s, \overline{b_0, b_1, \ldots, b_{r-1}}\big)$.

Теорема 1.25. *Каждое p-адическое число α имеет единственное представление в виде сходящегося ряда*

$$\alpha = p^m(a_0 + a_1 p + a_2 p^2 + \ldots), \qquad m \in \mathbb{Z}, \quad a_j \in \mathbb{Z}, \quad 0 \leqslant a_j < p.$$

При этом равенство $|\alpha|_p = p^{-m}$ продолжает p-адическое абсолютное значение, сохраняя свойства (1.8), с поля рациональных чисел на $\mathbb{Q}_p$.

Будет также использоваться обозначение $m = \nu_p(\alpha)$.

Обозначим $\mathbb{Z}_p$ множество, состоящее из всех p-адических чисел, норма которых не превосходит 1. Для любых двух чисел $x_1, x_2 \in \mathbb{Z}_p$ имеем $|x_1|_p \leqslant 1$, $|x_2|_p \leqslant 1$, так что

$$|x_1 + x_2|_p \leqslant \max(|x_1|_p\ ,\ |x_2|_p) \leqslant 1, \quad |x_1 \cdot x_2|_p = |x_1|_p \cdot |x_2|_p \leqslant 1. \quad (1.35)$$

Следовательно $\mathbb{Z}_p$ есть кольцо. Его называют кольцом целых p-адических чисел. Имеет место включение $\mathbb{Z} \subset \mathbb{Z}_p$.

Пример. Число $\dfrac{1}{2}$ есть целое 3-адическое число, но не целое 2-адическое.

Для целых p-адических чисел α выполняется неравенство $\nu_p(\alpha) \geqslant 0$. Следующая лемма описывает множество обратимых элементов кольца целых p-адических чисел.

Лемма 1.1. *Если $\alpha \in \mathbb{Q}_p$ и $|\alpha|_p = 1$, то $\alpha^{-1} \in \mathbb{Z}_p$.*

Доказательство. Из условия следует, что число α представимо рядом

$$\alpha = a_0 + a_1 p + a_2 p^2 + \ldots, \qquad a_j \in \mathbb{Z}, \quad 0 \leqslant a_j < p, \quad a_0 \neq 0.$$

Определим последовательность целых чисел $x_n = a_0 + a_1 p + \ldots + a_{n-1} p^{n-1}$. Вторая последовательность целых чисел y_n определяется условиями

$$x_n y_n \equiv 1 \pmod{p^n}, \qquad 0 \leqslant y_n < p^n. \quad (1.36)$$

Из равенства

$$x_n(y_{n+1} - y_n) = (x_{n+1}y_{n+1} - 1) - (x_n y_n - 1) - y_{n+1}(x_{n+1} - x_n)$$

следует $\nu_p(x_n(y_{n+1} - y_n)) \geqslant n$. Поскольку $a_0 \neq 0$, находим отсюда $\nu_p(y_{n+1} - y_n) \geqslant n$ или $y_{n+1} \equiv y_n \pmod{p^n}$. Следовательно y_n есть последовательность Коши в $\mathbb{Q}$ и определяет некоторое p-адическое число. Если $y_n = b_0 + b_1 p + \ldots + b_{n-1}p^{n-1}$, $0 \leqslant b_j < p$, то для $\beta = b_0 + b_1 p + b_2 p^2 + \ldots \in \mathbb{Z}_p$ с помощью сравнения (1.36) находим $\alpha\beta = 1$ и $\alpha^{-1} = \beta \in \mathbb{Z}_p$. □

В кольце $\mathbb{Z}_p$ можно рассматривать сравнения. Для любых $x, y, z \in \mathbb{Z}_p$ будем писать $x \equiv y \pmod{z}$, если $\nu_p(x - y) \geqslant \nu_p(z)$ или иначе $|x-y|_p \leqslant |z|_p$. Из свойств 1.35 легко следует, что сравнения по одному модулю можно почленно складывать, вычитать и перемножать.

Лемма 1.2. *Пусть b — натуральное число и $x \in \mathbb{Z}_p$. Тогда в кольце $\mathbb{Z}_p$ выполняется сравнение*

$$(1 + x)^b \equiv 1 + bx \pmod{pbx},$$

если $\nu_p(x) \geqslant 1$ и p нечетно или, если $p = 2$ и $\nu_2(x) \geqslant 2$. При $\nu_2(x) = 1$ выполняется сравнение $(1 + x)^b \equiv 1 \pmod{bx}$.

Доказательство. Пользуясь формулой Ньютона для бинома, находим

$$(1+x)^b = \sum_{k=0}^{b} \frac{b!}{k!(b-k)!}x^k = 1 + bx + \sum_{k=2}^{b} \frac{b}{k} \cdot \binom{b-1}{k-1}x^k = \\ = 1 + bx + bx\sum_{k=2}^{b} \binom{b-1}{k-1}\frac{x^{k-1}}{k}.$$

Предположим сначала, что p есть простое нечетное число. Тогда в силу неравенств $\nu_p(k) \leqslant k - 2$, выполняющихся при $k \geqslant 2$, находим

$$\nu_p\left(\frac{x^{k-1}}{k}\right) = (k-1)\nu_p(x) - \nu_p(k) \geqslant (k-1) - (k-2) = 1.$$

Это доказывает нужное сравнение.

Если $p = 2$ и $\nu_p(x) \geqslant 2$, имеем при $k \geqslant 2$

$$\nu_2\left(\frac{x^{k-1}}{k}\right) = (k-1)\nu_2(x) - \nu_2(k) \geqslant 2(k-1) - \log_2 k \geqslant 1.$$

Наконец, в случае $p = 2$ и $\nu_p(x) = 1$ при $k \geqslant 2$ имеем

$$\nu_2\left(\frac{x^{k-1}}{k}\right) = (k-1)\nu_2(x) - \nu_2(k) \geqslant k - 1 - \log_2 k \geqslant 0$$

и это доказывает последнее утверждение леммы. □

Пример. Пусть $x_n = 2^{5^n},\ n \geqslant 0$. Тогда

$$x_{n+1} - x_n = 2^{5^n}\left(2^{4\cdot 5^n} - 1\right) \equiv 0 \pmod{5^{n+1}}.$$

Сравнение выполняется по теореме Эйлера, ведь $\varphi(5^{n+1}) = 4 \cdot 5^n$. Это сравнение можно переписать иначе в виде $|x_{n+1} - x_n|_p \leqslant 5^{-n-1}$. Таким образом, последовательность x_n есть последовательность Коши и существует предел $\lim\limits_{n\to\infty} x_n = c \in \mathbb{Q}_5$. Пользуясь леммой 1.2, находим

$$x_n^2 = 4^{5^n} = -(1-5)^{5^n} \equiv -1 + 5^{n+1} \pmod{5^{n+2}}.$$

Поэтому $|x_n^2+1|_5 = 5^{-n-1}$, так что $x_n^2+1 \to 0$. Следовательно, $c^2+1 = 0$, и уравнение $x^2 + 1 = 0$ разрешимо в поле $\mathbb{Q}_5$.

Далее мы определим некоторые функции на множестве p-адических чисел и рассмотрим ряд их свойств.

1.8.1 Логарифмическая функция

Эта функция определяется рядом

$$L_p(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1}\frac{x^n}{n}. \tag{1.37}$$

Теорема 1.26. *Ряд (1.37) сходится при любом $x \in \mathbb{Z}_p$, $|x|_p < 1$. Кроме того, для любых $u, v \in \mathbb{Z}_p$ с условиями $|u-1|_p < 1$, $|v-1|_p < 1$ выполняется равенство*

$$L_p(uv) = L_p(u) + L_p(v).$$

Доказательство. При любом натуральном k справедливо неравенство $|k|_p \geqslant k^{-1}$. Поэтому при $|x|_p < 1$ имеем

$$\left|\frac{x^k}{k}\right|_p = \frac{|x|_p^k}{|k|_p} \leqslant k|x|_p^k \ \to 0, \quad \text{при} \quad k \to \infty.$$

Это означает сходимость ряда (1.37).

Для доказательства второго утверждения теоремы понадобится следующее вспомогательное утверждение.

Лемма 1.3. *Пусть N — натуральное число и многочлен $P(z)$ определен равенством*

$$P(z) = \sum_{n=1}^{N} (-1)^{n-1} \frac{z^n}{n}.$$

Тогда справедливо тождество

$$P(z) + P(y) - P(y + z + yz) = \sum_{i+j>N} c_{i,j} y^i z^j, \tag{1.38}$$

где $c_{i,j}$ — рациональные числа, знаменатели которых не превосходят N.

Доказательство. Рассмотрим многочлен $F(y, z) = P(y + z + yz) - P(y) - P(z)$. Пусть $cy^k z^\ell$ — моном, входящий в этот многочлен с ненулевым коэффициентом c. В силу симметрии по переменным y, z многочлен $F(y, z)$ содержит также моном $cy^\ell z^k$. Так как $F(0, 0) = 0$, то $k+\ell > 0$. Кроме того, $k, \ell \leqslant N$. Для частной производной многочлена

$F(y,z)$ по переменной y имеем следующее выражение

$$F'_y(y,z) = (1+z)\sum_{k=1}^{N}(-1)^{n-1}(y+z+yz)^{n-1} - \sum_{k=1}^{N}(-1)^{n-1}y^{n-1} =$$
$$(-1)^{N-1}\frac{(y+z+yz)^N - y^N}{1+y} = (-1)^{N-1}z\sum_{i+j=N-1} y^i(y+z+yz)^j.$$

Получившийся многочлен не содержит мономов степени, меньшей N. Но он должен содержать мономы $kcy^{k-1}z^\ell$ и $\ell cy^{\ell-1}z^k$. Поэтому должно выполняться неравенство $k+\ell-1 \geqslant N$ и $k+\ell > N$. Кроме того, из включений $kc \in \mathbb{Z}$, $\ell c \in \mathbb{Z}$ следует, что знаменатель числа c не превосходит N. □

Причиной тождества (1.38), конечно, является аналогичное тождество для степенных рядов

$$\ln(1+y) + \ln(1+z) = \ln((1+y)(1+z)) = \ln(1+y+z+yz).$$

Докажем второе утверждение теоремы. Согласно условию величина $\rho = \max(|u-1|_p\ ,\ |v-1|_p)$ удовлетворяет неравенствам $0 \leqslant \rho < 1$. Выберем достаточно большое целое число N и подставим в тождество (1.38) $y = u-1$ и $z = v-1$. Согласно утверждению леммы выполняются неравенства $|c_{i,j}|_p < N$. Поэтому

$$|P(u-1) + P(v-1) - P(uv-1)|_p \leqslant N\cdot\rho^{N+1}. \qquad (1.39)$$

Перейдем в этом неравенстве к пределу при $N \to \infty$. В силу сходимости рядов $L_p(u)$, $L_p(v)$ и $L_p(uv)$ заключаем, что $P(u-1) \to L_p(u)$, $P(v-1) \to L_p(v)$, $P(uv-1) \to L_p(uv)$. Теперь из (1.39) получаем второе утверждение теоремы 1.26. □

Теорема 1.27. *Если $x \in \mathbb{Z}_p$, $|x|_p < 1$, то справедливы сравнения*

$$L_p(1+x) \equiv x \pmod{x^2} \quad \textit{при} \quad p \geqslant 3,$$

и

$$L_2(1+x) \equiv x \pmod{x^2/2}.$$

В частности, $|L_p(1+x)|_p = |x|_p$ *при* $p \geqslant 3$. *Если же* $p = 2$, *то* $|L_2(1+x)|_2 = |x|_2$ *при* $\nu_2(x) \geqslant 2$ *и* $|L_2(1+x)|_2 \leqslant |x|_2$ *при* $\nu_2(x) = 1$.

Доказательство. Предположим сначала, что p простое нечетное число. При $k = 2$, очевидно, имеем $\nu_p(x^{k-2}/k) = 0$. Если же $k \geqslant 3$, то

$$\nu_p\left(\frac{x^{k-2}}{k}\right) = (k-2)\nu_p(x) - \nu_p(k) \geqslant k - 2 - \log_p k \geqslant k - 2 - \log_3 k \geqslant 0.$$

Это в силу равенства

$$L_p(1+x) = x + x^2 \sum_{k=2}^{\infty} (-1)^{k-1} \frac{x^{k-2}}{k}.$$

доказывает первое сравнение.

При p=2 для $k = 2,\ 3$, очевидно, имеем $\nu_2(x^{k-2}/k) \geqslant -1$. Далее для $k \geqslant 4$ получаем

$$\nu_2\left(\frac{x^{k-2}}{k}\right) \geqslant k - 2 - \log_2 k \geqslant -1.$$

Это доказывает второе сравнение.

Утверждения теоремы об абсолютной величине p-адических логарифмов сразу же следуют из доказанных сравнений. □

Следствие 1.1. *Пусть* $u \in \mathbb{Z}_p$, $\nu_p(u-1) \geqslant 1$.
1. При $p \geqslant 3$ *равенство* $L_p(u) = 0$ *выполняется только для* $u = 1$.
2. Равенству $L_2(u) = 0$ *удовлетворяют только два числа* $u = \pm 1$.

Доказательство. Равенство $L_p(1) = 0$, очевидно, выполняется при любом простом $p \geqslant 2$. Так как $-1 = 1 - 2$, то логарифм $L_2(-1)$ определен. По теореме 1.26 находим $2L_2(-1) = L_2(1) = 0$. Поэтому $L_2(-1) = 0$.

Докажем теперь утверждения в обратную сторону. В первом случае, согласно теореме 1.27 находим

$$0 = L_p(u) \equiv u - 1 \pmod{(u-1)^2} \tag{1.40}$$

и $|u-1|_p \leqslant |u-1|^2$. Это неравенство совместно с $|u-1|_p < 1$ может выполняться лишь для $u = 1$.

Далее будем считать, что $u \neq \pm 1$. Так как каждое нечетное число сравнимо по модулю 4 либо с 1, либо с -1, то возможны два варианта $u = 1+c2^r$ или $u = -1+c2^r$, где $r \geqslant 2$ и $2 \nmid c$. В первом случае имеем по теореме 1.27 $0 = L_2(u) \equiv u - 1 \pmod{2^{2r-1}}$, т.е. $c2^r \equiv 0 \pmod{2^{2r-1}}$. Но это невозможно, так как $2 \nmid c$. Во втором случае находим

$$0 = L_2(-1 + c2^r) = L_2(-1) + L_2(1 - c2^r) = \\ = L_2(1 - c2^r) \equiv -c2^r \pmod{2^{2r-1}}.$$

Как и в предыдущем случае, это сравнение невозможно. Утверждение доказано. □

Следствие 1.2. *При простом $p \geqslant 3$ уравнение $x^p = 1$ имеет в поле $\mathbb{Q}_p$ единственное решение $x = 1$. Если же $p = 2$, этому уравнению удовлетворяют два 2-адических числа $x = \pm 1$.*

Доказательство. Из равенства $x^p = 1$ следует $|x|_p^p = |x^p|_p = |1|_p = 1$, так что $|x|_p = 1$ и x есть целое p-адическое число. Кроме того, отсюда следует, что в представлении $x = a_0 + a_1 p + \ldots$, $0 \leqslant a_j < p$, первый коэффициент a_0 отличен от нуля. Но тогда по малой теореме Ферма

$$a_0 \equiv a_0^p \equiv x^p = 1 \pmod{p}.$$

Это значит, что определена величина $L_p(x)$ и $pL_p(x) = L_p(x^p) = L_p(1) = 0$. Итак, $L_p(x) = 0$. Теперь следствие 1.1 дает нам $x = 1$ при $p \geqslant 3$ и $x = \pm 1$ при $p = 2$. □

1.8.2 Показательная функция

Пусть a, x — целые p-адические числа, причем $|a-1|_p < 1$ и $x = c_0 + c_1 p + c_2 p^2 + \ldots$, где $c_k \in \mathbb{Z}, 0 \leqslant c_k < p$. Рассмотрим последовательности $x_n = c_0 + c_1 p + \ldots + c_n p^n \in \mathbb{Z}$ и $y_n = a^{x_n} \in \mathbb{Z}_p$ при $n \geqslant 0$. Имеем

$$y_{n+1} - y_n = a^{x_n}\left(a^{c_n p^n} - 1\right) \equiv 0 \pmod{(a-1)p^n}.$$

Сравнение выполняется в силу леммы 1.2. Таким образом, $|y_{n+1} - y_n|_p \leqslant p^{-n-1}$, и последовательность y_n есть последовательность Коши. Учитывая полноту $\mathbb{Q}_p$, заключаем, что последовательность y_n имеет предел в поле $\mathbb{Q}_p$, т.е. $y_n \to b \in \mathbb{Q}_p$. Определим теперь

$$a^x = b.$$

Докажем некоторые свойства показательной функции a^x.

1. Если последовательность целых чисел u_n стремится в $\mathbb{Q}_p$ к некоторому p-адическому числу x, то $a^{u_n} \to a^x$. Действительно, используя определенную выше последовательность x_n, с помощью леммы 1.2 находим $a^{x_n - u_n} \equiv 1 \pmod{(x_n - u_n)(a-1)}$, так что

$$|a^{x_n} - a^{u_n}|_p = |a^{x_n - u_n} - 1|_p \leqslant |x_n - u_n|_p \cdot |a-1|_p < |x_n - u_n|_p.$$

Учитывая, что $|x_n - u_n|_p \leqslant \max(|x_n - x|_p\ ,\ |u_n - x|_p)$, заключаем, что

$$|a^x - a^{u_n}|_p \leqslant \max\left(|a^x - a^{x_n}|_p\ ,\ |u_n - x|_p\ ,\ |x_n - x|_p\right).$$

Поэтому $a^{u_n} \to a^x$.

2. Пусть $u, v \in \mathbb{Z}_p$ и u_n, v_n — последовательности целых чисел, сходящиеся к u и v соответственно. Тогда $u_n + v_n \to u + v$ и, так как $a^{u_n + v_n} = a_{u_n} a^{v_n}$, то, переходя в этом равенстве к пределу при $n \to \infty$, заключаем

$$a^{u+v} = a^u \cdot a^v.$$

3. Докажем, что при любом $x \in \mathbb{Z}_p$ и $a \in \mathbb{Z}_p, |a-1|_p < 1$ выполняется неравенство

$$|a^x - 1| \leqslant |(a-1)x|_p. \tag{1.41}$$

Пусть x_n — последовательность целых чисел, определенная выше для числа x. При всех достаточно больших n, учитывая, что $x_n \to x$, находим

$$|x_n|_p \leqslant \max(|x|_p\ ,\ |x_n - x|_p) \leqslant |x|_p.$$

Теперь из леммы 1.2 следует

$$|a^{x_n} - 1|_p \leqslant |a-1|_p \cdot |x_n| \leqslant |a-1|_p \cdot |x|.$$

Переходя в этом неравенстве к пределу при $n \to \infty$, получаем (1.41). Из этого неравенства при любых $u, v \in \mathbb{Z}_p$ находим

$$|a^u - a^v| = |a^{u-v} - 1|_p \leqslant |a-1|_p \cdot |u-v|_p.$$

В частности, это означает *непрерывность* функции a^x в каждой точке области $|x|_p \leqslant 1$.

Следующее утверждение связывает показательную и логарифмическую функции.

Лемма 1.4. *Если a, x — целые p-адические числа, и $\nu_p(a-1) \geqslant 1$, то*

$$L_p(a^x) = xL_p(a).$$

По условию леммы, а также в силу неравенства (1.41) имеем $|a^x - 1|_p < 1$. Поэтому логарифм $L_p(a^x)$ определен.

Доказательство. Если x — натуральное число, утверждение следует из теоремы 1.26. В общем случае мы воспользуемся тем, что каждое целое p-адическое число может быть с любой точностью в p-адической метрике аппроксимировано целыми натуральными числами. Определим как и ранее последовательность целых чисел x_n условиями $x_n \to x$, $0 \leqslant x_n < p^n$. Тогда

$$|L_p(a^x) - xL_p(a)|_p \leqslant \max(|L_p(a^x) - L_p(a^{x_n})|_p \ , \ |L_p(a^{x_n}) - xL_p(a)|_p).$$

С помощью неравенства (1.41) и теорем 1.26, 1.27 получаем

$$|L_p(a^x) - L_p(a^{x_n})|_p = |L_p(a^{x-x_n})|_p \leqslant |a^{x-x_n} - 1|_p = |a^x - a^{x_n}|_p \to 0$$

при $n \to \infty$. Кроме того

$$|L_p(a^{x_n}) - xL_p(a)|_p = |x_n - x|_p \cdot |L_p(a)| \to 0$$

при $n \to \infty$. □

Теорема 1.28. *Пусть a, b — целые p-адические числа, $a \neq 1$, и*

$$\nu_p(b-1) \geqslant \nu_p(a-1) \geqslant \begin{cases} 1, & \text{при } p \geqslant 3, \\ 2, & \text{при } p = 2. \end{cases}$$

Тогда существует единственное целое p-адическое число x такое, что $a^x = b$. При этом $xL_p(a) = L_p(b)$.

Доказательство. Так как $a \neq 1$ и $\nu_p(a-1) \geqslant 2$ при $p = 2$, то $L_p(a) \neq 0$, см. следствие 1.1.

Определим p-адическое число x равенством $xL_p(a) = L_p(b)$. Пользуясь теоремой 1.27, находим $|L_p(a)|_p = |a-1|_p \geqslant |b-1|_p = |L_p(b)|_p$. Следовательно $|x|_p \leqslant 1$, т.е. $x \in \mathbb{Z}_p$. Далее по лемме 1.4 выполняется $L_p(b) = xL_p(a) = L_p(a^x)$, и согласно теореме 1.26 получаем $L_p(a^x b^{-1}) = 0$. Из неравенств $|b-1|_p < 1$ и $|a^x - 1|_p \leqslant |a-1|_p \cdot |x|_p < 1$ следует, что $a^x, b^{-1} \in \mathbb{Z}_p$ и $|a^x b^{-1} - 1|_p = |a^x - b|_p \leqslant \max(|a^x - 1|_p, |b-1|_p) < 1$. По следствию 1.1 получаем теперь $a^x b^{-1} = 1$ или $a^x = b$.

Если при некотором целом p-адическом x выполняется равенство $a^x = b$, то по лемме 1.4

$$L_p(b) = L_p(a^x) = xL_p(a),$$

так что, число x определяется единственным способом. □

1.9 Алгебраические числа

Алгебраические числа были введены и впоследствии изучались с целью решения задач об обычных целых числах, например решения диофантовых уравнений. В настоящее время с алгебраическими числами связаны наиболее эффективные алгоритмы проверки чисел на простоту, разложения целых чисел на множители, дискретного логарифмирования. Теория алгебраических чисел обширна и не проста. Мы ограничимся в этом параграфе лишь описанием некоторых относящихся к ней фактов.

Комплексное число α называется *алгебраическим*, если найдется отличный от нуля многочлен $f(x) \in \mathbb{Q}[x]$, для которого $f(\alpha) = 0$.

Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен называется *минимальным многочленом* α. Его степень называется *степенью* α и будет обозначаться $\deg \alpha$.

Примеры 1. Любое рациональное число a является алгебраическим, как корень многочлена $f(x) = x - a \in \mathbb{Q}[x]$. Указанный многочлен, очевидно, является минимальным многочленом числа a, и потому $\deg a = 1$.

2. Любая квадратичная иррациональность α есть корень некоторого многочлена с целыми коэффициентами $ax^2 + bx + c$. Так как α не рационально, то этот многочлен имеет минимальную степень среди всех, лежащих в кольце $\mathbb{Q}[x]$ и обращающихся в нуль при подстановке α вместо x. Поэтому $f(x) = x^2 + \frac{b}{a}x + \frac{c}{a} \in \mathbb{Q}[x]$ — минимальный многочлен α и $\deg \alpha = 2$. Например, $i, \sqrt{7}$ — алгебраические числа степени 2.

Укажем некоторые свойства минимального многочлена. Минимальный многочлен любого алгебраического числа неприводим. Если $f(x)$ — минимальный многочлен числа α, которое также является корнем многочлена $g(x) \in \mathbb{Q}[x]$, то многочлен $g(x)$ делится на $f(x)$. Неприводимый многочлен со старшим коэффициентом 1 служит минимальным многочленом для каждого из своих корней. Все корни минимального многочлена различны.

Если α — алгебраическое число степени n, то корни $\alpha_1, \ldots, \alpha_n$ его минимального многочлена называются числами, *сопряженными* с α.

Теорема 1.29. *Если α и β — алгебраические числа, то числа $\alpha + \beta$, $\beta - \alpha$, $\alpha\beta$, а в случае, если $\alpha \neq 0$, то и β/α являются алгебраическими числами.*

Из этой теоремы следует, что множество всех алгебраических чисел является полем.

Пусть $\xi_1, \ldots, \xi_m$ — алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа ξ_i, а также поле рациональных чисел $\mathbb{Q}$. Это поле, как легко видеть, состоит из

всевозможных дробей вида

$$\frac{A(\xi_1,\ldots,\xi_m)}{B(\xi_1,\ldots,\xi_m)}, \qquad B(\xi_1,\ldots,\xi_m)\neq 0.$$

где A, B — многочлены от переменных $x_1,\ldots,x_m$ с рациональными коэффициентами. Говорят, что числа $\xi_1,\ldots,\xi_m$ порождают поле $\mathbb{Q}(\xi_1,\ldots,\xi_m)$. Из теоремы 1.29 следует, что все его элементы являются алгебраическими числами.

Теорема 1.30. *Всякое поле $K=\mathbb{Q}(\xi_1,\ldots,\xi_m)$, порожденное алгебраическими числами $\xi_1,\ldots,\xi_m$, может быть порождено одним числом. Другими словами, существует такое число $\theta\in K$, что $K=\mathbb{Q}(\theta)$.*

Если степень алгебраического числа θ равна n, то каждый элемент α поля $K=\mathbb{Q}(\theta)$ единственным образом представляется в виде

$$\alpha = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}, \qquad r_j\in\mathbb{Q}. \tag{1.42}$$

Число θ, порождающее поле K, называется его *примитивным элементом*. Примитивный элемент поля $K=\mathbb{Q}(\xi_1,\ldots,\xi_m)$ всегда может быть выбран в виде

$$\theta = c_1\xi_1 + \ldots + c_m\xi_m, \qquad c_j\in\mathbb{Z}.$$

Рассмотрим, например, поле $\mathbb{Q}(\sqrt{2},\sqrt{3})$ и число $\theta=\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. Справедливы равенства

$$(\theta-\sqrt{2})^2=3, \qquad (\theta-\sqrt{3})^2=2,$$

из которых следует, что

$$\sqrt{2}=\frac{\theta^2-1}{2\theta}, \qquad \sqrt{3}=\frac{\theta^2+1}{2\theta}.$$

Поэтому $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\theta)$ и $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\theta)$.

Допустим, что $K=\mathbb{Q}(\eta), L=\mathbb{Q}(\xi)$, где η,ξ — алгебраические числа. В случае $K\subset L$ говорят, что поле L есть расширение поля K.

Теорема 1.31. *Если число ξ — корень многочлена*

$$\varphi(x) = \alpha_m x^m + \ldots + \alpha_1 x + \alpha_0$$

с алгебраическими коэффициентами α_i, то ξ — алгебраическое число.

Иными словами, эта теорема утверждает, что поле всех алгебраических чисел нельзя расширить, присоединив к нему корень какого-либо многочлена с алгебраическими коэффициентами. Это свойство называется *алгебраической замкнутостью*. Поле комплексных чисел также обладает этим свойством.

Из теоремы 1.30 следует, что поле $K = \mathbb{Q}(\xi_1, \ldots, \xi_m)$ есть конечномерное линейное пространство над $\mathbb{Q}$. Базисом его является, например, набор чисел $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Размерность этого линейного пространства n, равная степени примитивного элемента θ, называется *степенью* поля K. Любой базис этого линейного пространства называется *базисом* поля K.

Пусть $\alpha \in K$. Умножение элементов K на α определяет некоторое линейное отображение поля K на себя, $x \mapsto \alpha x$. Если $\omega_1, \ldots, \omega_n$ — какой-либо базис поля K, то

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j, \qquad a_{i,j} \in \mathbb{Q}, \tag{1.43}$$

и $A = \|a_{i,j}\|$ — матрица линейного отображения — умножения на α в базисе ω_j. След этой матрицы называется *следом* α (обозначение $Tr(\alpha)$), а её определитель называется *нормой* α (обозначение $N(\alpha)$). Таким образом,

$$Tr(\alpha) = Tr(A) = a_{1,1} + a_{2,2} + \ldots + a_{n,n}, \qquad N(\alpha) = \det A.$$

Величины $Tr(\alpha)$ и $N(\alpha)$ суть рациональные числа и, как хорошо известно, не зависят от выбора базиса в поле K.

Для любых чисел $\alpha, \beta \in K$ выполняются равенства

1. $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$, и $Tr(\lambda\alpha) = \lambda Tr(\alpha)$ при любом $\lambda \in \mathbb{Q}$.

2. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Другими словами: след есть $\mathbb{Q}$–линейная функция на поле K, а норма мультипликативна.

Если $\alpha \in K$ и $p(x) = x^m + c_1x^{m-1} + \cdots + c_m$ — минимальный многочлен числа α, то

$$Tr(\alpha) = -s \cdot c_1, \qquad N(\alpha) = (-1)^n c_m^s,$$

где целое число s равно $\frac{n}{m}$.

Поле $K = \mathbb{Q}(\xi_1, \ldots, \xi_m)$ называется *нормальным*, если оно содержит все сопряженные каждого из чисел ξ_j. Это свойство не зависит от выбора системы элементов, порождающих поле K. Так, если θ — примитивный элемент нормального поля K, то все числа, сопряженные с θ принадлежат K.

Например, поле $\mathbb{Q}(\sqrt{2})$ нормально над $\mathbb{Q}$. Поле $\mathbb{Q}(\sqrt[4]{2})$ не нормально, т.к. не содержит число $i\sqrt[4]{2}$, сопряженное с $\sqrt[4]{2}$ над $\mathbb{Q}$.

Пусть $\theta = \theta_1, \theta_2, \ldots, \theta_n$ — все числа, сопряженные с примитивным элементом θ нормального поля K. Тогда для каждого $j = 1, \ldots, n$ отображение $\sigma_j : K \to K$, переводящее число

$$\alpha = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1} \in K, \qquad r_i \in \mathbb{Q}$$

в

$$\sigma_j(\alpha) = r_0 + r_1\theta_j + \cdots + r_{n-1}\theta_j^{n-1}$$

есть автоморфизм поля K, т.е. σ_j взаимно однозначно отображает поле K на себя и сохраняет арифметические операции, т.е. сумму чисел переводит в сумму их образов, произведение чисел — в произведение их образов, так же и для разности и отношения. Можно доказать, что указанные отображения не зависят от выбора примитивного элемента θ, все эти отображения различны, и любой автоморфизм поля K совпадает с одним из них.

Пусть $K = \mathbb{Q}(\sqrt{2})$. Отображение τ переводящее каждое число $\alpha = a + b\sqrt{2} \in K$, $a, b \in \mathbb{Q}$, в $a - b\sqrt{2}$ есть автоморфизм поля $\mathbb{Q}(\sqrt{2})$.

Из-за взаимной однозначности каждый автоморфизм имеет обратное отображение, также являющееся автоморфизмом поля K, а потому совпадающее с одним из σ_j. Кроме того, последовательное выполнение любых двух автоморфизмов поля K также является автоморфизмом. Из сказанного следует, что множество всех автоморфизмов поля K составляет конечную группу порядка n. Она называется *группой Галуа* поля K.

Группа Галуа поля $\mathbb{Q}(\sqrt{2})$ состоит из двух элементов: построенного выше отображения τ и тождественного отображения.

Для каждого числа $\alpha \in K$ справедливы равенства

$$Tr(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha), \qquad N(\alpha) = \prod_{j=1}^{n} \sigma_j(\alpha).$$

Каждое из чисел $\sigma_j(\alpha), 1 \leqslant j \leqslant n$, сопряжено с α, любое сопряженное в этом наборе присутствует, а равные числа повторяются одинаково часто.

Если $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, то $T(\alpha) = 2a, N(\alpha) = a^2 - 2b^2$.

Алгебраическое число α называется *целым алгебраическим*, если его минимальный многочлен имеет целые коэффициенты. Например, минимальный многочлен числа $\frac{1+\sqrt{17}}{2}$ равен $x^2 - x - 4$, так что это число есть целое алгебраическое. Множество всех целых алгебраических чисел замкнуто относительно операций сложения, вычитания и умножения. Множество целых алгебраических чисел поля $K = \mathbb{Q}(\xi_1, \ldots, \xi_m)$ образует подкольцо этого поля, которое будет обозначаться символом $\mathbb{Z}_K$. Например, $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$. Можно доказать, что каждое конечно порожденное поле алгебраических чисел K имеет базис $\omega_1, \ldots, \omega_n$, для которого

$$\mathbb{Z}_K = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n.$$

Такой базис называется *фундаментальным базисом* поля K.

Пример. Пусть d — целое число, не делящееся на квадрат никакого простого числа, $K = \mathbb{Q}(\sqrt{d})$ — квадратичное расширение поля

рациональных чисел. Не трудно доказать, что кольцо $\mathbb{Z}_K$ целых чисел поля K имеет вид

$$\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\omega,$$

где

$$\omega = \begin{cases} \sqrt{d} & \text{если} \quad d \equiv 2,\, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{если} \quad d \equiv 1 \pmod 4. \end{cases} \tag{1.44}$$

В кольцах целых алгебраических чисел может не выполняться свойство единственности разложения элементов в произведение простых. Так в поле $K = \mathbb{Q}(\sqrt{-23})$ кольцо целых чисел имеет вид $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\omega$, где $\omega = \frac{1+\sqrt{-23}}{2}$. В этом кольце нет единственности разложения на простые множители:

$$3 \cdot 3 \cdot 3 = 27 = (2 + \sqrt{-23}) \cdot (2 - \sqrt{-23}).$$

Легко проверить, что каждое из чисел $3, 2 \pm \sqrt{-23}$ не может быть разложено в произведение необратимых элементов кольца $\mathbb{Z}_K$, т.е. является простым в этом кольце.

Эффективная замена отсутствующего в кольцах целых алгебраических чисел свойства единственности разложения на простые множители связана с использованием идеалов. *Идеалом* в кольце $\mathbb{Z}_K$ называется любая аддитивная подгруппа $\mathbb{Z}_K$, замкнутая относительно умножения на элементы $\mathbb{Z}_K$. Идеал $\mathfrak{p} \subset \mathbb{Z}_K$ называется *простым*, если для любых двух элементов $a, b \in \mathbb{Z}_K$ включение $ab \in \mathfrak{p}$ возможно лишь в случаях $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$.

Например, для каждого ненулевого числа $\alpha \in \mathbb{Z}_K$ совокупность всех чисел кольца $\mathbb{Z}_K$, делящихся на α, т.е. множество $\alpha\mathbb{Z}_K$ есть идеал кольца $\mathbb{Z}_K$. Такие идеалы называются *главными* и обозначаются (α). Число α называется *образующим элементом* идеала (α). Для любого набора чисел $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}_K$ множество $\alpha_1\mathbb{Z}_K + \ldots + \alpha_r\mathbb{Z}_K$ также является идеалом кольца $\mathbb{Z}_K$. Оно обозначается $(\alpha_1, \ldots, \alpha_r)$.

В множестве идеалов поля K можно ввести операцию умножения. Произведением двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ называется множество конечных

сумм попарных произведений элементов из $\mathfrak{a}$ и $\mathfrak{b}$, т.е.

$$\mathfrak{ab} = \Big\{ \sum_i \alpha_i \cdot \beta_i \quad \Big| \quad \alpha_i \in \mathfrak{a},\, \beta_i \in \mathfrak{b} \Big\}.$$

Не трудно доказать, что множество $\mathfrak{ab}$ также является идеалом. Операция умножения идеалов ассоциативна и коммутативна.

Как и для чисел, для каждого идеала $\mathfrak{a} \subset \mathbb{Z}_K$ можно ввести понятие нормы. Рассмотрим для этого кольцо классов вычетов $\mathbb{Z}_K/\mathfrak{a}$. Оно конечно, количество элементов в нем называется *нормой идеала* $\mathfrak{a}$ и обозначается $N(\mathfrak{a})$. Норма любого главного идеала (α) связана с нормой его образующего элемента α равенством $N((\alpha)) = |N(\alpha)|$. Можно доказать, что норма идеала мультипликативна, т.е. для любых двух идеалов $\mathfrak{a}, \mathfrak{b}$ выполняется равенство $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Для любого простого идеала $\mathfrak{p}$ имеем $N(\mathfrak{p}) = p^f$, где p — единственное простое число, содержащееся в $\mathfrak{p}$, а f — натуральное число, называемое *степенью поля вычетов* идеала $\mathfrak{p}$.

Имеет место единственность разложения идеалов в произведение простых.

Теорема 1.32. *Для каждого идеала $\mathfrak{a} \subset \mathbb{Z}_K$ существуют единственным образом определенные совокупности простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathbb{Z}_K$ и натуральных чисел $k_1, \ldots, k_r$ такие, что*

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}.$$

Укажем далее, как в кольце $\mathbb{Z}_K$ раскладываются в произведение простых идеалов главные идеалы (p), порождаемые простыми числами p. Пусть $K = \mathbb{Q}(\theta)$ — поле алгебраических чисел степени n, $\theta \in \mathbb{Z}_K$, и $\omega_1, \ldots, \omega_n$ — фундаментальный базис поля K. Тогда с некоторыми целыми числами $c_{i,j}$ выполняются равенства

$$\theta^{i-1} = \sum_{j=1}^{n} c_{i,j}\omega_j, \qquad 1 \leqslant i \leqslant n.$$

Абсолютная величина определителя матрицы $C = \|c_{i,j}\|_{1 \leqslant i,j \leqslant n}$ называется *индексом* числа θ. Он не зависит от выбора фундаментального

базиса поля K и будет обозначаться d_θ. В частности, если кольцо целых чисел $\mathbb{Z}_K$ имеет вид $\mathbb{Z}[\theta]$, то $d_\theta = 1$.

В формулировке следующего утверждения будет присутствовать некоторое простое число p. Для каждого многочлена $u(x) \in \mathbb{Z}[x]$ будем обозначать символом $\overline{u}(x)$ многочлен в кольце $F_p[x]$, коэффициенты которого суть классы вычетов по модулю p соответствующих коэффициентов многочлена $u(x)$.

Теорема 1.33. *Пусть p — простое число, не делящее индекс d_θ числа θ, $q(x)$ — минимальный многочлен θ. Пусть также*

$$\overline{q}(x) = \prod_{j=1}^{r} \overline{g}_j(x)^{e_j}$$

— разложение на неприводимые множители над полем F_p с некоторыми многочленами $g_j(x) \in \mathbb{Z}[x]$. Тогда $\mathfrak{p}_j = (p, g_j(\theta))$, $j = 1, \ldots, r$, — простые идеалы, и в кольце $\mathbb{Z}_K$ справедливо равенство

$$(p) = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}. \tag{1.45}$$

При этом $N(\mathfrak{p}_j) = p^{f_j}$, где $f_j = \deg \overline{g}_j(x)$.

Заметим, что в случае $\mathbb{Z}_K = \mathbb{Z}[\theta]$ утверждение теоремы выполняется для любого простого числа p.

Пример. Разложим в поле $\mathbb{Q}(\sqrt{-19})$ в произведение простых идеалов число 7.

Кольцо целых чисел поля $\mathbb{Q}(\sqrt{-19})$ имеет вид $\mathbb{Z}[\omega]$, где $\omega = \frac{1+\sqrt{-19}}{2}$. Минимальный многочлен для ω равен $p(x) = x^2 - x + 5$. Справедливо разложение

$$p(x) \equiv (x+1)(x-2) \pmod 7.$$

Поэтому $(7) = \mathfrak{p}_1\mathfrak{p}_2$, где

$$\mathfrak{p}_1 = (7, \omega + 1), \qquad \mathfrak{p}_2 = (7, \omega - 2).$$

Оба получившиеся простые идеала главные. Действительно, из равенства $(\omega+1)(\omega-2)=-7$ следует, что в кольце $\mathbb{Z}_K$ число 7 делится на целые числа $\omega+1, \omega-2$. Поэтому

$$\mathfrak{p}_1=(\omega+1), \qquad \mathfrak{p}_2=(\omega-2).$$

В том же поле $(19)=\mathfrak{p}^2$, где $\mathfrak{p}=(19,\omega-10)$.

Глава 2

Быстрые алгоритмы

2.1 Алгоритм Евклида

Рассмотрим следующую задачу. Пусть a, b — натуральные числа. Требуется найти (a, b) — наибольший общий делитель a, b. Задача эта решается достаточно быстро с помощью хорошо известного алгоритма Евклида без разложения чисел на множители. В основе его лежит равенство $(a, b) = (b, r)$, где r — остаток от деления числа a на b, см. §1.1.

Алгоритм 2.1. Даны: *Натуральные числа a и b; $b < a$.*
Найти: *Наибольший общий делитель (a, b).*

1. Вычислить r — остаток от деления a на b, т.е. найти целое r, удовлетворяющее условиям $a = bq + r,\ 0 \leqslant r < b$.
2. Если $r = 0$, то $(a, b) = b$, СТОП.
3. Если $r \neq 0$, то заменить пару $\{a, b\}$ парой $\{b, r\}$ и перейти в пункт 1 алгоритма.

Обоснование алгоритма содержится в §1.1. Мы займемся здесь оценкой его сложности.

Теорема 2.1 (Ламе, 1845)**.** *Пусть $a > b$ — натуральные числа. При вычислении (a, b) с помощью алгоритма Евклида будет выполнено не более $5m$ операций деления с остатком, где m есть количество цифр в десятичной записи числа b.*

Доказательство. Положим $r_0 = a$ и обозначим $r_1, r_2, \ldots, r_n$ — последовательность делителей в алгоритме Евклида. Тогда $r_1 = b$,

$$r_{i-1} = a_i r_i + r_{i+1}, \quad 0 \leqslant r_{i+1} < r_i,\ a_i \in \mathbb{N}, \quad i = 1, 2, \ldots, n-1,$$

$r_n = (a, b)$.

Докажем справедливость следующих неравенств

$$r_i \geqslant \lambda^{n-i}, \qquad i = 1, 2, \ldots, n, \tag{2.1}$$

где $\lambda = \frac{1+\sqrt{5}}{2} = 1,61...$ есть корень квадратного уравнения $\lambda^2 - \lambda - 1 = 0$. Для этого воспользуемся индукцией по индексу i, двигаясь в обратном направлении от n к 1. При $i = n$ имеем $r_n \geqslant 1 = \lambda^0$. При $i = n-1$ находим $r_{n-1} \geqslant r_n + 1 \geqslant 2 > \lambda$, так что неравенство (2.1) опять справедливо. Предположим теперь, что $k < n$ и неравенство (2.1) выполняется при всех $i \geqslant k$. Имеем следующую цепочку равенств и неравенств

$$r_{k-1} = a_k r_k + r_{k+1} \geqslant r_k + r_{k+1} \geqslant \lambda^{n-k} + \lambda^{n-k-1} = \lambda^{n-k-1}(\lambda+1) = \lambda^{n-k+1}.$$

Таким образом, неравенство (2.1) выполняется и при $i = k-1$. Это доказывает справедливость (2.1) при всех $i = 1, 2, \ldots, n$.

Поскольку десятичная запись b содержит m знаков, то $10^m > b$, и

$$10^m > b = r_1 \geqslant \lambda^{n-1}.$$

Из этих неравенств следует, что

$$m > (n-1)\log_{10}\lambda > (n-1)/5.$$

Последнее неравенство выполняется, поскольку $\lambda > 10^{1/5} = 1,58...$. Таким образом, $n < 5m + 1$, что завершает доказательство теоремы. □

Поскольку $m \leqslant 1 + \log b$, из теоремы 2.1 следует, что алгоритм Евклида имеет полиномиальную сложность.

2.2 Символы Лежандра и Якоби

В этом параграфе мы рассмотрим вопрос о том, как узнать, разрешимо или нет по простому модулю $p > 2$ квадратичное сравнение. Хорошо известно, что сравнение

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad a, b, c \in \mathbb{Z},\ p \nmid a,$$

сводится выделением полного квадрата к сравнению

$$x^2 \equiv d \pmod{p}, \qquad d \in \mathbb{Z}. \tag{2.2}$$

Ответ находится тривиально в случае $p \mid d$, решениями являются числа $x \equiv 0 \pmod{p}$.

Если $p \nmid d$, вопрос о разрешимости (2.2) также может быть решен достаточно быстро. Мы изложим ниже соответствующую теорию, отсылая за доказательствами к [5].

Определение 2.1. *Пусть p — простое нечетное число. Целое число d, не делящееся на p, называется* квадратичным вычетом *по модулю p, если сравнение (2.2) разрешимо. В противном случае оно называется* квадратичным невычетом *по модулю p.*

Если $d_1 \equiv d_2 \pmod{p}$, то числа d_1, d_2 одновременно являются квадратичными вычетами или квадратичными невычетами. Для каждого $p \geqslant 3$ имеется $(p-1)/2$ классов квадратичных вычетов и равно столько же классов квадратичных невычетов.

Определение 2.2. Символ Лежандра $\left(\frac{d}{p}\right)$ *есть функция от двух аргументов: d есть целое число, а p — простое нечетное. Значение символа Лежандра равно 1, если d есть квадратичный вычет по модулю p, оно равно -1, если d есть квадратичный невычет по модулю p, и оно равно 0, если $p \mid d$.*

Определенная так функция обладает рядом простых свойств, позволяющих легко вычислять ее значения и тем самым получать ответ на вопрос о разрешимости сравнения (2.2).

Свойства символа Лежандра

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
2. *Если* $a \equiv b \pmod{p}$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. $\left(\frac{1}{p}\right) = 1; \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}; \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
5. *Если* p *и* q *— различные нечетные простые числа, то*

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

Последнее свойство носит название *квадратичный закон взаимности*. Оно впервые было доказано Гауссом в 1796г.

Следующий пример показывает, как эти свойства позволяют вычислять символ Лежандра. Для удобства вычислений заметим, что числа $\frac{p-1}{2}$ и $\frac{p^2-1}{8}$ будут четными, соответственно, в случаях $p \equiv 1 \pmod{4}$ и $p \equiv \pm 1 \pmod{8}$.

Пример. Выяснить, разрешимо ли сравнение

$$x^2 \equiv 184 \pmod{347} \tag{2.3}$$

Для того, чтобы ответить на этот вопрос, необходимо вычислить значение $\left(\frac{184}{347}\right)$, поскольку 347 есть простое число. Так как $184 = 2^3 \cdot 23$, то пользуясь свойствами символа Лежандра, находим

$$\left(\frac{184}{347}\right) = \left(\frac{2}{347}\right)^3 \left(\frac{23}{347}\right) = -\left(\frac{23}{347}\right) = \left(\frac{347}{23}\right) = \left(\frac{2}{23}\right) = 1.$$

Таким образом, сравнение (2.3) разрешимо. Конечно, указанное вычисление не позволяет найти сами решения.

Вычисление символа Лежандра $\left(\frac{d}{p}\right)$, основанное на свойствах 2)-5), требует разложения числа d на простые множители. В настоящее время это очень трудоемкая задача. Ниже мы опишем более совершенный способ вычисления символа Лежандра. Соответствующий алгоритм имеет полиномиальную сложность и не использует ни проверки чисел на простоту, ни разложения на простые множители. В основе его лежит возможность продолжить функцию $\left(\frac{d}{p}\right)$ на множество всех пар взаимно простых целых чисел D, P, где P — произвольное нечетное число, с сохранением свойств 2)-5). Продолженная таким образом функция носит название *символ Якоби*.

Определение 2.3. *Пусть* $P = p_1 \cdots p_r$, *где* p_j — *нечетные простые числа, и* $D \in \mathbb{Z}$, $(D, P) = 1$. *Символ Якоби* $\left(\frac{D}{P}\right)$ *определяется равенством*

$$\left(\frac{D}{P}\right) = \left(\frac{D}{p_1}\right) \cdots \left(\frac{D}{p_r}\right),$$

где $\left(\frac{D}{p_j}\right)$ — *значения символа Лежандра.*

Если P — простое число, то символы Лежандра и Якоби со знаменателем P совпадают.

Вообще говоря, значение символа Якоби не связано с разрешимостью сравнений.

Пример. Легко проверить, что сравнение $x^2 \equiv 2 \pmod{15}$ не имеет решений. Тем не менее символ Якоби в этом случае равен

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1.$$

Следующие свойства подобны соответствующим свойствам символа Лежандра.

Свойства символа Якоби

2. *Если* $a \equiv b \pmod{P}$, *то* $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.

3. $\left(\frac{1}{P}\right) = 1; \quad \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}; \quad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$

4. $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right).$

5. *Если P и Q — положительные нечетные взаимно простые числа, то*

$$\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Покажем теперь, как с помощью этих свойств можно вычислить значение символа Якоби. При этом не используется разложение на простые множители, а лишь выделяется максимальная степень числа 2, входящая в разложение числителя. Рассмотрим сначала следующий пример.

Пример. Выяснить, разрешимо ли сравнение

$$x^2 \equiv 753 \pmod{811}$$

Отметим, что число 811 простое, так что для решения задачи достаточно вычислить соответствующий символ Якоби:

$$\left(\frac{753}{811}\right) = \left(\frac{811}{753}\right) = \left(\frac{58}{753}\right) = \left(\frac{29}{753}\right) = \left(\frac{753}{29}\right) = \left(\frac{-1}{29}\right) = 1.$$

При этом вычислении использовались следующие соотношения $753 \equiv 1 \pmod 8$, $811 \equiv 58 \pmod{753}$, $753 \equiv -1 \pmod{29}$, $29 \equiv 1 \pmod 4$. Итак, данное в примере сравнение разрешимо.

Легко проверить, что множество решений этого сравнения состоит из двух классов вычетов $x \equiv 276 \pmod{811}$, $x \equiv 535 \pmod{811}$. Методы нахождения решений и разложения многочленов на множители над конечными полями будут обсуждаться позднее в гл. 2.

Способ вычисления символа Якоби, использовавшийся в рассмотренном примере может быть оформлен в виде следующего алгоритма.

Алгоритм 2.2. Данные: *Целые взаимно простые числа Q и $P > 2$, P нечетно.*

Найти: *Значение символа Якоби* $\left(\frac{Q}{P}\right)$.

1. Положить $s = 0,\ u = Q,\ v = P$.

2. Найти r *— наименьший положительный остаток от деления числа* u *на* v, *т.е. целое число, удовлетворяющее условиям*

$$u = vq + r, \qquad 0 < r < v;$$

вычислить целое $k \geqslant 0$ *и нечетное* t, *для которых* $r = 2^k t$; *положить*

$$s \equiv s + k \cdot \frac{v^2 - 1}{8} + \frac{(t-1)(v-1)}{4} \pmod 2.$$

3. Если $t = 1$, *положить*

$$\left(\frac{Q}{P}\right) = (-1)^s.$$

СТОП.

4. Если $t \geqslant 3$, *положить* $u = v,\ v = t$, *перейти в пункт 2.*

Докажем, что приведенный алгоритм действительно вычисляет символ Якоби и получим оценку его сложности.

Теорема 2.2. *Приведенный алгоритм вычисляет символ Якоби* $\left(\frac{Q}{P}\right)$ *за* $O(m)$ *арифметических операций, где* m *есть количество цифр в десятичной записи меньшего из чисел* $P,\ Q$.

Доказательство. В процессе работы алгоритма число v убывает. Это значит, что алгоритм не может работать бесконечно долго и, следовательно, завершит свою работу.

Обозначим буквой n количество проходов алгоритма через пункт 2. Пусть также $s_j,\ u_j,\ v_j$ — значения параметров $s,\ u,\ v$ перед j-м входом в пункт 2. Тогда $s_1 = 0, u_1 = Q, v_1 = P$. Докажем индукцией по j справедливость равенств

$$\left(\frac{Q}{P}\right) = (-1)^{s_j} \cdot \left(\frac{u_j}{v_j}\right), \qquad j = 1, \ldots, n. \tag{2.4}$$

При $j = 1$ это равенство, очевидно, выполняется. Пусть $j < n$ и (2.4) справедливо. В процессе выполнения пункта 2 алгоритма в j-й раз будут найдены числа $q,\ k,\ t$, для которых $u_j = qv_j + 2^k t$. Тогда

$$\left(\frac{u_j}{v_j}\right) = \left(\frac{2^k t}{v_j}\right) = \left(\frac{2}{v_j}\right)^k \cdot \left(\frac{t}{v_j}\right) = (-1)^{k\frac{v_j^2-1}{8}+\frac{t-1}{2}\frac{v_j-1}{2}} \left(\frac{v_j}{t}\right).$$

Это равенство вместе с (2.4) завершает шаг индукции. Итак, равенство (2.4) справедливо для всех j.

При $j = n$, т.е. при последнем выходе из пункта 2) будем иметь $t = 1$ и, следовательно,

$$\left(\frac{Q}{P}\right) = (-1)^{s_n} \cdot \left(\frac{u_n}{v_n}\right) = (-1)^{s_n} \left(\frac{2}{v_n}\right)^k = (-1)^{s_n + k\frac{v_n^2-1}{8}}.$$

Это доказывает, что алгоритм действительно вычисляет значение символа Якоби $\left(\frac{Q}{P}\right)$.

Учитывая равенства $u_j = v_{j-1}, t = v_{j+1}$, находим, что

$$v_{j-1} \geqslant v_j + v_{j+1}, \qquad j \geqslant 2.$$

Получившиеся неравенства, как и в доказательстве теоремы 2.1 приводят к оценке $v_j \geqslant \lambda^{n-j}$, доказывающей при $j = 1$, что $n = O(\ln P) = O(m)$. Оценка количества арифметических операций в алгоритме имеет, очевидно, тот же порядок. □

2.3 Быстрый алгоритм возведения в степень.

Пусть A — некоторое кольцо, $a \in A$ и d — натуральное число. В этом параграфе мы обсудим быстрый алгоритм вычисления степени a^d. Тривиальный алгоритм, состоящий в последовательном умножении на a результата предшествующего вычисления, требует $d-1$ умножений. Следующий алгоритм вычисляет степень существенно быстрее.

Алгоритм 2.3. Данные: *Элемент $a \in A$ и натуральное число d.* Найти: *Элемент a^d.*

1. Представить d в двоичной системе счисления, т.е. найти такие числа $d_j \in \{0,\ 1\}$, что $d = d_0 2^r + \cdots + d_{r-1}2 + d_r,\ d_0 = 1$.
2. Положить $a_0 = a$ и затем для $i = 1, \ldots, r$ вычислить

$$a_i = a_{i-1}^2 \cdot a^{d_i}. \tag{2.5}$$

3. Положить $a^d = a_r$.

Теорема 2.3. *Алгоритм действительно вычисляет степень a^d. Он использует для этого не более $2[\log_2 d]$ умножений в кольце A.*

Доказательство. При всех $i = 0, 1, \ldots, r$ справедливы равенства

$$a_i = a^{d_0 2^i + \cdots + d_i}. \tag{2.6}$$

Докажем это индукцией по i. При $i = 0$ утверждение выполняется, т.к. $d_0 = 1$. Подставляя (2.6) в равенство $a_{i+1} = a_i^2 \cdot a^{d_{i+1}}$, находим равенство (2.6) для a_{i+1}. Это доказывает (2.6) для всех i. При $i = r$ получаем $a_r = a^d$, что доказывает корректность алгоритма.

Для оценки сложности обозначим символом $c(d)$ количество умножений, необходимых алгоритму для вычисления a^d. Докажем индукцией по d неравенство

$$c(d) \leqslant 2[\log_2 d]. \tag{2.7}$$

Обозначим для этого $m = d_0 2^{r-1} + \cdots + d_{r-1}$. Тогда $d = 2m + d_r \geqslant 2m$.

При $d = 1,\ 2$ неравенство (2.7), очевидно, выполняется. Пусть теперь $d \geqslant 3$. В силу алгоритма справедливы соотношения

$$c(d) = c(m) + 1 + d_r \leqslant c(m) + 2 \leqslant 2[\log_2 m] + 2 = 2[\log_2 2m] \leqslant 2[\log_2 d],$$

доказывающие нужное неравенство. □

Рассмотрим некоторые примеры использования описанного алгоритма.

Пример 1. Пусть m — натуральное число и $A = \mathbb{Z}/m\mathbb{Z}$ — кольцо вычетов по модулю m. Алгоритм реализует вычисление степеней в кольце вычетов по модулю m. Классическая теорема Эйлера утверждает, что $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — функция Эйлера. Поэтому, заменив показатель степени d его остатком от деления на $\varphi(m)$ (на что потребуется одна арифметическая операция), задачу вычисления $a^d \pmod{m}$ всегда можно свести к случаю $d \leqslant \varphi(m)$. Это показывает, что сложность алгоритма возведения в степень в кольце вычетов $\mathbb{Z}/m\mathbb{Z}$ есть $O(\ln m)$.

В частности, если $m = p$ — простое нечетное число, то в силу свойства 1 символа Лежандра имеем

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

так что алгоритм 3 дает другой способ вычисления символа Лежандра за $O(\log p)$ арифметических операций.

Пример 2. Пусть R — кольцо и последовательность элементов u_0, u_1, $u_2, \ldots \in R$ задана рекуррентно

$$u_n = a_1 u_{n-1} + \cdots + a_h u_{n-h}, \qquad n \geqslant h, \quad a_j \in R.$$

Например, можно взять $R = \mathbb{Z}/m\mathbb{Z}$. Как вычислить u_d для заданного индекса d? Введем для этого вектора

$$\overline{u}_n = (u_n, u_{n-1}, \ldots, u_{n-h+1}), \qquad n \geqslant h.$$

Тогда справедливо равенство $\overline{u}_n = \overline{u}_{n-1} \cdot M$, где

$$M = \begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 \\ a_2 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{h-1} & 0 & 0 & \cdots & 1 \\ a_h & 0 & 0 & \cdots & 0 \end{pmatrix},$$

— квадратная матрица из h строк и столбцов с элементами в кольце R. Очевидно равенство $\overline{u}_n = \overline{u}_h \cdot M^{n-h}$, из которого следует, что

вычисление u_d сводится к вычислению M^{d-h} в кольце A квадратных матриц размера h с элементами в R. Сложность вычисления u_d таким способом оценивается величиной $O(h^2 \ln d)$, где постоянная в $O(\cdot)$ абсолютна.

2.4 Вероятностные алгоритмы

Рассмотренные выше алгоритмы относятся к разряду детерминированных. Так называют алгоритмы, в которых результат каждого шага однозначно определяется предшествующими вычислениями. Однако, существуют и другие типы алгоритмов, весьма удобные на практике.

Пусть p — простое число, $p > 2$. В этом параграфе мы рассмотрим следующую важную задачу: найти какой-либо квадратичный невычет по модулю p. Умение вычислять квадратичные невычеты понадобится, например, в параграфе 2.5 при решении квадратичных сравнений.

Можно решить ее, например, следующим образом. Для любого $a \in \mathbb{Z}$ легко проверить, будет это число квадратичным вычетом или нет. Для этого достаточно вычислить символ Лежандра $\left(\frac{a}{p}\right)$ или $a^{\frac{p-1}{2}} \pmod p$. В случае, если получившееся значение равно -1, число a будет квадратичным невычетом по модулю p. Можно попытаться организовать такую проверку последовательно для $a = 2, 3, \ldots$ до тех пор, пока не будет обнаружен квадратичный невычет.

Такой способ решения, естественно ставит вопрос: сколь быстро найдется невычет? Другими словами, какова граница сверху для наименьшего положительного квадратичного невычета по модулю p? В 1926г. И.М. Виноградов доказал, что наименьший квадратичный невычет имеет порядок $O(p^{\frac{1}{2\sqrt{e}}} \ln^2 p)$. В 1958г. этот результат был усилен Берджесом, получившим оценку $O(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$ для любого положительного ε. Эта оценка не улучшена до сих пор и является также оценкой сложности указанного алгоритма.

Оценка Берджеса весьма велика. В соответствии с ней при больших p алгоритм будет работать достаточно долго. Предполагается,

что в действительности наименьший невычет существенно меньше. Если справедлива так называемая расширенная гипотеза Римана, то наименьший квадратичный невычет может быть оценен сверху величиной $2\ln^2 p$. Таким образом, получается полиномиальная оценка сложности алгоритма. К сожалению, она носит условный характер, ведь даже обычная гипотеза Римана все еще не доказана.

Несмотря на отсутствие быстрого детерминированного алгоритма, рассмотренная задача может быть весьма успешно решена на практике. Напомним, что количество квадратичных невычетов по модулю p равно $\frac{p-1}{2}$. Это значит, что, выбирая случайным образом число a из промежутка $1 \leqslant a < p$, можно с вероятностью, близкой к $1/2$ (при больших p), попасть на невычет и убедиться в этом, вычислив $\left(\frac{a}{p}\right)$.

При N испытаниях вероятность не найти невычет близка к 2^{-N}. На практике такие алгоритмы работают достаточно эффективно.

Для оценки сложности вероятностного алгоритма, что нужно для сравнения эффективности различных алгоритмов, можно использовать математическое ожидание времени работы. Вычислим его в приведенном примере.

Пусть A_k — событие, состоящее в том, что невычет будет найден впервые при испытании с номером k. Вероятность этого события $p(A_k)$, как это указывалось, близка к 2^{-k}. Для упрощения вычислений будем считать $p(A_k) = 2^{-k}$.

Количество арифметических операций, необходимых для выполнения одного испытания (скажем, вычисления $a^{\frac{p-1}{2}} \pmod p$), может быть оценено сверху величиной $L = O(\ln p)$. Тогда количество арифметических операций при наступлении события A_k равно kL, а математическое ожидание количества операций M равно

$$M = \sum_{k=1}^{\infty} kL \cdot 2^{-k} = L \sum_{k=1}^{\infty} k2^{-k} = 2L.$$

При вычислении последней суммы использовалось тождество

$$\sum_{k=1}^{\infty} kx^k = \frac{x}{(1-x)^2}.$$

Таким образом, среднее время работы алгоритма равно $O(\ln p)$. Нами доказана следующая

Теорема 2.4. *Сложность вероятностного алгоритма вычисления квадратичного невычета по модулю p равна $O(\ln p)$.*

Рассмотрим еще один вероятностный алгоритм и оценим его сложность. Пусть p — простое нечетное число. Как известно, мультипликативная группа $(\mathbb{Z}/p\mathbb{Z})^*$ классов вычетов циклична. Ее образующие называются *первообразными корнями* по модулю p. Известно, что $g \in (\mathbb{Z}/p\mathbb{Z})^*$ есть первообразный корень в том и только том случае, когда *для любого простого числа q, делящего $p-1$, выполняется*

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}.$$

В случае, если известно разложение $p-1$ на простые сомножители, это позволяет легко проверить, будет число g первообразным корнем или нет. Количество первообразных корней равно

$$\varphi(p-1) = (p-1) \prod_{q|p-1} \left(1 - \frac{1}{q}\right).$$

Следовательно вероятность при случайном выборе g попасть на первообразный корень есть $\prod_{q|p-1} \left(1 - \frac{1}{q}\right)$.

Теорема 2.5. *Сложность вероятностного алгоритма для вычисления первообразного корня по модулю p при известном разложении $p-1$ на простые сомножители равна $O(\ln^2 p)$.*

Для доказательства этой теоремы понадобятся два вспомогательных утверждения о простых числах.

Лемма 2.1. *Справедливы следующие неравенства*

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)^{-1}\leqslant c_1\ln x,\qquad \sum_{p\leqslant x}\ln p\geqslant c_2 x.$$

где c_1, c_2 — абсолютные постоянные, а p пробегает все простые числа, не превосходящие x.

Первое неравенство впервые было доказано Мертенсом, а второе — Чебышевым. Доказательства можно найти, например, в [11]. Следующее утверждение было доказано в 1903г. Э.Ландау.

Предложение 2.1. *С некоторой абсолютной постоянной выполняется неравенство*

$$\varphi(n)\geqslant c\frac{n}{\ln\ln n}.$$

Доказательство. Справедливо представление

$$\frac{n}{\varphi(n)}=\prod_{q|n}\left(1-\frac{1}{q}\right)^{-1},$$

где q пробегает все простые делители n. Обозначим буквой v количество этих делителей. Пусть также p_v — простое число с номером v. Тогда по лемме 2.1

$$\frac{n}{\varphi(n)}\leqslant\prod_{p\leqslant p_v}\left(1-\frac{1}{p}\right)^{-1}\leqslant c_1\ln p_v.$$

С другой стороны, по второму неравенству леммы 2.1

$$\ln n\geqslant\sum_{q|n}\ln q\geqslant\sum_{p\leqslant p_v}\ln p\geqslant c_2 p_v.$$

Так что $p_v\leqslant\frac{1}{c_2}\ln n$ и

$$\frac{n}{\varphi(n)}\leqslant c_1\ln\left(\frac{1}{c_2}\ln n\right)\leqslant\frac{1}{c}\ln\ln n.$$

□

Перейдем теперь непосредственно к доказательству теоремы 2.5.

Доказательство. Пусть $L = O(\ln p)$ — оценка сверху для количества арифметических операций при вычислении $a^{\frac{p-1}{q}} \pmod p$, где q — произвольный простой делитель числа $p-1$. Обозначим буквой v — количество различных простых делителей $p-1$. Тогда, как это следует из доказательства предложения 2.1, справедливо неравенство $p_v \leqslant \frac{1}{c_2}\ln(p-1)$ и, согласно неравенству Чебышева, см. [11], находим

$$v = \pi(p_v) \leqslant c_3\frac{p_v}{\ln p_v} \leqslant c_4\frac{\ln p}{\ln\ln p}.$$

Таким образом, проверка, является a первообразным корнем или нет, осуществляется не более чем за $L\cdot c_4\frac{\ln p}{\ln\ln p} = O\left(\frac{\ln^2 p}{\ln\ln p}\right)$ арифметических операций.

Пусть ρ — вероятность попасть на первообразный корень при случайном выборе $a \in [1, p-1]$. Тогда, в силу предложения 2.1,

$$\rho = \frac{\varphi(p-1)}{p-1} > \frac{c}{\ln\ln p}.$$

Если A_k — событие, состоящее в том, что первообразный корень будет впервые выбран при испытании с номером k, то $p(A_k) = (1-\rho)^{k-1}\cdot\rho$. Следовательно математическое ожидание времени работы алгоритма не превосходит

$$\sum_{k=1}^{\infty} kL\cdot c_4\frac{\ln p}{\ln\ln p}\cdot(1-\rho)^{k-1}\rho = Lc_4\frac{\ln p}{\ln\ln p}\rho^{-1} = O(\ln^2 p).$$

□

С помощью расширенной гипотезы Римана можно доказать, что наименьший первообразный корень по модулю $p > 2$ имеет величину $O(\ln^6 p)$. Это, при известном разложении $p-1$ на простые множители и справедливости расширенной гипотезы Римана, дает детерминированный полиномиальный алгоритм для вычисления первообразного корня.

2.5 Решение квадратичных сравнений (алгоритм Шенкса).

Пусть p — нечетное простое число, $a \in \mathbb{Z}$, $p \nmid a$. В этом параграфе будет описан алгоритм нахождения решений сравнения

$$x^2 \equiv a \pmod{p}. \tag{2.8}$$

При этом будет предполагаться известным какой-либо квадратичный невычет z по модулю p. По свойствам невычетов

$$-1 = \left(\frac{z}{p}\right) \equiv z^{\frac{p-1}{2}} \pmod{p}. \tag{2.9}$$

Если $\left(\frac{a}{p}\right) = -1$, то по определению символа Лежандра сравнение (2.8) решений не имеет. Поэтому далее будем считать, что $\left(\frac{a}{p}\right) = 1$, т.е.

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{2.10}$$

Определим натуральные числа k, h равенством

$$p - 1 = 2^k \cdot h, \qquad h \text{ нечетно}. \tag{2.11}$$

Обозначим буквой S множество пар целых неотрицательных чисел $\{j, v\}$ с условием

$$a^{2^j h} \cdot v^{2^{j+1}} \equiv 1 \pmod{p}.$$

Сравнение (2.10) означает, что $\{k-1, 1\} \in S$.

Алгоритм Шенкса строит, начиная с $\{k-1, 1\}$, последовательность пар $\{j, v\} \in S$ с убывающей до нуля первой координатой. Пара $\{0, w\} \in S$ дает решение сравнения (2.8). Действительно, положим

$$x \equiv \pm a^{\frac{h+1}{2}} \cdot w \pmod{p}. \tag{2.12}$$

Тогда

$$x^2 \equiv a^{h+1} w^2 \pmod{p}. \tag{2.13}$$

Поскольку $\{0, w\} \in S$, то имеет место сравнение $a^h w^2 \equiv 1 \pmod{p}$, означающее, что (2.13) совпадает с (2.8). Таким образом, сравнения (2.12) дают решения (2.8). Других решений, как известно, это сравнение не имеет.

Алгоритм 2.4. Данные: *Простое нечетное число p, целое число a, $p \nmid a$, квадратичный невычет z по модулю p.*
Найти: *Решения сравнения (2.8).*

1. Найти натуральные числа k, h, определенные условиями (2.11).
2. Положить $j = k - 1,\ v = 1$.
3. Перебирая последовательно $r = 0, 1, \ldots$ найти наименьшее число r с условием

$$a^{2^r h} v^{2^{r+1}} \equiv 1 \pmod{p}. \tag{2.14}$$

4. Если $r = 0$, положить

$$x \equiv \pm a^{\frac{h+1}{2}} \cdot v \pmod{p}.$$

СТОП.
5. Если $r \geqslant 1$, определить

$$w \equiv v \cdot z^{2^{k-1-r}h} \pmod{p}$$

и положить $j = r - 1,\ v = w$. Перейти в пункт 3.

Теорема 2.6. *Алгоритм 2.4 действительно находит решения сравнения (2.8). Его сложность при известном квадратичном невычете по модулю p оценивается величиной $O(\ln^2 p)$.*

Доказательство. Покажем, что перед каждым входом в пункт 3 алгоритма параметры j, v принимают такие значения, что пара $\{j, v\}$ принадлежат множеству S. Это так для первой пары $\{k-1, 1\}$. Допустим, что это свойство имеет место для некоторой пары $\{j, v\}$ и докажем его для следующей. Множество чисел r, удовлетворяющих сравнению (2.14), не пусто. Ему, в силу предположения, удовлетворяет число j. В частности, это означает, что минимальное значение

r удовлетворяет неравенству $r \leqslant j$. Из сравнения (2.14) следует, что пара $\{r, v\}$ принадлежит множеству S. Проверим, что при этом пара $\{r-1, w\}$ также принадлежит множеству S. Сравнение (2.14) может быть переписано в виде

$$\left(a^{2^{r-1}h} v^{2^r}\right)^2 \equiv 1 \pmod{p}.$$

Условие минимальности r означает, что выражение в скобках последнего сравнения не может быть сравнимо с 1 и потому

$$a^{2^{r-1}h} v^{2^r} \equiv -1 \pmod{p}.$$

Теперь в силу (2.9) и (2.11) имеем

$$a^{2^{r-1}h} w^{2^r} \equiv a^{2^{r-1}h} \left(v \cdot z^{2^{k-1-r}h}\right)^{2^r} \equiv -a^{2^{r-1}h} v^{2^r} \equiv 1 \pmod{p}.$$

Таким образом, новая пара $\{j, v\}$, возникающая на выходе из пункта 5, также принадлежит множеству S. В процессе работы алгоритма параметр j убывает до нулевого значения. Поэтому алгоритм всегда завершает свою работу и находит множество решений сравнения (2.8).

Оценим сложность алгоритма. Вычисление k, h и $a^h \pmod{p}$ требует $O(\ln p)$ арифметических операций. При этом $k = O(\ln p)$. При фиксированных $\{j, v\}$ вычисление величин r и $z^{2^{k-1-r}}$ требует $O(\ln p)$ арифметических операций. Таким образом, новая пара величин $\{j, v\}$ вычисляется по предыдущей за $O(\ln p)$ арифметических операций. Поскольку параметр j принимает не более $k = O(\ln p)$ значений, можно заключить, что решения сравнения (2.8) будут найдены не более чем за $O(\ln^2 p)$ арифметических операций. □

Отметим, что алгоритм 2.4 имеет полиномиальную сложность, лишь если известен какой-либо квадратичный невычет по модулю p. Это обстоятельство можно выразить, сказав, что алгоритм *полиномиально сводит* задачу решения сравнения (2.8) к нахождению квадратичного невычета. Последняя задача, как указано в параграфе 2.4, решается вероятностным алгоритмом полиномиальной сложности, поэтому сравнение (2.8) на практике также решается достаточно быстро.

2.6 Вероятностные методы отсеивания составных чисел.

Пусть N — натуральное число, вообще говоря, большое. Оно может быть либо составным, либо простым. Соответственно, можно рассмотреть две важные задачи.

1. N — составное число, и требуется доказать это.

2. N — простое число, и требуется доказать это.

В настоящем параграфе будет рассматриваться первая из задач. Мы покажем, что существуют достаточно быстрые вероятностные алгоритмы, решающие ее и не использующие при этом разложение N на множители.

Выберем целое число $a, 1 < a < N$. Справедливо следующее утверждение:

1) Если наибольший общий делитель $(a, N) > 1$, то N — составное число.

Условие $(a, N) > 1$ легко проверить, вычислив (a, N) с помощью алгоритма Евклида.

2) Если $(a, N) = 1$ и $a^{N-1} \not\equiv 1 \pmod{N}$, то N — составное число.

Это утверждение следует из малой теоремы Ферма, и его также легко проверить с помощью алгоритма возведения в степень.

К сожалению, утверждений 1)–2) не достаточно для доказательства того, что испытываемое число N — составное. Существуют составные числа, для которых выполняется сравнение $a^{N-1} \equiv 1 \pmod{N}$ при любом целом $a, (a, N) = 1$.

Определение 2.4. *Составное число N называется числом Кармайкла, если при любом $a, (a, N) = 1$, выполняется сравнение*

$$a^{N-1} \equiv 1 \pmod{N}. \tag{2.15}$$

Пример. $N = 561 = 3 \cdot 11 \cdot 17$.

Для каждого целого $a, (a, 561) = 1$, имеем $(a, 3) = (a, 11) =$

$(a, 17) = 1$ и по малой теореме Ферма выполняются сравнения

$$a^2 \equiv 1 \pmod 3, \qquad a^{10} \equiv 1 \pmod{11}, \qquad a^{16} \equiv 1 \pmod{17}.$$

Так как 560 делится на 2, 10 и 16, то число $a^{560} - 1$ делится на каждую из разностей $a^2 - 1, a^{10} - 1, a^{16} - 1$. Значит, $a^{560} - 1$ делится на 3, 11, 17 и потому делится на произведение этих чисел, т.е. делится на 561. Число 561 есть число Кармайкла.

Теорема 2.7. *Число N есть число Кармайкла, если и только если это число есть произведение не менее трех различных нечетных простых чисел, $N = p_1 \cdots p_r$, $r \geqslant 3$, $p_i \neq p_j$, причем*

$$(p_j - 1) \mid (N - 1).$$

Доказательство. Докажем достаточность условий теоремы 2.7. Если целое число a взаимно просто с N, то оно не делится на p_j и согласно малой теореме Ферма выполняется сравнение

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

Возводя обе части этого сравнения в целую степень $(N-1)/(p_j - 1)$, находим

$$a^{N-1} \equiv 1 \pmod{p_j}.$$

Так как по доказанному число $a^{N-1} - 1$ делится на все числа p_j, $j = 1, \ldots, r$, то оно делится и на произведение этих чисел, т.е. на N. Таким образом, выполняется сравнение (2.15), т.е. N есть число Кармайкла.

Предположим теперь, что N есть число Кармайкла. Тогда N — составное число, и, значит, $N \geqslant 4$. Если $N = 2^k, k \geqslant 2$, то $(-1)^{N-1} = -1 \not\equiv 1 \pmod N$, то-есть нарушается определение чисел Кармайкла. Следовательно, N имеет нечетные простые делители, то-есть имеет место представление $N = p^k \cdot M$, где p — простое нечетное число, и целое число M не делится на p. Пусть g — первообразный корень по модулю p^k и целое число a есть решение системы сравнений

$$a \equiv g \pmod{p^k}, \qquad a \equiv 1 \pmod M.$$

Тогда $(a, N) = 1$, и согласно определению чисел Кармайкла имеем $a^{N-1} \equiv 1 \pmod{N}$. Но тогда $a^{N-1} \equiv 1 \pmod{p^k}$ и $g^{N-1} \equiv 1 \pmod{p^k}$. Учитывая, что g есть первообразный корень по модулю p^k, заключаем теперь, что

$$\varphi(p^k) = p^{k-1}(p-1) | (N-1).$$

Отсюда следует, что $(p-1)|(N-1)$, так что N нечетно. Кроме того, в случае $k \geqslant 2$, имеем $p|(N-1)$, что невозможно, так как p есть делитель N. Итак, каждое число Кармайкла есть произведение различных нечетных простых чисел p с условием $(p-1)|(N-1)$.

Допустим теперь, что $N = pq$, где p, q — различные нечетные простые числа, $p < q$. По доказанному $N - 1 = d(q-1)$ с некоторым натуральным d. Из этого равенства находим $d \equiv 1 \pmod{q}$, а кроме того

$$(q-1)q > pq = N = d(q-1) + 1 > d(q-1).$$

Отсюда следует $d < q$ и, значит, $d = 1$. Но тогда $N = q$, что неверно. Итак, $N = p_1 \cdots p_r$ есть произведение не менее трех различных простых чисел, удовлетворяющих условиям $(p_j - 1)|(N-1)$. □

В 1994г. Алфорд, Гронвилль и Померанс доказали, что множество чисел Кармайкла бесконечно, см. [15]. Существование чисел Кармайкла показывает необходимость уточнения свойств 1)-2) для доказательства непростоты чисел. В настоящее время известны два таких уточнения, позволяющих достаточно эффективно решать рассматриваемую задачу.

Тест 1 (Соловей, Штрассен, [30]). *Пусть $N > 2$ — нечетное натуральное число. Выберем целое число $a, 1 < a < N$.*
1) Если $(a, N) > 1$, то N — составное число.
2) Если $(a, N) = 1$ и

$$a^{\frac{N-1}{2}} \not\equiv \left(\frac{a}{N}\right) \pmod{N},$$

то N — составное число.

Отметим, что в правой части второго утверждения стоит символ Якоби. Справедливость первого утверждения очевидна. Второе следует из первого свойства символа Лежандра, так как для простого числа N символы Якоби и Лежандра совпадают.

Рассмотрим множество $S(N)$, состоящее из всех чисел $a \in \mathbb{Z},\ 1 \leqslant a < N, (a, N) = 1$ с условием, что

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}. \tag{2.16}$$

Если N — простое число, то $\#S(N) = \varphi(N) = N - 1$. Ниже будет доказано, что для составного числа N множество $S(N)$ мало. С помощью вероятностных соображений можно получать информацию о количестве элементов в множестве $S(N)$ и таким образом судить о том будет ли число N составным.

Тест 2 (Миллер, Рабин, [27]). *Пусть $N > 2$ — нечетное натуральное число. Определим целые числа s, t равенством $N - 1 = 2^s t$, где t нечетно. Выберем целое число $a, a > 1$.*
1) Если $(a, N) > 1$, то N составное число.
2) Если $(a, N) = 1$ и выполнены условия

$$a^t \not\equiv 1 \pmod{N}, \quad a^{2^k t} \not\equiv -1 \pmod{N}, \quad k = 0, 1, \ldots, s-1, \tag{2.17}$$

то N составное число.

Справедливо разложение на множители

$$a^{N-1} - 1 = (a^t - 1)(a^t + 1)(a^{2t} + 1) \cdots (a^{2^{s-1}t} + 1).$$

Если N — простое число, то по малой теореме Ферма обе части последнего равенства должны делиться на N. Поскольку N — простое, то хотя бы один из сомножителей в правой части этого равенства должен делиться на N. Значит, хотя бы одно из условий (2.17) будет нарушено. Это доказывает справедливость второго утверждения теста Миллера–Рабина.

Рассмотрим множество $M(N)$ состоящее из чисел $a \in \mathbb{Z},\ 1 \leqslant a < N,\ (a, N) = 1$ и таких, что нарушается хотя бы одно из условий (2.17).

Если N — простое число, то $\#M(N) = N - 1$. Это следует из справедливости второго утверждения теста Миллера–Рабина. Мы покажем ниже, что для составных N множество $M(N)$ будет достаточно малым. Следующая теорема показывает, что в этом отношении тест Миллера–Рабина более практичен, чем тест Соловея–Штрассена.

Теорема 2.8. *Справедливо включение* $M(N) \subset S(N)$.

Доказательство. Утверждение очевидно, если N — простое число. В этом случае оба множества состоят из всех чисел промежутка $1 \leqslant a < N$. Далее будем считать, что N — составное число, $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Выберем $a \in M(N)$. Далее будут рассмотрены два случая.

1. Пусть $a^t \equiv 1 \pmod N$. Тогда

$$a^{\frac{N-1}{2}} = a^{2^{s-1}t} \equiv 1 \pmod N. \tag{2.18}$$

Для любого простого числа $p \mid N$ имеем $a^t \equiv 1 \pmod p$ и, так как t нечетно, то пользуясь свойствами символа Лежандра, находим

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

Тогда

$$\left(\frac{a}{N}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i} = 1.$$

Последнее равенство вместе с (2.18) доказывают, что $a \in S(N)$.

2. Пусть $a^t \not\equiv 1 \pmod N$. Тогда существует целое $h, 0 \leqslant h < s$, с условием

$$a^{2^h t} \equiv -1 \pmod N, \qquad a^{2^{h+1} t} \equiv 1 \pmod N. \tag{2.19}$$

2.1. Докажем, что для любого простого числа $p \mid N$ выполняется неравенство

$$\nu_2(p-1) \geqslant h + 1. \tag{2.20}$$

Обозначим $\beta = \nu_2(p-1)$, и пусть $p-1 = 2^\beta u$, u нечетно. Сравнение $tx \equiv u \pmod{p-1}$ разрешимо, так как $(t, p-1) = (t,u) \mid u$. Пусть v — решение этого сравнения, т.е. $tv \equiv u \pmod{p-1}$. Поскольку u и v имеют одинаковую четность, то v нечетно. Из (2.19) следует $a^{2^h tv} \equiv -1 \pmod{p}$, так что $a^{2^h u} \equiv -1 \pmod{p}$. Учитывая, что согласно малой теореме Ферма должно выполняться сравнение $a^{2^\beta u} \equiv 1 \pmod{p}$, получаем справедливость (2.20).

2.2. Докажем, что для каждого простого числа $p \mid N$ справедливы утверждения:

а) *Если* $\nu_2(p-1) = h+1$, *то* $\left(\frac{a}{p}\right) = -1$.

б) *Если* $\nu_2(p-1) > h+1$, *то* $\left(\frac{a}{p}\right) = 1$.

Будем использовать обозначения, введенные в предыдущем пункте. При $\beta = h+1$ имеем

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

В случае $\beta > h+1$ с помощью второго сравнения (2.19) находим $a^{2^{\beta-1}t} \equiv 1 \pmod{p}$. Поэтому справедливы сравнения

$$\left(\frac{a}{p}\right) \equiv a^{2^{\beta-1}u} \equiv a^{2^{\beta-1}tv} \equiv 1 \pmod{p}.$$

2.3. Далее будем считать, что простые числа $p_1, \ldots, p_r$ пронумерованы так, что последовательность $\nu_2(p_i - 1)$, $i = 1, \ldots, r$, неубывает. Пусть $p_1, \ldots, p_k$, $k \geqslant 0$, — все простые делители N с условиями

$$\nu_2(p_i - 1) = h+1, \qquad \alpha_i \text{ нечетно.}$$

Согласно результатам пункта 2.2 имеем

$$\left(\frac{a}{N}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right) = (-1)^k. \qquad (2.21)$$

Вычислим теперь $a^{\frac{N-1}{2}} \pmod{N}$.

Если $i \geqslant k+1$, то
при $\nu_2(p_i-1) > h+1$ *имеем* $\nu_2(p_i^{\alpha_i}-1) > h+1$;
при $\nu_2(p_i-1) = h+1$ *показатель степени* α_i *четен, так что*

$$\nu_2(p_i^{\alpha_i}-1) = \nu_2(p_i^{\alpha_i/2}-1) + \nu_2(p_i^{\alpha_i/2}+1) \geqslant (h+1)+1 > h+1.$$

Если $i \leqslant k$, то показатель α_i нечетен и $\nu_2(p_i^{\alpha_i}-1) = h+1$. Последнее равенство может быть записано в виде $p_i^{\alpha_i} \equiv 1 \pmod{2^{h+1}}$.

Применив доказанное к тождеству

$$N-1 = p_1^{\alpha_1}\cdots p_r^{\alpha_r} - 1 = \sum_{i=1}^{r}(p_i^{\alpha_i}-1)p_{i+1}^{\alpha_{i+1}}\cdots p_r^{\alpha_r},$$

находим сравнение

$$N-1 \equiv \sum_{i=1}^{k}(p_i^{\alpha_i}-1)p_{i+1}^{\alpha_{i+1}}\cdots p_r^{\alpha_r} \pmod{2^{h+2}} \equiv k2^{h+1} \pmod{2^{h+2}}.$$

Отсюда следует, что

$$\frac{N-1}{2} \equiv k2^h \equiv k2^h t \pmod{2^{h+1}}$$

и, следовательно,

$$\frac{N-1}{2} \equiv k2^h t \pmod{2^{h+1}t}.$$

Учитывая теперь сравнение (2.19) и равенство (2.21), находим

$$a^{\frac{N-1}{2}} \equiv a^{2^h tk} \equiv (-1)^k \equiv \left(\frac{a}{N}\right) \pmod{N}.$$

Значит, и во втором случае выполнено сравнение, определяющее множество $S(N)$, т.е. $a \in S(N)$. Теорема 2.8 доказана. □

Теорема 2.9. *Пусть* N *— натуральное нечетное составное число. Тогда*

$$\#S(N) \leqslant \frac{1}{2}\varphi(N).$$

Доказательство. Обозначим буквой G мультипликативную группу классов вычетов в кольце $\mathbb{Z}/N\mathbb{Z}$, т.е. $G = (\mathbb{Z}/N\mathbb{Z})^*$. Тогда $\#G = \varphi(N)$. Будем использовать обозначение $\overline{a}$ для класса вычетов, содержащего целое число a. Пусть также H — подмножество G, определенное условиями

$$H = \{\overline{a} \in G \mid a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}\},$$

где $(\frac{a}{N})$ — символ Якоби. Обе части последнего сравнения мультипликативны по a. Поэтому множество H замкнуто относительно операции умножения. Так как оно вместе с каждым элементом $\overline{a}$ содержит, как легко видеть, и элемент $\overline{b}$ с условием $ab \equiv 1 \pmod{N}$, то H — подгруппа в G. Если H — собственная подгруппа, то $[G : H] \geqslant 2$ и

$$\#S(N) = \mid H \mid \leqslant \frac{1}{2} \mid G \mid = \frac{1}{2}\varphi(N).$$

Поэтому для завершения доказательства достаточно установить, что H — собственная подгруппа G.

Предположим противное, т.е. что $H = G$. Тогда

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}, \qquad \text{для каждого } \overline{a} \in G. \tag{2.22}$$

Допустим, что $N = M^s$, где M, s — натуральные числа и $s \geqslant 2$. Выберем $a = 1 + M^{s-1}$. Тогда, вычисляя символ Якоби, находим

$$\left(\frac{a}{N}\right) = \left(\frac{a}{M^s}\right) = \left(\frac{a}{M}\right)^s = \left(\frac{1}{M}\right)^s = 1.$$

Из (2.22) следует, что

$$\left(1 + M^{s-1}\right)^{\frac{M^s-1}{2}} \equiv 1 \pmod{M^s}.$$

С помощью формулы Ньютона для бинома получаем

$$\left(1 + M^{s-1}\right)^{\frac{M^s-1}{2}} \equiv 1 + \frac{M^s - 1}{2} M^{s-1} \pmod{M^s}.$$

Поэтому $\frac{M^s-1}{2}M^{s-1} \equiv 0 \pmod{M^s}$ и $M^s - 1 \equiv 0 \pmod{M}$, что неверно.

Так как рассмотренный случай невозможен, заключаем, что $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, где $r \geqslant 2$, и, так как по доказанному N отлично от квадрата, то среди α_i есть нечетные числа. Не уменьшая общности можно считать, что α_1 нечетно.

Пусть a_1 — какой-нибудь квадратичный невычет по модулю p_1 и a — решение системы сравнений

$$a \equiv a_1 \pmod{p_1^{\alpha_1}}, \qquad a \equiv 1 \pmod{p_2^{\alpha_2} \cdots p_r^{\alpha_r}}.$$

Тогда

$$\left(\frac{a}{N}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i} = \left(\frac{a}{p_1}\right)^{\alpha_1} = \left(\frac{a_1}{p_1}\right)^{\alpha_1} = (-1)^{\alpha_1} = -1.$$

Значит, $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ и $a^{\frac{N-1}{2}} \equiv -1 \pmod{p_2}$. Но это противоречит определению a.

Получившееся противоречие завершает доказательство теоремы. □

Оценка теоремы 2.9 точна.

Замечание. *Пусть N — число Кармайкла с условием*

$$\nu_2(N-1) > \nu_2(p_i - 1), \qquad i = 1, \ldots, r. \tag{2.23}$$

Тогда $\#S(N) = \frac{1}{2}\varphi(N)$.

Доказательство. Так как N — число Кармайкла, то $N = p_1 \cdots p_r$, причем $(p_i - 1) \mid (N-1)$, см. теорему 2.7. Пользуясь также (2.23), находим $(p_i - 1) \mid \frac{N-1}{2}$. Так как для каждого $a \in \mathbb{Z}$ с условием $(a, N) = 1$ по малой теореме Ферма выполняется сравнение $a^{p_i-1} \equiv 1 \pmod{p_i}$, то получаем $a^{\frac{N-1}{2}} \equiv 1 \pmod{p_i}$ и, следовательно,

$$a^{\frac{N-1}{2}} \equiv 1 \pmod{N}, \text{ для любого } a \in \mathbb{Z}, \ (a, N) = 1.$$

Это значит, что $H = \{\overline{a} \in G \mid \left(\frac{a}{N}\right) = 1\}$.

Пусть a_1 — квадратичный невычет по модулю p_1 и b — решение системы сравнений

$$b \equiv a_1 \pmod{p_1}, \qquad b \equiv 1 \pmod{p_2 \cdots p_r}.$$

Тогда

$$\left(\frac{b}{N}\right) = \prod_{i=1}^{r} \left(\frac{b}{p_i}\right) = \left(\frac{a_1}{p_1}\right) \prod_{i=2}^{r} \left(\frac{1}{p_i}\right) = \left(\frac{a_1}{p_1}\right) = -1.$$

Это значит, что $\overline{b} \notin H$. Докажем, что $G = H \cup bH$.

Пусть $a \in G \backslash H$, т.е. $\left(\frac{a}{N}\right) = -1$, и c — решение сравнения $bc \equiv a \pmod{N}$. Тогда

$$-1 = \left(\frac{a}{N}\right) = \left(\frac{bc}{N}\right) = \left(\frac{b}{N}\right) \cdot \left(\frac{c}{N}\right) = -\left(\frac{c}{N}\right).$$

Таким обазом, $\left(\frac{c}{N}\right) = 1$. Это значит, что $\overline{c} \in H$ или $\overline{a} \in \overline{b}H$. Итак, доказано, что $[G : H] = 2$ и $\#H = \frac{1}{2}\varphi(N)$. □

Пример. $N = 1729 = 7{\cdot}13{\cdot}19$ — *число Кармайкла, удовлетворяющее (2.23).*

Можно доказать, что числа Кармайкла с условием (2.23) исчерпывают все числа, для которых $\#S(N) = \frac{1}{2}\varphi(N)$.

Теорема 2.10 (Рабин, 1980г.)**.** *Пусть N — нечетное составное число, $N \neq 9$. Тогда $\#M(N) \leqslant \frac{1}{4}\varphi(N)$.*

Пример. *Для $N = 9$ имеем $M(9) = \{1,\ 8\}$ и $\#M(9) = 2 = \frac{1}{3}\varphi(9)$.*

В следующей лемме, пользуясь теоремами 1.16 и 1.17, мы найдем явное выражение для числа $\#M(N)$, участвующего в формулировке теоремы 2.10.

Лемма 2.2. *Пусть $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ — нечетно и*

$$N = 1 + 2^s t, \qquad p_i = 1 + 2^{s_i} t_i, \quad i = 1, \ldots, r,$$

где все $t, t_1, \ldots, t_r$ *нечетны. Если* $s_1 \leqslant \cdots \leqslant s_r$, *то*

$$\#M(N) = \left(1 + \sum_{j=0}^{s_1-1} 2^{jr}\right) \cdot \prod_{i=1}^{r} (t, t_i).$$

Доказательство. Определим множества

$$\mathcal{P} = \{\overline{x} \in (\mathbb{Z}/N\mathbb{Z})^* \mid x^t \equiv 1 \pmod{N}\},$$

$$\mathcal{Q}_j = \{\overline{x} \in (\mathbb{Z}/N\mathbb{Z})^* \mid x^{2^j t} \equiv -1 \pmod{N}\}, \qquad 0 \leqslant j < s.$$

Так как эти множества не пересекаются, то

$$\#M(N) = \#\mathcal{P} + \sum_{j=0}^{s-1} \#\mathcal{Q}_j. \tag{2.24}$$

По теореме 1.16 количество решений сравнения $x^t \equiv 1 \pmod{p_i^{\alpha_i}}$ равно

$$(t, \varphi(p_i^{\alpha_i})) = (t, p_i^{\alpha_i - 1} \cdot 2^{s_i} t_i) = (t, t_i).$$

Пользуясь теоремой 1.17, заключаем, что

$$\#\mathcal{P} = \prod_{i=1}^{r} (t, t_i).$$

Если $j \geqslant s_1$, то сравнение $x^{2^j t} \equiv -1 \pmod{p_1^{\alpha_1}}$ в силу теоремы 1.16 решений не имеет. Действительно, в этом случае

$$(-1)^{\dfrac{\varphi(p_1^{\alpha_1})}{(2^j t,\ \varphi(p_1^{\alpha_1}))}} = (-1)^{\dfrac{p_1^{\alpha_1 - 1} 2^{s_1} t_1}{(2^j t,\ 2^{s_1} t_1)}} = -1.$$

Таким образом, $\#\mathcal{Q}_j = 0$.

Если $j < s_1$, то $j < s_i$, $i = 1, \ldots, r$ и по теореме 1.16 количество решений сравнения $x^{2^j t} \equiv -1 \pmod{p_i^{\alpha_i}}$ равно

$$(2^j t,\ p_i^{\alpha_i - 1} 2^{s_i} t_i) = 2^j (t, t_i).$$

По теореме 1.17 при $j < s_1$ имеем

$$\#\mathcal{Q}_j = 2^{rj} \prod_{i=1}^{r} (t, t_i).$$

Поскольку $p_i \equiv 1 \pmod{2^{s_i}}$, так что $p_i \equiv 1 \pmod{2^{s_1}}$, то $N \equiv 1 \pmod{2^{s_1}}$ и $s \geqslant s_1$. Теперь в силу (2.24) находим

$$\#M(N) = \prod_{i=1}^{r} (t, t_i) + \sum_{j=0}^{s_1-1} 2^{rj} \prod_{i=1}^{r} (t, t_i).$$

Это завершает доказательство леммы. □

Перейдем теперь непосредственно к доказательству теоремы 2.10.

Доказательство. Поскольку $\varphi(N) = \prod_{i=1}^{r} p_i^{\alpha_i - 1} 2^{s_i} t_i$, то пользуясь леммой 2.2, находим

$$\frac{\#M(N)}{\varphi(N)} = \prod_{i=1}^{r} \left(\frac{(t, t_i)}{t_i} \cdot p_i^{1-\alpha_i} \cdot 2^{-s_i} \right) (1 + \sum_{j=0}^{s_1-1} 2^{jr}) \leqslant$$

$$\leqslant \left(1 + \frac{2^{s_1 r} - 1}{2^r - 1} \right) \cdot 2^{-r s_1} \cdot \prod_{i=1}^{r} p_i^{1-\alpha_i} \leqslant 2^{1-r} \prod_{i=1}^{r} p_i^{1-\alpha_i}. \quad (2.25)$$

Последнее неравенство имеет место в силу того, что выражение

$$\left(1 + \frac{2^{s_1 r} - 1}{2^r - 1} \right) \cdot 2^{-r s_1} = \left(1 - \frac{1}{2^r - 1} \right) \cdot 2^{-r s_1} + \frac{1}{2^r - 1}$$

есть невозрастающая функция в зависимости от s_1.

Далее рассмотрим несколько случаев.

1) $r = 1$.

В этом случае из (2.25) находим

$$\frac{\#M(N)}{\varphi(N)} \leqslant p_1^{1-\alpha_1}.$$

Так как по условию N — составное число, то в рассматриваемом случае $\alpha_1 \geqslant 2$ и при $p_1 \geqslant 5$ имеем $p_1^{1-\alpha_1} \leqslant p_1^{-1} \leqslant 1/5$.

Если же $p_1 = 3$, то согласно условию должно выполняться неравенство $\alpha_1 \geqslant 3$, так что $p_1^{1-\alpha_1} \leqslant 1/9$.

Итак, при $r = 1$ нужное неравенство выполняется. Далее будем считать, что $r \geqslant 2$.

2) $r \geqslant 3$.

В этом случае из (2.25) следует

$$\frac{\#M(N)}{\varphi(N)} \leqslant 2^{1-r} \leqslant \frac{1}{4}.$$

Нужное неравенство выполнено. Далее будем считать, что $r = 2$.

3) Существует $\alpha_i \geqslant 2$.

Из (2.25) находим

$$\frac{\#M(N)}{\varphi(N)} \leqslant \frac{1}{2} \cdot \frac{1}{p_i} \leqslant \frac{1}{6}.$$

И в этом случае нужное неравенство доказано. В дальнейшем можно считать, что $N = p_1 \cdot p_2$, причем p_j различны.

4) $N = p_1 \cdot p_2,\ s_1 < s_2$.

В этом случае имеем

$$\frac{\#M(N)}{\varphi(N)} \leqslant \left(1 + \frac{2^{2s_1} - 1}{3}\right) \cdot 2^{-2s_1-1} = \frac{2^{-2s_1} + 2^{-1}}{3} \leqslant \frac{1}{4}.$$

Остался последний случай.

5) $N = p_1 \cdot p_2,\ s_1 = s_2$.

В этом случае

$$\frac{\#M(N)}{\varphi(N)} = \left(1 + \frac{2^{2s_1} - 1}{3}\right) \cdot 2^{-2s_1} \prod_{i=1}^{2} \frac{(t,\ t_i)}{t_i} \leqslant \frac{1}{2} \cdot \prod_{i=1}^{2} \frac{(t,\ t_i)}{t_i}. \quad (2.26)$$

Так как $p_1 \neq p_2$, то $t_1 \neq t_2$. Пусть $t_1 > t_2$. Если $(t,\ t_1) = t_1$, т.е. $t_1 \mid t$, то $N \equiv 1 \pmod{t_1}$. Из тождества

$$N - 1 = p_2(p_1 - 1) + p_2 - 1$$

теперь следует, что $t_1 \mid (p_2 - 1)$ или $t_1 \mid 2^{s_1} t_2$. Последняя делимость невозможна, так как t_1 нечетно и $t_1 > t_2$.

Получившееся противоречие доказывает, что $t_1 \nmid t$ и, значит, согласно (2.26)

$$\frac{\#M(N)}{\varphi(N)} \leqslant \frac{1}{2} \cdot \frac{(t,\ t_1)}{t_1} \leqslant \frac{1}{6}.$$

Это завершает доказательство теоремы 2.10. □

Следующий ниже вероятностный алгоритм, удостоверяет, что заданное число — составное. Он основан на тесте Миллера–Рабина.

Алгоритм 2.5. Данные: *Нечетное составное число* $N > 9$.
Доказать: *Число* N *составное.*

1) Вычислить натуральные числа s, t *такие, что* $N - 1 = 2^s t$ *и* t *нечетно.*
2) Выбрать случайным образом число $a, 1 < a < N$ *и проверить выполнимость условий 1) и 2) теста Миллера–Рабина.*
3) Если хотя бы одно из условий теста выполнено, то число N *составное; СТОП.*
4) Если оба условия теста нарушаются, то перейти в пункт 2.

Сложность этого вероятностного алгоритма есть $O(\ln p)$. Действительно, согласно определению множества $M(N)$ любое целое число a, $1 \leqslant a < N$, не принадлежащее этому множеству, подтвердит с помощью теста Миллера–Рабина, что число N составное. Значит по теореме 2.10 при случайном выборе a мы с вероятностью

$$\rho = \frac{N - 1 - \#M(N)}{N - 1} \geqslant 1 - \frac{1}{4}\frac{\varphi(N)}{N - 1} \geqslant \frac{3}{4}$$

попадаем на хорошее a (свидетель непростоты). Пусть A_k — событие, состоящее в том, что при k испытаниях $k - 1$ раз попадались плохие a и в k-й раз попалось хорошее. Тогда $p(A_k) = (1 - \rho)^{k-1}\rho$.

При фиксированном a для проверки условий теста 2 требуется, как легко видеть, $O(\ln N)$ арифметических операций. Математиче-

ское ожидание количества операций в алгоритме есть

$$O(\ln N) \cdot \sum_{k=1}^{\infty} k(1-\rho)^{k-1}\rho = \rho^{-1} \cdot O(\ln N) = O(\ln N).$$

На практике алгоритм 2.5 является очень важной составляющей общей стратегии доказательства простоты чисел. Если заданное число N, о котором не известно простое оно или составное, прошло достаточно много шагов алгоритма 2.5, то оно наверное будет простым. Ведь вероятность составному числу N выдержать d испытаний не превосходит 4^{-d}. Таким образом, остается только вопрос, как доказать, что это число простое? Мы обсудим такие алгоритмы в главе 4.

2.7 Быстрые алгоритмы умножения и деления целых чисел.

2.7.1 Алгоритм Карацубы умножения целых чисел.

Пусть a и b — произвольные натуральные числа. Они имеют, соответственно, по $[\log_2 a]+1$ и $[\log_2 b]+1$ цифр в двоичной записи. Пусть n — минимальное целое число, такое что

$$\max\Big([\log_2 a]+1,\ [\log_2 b]+1\Big) \leqslant 2^n.$$

Описываемый ниже метод сводит задачу умножения чисел a и b к нескольким умножениям чисел, длина которых в двоичной записи на превосходит $k = 2^{n-1}$, и рекурсивно применяется к этим новым числам. По этой причине принцип, лежащий в основе данного метода, называется *принципом "разделяй и властвуй"*, а также *принципом дихотомии.*

Представим числа a и b в виде

$$a = a_1 + 2^k a_2, \qquad b = b_1 + 2^k b_2,$$

где a_1, a_2, b_1, b_2 — числа, длина которых в двоичной записи не превосходит k. Справедливо равенство

$$ab = a_1b_1 + 2^k((a_1 + a_2)(b_1 + b_2) - (a_1b_1 + a_2b_2)) + 2^{2k}a_2b_2. \quad (2.27)$$

Числа $a_1 + a_2$ и $b_1 + b_2$ могут иметь в двоичной записи длину $k + 1$, но их можно представить в виде

$$a_1 + a_2 = a_3 + 2a_4, \qquad b_1 + b_2 = b_3 + 2b_4,$$

где числа a_4 и b_4 имеют длину не больше, чем k, а числа a_3 и b_3 суть нули или единицы. Стало быть, (2.27) можно переписать в виде

$$ab = a_1b_1+2^k(a_3b_3+2a_3b_4+2b_3a_4+4a_4b_4-(a_1b_1+a_2b_2))+2^{2k}a_2b_2. \quad (2.28)$$

Таким образом, исходная задача при помощи нескольких операций сложения, вычитания и домножения на степень двойки (которое является просто-напросто приписыванием соответствующего числа нулей) сводится к вычислению трех произведений a_1b_1, a_2b_2 и a_4b_4, каждое из которых является произведением чисел длины не более, чем $k = 2^{n-1}$. К этим трем произведениям рекурсивно применяем описанные рассуждения.

Обозначим через L_n количество битовых операций, необходимое для вычисления данным методом произведения двух произвольных чисел, длина которых в двоичной записи не превосходит 2^n. Тогда найдется такая константа C, что $L_0 \leqslant C$ и

$$L_n \leqslant 3L_{n-1} + 2^nC, \qquad n \geqslant 1.$$

Отсюда по индукции находим, что

$$L_n \leqslant C(3^{n+1} - 2^{n+1}).$$

Действительно, в предположении, что $L_{n-1} \leqslant C(3^n - 2^n)$, получаем:

$$L_n \leqslant 3C(3^n - 2^n) + C2^{n+1} = C(3^{n+1} - 2^{n+1}).$$

Стало быть,

$$L_n = O((2^n)^{\log_2 3}).$$

Таким образом, если a и b — натуральные числа и $a \geqslant b$, то перемножить их можно за $O((\ln a)^{\log_2 3})$ битовых операций.

2.7.2 Дискретное преобразование Фурье и алгоритм Шенхаге–Штрассена умножения целых чисел.

Дискретное преобразование Фурье.

Пусть $\mathcal{R}$ — произвольное ассоциативное коммутативное кольцо с единицей и d — некоторое натуральное число. Обозначим $\overline{d}$ элемент кольца $\mathcal{R}$, равный сумме d единиц этого кольца. Предположим, что $\overline{d}$ обратим в $\mathcal{R}$. Далее, предположим, что в $\mathcal{R}$ есть примитивный корень из единицы степени d, то есть такой элемент g, что

$$d = \min\{k \in \mathbb{N} \mid g^k = 1\}.$$

Отметим, что для целого t равенство $g^t = 1$ имеет место в том и только том случае, если $d \mid t$.

Определение 2.5. Дискретным преобразованием Фурье *называется отображение, сопоставляющее каждому набору* $x = (x_0, \ldots, x_{d-1}) \in \mathcal{R}^d$ *некоторый другой набор* $\hat{x} = (\hat{x}_0, \ldots, \hat{x}_{d-1}) \in \mathcal{R}^d$, *такой что*

$$\hat{x}_i = \sum_{j=0}^{d-1} x_j g^{ij}, \quad i = 0, \ldots, d-1. \tag{2.29}$$

Как видно из следующей леммы, обращение преобразования Фурье весьма напоминает само преобразование Фурье.

Лемма 2.3. *Справедливы равенства*

$$x_i = \overline{d}^{\,-1} \sum_{j=0}^{d-1} \hat{x}_j g^{-ij}, \quad i = 0, \ldots, d-1.$$

Доказательство. Действительно,

$$\overline{d}^{\,-1} \sum_{j=0}^{d-1} \hat{x}_j g^{-ij} = \overline{d}^{\,-1} \sum_{j=0}^{d-1} \Big(\sum_{k=0}^{d-1} x_k g^{jk} \Big) g^{-ij} = \overline{d}^{\,-1} \sum_{k=0}^{d-1} x_k \sum_{j=0}^{d-1} g^{j(k-i)} = x_i.$$

Последнее равенство следует из того факта, что для любого целого t, не делящегося на d,

$$\sum_{j=0}^{d-1} g^{tj} = \frac{1-g^{td}}{1-g^t} = 0.$$

□

Таким образом, *для того, чтобы вычислить обратное преобразование Фурье с примитивным корнем g, нужно вычислить прямое преобразование Фурье с примитивным корнем g^{-1}, и каждую координату результата разделить в кольце $\mathcal{R}$ на d.*

Свертка и преобразование Фурье.

Многие задачи теории чисел, в частности задача умножения двух чисел, используют явно или косвенно понятие свертки:

Определение 2.6. *Пусть заданы два набора $x = (x_0, \ldots, x_{d-1}) \in \mathcal{R}^d$ и $y = (y_0, \ldots, y_{d-1}) \in \mathcal{R}^d$. Их* сверткой $x * y$ *называется набор $z = (z_0, \ldots, z_{d-1}) \in \mathcal{R}^d$, такой что*

$$z_k = \sum_{i+j \equiv k \pmod d} x_i y_j, \qquad k = 0, \ldots, d-1.$$

Преобразование Фурье позволяет свести задачу вычисления свертки к вычислению покомпонентного произведения. Покомпонентное произведение наборов $x = (x_0, \ldots, x_{d-1}) \in \mathcal{R}^d$ и $y = (y_0, \ldots, y_{d-1}) \in \mathcal{R}^d$ будем обозначать $x \cdot y$, то есть

$$x \cdot y = (x_0 y_0, \ldots, x_{d-1} y_{d-1}).$$

Теорема 2.11. *Пусть заданы два набора $x = (x_0, \ldots, x_{d-1}) \in \mathcal{R}^d$, $y = (y_0, \ldots, y_{d-1}) \in \mathcal{R}^d$ и пусть $z = x * y$. Тогда*

$$\hat{z} = \hat{x} \cdot \hat{y}.$$

Доказательство. Действительно, для любого $l \in \{0, \ldots, d-1\}$

$$\sum_{k=0}^{d-1} z_k g^{lk} = \sum_{k=0}^{d-1} g^{lk} \left(\sum_{i+j \equiv k \pmod d} x_i y_j \right) = \\ = \sum_{i=0}^{d-1} x_i g^{li} \sum_{k=0}^{d-1} g^{l(k-i)} y_{k-i} = \sum_{i=0}^{d-1} x_i g^{li} \sum_{j=0}^{d-1} y_j g^{lj},$$

Здесь использовалось выполняющееся в кольце $\mathcal{R}$ равенство $g^d = 1$. □

Таким образом, *для того, чтобы вычислить свертку двух наборов, нужно сначала вычислить их преобразования Фурье, затем вычислить покомпонентное произведение получившихся наборов, и наконец, вычислить обратное преобразование Фурье.*

Быстрое преобразование Фурье.

Вычисление преобразования Фурье с помощью формулы (2.29), как легко видеть, требует $O(d^2)$ арифметических операций в кольце $\mathcal{R}$. Если же воспользоваться принципом "разделяй и властвуй" (на котором, напомним, основывается алгоритм Карацубы), то преобразование Фурье можно сосчитать гораздо быстрее — за $O(d \ln d)$ арифметических операций. Соответствующий алгоритм вычисления преобразования Фурье носит название *быстрого преобразования Фурье.*

Отметим один терминологический момент: дискретное преобразование Фурье — это *преобразование*, определяемое соотношениями (2.29), в то время как быстрое преобразование Фурье — это *алгоритм* его вычисления.

Пусть, для простоты, d — это степень двойки. Быстрое преобразование Фурье основывается на следующем простом соотношении:

$$\hat{x}_i = \sum_{j=0}^{d-1} x_j g^{ij} = \sum_{j=0}^{d/2-1} x_{2j} (g^2)^{ij} + g^i \sum_{j=0}^{d/2-1} x_{2j+1} (g^2)^{ij}. \qquad (2.30)$$

Данное тождество сводит вычисление преобразования Фурье набора длины d к вычислению преобразования Фурье двух наборов длины $d/2$. При этом g^2 автоматически будет примитивным корнем степени $d/2$. Получаем рекурсивный алгоритм:

Алгоритм 2.6. *Данные: Число d, равное некоторой степени двойки, набор $x = (x_0, \dots, x_{d-1}) \in \mathcal{R}^d$, g — примитивный корень из единицы степени d.*
Найти: Преобразование Фурье $\hat{x} = (\hat{x}_0, \dots, \hat{x}_{d-1})$.
1. Если $d = 1$, положить $\hat{x} = x$. СТОП.
2. Определить наборы

$$y = (y_0, y_1, \dots, y_{d/2-1}) \in \mathcal{R}^{d/2}, \quad z = (z_0, z_1, \dots, z_{d/2-1}) \in \mathcal{R}^{d/2}$$

следующим образом:

$$y = (y_0, y_1, \dots, y_{d/2-1}) = (x_0, x_2, \dots, x_{d-2}),$$
$$z = (z_0, z_1, \dots, z_{d/2-1}) = (x_1, x_3, \dots, x_{d-1}).$$

3. Взяв g^2 в качестве примитивного корня из единицы степени $d/2$, вычислить $\hat{y}$ и $\hat{z}$, применив рекурсивно данный алгоритм.
4. Определить наборы $u = (u_0, \dots, u_{d-1}) \in \mathcal{R}^d$, $v = (v_0, \dots, v_{d-1}) \in \mathcal{R}^d$ следующим образом:

$$u = (u_0, \dots, u_{d-1}) = (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_{d/2-1}, \hat{y}_0, \hat{y}_1, \dots, \hat{y}_{d/2-1}),$$
$$v = (v_0, \dots, v_{d-1}) = (\hat{z}_0, \hat{z}_1, \dots, \hat{z}_{d/2-1}, \hat{z}_0, \hat{z}_1, \dots, \hat{z}_{d/2-1}).$$

5. Положить $\hat{x}_i = u_i + g^i v_i$, $i = 0, \dots, d-1$. СТОП.

Корректность этого алгоритма следует из выполняющихся согласно (2.30) равенств

$$\hat{x}_i = \hat{y}_i + g^i \hat{z}_i, \qquad \hat{x}_{i+d/2} = \hat{y}_i + g^{i+d/2} \hat{z}_i, \qquad 0 \leqslant i < d/2.$$

Обозначим через L_d количество сложений и умножений в кольце $\mathcal{R}$, необходимое алгоритму 2.6 для вычисления преобразования Фурье

набора длины d. Для выполнения всех вычислений в пункте 5 требуется $O(d)$ операций. Следовательно, существует такая константа C, что

$$L_d \leqslant 2L_{d/2} + Cd, \qquad L_2 \leqslant 2C.$$

Отсюда по индукции находим $L_d \leqslant Cd \log_2 d$ и, значит,

$$L_d = O(d \ln d).$$

Действительно, в предположении, что

$$L_{d/2} \leqslant C\frac{d}{2} \log_2 \frac{d}{2},$$

получаем:

$$L_d \leqslant Cd \log_2 \frac{d}{2} + Cd = Cd \log_2 d.$$

Отметим, что все умножения, производящиеся в алгоритме 2.6 являются умножениями на элемент g, что бывает очень удобно при подходящим образом выбранном g.

Алгоритм Шенхаге–Штрассена.

Излагаемый в данном пункте алгоритм умножения натуральных чисел использует преобразование Фурье в кольце $\mathcal{R} = \mathbb{Z}/(2^m + 1)\mathbb{Z}$. В этом кольце элемент 2 является примитивным корнем из единицы степени $2m$. Действительно, из равенства

$$2^{2m} - 1 = (2^m + 1)(2^m - 1)$$

следует, что порядок r элемента $2 \in \mathcal{R}$ есть делитель числа $2m$. С другой стороны, из равенства

$$2^r - 1 = 2^{r-m}(2^m + 1) - (2^{r-m} + 1)$$

находим $2^m + 1 \mid 2^{r-m} + 1$, так что $m \leqslant r - m$ и $r \geqslant 2m$.

Поэтому для любого $d \mid m$ в качестве примитивного корня из единицы степени d можно брать элемент $2^{2m/d}$, что позволяет в случае

обратимости d по модулю 2^m+1 говорить о прямом и обратном преобразованиях Фурье наборов длины d. Отметим, что если d является степенью двойки, то требование обратимости выполняется автоматически, поскольку 2 обратимо по модулю 2^m+1.

Пусть a, b — произвольные натуральные числа, $a, b < 2^n$, n кратно 8. Рассмотрим какое-нибудь $k \in \mathbb{N}$, $k \geqslant 4$, такое что $2^k \mid 2n$, и минимальное целое число m, такое что

$$m \geqslant 4n/2^k + k \qquad \text{и} \qquad 2^k \mid 2m. \tag{2.31}$$

Рассмотрим наборы $x = (x_0, \ldots, x_{2^k-1})$ и $y = (y_0, \ldots, y_{2^k-1})$ длины 2^k, определяемые соотношениями

$$a = \sum_{i=0}^{2^k-1} x_i \bigl(2^{2n/2^k}\bigr)^i, \qquad 0 \leqslant x_i < 2^{2n/2^k}, \tag{2.32}$$

$$b = \sum_{i=0}^{2^k-1} y_i \bigl(2^{2n/2^k}\bigr)^i, \qquad 0 \leqslant y_i < 2^{2n/2^k}, \tag{2.33}$$

Тогда

$$ab = \sum_{i=0}^{2^{k+1}-2} z_i \bigl(2^{2n/2^k}\bigr)^i, \tag{2.34}$$

где

$$z_i = \sum_{j+l=i} x_j y_l. \tag{2.35}$$

Для каждого из z_i справедливы неравенства $0 \leqslant z_i \leqslant 2^{4n/2^k+k} < 2^m+1$. Стало быть, все x_i, y_i, z_i совпадают со своими остатками при делении на 2^m+1, то есть наборы x, y и набор $z = (z_0, \ldots, z_{2^k-2}, z_{2^k-1})$, где $z_{2^k-1} = 0$, можно рассматривать как элементы $(\mathbb{Z}/(2^m+1)\mathbb{Z})^{2^k}$. При этом $x_i = y_i = 0$ для всех $i = 2^{k-1}, \ldots, 2^k-1$, поскольку согласно условию $a, b < 2^n$. Следовательно, в силу (2.35),

$$z = x * y,$$

где свертка берется в кольце $\mathbb{Z}/(2^m+1)\mathbb{Z}$.

Поскольку наборы x и y имеют длину 2^k, их свертку можно вычислять при помощи преобразования Фурье в кольце $\mathbb{Z}/(2^m+1)\mathbb{Z}$, причем, как было сказано в начале данного пункта, в качестве примитивного корня из единицы можно взять элемент $g = 2^{2m/2^k}$.

Получаем следующий алгоритм:

Алгоритм 2.7. *Данные: Числа $a, b \in \mathbb{Z}$, $a \geqslant b \geqslant 0$, и число $k \in \mathbb{N}$, $k \geqslant 4$ (обычно k берут не большим 10).*
Найти: Произведение ab.
1. Если $b = 0$, положить $ab = 0$, СТОП. Если $b = 1$, положить $ab = a$, СТОП.
2. Положить n равным минимальному целому числу, кратному 2^k и большему, чем $\log_2 a$. Положить m равным минимальному целому числу, удовлетворяющему условиям (2.31).
3. Если $m \geqslant n$, вычислить произведение ab каким-нибудь стандартным способом, СТОП.
4. Определить наборы $x = (x_0, \ldots, x_{2^k-1})$ и $y = (y_0, \ldots, y_{2^k-1})$ соотношениями (2.32) и (2.33).
5. Рассматривая x и y как элементы $(\mathbb{Z}/(2^m+1)\mathbb{Z})^{2^k}$, вычислить их преобразования Фурье $\hat{x} = (\hat{x}_0, \ldots, \hat{x}_{2^k-1})$ и $\hat{y} = (\hat{y}_0, \ldots, \hat{y}_{2^k-1})$ при помощи алгоритма быстрого преобразования Фурье, взяв $g = 2^{2m/2^k}$ в качестве примитивного корня из единицы.
6. Вычислить $\hat{x} \cdot \hat{y} = (\hat{x}_0\hat{y}_0, \ldots, \hat{x}_{2^k-1}\hat{y}_{2^k-1})$. Для этого при каждом $i = 0, \ldots, 2^k-1$ рассмотреть $\hat{x}_i$, $\hat{y}_i$ как числа от 0 до 2^m, применить для вычисления их произведения рекурсивно данный алгоритм, а результат привести по модулю 2^m+1.
7. Вычислить обратное преобразование Фурье набора $\hat{x} \cdot \hat{y}$, то есть найти такой набор $z = (z_0, \ldots, z_{2^k-1})$, что $\hat{z} = \hat{x} \cdot \hat{y}$.
8. Считая z_i числами от 0 до 2^m, вычислить ab по формуле (2.34).

Во всех пунктах данного алгоритма, кроме пунктов 3 и 6, используется три вида операций: сложение, умножение на степень двойки и приведение по модулю 2^m+1. Умножение на степень двойки в двоичной записи делается быстро, ибо для этого нужно всего лишь при-

писать соответствующее число нулей. Найти же остаток от числа, записанного в двоичной записи, при делении на $2^m + 1$ тоже весьма просто: ввиду сравнения $2^m \equiv -1 \pmod{2^m + 1}$ достаточно разбить число на блоки по 2^m цифр и вычислить знакопеременную сумму получившихся чисел, после чего к результату, если он все еще больше, чем 2^m, применить эту же процедуру.

Авторами работы [29] был проведен тщательный анализ рекурсии в пункте 6 и доказано, что асимптотически алгоритм требует $O(n \ln n \ln\ln n)$ битовых операций для умножения двух натуральных чисел, длина которых в двоичной записи не превосходит n.

Предполагается, что асимптотически самый быстрый (пока не придуманный) алгоритм имеет сложность $O(n \ln n)$, то есть сложность алгоритма Шенхаге–Штрассена имеет лишний множитель $\ln\ln n$. Заменить этот множитель на более медленно растущую функцию удалось лишь спустя 35 лет после того, как был придуман алгоритм Шенхаге–Штрассена: в работе [22] был предложен алгоритм сложности $n \ln n\, 2^{O(\ln^* n)}$, где функция $\ln^* x$ рекурсивно определяется на $\mathbb{R}_+$ следующим образом:

$$\ln^* x = \begin{cases} 0, & \text{если } x \leqslant 1; \\ 1 + \ln^*(\ln x), & \text{если } x > 1. \end{cases}$$

Эта функция растет медленнее, чем любая итерация логарифма, однако совсем избавиться от растущего множителя пока никому не удалось.

2.7.3 Быстрый алгоритм деления целых чисел.

Как будет показано в данном пункте, целые числа можно делить друг на друга с остатком за время, всего лишь в несколько раз большее, чем время, требуемое для их умножения. Таким образом, имея алгоритм быстрого умножения, мы сразу получим алгоритм быстрого деления.

Пусть a, b — произвольные натуральные числа. Для того, чтобы найти неполное частное и остаток от деления a на b, то есть такие натуральные числа q и r, что $a = qb + r$, $0 \leqslant r < b$, можно вычислить с хорошей точностью число $1/b$, а затем умножить результат при помощи алгоритма быстрого умножения на a. Так мы получим некоторое приближение числа q, при помощи которого можно будет достаточно быстро найти само q, ведь q — целое число. Остаток r найдется по формуле $r = a - qb$ за время, в основном ограниченное временем умножения чисел q и b.

В оставшейся части данного пункта мы опишем, как строить приближения числа $1/b$.

Вместо $1/b$ удобно приближать число $1/\beta$, где $\beta = b/2^n$ и n таково, что $2^{n-1} \leqslant b < 2^n$. Тогда $1/2 \leqslant \beta < 1$ и

$$\beta = \sum_{i=1}^{\infty} \beta_i 2^{-i}, \qquad \beta_i \in \{0, 1\}, \qquad \beta_1 = 1.$$

Будем искать приближения к числу $1/\beta$ при помощи метода Ньютона численного решения уравнений вида $f(x) = 0$, где $f(x)$ — некоторая дифференцируемая функция. Напомним, что при заданном x_0 последовательность $\{x_k\}_{k=0}^{\infty}$ приближений к решению такого уравнения определяется рекуррентным соотношением

$$x_k = x_{k-1} - \frac{f(x_{k-1})}{f'(x_{k-1})}, \qquad k \in \mathbb{N}. \tag{2.36}$$

Для наших целей нужно взять функцию $f(x) = 1/x - \beta$. Тогда $f'(x) = -1/x^2$ и рекуррентное соотношение (2.36) принимает вид

$$x_k = 2x_{k-1} - \beta x_{k-1}^2, \qquad k \in \mathbb{N}. \tag{2.37}$$

В качестве x_0 возьмем $3/2$. Тогда

$$|1/\beta - x_0| \leqslant 1/2. \tag{2.38}$$

Если x_k определять формулой (2.37), то для каждого $k \in \mathbb{N}$ будет справедливо соотношение

$$1/\beta - x_k = \beta(1/\beta - x_{k-1})^2,$$

откуда видим, что, в силу (2.38),

$$0 \leqslant 1/\beta - x_k \leqslant 2^{-2^k}, \qquad \forall k \in \mathbb{N}. \tag{2.39}$$

Таким образом, если пользоваться формулой (2.37), то за k итераций можно вычислить $1/\beta$ с точностью 2^{-2^k}. Но в указанном виде эта формула предполагает умножение чисел, длина которых в двоичной записи сравнима с длиной числа $\beta = \frac{b}{2^n}$. То есть в итоге деление таким методом займет существенно больше времени, чем умножение.

Чтобы обойти эту сложность, мы положим

$$t_k = \sum_{i=1}^{2^k+3} \beta_i 2^{-i}, \qquad k \in \mathbb{N},$$

и рассмотрим вместо последовательности $\{x_k\}_{k=0}^{\infty}$, задаваемой соотношением (2.37), последовательность $\{y_k\}_{k=0}^{\infty}$, которую определим следующим образом:

$$y_0 = x_0, \qquad y_k = 2y_{k-1} - t_k y_{k-1}^2 + r_k, \qquad k \in \mathbb{N}, \tag{2.40}$$

где r_k — такое число из полуинтервала $[0, 2^{-2^k-1})$, что величина

$$2^{2^k+1}(2y_{k-1} - t_k y_{k-1}^2 + r_k)$$

является целым числом (такое r_k, очевидно, единственно).

Тогда для каждого $k \in \mathbb{N}$

$$\begin{aligned} 1/\beta - y_k &\leqslant 1/\beta - 2y_{k-1} + t_k y_{k-1}^2 \leqslant \\ &\leqslant 1/\beta - 2y_{k-1} + \beta y_{k-1}^2 = \beta(1/\beta - y_{k-1})^2. \end{aligned} \tag{2.41}$$

С другой стороны, из (2.40) видим, что

$$1/t_k - y_k = t_k(1/t_k - y_{k-1})^2 - r_k > -r_k, \tag{2.42}$$

то есть

$$\begin{aligned} 1/\beta - y_k \geqslant 1/\beta - 1/t_k - r_k = \frac{t_k - \beta}{t_k\beta} - r_k \geqslant \\ \geqslant -2^{-2^k-3+2} - 2^{-2^k-1} \geqslant -2^{-2^k}. \end{aligned} \tag{2.43}$$

Из (2.38), (2.41) и (2.43) получаем, что

$$|1/\beta - y_k| \leqslant 2^{-2^k}, \qquad k \in \mathbb{N}. \tag{2.44}$$

И при этом для вычисления y_k, кроме сложений и округлений, нужно вычислить $t_k y_{k-1}^2$, тогда как длина t_k в двоичной записи не превосходит $2^k + 3$, длина y_{k-1} не превосходит $2^{k-1} + 1$, а длина y_{k-1}^2 не превосходит $2^k + 2$.

Стало быть, если для всех встречающихся умножений использовать алгоритм, сложность которого равна $O(nf(n))$, где n — это длина перемножаемых чисел в двоичной записи, а f — какой-нибудь неубывающая функция, то для того, чтобы вычислить $1/\beta$ с точностью до 2^{-2^m}, потребуется

$$O\Big(\sum_{k=1}^{m} 2^k f(2^k)\Big) = O\Big(f(2^m)\sum_{k=1}^{m} 2^k\Big) = O(2^m f(2^m))$$

битовых операций.

Таким образом, сложность описанного алгоритма поиска обратного имеет такую же асимптотику, как и сложность используемого им алгоритма умножения.

Определим m как наименьшее натуральное число, удовлетворяющее неравенству $2^m \geqslant 2 + \log_2 a$. Тогда $y_m = c/2^{2^m+1}$, где c — целое число. Из неравенства (2.44) следует, что $0 < y_m < 4$ и потому $0 < c < 2^{2^m+3}$.

Из неравенства

$$|1/\beta - y_m| = \left|\frac{2^n}{b} - \frac{c}{2^{2^m+1}}\right| \leqslant 2^{-2^m}$$

следует

$$\left|\frac{a}{b} - \frac{ac}{2^{n+2^m+1}}\right| \leqslant a \cdot 2^{-n-2^m} \leqslant 2^{-n-2} \leqslant \frac{1}{4}\,.$$

Так как $a = bq + r$ и $0 \leqslant r < b$, то

$$\left|q - \frac{ac}{2^{n+2^m+1}}\right| \leqslant \frac{5}{4}. \tag{2.45}$$

Учитывая, что $\log_2 a \leqslant 2^m$ и $\log_2 c \leqslant 2^m + 3$, заключаем, что произведение ac может быть вычислено за $O(2^m m \log_2 m)$ битовых операций. Неравенству (2.45) удовлетворяет не более двух целых чисел, одно из которых есть $s = \left[ac \cdot 2^{-n-2^m-1}\right]$. Если $bs > a$, то $q = s - 1$. Если $bs \leqslant a - b$, то $q = s + 1$. Если же $a - b < bs \leqslant a$, то $q = s$.

Из этих рассуждений следует, что сложность вычисления неполного частного и остатка от деления a на b имеет такую же асимптотику, как и сложность используемого алгоритма умножения.

Глава 3

Разложение многочленов на множители над конечными полями

В параграфе 2.5 рассматривалась задача решения сравнения $x^2 \equiv a \pmod{p}$, где p — простое число. По другому эту задачу можно сформулировать так: разложить на линейные множители над конечным полем F_p многочлен $x^2 - a$. В этой главе подобные вопросы будут обсуждаться для произвольных многочленов и произвольных конечных полей.

Пусть p — простое число, $q = p^m$ и $F = F_q$ — конечное поле. Пусть также $f(x) \in F[x],\ \deg f = n \geqslant 2$. Рассматриваются две задачи.

1. Разложить $f(x)$ на неприводимые множители над полем F.

2. Найти все корни $f(x)$, принадлежащие F.

Вторая задача есть частный случай первой. Тем не менее ниже мы укажем алгоритм, сводящий решение первой задачи ко второй, и покажем, как может быть решена вторая задача.

Ясно, что эти задачи достаточно рассматривать для унитарных многочленов, т.е. многочленов старший коэффициент которых равен 1. Именно этот случай и будет рассматриваться в дальнейшем.

Обсудим несколько упрощающих действий. Пусть $f'(x)$ — производная $f(x)$, и $d(x) = (f(x), f'(x))$ — наибольший общий делитель указанных многочленов.

Возможны три случая.

1) $d(x) = f(x)$.

В этом случае $f'(x) = 0$ и $f(x) = g(x)^p$, где $g(x) \in F[x]$. Таким образом, задача сводится к разложению на множители или нахождению корней многочлена $g(x)$ меньшей степени.

2) $0 < \deg d(x) < \deg f(x)$.

В этом случае $d(x)$ — нетривиальный делитель $f(x)$ и задача сводится к разложению на множители или нахождению корней у многочленов $d(x)$, $f(x)/d(x)$, имеющих меньшую, чем $f(x)$, степень. В частности, многочлен $f(x)/d(x)$ равен произведению тех неприводимых делителей, которые входят в разложение $f(x)$ в степени, не кратной p.

3) $d(x) = 1$.

В этом случае многочлен $f(x)$ не имеет кратных корней. Общий случай, как указано выше, всегда сводится к этому. Именно он и будет рассматриваться в дальнейшем.

В этой главе будут использоваться сравнения в кольце многочленов над полем F. Модулем в таком случае является многочлен положительной степени. Все свойства сравнений в кольце многочленов $F[x]$ подобны свойствам числовых сравнений, обсуждавшихся в первой главе. Доказательства их похожи, и обычно рассматриваются в курсе алгебры.

3.1 Алгоритм Берлекемпа

Пусть $f(x)$ — унитарный многочлен без кратных корней. Ниже описывается алгоритм разложения его на неприводимые множители, предложенный в 1967 году Берлекемпом, [16].

Лемма 3.1. *Пусть $h(x) \in F[x]$ и выполнено сравнение*

$$h(x)^q - h(x) \equiv 0 \pmod{f(x)}. \tag{3.1}$$

Тогда

$$f(x) = \prod_{c \in F} (f(x),\ h(x) - c) \tag{3.2}$$

Доказательство. Если многочлен $g(x) \in F[x]$ делит $h(x)-c_1$ и $h(x)-c_2$ при различных $c_1, c_2 \in F$, то $g(x) \mid (c_1 - c_2)$, и $g(x) \in F$. Таким образом множители, стоящие в правой части равенства (3.2) взаимно просты. Поскольку каждый из них делит $f(x)$, заключаем, что правая часть (3.2) делит $f(x)$.

С другой стороны, тождество

$$y^q - y = \prod_{c \in F} (y - c)$$

показывает, что

$$h(x)^q - h(x) = \prod_{c \in F} (h(x) - c). \tag{3.3}$$

Условие (3.1) означает, что каждый неприводимый делитель многочлена $f(x)$ делит разность $h(x) - c$ при некотором $c \in F$ и, следовательно, делит правую часть равенства (3.2). Согласно условию многочлен $f(x)$ не имеет кратных делителей. Поэтому $f(x)$ делит правую часть равенства (3.2). Так как все рассматриваемые многочлены унитарны, это завершает доказательство леммы 3.1. □

Далее будем предполагать, что разложение $f(x)$ на неприводимые множители имеет вид

$$f(x) = f_1(x) \cdots f_k(x).$$

Лемма 3.2. *Многочлен $h(x)$ удовлетворяет сравнению (3.1), если и только если существуют элементы $c_j \in F$, $j = 1, \ldots, k$, для которых выполнены сравнения*

$$h(x) \equiv c_j \pmod{f_j(x)}, \qquad j = 1, \ldots, k. \tag{3.4}$$

Доказательство. Каждый из многочленов $f_j(x)$ делит правую часть (3.2) и потому делит разность $h(x) - c_j$ при некотором $c_j \in F$. Это доказывает (3.4).

Обратно, справедливость (3.4) при некотором $c_j \in F$ означает, что

$$h(x)^q \equiv c_j^q \equiv c_j \equiv h(x) \pmod{f_j(x)}, \qquad j = 1, \ldots, k.$$

В силу взаимной простоты многочленов $f_j(x)$, это влечет (3.1). Лемма доказана. □

Следствие 3.1. *Существует в точности q^k многочленов $h(x) \in F[x]$, удовлетворяющих условиям*

$$h(x)^q - h(x) \equiv 0 \pmod{f(x)}, \qquad \deg h(x) < \deg f(x). \tag{3.5}$$

Доказательство. Существует ровно q^k наборов $(c_1, \ldots, c_k) \in F^k$. Каждому из них согласно китайской теореме об остатках, примененной в кольце $F[x]$ к сравнениям (3.4), сопоставляется единственный многочлен $h(x)$, удовлетворяющий (3.5).

Лемма 3.2 утверждает, что так получаются все многочлены с условиями (3.5). □

Обозначим буквой $\mathcal{L}$ совокупность многочленов $h(x) \in F[x]$ с условиями (3.5). Это множество, очевидно, является линейным пространством над F и $\dim \mathcal{L} = k$.

Следствие 3.2. *Для любых двух неприводимых делителей $f_i(x)$, $f_j(x)$ многочлена $f(x)$, $i \neq j$, существует многочлен $h(x) \in \mathcal{L}$ такой, что*

$$f_i(x) \mid h(x), \qquad f_j(x) \nmid h(x).$$

Доказательство. Достаточно взять многочлен $h(x)$, удовлетворяющий сравнениям (3.4) при некотором наборе $(c_1, \ldots, c_k)$ с $c_i = 0$, $c_j \neq 0$. □

Обсудим теперь вопрос, как находить многочлены, удовлетворяющие (3.5). Определим элементы $b_{ij} \in F, 0 \leqslant i, j < n$, так, что

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \pmod{f(x)}, \tag{3.6}$$

и пусть $B = \|b_{ij}\|_{0 \leqslant i,j < n}$.

Лемма 3.3. *Многочлен* $h(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in F[x]$ *удовлетворяет условиям (3.5) тогда и только тогда, когда вектор* $\overline{a} = (a_0, \ldots, a_{n-1}) \in F^n$ *составляет решение системы уравнений*

$$\overline{a} \cdot (B - I) = 0. \tag{3.7}$$

Здесь I *— единичная* $n \times n$ *матрица.*

Доказательство. Справедливо тождество

$$h(x)^q = \sum_{i=0}^{n-1} a_i x^{iq} \equiv \sum_{j=0}^{n-1} x^j \left(\sum_{i=0}^{n-1} a_i b_{ij} \right) \pmod{f(x)}$$

из которого и следует нужное утверждение. □

Следствие 3.3. *Количество неприводимых делителей* $f(x)$ *равно*

$$n - \operatorname{rank}(B - I).$$

Действительно, из леммы 3.3 следует, что линейное пространство $\mathcal{L}$ изоморфно пространству решений системы (3.7). Поэтому

$$k = \dim \mathcal{L} = n - \operatorname{rank}(B - I).$$

Следствие 3.4. *Если* $\operatorname{rank}(B-I) = n-1$, *то многочлен* $f(x) \in F[x]$ *неприводим.*

Решая систему (3.7), можно найти базис $h_1(x), \ldots, h_k(x)$ пространства $\mathcal{L}$. При этом можно считать $h_1(x) = 1$.

Алгоритм 3.1. Данные: *Многочлен* $f(x) \in F[x]$ *без кратных корней.* Найти: *Разложение* $f(x)$ *на неприводимые множители.*

1. Вычислить матрицу $B = \|b_{ij}\|_{0 \leqslant i,j < n}$ *с помощью равенств (3.6).*
2. Решая систему (3.7), найти многочлены $h_1(x) = 1$, $h_2(x), \ldots, h_k(x)$, *составляющие базис пространства* $\mathcal{L}$. *Если* $k = 1$, *то СТОП, многочлен* $f(x)$ *неприводим.*
3. Положить $\mathcal{M} = \{f\}$.

4. Для каждого $j = 2, \dots, k$ и для каждого $c \in F$ до тех пор, пока не выполнится $\#\mathcal{M} = k$, проделать следующее:
для каждого $u \in \mathcal{M}$ вычислить

$$p(x) = (u(x),\ h_j(x) - c)$$

и, если $0 < \deg p(x) < \deg u(x)$, исключить $u(x)$ из $\mathcal{M}$ и заменить его парой многочленов $p(x),\ u(x)/p(x)$.
5. Если $\#\mathcal{M} = k$, СТОП. Множество $\mathcal{M}$ содержит все неприводимые делители $f(x)$.

Теорема 3.1. *Алгоритм находит разложение многочлена $f(x)$ на неприводимые множители. Для этого ему требуется $O(qn^3)$ арифметических операций в поле F.*

Доказательство. Заметим, что в процессе работы алгоритма всегда выполняются условия

$$f(x) = \prod_{u \in \mathcal{M}} u(x), \qquad \deg u(x) \geqslant 1.$$

Если при фиксированных j, c работа с множеством $\mathcal{M}$ в пункте 4 алгоритма завершилась, это значит, что для каждого $u(x) \in \mathcal{M}$ выполняется одно из условий

$$(u(x), h_j(x) - c) = 1 \quad \text{или} \quad u(x) \mid h_j(x) - c. \tag{3.8}$$

По завершении цикла по c можно утверждать, что каждый многочлен $u(x) \in \mathcal{M}$ при любом $c \in F$ удовлетворяет одному из условий (3.8).

Из леммы 3.1 следует, что для каждого $u(x) \mid f(x)$ справедливо разложение

$$u(x) = \prod_{c \in F} (u(x),\ h_j(x) - c),$$

так что равенство $(u(x), h_j(x) - c) = 1$ при всех $c \in F$ невозможно. Значит, найдется $c \in F$, для которого $u(x) \mid h_j(x) - c$. Итак, если при фиксированном j завершился цикл по c, то каждый из многочленов $u \in \mathcal{M}$ делит разность $h_j(x) - c$ при некотором $c \in F$.

Докажем теперь, что равенство $\#\mathcal{M} = k$ всегда достигается в процессе работы алгоритма. Если это не так, то в множестве $\mathcal{M}$ после перебора всех пар (j, c) останется многочлен $u(x)$, делящийся на два разных неприводимых делителя $f_i(x)$, $f_\ell(x)$ многочлена $f(x)$. По доказанному для любого $j, 2 \leqslant j \leqslant k$, найдется элемент $c_j \in F$ такой, что $u(x) \mid h_j(x) - c_j$. По следствию 3.4 из леммы 3.2 существует многочлен $h(x) \in \mathcal{L}$ такой, что

$$f_i(x) \mid h(x), \qquad f_\ell(x) \nmid h(x).$$

Пусть

$$h = \sum_{\nu=1}^{k} \gamma_\nu h_\nu, \quad \gamma_\nu \in F.$$

Тогда

$$h \equiv \sum_{\nu=1}^{k} \gamma_\nu c_\nu \pmod{u(x)}.$$

Так как $f_i(x) \mid u(x)$ и $f_i(x) \mid h(x)$, то $\sum_{\nu=1}^{k} \gamma_\nu c_\nu = 0$. Но тогда $f_\ell(x) \mid h(x)$, что неверно. Получившееся противоречие доказывает, что равенство $\#\mathcal{M} = k$ достигается.

Оценим теперь сложность алгоритма. Для вычисления матрицы B требуется $O(n^2 \ln q)$ арифметических операций в поле F. Вычисления в пункте 2 требуют $O(n^3)$ арифметических операций, а в шаге 4 — $O(qn^3)$ операций. Общая трудоемкость есть $O(qn^3)$ арифметических операций в поле F. □

3.2 Сведение задачи разложения на неприводимые множители к нахождению корней (алгоритм Цассенхауза).

Напомним, что основное поле $F = F_q$, над которым мы работаем, имеет характеристику p и $q = p^m$. В этом параграфе речь пойдет о

связи двух задач: разложения многочленов на неприводимые множители над полем F и нахождения корней многочленов в поле F.

Пусть $h(x) \in F[x]$ и $f(x) \mid h(x)^q - h(x)$. Обозначим

$$\mathcal{R} = \{c \in F \mid (f(x),\ h(x) - c) \neq 1\}.$$

Из (3.2) следует, что $\#\mathcal{R} \leqslant k$.

Пусть также d — наименьшее целое число, для которого существуют не равные одновременно нулю элементы $b_0, \ldots, b_d \in F$ такие, что

$$\sum_{j=0}^{d} b_j h(x)^j \equiv 0 \pmod{f(x)}. \tag{3.9}$$

Согласно лемме 3.2

$$f(x) = \prod_{c \in \mathcal{R}} (f(x), h(x) - c) \mid \prod_{c \in \mathcal{R}} (h(x) - c).$$

Поэтому $d \leqslant \#\mathcal{R}$.

Так как $b_d \neq 0$, можно считать, что $b_d = 1$.

Обозначим

$$g(y) = \sum_{j=0}^{d} b_j y^j.$$

Лемма 3.4. *Справедливо разложение*

$$g(y) = \prod_{c \in \mathcal{R}} (y - c).$$

Доказательство. Если $c \in \mathcal{R}$, то $(f(x), h(x) - c) \neq 1$ и существует неприводимый многочлен $f_j(x) \mid f(x)$, такой что $f_j(x) \mid h(x) - c$. Тогда согласно (3.9) имеем

$$g(c) \equiv g(h(x)) \equiv 0 \pmod{f_j(x)}.$$

Итак, $g(c) = 0$ и

$$g(y) = \phi(y) \cdot \prod_{c \in \mathcal{R}} (y - c), \qquad \phi(y) \in F[y].$$

Поскольку $d \leqslant \#\mathcal{R}$, заключаем, что $\deg \phi(x) = 0$. Это доказывает лемму. □

Следующий алгоритм сводит задачу разложения $f(x) \in F[x]$ на неприводимые над F множители к нахождению корней в поле F некоторой совокупности многочленов $g_j(x) \in F[x]$.

Алгоритм 3.2. Данные: *Многочлен $f(x) \in F[x]$ без кратных корней.* Найти: *Разложение $f(x)$ на неприводимые множители над полем F.*

1. Вычислить матрицу B, число k и многочлены $h_1(x) = 1, h_2(x)$, $\ldots$, $h_k(x)$, как в алгоритме Берлекемпа. Положить $\mathcal{M} = \{f(x)\}$.
2. Для каждого $j = 2, \ldots, k$ проделать следующие операции.
2.1. Вычислить наименьшее d такое, что векторы

$$\overline{c}_\ell = (c_{\ell,0}, \ldots, c_{\ell,n-1}) \in F^n, \qquad \ell = 0, \ldots d,$$

определенные сравнениями

$$h_j(x)^\ell \equiv \sum_{i=0}^{n-1} c_{\ell,i} x^i \pmod{f(x)}$$

линейно зависимы над F.
2.2 Вычислить коэффициенты $b_0, \ldots, b_d \in F$ такие, что

$$b_0\overline{c}_0 + \cdots + b_d\overline{c}_d = 0, \qquad b_d = 1.$$

Обозначить $g_j(y) = b_0 + b_1 y + \cdots + b_d y^d$.
2.3 Найти множество $\mathcal{R}_j$ корней многочлена $g_j(y)$, принадлежащих F.
2.4 Для каждого $c \in \mathcal{R}_j$ и каждого $u \in \mathcal{M}$ вычислить

$$p(x) = (u(x),\ h_j(x) - c)$$

u, если $1 \leqslant \deg p(x) < \deg u(x)$, исключить $u(x)$ из $\mathcal{M}$ и заменить его парой многочленов $p(x)$, $u(x)/p(x)$.
2.5 Если $\#\mathcal{M} = k$, СТОП. Множество $\mathcal{M}$ содержит все неприводимые делители $f(x)$.

Приведенный выше алгоритм отличается от алгоритма 3.1 лишь тем, что в нем вычисляются многочлены $p(x) = (u(x),\ h_j(x) - c)$ только в том случае, когда $c \in \mathcal{R}_j$, т.е. когда $p(x) \neq 1$. Обоснование его справедливости совпадает с обоснованием для алгоритма 3.1. Сложность алгорима 3.2, сводящего задачу разложения на множители к вычислению корней в том же поле, есть, как легко видеть, $O(n^2(k^2 + \ln q)$.

3.3 Нахождение корней многочленов в полях малой характеристики.

В этом параграфе, как и ранее, используются обозначения $F = F_q,\ q = p^m$, причем предполагается, что p не очень велико, но m — большое натуральное число.

Будет также предполагаться, что все корни многочлена $f(x) \in F[x]$ лежат в поле F и однократны. В противном случае можно заменить $f(x)$ на $(x^q - x,\ f(x))$.

Напомним некоторые факты из теории конечных полей. Существует элемент $\omega \in F$ такой, что $F = F_p(\omega), [F : F_p] = m$. Отображение

$$\sigma : F \to F, \qquad \sigma : \alpha \longrightarrow \alpha^p$$

есть автоморфизм поля F над F_p и называется автоморфизмом Фробениуса. Элементы

$$\sigma_j(\omega) = \sigma^j(\omega) = \omega^{p^j}, \qquad j = 0, 1, \ldots, m-1,$$

суть все сопряженные ω и потому различны.

Для каждого $\alpha \in F$ имеем след

$$\mathrm{Tr}(\alpha) = \sum_{j=0}^{m-1} \sigma_j(\alpha).$$

Так как

$$(\mathrm{Tr}(\alpha))^p = \left(\sum_{j=0}^{m-1} \alpha^{p^j}\right)^p = \sum_{j=1}^{m} \alpha^{p^j} = \mathrm{Tr}(\alpha),$$

то $\mathrm{Tr}(\alpha) \in F_p$.

Обозначим $S(x) = \sum_{j=0}^{m-1} x^{p^j}$. Если $\alpha \in F_q$, то

$$S(\alpha) = \mathrm{Tr}(\alpha) \in F_p. \tag{3.10}$$

Лемма 3.5. *Справедливо разложение на множители*

$$x^q - x = \prod_{c \in F_p} (S(x) - c). \tag{3.11}$$

Доказательство. Из равенства (3.10) следует, что каждый элемент $\alpha \in F$ является корнем правой части равенства (3.11). Отсюда следует, что правая часть делится на $x^q - x$. Степень правой части равна $p \cdot p^{m-1} = q$. Кроме того старшие коэффициенты обеих частей равенства (3.11) равны 1. Это доказывает лемму 3.5. □

Следствие 3.5. *Для каждого $\beta \in F_q$, $\beta \neq 0$, справедливо равенство*

$$x^q - x = \beta^{-1} \prod_{c \in F_p} (S(\beta x) - c).$$

Доказательство. Имеем с помощью (3.11)

$$\prod_{c \in F_p} (S(\beta x) - c) = (\beta x)^q - \beta x = \beta(x^q - x).$$

□

Алгоритм 3.3. Данные: *Многочлен $f(x) \in F[x]$ без кратных корней,* $\deg f(x) = n$. *Все его корни принадлежат F.*
Найти: *Все корни многочлена $f(x)$.*

1. Определить $\mathcal{M} = \{f(x)\}$.
2. Для каждого $j = 0, 1, \ldots, m-1$ и для каждого $c \in F_p$ выполнить следующее:
2.1. для каждого $u(x) \in \mathcal{M}$ вычислить

$$p(x) = (u(x),\ S(\omega^j x) - c).$$

2.2. Если $1 \leqslant \deg p(x) < \deg u(x)$, *исключить* $u(x)$ *из множества* $\mathcal{M}$ *и заменить его парой многочленов* $p(x),\ u(x)/p(x)$.
2.3. Если $\#\mathcal{M} = n$, *перейти в пункт 3.*
3. СТОП. В этом случае множество $\mathcal{M}$ *состоит из всех многочленов* $x - \gamma$, *где* $\gamma \in F$ *— корень* $f(x)$.

Перейдем к обоснованию этого алгоритма.

Теорема 3.2. *Алгоритм находит все корни многочлена* $f(x)$. *Для этого ему требуется* $O(m^2n^2p\ln p)$ *арифметических операций в поле* F_q.

Доказательство. Заметим, что в любой момент работы алгоритма выполняется равенство

$$f(x) = \prod_{u \in \mathcal{M}} u(x) \tag{3.12}$$

и неравенства $\deg u(x) \geqslant 1,\ u(x) \in \mathcal{M}$.

Если при фиксированных j, c работа с множеством $\mathcal{M}$ в пункте 2 алгоритма завершилась, это значит, что для каждого $u(x) \in \mathcal{M}$ выполняется одно из условий

$$(u(x),\ S(\omega^j x) - c) = 1 \quad \text{или} \quad u(x) \mid S(\omega^j x) - c. \tag{3.13}$$

По завершении цикла по c можно утверждать, что каждый многочлен $u(x) \in \mathcal{M}$ при любом $c \in F$ удовлетворяет одному из условий (3.13).

Если при всех $c \in F$ выполняется равенство $(u(x),\ S(\omega^j x) - c) = 1$, то по следствию 3.5, примененному к $\beta = \omega^j$, находим, что $(u(x), x^q - x) = 1$. Но это невозможно, т.к. все корни $u(x)$ принадлежат F и потому $u(x) \mid x^q - x$. Итак, равенство $(u(x),\ S(\omega^j x) - c) = 1$ при всех $c \in F$ невозможно. Значит, найдется $c \in F$, для которого $u(x) \mid S(\omega^j x) - c$. Таким образом, если при фиксированном j завершился цикл по c, то каждый многочлен из множества $\mathcal{M}$ делит некоторый многочлен $S(\omega^j x) - c$.

Предположение, что алгоритм завершит циклы по j и по c, но равенство $\#\mathcal{M} = n$ не будет достигнуто, означает, что найдется многочлен $u(x) \in \mathcal{M},\ \deg u(x) \geqslant 2$, и набор $c_0, c_1, \ldots, c_{m-1} \in F_p$ такие, что

$$S(\omega^k x) \equiv c_k \pmod{u(x)}, \qquad k = 0, 1, \ldots, m-1.$$

Пусть γ_1, γ_2 — два различных корня многочлена $u(x),\ \gamma_i \in F$. Тогда имеем

$$S(\omega^k \gamma_1) = c_k, \qquad S(\omega^k \gamma_2) = c_k, \qquad k = 0, 1, \ldots, m-1,$$

так что

$$S(\omega^k \gamma_1) - S(\omega^k \gamma_2) = 0, \qquad k = 0, 1, \ldots, m-1.$$

Пользуясь определением многочлена $S(x)$, получаем

$$0 = \sum_{j=0}^{m-1} \left((\omega^k \gamma_1)^{p^j} - (\omega^k \gamma_2)^{p^j} \right) = \sum_{j=0}^{m-1} \omega^{kp^j} (\gamma_1 - \gamma_2)^{p^j}, \quad 0 \leqslant k < m. \tag{3.14}$$

Все элементы $\omega^{p^j},\ j = 0, 1, \ldots, m-1$ различны. Поэтому определитель Вандермонда $\det \|\omega^{kp^j}\|_{0 \leqslant k, j < p}$ отличен от нуля. Но тогда равенства (3.14) означают

$$(\gamma_1 - \gamma_2)^{p^j} = 0, \qquad j = 0, 1, \ldots, m-1.$$

При $j = 0$ находим $\gamma_1 = \gamma_2$, что противоречит определению γ_i. Таким образом, в процессе работы алгоритма обязательно выполнится равенство $\#\mathcal{M} = n = \deg f(x)$.

Это равенство означает, что (3.12) есть разложение $f(x)$ на линейные множители. Каждый из них дает некоторый корень многочлена $f(x)$.

Для оценки сложности алгоритма заметим, что всего будет совершено не более mp шагов в циклах по j и c. Вычисление на каждом шаге требует не более $O(mn^2 \ln p + n^2) = O(mn^2 \ln p)$ арифметических операций. Так что общая оценка сложности есть $O(m^2 n^2 p \ln p)$ арифметических операций в поле F_q. □

Алгоритм можно несколько усовершенствовать. Во-первых, как только для некоторого $u(x) \in \mathcal{M}$ выполнится равенство $\deg u(x) = 1$, корень этого многочлена можно запомнить (он будет также корнем $f(x)$) и исключить $u(x)$ из множества $\mathcal{M}$ и дальнейших операций.

Во-вторых, выполняя цикл по c при фиксированном j, многочлен $u(x) \in \mathcal{M}$ можно исключить из операций в этом цикле, если известно, что он делит некоторую разность $S(\omega^j x) - c$. Ведь такая разность может быть только одна.

3.4 Нахождение корней многочленов в полях большой характеристики.

Описываемые здесь алгоритмы носят вероятностный характер и довольно эффективны на практике.

1. Рассмотрим сначала случай $q = p \geqslant 3$.

Алгоритм 3.4. Данные: *Многочлен* $f(x) \in F[x]$, $n = \deg f(x) \geqslant 2$. *Все его корни однократны и принадлежат* F.
Найти: *Все корни многочлена* $f(x)$.

1. Положить $\mathcal{M} = \{f(x)\}$.
2. Выбрать каким-либо способом элемент $c \in F_p$.
3. Для каждого $u(x) \in \mathcal{M}$ *выполнить следующие действия:*
3.1. Вычислить

$$d(x) = (u(x), (x + c)^{\frac{p-1}{2}} - 1).$$

3.2. Если $1 \leqslant \deg d(x) < \deg u(x)$, *то исключить* $u(x)$ *из множества* $\mathcal{M}$ *и заменить его парой многочленов* $d(x)$ *и* $u(x)/d(x)$.
3.3 Если $\#\mathcal{M} = n$, *то СТОП. Множество* $\mathcal{M}$ *состоит из всех многочленов вида* $x - \gamma$, *где* γ *— корень многочлена* $f(x)$.
4. Перейти к шагу 2.

Лемма 3.6. *Пусть* $u(x) \mid f(x), \deg u(x) \geqslant 2$. *При случайном выборе числа* $c \in F_p$ *вероятность того, что* $d(x)$ *будет собственным делителем многочлена* $u(x)$, *не меньше* $\frac{1}{2} - \frac{1}{2p}$.

Доказательство. Пусть γ_1, γ_2 — различные корни многочлена $u(x)$. Обозначим буквой $\mathcal{D}$ подмножество F_p, состоящее из элементов t, удовлетворяющих условиям

$$(t+\gamma_1)^{\frac{p-1}{2}} \neq (t+\gamma_2)^{\frac{p-1}{2}}, \qquad t \neq -\gamma_1, -\gamma_2.$$

Многочлен $(x+\gamma_1)^{\frac{p-1}{2}} - (x+\gamma_2)^{\frac{p-1}{2}}$ имеет не более $\frac{p-3}{2}$ корней. Поэтому

$$\#\mathcal{D} \geqslant p - \frac{p-3}{2} - 2 = \frac{p-1}{2}.$$

Каждый ненулевой элемент $b \in F_p$ удовлетворяет одному из равенств $b^{\frac{p-1}{2}} = 1$ или $b^{\frac{p-1}{2}} = -1$.

Если $c \in \mathcal{D}$, то $c+\gamma_1 \neq 0$, $c+\gamma_2 \neq 0$ и, значит, одно из чисел γ_1, γ_2 будет корнем многочлена $(x+c)^{\frac{p-1}{2}} - 1$, а другое нет. Следовательно, в этом случае $1 \leqslant \deg d(x) < \deg u(x)$, т.е. $d(x)$ есть собственный делитель $u(x)$. Оцениваемая вероятность не меньше

$$\frac{\#\mathcal{D}}{p} \geqslant \frac{1}{2} - \frac{1}{2p}.$$

□

Лемма 3.6 показывает, что при случайном выборе элемента $c \in F_p$ вероятность того, что величина $\#\mathcal{M}$ не увеличится после k повторений шагов 2 - 4 алгоритма, не превосходит $2^{-k} + O(p^{-1})$.

2. Пусть теперь $q = p^m, p \geqslant 3$. Описываемый ниже алгоритм предложен Кантором и Цассенхаузом в 1981 г., см. [17].

Алгоритм 3.5. Данные: *Многочлен* $f(x) \in F[x]$, $n = \deg f(x) \geqslant 2$. *Все его корни однократны и принадлежат* F.
Найти: *Все корни многочлена* $f(x)$.

1. Определить $\mathcal{M} = \{f(x)\}$.
2. Пусть $u(x)$ *— многочлен наибольшей степени в* $\mathcal{M}$. *Если таких*

многочленов несколько, положить $u(x)$ равным любому из них.
3. Если $\deg u(x) = 1$, *СТОП. В этом случае множество* $\mathcal{M}$ *содержит все линейные делители* $f(x)$. *Их корни составляют множество корней многочлена* $f(x)$.
4. Выбрать каким-либо способом ненулевой многочлен $v(x) \in F[x]$, $\deg v(x) < \deg u(x)$. *Вычислить* $p(x) = (u(x), v(x))$.
5. Если $p(x) \neq 1$, *исключить многочлен* $u(x)$ *из* $\mathcal{M}$ *и заменить его парой многочленов* $p(x), u(x)/p(x)$. *Перейти в шаг 2.*
6. Если $p(x) = 1$, *вычислить наибольший общий делитель*

$$d(x) = (u(x),\ v(x)^{\frac{q-1}{2}} - 1).$$

В случае $d(x) = 1$ *или* $d(x) = u(x)$, *перейти в шаг 4.*
7. Если $d(x)$ *отличен от* 1 *и* $u(x)$, *т.е.* $d(x)$ — *собственный делитель* $u(x)$, *исключить многочлен* $u(x)$ *из* $\mathcal{M}$ *и заменить его парой многочленов* $d(x), u(x)/d(x)$. *Перейти в шаг 2.*

Лемма 3.7. *Вероятность того, что выбранный в шаге 4 случайным образом многочлен* $v(x)$ *приведет к увеличению множества* $\mathcal{M}$, *не меньше, чем* $1/2$.

Доказательство. Пусть $u(x) \in \mathcal{M}$, $r = \deg u(x) \geqslant 2$ и $\gamma_1, \ldots, \gamma_r$ — все корни многочлена $u(x), \gamma_i \neq \gamma_j$.

Каждому многочлену $v(x) \in F[x], \deg v(x) < r$, поставим в соответствие вектор $\overline{c} = (c_1, \ldots, c_r) \in F^r$, положив $c_j = v(\gamma_j)$. Ввиду китайской теоремы об остатках, примененной к сравнениям $v(x) \equiv c_j \pmod{x - \gamma_j}$ в кольце $F[x]$, это соответствие взаимно однозначно.

Подсчитаем количество многочленов $v(x)$, не приводящих в п.п. 5 - 7 к увеличению множества $\mathcal{M}$.

Пусть $v(x) \neq 0$ и $p(x) = 1$. Условие $d(x) = 1$ выполняется в случае, если ни одно из чисел γ_i не является корнем многочлена $v(x)^{\frac{q-1}{2}} - 1$. Но тогда все числа $c_j = v(\gamma_j)$ удовлетворяют уравнению $y^{\frac{q-1}{2}} + 1 = 0$. Это уравнение имеет не более $\frac{q-1}{2}$ корней. Значит, существует не более $\left(\frac{q-1}{2}\right)^r$ многочленов $v(x)$ с условием $d(x) = 1$.

Аналогично, условие $d(x) = u(x)$ выполняется в случае, если все числа γ_i удовлетворяют уравнению $v(x)^{\frac{q-1}{2}} - 1 = 0$. Это значит, что все координаты вектора $\overline{c}$ суть решения уравнения $y^{\frac{q-1}{2}} - 1 = 0$. Таких векторов не более $\left(\frac{q-1}{2}\right)^r$ и, следовательно, существует не более $\left(\frac{q-1}{2}\right)^r$ многочленов $v(x) \neq 0$ с условиями $p(x) = 1, d(x) = u(x)$.

Таким образом, количество многочленов

$$v(x) \in F[x], \qquad \deg v(x) < r, \tag{3.15}$$

не приводящих в п.п. 5 - 7 к увеличению множества $\mathcal{M}$, не превосходит $1 + 2\left(\frac{q-1}{2}\right)^r$. Общее количество многочленов (3.15) равно q^r. Поэтому вероятность выбрать многочлен, не приводящий к увеличению $\#\mathcal{M}$ не превосходит

$$q^{-r}\left(1 + 2\left(\frac{q-1}{2}\right)^r\right) = q^{-r} + 2\left(\frac{q-1}{2q}\right)^r,$$

что оценивается сверху величиной

$$q^{-2} + 2\left(\frac{q-1}{2q}\right)^2 \leqslant \frac{1}{2}.$$

Это доказывает лемму 3.7. □

Заметим, что алгоритм 3.4 по существу совпадает с алгоритмом 3.5 при $m = 1$.

Глава 4

Алгоритмы, распознающие простоту чисел

Эта глава посвящена методам проверки на простоту и построения больших простых чисел. Иначе говоря, здесь обсуждается, каким образом можно доказать простоту натурального числа, если оно действительно является простым. Для решения этой задачи известны различные алгоритмы: детерминированные, вероятностные, условные. В целом, можно сказать, что доказательство простоты чисел с практической точки зрения есть не очень трудоемкая задача. Вместе с тем, оценки сложности алгоритмов, успешно работающих на практике, зачастую опираются на ряд гипотез, в настоящее время не доказанных. В первом параграфе этой главы будет рассмотрен полиномиальный алгоритм проверки чисел на простоту. Несмотря на очень хорошую оценку сложности, этот алгоритм не используется на практике, так как справедливость даваемого им заключения о простоте числа зависит от недоказанной в настоящее время так называемой расширенной гипотезы Римана.

4.1 Условный алгоритм Миллера.

Для того, чтобы сформулировать расширенную гипотезу Римана, напомним определение *характеров*. Пусть G — конечная абелева груп-

па. Любой гомоморфизм

$$\chi \ : G \longrightarrow \mathbb{C}^*$$

называется *характером* группы G. Например, функция $\chi_0(a)$, равная 1 при любом $a \in G$ есть характер, называемый *главным*. Отметим следующие свойства.

1. Если $d =\mid G \mid$, то для любого $a \in G$ значение $\chi(a)$ есть корень из 1 степени d.

2. Группа G имеет в точности d характеров.

Пусть теперь m — натуральное число и $G = (\mathbb{Z}/m\mathbb{Z})^*$. Будем обозначать символом $\overline{n}$ класс вычетов $n \pmod m$. Для каждого характера $\chi(\overline{n})$ группы G определим функцию на множестве $\mathbb{Z}$, также обозначаемую символом χ, при помощи равенства

$$\chi(n) = \begin{cases} 0, & \text{если } (n,m) \neq 1 \\ \chi(\overline{n}), & \text{если } (n,m) = 1. \end{cases}$$

Такие функции называются *характерами Дирихле*. При любых $u, v \in \mathbb{Z}$ имеем

1. $\chi(u+m) = \chi(u)$,
2. $\chi(u) \neq 0$, если и только если $(u,m) = 1$,
3. $\chi(uv) = \chi(u)\chi(v)$.

Приведем некоторые примеры. Функция

$$\chi_0(n) = \begin{cases} 0, & \text{если } (n,m) \neq 1 \\ 1, & \text{если } (n,m) = 1, \end{cases}$$

называется *главный характер* Дирихле.

Если m нечетно, $b \mid m$ и $\left(\frac{n}{b}\right)$ — символ Якоби, то функция

$$\chi(n) = \begin{cases} 0, & \text{если } (n,m) \neq 1 \\ \left(\frac{n}{b}\right), & \text{если } (n,m) = 1, \end{cases}$$

также есть характер Дирихле.

Определение 4.1. *Для каждого характера χ функция комплексного переменного s, определяемая рядом*

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \tag{4.1}$$

называется L-функцией Дирихле.

В частности, при $m=1$, т.е. в случае $\chi(n)=1$ при любом $n\geqslant 1$ ряд (4.1) определяет дзета-функцию

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}. \tag{4.2}$$

Ряд (4.2) сходится при каждом действительном $s>1$ и расходится при $s\leqslant 1$. Свойства дзета-функции тесно связаны со свойствами множества простых чисел, что позволяет использовать для исследования простых чисел методы теории функций. При каждом $s>1$ справедливо тождество

$$\zeta(s)=\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}=\lim_{x\to\infty}\prod_{p\leqslant x}\left(1-\frac{1}{p^s}\right)^{-1}, \tag{4.3}$$

называемое тождеством Эйлера.

В 1859г. Б. Риман[1] определил дзета-функцию при любом комплексном значении s и установил ряд ее глубоких свойств. Он также первым использовал обозначение $\zeta(s)$ для функции (4.2), получившей впоследствии название дзета-функция Римана. Как функция комплексного переменного $s=\sigma+it$ дзета функция аналитична во всех точках комплексной плоскости, за исключением точки $s=1$, где она имеет полюс первого порядка. Дзета-функция $\zeta(s)$ обладает симметрией относительно точки $s=1/2$, а именно удовлетворяет некоторому функциональному уравнению. Она обращается в нуль в точках

[1]Бернхард Риман, 1826-1866, — немецкий математик, оказавший существенное влияние на развитие теории аналитических функций, геометрии и теории чисел.

$s = -2, -4, -6, \ldots$, а, кроме того, как предположил Риман, имеет бесконечное количество нулей в полосе $0 \leqslant \sigma \leqslant 1$, расположенных симметрично относительно прямой $\sigma = 1/2$ и вещественной оси (этот факт был доказан в 1893г. Ж. Адамаром[2]). Риман высказал без доказательства и приближенную формулу[3] для количества таких нулей в прямоугольнике $0 \leqslant \sigma \leqslant 1, 0 \leqslant t \leqslant T$. Он также предположил, что все нули $\zeta(s)$ в полосе $0 \leqslant \sigma \leqslant 1$ в действительности лежат на прямой $\sigma = 1/2$. Эта гипотеза — знаменитая "гипотеза Римана" не доказана до сих пор. Риман показал, что поведение функция $\pi(x)$ тесно связано с расположением нулей $\zeta(s)$.

Рассматривая дзета-функцию, как функцию комплексного переменного, Ж. Адамар и Ш.Ж. Валле-Пуссен[4] установили точный порядок роста функции $\pi(x)$, доказав в 1896г., что

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{при} \quad x \to \infty \quad \text{т.е.} \quad \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1. \tag{4.4}$$

Это утверждение называется *асимптотическим законом распределения простых чисел.*

L-функции также играют важную роль в исследованиях вопросов распределения простых чисел. С их помощью в 1839г. Дирихле доказал, что *каждая арифметическая прогрессия, разность и первый член которой суть натуральные взаимно простые числа, содержит бесконечное количество простых чисел.* Другими словами, для любых натуральных взаимно простых a, b имеется бесконечное множество простых чисел вида $an + b$.

Ряд (4.1) абсолютно сходится в области $\Re s > 1$ и определяет в этой области аналитическую функцию. Она может быть аналитически продолжена на всю комплексную плоскость и не имеет нулей в области $\Re s \geqslant 1$.

Расширенная гипотеза Римана: *Комплексные нули всех L-функций Дирихле, расположенные в полосе $0 < \Re s < 1$, лежат на прямой*

[2] Жак Адамар, 1865-1963, — французский математик.

[3] Ее доказал в 1895г. немецкий математик Ханс фон Мангольдт, 1854-1925.

[4] Шарль Жан де ла Валле-Пуссен, 1866-1962, французский математик.

$\Re s = \frac{1}{2}$.

На справедливости расширенной гипотезы Римана основан ряд важных алгоритмов теории чисел, а также оценки их сложности. Доказательство этой гипотезы, как и классической гипотезы Римана, до сих пор не найдено.

Классическая гипотеза Римана о нулях дзета-функции $\zeta(s)$ является частным случаем расширенной гипотезы.

Условия следующей леммы по существу совпадают с утверждением расширенной гипотезы Римана для функции $L(s, \chi)$.

Лемма 4.1. *Если χ — неглавный характер по модулю m и $L(s, \chi)$ не имеет нулей в области $\Re s > \frac{1}{2}$, то существует целое число a с условиями*

$$\chi(a) \neq 0, \quad \chi(a) \neq 1, \quad 2 \leqslant a \leqslant \gamma \ln^2 m,$$

где γ положительная постоянная.

Доказательство. см. [8]. □

Наилучшее в настоящее время значение γ равно 2.

Если $m = p$ есть простое число и $\chi(n) = \left(\frac{n}{p}\right)$ — символ Лежандра, то лемма 4.1 утверждает существование малого квадратичного невычета a по модулю p, а именно, $a \leqslant \gamma \ln^2 p$. Задача об оценке наименьшего квадратичного невычета рассматривалась впервые И.М.Виноградовым, который доказал в 1926г., что наименьший квадратичный невычет оценивается величиной $O(p^{\frac{1}{2\sqrt{e}}} \ln^2 p)$. Лучшая в настоящее время безусловная оценка доказана в 1957г. Берджесом — $O(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$.

Следующая теорема служит основой условного алгоритма Миллера доказательства простоты чисел.

Теорема 4.1. *Пусть N — нечетное натуральное число, не являющееся квадратом, $N = 1 + 2^s t$, где t нечетно. Если при каждом целом a, $2 \leqslant a \leqslant \gamma \ln^2 N$, не делящемся на N, выполнено сравнение*

$$a^t \equiv 1 \pmod{N}$$

или существует целое h, $0 \leqslant h < s$, *для которого*

$$a^{2^h t} \equiv -1 \pmod{N},$$

то, в случае справедливости расширенной гипотезы Римана, можно утверждать, что N *— простое число.*

Доказательство. Предположим, что N — составное число, отличное от квадрата. Обозначим $G = (\mathbb{Z}/N\mathbb{Z})^* = \{\overline{a} \mid (a, N) = 1\}$ и

$$H = \{\overline{a} \in G \mid a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}\}.$$

Как и в доказательстве теоремы 2.9, можно утверждать, что H есть собственная подгруппа в G. Обозначим буквой λ какой-либо неглавный характер на группе G/H и определим χ — числовой характер по модулю N, положив $\chi(a) = \lambda(aH)$. Тогда χ — неглавный характер по модулю N такой, что для каждого целого n с условием $\overline{n} \in H$ выполняется $\chi(n) = 1$. Пусть a — число, для которого согласно лемме 4.1 выполнены условия

$$\chi(a) \neq 0, \quad \chi(a) \neq 1, \quad 2 \leqslant a \leqslant \gamma \ln^2 N.$$

Тогда $N \nmid a$.

В параграфе 2.6 главы 2 были определены множества $S(N)$ и $M(N)$. Если $a \in M(N)$, то по теореме 2.8 имеем $a \in S(N)$. Это означает, что $\overline{a} \in H$, так что $\chi(a) = 1$. Но это противоречит определению a.

Значит, $a \notin M(N)$, что приводит, согласно определению последнего множества, к противоречию, доказывающему простоту N. □

4.2 $N - 1$ методы доказательства простоты чисел.

Методы, название которых вынесено в заголовок параграфа, применимы для доказательства простоты чисел N с условием, что $N - 1$ раскладывается в произведение малых простых чисел. Простейший

пример чисел такого рода представляют так называемые числа Ферма.

Число $N = 2^m + 1$ будет составным, если m имеет нечетный делитель. Это следует из тождества

$$x^q + 1 = (x+1)(1 - x + x^2 - \cdots + x^{q-1}),$$

справедливого при любом нечетном q. Действительно, если $m = q\ell$ при нечетном q, то $N = \left(2^\ell\right)^q + 1$ делится на $2^\ell + 1$. Значит, N может быть простым, только если m не имеет нечетных простых делителей, т.е. $m = 2^n$. Числа

$$F_n = 2^{2^n} + 1, \qquad n = 1, 2, \ldots$$

называются числами Ферма. Первые четыре числа Ферма

$$F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537 \tag{4.5}$$

просты. В 1640г. П. Ферма предположил, что при любом целом $n \geqslant 1$, число F_n будет простым, но не смог доказать это для F_5. Л. Эйлер в 1729г. показал, что F_5 делится на 641 и тем опроверг гипотезу Ферма. Эта делимость легко следует из представлений

$$641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4.$$

Действительно, справедливы сравнения

$$F_5 = 2^{32} + 1 \equiv -5^4 \cdot 2^{28} + 1 \equiv -(5 \cdot 2^7)^4 + 1 \equiv -1 + 1 \equiv 0 \pmod{641}.$$

Позже было доказано, что числа Ферма с номерами от 6 до 11 — составные. Число F_{12} также составное, но не все его простые делители известны. В настоящее время неизвестно, является ли число F_{33} простым или составным. Не найдено ни одного простого числа Ферма, отличного от чисел (4.5)

Следующее утверждение, называемое тестом Пепина дает простой способ определить, является ли число Ферма F_n простым или нет. Задача сводится к выполнению некоторых вычислений, которые и представляет основную трудность, ибо числа, с которыми приходится работать очень велики.

Предложение 4.1 (Пепин,1877). *Число Ферма F_n, $n \geqslant 1$, будет простым, если и только если справедливо сравнение*

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \tag{4.6}$$

Доказательство. Пусть выполнено сравнение (4.6) и p — простой делитель F_n. Ясно, что $p \geqslant 5$. Обозначим буквой d порядок числа 3 по модулю F_n, т.е. наименьшее натуральное число с условием $3^d \equiv 1 \pmod{p}$. Из сравнения (4.6) следует $3^{F_n-1} \equiv 1 \pmod{F_n}$. Поэтому $3^{F_n-1} \equiv 1 \pmod{p}$ и, следовательно, $d|F_n - 1 = 2^{2^n}$. Сравнение (4.6) означает также, что $d \nmid (F_n-1)/2 = 2^{2^n-1}$, так что $d = 2^{2^n} = F_n - 1$. Согласно малой теореме Ферма имеем $3^{p-1} \equiv 1 \pmod{p}$. Следовательно, $d|(p-1)$ и $F_n - 1 = d \leqslant p-1$. Значит, $p \geqslant F_n$ и $p = F_n$. Это доказывает, что F_n есть простое число.

Предположим теперь, что F_n — простое. По квадратичному закону взаимности имеем

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Поэтому

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

что завершает доказательство предложения. □

В связи с числами Ферма отметим знаменитую теорему Гаусса: правильный n-угольник может быть построен с помощью циркуля и линейки лишь в случае, когда $n = 2^k p_1 \cdots p_r$, где p_j — различные простые Ферма.

В основе всех $N-1$ методов доказательства простоты лежит следующее утверждение.

Теорема 4.2. *Пусть N — нечетное и m — натуральное число такие, что для любого простого числа $q|m$ существует целое a с условиями*

$$a^m \equiv 1 \pmod{N}, \qquad \left(a^{m/q} - 1,\, N\right) = 1. \tag{4.7}$$

Тогда любой простой делитель p числа N удовлетворяет сравнению

$$p \equiv 1 \pmod{m}.$$

Заметим, что первая часть доказательства теста Пепина следует из этого утверждения с $N = F_n$, $m = 2^{2^n}$, $a = 3$, $q = 2$.

Доказательство. Пусть p — простой делитель N, q — простой делитель m и a — число, удовлетворяющее (4.7). Тогда a не делится на p. Обозначим буквой d порядок a по модулю p, т.е. наименьшее натуральное число с условием $a^d \equiv 1 \pmod{p}$. Так как по малой теореме Ферма

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

то $d|p-1$ и

$$\nu_q(d) \leqslant \nu_q(p-1). \tag{4.8}$$

Из (4.7) следует, что

$$a^m \equiv 1 \pmod{p}, \qquad a^{m/q} \not\equiv 1 \pmod{p}.$$

Следовательно $d|m$ и $d \nmid m/q$. Это возможно лишь в случае, когда

$$\nu_q(m) = \nu_q(d). \tag{4.9}$$

Из (4.8) и (4.9) находим

$$\nu_q(m) = \nu_q(d) \leqslant \nu_q(p-1).$$

Так как последнее неравенство справедливо для любого простого делителя q числа m, то $m|p-1$ или $p \equiv 1 \pmod{m}$. □

Как иллюстрацию применения теоремы 4.2 рассмотрим $N = F_5 = 2^{32} + 1$, $m = 128$ и $a = 2^{16} + 1$. Так как

$$a^2 = 2^{32} + 2 \cdot 2^{16} + 1 \equiv 2^{17} \pmod{N},$$

то

$$a^{64} \equiv 2^{17 \cdot 32} \equiv (-1)^{17} \equiv -1 \pmod{N}.$$

Следовательно,

$$a^{128} \equiv 1 \pmod{N}, \qquad (a^{64} - 1, N) = (2, N) = 1,$$

и согласно теореме 4.2 каждый простой делитель p числа F_5 должен удовлетворять сравнению $p \equiv 1 \pmod{128}$. Первые простые числа в прогрессии $1 + 128 \cdot k$ суть 257 и 641. Они получаются при $k = 2$ и $k = 5$, соответственно. Второе из них есть делитель числа Ферма F_5.

В следующем утверждении предполагается, что нам известна лишь часть F разложения числа $N - 1$ на простые сомножители. Эта информация позволяет сделать некоторые заключения о свойствах неизвестных делителей числа N.

Следствие 4.1 (Лемер, Поклингтон)**.** *Пусть N нечетно, $N - 1 = F \cdot R$, причем для каждого простого делителя q числа F с некоторым целым b выполнены условия*

$$b^{N-1} \equiv 1 \pmod{N}, \qquad \left(b^{(N-1)/q} - 1,\ N\right) = 1. \tag{4.10}$$

Тогда любой простой делитель p числа N удовлетворяет сравнению

$$p \equiv 1 \pmod{F}$$

Доказательство. Применим теорему 4.2 к $m = F$ и $a = b^R$. □

Если известна достаточно большая часть разложения $N-1$ на простые сомножители, то иногда можно сделать заключение о простоте N.

Следствие 4.2. *Если в условиях следствия 4.1 выполнено неравенство*

$$R \leqslant F + 1$$

то N — простое.

Доказательство. Согласно следствию 4.1 каждое простое $p|N$ удовлетворяет сравнению $p \equiv 1 \pmod{F}$ и, значит, удовлетворяет неравенству $p \geqslant 1 + F$. Предположим, что N — составное. Тогда

$$(F + 1)^2 \leqslant N = FR + 1 \leqslant F^2 + F + 1.$$

Получившееся противоречие завершает доказательство. □

Следствие 4.3. *Если в условиях следствия 4.1 выполнено неравенство* $F \geqslant N^{1/3}$, *то или* N — *простое число, или число* N *раскладывается на два простых множителя*

$$N = (1 + Fx)(1 + Fy),$$

где x, y — *целые положительные корни квадратного уравнения*

$$t^2 - ut + v = 0, \tag{4.11}$$

а целые числа u, v *определяются единственным способом условиями*

$$R = Fv + u, \qquad 0 < u \leqslant F.$$

Доказательство. Пусть $N = p_1 \cdots p_r$. По следствию 4.1 находим $p_i \geqslant F + 1 > F$ и тогда $N > F^r \geqslant N^{r/3}$. Значит $r \leqslant 2$. Если $r = 1$, то N — простое.

Если $r = 2$, то по этому же следствию $p_1 = 1 + Fx$, $p_2 = 1 + Fy$ с натуральными числами x, y. Имеем

$$(1 + Fx)(1 + Fy) = FR + 1 = N \tag{4.12}$$

и, раскрывая скобки,

$$x + y + Fxy = R.$$

Обозначим $u = x + y$, $v = xy$. Тогда $u + Fv = R$ и числа x, y суть корни квадратного уравнения (4.11). Из (4.12) также следует $xy < N/F^2 \leqslant F$. Так как $(x - 1)(y - 1) \geqslant 0$, то

$$x + y \leqslant xy + 1 \leqslant F.$$

Это завершает доказательство следствия. □

Приведем вероятностный алгоритм, основанный на тех же принципах, что и доказательство теоремы 4.2 и предполагающий, что известны все простые делители числа $N - 1$.

Алгоритм 4.1. *Даны нечетное $N \geqslant 3$ и множество S всех простых делителей числа $N-1$. Требуется установить простоту числа N, если оно является таковым.*

1. Выбрать случайно $a \in \{2, 3, \ldots, N-1\}$ и проверить сравнение

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

Если это сравнение не выполнено, то N — составное число. Алгоритм останавливается.

2. Для каждого $q \in S$ проверить условие

$$a^{(N-1)/q} \not\equiv 1 \pmod{N}.$$

Если условие выполнено, то исключить соответствующее q из множества S.

3. Если $S \neq \emptyset$, переходим в пункт 1.

4. Если $S = \emptyset$, то N — простое число. Алгоритм останавливается.

Справедливость утверждения в пункте 4 вытекает из следующего утверждения.

Лемма 4.2. *Целое число N будет простым, если и только если для каждого простого $q|N-1$ существует целое число a с условиями*

$$a^{N-1} \equiv 1 \pmod{N}, \qquad a^{(N-1)/q} \not\equiv 1 \pmod{N}. \tag{4.13}$$

Доказательство. Если N — простое число и a — первообразный корень по модулю N, то условия (4.13) выполнены для любого простого $q|N-1$.

Для того, чтобы доказать утверждение в обратную сторону, обозначим через $q_1, \ldots, q_m$ все простые делители числа $N-1$ и через a_i — соответствующие им числа, удовлетворяющие условиям (4.13). Определим натуральные числа $x_i, i = 1, \ldots, m$, сравнениями

$$x_i \equiv 1 \pmod{q_i}, \quad x_i \equiv 0 \pmod{q_j}, \quad j \neq i.$$

Положим, наконец, $g = a_1^{x_1} \cdots a_m^{x_m}$. Тогда $g^{N-1} \equiv 1 \pmod{N}$. Кроме того, при любом j имеем

$$g^{(N-1)/q_j} = \prod_{i=1}^{m} a_i^{(N-1)x_i/q_j} \equiv a_j^{(N-1)x_j/q_j} \equiv a_j^{(N-1)/q_j} \not\equiv 1 \pmod{N}.$$

Пусть d — порядок g по модулю N. Тогда $d|N-1$ и $d \nmid (N-1)/q_i$ при любом i. Это возможно лишь при $d = N-1$. Так как по теореме Эйлера выполняется сравнение $g^{\varphi(N)} \equiv 1 \pmod{N}$, то $d = N-1|\varphi(N)$. Для составного N имеем

$$\varphi(N) = N \prod_{p|N} (1 - p^{-1}) < N - 1,$$

что невозможно. Следовательно, N — простое. □

Оценим теперь среднее время работы алгоритма 4.1, если N — простое число. В этом случае сравнение $a^{N-1} \equiv 1 \pmod{N}$ выполняется для любого a, $1 \leqslant a < N$. Так как при этом количество решений сравнения $x^{(N-1)/q} \equiv 1 \pmod{N}$ не превосходит $(N-1)/q$, то с вероятностью $\geqslant 1 - \frac{1}{q} \geqslant 1/2$ при каждом выборе a в шаге 1 алгоритма множество S будет уменьшаться. Математическое ожидание времени работы алгоритма в случае простого N есть $O(m \log N) = O(\log^2 N)$ арифметических операций.

4.3 Построение больших простых чисел.

Как правило, необходимость в больших простых числах возникает в связи с их использованием в различных криптографических протоколах, схемах шифрования и т.п. При этом, естественно, к конструируемым числам предъявляются определенные требования. Например, конструкция простых чисел должна быть массовой, они должны быть расположены в заданном интервале и должны быть в каком-то смысле хорошо распределенными в нем. Для нужд криптографии естественно требовать, чтобы конструируемые простые числа, по крайней мере внешне, не имели каких-либо особенностей, выделяющих

эти числа среди множества всех простых, а кроме того не обладали свойствами, снижающими сложность используемых задач, т.е. позволяющими решать, эти задачи сравнительно быстро. С другой стороны на практике иногда нужны простые числа, обладающие какими-либо дополнительными особенностями. Это вносит ряд осложнений в работу описываемых ниже алгоритмов. Впрочем, они допускают массу вариаций.

Наиболее эффективным средством построения простых чисел является несколько модифицированная малая теорема Ферма. Все применяемые алгоритмы строят возрастающую последовательность простых чисел, используя на каждом шаге простые числа, построенные ранее. Процесс продолжается до тех пор, пока не будет построено простое число нужной величины. В качестве простейшего примера рассмотрим следующий алгоритм.

Алгоритм 4.2. *Задано некоторое положительное число B. Требуется построить простое число $p > B$. Предполагается также заданной некоторая функция $\rho(p)$, определенная на множестве простых чисел и удовлетворяющая неравенствам $0 \leqslant \rho(p) \leqslant 1$. В процессе работы алгоритма будет конструироваться некоторое увеличивающееся множество S простых чисел.*

1. Положим $S = \{2\}$.

2. Строим некоторое подмножество $T \subset S$, выбирая в него каждый элемент p из S с заданной вероятностью $\rho(p)$.

3. Проверяем, является ли число

$$N = 2\prod_{p \in T} p + 1$$

простым. Для отсева составных чисел N можно использовать, например, тест Миллера–Рабина, а для доказательства простоты N — алгоритмы, описанные в предыдущем параграфе, ведь разложение $N - 1$ на простые сомножители известно.

4. Если N — составное, то переходим в пункт 2.

5. Если N — простое и $N < B$, то добавляем N в множество S.

6. Если N — простое и $N \geqslant B$, то алгоритм останавливается. Нужное простое число $p = N$ построено.

Функцию $\rho(p)$ можно выбирать равной $1/2$ или $1/\log p$, или каким-либо другим способом. Можно строить число N в виде

$$N = 2\prod_{p\in T} p^{e(p)} + 1,$$

выбирая целые неотрицательные числа — кратности $e(p)$ в соответствии с некоторым вероятностным законом. В пункте 1 можно определить множество S состоящим из всех простых чисел от 2 до некоторой границы, например, до 100.

Наконец, в описанной схеме возможно построение простых чисел N с использованием лишь части простых делителей $N-1$. Покажем, как с помощью следствия 4.1, имея большое простое число F, можно построить существенно большее простое число N. Выберем для этого случайным образом четное число R на промежутке $F \leqslant R \leqslant 4F+2$ и положим $N = FR + 1$. Затем можно проверить число N на отсутствие малых простых делителей. Испытать его некоторое количество раз с помощью алгоритма Миллера–Рабина. Если при этом выяснится, что N — составное число, следует выбрать новое значение R и опять повторить вычисления. Так следует делать до тех пор, пока не будет найдено число N, выдержавшее испытания алгоритмом Миллера–Рабина достаточно много раз. В этом случае появляется надежда на то, что N — простое число, и следует попытаться доказать это с помощью следствия 4.1. Для этого можно случайным образом выбирать число $b, 1 < b < N$, и, поскольку F — простое число, проверять для него выполнимость условий

$$b^{N-1} \equiv 1 \pmod{N}, \qquad \bigl(b^R - 1, N\bigr) = 1. \tag{4.14}$$

Если при выбранном b эти соотношения выполняются, то можно утверждать, что число N — простое. Действительно, следствие 4.1 утверждает, что каждый простой делитель p числа N должен удовлетворять сравнению $p \equiv 1 \pmod{F}$. Кроме того, p нечетно, так что

$p \equiv 1 \pmod{2F}$ и $p \geqslant 2F+1$. Для составного N имеем неравенства

$$(2F+1)^2 \leqslant N = FR+1 \leqslant 4F^2+2F+1,$$

что неверно. Значит, N — простое число.

Если условия (4.14) нарушаются, нужно выбрать другое значение b и повторять эти операции до тех пор, пока такое число не будет обнаружено.

Предположим теперь, что построенное число N действительно является простым. Зададимся вопросом, сколь долго придется перебирать числа b, пока не будет найдено такое, для которого выполнены условия (4.14). Заметим, что для простого числа N первое условие (4.14), согласно малой теореме Ферма, будет выполняться всегда. Те же числа b, для которых нарушается второе условие (4.14), удовлетворяют сравнению $b^R \equiv 1 \pmod{N}$. Как известно, уравнение $x^R = 1$ в поле вычетов $\mathbb{Z}/N\mathbb{Z}$ имеет не более R решений. Одно из них — $x = 1$. Поэтому на промежутке $1 < b < N$ имеется не более $R-1$ чисел, для которых не выполняются условия (4.14). Это означает, что, выбирая случайным образом число b на промежутке $1 < b < N$, при простом N можно с вероятностью большей, чем $1 - F^{-1}$, найти число b, для которого будут выполнены условия следствия 4.14, и тем доказать, что N действительно является простым числом.

Заметим, что построенное таким способом простое число N будет удовлетворять неравенству $N > F^2$, т.е. будет записываться вдвое большим количеством цифр, чем исходное простое число F. Заменив теперь число F на найденное простое число N и повторив с этим новым F все указанные выше действия, можно построить еще большее простое число. Начав с какого-нибудь простого числа, скажем, записанного 10 десятичными цифрами (простоту его можно проверить, например, делением на маленькие табличные простые числа), и повторив указанную процедуру достаточное число раз, можно построить простые числа нужной величины.

Обсудим теперь некоторые теоретические вопросы, возникающие в связи с нахождением числа R, удовлетворяющего неравенствам $F \leqslant$

$R \leqslant 4F + 2$, и такого, что $N = FR + 1$ — простое число. Прежде всего, согласно теореме Дирихле, доказанной еще в 1839г., прогрессия $2Fn + 1, n = 1, 2, 3, \ldots$ содержит бесконечное количество простых чисел. Нас интересуют простые числа, лежащие недалеко от начала прогрессии. Оценка наименьшего простого числа в арифметической прогрессии была получена в 1944г. Ю.В.Линником. Соответствующая теорема утверждает, что наименьшее простое число в арифметической прогрессии $2Fn+1$ не превосходит F^C, где C — некоторая достаточно большая абсолютная постоянная. В предположении справедливости расширенной гипотезы Римана можно доказать, что наименьшее такое простое число не превосходит $c(\varepsilon)F^{2+\varepsilon}$ при любом $\varepsilon > 0$.

Таким образом, в настоящее время никаких теоретических гарантий для существования простого числа $N = FR+1, F \leqslant R \leqslant 4F+2$, не существует. Тем не менее, опыт вычислений на ЭВМ показывает, что простые числа в арифметической прогрессии встречаются достаточно близко к ее началу. Упомянем в этой связи гипотезу о существовании бесконечного количества простых чисел q с условием, что число $2q + 1$ также простое, т.е. простым является уже первый член прогрессии.

Очень важен в связи с описываемым методом построения простых чисел также вопрос о расстоянии между соседними простыми числами в арифметической прогрессии. Ведь убедившись, что при некотором R число $N = FR + 1$ составное, можно следующее значение R взять равным $R + 2$ и действовать так далее, пока не будет найдено простое число N. Но, если расстояние между соседними простыми числами в прогрессии велико, нет надежды быстро построить нужное число N. Перебор чисел R до того момента, как мы наткнемся на простое число N окажется слишком долгим. В более простом вопросе о расстоянии между соседними простыми числами p_n и p_{n+1} в натуральном ряде доказана лишь оценка $p_{n+1} - p_n = O(p_n^{\frac{38}{61}+\varepsilon})$, что, конечно, не очень хорошо для наших целей. Вместе с тем существует так называемая гипотеза Крамера (1936г.), что $p_{n+1} - p_n = O(\ln^2 p_n)$,

дающая вполне приемлемую оценку. Примерно такой же результат следует и из расширенной гипотезы Римана. Вычисления на ЭВМ показывают, что простые числа в арифметических прогрессиях расположены достаточно плотно.

В качестве итога обсуждения в этом пункте подчеркнем следующее: если принять на веру, что наименьшее простое число, а также расстояние между соседними простыми числами в прогрессии $2Fn+1$ при $F \leqslant n \leqslant 4F+2$ оцениваются величиной $O(\ln^2 F)$, то описанная схема построения больших простых чисел имеет полиномиальную оценку сложности. Кроме того, несмотря на отсутствие теоретических оценок времени работы алгоритмов, отыскивающих простые числа в арифметических прогрессиях со сравнительно большой разностью, на практике эти алгоритмы работают вполне удовлетворительно.

4.4 $N+1$ методы доказательства простоты чисел.

Пусть Δ — целое число, не делящееся на квадрат простого, и

$$K = \mathbb{Q}(\sqrt{\Delta}) = \{\alpha = x + y\sqrt{\Delta}\,, \quad x, y \in \mathbb{Q}\}$$

— квадратичное расширение поля рациональных чисел. Для $\alpha \in K$ будем обозначать $\overline{\alpha} = x - y\sqrt{\Delta}$ — число, сопряженное с α, и $N(\alpha) = \alpha\overline{\alpha} = x^2 - \Delta y^2$ — норму α. Норма, как известно, мультипликативна, т.е. для любых двух чисел $\alpha, \beta \in K$ имеем $N(\alpha\beta) = N(\alpha)N(\beta)$.

Пусть N — натуральное число. Обозначим

$$\mathcal{R}_N = \{\alpha = (a + b\sqrt{\Delta})/m \,|\, a, b, m \in \mathbb{Z},\ (m, N) = 1\}.$$

Множество $\mathcal{R}_N$, очевидно, является кольцом, причем $\mathbb{Z} \subset \mathcal{R}_N \subset K$.

В $\mathcal{R}_N$ определено понятие делимости. Число $\alpha \in \mathcal{R}_N$ делится на $\beta \in \mathcal{R}_N, \beta \neq 0$, если $\alpha/\beta \in \mathcal{R}_N$. Это свойство будет обозначаться в дальнейшем символом $\beta|\alpha$. Можно также определить понятие сравнимости элементов кольца $\mathcal{R}_N$, записывая $\alpha \equiv \beta \pmod{\delta}$ для $\alpha, \beta, \delta \in \mathcal{R}_N$, если $\delta|\beta-\alpha$. Как и для целых рациональных чисел, сравнения можно почленно складывать, вычитать и перемножать. Если

$\alpha \in \mathcal{R}_N$, то $N(\alpha)$ есть рациональное число, знаменатель которого взаимно прост с N, то-есть $N(\alpha) \in \mathcal{R}_N$. Легко видеть, что число $\alpha \in \mathcal{R}_N$ обратимо в кольце $\mathcal{R}_N$, если его норма есть рациональное число, числитель и знаменатель которого взаимно просты с N. Для любых двух $\alpha, \beta \in \mathcal{R}_N$ будем писать $(\alpha, \beta) = 1$, если множество общих делителей α и β исчерпывается обратимыми элементами кольца $\mathcal{R}_N$.

Следующее утверждение есть аналог малой теоремы Ферма для кольца $\mathcal{R}_N$. В его формулировке используется символ Лежандра.

Лемма 4.3. *Пусть p — простое нечетное число, $p \nmid \Delta$ и $\alpha \in \mathcal{R}_p$. Тогда*

$$\alpha^p \equiv \begin{cases} \alpha \pmod p, & \text{если } \left(\frac{\Delta}{p}\right) = 1 \\ \overline{\alpha} \pmod p, & \text{если } \left(\frac{\Delta}{p}\right) = -1. \end{cases}$$

Доказательство. Пусть $\alpha = a/m \in \mathcal{R}_p \cap \mathbb{Q}$, т.е $a, m \in \mathbb{Z}$, $p \nmid m$. Тогда по малой теореме Ферма

$$\alpha^p - \alpha = \frac{a(a^{p-1} - m^{p-1})}{m^p} \equiv 0 \pmod p.$$

Утверждение леммы в этом случае выполняется.

Пусть теперь $\alpha = x + y\sqrt{\Delta} \in \mathcal{R}_p$, $y \neq 0$. Тогда, используя уже доказанное сравнение и свойство символа Лежандра, находим

$$\begin{aligned} \alpha^p =& (x + y\sqrt{\Delta})^p \equiv x^p + y^p \Delta^{p/2} \equiv x + y\Delta^{(p-1)/2}\sqrt{\Delta} \equiv \\ \equiv& x + y\left(\frac{\Delta}{p}\right)\sqrt{\Delta} \pmod p. \end{aligned}$$

□

Следствие 4.4. *В условиях леммы 4.3 для каждого $\alpha \in \mathcal{R}_p$ такого, что $N(\alpha) \equiv 1 \pmod p$, выполняется сравнение*

$$\alpha^{p-(\Delta/p)} \equiv 1 \pmod p.$$

Доказательство. Пользуясь сравнением, доказанным в лемме 4.3, в случае $\left(\frac{\Delta}{p}\right) = -1$ находим

$$\alpha^{p+1} = \alpha\alpha^p \equiv \alpha\overline{\alpha} \equiv N(\alpha) \equiv 1 \pmod p.$$

Если же $\left(\frac{\Delta}{p}\right) = 1$, то

$$\alpha^{p-1} \equiv \alpha^{p-1} N(\alpha) \equiv \alpha^p \overline{\alpha} \equiv \alpha\overline{\alpha} \equiv N(\alpha) \equiv 1 \pmod{p}.$$

□

Следующее утверждение есть аналог теоремы 4.2 и следствия 4.1 для поля $\mathbb{Q}(\sqrt{\Delta})$.

Теорема 4.3. *Пусть N — нечетное число, $N+1 = FR$, Δ — целое с условием $(N, \Delta) = 1$. Если для каждого простого делителя q числа F существует $\alpha \in \mathcal{R}_N \subset \mathbb{Q}(\sqrt{\Delta})$, удовлетворяющее условиям*

$$\alpha^{N+1} \equiv 1 \pmod{N},\ N(\alpha) \equiv 1 \pmod{N}, \quad \left(\alpha^{(N+1)/q} - 1,\ N\right) = 1, \tag{4.15}$$

то любой простой делитель p числа N удовлетворяет сравнению

$$p \equiv \left(\frac{\Delta}{p}\right) \pmod{F}.$$

Доказательство. Пусть q — простой делитель F и $\alpha \in \mathcal{R}_N$ удовлетворяет условиям (4.15). Из первого условия следует $\alpha^{N+1} \equiv 1 \pmod{p}$. Обозначим буквой d наименьшее натуральное число, для которого $\alpha^d \equiv 1 \pmod{p}$. Тогда $d | N+1 = FR$.

Поскольку $\alpha^{(N+1)/q} \not\equiv 1 \pmod{p}$, в силу третьего условия (4.15), то $d \nmid (N+1)/q$ и, значит, $\nu_q(d) = \nu_q(N+1) \geqslant \nu_q(F)$.

Так как $N(\alpha) \equiv 1 \pmod{N}$, то $N(\alpha) \equiv 1 \pmod{p}$ и по следствию 4.4 имеем

$$\alpha^{p-(\Delta/p)} \equiv 1 \pmod{p}.$$

Значит, $d \big| \big(p - (\Delta/p)\big)$ и

$$\nu_q(p - (\Delta/p)) \geqslant \nu_q(d) \geqslant \nu_q(F).$$

Так как это верно для любого простого $q | F$, то $F | p - (\Delta/p)$. □

Если N — нечетное простое число и α удовлетворяет условиям (4.15) при любом простом q, делящем F, причем $F > 2$, то обязательно $\left(\frac{\Delta}{N}\right) = -1$. Действительно, в противном случае согласно первому из условий (4.15) и лемме 4.3 должны быть выполнены сравнения

$$\alpha^{N+1} \equiv 1 \pmod{N}, \qquad \alpha^N \equiv \alpha \pmod{N},$$

так что $\alpha^2 \equiv 1 \pmod{N}$. Но тогда согласно третьему условию (4.15) отношение $(N+1)/q$ должно быть нечетным для любого простого делителя q числа F. Но это возможно лишь при $F = 2$.

Следствие 4.5. *Если в условиях теоремы 4.3 выполнено неравенство $F > \sqrt{N} + 1$, то N — простое число.*

Доказательство. Предположим, что N — составное число и p — его наименьший простой делитель. Тогда $p \leqslant \sqrt{N}$ и согласно теореме 4.3 имеем $p \geqslant F - 1$ и $F \leqslant \sqrt{N} + 1$. □

Рассмотрим некоторые примеры использования теоремы 4.3 для доказательства простоты чисел.

Пусть $M_n = 2^n - 1$. Если $n = uv$ — составное, то $M_n = 2^{uv} - 1$ делится на $M_u = 2^u - 1$. Значит, M_n может быть простым, только если n — простое число. Числа M_p при простом p называются *числами Мерсенна*. Эти числа могут быть как простыми, так и составными. Так, например,

$$M_{11} = 2047 = 23 \cdot 89, \quad M_{23} = 8388607 = 47 \cdot 178481,$$

а остальные M_p при $p < 30$ просты.

В 1772 году Эйлер доказал простоту числа $2^{31} - 1$, а Люка в 1878г. установил простоту числа $2^{127} - 1$ и доказал, что $2^{61} - 1$ — составное число.

Теорема 4.4 (Люка 1878, Лемер, 1930)**.** *Пусть m — нечетное число, $m \geqslant 3$, и последовательность целых чисел L_n, $0 \leqslant L_n < 2^m - 1$, задается правилом*

$$L_0 = 4, \qquad L_{n+1} \equiv L_n^2 - 2 \pmod{2^m - 1}, \quad n \geqslant 0.$$

Число $2^m - 1$ *будет простым тогда и только тогда, когда*

$$L_{m-2} = 0.$$

Доказательство. Обозначим $N = 2^m - 1$, $K = \mathbb{Q}(\sqrt{3})$ и $\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$ — корни многочлена $x^2 - 4x + 1$. Пусть также $V_k = \alpha^k + \beta^k$, $k \geqslant 0$. Имеем

$$V_0 = 2,\ V_1 = 4, \quad V_{k+2} - 4V_{k+1} + V_k = 0,\ k \geqslant 0,$$

так что $V_k \in \mathbb{Z}$. Кроме того,

$$V_{2k} = \alpha^{2k} + \beta^{2k} = V_k^2 - 2.$$

Из последнего равенства легко следует сравнение

$$L_n \equiv V_{2^n} = \alpha^{2^n} + \beta^{2^n} \pmod{N}. \tag{4.16}$$

Действительно, оно, очевидно, имеет место при $n = 0$. Предположив же его справедливость при некотором $n \geqslant 0$, имеем

$$L_{n+1} \equiv L_n^2 - 2 \equiv V_{2^n}^2 - 2 \equiv V_{n+1} \pmod{N}.$$

Предположим, что $L_{m-2} = 0$ и докажем, что N — простое. Воспользуемся следствием 4.5 при $\alpha = 2 + \sqrt{3}$. Из (4.16) следует, что

$$\alpha^{2^{m-2}} + \beta^{2^{m-2}} \equiv 0 \pmod{N}. \tag{4.17}$$

Умножая это сравнение на $\alpha^{2^{m-2}}$, находим $\alpha^{2^{m-1}} \equiv -1 \pmod{N}$ или $\alpha^{(N+1)/2} \equiv -1 \pmod{N}$. Поэтому

$$\left(\alpha^{(N+1)/2} - 1, N\right) = (-2, N) = 1$$

и $\alpha^{N+1} \equiv 1 \pmod{N}$. Кроме того, $N(\alpha) = \alpha\beta = 1$. Поскольку $N+1 = 2^m$, то с $F = 2^m$ и $R = 1$ имеем $F - 1 = N > \sqrt{N}$, так что согласно следствию 4.5 число N должно быть простым.

Пусть теперь N — простое число. Необходимо доказать сравнение (4.17). Так как $(1 + \sqrt{3})^2 = 2(2 + \sqrt{3})$, то

$$(1 + \sqrt{3})^{N+1} = 2^{(N+1)/2}(2 + \sqrt{3})^{(N+1)/2}. \tag{4.18}$$

Далее в доказательстве будет использоваться квадратичный закон взаимности. Справедливы сравнения

$$2^{(N+1)/2} = 2 \cdot 2^{(N-1)/2} \equiv 2 \cdot \left(\frac{2}{N}\right) \equiv 2 \cdot (-1)^{(N^2-1)/8} \equiv 2 \pmod{N}. \tag{4.19}$$

Последнее сравнение имеет место в силу того, что $\nu_2(N^2-1) = 1 + \nu_2(N+1) = 1+m \geqslant 4$. Так как $N \equiv 3 \pmod 4$ и $N \equiv (-1)^m - 1 \equiv 1 \pmod 3$, то

$$\left(\frac{3}{N}\right) = -\left(\frac{N}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

По лемме 4.3 имеем

$$(1+\sqrt{3})^{N+1} \equiv (1+\sqrt{3})(1-\sqrt{3}) \equiv -2 \pmod{N}.$$

А из этого сравнения и (4.18), (4.19) следует

$$(2+\sqrt{3})^{(N+1)/2} \equiv -1 \pmod{N}$$

или $\alpha^{2^{m-1}} \equiv -1 \pmod N$. Умножая это сравнение на $\beta^{2^{m-2}}$, находим $\alpha^{2^{m-2}} + \beta^{2^{m-2}} \equiv 0 \pmod N$ или $L_{m-2} \equiv 0 \pmod N$. □

Теорема 4.4 сводит доказательство простоты чисел Мерсенна к рутинным вычислениям, выполняемым, правда, с очень большими числами. Так, например, была доказана простота числа $2^{32582657} - 1$.

С простыми числами Мерсенна связаны так называемые *совершенные* числа. Целое число A называется совершенным, если сумма его собственных делителей равна A. Например, число 6 совершенно, так как 6=1+2+3. Эйлер доказал, что четное число A совершенно, если и только если $A = 2^n(2^{n+1}-1)$, где $2^{n+1}-1$ — простое число, т.е. число Мерсенна. Нечетные совершенные числа неизвестны.

Еще один пример использования доказанных теорем — поиск пар простых чисел-близнецов. Простые числа p, q называются *близнецами*, если $p - q = 2$. Поиск таких пар простых чисел можно вести, перебирая четные числа $M = FR$ с известным разложением F на множители, пытаясь доказать простоту $p = M+1$ с помощью $p-1$ —

теста, а простоту $q = M-1$ — с помощью $q+1$ — теста. Если оба числа p и q окажутся простыми, будет построена пара простых-близнецов. Так, например, оба числа

$$242206083 \cdot 2^{38880} \pm 1 \tag{4.20}$$

просты. Числа (4.20) составляют не самую большую из известных пар простых чисел-близнецов. Предполагается, что множество таких пар бесконечно. Но эта, одна из самых известных в теории чисел гипотез, в настоящее время не доказана.

Еще один пример использования $N+1$ — тестов на простоту связан с поисками так называемых *дружественных* чисел. Натуральные числа A и B называются дружественными, если сумма собственных делителей A равна B и наоборот. В IX веке, Сабит ибн Корра доказал, что если все три числа

$$p = 3 \cdot 2^{n-1} - 1, \quad q = 3 \cdot 2^n - 1, \quad r = 9 \cdot 2^{2n-1} - 1$$

просты, то

$$A = 2^n pq, \qquad B = 2^n r$$

— дружественные. Так, дружественные числа $A = 220, B = 284$ получаются при $n = 2, p = 5, q = 11, r = 71$. Этот пример был известен Пифагору. Известны дружественные числа, получаемые и с помощью других конструкций.

Наконец, рассмотрим некоторый аналог теоремы 4.3, формулируемый на языке рекуррентных последовательностей второго порядка — так называемых *последовательностей Люка*. Пусть P, Q — целые и взаимно простые числа, α, β — корни многочлена $x^2 - Px + Q$, а $\Delta = P^2 - 4Q$ — дискриминант этого многочлена. Последовательность целых чисел U_n, называемая последовательностью Люка, определяется с помощью равенства

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad n \geqslant 0.$$

Она удовлетворяет рекуррентному уравнению

$$U_{n+1} = PU_n - QU_{n-1}, \qquad U_0 = 0,\ U_1 = 1,$$

и потому все ее члены являются целыми числами.

Теорема 4.5 (Моррисон, 1975). *Пусть N — нечетное число, $N+1 = FR$, $(F,R) = 1$ и Δ — целое число, взаимно простое с N. Если для каждого простого q, делящего F, существуют целые P, Q с условиями $(Q,N) = 1$, $P^2 - 4Q = \Delta$ и такие, что члены соответствующей последовательности Люка удовлетворяют условиям*

$$U_{N+1} \equiv 0 \pmod{N}, \qquad (N, U_{(N+1)/q}) = 1,$$

то каждый простой делитель p числа N удовлетворяет сравнению

$$p \equiv \left(\frac{\Delta}{p}\right) \pmod{F}.$$

Доказательство. Обозначим $\alpha = (P + \sqrt{\Delta})/2$, $\beta = (P - \sqrt{\Delta})/2$ и $\gamma = \alpha/\beta = \alpha^2/Q \in \mathcal{R}_N$. Так как $N(\alpha) = N(\beta) = (P^2 - \Delta)/4 = Q$, то $N(\gamma) = N(\alpha)/N(\beta) = 1$. Кроме того,

$$\gamma^{N+1} - 1 = \frac{\alpha^{N+1} - \beta^{N+1}}{\beta^{N+1}} = \frac{\alpha^{N+1}}{Q^{N+1}}(\alpha - \beta)U_{N+1} \equiv 0 \pmod{N}$$

и

$$\gamma^{(N+1)/q} - 1 = \frac{\alpha^{(N+1)/q}}{Q^{(N+1)/q}}(\alpha - \beta)U_{(N+1)/q}.$$

Учитывая, что оба числа $N(\alpha) = Q$, $N(\alpha - \beta) = -\Delta$ взаимно просты с N, заключаем, что $\gamma^{(N+1)/q} - 1$ и N взаимно просты в кольце $\mathcal{R}_N$. Таким образом, для чисел γ и N выполнены условия теоремы 4.3. Применяя эту теорему, получаем нужное утверждение. □

Сделаем несколько замечаний по поводу приведенных тестов на простоту.

1. Пусть $P_i^2 - 4Q_i = \Delta$. Положим

$$P_{i+1} = P_i + 2, \qquad Q_{i+1} = P_i + Q_i + 1.$$

Тогда

$$P_{i+1}^2 - 4Q_{i+1} = P_i^2 - 4Q_i = \Delta.$$

Это позволяет при фиксированном Δ размножать последовательности Люка $U_n^{(i)}$ с тем, чтобы найти последовательность, удовлетворяющую условиям теоремы 4.5.

2. Возможно совместное использование $N-1$ и $N+1$ — тестов для доказательства простоты числа N. Если $N-1 = F_1R_1$ и $N+1 = F_2R_2$, где F_1 и F_2 — известные части разложений $N-1$ и $N+1$ на простые сомножители, то, при выполнении условий в следствии 4.1 и теореме 4.3, каждый простой делитель p числа N удовлетворяет условиям

$$p \equiv 1 \pmod{F_1}, \qquad p \equiv \left(\frac{\Delta}{p}\right) \pmod{F_2}.$$

Если предположить, что $\left(\frac{\Delta}{N}\right) = -1$ (см. замечание после доказательства теоремы 4.3), то среди простых делителей числа N должен существовать такой делитель p, что $\left(\frac{\Delta}{p}\right) = -1$ и, значит,

$$p \equiv 1 \pmod{F_1}, \qquad p \equiv -1 \pmod{F_2}. \tag{4.21}$$

Так как $N = pv$ с некоторым целым v, то

$$v \equiv pv \equiv 1 \pmod{F_1}, \qquad v \equiv -pv = -N \equiv 1 \pmod{F_2}$$

и, следовательно, $v-1$ делится на наименьшее общее кратное чисел F_1, F_2. Учитывая, что $(F_1, F_2)|(N-1, N+1) = 2$, получаем, что это наименьшее общее кратное не меньше, чем $F_1F_2/2$, так что в предположении, что N не просто, т.е. $v > 1$, получаем неравенство

$$v \geqslant 1 + \frac{F_1F_2}{2}.$$

Из (4.21) следует

$$p \geqslant \max\{F_1 + 1,\ F_2 - 1\}.$$

Таким образом,

$$N = pv \geqslant (1 + F_1F_2/2)\max\{F_1 + 1,\ F_2 - 1\}.$$

Значит, если выполняется неравенство

$$(1 + F_1F_2/2)\max\{F_1 + 1,\ F_2 - 1\} > N$$

и выполнены указанные выше условия, то можно утверждать, что N — простое число.

3. Существуют тесты использующие не только делители чисел $N \pm 1$, но и делители чисел $N^2 + 1$, $N^2 \pm N + 1$. Указанные выше многочлены от N суть минимальные многочлены корней из единицы степеней 4, 3 и 6.

4. Пусть $N + 1 = FR$ и для любого простого делителя $p|N$ выполнено сравнение $p \equiv \left(\frac{\Delta}{p}\right) \pmod F$. Учитывая, что $N^0 = 1$ и $N \equiv -1 \pmod F$, сравнение для p можно переписать в виде

$$p \equiv N^i \pmod F, \qquad i \in \{0, 1\}.$$

4.5 Алгоритм Коэна–Ленстры.

В 1980 г. Адлеман и Рамели предложили алгоритм, доказывающий простоту числа N за $O((\log N)^{c \log\log\log N})$ арифметических операций. В этом алгоритме число N подвергается ряду тестов, причем либо обнаруживается, что число N составное, либо получается некоторая информация о возможных простых делителях N. Эта информация, накопленная после прохождения числом N всех тестов, позволяет резко сузить множество возможных делителей N. Количество возможных кандидатов становится столь маленьким, что их можно перебрать за приемлемое время и найти таким способом делитель N или доказать, что N — простое. Поскольку в пределах возможных приложений величина $\log\log\log N$ сравнительно невелика, алгоритм оказался эффективным на практике.

В 1982 г Х. Ленстра упростил этот алгоритм, отказавшись от использования закона взаимности в круговых полях, и заменил его тестами, использующими суммы Гаусса.

Последние усовершенствования были внесены в алгоритм в 1984г. А.Коэном и Х.Ленстрой. Именно эта версия обсуждается в дальнейшем. Сейчас будет описана общая схема алгоритма, детали его будут изложены в последующих параграфах.

Алгоритм 4.3. *Дано натуральное число N. Требуется установить составное оно или простое.*

1. Выбираются натуральные числа s и t, взаимно простые с N и обладающие следующими свойствами:

а) t не очень велико,

б) $s > N^{1/2}$,

в) для любого целого a, взаимно простого с s, имеет место сравнение $a^t \equiv 1 \pmod{s}$.

г) известны разложения на множители чисел s и t.

2. Число N подвергается ряду тестов, подобных малой теореме Ферма. Если какой-либо тест не проходит, то число N — составное.

3. Определить числа

$$r_i \equiv N^i \pmod{s}, \quad 1 \leqslant r_i < s, \qquad i = 0, 1, \ldots, t.$$

Если ни одно из чисел r_i не является делителем N, то N — простое число.

Можно доказать, что если число N прошло все тесты пункта 2, то каждый делитель r числа N удовлетворяет сравнению

$$r \equiv N^i \pmod{s}$$

при некотором i из промежутка $0 \leqslant i \leqslant t$. Поэтому, если N — составное и p — наименьший простой делитель N, то при некотором i, $0 \leqslant i \leqslant t$ должны выполняться условия

$$p \leqslant \sqrt{N} < s, \qquad p \equiv r_i \pmod{s},$$

означающие, что $p = r_i$. Это объясняет утверждение пункта 3 в алгоритме.

Условие в) пункта 1 алгоритма можно обеспечить, определив при фиксированном четном t параметр s с помощью равенства

$$s = e(t) = 2 \cdot \prod_{q-1|t} q^{\nu_q(t)+1}, \tag{4.22}$$

где произведение берется по всем простым q с условием $q-1|t$. Для нечетного q имеем $\varphi(q^{\nu_q(t)+1}) = q^{\nu_q(t)}(q-1)|t$, здесь $\varphi(n)$ — функция Эйлера, и, значит, в силу малой теоремы Ферма, $a^t \equiv 1 \pmod{q^{\nu_q(t)+1}}$ при любом целом a, взаимно простом с s. Если же $q = 2$, то $m = \nu_2(s) = 2 + \nu_2(t) \geqslant 3$, и для любого нечетного a имеем сравнение $a^{2^{m-2}} \equiv 1 \pmod{2^m}$, так что в силу равенства $\nu_2(t) = m-2$ имеем $a^t \equiv 1 \pmod{2^m}$. Условие в) следует из доказанных сравнений. При заданном N число t можно выбрать в виде произведения степеней малых простых и притом так, чтобы выполнялось неравенство $s > N^{1/2}$.

Например, взяв $t = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, мы получим

$$s = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 113 \cdot$$
$$127 \cdot 181 \cdot 211 \cdot 241 \cdot 281 \cdot 337 \cdot 421 \cdot 631 \cdot 1009 \cdot 2521 \sim 1,532 \cdot 10^{52},$$

и такой выбор параметров позволит проверять простоту всех чисел, ограниченных величиной 10^{100}.

Следующая теорема, показывающая соотношение величин параметров t и s в алгоритме и приводимая здесь без доказательства, была установлена Померанцем и Одлыжкой.

Теорема 4.6. *Существует эффективно вычислимая постоянная $c > 0$ такая, что для любого $N > e^e$ найдется положительное целое число t с условиями*

$$t < (\ln N)^{c \ln\ln\ln N}, \qquad e(t) > N^{1/2}.$$

Количество арифметических операций в алгоритмах Адлемана–Рамели и Ленстры оценивается сверху величиной $O\Big((\ln N)^{c \ln\ln\ln N}\Big)$. Доказательство этой оценки опирается на теорему 4.6. Для алгоритма, предложенного Коэном и Ленстрой такую оценку доказать не удается, хотя он наиболее эффективен на практике.

4.5.1 Корни из единицы и суммы Гаусса.

При любом целом $m \geqslant 2$ числа $e^{\frac{2\pi ik}{m}}$, $1 \leqslant k \leqslant m$, лежат в комплексной плоскости на окружности единичного радиуса с центром в точке 0 и являются вершинами правильного m — угольника, вписанного в эту окружность. Каждое из них есть корень многочлена $x^m - 1$ и потому справедливо равенство

$$x^m - 1 = \prod_{k=1}^{m} \left(x - e^{\frac{2\pi ik}{m}} \right)$$

Многочленом деления круга на m частей называют

$$\Phi_m(x) = \prod_{(k,m)=1} \left(x - e^{\frac{2\pi ik}{m}} \right).$$

Здесь произведение берется по всем целым числам $k, 1 \leqslant k \leqslant m$, взаимно простым с m. Из этого определения следует, что коэффициент при старшей степени x в многочлене $\Phi_m(x)$ равен 1 и $\deg \Phi_m(x) = \varphi(m)$, где, как и ранее, $\varphi(m)$ — функция Эйлера.

Для каждого натурального d, делящего m, и любого целого $c, 1 \leqslant c \leqslant d, (c,d) = 1$, рациональное число $\frac{c}{d}$ содержится среди дробей $\frac{k}{m}$, $1 \leqslant k \leqslant m$. Поэтому $\Phi_d(x) | x^m - 1$. С другой стороны, взяв любую дробь $\frac{k}{m}, 1 \leqslant k \leqslant m$ и сократив ее на наибольший общий делитель числителя и знаменателя, найдем представление $\frac{k}{m} = \frac{c}{d}$, $1 \leqslant c \leqslant d$, $(c,d) = 1$. Это приводит к равенству

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

Доказанное тождество дает нам

$$\Phi_1(x) = x - 1,\ \Phi_2(x) = \frac{x^2 - 1}{\Phi_1(x)} = x + 1,\ \Phi_3(x) = \frac{x^3 - 1}{\Phi_1(x)} = x^2 + x + 1,$$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1.$$

Таким же способом с помощью метода математической индукции можно доказать, что при любом натуральном m многочлен $\Phi_m(x)$ имеет целые коэффициенты.

Комплексное число $e^{\frac{2\pi i}{m}}$ будем в дальнейшем обозначать для краткости символом ζ_m. Можно доказать, см., например, [3], что при любом целом $m \geqslant 2$ многочлен $\Phi_m(x)$ неприводим над полем рациональных чисел $\mathbb{Q}$.

Кольцо $\mathbb{Z}[\zeta_m]$ состоит из чисел вида $f(\zeta_m)$, где $f(x)$ — произвольный многочлен с целыми коэффициентами. Из указанных выше свойств многочленов деления круга следует, что каждое число $\alpha \in \mathbb{Z}[\zeta_m]$ единственным способом представляется в виде $\alpha = f(\zeta_m)$, где $f(x) \in \mathbb{Z}[x], \deg f(x) < \varphi(m)$.

Пусть q — простое нечетное число, g — первообразный корень по модулю q и ξ — произвольный корень из 1 степени $q-1$. Определим функцию натурального аргумента

$$\chi(x) = \begin{cases} 0 & \text{если } q|x, \\ \xi^u & \text{если } q \nmid x \text{ и } x \equiv g^u \pmod{q} \end{cases}. \tag{4.23}$$

Легко проверить следующие ее свойства.

1. $\chi(x) = 0$, если и только если x делится на q,
2. $\chi(x+q) = \chi(x)$ при любом целом x,
3. $\chi(xy) = \chi(x)\chi(y)$ при любых целых x и y.

Таким образом, $\chi(x)$ есть характер по модулю q, см. параграф 4.1.

В силу равенства $\chi(g) = \xi$ различным корням из единицы ξ соответствуют различные характеры. Поэтому для любого простого числа q существует в точности $q-1$ различных характеров. В частности, при $\xi = 1$ получаем так называемый главный характер

$$\chi_0(x) = \begin{cases} 0 & \text{если } q|x, \\ 1 & \text{если } q \nmid x \end{cases}.$$

Выберем $\xi = -1$, это возможно так как $q-1$ четное число, а соответствующий характер обозначим $\chi_-(x)$. Тогда из формулы (4.23)

следует, что для каждого целого числа x, не делящегося на q, выполняется $\chi_-(x) = 1$ в том и только том случае, когда число u четное, и $\chi_-(x) = -1$, когда u нечетное число. Первый случай имеет место для квадратичных вычетов по модулю q, а второй для квадратичных невычетов. Но это означает, что

$$\chi_-(x) = \left(\frac{x}{q}\right)$$

— символ Лежандра.

Если $x \not\equiv y \pmod q$, то существует характер χ по модулю q такой, что $\chi(x) \neq \chi(y)$. Действительно, возьмем $\xi = \zeta_{q-1}$. Пусть $x \equiv g^u \pmod q$ и $y \equiv g^v \pmod q$. Тогда $\chi(x) = \zeta_{q-1}^u$, $\chi(y) = \zeta_{q-1}^v$. Равенство $\chi(x) = \chi(y)$ означает $\zeta_{q-1}^u = \zeta_{q-1}^v$. Следовательно $q-1|(u-v)$ и $x \equiv y \pmod q$.

Характеры при фиксированном q образуют группу по умножению. Роль единицы этой группы играет главный характер $\chi_0(x)$. Пусть характер χ соответствует корню из единицы ξ. Обратным к χ будет характер, соответствующий корню ξ^{-1}, ведь $\chi \cdot \chi^{-1} = \chi_0$. В этой группе можно выделить некоторые основные характеры.

Пусть $q - 1 = p_1^{k_1} \cdots p_\nu^{k_\nu}$ — разложение на простые множители. Рассмотрим p — одно из простых чисел p_j и k — соответствующий показатель степени k_j. Так как $p^k|q-1$, то число ζ_{p^k} есть корень из единицы степени $q-1$. Характер, определенный с помощью равенства (4.23) для корня $\xi = \zeta_{p^k}$ будем в дальнейшем обозначать символом $\chi_{p,q}$. Произвольный корень из единицы η степени $q-1$ имеет виде $\eta = \zeta_{q-1}^r$. Представим рациональное число $\frac{r}{q-1}$ суммой дробей, знаменатели которых есть степени простых чисел, входящих в разложение $q-1$, т.е.

$$\frac{r}{q-1} = \frac{u_1}{p_1^{k_1}} + \cdots + \frac{u_\nu}{p_\nu^{k_\nu}}, \qquad u_j \in \mathbb{Z}.$$

Тогда $\eta = \prod_{j=1}^{\nu} \zeta_{p_j^{k_j}}^{u_j}$ и для характера χ, соответствующего корню η,

находим представление

$$\chi = \prod_{j=1}^{\nu} \chi_{p_j,q}^{u_j}.$$

Таким образом, каждый из $q-1$ характеров по модулю q может быть представлен в виде произведения степеней базисных характеров $\chi_{p,q}$. Это позволяет ограничиться при проверке необходимых свойств в алгоритме лишь сравнительно небольшим множеством характеров вида $\chi_{p,q}$. Их количество равно числу простых делителей у $q-1$.

Суммы вида

$$\tau(\chi) = \sum_{x=1}^{q-1} \chi(x)\zeta_q^x,$$

обладающие рядом замечательных свойств, носят название *сумм Гаусса*. Например,

$$\tau(\chi_0) = \sum_{x=1}^{q-1} \zeta_q^x = \frac{\zeta_q - \zeta_q^q}{1-\zeta_q} = -1.$$

Пусть ξ — корень из 1 степени $q-1$, $\chi(x)$ — соответствующий характер. Тогда из определения суммы Гаусса следует, что $\tau(\chi) \in \mathbf{A} = \mathbb{Z}[\xi, \zeta_q]$.

Пусть N — натуральное число. Любые два числа α, β кольца $\mathbf{A}$ называются сравнимыми по модулю N, если разность $\alpha - \beta$ делится в кольце $\mathbf{A}$ на N, т.е. если существует число $\gamma \in \mathbf{A}$, для которого $\alpha - \beta = N\gamma$. Сравнимость как и для целых чисел будет обозначаться $\alpha \equiv \beta \pmod{N}$.

Лемма 4.4. *Пусть N — простое число, отличное от q. В кольце $\mathbf{A}$ выполняется сравнение*

$$\tau(\chi)^N \equiv \tau(\chi^N)\chi(N)^{-N} \pmod{N}. \tag{4.24}$$

Доказательство. Так как N — простое число, то каждый биномиальный коэффициент $\binom{N}{k}, 0 < k < N$, делится на N. Из формулы

Ньютона для бинома следует теперь сравнение $(\alpha+\beta)^N \equiv \alpha^N + \beta^N \pmod N$, справедливое при любых $\alpha, \beta \in \mathbf{A}$. Оно справедливо для любого количества слагаемых, поэтому

$$\tau(\chi)^N \equiv \sum_{x=1}^{q-1} \chi(x)^N \zeta_q^{Nx} \equiv \chi(N)^{-N} \sum_{x=1}^{q-1} \chi(Nx)^N \zeta_q^{Nx} \pmod N.$$

Учитывая, что при $x = 1, 2, \ldots, q-1$ числа $N, 2N, \ldots, (q-1)N$ пробегают все классы вычетов по модулю q, состоящие из целых чисел, не делящихся на q, можем продолжить сравнение

$$\tau(\chi)^N \equiv \chi(N)^{-N} \sum_{y=1}^{q-1} \chi(y)^N \zeta_q^y = \chi(N)^{-N} \tau(\chi^N) \pmod N.$$

□

Сравнение из леммы 4.4 это аналог малой теоремы Ферма для кольца $\mathbf{A}$. Если при некотором натуральном N, не делящемся на q оно нарушается, значит, N составное число. Выбирая разными способами простые числа q и характеры χ можно увеличить количество тестов.

Лемма 4.5. *Если $\chi \neq \chi_0$, то для любого характера χ выполняется*

$$\tau(\chi)\tau(\chi^{-1}) = \chi(-1)q.$$

Эта лемма показывает, что при каждом N взаимно простом с q гауссова сумма $\tau(\chi)$ будет обратима по модулю N в кольце $\mathbf{A}$.

Доказательство. Имеем

$$\tau(\chi)\tau(\chi^{-1}) = \sum_{x=1}^{q-1} \sum_{y=1}^{q-1} \chi(x)\chi^{-1}(y)\zeta_q^{x+y} = \sum_{y=1}^{q-1} \chi^{-1}(y) \sum_{x=1}^{q-1} \chi(x)\zeta_q^{x+y}.$$

При каждом фиксированном y во внутренней сумме сделаем замену переменных $x = zy$. Если z пробегает промежуток $1 \leqslant z \leqslant q-1$,

то x будет пробегать все ненулевые классы вычетов по модулю q. Учитывая, что функция $\chi(x)\zeta_q^{x+y}$ имеет период q по переменной x, находим

$$\tau(\chi)\tau(\chi^{-1}) = \sum_{y=1}^{q-1} \chi^{-1}(y) \sum_{z=1}^{q-1} \chi(zy)\zeta_q^{y(1+z)} = \sum_{z=1}^{q-1} \chi(z) \sum_{y=1}^{q-1} \left(\zeta_q^{1+z}\right)^y.$$

При $z = q-1$ последняя внутренняя сумма равна $q-1$, а при остальных значениях z с $\eta = \zeta_q^{1+z}$ находим $\sum_{y=1}^{q-1} \eta^y = \frac{\eta-\eta^q}{1-\eta} = -1$. Поэтому

$$\tau(\chi)\tau(\chi^{-1}) = \chi(q-1)(q-1) - \sum_{z=1}^{q-2} \chi(z) = \chi(-1)q - \sum_{z=1}^{q-1} \chi(z) = \chi(-1)q.$$

Для доказательства последнего равенства заметим, что когда переменная z пробегает промежуток $1 \leqslant z \leqslant q-1$, целое число u, определенное условиями $z \equiv g^u \pmod q$, см. (4.23), пробегает весь промежуток $0 \leqslant u \leqslant q-2$. Поэтому

$$\sum_{z=1}^{q-1} \chi(z) = \sum_{u=0}^{q-2} \xi^u = \frac{1-\xi^{q-1}}{1-\xi} = 0. \tag{4.25}$$

□

Пусть p — простой делитель $q-1$. Рассмотрим поля алгебраических чисел $K = \mathbb{Q}(\zeta_q) \subset E = \mathbb{Q}(\zeta_{p^k}, \zeta_q)$, где k — кратность, с которой p входит в разложение $q-1$ на простые сомножители. Минимальные многочлены чисел ζ_q и ζ_{p^k}, как указывалось выше, равны $\Phi_q(x)$ и $\Phi_{p^k}(x)$. Поэтому все сопряженные числа ζ_q имеют вид $\zeta_q^\ell, 1 \leqslant \ell \leqslant q-1$ и принадлежат полю K. Значит, K нормальное поле. Точно так же все сопряженные числа ζ_{p^k} равны $\zeta_{p^k}^\ell, 1 \leqslant \ell \leqslant p^k, p \nmid \ell$. Все они, как и все сопряженные числа ζ_q, содержатся в поле E. Значит, это поле также нормально.

Не трудно проверить, что число ζ_m, при $m = qp^k$, есть примитивный элемент поля E. Это следует из равенств

$$\zeta_{p^k} = \zeta_m^q, \qquad \zeta_q = \zeta_m^{p^k}, \qquad \zeta_m = \zeta_{p^k}\zeta_q^{-w}, \tag{4.26}$$

где $w = \frac{q-1}{p^k} \in \mathbb{Z}$. Значит, $E = \mathbb{Q}(\zeta_m)$, и степень поля E равна $\varphi(m)$.

Для каждого целого ℓ с условиями

$$1 \leqslant \ell < p^k, \qquad p \nmid \ell, \tag{4.27}$$

определим автоморфизм σ_ℓ поля E равенством $\sigma_\ell(\zeta_m) = \zeta_m^r$, где целое число $r, 0 \leqslant r < m$, определяется условиями

$$r \equiv 1 \pmod{q}, \qquad r \equiv \ell \pmod{p^k}, \tag{4.28}$$

см. §1.9. Заметим, что таким способом определяется $\varphi(p^k)$ различных автоморфизмов поля E.

Из равенств (4.26) следует, что

$$\sigma_\ell(\zeta_q) = \sigma_\ell(\zeta_m^{p_k}) = \zeta_m^{rp^k} = \zeta_q^r = \zeta_q, \quad \sigma_\ell(\zeta_{p^k}) = \sigma_\ell(\zeta_m^q) = \zeta_m^{rq} = \zeta_{p^k}^r = \zeta_{p^k}^\ell.$$

Таким образом, все автоморфизмы σ_ℓ действуют как тождественные отображения на поле K, а при ограничении на поле $\mathbb{Q}(\zeta_{p^k})$ дают всю группу автоморфизмов этого поля. Автоморфизм σ_1 есть тождественное отображение на поле E.

Пример. Так как значения характера $\chi = \chi_{p,q}$ есть корни из единицы степени p^k, имеем $\sigma_\ell(\chi(x)) = \chi(x)^\ell$ и

$$\sigma_\ell(\tau(\chi)) = \sum_{x=1}^{q-1} \chi(x)^\ell \zeta_q^x = \tau(\chi^\ell).$$

Обозначим буквой G множество всех автоморфизмов σ_ℓ. Из (4.28) следует, что для любых двух индексов u, v с условиями $\sigma_u, \sigma_v \in G$ следует $\sigma_s \in G$, где $s \equiv uv \pmod{p^k}$, а кроме того

$$\sigma_u\sigma_v(\zeta_{p^k}) = \sigma_u(\zeta_{p^k}^v) = \zeta_{p^k}^{uv} = \zeta_{p^k}^s = \sigma_s(\zeta_{p^k}).$$

Таким образом, $\sigma_u\sigma_v = \sigma_s$. В частности, если $uv \equiv 1 \pmod{p^k}$, то $\sigma_u\sigma_v = \sigma_1$. Эти свойства означают, что G есть мультипликативная группа, изоморфная группе $(\mathbb{Z}/p^k\mathbb{Z})^*$ обратимых элементов кольца классов вычетов $\mathbb{Z}/p^k\mathbb{Z}$. Расширим обозначения σ_ℓ на произвольные

целые индексы $\ell, p \nmid \ell$, полагая $\sigma_r = \sigma_s$, если $r \equiv s \pmod{p^k}$. Тогда, например, можно писать $\sigma_u \sigma_v = \sigma_{uv}$.

Степень поля E равна $\varphi(m) = (q-1)(p^k - p^{k-1})$, и любой его базис состоит из $\varphi(m)$ чисел. Если фиксировать какой-либо базис, то элементы E представляются при вычислениях векторами коэффициентов при разложении по этому базису, т.е. векторами очень большой длины. Действуя на сравнение (4.24) элементами $\sigma \in G$ и перемножая получившиеся сравнения, можно скомбинировать их так, что обе части результата будут принадлежать кольцу $\mathbb{Z}[\zeta_{p^k}]$, т.е. будут представлены векторами, намного более короткими. Итак, мы будем перемножать, возводя в целые степени, различные сопряженные чисел $\tau(\chi)$. Для упрощения записи удобно ввести некоторые специальные обозначения.

Пусть L множество целых чисел ℓ, удовлетворяющих условиям (4.27). Рассмотрим кольцо $\mathbb{Z}[G]$, элементами которого являются всевозможные формальные суммы

$$\sum_{j \in L} n_j \sigma_j, \qquad n_j \in \mathbb{Z}.$$

Эти суммы можно складывать покоординатно, т.е. прибавляя друг к другу коэффициенты при одинаковых автоморфизмах σ_j. Их также можно перемножать, пользуясь равенством $\sigma_u \sigma_v = \sigma_{uv}$ и перемножая коэффициенты по обычным правилам. Элемент σ_1 играет роль единицы в кольце $\mathbb{Z}[G]$. Для краткости элемент $N\sigma_1 \in \mathbb{Z}[G]$ будем обозначать буквой N.

Определим операцию возведения чисел из поля E в степень, равную какому-либо элементу кольца $\mathbb{Z}[G]$. Для каждого ненулевого числа $b \in E$ и элемента $\alpha = \sum_{j \in L} n_j \sigma_j \in \mathbb{Z}[G]$ положим

$$b^\alpha = \prod_{j \in L} \sigma_j(b)^{n_j}.$$

Эта операция, как легко следует из ее определения, обладает обычными свойствами возведения в степень. Какие бы два числа $a, b \in E$

ни взять, при любых $\alpha, \beta \in \mathbb{Z}[G]$ выполняются равенства

$$(ab)^\alpha = a^\alpha b^\alpha, \qquad a^{\alpha+\beta} = a^\alpha a^\beta, \qquad a^{\alpha\beta} = (a^\alpha)^\beta, \qquad a^{\alpha\beta} = a^{\beta\alpha}.$$

Например, учитывая лемму 4.5 и пользуясь введенными обозначениями, перепишем лемму 4.4 в виде

Лемма 4.6. *Пусть N — простое число, отличное от q и p. В кольце $\mathbf{B} = \mathbf{A}[1/q]$ выполняется сравнение*

$$\tau(\chi)^{N-\sigma_N} \equiv \chi(N)^{-N} \pmod{N}. \tag{4.29}$$

Сравнение (4.29) можно записать в виде равенства

$$\tau(\chi)^{N-\sigma_N} = \chi(N)^{-N} + N\gamma, \qquad \gamma \in \mathbf{B}.$$

Действуя на это равенство произвольным автоморфизмом $\sigma \in G$ и пользуясь указанными выше свойствами возведения в степень, находим

$$\tau(\chi)^{(N-\sigma_N)\sigma} = \chi(N)^{-N\sigma} + N\sigma(\gamma), \qquad \gamma \in \mathbf{B}.$$

Так как $\sigma(\mathbf{B}) \subset \mathbf{B}$, получившееся равенство можно переписать в виде сравнения в кольце $\mathbf{B}$

$$\tau(\chi)^{(N-\sigma_N)\sigma} \equiv \chi(N)^{-N\sigma} \pmod{N}. \tag{4.30}$$

Пусть теперь $\beta = \sum_{j\in L} n_j\sigma_j$ какой-либо элемент из кольца $\mathbb{Z}[G]$. Возводя сравнение (4.30) при $\sigma = \sigma_j$ в степень n_j и перемножая получившиеся сравнения при всех $j \in L$, находим

Следствие 4.6. *Пусть N — простое число, отличное от q и p. Для любого элемента $\beta \in \mathbb{Z}[G]$ в кольце $\mathbf{B} = \mathbf{A}[1/q]$ выполняется сравнение*

$$\tau(\chi)^{(N-\sigma_N)\beta} \equiv \chi(N)^{-N\beta} \pmod{N}. \tag{4.31}$$

Элемент β с нужными свойствами будет выбран в дальнейшем.

4.5.2 Основная теорема.

В этом параграфе будет доказана теорема, на которой основано утверждение из пункта 3 алгоритма 4.3. Ее формулировка и доказательство используют p-адические числа, см. §1.8.

Теорема 4.7. *Пусть N — целое число, $N > 1$, натуральные числа s, t таковы, что $(N, st) = 1$ и для любого целого a, взаимно простого с s, имеет место сравнение $a^t \equiv 1 \pmod{s}$. Пусть также элемент $\beta \in \mathbb{Z}[G]$ таков, что $\zeta_p^\beta \neq 1$, и выполнены два условия*
1. Для каждой пары простых чисел p, q с условиями $q|s, p|(q-1)$ и характера $\chi = \chi_{p,q}$ выполняется сравнение

$$\tau(\chi)^{(N-\sigma_N)\beta} \equiv \xi \pmod{N}, \tag{4.32}$$

где ξ — какой-либо корень из единицы степени p^k, $k = \nu_p(q-1)$.
2. Для каждого простого $p|t$ и каждого простого делителя r числа N существует целое p-адическое число $\ell_p(r)$, для которого

$$r^{p-1} = (N^{p-1})^{\ell_p(r)}. \tag{4.33}$$

Тогда для каждого натурального числа R, делящего N, найдется такое целое $i, 0 \leqslant i < t$, что

$$R \equiv N^i \pmod{s}.$$

Доказательство. Достаточно длинное доказательство мы разобьем на несколько пунктов.

1. Фиксируем пару простых чисел p, q с условиями $p|(q-1), q|s$, и пусть $k = \nu_p(q-1)$. Выберем целое x так, чтобы число $\eta = e^{2\pi i x/p^k} = \zeta_{p^k}^x$ удовлетворяло равенству $\xi = \eta^{-N\beta}$, где ξ — число из условия теоремы 4.7. Докажем, что такое число x существует. Пусть $\beta = \sum_j n_j \sigma_j$, где суммирование происходит по всем целым $j, 1 \leqslant j \leqslant p^k, p \nmid j$. Так как

$$\zeta_p^\beta = \prod_j \sigma_j(\zeta_p)^{n_j} = \prod_j \zeta_p^{jn_j} = e^{\frac{2\pi i}{p} \sum_j jn_j} \neq 1,$$

то $\sum_j jn_j \not\equiv 0 \pmod{p}$. Имеем

$$\eta^\beta = \prod_j \sigma_j(\eta)^{n_j} = \prod_j \zeta_{p^k}^{xjn_j} = \zeta_{p^k}^{x\sum_j jn_j}.$$

Пусть $\xi = \zeta_{p^k}^{\lambda}$. Равенство $\xi = \eta^{-N\beta}$ эквивалентно сравнению

$$-x\left(N\sum_j jn_j\right) \equiv \lambda \pmod{p^k},$$

которое разрешимо относительно x, ведь $p \nmid \sum_j jn_j$. Существование нужного x доказано.

Теперь сравнение (4.32) может быть переписано в виде

$$\tau(\chi)^{(N-\sigma_N)\beta} \equiv \eta^{-N\beta} \pmod{N}.$$

Обозначив $u = \tau(\chi)^\beta \in \mathbf{B} = \mathbb{Z}[\zeta_{p^k}, \zeta_q, \frac{1}{q}]$, находим

$$u^{N-\sigma_N} \equiv \eta^{-N\beta} \pmod{N}, \qquad \eta^{p^k} = 1.$$

2. При любом целом неотрицательном ℓ справедливо тождество

$$N^\ell - \sigma_N^\ell = (N-\sigma_N)\sum_{j=0}^{\ell-1} N^{\ell-1-j}\sigma_N^j.$$

Так как $\sigma_N(\eta) = \eta^N$, то находим

$$u^{N^\ell - \sigma_N^\ell} \equiv \eta^{-N\beta\sum_{j=0}^{\ell-1} N^{\ell-1-j}\sigma_N^j} = \eta^{-\ell N^\ell \beta} \pmod{N}.$$

Итак,

$$u^{N^\ell - \sigma_N^\ell} \equiv \eta^{-\ell N^\ell \beta} \pmod{N}, \qquad \ell = 0, 1, 2, \ldots. \tag{4.34}$$

Выберем $\ell = p^k(p-1)$. Тогда

$$u^{N^{p^k(p-1)} - \sigma_N^{p^k(p-1)}} \equiv 1 \pmod{N}.$$

Учитывая, что $\varphi(p^{k+1}) = p^k(p-1)$, и пользуясь теоремой Эйлера, находим $N^{p^k(p-1)} \equiv 1 \pmod{p^{k+1}}$. Поэтому $\sigma_N^{p^k(p-1)} = \sigma_{N^{p^k(p-1)}} = \sigma_1$ и, значит,

$$u^{N^{p^k(p-1)}-1} \equiv 1 \pmod{N}. \tag{4.35}$$

Пусть r — простой делитель числа N. Применяя следствие 4.6 к простому числу r, находим

$$u^{r-\sigma_r} \equiv \chi(r)^{-r\beta} \pmod{r}. \tag{4.36}$$

Отсюда, так же как и (4.34), выводим

$$u^{r^\ell-\sigma_r^\ell} \equiv \chi(r)^{-\ell r^\ell \beta} \pmod{r}, \qquad \ell = 0, 1, 2, \ldots. \tag{4.37}$$

Имеем $p|(q-1)$, $(q-1)|t$, так что $p|t$. Согласно условию теоремы с некоторым p-адическим числом $\ell_p(r) \in \mathbb{Z}_p$ выполняется сравнение (4.33). Определим целое положительное число m сравнением

$$m \equiv \ell_p(r) \pmod{p^h},$$

где целое число h выбрано столь большим, чтобы выполнялись неравенства $h \geqslant k$, $h \geqslant \nu_p(N^{p^k(p-1)} - 1)$. Из неравенства (1.41) при $a = N^{p-1}$ и $x = \ell_p(r) - m$ находим

$$\begin{aligned}\left|r^{p-1} - N^{(p-1)m}\right|_p &= \left|N^{(p-1)\ell_p(r)} - N^{(p-1)m}\right|_p = \\ &= \left|N^{(p-1)(\ell_p(r)-m)} - 1\right|_p \leqslant |N^{p-1}-1|_p \cdot |\ell_p(r) - m|_p \leqslant p^{-1-h}.\end{aligned}$$

В частности, эти неравенства означают, что $\nu_p\left(r^{p-1} - N^{(p-1)m}\right) \geqslant h+1 > \nu_p(N^{p^k(p-1)} - 1)$ и

$$d = \frac{N^{(p-1)m} - r^{p-1}}{N^{p^k(p-1)} - 1} = \frac{a}{b}, \tag{4.38}$$

где a, b — целые числа, причем $p \nmid b$. В дальнейшем числа a, b будут выбраны удовлетворяющими некоторым дополнительным свойствам.

Из (4.37) при $\ell = p-1$ находим

$$u^{r^{p-1}-\sigma_r^{p-1}} \equiv \chi(r)^{-(p-1)r^{p-1}\beta} \pmod{r},$$

а из (4.34) при $\ell = (p-1)m$ получаем

$$u^{N^{(p-1)m}-\sigma_N^{(p-1)m}} \equiv \eta^{-(p-1)mN^{(p-1)m}\beta} \pmod{r}.$$

Так как $r^{p-1} \equiv N^{(p-1)m} \pmod{p^k}$, то $\sigma_r^{p-1} = \sigma_{r^{p-1}} = \sigma_{N^{(p-1)m}} = \sigma_N^{(p-1)m}$ и

$$u^{N^{(p-1)m}-r^{p-1}} \equiv (\chi(r)\eta^{-m})^{(p-1)r^{p-1}\beta} \pmod{r}.$$

Возводя это сравнение в степень b, пользуясь (4.38) и (4.35), находим

$$1 \equiv (\chi(r)\eta^{-m})^{(p-1)r^{p-1}\beta} \pmod{r}.$$

Отсюда, поскольку $\sigma_j(\zeta_{p^k}) = \zeta_{p^k}^j$ следует

$$1 \equiv (\chi(r)\eta^{-m})^{(p-1)r^{p-1}b\sum_j jn_j} \pmod{r}. \tag{4.39}$$

Выберем теперь представление (4.38) с нужным свойством. Пусть $d = \frac{a_1}{b_1}$, $(a_1, b_1) = 1$. Так как

$$p \nmid (p-1)r^{p-1}b_1 \sum_j jn_j,$$

то найдется целое y с условием

$$(p-1)r^{p-1}b_1 \sum_j jn_j \cdot y \equiv 1 \pmod{p^k}.$$

Положим $b = b_1 y$ и $a = a_1 y$. Тогда $d = \frac{a}{b}$ и

$$(p-1)r^{p-1}b \sum_j jn_j \equiv 1 \pmod{p^k}.$$

Теперь из (4.39) следует

$$1 \equiv \chi(r)\eta^{-m} \pmod{r}. \tag{4.40}$$

3. Положим $\rho = \chi(r)\eta^{-m}$, $\rho^{p^k} = 1$. Допустим, что $\rho = \zeta_{p^k}^{\nu}$, $0 \leqslant \nu < p^k$, т.е. $\nu \neq 0$. Из тождества

$$1 + x + \ldots + x^{p^k-1} = \frac{x^{p^k} - 1}{x - 1} = \prod_{\ell=1}^{p^k-1} (x - \zeta_{p^k}^{\ell})$$

при $x = 1$, в силу (4.40), находим

$$p^k = \prod_{\ell=1}^{p^k-1} (1 - \zeta_{p^k}^{\ell}) \equiv 0 \pmod{r}.$$

Но это невозможно. Значит, $\rho = 1$, т.е.

$$\chi(r) = \eta^m = \eta^{\ell_p(r)}. \tag{4.41}$$

Если $x_n \in \mathbb{Z}$, $0 \leqslant x_n < p^n$, $\nu_p(\ell_p(r) - x_n) \geqslant n$, то последовательность η^{x_n} стабилизируется при $n \geqslant k$. Это число и обозначено выше $\eta^{\ell_p(r)}$.

Равенство (4.41) доказано выше для простых делителей r числа N. Из (4.33) следует $L_p(r^{p-1}) = \ell_p(r) L_p(N^{p-1})$. Если $N = r_1^{k_1} \cdots r_w^{k_w}$, то

$$L_p(N^{p-1}) = L_p\left(r_1^{(p-1)k_1} \cdots r_w^{(p-1)k_w}\right) = \sum_{j=1}^{w} k_j L_p(r_j^{p-1}) =$$
$$= \left(\sum_{j=1}^{w} k_j \ell_p(r_j)\right) L_p(N^{p-1}).$$

Так как $N^{p-1} \neq \pm 1$, то $L_p(N^{p-1}) \neq 0$ и

$$\sum_{j=1}^{w} k_j \ell_p(r_j) = 1.$$

Имеем

$$\chi(N) = \prod_{j=1}^{w} \chi(r_j)^{k_j} = \prod_{j=1}^{w} \eta^{k_j \ell_p(r_j)} = \eta^{\sum_{j=1}^{w} k_j \ell_p(r_j)} = \eta.$$

Теперь (4.41) может быть переписано в виде

$$\chi(r) = \chi(N)^{\ell_p(r)}, \qquad \chi = \chi_{p,q} \tag{4.42}$$

для любого простого r, делящего N.

4. Пусть r — простой делитель N. Определим целое число $\ell(r)$ с помощью системы сравнений

$$\ell(r) \equiv \ell_p(r) \pmod{p^h} \quad \text{при любом} \quad p|t, \tag{4.43}$$

где h — целое число, удовлетворяющее неравенствам

$$h > \max_{p|t} \max_{p|(q-1)} \nu_p(q-1), \qquad h > \max_{q|s} \nu_q(s).$$

Для любой пары p, q с условием $p|(q-1)$, пользуясь (4.42), находим

$$\chi_{p,q}(r) = \chi_{p,q}(N)^{\ell_p(r)} = \chi_{p,q}(N)^{\ell(r)} = \chi_{p,q}(N^{\ell(r)}).$$

Так как это равенство верно для любого p с условием $p|(q-1)$, то для любого характера χ по модулю q имеем $\chi(r) = \chi(N^{\ell(r)})$ и, значит,

$$r \equiv N^{\ell(r)} \pmod{q}. \tag{4.44}$$

Докажем, что

$$r \equiv N^{\ell(r)} \pmod{s}. \tag{4.45}$$

Если это не так, то существует такое простое число $q|s$, что $\nu_q(N^{\ell(r)} - r) < \nu_q(s) = m$. Тогда $m \geqslant 2$. Обозначим буквой a первообразный корень по модулю q^m взаимно простой с s. Согласно условию теоремы должно выполняться сравнение $a^t \equiv 1 \pmod{s}$. Тогда $a^t \equiv 1 \pmod{q^m}$ и, значит, $q^{m-1}(q-1)|t$. Так как при этом $q|t$, то по условию (4.33) имеем

$$r^{q-1} = (N^{q-1})^{\ell_q(r)}.$$

Из (4.43) следует $N^{(q-1)\ell_q(r)} \equiv N^{(q-1)\ell(r)} \pmod{q^h}$, так что

$$r^{q-1} \equiv N^{(q-1)\ell(r)} \pmod{q^h}. \tag{4.46}$$

Если $q = 2$, отсюда находим $\nu_2(N^{\ell(r)} - r) \geqslant h > m$. Но это невозможно. Значит, $q \geqslant 3$. Положим $a = rN^{-\ell(r)} \in \mathbb{Z}_q \cap \mathbb{Q}$. Из (4.44) следует, что

$$a = 1 + cq^{\lambda}, \qquad \lambda \geqslant 1, \qquad q \nmid c.$$

С помощью леммы 1.2 находим

$$a^{q-1} \equiv 1 + cq^{\lambda}(q-1) \pmod{q^{\lambda+1}},$$

т.е. $\nu_q(a^{q-1} - 1) = \lambda$. Теперь из (4.46) получаем $\lambda \geqslant h$. Это означает, что $a \equiv 1 \pmod{q^h}$ и $r \equiv N^{\ell(r)} \pmod{q^h}$. Следовательно $h < m = \nu_q(s)$. Получившееся противоречие доказывает (4.45).

5. По доказанному каждый простой делитель N сравним с некоторой степенью N по модулю s. Но тогда это верно и для любого делителя $R|N$, т.е. $R \equiv N^i \pmod{s}$. Поскольку $N^t \equiv 1 \pmod{s}$, можно считать, что $0 \leqslant i < t$, и это завершает доказательство теоремы. □

Замечание. Если $p \geqslant 3$ и $p^2 \nmid N^{p-1} - 1$, то условие 2) теоремы выполняется. Действительно, в этом случае $\nu_p(N^{p-1} - 1) = 1$ и для любого простого делителя r числа N имеем $\nu_p(r^{p-1} - 1) \geqslant 1 = \nu_p(N^{p-1} - 1)$. Согласно теореме 1.28 в этом случае существует единственное число $\ell_p(r)$ такое, что $r^{p-1} = N^{(p-1)\ell_p(r)}$.

Еще одно свойство, обеспечивающее выполнимость условия 2) теоремы, дает следующее утверждение.

Лемма 4.7. *Если χ — характер по модулю q порядка $p^k, p \geqslant 3$, и условие 1) теоремы 4.7, т.е. сравнение*

$$\tau(\chi)^{(N-\sigma_N)\beta} \equiv \xi \pmod{N}$$

выполняется с примитивным корнем ξ из 1 степени p^k, то условие 2) теоремы также выполняется.

Доказательство. Пусть корень из единицы η определен, как и ранее, равенством $\xi = \eta^{-N\beta}$. Так как при этом $p \nmid N$ и $\sum_j jn_j \not\equiv 0 \pmod{p}$, то η есть примитивный корень из 1 степени p^k. Пусть $u = \tau(\chi)^{\beta}$.

Для любого $\ell = 0, 1, \ldots$ в доказательстве теоремы были установлены сравнения

$$u^{N^\ell - \sigma_N^\ell} \equiv \eta^{-\ell N^\ell \beta} \pmod{N}, \qquad u^{r^\ell - \sigma_r^\ell} \equiv \chi(r)^{-\ell r^\ell \beta} \pmod{r},$$

см. (4.34) и (4.37). Поскольку $r|N$, первое сравнение выполняется и по модулю r. Обозначим буквой d порядок элемента $u \pmod{r}$ в мультипликативной группе вычетов кольца $\mathbf{B}$ по модулю r. Положим $\ell = p^{k-1}(p-1) = \varphi(p^k)$. Так как

$$N^{p^{k-1}(p-1)} \equiv 1 \equiv r^{p^{k-1}(p-1)} \pmod{p^k},$$

то при выбранном значении ℓ имеем $\sigma_N^\ell = \sigma_1 = \sigma_r^\ell$ и

$$u^{N^{\varphi(p^k)}-1} \equiv \eta^{-p^{k-1}(p-1)N^{\varphi(p^k)}\beta} = \eta^{p^{k-1}\beta} \pmod{r}, \tag{4.47}$$

$$u^{r^{\varphi(p^k)}-1} \equiv \chi(r)^{-p^{k-1}(p-1)r^{\varphi(p^k)}\beta} = \chi(r)^{p^{k-1}\beta} \pmod{r}. \tag{4.48}$$

Учитывая, что η — примитивный корень из 1 степени p^k, получаем $\eta^{p^{k-1}\beta} \neq 1$ и, поскольку $(p, r) = 1$, как и в пункте 3) доказательства теоремы, заключаем, что $\eta^{p^{k-1}\beta} \not\equiv 1 \pmod{r}$. Из (4.47) следует теперь, что $d \nmid N^{\varphi(p^k)} - 1$, но $d|p(N^{\varphi(p^k)} - 1)$. Поэтому $\nu_p(d) = \nu_p(N^{\varphi(p^k)} - 1) + 1$. Из (4.48) находим $d|p(r^{\varphi(p^k)} - 1)$ и $\nu_p(d) \leqslant 1 + \nu_p(r^{\varphi(p^k)} - 1)$. Поэтому

$$\nu_p(r^{\varphi(p^k)} - 1) \geqslant \nu_p(N^{\varphi(p^k)} - 1).$$

Из этого неравенства следует по теореме 1.28, что с некоторым целым p-адическим числом ℓ выполняется равенство

$$r^{p^{k-1}(p-1)} = N^{p^{k-1}(p-1)\ell}.$$

Отсюда же с помощью следствия 1.2 заключаем $r^{p-1} = N^{(p-1)\ell}$. Лемма доказана. □

Замечание. Если число N простое и условие леммы 4.7 нарушается при любом $q|s$, то условие 2) теоремы 4.7 можно подтвердить следующим образом.

Выберем простое число q так, чтобы

$$q \equiv 1 \pmod{p}, \quad \text{и} \quad N^{\frac{q-1}{p}} \not\equiv 1 \pmod{q}. \tag{4.49}$$

Пусть g — первообразный корень по модулю q и $N \equiv g^{\nu} \pmod{q}$, т.е. $\nu = \operatorname{ind} N$. Второе сравнение (4.49) означает, что $p \nmid \nu$.

Предположим, что $q|s$. Тогда для $\chi = \chi_{p,q}$ имеем

$$\tau(\chi)^{(N-\sigma_N)\beta} \equiv \chi(N)^{-N\beta} \pmod{N}. \tag{4.50}$$

Так как $\chi(N) = \zeta_{p^k}^{\nu}$ и $p \nmid \nu$, то $\chi(N)$ — примитивный корень из 1 степени p^k. Но тогда и $\xi = \chi(N)^{-N\beta}$ есть примитивный корень. Но это противоречит тому, что условие леммы 4.7 нарушается при любом $q|s$.

Значит, $q \nmid s$. Выберем теперь χ — характер порядка p и проверим для него условие леммы 4.5. Так как должно быть выполнено сравнение (4.50) и $\chi(N) = \zeta_p^{\nu}$ есть примитивный корень степени p, то по лемме 4.5 условие 2) теоремы 4.7 выполнено.

Можно доказать, что при фиксированном p вероятность найти подходящее q в прогрессии $1 + pj,\ j = 0, 1, 2, \ldots$ не меньше $1 - \frac{1}{p}$.

Подобные утверждения справедливы и при $p = 2$. Следующую лемму мы приводим без доказательства.

Лемма 4.8. *1. Если $N \equiv 1 \pmod{4}$ и существует целое число a с условием $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$, то условие 2) теоремы 4.7 выполняется при $p = 2$.*

2. Если $N \equiv 3 \pmod{8}$ и $2^{\frac{N-1}{2}} \equiv -1 \pmod{N}$, то условие 2) теоремы 4.7 выполняется при $p = 2$.

3. Если χ — характер по модулю q порядка 2^k, $k \geqslant 2$, и условие 1) теоремы 4.7 выполняется с примитивным корнем из 1 степени 2^k и $q^{\frac{N-1}{2}} \equiv -1 \pmod{N}$, то условие 2) этой теоремы выполняется при $p = 2$.

4.5.3 Суммы Якоби и тесты в алгоритме Коэна–Ленстры.

Пусть χ_1, χ_2 — некоторые характеры по модулю q. *Суммой Якоби* называется выражение

$$J(\chi_1, \chi_2) = \sum_{x=0}^{q} \chi_1(x)\chi_2(1-x).$$

Эти суммы тесно связаны с рассматривавшимися выше гауссовыми суммами $\tau(\chi)$.

Лемма 4.9. *Если* $\chi_1 \neq \chi_2^{-1}$, *то выполняется равенство*

$$J(\chi_1, \chi_2) = \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)}.$$

Доказательство. Имеем

$$\tau(\chi_1)\tau(\chi_2) = \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \chi_1(x)\chi_2(y)\zeta_q^{x+y} = \sum_{t=0}^{q-1}\left(\sum_{x+y\equiv t} \chi_1(x)\chi_2(y)\right)\zeta_q^t. \tag{4.51}$$

В последней внутренней сумме суммирование ведется по всем парам целых чисел x, y, $0 \leqslant x, y \leqslant q-1$, удовлетворяющих сравнению $x + y \equiv t \pmod q$. Для вычисления этой суммы рассмотрим отдельно два случая.

1) $t = 0$.

В этом случае внутренняя сумма равна

$$\sum_{x=0}^{q-1} \chi_1(x)\chi_2(-x) = \chi_2(-1)\sum_{x=0}^{q-1} \chi_1\chi_2(x) = 0.$$

Последнее равенство выполняется в силу того, что $\chi_1\chi_2 \neq \chi_0$, см. (4.25).

2) $t \neq 0$.

Так как $q \nmid t$, то для любых целых чисел x, y из рассмотренной выше внутренней суммы найдется такое целое число u, что

$$x \equiv tu \pmod q, \qquad y \equiv t(1-u) \pmod q, \qquad 0 \leqslant u < q.$$

Поэтому внутренняя сумма равна

$$\sum_{x+y\equiv t} \chi_1(x)\chi_2(y) = \chi_1(t)\chi_2(t)\sum_{u=0}^{q-1} \chi_1(u)\chi_2(1-u) = \chi_1\chi_2(t)J(\chi_1,\chi_2).$$

Подставляя в (4.51) вычисленные значения внутренних сумм, находим

$$\tau(\chi_1)\tau(\chi_2) = \sum_{t=1}^{q-1} \chi_1\chi_2(t)J(\chi_1,\chi_2)\zeta_q^t = J(\chi_1,\chi_2)\tau(\chi_1\chi_2).$$

□

Пусть $\chi = \chi_{p,q}$ определенный выше для любой пары простых чисел p, q с условием $p|q-1$ характер. Пусть также a, b целые числа, не делящиеся на p, и $\chi_1 = \chi^a, \chi_2 = \chi^b$. Определенные так характеры удовлетворяют условию $\chi_1^{p^k} = \chi_2^{p^k} = \chi_0$, т.е. их значения в любой точке принадлежат полю $\mathbb{Q}(\zeta_{p^k})$. Но тогда $J(\chi^a, \chi^b) \in \mathbb{Z}[\zeta_{p^k}]$ и все вычисления с суммами Якоби $J(\chi^a, \chi^b)$ можно проводить в сравнительно небольшом кольце $\mathbb{Z}[\zeta_{p^k}]$.

Заметим, что если $p \nmid ab(a+b)$, в этом случае p должно быть нечетным, равенство из леммы 4.9 может быть записано в виде

$$J(\chi^a, \chi^b) = \frac{\tau(\chi^a)\tau(\chi^b)}{\tau(\chi^{a+b})} = \tau(\chi)^{\sigma_a+\sigma_b-\sigma_{a+b}}. \tag{4.52}$$

Лемма 4.10. *Пусть a, b целые числа с условием $p \nmid ab(a+b)$. Определим элементы $\alpha, \beta \in \mathbb{Z}[G]$ равенствами*

$$\alpha = \sum_{\substack{1\leqslant x<p^k \\ p\nmid x}} \left[\frac{Nx}{p^k}\right]\sigma_x^{-1}, \quad \beta = \sum_{\substack{1\leqslant x<p^k \\ p\nmid x}} \left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right)\sigma_x^{-1}.$$

Тогда в кольце $\mathbb{Z}[G]$ имеем

$$(N\sigma_1 - \sigma_N)\beta = (\sigma_a + \sigma_b - \sigma_{a+b})\alpha.$$

Доказательство. Для каждого целого x, $1 \leqslant x < p^k$, не делящегося на p определим целое j с помощью условий $aj \equiv x \pmod{p^k}, 1 \leqslant j < p^k$. Так как a не делится на p, последнее сравнение разрешимо и $x = aj - p^k \left[\frac{aj}{p^k}\right]$. Если x пробегает все числа из промежутка $1 \leqslant x < p^k$, не делящиеся на p, то, очевидно, j пробегает все числа из того же множества. Для каждого x выполняется равенство $\sigma_a \sigma_j = \sigma_x$, так что $\sigma_a \sigma_x^{-1} = \sigma_j^{-1}$, а потому

$$\sigma_a \alpha = \sum_{\substack{1 \leqslant j < p^k \\ p \nmid j}} \left[\frac{Nx}{p^k}\right] \sigma_j^{-1} = \sum_{\substack{1 \leqslant j < p^k \\ p \nmid j}} \left(\left[\frac{Naj}{p^k}\right] - N\left[\frac{aj}{p^k}\right]\right) \sigma_j^{-1}.$$

Такое же равенство имеет место для σ_b, σ_{a+b}. Поэтому

$$(\sigma_a + \sigma_b - \sigma_{a+b})\alpha = \sum_{\substack{1 \leqslant j < p^k \\ p \nmid j}} \left(\left[\frac{Naj}{p^k}\right] + \left[\frac{Nbj}{p^k}\right] - \left[\frac{N(a+b)j}{p^k}\right]\right) \sigma_j^{-1} +$$
$$+ N \sum_{\substack{1 \leqslant j < p^k \\ p \nmid j}} \left(\left[\frac{(a+b)j}{p^k}\right] - \left[\frac{aj}{p^k}\right] - \left[\frac{bj}{p^k}\right]\right) \sigma_j^{-1}.$$

Из равенства $Nj = y + p^k \left[\frac{Nj}{p^k}\right]$ следует, что

$$\left[\frac{Naj}{p^k}\right] + \left[\frac{Nbj}{p^k}\right] - \left[\frac{N(a+b)j}{p^k}\right] = \left[\frac{ay}{p^k}\right] + \left[\frac{by}{p^k}\right] - \left[\frac{(a+b)y}{p^k}\right]$$

и это в силу равенства $\sigma_N \sigma_y^{-1} = \sigma_j^{-1}$ доказывает нужное утверждение. □

Итог этого параграфа подводит следующая теорема.

Теорема 4.8. *Пусть $\chi = \chi_{p,q}$ характер, определенный для некоторых нечетных простых чисел p, q с условием $p | q - 1$. Пусть a, b такие целые числа, что $p \nmid ab(a+b)$. Тогда для любого простого числа N, отличного от p и q, в кольце $\mathbb{Z}[\zeta_{p^k}]$ выполняется сравнение*

$$J(\chi^a, \chi^b)^\alpha \equiv \xi \pmod{N}, \tag{4.53}$$

где ξ — некоторый корень из единицы степени p^k.

Доказательство. Из равенств (4.52), сравнения (4.31) и леммы 4.10 следует

$$J(\chi^a, \chi^b)^\alpha = \tau(\chi)^{(\sigma_a+\sigma_b-\sigma_{a+b})\alpha} = \tau(\chi)^{(N\sigma_1-\sigma_N)\beta} \equiv \chi(N)^{-N\beta} \pmod N.$$

Учитывая, что число $\chi(N)$ и все его сопряженные есть корни из единицы степени p^k, получаем нужное утверждение. □

Рассмотрим пример. Пусть $p = 3, q = 7$. Если $\zeta = e^{2\pi i/3}$ кубический корень из 1 и 5 — первообразный корень по модулю 7, можно определить характер χ равенством

$$\chi(x) = \begin{cases} \zeta^u, & \text{если} \quad x \equiv 5^u \pmod 7, \\ 0, & \text{если} \quad x \equiv 0 \pmod 7. \end{cases}$$

При $a = b = 1$ находим сумму Якоби

$$J(\chi, \chi) = \sum_{x=1}^{6} \chi(x)\chi(1-x) = 3\zeta + 2.$$

Имеем $\sigma_2(3\zeta+2) = 3\zeta^2+2 = -3\zeta-1$. Поэтому сравнение из теоремы 4.8 принимает вид

$$(3\zeta+2)^{\left[\frac{n}{3}\right]}(-3\zeta-1)^{\left[\frac{2n}{3}\right]} \equiv \xi \pmod{N\mathbb{Z}[\zeta]},$$

где ζ некоторый кубический корень из 1.

Сравнение (4.53) есть аналог малой теоремы Ферма и может использоваться для отсеивания составных чисел. Если для некоторого N сравнение (4.53) нарушается, то N — составное число. Если же это сравнение выполняется для всех пар простых чисел p, q, с условием $q|s$, $p|q-1$, см. алгоритм, описанный в разделе 4.5, то при некоторых дополнительных ограничениях на числа a, b, ξ можно доказать, что все возможные делители числа N содержатся среди чисел, определенных в пункте 3 алгоритма.

4.6 Полиномиальный алгоритм проверки чисел на простоту.

Сравнительно недавно, в 2000 г., был найден детерминированный алгоритм полиномиальной сложности, позволяющий по заданному натуральному числу N сказать, будут оно простым или составным. Полному описанию этого алгоритма (основные его идеи были предложены индийскими математиками М. Агравалом, Н. Кайалом, Н. Саксеной), а также необходимых теоретических утверждений посвящен настоящий параграф. В отличие от оригинального алгоритма, который использовал вычисления в кольцах многочленов, мы используем здесь вычисления в полях, порожденных корнями из единицы.

В основе алгоритма лежит малая теорема Ферма, применяемая в кольце целых чисел $\mathbb{Z}[\zeta]$ кругового поля $\mathbb{Q}(\zeta)$, порожденного корнем из единицы $\zeta = e^{2\pi i/r}$ при некотором натуральном r. Напомним, что минимальный многочлен числа ζ есть $\Phi_r(x)$ — многочлен деления круга на r частей. Степень его равна $\varphi(r)$ и каждый элемент кольца $\mathbb{Z}[\zeta]$ единственным образом представляется в виде линейной комбинации чисел ζ^k, $0 \leqslant k < \varphi(r)$. Любые два элемента этого кольца сравнимы по модулю $N \in \mathbb{Z}$, если соответствующие целые коэффициенты в разложении этих чисел по указанному базису ζ^k сравнимы между собой по модулю N.

Алгоритм 4.4. *Дано нечетное число $N > 3$. Требуется определить, простое оно или составное.*

1. Проверить, равно ли N степени целого числа, т.е. выяснить, верно ли равенство $N = a^b$, $a, b \in \mathbb{Z}, b \geqslant 2$. Если верно, то N — составное число.

2. Перебирая последовательно все натуральные числа, найти наименьшее число r, для которого выполняется по крайней мере одно из условий

а) $(r, N) \neq 1$,

б) при всех k, $1 \leqslant k < \log^2 N$ имеем $r \nmid N^k - 1$.

3. Если $1 < (r, N) < N$, *то* N *составное.*

4. Если $(r, N) = N$, *то* N *простое.*

5. Положить $\zeta = \exp(\frac{2\pi i}{r})$, $T = \{1, 2, \ldots, [\sqrt{\varphi(r)}\log N]\}$ *и проверить выполнимость в кольце* $\mathbb{Z}[\zeta]$ *сравнений*

$$(\zeta + b)^N \equiv \zeta^N + b \pmod{N}, \quad \textit{при всех} \quad b \in T. \tag{4.54}$$

Если хотя бы одно из этих сравнений нарушается, то N *— составное. Если же все сравнения выполнены, то* N *— простое число.*

В описании алгоритма и далее в этом параграфе $\log x$ обозначает логарифм числа x по основанию 2.

Проверим сначала, что алгоритм работает корректно. Если он завершает свою работу в пунктах 1 или 3, то, очевидно, его ответ верен.

Если алгоритм завершил свою работу в пункте 4, то, согласно определению числа r, для каждого $k, 1 \leqslant k < r$, выполняется равенство $(k, N) = 1$. Но тогда $N \geqslant r$ и, поскольку $N|r$, заключаем, что $r = N$ — простое число. И в этом случае алгоритм дает правильный ответ.

Допустим теперь, что алгоритм завершил работу в пункте 5. Предположим, что N — простое число. В этом случае все биномиальные коэффициенты $\binom{N}{k}$ при $1 < k < N$ делятся на N, так что при любом $b \in \mathbb{Z}$ выполняется сравнение

$$(\zeta + b)^N \equiv \zeta^N + b^N \equiv \zeta^N + b \pmod{N}.$$

Значит, если хотя бы одно из сравнений (4.54) нарушается, можно утверждать, что N не простое, т.е. составное, число. Ответ алгоритма в этом случае верен.

Осталось доказать, что если алгоритм дошел до пункта 5 и все сравнения этого пункта верны, то число N действительно простое. Это доказательство основано на следующей теореме.

Теорема 4.9. *Пусть* $N > 3, r > 1$ *— целые взаимно простые числа,* N *не имеет простых делителей, меньших* $t = [\sqrt{\varphi(r)}\log N] + 1$, *и порядок* N *в мультипликативной группе* $(\mathbb{Z}/r\mathbb{Z})^*$ *не меньше, чем*

$\log^2 N$. *Пусть также* $\zeta = \exp(\frac{2\pi i}{r})$ *и при любом* $b \in \mathbb{Z}, 0 \leqslant b < t$, *в кольце* $\mathbb{Z}[\zeta]$ *выполняется сравнение*

$$(\zeta + b)^N \equiv \zeta^N + b \pmod{N}. \tag{4.55}$$

Тогда N *имеет единственный простой делитель.*

Докажем справедливость последнего утверждения из пункта 5 алгоритма. Так как алгоритм прошел пункты 3, 4 и не остановился, то имеем $(r, N) = 1$. Согласно определению r в пункте 2 алгоритма можно утверждать, что $\operatorname{ord}_r N$ — порядок элемента N в мультипликативной группе $(\mathbb{Z}/r\mathbb{Z})^*$ удовлетворяет неравенству $\operatorname{ord}_r N \geqslant \log^2 N$. Из того же определения следует, что N не имеет простых делителей меньших r. Поскольку $r > \varphi(r) \geqslant \operatorname{ord}_r N \geqslant \log^2 N$, то $r \geqslant \sqrt{r}\log N > \sqrt{\varphi(r)}\log N$ и $r \geqslant t = [\sqrt{\varphi(r)}\log N] + 1$. Таким образом, справедливость сравнений (4.54) означает, что выполнены все условия теоремы 4.9, и по этой теореме N имеет единственный простой делитель. Так как алгоритм прошел пункт 1, можно утверждать, что N — простое число.

Далее следует доказательство теоремы 4.9.

Пусть p — некоторый простой делитель числа N и $\mathfrak{p}$ — какой-либо простой идеал кольца $\mathbb{Z}[\zeta]$, лежащий над p.

Покажем сначала, что все числа $1, \zeta, \zeta^2, \ldots, \zeta^{r-1}$ лежат в различных классах вычетов кольца $\mathbb{Z}[\zeta]$ по модулю $\mathfrak{p}$. Предположим, что при некоторых целых k, ℓ с условиями $0 \leqslant \ell < k < r$ выполняется сравнение $\zeta^k \equiv \zeta^\ell \pmod{\mathfrak{p}}$. Умножив это сравнение на $\zeta^{-\ell} = \zeta^{r-\ell}$, приходим к сравнению $\zeta^s \equiv 1 \pmod{\mathfrak{p}}$, где $s = k - \ell$, которое также можно переписать в виде включения $1 - \zeta^s \in \mathfrak{p}$. Справедливо тождество

$$1 + x + \ldots + x^{r-1} = \frac{x^r - 1}{x - 1} = \prod_{j=1}^{r-1}(x - \zeta^j).$$

Подставляя в него 1 вместо переменной x найдем

$$r = \prod_{j=1}^{r-1}(1-\zeta^j). \tag{4.56}$$

Так как $1 \leqslant s < r$ и $1-\zeta^s \in \mathfrak{p}$, то из равенства (4.56) следует $r \in \mathfrak{p}$ или $p|r$. Последняя делимость противоречит взаимной простоте r и N. Итак, все классы вычетов $\zeta^k \pmod{\mathfrak{p}}$ различны.

В дальнейшем для краткости буквой S будет обозначаться совокупность всех целых чисел b, удовлетворяющих неравенствам $0 \leqslant b < t$. Предположим, что для некоторого $b \in S$ выполняется включение $\zeta + b \in \mathfrak{p}$. Согласно условию теоремы имеем сравнение

$$(\zeta+b)^N \equiv \zeta^N + b \pmod{p}$$

и, следовательно,

$$(\zeta+b)^N \equiv \zeta^N + b \pmod{\mathfrak{p}}.$$

Но тогда $\zeta^N + b \in \mathfrak{p}$ и $\zeta^N - \zeta \in \mathfrak{p}$. Таким образом, $\zeta^{N-1} \equiv 1 \pmod{\mathfrak{p}}$. Обозначим буквой s остаток от деления числа $N-1$ на r, $0 \leqslant s < r$. Учитывая, что $\zeta^r = 1$, находим $\zeta^s \equiv 1 \pmod{\mathfrak{p}}$. По доказанному ранее это возможно лишь при $s = 0$, т.е. при $r|(N-1)$. Последняя делимость означает, что порядок N в мультипликативной группе классов вычетов $(\mathbb{Z}/r\mathbb{Z})^*$ равен 1, вопреки условию теоремы. Итак $\zeta + b \notin \mathfrak{p}$ при каждом $b \in S$.

Пусть $K = \mathbb{Z}[\zeta]/\mathfrak{p}$ — поле вычетов идеала $\mathfrak{p}$, K^* — мультипликативная группа, состоящая из ненулевых элементов K. Буквой Γ обозначим мультипликативную подгруппу K^*, порожденную элементами $(\zeta + b) \pmod{\mathfrak{p}}$ для всех $b \in S$. В дальнейшем, предположив, что N имеет по крайней мере два различных простых делителя, мы оценим сверху и снизу $|\Gamma|$ — количество элементов в группе Γ. Эти оценки будут противоречить друг другу, что и завершит доказательство теоремы 4.9.

Обозначим буквой I совокупность целых неотрицательных чисел v, взаимно простых с r и удовлетворяющих условию

$$(\zeta + b)^v \equiv \zeta^v + b \pmod{p} \quad \text{для любого} \quad b \in S. \tag{4.57}$$

Справедливы включения

$$N \in I, \qquad p \in I. \tag{4.58}$$

Первое из них выполняется в силу сравнения (4.54), а второе — поскольку все биномиальные коэффициенты $\binom{p}{k}$, $0 < k < p$, делятся на p.

Лемма 4.11. *Пусть v, u — натуральные числа, взаимно простые с r.*

1. *Если $v, u \in I$, то $vu \in I$.*
2. *Если $v \in I, vu \in I$, то $u \in I$.*

Доказательство. В доказательстве этой леммы и далее мы будем применять обозначение σ_k для автоморфизма поля $\mathbb{Q}(\zeta)$, переводящего число ζ в ζ^k. Пусть b — произвольный элемент множества S.

1. Применяя к сравнению (4.57) автоморфизм σ_u, находим

$$(\zeta^u + b)^v \equiv \zeta^{vu} + b \pmod{p} \quad \text{для любого} \quad b \in S.$$

Поскольку $u \in I$, это сравнение приводит к

$$(\zeta + b)^{vu} \equiv (\zeta^u + b)^v \equiv \zeta^{vu} + b \pmod{p}.$$

Это доказывает первое утверждение леммы.

2. Определим натуральное число k так, чтобы выполнялось сравнение $vk \equiv 1 \pmod{r}$. Применяя к сравнениям

$$(\zeta + b)^v \equiv \zeta^v + b \pmod{p}, \quad (\zeta + b)^{vu} \equiv \zeta^{vu} + b \pmod{p}$$

автоморфизм σ_k, находим

$$(\zeta^k + b)^v \equiv \zeta^{vk} + b = \zeta + b \pmod{p},$$
$$(\zeta^k + b)^{vu} \equiv \zeta^{vuk} + b = \zeta^u + b \pmod{p}.$$

Возводя первое из сравнений в степень u и применяя затем второе сравнение, приходим ко второму утверждению леммы. □

Теперь мы займемся нижней оценкой для $|\Gamma|$. Рассмотрим для этого $H = \langle N, p\rangle$ подгруппу группы $(\mathbb{Z}/r\mathbb{Z})^*$, порожденную классами вычетов чисел N и p, порядок ее $|H|$ для краткости обозначим буквой q.

Лемма 4.12. *Справедливо неравенство*

$$|\Gamma| \geqslant \binom{t+q-1}{t}.$$

Доказательство. Обозначим буквой $\mathcal{G}$ совокупность многочленов

$$g(x) = \prod_{j\in S}(x+j)^{k_j} \in \mathbb{Z}[x],$$

с условиями

$$k_j \geqslant 0, \qquad \sum_{j\in S} k_j \leqslant q-1. \tag{4.59}$$

Количество многочленов в множестве $\mathcal{G}$ равно количеству различных наборов показателей $\{k_j, j \in S\}$, с условиями (4.59), т.е.

$$|\mathcal{G}| = \binom{t+q-1}{t}.$$

Рассмотрим теперь отображение $\mathcal{G} \longmapsto \Gamma$, определенное следующим образом

$$g(x) \longmapsto g(\zeta) \pmod{\mathfrak{p}}. \tag{4.60}$$

Докажем, что это отображение является вложением.

Допустим, что $g(x)$ и $e(x)$ принадлежат множеству $\mathcal{G}$, различны и имеют одинаковые образы при отображении (4.60). Это равносильно сравнению

$$g(\zeta) \equiv e(\zeta) \pmod{\mathfrak{p}}. \tag{4.61}$$

В силу (4.57) при любом $v \in I$ получаем

$$g(\zeta^v) \equiv g(\zeta)^v \equiv e(\zeta)^v \equiv e(\zeta^v) \pmod{\mathfrak{p}},$$

и это сравнение означает, что в поле K многочлен

$$f(x) = g(x) - e(x) \pmod{p} \in F_p[x]$$

имеет корнями все элементы $\zeta^v \pmod{\mathfrak{p}}, v \in I$.

Согласно условию теоремы, многочлены $x + b, b \in S$, при переходе в кольцо $F_p[x]$ остаются различными и неприводимыми. В силу единственности разложения на неприводимые сомножители в $F_p[x]$ получаем, что $f(x) \not\equiv 0$.

Степень многочлена $f(x)$ не превосходит $q - 1$, значит, и количество его корней в поле K не превосходит $q - 1$. Все элементы $\zeta^v \pmod{\mathfrak{p}}, v \in I$ являются корнями $f(x)$. Сравнение $\zeta^u \equiv \zeta^v \pmod{\mathfrak{p}}$ при некоторых $u, v \in I$, по доказанному ранее возможно лишь в случае $u \equiv v \pmod{r}$. Таким образом, количество корней многочлена $f(x)$ в поле K не меньше $|H| = q$. Получившееся противоречие доказывает, что отображение (4.60) является вложением. Это в силу неравенства

$$|\Gamma| \geqslant |\mathcal{G}| = \binom{t+q-1}{t}$$

завершает доказательство леммы 4.12. □

Теперь перейдем к оценке $|\Gamma|$ сверху. Из (4.58) и леммы 4.11 следует

$$N/p \in I, \quad (N/p)^i p^j \in I, \quad \text{при любых} \quad i, j \in \mathbb{Z}_{\geqslant 0}. \tag{4.62}$$

Лемма 4.13. *Если N имеет по крайней мере два различных простых делителя, то*

$$|\Gamma| \leqslant N^{\sqrt{q}} - 1.$$

Доказательство. Если для каких-либо различных пар целых чисел (i, j) и (k, ℓ) выполняется равенство $N^i p^j = N^k p^\ell$, то N есть степень p, вопреки условию леммы. Следовательно, все произведения $(N/p)^i p^j \in I$ с условиями $0 \leqslant i \leqslant [\sqrt{q}]$, $0 \leqslant j \leqslant [\sqrt{q}]$ различны. Их количество $(1+[\sqrt{q}])(1+[\sqrt{q}]) > q$. Классы вычетов этих произведений по модулю r лежат в группе $H = \langle N, p \rangle$ порядка q. Значит, среди них есть два

произведения v и u такие, что $v \equiv u \pmod r$. Не уменьшая общности можно считать, что $v > u$. Тогда

$$1 \leqslant u < v = (N/p)^i p^j \leqslant (N/p)^{\sqrt{q}} \cdot p^{\sqrt{q}} = N^{\sqrt{q}}.$$

Согласно определению множества I при любом $b \in S$ имеем сравнение по модулю p

$$(\zeta + b)^v \equiv \zeta^v + b = \zeta^u + b \equiv (\zeta + b)^u.$$

Учитывая, что по доказанному ранее $\zeta + b \notin \mathfrak{p}$, заключаем

$$(\zeta + b)^{v-u} \equiv 1 \pmod{\mathfrak{p}}.$$

Отсюда же следует, что каждый элемент группы $\Gamma \subset K^*$ является корнем многочлена $x^{v-u} - 1$. Так что

$$|\Gamma| \leqslant v - u \leqslant N^{\sqrt{q}} - 1.$$

Это завершает доказательство леммы. □

Для завершения доказательства теоремы 4.9 осталось проверить, что оценки лемм 4.12 и 4.13 противоречат друг другу.

При любых действительных числах a, b, удовлетворяющих $b \geqslant a > 0$, имеем

$$\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} = \int_0^1 x^{a-1}(1-x)^{b-1}dx \leqslant \int_0^1 x^{a-1}(1-x)^{a-1}dx \leqslant \frac{1}{4^{a-1}}.$$

Положим $a = \sqrt{q}\log N$ и $b = q$. Так как $N \pmod r \in H$, то согласно условию теоремы имеем $|H| \geqslant \log^2 N$ и

$$b = q = |H| \geqslant a = \sqrt{q}\log N.$$

Из определения t находим также $t > \sqrt{\varphi(r)}\log N \geqslant a$. Отсюда следует

$$\begin{aligned}\binom{t+q-1}{t} =& \frac{(t+1)\cdots(t+q-1)}{(q-1)!} > \frac{(a+1)\cdots(a+q-1)}{(q-1)!} = \\ =& \frac{\Gamma(a+q)}{a\Gamma(a)\Gamma(q)} \geqslant 4^{a-1}/a \geqslant 2^a = N^{\sqrt{q}}.\end{aligned}$$

Доказанное неравенство приводит в противоречие утверждения лемм 4.12 и 4.13. Значит, условие леммы 4.12 не выполняется и N имеет единственный простой делитель. Это завершает доказательство теоремы 4.9 и обоснование корректности алгоритма 4.4.

Перейдем теперь к оценке сложности алгоритма 4.4 и докажем его полиномиальность. Для этого прежде всего необходимо оценить число r, определенное в пункте 2 алгоритма. Докажем, что оно не очень велико, а именно, при всех достаточно больших N выполнено неравенство $r \leqslant M = [\log^5 N]$. Предположим противное. Тогда $r > M$ и согласно определению r для каждого целого числа $m \leqslant M$ нарушаются оба условия пункта 2 алгоритма, т.е. m взаимно просто с N и при некотором $k < \log^2 N$ число $N^k - 1$ делится на m. Но тогда и произведение

$$Q = \prod_{k<\log^2 N} (N^k - 1)$$

делится на m. Обозначим буквой P наименьшее общее кратное всех целых чисел m, $2 \leqslant m \leqslant M$. Так как Q делится на каждое целое число m из промежутка $2 \leqslant m \leqslant M$, то $P \leqslant Q$ и

$$\log P \leqslant \log Q = \sum_{k<\log^2 N} \log(N^k - 1) \leqslant \log N \sum_{k<\log^2 N} k \sim \frac{1}{2}\log^5 N \tag{4.63}$$

при $N \to \infty$. Но согласно асимптотическому закону распределения простых чисел $\ln P \sim M$ при $M \to \infty$. Так что $\log P = \frac{\ln P}{\ln 2} \sim \frac{\log^5 N}{\ln 2}$. Учитывая, что $0 < \ln 2 < 1$ приходим к противоречию с (4.63). Следовательно $r \leqslant \log^5 N$.

Оценим количество арифметических операций, нужных для выполнения первого пункта алгоритма. Из равенства $N = a^b$, выполняющегося с целыми $a \geqslant 2, b \geqslant 2$ следует $N \geqslant 2^b$ и $b \leqslant \log N$, а также $N \geqslant a^2$ и $a \leqslant \sqrt{N}$. При каждом фиксированном целом $b, 2 \leqslant b \leqslant \log N$ необходимо выяснить, имеет ли уравнение $x^b = N$ целый корень. Это можно сделать, затратив $O(\log^2 N)$ арифметических

операций. Например, можно с помощью деления пополам построить последовательность укорачивающихся вдвое отрезков, содержащих упомянутый выше корень. Остановиться при этом следует, как только длина отрезка станет меньше 1. Такой отрезок содержит не более одного целого числа, и проверка, удовлетворяет оно уравнению $x^b = N$ или нет, требует $O(\log N)$ арифметических операций. Выполнение первого пункта алгоритма потребует таким образом $O(\log^3 N)$ арифметических операций.

Вычисляя последовательно $N^\ell \pmod k$ при $1 \leqslant \ell \leqslant [\log^2 N]$, можно за $\widetilde{O}(\log^2 N)$ арифметических операций установить, будет порядок N по модулю k превышать $\log^2 N$ или нет. Здесь и далее символом $\widetilde{O}(m)$ обозначаются величины имеющие порядок роста $O(m \log^c m)$ при некоторой положительной постоянной c. Из доказанной выше оценки для числа r следует, что перебирая последовательно целые числа $k = 2, 3, \ldots$ и вычисляя порядок, можно найти нужное число r, выполнив $\widetilde{O}(r \log^2 N) = \widetilde{O}(\log^7 N)$ арифметических операций. Заметим, что вычисление (k, N) в пункте 2 алгоритма требует меньшего количества операций.

Пункты 3 и 4 алгоритма не требуют дополнительных вычислений, так как величина (r, N) уже найдена на предыдущем шаге.

Последний пункт требует наибольшего количества арифметических операций. Прежде всего нужно иметь в виду, что каждый элемент кольца $\mathbb{Z}[\zeta]$ представляется вектором коэффициентов в разложении по степеням ζ, имеющим длину $\varphi(r) = O(r)$. Так что каждое умножение двух элементов кольца $\mathbb{Z}[\zeta]$ по модулю N потребует выполнения $O(r^2)$ арифметических операций с элементами кольца $\mathbb{Z}/N\mathbb{Z}$. Операцию умножения в кольце $\mathbb{Z}[\zeta]/N\mathbb{Z}[\zeta]$ можно ускорить, если воспользоваться быстрым преобразованием Фурье, см. раздел 2.7.2. В этом случае количество арифметических операций сократится до $\widetilde{O}(r)$. Если учесть, что для проверки одного из сравнений (4.55) потребуется $O(\log N)$ таких умножений, и количество таких сравнений равно $[\varphi(r)^{1/2} \log N] = O(r^{1/2} \log N)$, то общее количество арифметических операций с элементами кольца $\mathbb{Z}[\zeta]/N\mathbb{Z}[\zeta]$ будет иметь

величину $\widetilde{O}(r^{1/2}\log^2 N)$. Значит, выполнение последнего пункта алгоритма 4.4 потребует $\widetilde{O}(r^{3/2}\log^2 N)$ арифметических операций в кольце $\mathbb{Z}/N\mathbb{Z}$, т.е. $\widetilde{O}(r^{3/2}\log^3 N) = \widetilde{O}(\log^{10{,}5} N)$ битовых операций. Такую же оценку имеет и общая трудоемкость алгоритма. Он имеет полиномиальную сложность.

Заметим, что условие минимальности r из пункта 2 алгоритма не используется ни в его работе, ни в обосновании его корректности. Оно необходимо лишь для оценки величины r. Существенными для работы алгоритма являются условия

$$(r, N) = 1, \qquad \operatorname{ord}_r N \geqslant \log^2 N. \tag{4.64}$$

Для многих чисел N можно найти значительно меньшие, чем $\log^5 N$ значения r, удовлетворяющие (4.64). Для этих N алгоритм будет иметь лучшие оценки сложности. Например, если $k = \nu_2(N^2-1) \geqslant 1$ — кратность, с которой 2 входит в разложение N^2-1 на простые сомножители, то при любом $j \geqslant 1$ справедливо равенство $N^{2^j} = 1+\gamma\cdot 2^{k-1+j}$, где γ — целое нечетное число. Это утверждение легко доказать с помощью индукции по j. Из него нетрудно вывести, что при любом $d \geqslant k$ порядок N в мультипликативной группе вычетов по модулю 2^d равен 2^{d+1-k}. В частности, выбрав $r = 2^{k+[2\log\log N]}$, получим, что $\operatorname{ord}_r(N) = 2^{1+[2\log\log N]} > \log^2 N$ и $r \leqslant 2^{k+2\log\log N} = 2^k\log^2 N$. Например, если $N \equiv \pm 3 \pmod 8$, имеем $k = 3$ и $r \leqslant 8\log^2 N$. Таким образом, для половины нечетных чисел N указанным способом получается нужное число r с оценкой $r \leqslant 8\log^2 N$. Для них алгоритм будет иметь сложность $\widetilde{O}(\log^6 N)$ битовых операций.

Подобное рассуждение можно выполнить заменив 2 каким-либо другим простым числом, не делящим N.

Существенным недостатком этого алгоритма, не позволяющим использовать его на практике, является потребность очень большой памяти. Как уже указывалось, каждый элемент кольца $\mathbb{Z}[\zeta]$ представляется вектором длины $O(\log^5 N)$, компоненты которого есть целые числа, записываемые $O(\log N)$ двоичными цифрами. Значит, необходимая для работы алгоритма память оценивается величиной $O(\log^6 N)$

бит, что при больших N намного превосходит память, требующуюся алгоритму Коэна–Ленстры.

Глава 5

Разложение целых чисел на множители

В этой главе будут рассматриваться методы разложения целых чисел на простые сомножители, т.е. методы поиска для заданного целого $N > 1$ простых чисел $p_1, \ldots, p_r$ таких, что

$$N = p_1^{k_1} \cdots p_r^{k_r}, \qquad k_j \geqslant 1,\ k_j \in \mathbb{Z}.$$

При этом будет предполагаться, что разлагаемое число N составное, в чем можно убедиться с помощью тестов из параграфа 2.6.

Достаточно уметь решать более простую задачу о разложении целого числа на два меньших множителя, т.е. задачу о решении в целых числах $a > 1, b > 1$ уравнения $N = ab$. Действительно, в этом случае выполняются неравенства $a < N, b < N$, можно разложить на два меньших множителя каждое из чисел a, b, и продолжать далее эту процедуру, пока такое разложение будет возможным, т.е. до тех пор, пока все сомножители не станут простыми.

Существующие алгоритмы разложения чисел на множители могут быть распределены на группы в зависимости от количества арифметических операций, которые алгоритм требует для своей работы.

1) *Алгоритмы экспоненциальной сложности* используют $O(N^c)$ арифметических операций. Здесь c — положительная постоянная.

2) *Алгоритмы субэкспоненциальной сложности* требуют для своей работы $O(e^{c(\ln N)^\alpha (\ln \ln N)^\beta})$ арифметических операций. Здесь α, β, c

— положительные постоянные, $\alpha + \beta = 1$. Заметим, что при $\alpha = 1$, т.е. $\beta = 0$, оценка совпадает с оценкой сложности экспоненциальных алгоритмов.

Для наиболее быстрого из субэкспоненциальных алгоритмов, так называемого *метода решета числового поля*, имеем $\alpha = \frac{1}{3}, \beta = \frac{2}{3}$.

Алгоритмы полиномиальной сложности, $\alpha = 0, \beta = 1$, для задачи факторизации не известны, и весьма вероятно, что их не существует.

Деятельность по разложению чисел на множители сочетает в себе черты инженерной науки, поскольку во многом опирается на допущения, основанные на опыте и не имеющие теоретических обоснований, а с другой стороны она сродни искусству, так как зачастую продолжительность работы алгоритма и результат зависят от удачного выбора параметров.

5.1 Алгоритмы экспоненциальной сложности.

5.1.1 Алгоритм пробных делений.

Пусть $d_1 < d_2 < \ldots$ — последовательность целых чисел, содержащая все простые числа. Алгоритм пробных делений состоит в последовательном делении N на числа $d_1, d_2, \ldots$, не превосходящие $\sqrt{N}$. Если N составное число, то оно имеет простой делитель $p \leqslant \sqrt{N}$ и потому будет разложено на множители.

Этот алгоритм часто используется для нахождения всех простых делителей числа N, не превосходящих некоторой заданной границы B.

Последовательность d_i может совпадать с множеством простых чисел. Но в этом случае необходим алгоритм, строящий все простые числа до заданной границы. Иногда бывает проще использовать последовательности, содержащие и составные числа, но менее сложные в реализации.

Пример. Каждое простое число $p > 6$ удовлетворяет одному из двух сравнений $p \equiv 1 \pmod 6$ или $p \equiv 5 \pmod 6$. Поэтому после-

довательность $2, 3, 5, 7, 11, 13, 17, 19, 23, 25, \ldots$, содержащая все числа вида $6n \pm 1, n \in \mathbb{N}$, включает в себя и все простые числа. Правило порождения этой последовательности имеет вид

$$d_1 = 2,\ d_2 = 3,\ d_3 = 5, \quad d_{2k} = d_{2k-1} + 2, \quad d_{2k+1} = d_{2k} + 4, \quad k \geqslant 2.$$

При таком выборе d_i алгоритм требует $O(N^{1/2})$ арифметических операций и $O(1)$ памяти.

В качестве модуля в сравнениях вместо 6 можно взять число $m = 2 \cdot 3 \cdot 5 = 30$. Все простые числа $p > 5$ будут содержаться в восьми прогрессиях с разностью 30, начинающихся с чисел $1, 7, 11, 13, 17, 19, 23, 29$. Соответствующая последовательность d_i будет содержать меньшую долю составных чисел. Если $m = \prod_{p \leqslant r} p$, то количество арифметических прогрессий, составляющих эту последовательность равно $\varphi(m)$, а доля чисел из $\{d_i\}$ в натуральном ряде есть $\dfrac{\varphi(m)}{m} = \prod_{p \leqslant r} \left(1 - \dfrac{1}{p}\right)$. При $m = 6$ она равна $\dfrac{1}{3}$.

5.1.2 Алгоритм Ферма.

Если N нечетно и $N = ab, a \geqslant b$, то при $x = \frac{a+b}{2}$, $y = \frac{a-b}{2}$ имеем

$$x^2 - y^2 = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = ab = N.$$

И наоборот, любое решение уравнения $x^2 - y^2 = N$ в силу равенства $N = (x+y)(x-y)$ дает разложение N на множители. Получившееся разложение будет тривиальным лишь в том случае, если $x - y = 1$ или, что то же самое, $x + y = N$. Таким образом, задача разложения чисел на множители эквивалентна поиску решений уравнения $x^2 - y^2 = N$. Далее будем считать, что N не есть квадрат целого числа.

Положим $z_k = k^2 - N, k \geqslant [\sqrt{N}] + 1$. Если при каком-то k имеем $z_k = y^2, y \in \mathbb{Z}$, то $k^2 - N = y^2$ и $N = k^2 - y^2 = (k-y)(k+y)$. Для вычисления z_k заметим, что

$$z_{k+1} - z_k = (k+1)^2 - k^2 = 2k + 1,$$

т.е. $z_{k+1} = z_k + 2k + 1$. Следующий алгоритм построен на этих соотношениях.

Алгоритм 5.1. *Дано нечетное натуральное число N. Требуется найти целые числа $a \geqslant b > 1$ такие, что $N = ab$.*

1. Вычислить $k = [\sqrt{N}]$ и $z = k^2 - N$.

2. Если $z = y^2$ при $y \in \mathbb{Z}, y \geqslant 0$, то положить $a = k+y, b = k-y$. Алгоритм останавливается, нужное разложение на множители найдено.

3. Положить $z = z + 2k + 1, k = k + 1$ и перейти в пункт 2 алгоритма.

Пусть $N = ab$, $a > b$. Алгоритм закончит работу, когда параметр k достигнет величины $\dfrac{a+b}{2}$. Количество шагов алгоритма оценивается величиной

$$\frac{a+b}{2} - \sqrt{N} = \frac{a+b-2\sqrt{ab}}{2} = \frac{(\sqrt{a}-\sqrt{b})^2}{2},$$

т.е. чем ближе друг к другу делители числа N, тем быстрее алгоритм закончит работу.

Иногда поэтому удобнее применять алгоритм Ферма к числу kN вместо N, выбрав каким-либо способом нечетное число k. Так, если $N = pq$, где p, q — простые числа и $\dfrac{q}{p} \sim k > 1$, то число $kN = q \cdot (kp)$ разлагается на два примерно равные по величине множителя.

Например, для разложения на два меньших множителя числа 7493 потребуется восемь шагов алгоритма Ферма, пока не будет найдено число $z = 1156 = 34^2$ и соответствующее разложение $7493 = 59 \cdot 127$. А если раскладывать таким способом число $22479 = 3 \cdot 7459$, уже на четвертом шаге будет найдено число $z = 625 = 25^2$ и получено разложение $22479 = 177 \cdot 127 = 3 \cdot 59 \cdot 127$.

5.1.3 Алгоритм Лемана.

В основе алгоритма лежит следующая теорема.

Теорема 5.1. *Пусть $N \geqslant 15$ — составное число, все простые делители которого больше $N^{1/3}$. Тогда существуют целые числа k, a, b такие, что*

$$4kN = a^2 - b^2 \tag{5.1}$$

$$0 < k < N^{1/3}, \qquad 0 < a < \sqrt{4kN} + \frac{N^{1/6}}{4\sqrt{k}}, \qquad 0 \leqslant b. \tag{5.2}$$

Следствие 5.1. *Если в условиях теоремы числа k, a, b удовлетворяют условиям (5.1), (5.2), то выполняется неравенство*

$$a + b < N.$$

Для доказательства следствия заметим, что из (5.1) и (5.2) следует

$$b^2 = a^2 - 4kN < \left(\sqrt{4kN} + \frac{N^{1/6}}{4\sqrt{k}}\right)^2 - 4kN = N^{2/3} + \frac{N^{1/3}}{16k} <$$
$$< \left(N^{1/3} + \frac{1}{32}\right)^2, \quad \text{то есть} \quad b < N^{1/3} + \frac{1}{32}.$$

Поэтому

$$a + b < \sqrt{4kN} + \frac{N^{1/6}}{4\sqrt{k}} + N^{1/3} + \frac{1}{32} < 2N^{2/3} + \frac{1}{4} + N^{1/3} + \frac{1}{32} < N.$$

Здесь использовано, что максимум выражения $\sqrt{4kN} + \dfrac{N^{1/6}}{4\sqrt{k}}$, где $1 \leqslant k \leqslant N^{1/3}$, достигается при $k = N^{1/3}$, а последнее неравенство выполнено при $N \geqslant 15$.

Теперь опишем алгоритм Лемана, теорема 5.1 будет доказана позже.

Алгоритм 5.2. Дано: *нечетное составное N.* Найти: *целые числа, $u > 1, v > 1$ такие, что $N = uv$*

1. Разделить N последовательно на все целые числа $d, 2 \leqslant d \leqslant [N^{1/3}]$. Если при этом найдется делитель, то N разложится на два множителя.

2. Для каждого $k = 1, 2, \ldots, [N^{1/3}]$ *и каждого* $\ell = 0, 1, 2, \ldots, \left[\dfrac{N^{1/6}}{4\sqrt{k}}\right] + 1$ *проверить, будет ли число*

$$\left(\left[\sqrt{4kN}\right] + \ell\right)^2 - 4kN = b^2 \tag{5.3}$$

квадратом целого числа.

3. Если равенство (5.3) выполняется с целым $b \geqslant 0$*, то вычислить*

$$u = \left(\left[\sqrt{4kN}\right] + \ell + b,\ N\right), \qquad v = \frac{N}{u}.$$

Алгоритм завершает свою работу. Числа u, v *найденные в п.3, дают нетривиальное разложение* N *на множители.*

Объясним почему алгоритм 5.2 действительно разложит N на нетривиальные множители. Если число N прошло пункт 1 алгоритма и не было разложено на меньшие множители, то все его простые делители больше $N^{1/3}$.

Пусть k, a, b — числа, существование которых следует из теоремы 5.1. Определим

$$\ell = a - [\sqrt{4kN}].$$

Тогда

$$0 \leqslant \ell < \sqrt{4kN} + \frac{N^{1/6}}{4\sqrt{k}} - [\sqrt{4kN}] < \frac{N^{1/6}}{4\sqrt{k}} + 1.$$

Это доказывает существование пары чисел k, ℓ, при которых в пункте 2 алгоритма будет найдено равенство (5.3) с целым неотрицательным b.

Из (5.3) следует, что

$$a^2 - b^2 \equiv 0 \pmod{N},$$

т.е. $N|(a-b)(a+b)$. Здесь $a = [\sqrt{4kN}] + \ell$. По следствию из теоремы

$$0 < a - b \leqslant a + b < N.$$

Поэтому $u = (a + b, N)$ удовлетворяет неравенствам $1 < u < N$, и алгоритм найдет нетривиальное разложение N на множители.

Справедливы равенства

$$\sum_{k=1}^{[N^{1/3}]} \left(\left[\frac{N^{1/6}}{4\sqrt{k}} \right] + 2 \right) = O\left(N^{1/6} \sum_{k=1}^{[N^{1/3}]} \frac{1}{\sqrt{k}} + N^{1/3} \right) =$$

$$= O\left(N^{1/6} \cdot N^{1/6} + N^{1/3} \right) = O\left(N^{1/3} \right).$$

Из них следует, что равенство (5.3) будет проверяться $O\left(N^{1/3}\right)$ раз и, значит, алгоритму 5.2 требуется $O\left(N^{1/3} \ln N\right)$ арифметических операций для разложения числа N на множители.

Перейдем к доказательству теоремы 5.1 и установим сначала вспомогательное утверждение.

Лемма 5.1. *Пусть в условиях теоремы 5.1 имеет место разложение на множители $N = uv$, причем $N^{1/3} < u \leqslant v < N^{2/3}$. Тогда существуют натуральные числа r и s, такие, что*

$$rs < N^{1/3}, \qquad |ur - vs| < N^{1/3}.$$

Доказательство. Если $u = v$, положим $r = s = 1$. Нужные неравенства, очевидно, выполняются. Далее будем считать, что $u < v$. Так как в условиях леммы число N не может быть произведением более двух простых сомножителей, заключаем, что u, v — различные простые числа. В частности, дробь $\alpha = \frac{v}{u} > 1$ несократима.

Далее для доказательства леммы понадобятся некоторые свойства цепных дробей. Пусть $\alpha = [a_0; a_1, a_2, \ldots, a_n]$ — разложение в цепную дробь, $a_j \geqslant 1$ при $j \geqslant 0$. Числители и знаменатели подходящих дробей числа α положительны и образуют возрастающие последовательности. Пусть m — наибольший номер подходящей дроби числа α, для которой выполнено неравенство $P_m Q_m < N^{1/3}$. Заметим, что $\frac{P_m}{Q_m} \neq \alpha$, так как дробь $\alpha = \frac{u}{v}$ несократима и $Q_m < N^{1/3} < v$. В частности, это влечет неравенство $m < n$.

Положим $r = P_m, s = Q_m$. Тогда

$$rs = P_m Q_m < N^{1/3}.$$

Заметим, что $\alpha^{-1} = \dfrac{u}{v} < 1$, и цепная дробь этого числа равна

$$\alpha^{-1} = [0; a_0, a_1, \ldots, a_n].$$

Отсюда следует, что последовательность подходящих дробей числа α^{-1} имеет вид $0, \dfrac{Q_0}{P_0}, \dfrac{Q_1}{P_1}, \ldots$. Применяя теперь неравенство (1.28) к подходящим дробям чисел α и α^{-1}, находим

$$\left|\frac{v}{u} - \frac{P_m}{Q_m}\right| < \frac{1}{Q_m Q_{m+1}}, \qquad \left|\frac{u}{v} - \frac{Q_m}{P_m}\right| < \frac{1}{P_m P_{m+1}}.$$

Эти неравенства могут быть переписаны в виде

$$\left|\frac{v}{u} - \frac{r}{s}\right| < \frac{1}{sQ_{m+1}}, \qquad \left|\frac{u}{v} - \frac{s}{r}\right| < \frac{1}{rP_{m+1}}$$

или так:

$$|vs - ur| < \frac{u}{Q_{m+1}}, \qquad |vs - ur| < \frac{v}{P_{m+1}}$$

Перемножая почленно получившиеся неравенства и пользуясь тем, что $uv = N$, а согласно определению номера m выполняется неравенство $P_{m+1}Q_{m+1} \geqslant N^{1/3}$, находим

$$|vs - ur|^2 < \frac{uv}{P_{m+1}Q_{m+1}} \leqslant \frac{N}{N^{1/3}} = N^{2/3}.$$

Извлекая корень из обеих частей получившегося неравенства, завершаем доказательство леммы. □

Доказательство теоремы 5.1. Положим $k = rs$, где r и s — числа из леммы 5.1. Тогда $1 \leqslant k < N^{1/3}$. Справедливо тождество

$$4kN = (ur + vs)^2 - (ur - vs)^2.$$

Положим $a = ur + vs$ и $b = |ur - vs|$. Согласно лемме 5.1 имеем

$$a^2 = (ur+vs)^2 = (ur-vs)^2+4kN < N^{2/3}+4kN < \left(\sqrt{4kN} + \frac{N^{1/6}}{4\sqrt{k}}\right)^2$$

и $a < \sqrt{4kN} + \dfrac{N^{1/6}}{4\sqrt{k}}$. □

5.1.4 ρ–метод Полларда.

Пусть $f(x)$ — "достаточно случайный" многочлен. Выберем "случайно" $x_0 \in \mathbb{Z}, 1 < x_0 < N$, и рассмотрим последовательность

$$x_{k+1} \equiv f(x_k) \pmod N, \qquad k \geqslant 0,$$

Так как количество классов вычетов по модулю N не превосходит N, то существуют такие индексы $i, j, 0 \leqslant i, j < N$, что $x_i \equiv x_j \pmod N$ и значит, последовательность $x_k \pmod N$ зацикливается. Период этой последовательности не всегда начинается с самого начала, она может иметь предпериодическую часть. Символически такую последовательность можно изобразить в виде греческой буквы ρ. Подходящая снизу ножка этой буквы соответствует предпериодической части последовательности, она переходит в замкнутую петлю, соответствующую периодической части. Эта аналогия и дала название алгоритму.

Полларда обнаружил, что для простых p, как правило, длина периода и предпериодическая часть последовательности

$$x_{k+1} \equiv f(x_k) \pmod p, \qquad k \geqslant 0,$$

ограничены сверху величиной $c\sqrt{p}$, где c — некоторая константа.

Идея алгоритма состоит в том, чтобы последовательно вычислять наибольшие общие делители $(x_{2i} - x_i, N)$, $i = 1, 2, 3, \ldots$. Если p — простой делитель N, ℓ — длина периода и a — длина предпериодической части последовательности $x_{k+1} \equiv f(x_k) \pmod p$, то для номера i, удовлетворяющего условиям

$$i > a, \qquad \ell | i, \tag{5.4}$$

имеем $x_{2i} \equiv x_i \pmod{p}$, так что $(x_{2i} - x_i, N) > 1$. Ясно, что существует число i, удовлетворяющее условиям (5.4) и неравенству $i \leqslant a + \ell = O(\sqrt{p})$. Конечно, может случиться, что $N | x_{2i} - x_i$. Тогда нужно выбирать иное начальное значение x_0.

Если p — наименьший простой делитель N, то $p \leqslant N^{1/2}$, так что $i = O(N^{1/4})$.

В следующем ниже алгоритме вычисляются пары $\{x_i, x_{2i}\}, i \geqslant 1$. Для нахождения следующей пары $\{x_{i+1}, x_{2i+2}\}$ нужно вычислить

$$x_{i+1} \equiv f(x_i) (\mathrm{mod}\, N), \quad x_{2i+1} \equiv f(x_{2i}) (\mathrm{mod}\, N),$$
$$x_{2i+2} \equiv f(x_{2i+1}) (\mathrm{mod}\, N),$$

т.е. выполнить $O(1)$ арифметических операций.

Алгоритм 5.3. Дано: *составное число* N.
Найти: *нетривиальный делитель* N .

1. Выбрать случайно $x_0 \in \mathbb{Z}, 1 < x_0 < N$, *и положить*

$$x = f(x_0) \pmod{N}, \qquad y = f(x) \pmod{N}.$$

2. Вычислить $d = (y - x, N)$. *Если* $1 < d < N$ *алгоритм останавливается, нетривиальный делитель* d *числа* N *найден.*

3. Если $d = N$, *перейти в п. 1.*

4. Положить

$$x = f(x) \pmod{N}, \quad z = f(y) \pmod{N}, \quad y = f(z) \pmod{N}$$

и перейти в пункт 2 алгоритма.

Если все удачно сложится, то нетривиальный делитель числа N будет найден за $O(p^{1/2})$ арифметических операций, где p — наименьший простой делитель N, т.е. за $O(N^{1/4})$ арифметических операций.

В силу оценки сложности $O(p^{1/2})$ алгоритм удобен для нахождения не очень больших делителей p числа N, если они есть.

В качестве $f(x)$ обычно выбираются многочлены вида $x^2 + a$. Например, можно взять $f(x) = x^2 + 1$ или $f(x) = x^2 - 1$. В то же время

выбор $f(x) = x^2 - 2$ и $x_0 = 2$ не очень удачен, так как в этом случае последовательность x_k имеет период 1.

Приведем теперь некоторые эвристические соображения в пользу того, что длина периода и предпериодическая часть последовательности $x_{k+1} \equiv f(x_k) \pmod{p}$ оцениваются сверху величиной $O(p^{1/2})$.

Пусть M — достаточно большое число, но при этом $M = o(p^{2/3})$. Будем делать случайные выборки наборов $\overline{z} = \{z_1, \ldots, z_M\}$, $0 \leqslant z_i < p$. Какова вероятность того, что среди выбранных чисел z_i найдутся два одинаковых элемента?

Количество всех возможных наборов $\overline{z}$ равно p^M. Среди них имеется $p(p-1)\cdots(p-M+1)$ наборов с попарно различными координатами. Поэтому вероятность случайному набору $\overline{z}$ иметь различные координаты равна

$$\mu = \frac{p(p-1)\cdots(p-M+1)}{p^M} = \frac{p!}{p^M(p-M)!}.$$

Пользуясь формулой Стирлинга $N! \sim N^N e^{-N}\sqrt{2\pi N}$, находим

$$\mu \sim \frac{p^p e^{-p}\sqrt{2\pi p}}{p^M (p-M)^{p-M} e^{-p+M}\sqrt{2\pi(p-M)}}.$$

Так как

$$(p-M)\ln\left(1-\frac{M}{p}\right) = -M + \frac{M^2}{2p} + o(1),$$

то $\mu \sim e^{-M^2/(2p)}$ при $p \to \infty$. Если $M = \sqrt{2p\ln 2} + O(1) = O(p^{1/2})$, то $\dfrac{M^2}{2p} = \ln 2 + o(1)$ и $\mu = \dfrac{1}{2} + o(1)$.

Это значит, что если многочлен $f(x)$ порождает "случайную" последовательность $x_0, x_1, x_2, \ldots$, то набор $x_{k+1}, x_{k+2}, \ldots, x_{k+M}$ длины $O(p^{1/2})$ с вероятностью близкой к $\dfrac{1}{2}$ будет иметь два одинаковых члена.

Конечно, это рассуждение не является доказательством, но оно дает правдоподобное объяснение, почему ρ–метод Полларда достаточно

быстро на практике находит небольшие простые делители составных чисел.

Заметим также, что скорость работы этого алгоритма может быть увеличена, если наибольший общий делитель $(x_{2i} - x_i, N)$ вычислять не на каждом шаге. Например, можно для последовательности $i = 0, d, 2d, \ldots$ вычислять $(\prod_{k=i+1}^{i+d}(x_{2k} - x_k), N)$, выбрав d не очень большим.

5.1.5 (p-1)–метод Полларда.

Пусть N — составное число и пусть p — некоторый его простой делитель. По теореме Эйлера, при любом a, взаимно простом с N, и любом натуральном t справедливо сравнение

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

Следовательно, число $d = (a^{t(p-1)} - 1, N)$ делится на p, то есть является делителем N, отличным от 1. Конечно, если t слишком велико или порядок a по модулю N слишком мал, может оказаться, что $d = N$. Но, если a выбирать случайным образом, то с большой вероятностью порядок a по модулю N будет большим, и тогда для разложения N на множители достаточно найти как можно меньшую степень, в которой a будет сравнимо с 1 по модулю p. В случае, когда $p-1$ является произведением маленьких простых, эта задача решается довольно быстро.

Алгоритм 5.4. Дано: *Составное число N, целое число a, взаимно простое с N, граница гладкости B.*
Найти: *Нетривиальный делитель N.*

1. Положить $b = a$.

2. Для каждого простого числа $q \leqslant B$ найти максимальное натуральное c, такое что $q^c \leqslant N$, и заменить b на остаток от деления b^{q^c} на N.

3. Вычислить $d = (b - 1, N)$.

4. Если $1 < d < N$, то d — нетривиальный делитель N. СТОП.

5. Если $d = 1$, то любое число $p - 1$, где p — простой делитель N, делится на какое-то простое число, большее B. СТОП.

6. Если $d = N$, то либо B слишком велико, либо порядок a по модулю N слишком мал. СТОП.

После прохождения пункта 2 имеем $b \equiv a^M \pmod N$, где $M = \prod\limits_{q \leqslant B} q^{c(q)}$ и $c(q)$ — наибольшее натуральное число с условием $q^{c(q)} \leqslant N$. Таким образом, в пункте 2 число a возводится по модулю N в степень, которая делится на любое B–гладкое число, не превосходящее N, в частности, на все B–гладкие числа $p - 1$, где p — какой-то простой делитель N. Пункт 2 требует $O\bigl(\frac{B}{\ln B} \ln N\bigr)$ арифметических операций. Следовательно, при малых значениях B алгоритм способен довольно быстро находить те простые делители p числа N, для которых число $p-1$ является B–гладким. В худшем же случае, для того, чтобы выделить из N нетривиальный простой делитель, может понадобиться взять B порядка $N^{1/2}$, и тогда количество арифметических операций в алгоритме будет оцениваться величиной $O(N^{1/2})$.

5.2 Субэкспоненциальные алгоритмы.

Многие алгоритмы для разложения составных чисел N на множители используют следующую идею:

1. Найти такие целые числа x, y, что

$$x^2 \equiv y^2 \pmod N. \tag{5.5}$$

2. Вычислить $d = (x - y, N)$. Если $1 < d < N$, то d — собственный делитель N.

Для построения таких пар (x, y) часто используется еще одно соображение. Каким-либо образом строится последовательность пар целых чисел $(R_i, z_i), i = 1, 2, \ldots$, таких, что

$$z_i^2 \equiv R_i \pmod N, \qquad i = 1, 2, \ldots . \tag{5.6}$$

Допустим, что при этом есть возможность находить совокупности $\mathcal{L}$ индексов $\{i_1, \ldots, i_\ell\}$ таких, что

$$R_{i_1} \cdots R_{i_\ell} = y^2\,, \qquad y \in \mathbb{Z}. \tag{5.7}$$

Тогда для $x \equiv z_{i_1} \cdots z_{i_\ell} \pmod N$ имеем

$$x^2 \equiv z_{i_1}^2 \cdots z_{i_\ell}^2 \equiv R_{i_1} \cdots R_{i_\ell} = y^2 \pmod N,$$

что дает пару чисел (x, y) с условием (5.5).

В этой связи возникают два вопроса:

1. *как строить последовательности, удовлетворяющие (5.6), и*

2. *как выбирать наборы $(i_1, \ldots, i_\ell)$, удовлетворяющие (5.7)?*

Для ответа на второй вопрос обычно поступают так. Выбирают некоторое конечное множество

$$\mathcal{B} = \{p_0 = -1, p_1, p_2, \ldots, p_\ell\},$$

где $p_1, \ldots, p_\ell$ — различные простые числа. Это множество называется *базой разложения* (факторной базой). Затем с помощью метода пробных делений на элементы $\mathcal{B}$ пытаются разложить числа R_i на простые множители. Если

$$R_i = \prod_{j=0}^{\ell} p_j^{\alpha_{i,j}},$$

то индекс i помещают в $\mathcal{L}$. В противном случае этот индекс отбрасывается. Положим

$$a_{i,j} \equiv \alpha_{i,j} \pmod 2, \qquad a_{i,j} \in \{0, 1\}, \quad j = 0, 1, \ldots, \ell.$$

и определим вектор $\overline{e}_i = (a_{i,0}, \ldots, a_{i,\ell}) \in \mathbb{F}_2^{\ell+1}$.

Если $|\mathcal{L}| > \ell + 1$, то векторы $\overline{e}_i, i \in \mathcal{L}$, линейно зависимы над $\mathbb{F}_2$. Это значит, что существуют не равные одновременно нулю числа $b_i \in \{0, 1\}$, $i \in \mathcal{L}$, такие, что

$$\sum_{i \in \mathcal{L}} b_i \overline{e}_i = 0 \tag{5.8}$$

в поле $\mathbb{F}_2$.

Тогда

$$\prod_{i\in\mathcal{L}} R_i^{b_i} = \prod_{j=0}^{\ell}\prod_{i\in\mathcal{L}} p_j^{b_i\alpha_{i,j}} = \prod_{j=0}^{\ell} p_j^{\sum_{i\in\mathcal{L}} b_i\alpha_{i,j}}\,.$$

Поскольку согласно определению $a_{i,j}$ и (5.8)

$$\sum_{i\in\mathcal{L}} b_i\alpha_{i,j} \equiv \sum_{i\in\mathcal{L}} b_i a_{i,j} \equiv 0 \pmod 2,$$

то положив

$$c_j = \frac{1}{2}\sum_{i\in\mathcal{L}} b_i\alpha_{i,j} \in \mathbb{Z}\,, \qquad y = \prod_{j=0}^{\ell} p_j^{c_j},$$

будем иметь

$$\prod_{i\in\mathcal{L}} R_i^{b_i} = y^2.$$

Зависимостей вида (5.8) при $|\mathcal{L}|$ существенно превышающем $\ell+1$ может быть несколько, и это дает несколько пар (x,y), удовлетворяющих (5.5), что важно, если для первой из этих пар выполняется $(x-y,N)\in\{1,N\}$.

Теперь перейдем к конструкции последовательностей.

5.2.1 Алгоритм цепных дробей.

С помощью этого метода Дж.Моррисон и М.Бриллхарт впервые в 1975г. разложили на множители число

$$F_7 = 2^{2^7}+1 = 340282366920938463463374607431768211457 =$$
$$= 59649589127497217\cdot 5704689200685129054721.$$

Для описания алгоритма понадобятся свойства разложений в цепные дроби чисел вида $\sqrt{N}$, где N — натуральное число, не являющееся квадратом. Так как $\sqrt{N}$ есть корень многочлена x^2-N второй степени с целыми коэффициентами, то по теореме Лагранжа, относящейся к произвольным квадратичным иррациональностям, цепная

дробь $\sqrt{N} = [a_0; a_1, a_2, \ldots]$ периодична, т.е. для некоторого целого k при всех достаточно больших n выполняется равенство $a_{n+k} = a_n$. Это свойство обозначается записью

$$[\ a_0; a_1, \ldots, a_h, \overline{a_{h+1}, \ldots, a_{h+k}}\ ],$$

где $a_{h+1}, \ldots, a_{h+k}$ — период. Например,

$$\sqrt{69} = [8; \overline{3, 3, 1, 4, 1, 3, 3, 16}]$$

И в общем случае можно доказать, что если N — натуральное число, не являющееся квадратом никакого целого числа, то

$$\sqrt{N} = [a_0; \overline{a_1, \ldots, a_k, 2a_0}],$$

где $a_0 = [\sqrt{N}]$, причем упорядоченный набор чисел $a_1, \ldots, a_k$ симметричен, т.е. $a_1 = a_k$, $a_2 = a_{k-1}$ и т.д. Разложения таких специальных чисел обладают и рядом других особенностей. Так, если $\dfrac{P_k}{Q_k}$ — подходящие дроби к числу $\sqrt{N}$, то

$$\alpha_{k+1} = \frac{A_{k+1} + \sqrt{N}}{B_{k+1}}, \qquad k \geqslant 0,$$

где

$$\begin{aligned} B_{k+1} &= (-1)^{k+1}(P_k^2 - NQ_k^2), \\ A_{k+1} &= (-1)^{k+1}(NQ_kQ_{k-1} - P_kP_{k-1}) \end{aligned} \tag{5.9}$$

суть целые числа, причем $B_{k+1} > 0$. Из равенства (5.9) следует, что

$$P_k^2 \equiv (-1)^{k+1} B_{k+1} \pmod{N}.$$

Таким образом, числа $R_k = (-1)^{k+1}B_{k+1}, z_k = P_k$ удовлетворяют условию (5.6). Последовательность (A_k, B_k) удобно вычисляется с помощью соотношений

$$A_{k+1} = a_kB_k - A_k, \quad B_{k+1} = \frac{N - A_{k+1}^2}{B_k}, \quad a_k = \left[\frac{A_k + \left[\sqrt{N}\right]}{B_k}\right].$$

Из них, поскольку $B_k > 0, k \geqslant 0$, следует $|A_{k+1}| < \sqrt{N}$ и

$$B_k = \frac{A_k + A_{k+1}}{a_k} < 2\sqrt{N}.$$

Таким образом, последовательность B_k ограничена, и по величине ее члены существенно меньше N.

Если p — простое число, входящее в разложение B_{k+1} на простые сомножители, то из равенства (5.9) следует, что $P_k^2 \equiv NQ_k^2 \pmod{p}$, и $p \nmid Q_k$, ведь числа P_k, Q_k взаимно просты. Поэтому N — квадратичный вычет по модулю p и в базу множителей $\mathcal{B}$ помимо $p_0 = -1$ следует включать только простые числа с условием $\left(\dfrac{N}{p}\right) = 1$.

Если в множество $\mathcal{B}$ отнести все простые числа p с условиями $\left(\frac{N}{p}\right) = 1$, $p \leqslant L^a$, где $L = e^{(\ln N \ln\ln N)^{1/2}}$ и $a = \dfrac{1}{\sqrt{2}}$, то, как можно проверить, для разложения числа N на множители алгоритму непрерывных дробей потребуется

$$O(L^{\sqrt{2}+o(1)}) = O(e^{\sqrt{(2+o(1))\ln N \ln\ln N}})$$

арифметических операций.

5.2.2 Алгоритм Диксона.

Описываемый ниже вероятностный алгоритм разложения чисел на множители не имеет практического значения. К его достоинствам можно отнести то, что вероятность срабатывания и среднее количество арифметических операций, необходимых этому алгоритму для разложения числа на множители, оцениваются без использования каких-либо не доказанных гипотез и носят субэкспоненциальный характер.

Алгоритм 5.5. Дано: *составное число N, а также v, n — фиксированные натуральные числа; N не имеет простых делителей, меньших v.*

Найти: *разложение N на меньшие множители.*

Определить

$$\mathcal{B} = \{p \leqslant v\} = \{p_1, \ldots, p_\ell\}$$

— совокупность всех простых чисел, не превосходящих v; выбрать каким-либо способом

$$L = \{z_1, \ldots, z_n\}$$

— множество целых чисел, $1 < z_j < N$; положить

$$\mathcal{L} = \emptyset\,, \qquad i = 0.$$

1. Если $i \geqslant n$, алгоритм останавливается, не выдавая разложения. Он оказался безуспешным. Иначе, положить $i = i + 1$.

2. Пусть $R_i \equiv z_i^2 \pmod N, 1 \leqslant R_i \leqslant N$. С помощью пробных делений на числа из $\mathcal{B}$ представить R_i в виде

$$R_i = S \cdot \prod_{k=1}^{\ell} p_k^{\alpha_{i,k}},$$

где S не имеет простых делителей из $\mathcal{B}$. Если $S = 1$, перейти в пункт 3 алгоритма, иначе перейти в пункт 1.

3. Поместить индекс i в множество $\mathcal{L}$ и запомнить вектор $\overline{\alpha}_i = (\alpha_{i,1}, \ldots, \alpha_{i,n})$. Если $|\mathcal{L}| \leqslant \ell$, перейти в пункт 1, иначе перейти в пункт 4.

4. Найти наименьший индекс $j \in \mathcal{L}$ такой, что

$$\overline{\alpha}_j \equiv \sum_{\substack{i \in \mathcal{L} \\ i<j}} b_i \overline{\alpha}_i \pmod 2\,, \qquad b_i \in \{0; 1\}.$$

Исключить j из $\mathcal{L}$. Положить

$$\overline{c} = (c_1, \ldots, c_\ell) = \frac{1}{2} \cdot (\overline{\alpha}_j + \sum_{\substack{i \in \mathcal{L} \\ i<j}} b_i \overline{\alpha}_i)$$

и перейти в пункт 5.

5. Положить

$$x \equiv z_j \prod_{\substack{i \in \mathcal{L} \\ i<j}} z_i^{b_i} \pmod N, \qquad y \equiv \prod_{k=1}^{\ell} p_k^{c_k} \pmod N.$$

Если $x \equiv y \pmod N$ *или* $x \equiv -y \pmod N$, *перейти в пункт 1. Иначе, вычислить* $d = (x+y, N)$ *— нетривиальный делитель* N.

Заметим, что

$$x^2 \equiv R_j \prod_{\substack{i \in \mathcal{L} \\ i<j}} R_i^{b_i} \equiv \prod_{k=1}^{\ell} p_k^{2c_k} \equiv y^2 \pmod N.$$

Успех алгоритма зависит от выбора множества $L = (z_1, \ldots, z_n)$.

Теорема 5.2. *Пусть* N *— целое число, имеющее по крайней мере два различных простых делителя, пусть также*

$$v = e^{(2 \ln N \ln\ln N)^{1/2}}, \qquad n = [v^2 + 1]. \tag{5.10}$$

Тогда для разложения числа N *на множители алгоритм Диксона в среднем требует* $O\left(e^{3(2 \ln N \ln\ln N)^{1/2}}\right)$ *арифметических операций, и доля тех множеств* L, *для которых число* N *не будет разложено составляет* $O(v^{-1})$.

Остаток параграфа будет посвящен доказательству этой теоремы. Для его описания удобно ввести новое понятие, которое будет использоваться и в других разделах книги.

Определение 5.1. *Пусть* y *— положительное число. Целое число* n *называется* y-гладким, *если все его простые делители не превосходят* y.

Предложение 5.1. *Пусть* v *— число, определенное в (5.10). Количество целых чисел* $z, 1 \leqslant z \leqslant N$, *с условием, что* w, *определенное условиями* $w \equiv z^2 \pmod N, 1 \leqslant w \leqslant N$, *есть* v*-гладкое число, не меньше*

$$N \cdot v^{-1/2+o(1)}, \quad \text{при} \quad N \to \infty.$$

Доказательство этого предложения использует некоторые факты о распределении простых чисел и носит технический характер. Мы его здесь не приводим.

Следующая лемма относится к свойствам алгоритма 5.5.

Лемма 5.2. *Доля тех последовательностей $L = (z_1, \ldots, z_n)$, при которых пункт 5 алгоритма проходится более ℓ раз, не превосходит $2^{-\ell}$.*

Доказательство. Назовем последовательность "плохой", если алгоритм на этой последовательности более ℓ раз проходит пункт 5.

Для каждой последовательности $L = (z_1, \ldots, z_n)$ положим $w(L) = (w_1, \ldots, w_n)$, где $w_j \equiv z_j^2 \pmod N, 1 \leqslant w_j \leqslant N$. Разобьем множество последовательностей L на классы, отнеся в один класс последовательности с одинаковым значением $w(L)$.

Достаточно доказать, что доля "плохих" последовательностей в каждом из классов не превосходит $2^{-\ell}$.

Пусть $\mathcal{K}$ — некоторый класс последовательностей и $(w_1, \ldots, w_n)$ — соответствующий ему вектор. Для любой последовательности $L = (z_1, \ldots, z_n) \in \mathcal{K}$ выполняются сравнения $z_k^2 \equiv w_k \pmod N, k = 1, \ldots, n$. При каждом k сравнение $x^2 \equiv w_k \pmod N$ имеет 2^m решений, где m — количество простых делителей N. Поэтому $|\mathcal{K}| = 2^{mn}$.

Пусть $L_0 = (\tilde{z}_1, \ldots, \tilde{z}_n) \in \mathcal{K}$ — "плохая" последовательность. Обозначим через $j_1, \ldots, j_\ell$ первые ℓ значений параметра j, при которых алгоритм проходит через шаг 5. Если $L \in \mathcal{K}$ — плохая последовательность, то при фиксированных значениях $z_j, j \neq j_1, \ldots, j_\ell$, каждая из переменных $z_{j_1}, \ldots, z_{j_\ell}$ принимает не более двух значений. Ведь тогда должны выполняться сравнения

$$z_{j_k} \cdot \prod_{\substack{i \in \mathcal{L} \\ i < j_k}} z_i^{b_i} \equiv \pm y \pmod N,$$

а величина y зависит только от $w(L)$ и индекса j_k. Следовательно, количество плохих последовательностей не превосходит $2^{m(n-\ell)} \cdot 2^\ell$.

Учитывая, что $|\mathcal{K}| = 2^{mn}$, заключаем, что доля плохих последовательностей в $\mathcal{K}$ не превосходит

$$\frac{2^{m(n-\ell)+\ell}}{2^{mn}} = 2^{-\ell(m-1)} \leqslant 2^{-\ell}.$$

□

Перейдем теперь непосредственно к доказательству теоремы 5.2.

Доказательство. Рассмотрим множество последовательностей $L = (z_1, \ldots, z_n) \in \mathbb{Z}^n, 1 \leqslant z_j \leqslant N$, и определим на нем случайную величину X_L равной количеству v-гладких чисел в наборе $w(L)$.

Обозначим буквой λ — вероятность появления v-гладкого числа $w \equiv z^2 \pmod N, 1 \leqslant w \leqslant N$ при случайном выборе целого z на отрезке $1 \leqslant z \leqslant N$. Согласно предложению 5.1 справедливо неравенство

$$\lambda \geqslant v^{-1/2+o(1)}.$$

Оценим теперь вероятность появления k v-гладких чисел в последовательности $w(L)$ при случайном выборе L. Здесь применима так называемая схема Бернулли для подсчета вероятности k успехов при n испытаниях. Имеем для этой вероятности значение

$$P\left(X_L = k\right) = \binom{n}{k} \lambda^k (1-\lambda)^{n-k}.$$

Теперь находим математическое ожидание этой величины

$$M(X_L) = \sum_{k=0}^{n} k \binom{n}{k} \lambda^k (1-\lambda)^{n-k} = n\lambda$$

и ее дисперсию

$$D(X_L) = \sum_{k=0}^{n} (k - n\lambda)^2 \binom{n}{k} \lambda^k (1-\lambda)^{n-k} = n\lambda(1-\lambda).$$

Согласно неравенству Чебышева имеем

$$P\left(|X_L - \lambda n| \geqslant \frac{\lambda n}{2}\right) \leqslant \frac{n\lambda(1-\lambda)}{\left(\frac{1}{2}\lambda n\right)^2} = \frac{4(1-\lambda)}{n\lambda} < \frac{4}{n\lambda}.$$

Из этого неравенства следует, что

$$P\left(X_L \leqslant \frac{\lambda n}{2}\right) = P\left(X_L - \lambda n \leqslant -\frac{\lambda n}{2}\right) \leqslant$$
$$\leqslant P\left(|X_L - \lambda n| \geqslant \frac{\lambda n}{2}\right) < \frac{4}{\lambda n}.$$

Таким образом, для подавляющего количества множеств L последовательность $w(L)$ будет содержать более $\dfrac{\lambda n}{2}$ чисел, являющихся v-гладкими.

По асимптотическому закону распределения простых чисел при всех достаточно больших x количество $\pi(x)$ простых чисел $p \leqslant x$ ограничено сверху величиной $2\dfrac{x}{\ln x}$. Поэтому $\ell = \pi(v) < 2\dfrac{v}{\ln v}$ и, значит,

$$\lambda n \geqslant n v^{-1/2+o(1)} \geqslant v \geqslant 8\frac{v}{\ln v} > 4\ell.$$

Пусть теперь последовательность L такова, что $X_L > \frac{\lambda n}{2} > 2\ell$ и алгоритм не разложил N на множители.

В процессе своей работы алгоритм n раз пройдет через пункт 1. Последовательность значений $|\mathcal{L}|$, вычисленных после прохождения алгоритма через пункт 1, не убывает, а если алгоритм пришел в пункт 1 из пункта 3, то она возрастает. Значит, если в какой-то момент выполнилось неравенство $|\mathcal{L}| > \ell$, в дальнейшем алгоритм из пункта 3 будет всегда следовать в пункт 4. Так как величина $|\mathcal{L}|$ может возрастать не более ℓ раз, то алгоритм не менее $X_L - \ell > \ell$ раз пройдет из пункта 3 в пункт 4 и далее в пункт 5. Согласно лемме 5.2 доля таких множеств L составляет не более $2^{-\ell}$.

Число N не будет разложено алгоритмом с помощью последовательности L, если $X_L \leqslant \frac{\lambda n}{2}$, т.е. количество v-гладких чисел в последовательности R_i мало, или, если $X_L > \frac{\lambda n}{2}$ и L — плохое множество.

Поэтому доля тех L, для которых алгоритм не разложит N, не превосходит

$$\frac{4}{n\lambda} + 2^{-\ell} \leqslant \frac{4}{v^2} \cdot (v^{1/2+o(1)}) + 2^{-\frac{v}{2\ln v}} = O\left(v^{-3/2+o(1)}\right).$$

Здесь использовались неравенства $n > v^2, \lambda \geqslant v^{-\frac{1}{2}+o(1)}, \ell \geqslant \frac{v}{2\ln v}$. Второе утверждение теоремы доказано.

Оценка среднего количества арифметических операций в алгоритме доказывается с помощью непосредственных вычислений, и мы ее опускаем. □

Возможны усовершенствования алгоритма, незначительно уменьшающие его сложность. Они могут применяться и в связи с другими алгоритмами.

1. *Использование более совершенных методов разложения* на множители в пункте 2 алгоритма.

2. *Использование больших простых чисел.* Если в шаге 2

$$R_i = S \cdot \prod_{j=1}^{\ell} p_j^{\alpha_{i,j}},$$

причем $S \leqslant v^2$, то S — простое число. Иначе оно имело бы простой делитель, оцениваемый величиной $\sqrt{S} \leqslant v$, что неверно. Такие индексы i можно не отбрасывать, а запоминать в порядке возрастания S. Пройдем затем по всей сохраненной таблице и сравним разложения с одинаковыми S. Из двух таких разложений, перемножив их, можно исключить S. Действительно, если

$$z_i^2 \equiv S \cdot \prod_{j=1}^{\ell} p_j^{\alpha_{i,j}} \pmod{N}, \quad z_k^2 \equiv S \cdot \prod_{j=1}^{\ell} p_j^{\alpha_{k,j}} \pmod{N},$$

и целое число T определено сравнением $ST \equiv z_i z_k \pmod{N}$, то

$$T^2 \equiv \prod_{j=1}^{\ell} p_j^{\alpha_{i,j}+\alpha_{k,j}} \pmod{N}.$$

И это сравнение можно использовать в работе алгоритма. Несмотря на то, что сравнений с большим простым S довольно много, асимптотически их использование не улучшает оценку сложности. На практике успешно применялись также алгоритмы, использующие числа S, раскладывающиеся в произведение двух больших простых сомножителей.

3. *Стратегия раннего обрыва.* При разложении чисел R_i на множители можно отбрасывать индекс i до того, как R_i было разделено на все простые числа из $\mathcal{B}$. Например, задавшись параметрами θ, γ, можно разделить R_i на все простые числа $p \in \mathcal{B}, p \leqslant v^\theta$ и, если неразложившаяся часть R_i превышает N^γ, такое i можно отбросить.

Этот подход при правильном выборе параметров v, θ, γ позволяет снизить количество арифметических операций в алгоритме.

4. Алгоритм Диксона допускает *распараллеливание вычислений* пар R_i, z_i.

5.2.3 Алгоритм просеивания.

В алгоритмах разложения на множители и при решении других теоретико-числовых задач важную роль играет так называемый алгоритм просеивания. Предположим, что задан некоторый многочлен $f(x) \in \mathbb{Z}[x]$ и требуется найти все целые числа k, расположенные на некотором отрезке $A \leqslant k \leqslant B$ и такие, что значения $f(k)$ раскладываются в произведение простых чисел из заданного множества $\mathcal{B}$. Идея алгоритма просеивания заключается в том, что если $f(a) \equiv 0 \pmod{p^t}$, то при любом целом ℓ выполняется также сравнение $f(a + \ell p^t) \equiv 0 \pmod{p^t}$. Это позволяет фиксировать сразу некоторое множество чисел k, для которых в разложение $f(k)$ на простые множители входит простое число p в степени не меньшей t. В результате процесс поиска нужных чисел k ускоряется. Мы рассмотрим этот алгоритм сразу для нескольких многочленов $f(x)$, что требуется в приложениях.

Пусть $f_1(x), \ldots, f_r(x)$ — многочлены с целыми коэффициентами и $\mathcal{B}$ — некоторое множество простых чисел. Требуется найти целые

числа $k \in [A, B]$ такие, что все значения $f_j(k), 1 \leqslant j \leqslant r$, раскладываются только на простые множители из $\mathcal{B}$. При этом предполагается, что длина отрезка $[A, B]$ и множество $\mathcal{B}$ велики, а число r мало, скажем $r = 1$ или $r = 2$. В описываемом ниже алгоритме присутствует некоторый целый параметр D и кратности $v_p, p \in \mathcal{B}$, вычисляемые в зависимости от реальной задачи.

Алгоритм 5.6. Вход: *многочлены $f_1(x), \ldots, f_r(x)$ с целыми коэффициентами и целые числа $A < B$.*

Выход: *Множество всех целых чисел k, $A \leqslant k \leqslant B$, для которых каждое из чисел $f_1(k), \ldots, f_r(k)$ раскладывается на простые множители из $\mathcal{B}$.*

1. Для каждого $p \in \mathcal{B}$ и всех $j = 1, \ldots, r$, $i = 1, \ldots, v_p$ вычислить множества

$$S_j(p, i) = \{c \in \mathbb{Z} \quad | \quad 0 \leqslant c < p^i, \quad f_j(c) \equiv 0 \pmod{p^i}\}.$$

2. Вычислить $\ln p$, $p \in \mathcal{B}$, и для всех $j = 1, \ldots, r$, $k \in [A, B]$ вычислить

$$a_{k,j} = \ln |f_j(k)|.$$

3. (Просеивание) Для каждого набора параметров (p, i, j, c) с условиями

$$p \in \mathcal{B}, \quad 1 \leqslant i \leqslant v_p, \quad 1 \leqslant j \leqslant r, \quad c \in S_j(p, i)$$

и каждого целого ℓ, для которого

$$k = c + \ell p^i \in [A, B]$$

пересчитать значение $a_{k,j}$, а именно

$$a_{k,j} = a_{k,j} - \ln p.$$

Значения ℓ перебираются последовательно. При этом k пробегает арифметическую прогрессию с шагом p^i.

4. Для всех чисел k с условием

$$a_{k,j} < D \tag{5.11}$$

произвести разложение всех $f_j(k), 1 \leqslant j \leqslant r$, *на множители пробными делениями на элементы из множества* $\mathcal{B}$.

Ограничимся лишь некоторыми замечаниями в связи с работой этого алгоритма.

1. В пункте 1 алгоритма следует найти решения сравнений $f_j(x) \equiv (\mathrm{mod}\ p)$, а затем выполнить подъем этих решений по модулю p^i.

2. При фиксированных p, j, k с условиями $p \in \mathcal{B}, 1 \leqslant j \leqslant r, k \in [A, B]$ пересчет значений $a_{k,j}$ в пункте 3 будет производиться $\nu_p(f_j(k))$ раз. Количество вычитаний будет равно количеству индексов i таких, что число c из интервала $[0, p^i)$, определенное сравнением $k \equiv c \pmod{p^i}$, принадлежит множеству $S_j(p, i)$, т.е. удовлетворяет сравнению $f_j(c) \equiv 0 \pmod{p^i}$. Последнее выполнено тогда и только тогда, когда $f_j(k) \equiv 0 \pmod{p^i}$.

3. Если число $k \in [A, B]$ удовлетворяет неравенствам (5.11) при $j = 1, \ldots, r$, то справедливы разложения

$$f_j(k) = q_j \prod_{p \in \mathcal{B}} p^{\alpha_j(p)},$$

где $\alpha_j(p)$ — целые неотрицательные числа и $q_j \in \mathbb{Z}, 1 \leqslant q_j \leqslant e^D$. Если $\nu_p(f_j(k)) \leqslant v_p$, то $\alpha_j(p) = \nu_p(f_j(k))$. Реальные вычисления логарифмов производятся с некоторой ошибкой, поэтому реальные значения q_j могут несколько превышать границу e^D.

5.2.4 Квадратичное решето.

Рассмотрим многочлен

$$R(x) = (x + [\sqrt{N}])^2 - N.$$

Тогда пара чисел

$$z_i = i + [\sqrt{N}], \quad R_i = R(i)$$

удовлетворяет сравнению

$$z_i^2 \equiv R_i \pmod{N}.$$

Кроме того,

$$R_i = (i + [\sqrt{N}])^2 - N \leqslant (i + \sqrt{N})^2 - N = i^2 + 2i\sqrt{N}.$$

Если $i = O(N^\varepsilon)$, где $\varepsilon > 0$, то $R_i = O(N^{1/2+\varepsilon})$.

Важное преимущество этого подхода состоит в том, что можно организовать разложение чисел R_i не поодиночке, а всех сразу, используя алгоритм просеивания.

Для каждого простого $p|R_i$ имеем

$$z_i^2 \equiv N \pmod{p}.$$

Поэтому в базу множителей имеет смысл включить только те простые числа p, для которых символ Лежандра равен $\left(\frac{N}{p}\right) = 1$.

Определим при некотором v множество $\mathcal{B}$ равенством

$$\mathcal{B} = \{p_1, \ldots, p_\ell\} = \left\{p \leqslant v, \quad \left(\frac{N}{p}\right) = 1\right\}.$$

Далее, для нахождения чисел $i, 1 \leqslant i \leqslant B = O(N^\varepsilon)$ с условием, что $R_i = R(i)$ раскладывается на простые множители $p \in \mathcal{B}$ используется алгоритм просеивания с многочленом $f_1(x) = R(x)$. Если параметр D в алгоритме просеивания удовлетворяет неравенству $D < \ln v$, то раскладываемые с помощью пробных делений числа R_i будут разложены полностью. Ведь числа q_j будут удовлетворять неравенству $\ln q_j \leqslant \ln v$.

Далее алгоритм разложения на множители с помощью квадратичного решета выполняется так же, как и алгоритм Диксона.

Приняв на веру ряд недоказанных гипотез о распределении простых чисел, можно показать, что при некотором выборе чисел v и B в зависимости от N алгоритм требует $O(e^{\sqrt{(1+o(1))\ln N \ln\ln N}})$ арифметических операций.

Этот алгоритм допускает различные усовершенствования.

1. Вместо N его можно применять к числу kN, где k выбрано так, что для всех достаточно малых простых p выполняется условие $\left(\frac{kN}{p}\right) = 1$. Это увеличит базу множителей $\mathcal{B}$.

2. Можно выбрать параметр $D = 2\ln v$ и использовать большие простые числа, не входящие в $\mathcal{B}$, как это объяснялось в конце раздела 5.2.2, пункт 2.

3. Вместо многочлена $f(x) = (x+[\sqrt{N}])^2 - N$ можно рассматривать многочлены $f(x) = ax^2 + 2bx + c$ такие, что $a > 0$ и $N = b^2 - ac$. Тогда

$$af(x) = (ax+b)^2 - (b^2 - ac) \equiv (ax+b)^2 \pmod{N}$$

и для целых $x \in \left[-\frac{b}{a} - M,\ -\frac{b}{a} + M\right]$, где M — натуральное число, $M = N^{\varepsilon}$, имеем

$$-N \leqslant af(x) \leqslant a^2M^2 - N.$$

Выберем a так, что $a^2M^2 \leqslant 2N$ и $a^2M^2 \sim 2N$. Тогда $|f(x)| \leqslant \frac{N}{a} \sim M\sqrt{\frac{N}{2}} = O(N^{1/2+\varepsilon})$. Можно выбирать a простым числом, близким к $\frac{\sqrt{2N}}{M}$, и так, что $\left(\frac{N}{a}\right) = 1$. Решая сравнение $b^2 \equiv N \pmod{a}$, находим b и $c = \frac{b^2-N}{a}$.

Для каждого многочлена $f(x)$ можно производить свое просеивание. Изложенная схема называется квадратичное решето *с несколькими полиномами*. Этот алгоритм может раскладывать на множители числа, доходящие до 10^{130}.

В 1977 г. Райвест, Шамир и Адлеман предложили схему шифрования (RSA), основанную на том, что задача разложения целых чисел на множители сложна в вычислительном отношении, см. раздел 8.2. Для иллюстрации стойкости своего метода они зашифровали некоторую английскую фразу, выбрав в качестве ключа число $N = pq$, где p и q — простые числа, записываемые, соответственно, 64 и 65 десятичными знаками. Для расшифровки необходимо было найти p и q, т.е. разложить известное всем число N на простые множители. Это число было разложено на множители лишь в 1994 г. Использовался метод квадратичного решета, и далее мы приведем некоторые комментарии.

1. Вместо N раскладывалось число $5N$.

2. В базу множителей входили простые числа p, для которых $\left(\frac{5N}{p}\right) = 1$ при $p \leqslant 16333609 = v$, а также -1, всего 524339 элементов.

3. Использовались разложения

$$z^2 \equiv Q \equiv q_1 q_2 \cdot \prod_{j=0}^{\ell} p_j^{\alpha_j}, \tag{5.12}$$

где q_1, q_2 простые, $v < q_i \leqslant v' = 2^{30}$.

4. Было найдено более $8,25 \cdot 10^6$ соотношений (5.12), из которых 112001 соотношений имели $q_1 = q_2 = 1$, еще 1431337 соотношений имели $q_2 = 1$ и, наконец, в 6881138 соотношениях $q_1 \neq 1$, $q_2 \neq 1$. На это было потрачено 220 дней просеивания. Использовались более 1600 компьютеров. В результате исключения q_i были получены 569466 векторов размерности 524339.

5. Для обработки полученной разреженной матрицы применялись специальные процедуры исключения. Первые три зависимости $x^2 \equiv y^2 \pmod N$ не разложили N. На четвертой число N было разложено.

5.2.5 Решето числового поля

Описываемый в этом разделе алгоритм при некоторых правдоподобных допущениях имеет оценку $O\left(e^{(\ln N)^{1/3}(\ln\ln N)^{2/3}(c+o(1))}\right)$ для количества арифметических операций, где можно взять $c = \sqrt[3]{\frac{64}{9}}$. Это асимптотически наиболее быстрый в настоящее время алгоритм. С его помощью, например, в 2005 году было разложено на множители число, записываемое 200 десятичными знаками и не имеющее каких-либо особенностей.

Пусть $K = \mathbb{Q}(\theta)$ — алгебраическое числовое поле, $d = [K : \mathbb{Q}]$, $\theta \in \mathbb{Z}_K$ и $T(x)$ — минимальный многочлен θ. Для простоты изложения мы будем считать, что $\mathbb{Z}_K = \mathbb{Z}[\theta]$ и, что $\mathbb{Z}[\theta]$ есть кольцо главных идеалов.

Пусть $m \in \mathbb{Z}$ удовлетворяет сравнению $T(m) \equiv 0 \pmod N$. Определим отображение

$$\varphi : \ \mathbb{Z}[\theta] \to \mathbb{Z}/N\mathbb{Z}, \tag{5.13}$$

положив $\varphi(\alpha)$ для каждого $\alpha = f(\theta) \in \mathbb{Z}_K$ равным $f(m) \pmod N$. Таким образом

$$\varphi(\alpha) = f(m) \pmod N.$$

Это отображение не зависит от представления $\alpha = f(\theta)$. Действительно, если $\alpha = g(\theta), g(x) \in \mathbb{Z}[x]$, то $f(\theta) - g(\theta) = 0$ и, следовательно,

$$f(x) - g(x) = T(x)u(x), \qquad u(x) \in \mathbb{Z}[x].$$

Подставляя в последнее равенство $x = m$, находим

$$f(m) - g(m) = T(m)u(m) \equiv 0 \pmod N.$$

Значит, $f(m) \pmod N = g(m) \pmod N$ и отображение (5.13) не зависит от выбора представления $\alpha = f(\theta)$. Так как для каждого $\overline{a} = a \pmod N, a \in \mathbb{Z}$, имеем $\varphi(a) = \overline{a}$, то φ есть отображение "на". Кроме того, из определения и доказанного следует, что φ есть гомоморфизм.

Отображение φ может быть использовано для разложения N на множители следующим образом. Предположим, что найдены такие целые числа a, b, что

$$\alpha = a + b\theta = \beta^2, \quad \beta \in \mathbb{Z}[\theta], \qquad a + bm = x^2, \quad x \in \mathbb{Z}.$$

Обозначив $\varphi(\beta) = y \pmod N$, где $y \in \mathbb{Z}$, находим

$$x^2 = a + bm \equiv \varphi(a + b\theta) = \varphi(\beta)^2 \equiv y^2 \pmod N.$$

Тогда наибольший общий делитель $(x - y, N)$ может быть нетривиальным делителем N.

На практике для нахождения таких чисел a, b используются базы множителей и решето.

Первая база множителей $\mathfrak{B}_1$ состоит из простых чисел p, не превосходящих некоторой границы B, т.е. $p \leqslant B$. Она используется для разложения на множители целых чисел $a + bm$.

Теперь опишем вторую базу множителей, которая используется для разложения алгебраических чисел.

Напомним, что по предположению $\mathbb{Z}_K$ есть кольцо главных идеалов. Поэтому каждый простой идеал состоит из чисел, делящихся на некоторое число $g \in \mathbb{Z}_K$, то есть $\mathfrak{p} = (g)$. Обозначим буквой G множество всех образующих g простых идеалов $\mathfrak{p}$ вида $(p, \theta - c), c \in \mathbb{Z}$, где $p \leqslant B$. Совокупность таких идеалов можно построить с помощью теоремы 1.33, отобрав в разложении (1.45) простые идеалы $\mathfrak{p}_j$ с условием $f_j = 1$. А образующую g простого идеала $\mathfrak{p} = (p, \theta - c)$ можно найти в виде $g = h(\theta), h(x) \in \mathbb{Z}[x]$, где многочлен $h(x)$ выбирается так, чтобы выполнялись условия

$$\deg h(x) < \deg T(x), \qquad h(c) \equiv 0 \pmod{p}, \qquad |N(g)| = p. \quad (5.14)$$

Тогда из неравенств $p = N(\mathfrak{p}) \leqslant N((g)) = |N(g)| = p$ следует, что $(g) = \mathfrak{p}$. Многочлен $h(x)$ можно найти перебирая его целые коэффициенты в некоторой ограниченной области и проверяя условия (5.14).

Вторая база множителей $\mathfrak{B}_2$ состоит из элементов множества G и так называемых фундаментальных единиц поля K. Напомним, что единицами называются обратимые элементы кольца целых чисел $\mathbb{Z}_K$. Согласно теореме Дирихле о единицах мультипликативная группа единиц поля K конечно порождена. Элементы ее базиса $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r$ называются *фундаментальными единицами* поля K.

Пусть $\alpha \in \mathbb{Z}[\theta]$. Тогда главный идеал (α) единственным способом раскладывается в конечное произведение простых идеалов

$$(\alpha) = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_s^{v_s}, \qquad v_j \geqslant 1. \quad (5.15)$$

Если $\alpha = a + b\theta, (a, b) = 1$, и $\mathfrak{p}$ — простой идеал, входящий в разложение (5.15), то $\alpha \in \mathfrak{p}$ и, значит, $a + b\theta \equiv 0 \pmod{\mathfrak{p}}$. Как известно, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, где p — некоторое простое число. Если $p|b$, то $b \in \mathfrak{p}$. Но тогда $a \in \mathfrak{p}$ и, следовательно $p|a$. Но это невозможно, так как $(a, b) = 1$. Значит, $p \nmid b$, и существует целое число c, удовлетворяющее сравнению

$$0 \equiv a + b\theta \pmod{\mathfrak{p}} \equiv b(\theta - c) \pmod{\mathfrak{p}}.$$

Поскольку $b \notin \mathfrak{p}$, отсюда следует, что $\theta - c \in \mathfrak{p}$ и, значит, $\mathfrak{p} = (p, \theta - c)$.

Если норма $N(a+b\theta)$ раскладывается в произведение простых чисел $p \leqslant B$, то из сказанного следует, что в произведении (5.15) присутствуют только простые идеалы, образующие которых лежат в множестве G. Равенство (5.15) может быть переписано в виде

$$(\alpha) = \left(\prod_{g \in G} g^{v_g} \right), \qquad v_g \in \mathbb{Z}, \quad v_g \geqslant 0.$$

Так как любые две образующие одного и того же идеала отличаются обратимым множителем, то есть единицей, то последнее равенство идеалов может быть переписано в виде

$$\alpha = \varepsilon_0^{k_0} \varepsilon_1^{k_1} \cdots \varepsilon_r^{k_r} \prod_{g \in G} g^{v_g}.$$

Применяя к этому равенству гомоморфизм (5.13), находим

$$a + mb \equiv \varphi(\alpha) \equiv \varphi(\varepsilon_0)^{k_0} \varphi(\varepsilon_1)^{k_1} \cdots \varphi(\varepsilon_r)^{k_r} \prod_{g \in G} \varphi(g)^{v_g} \pmod{N}.$$

Если числа a, b таковы, что $a + mb$ есть B-гладкое число, то

$$a + mb = \prod_{p \leqslant B} p^{w_p}, \qquad w_p \in \mathbb{Z}, \quad w_p \geqslant 0.$$

Имеет место сравнение

$$\prod_{p \in \mathfrak{B}_1} p^{w_p} \equiv \varphi(\varepsilon_0)^{k_0} \varphi(\varepsilon_1)^{k_1} \cdots \varphi(\varepsilon_r)^{k_r} \prod_{g \in G} \varphi(g)^{v_g} \pmod{N}. \qquad (5.16)$$

Подобное сравнение можно получить для каждой пары чисел a, b с условием, что числа $a + bm$ и $N(a + b\theta)$ раскладываются в произведение простых $p \leqslant B$. Найти их можно с помощью алгоритма просеивания, примененного при каждом фиксированном целом b из некоторой ограниченной области, и многочленам $f_1(x) = x + bm, f_2(x) = N(x + b\theta)$.

Если в результате просеивания будет найдено более, чем $|\mathfrak{B}_1|+|\mathfrak{B}_2|$ сравнений (5.16), то работая с векторами $(w_p, k_j, v_g)_{p\in\mathfrak{B}_1, g\in G}$ подобно тому, как это объяснялось в связи с алгоритмом Диксона, можно скомбинировать соотношения (5.16) так, что получится сравнение $x^2 \equiv y^2 \pmod N$. С его помощью можно пытаться разложить N на множители.

Пример. Покажем, как описанный выше алгоритм использовался для разложения на простые множители числа Ферма $N = F_9 = 2^{512}+1$. Положим $m = 2^{205}$, тогда

$$m^5 - 2 = 2^{1025} - 2 = 2(2^{1024}-1) = 2(2^{512}-1)(2^{512}+1) \equiv 0 \pmod N.$$

Положим $K = \mathbb{Q}(\sqrt[5]{2})$. Можно доказать, что кольцо целых чисел этого поля имеет вид $\mathbb{Z}[\theta]$, $\theta = \sqrt[5]{2}$, и что это кольцо с однозначным разложением элементов на простые сомножители. Фундаментальные единицы поля K имеют вид $\varepsilon_1 = \theta - 1, \varepsilon_2 = 1 + \theta + \theta^3$ и, кроме того, $\varepsilon_0 = -1$.

В алгоритме для разложения использовались примерно 99500 простых идеалов $\mathfrak{p} = (p, \theta - c)$ с $p \leqslant 1294973$.

Если для разложения числа на множители используется сравнительно небольшое числовое поле, обычно это случается для чисел имеющих специальную структуру, как F_9, то соответствующий алгоритм называют специальным решетом числового поля (SNFS). Если же раскладываемое число не имеет каких-либо особенностей, позволяющих выбрать простое поле K, то возникают трудности, связанные с вычислением кольца целых чисел, фундаментальных единиц, образующих идеалов и т.п.. Тем не менее существует алгоритм, который может быть использован и в этой более сложной ситуации. Его называют общим алгоритмом решета числового поля (GNFS).

Глава 6

Дискретное логарифмирование

Пусть G — конечная абелева группа, $a, b \in G$. Задача дискретного логарифмирования состоит в том, чтобы выяснить, будет ли справедливо включение $b \in \langle a \rangle \subseteq G$ и, в случае справедливости, найти целое число $k \in \mathbb{Z}$, $0 \leqslant k < d = \operatorname{ord} a$, удовлетворяющее равенству

$$a^k = b.$$

В простейшем и наиболее важном случае $G = (\mathbb{Z}/p\mathbb{Z})^*$, где p — большое простое число, речь идет о разрешимости сравнения

$$a^x \equiv b \pmod{p}. \tag{6.1}$$

Если a — первообразный корень по модулю p, то сравнение (6.1) для b, не делящихся на p, всегда разрешимо. При этом найдется решение, удовлетворяющее неравенству $0 \leqslant x < p - 1$. Наименьшее целое неотрицательное число x, удовлетворяющее соотношению (6.1), называется *индексом* или *дискретным логарифмом* числа b по основанию a и обозначается $\operatorname{Log}_a b$ или просто $\operatorname{Log} b$, если из контекста ясно, по какому основанию берется логарифм.

Задача вычисления $a^x \bmod p$ (так мы будем обозначать остаток от деления числа a^x на p) по заданному x решается за $O(\log p)$ арифметических операций. Обратная задача — решение сравнения (6.1) — сложна и лучшие из известных алгоритмов ее решения, связанные с решетом числового поля требуют $O(\exp(c(\ln p)^{1/3}(\ln \ln p)^{2/3}))$ арифметических операций.

6.1 Метод Гельфонда.

Излагаемый здесь метод решения сравнения (6.1) требует $O(p^{1/2}\ln p)$ арифметических операций. В зарубежной литературе он называется "методом больших и малых шагов".

Лемма 6.1. *Пусть p — простое нечетное число и пусть $H = [\sqrt{p}]+1$. Тогда для каждого целого числа d, $1 \leqslant d < p$, найдутся целые числа u, v, удовлетворяющие условиям*

$$1 \leqslant u, v \leqslant H, \qquad Hu - v = d.$$

Доказательство. Положим

$$u = \left[\frac{d}{H}\right] + 1, \qquad v = Hu - d.$$

Тогда

$$\frac{d}{H} < u \leqslant \frac{d}{H} + 1,$$

откуда видим, что, во–первых,

$$0 < u < \frac{p}{\sqrt{p}} + 1 = \sqrt{p} + 1,$$

а во–вторых, $0 < Hu - d \leqslant H$. Остается воспользоваться тем, что числа u и v целые. □

Алгоритм 6.1. Данные: *Простое число $p \geqslant 3$, первообразный корень a по модулю p, число $b \in \mathbb{Z}$, $p \nmid b$.*
Найти: *Решение сравнения* (6.1).
1. Вычислить $H = [\sqrt{p}] + 1$.
2. Положить $c = a^H \bmod p$.
3. Составить два набора чисел

$$S_1 = \{c^u \bmod p : 1 \leqslant u \leqslant H\}, \quad S_2 = \{ba^v \bmod p : 1 \leqslant v \leqslant H\}.$$

4. Упорядочить по возрастанию оба набора S_1 и S_2. Найти совпавшие элементы этих наборов, то есть такие числа u, v, для которых

$$c^u \equiv ba^v \pmod{p}. \tag{6.2}$$

5. Положить

$$\operatorname{Log} b = Hu - v. \tag{6.3}$$

Пересечение множеств S_1 и S_2 не пусто, так как сравнение (6.2) равносильно представлению (6.3), а последнее, согласно лемме 6.1, существует всегда.

Вычисления в пунктах 1 и 2 требуют $O(\ln p)$ арифметических операций. Вычисления в пункте 3 требуют $O(H \ln p) = O(\sqrt{p} \ln p)$ арифметических операций. Для упорядочения каждого из множеств S_1, S_2 нужно $O(H \ln H) = O(\sqrt{p} \ln p)$ арифметических операций. Для нахождения одинаковых элементов в упорядоченных множествах S_1, S_2 нужно $O(H) = O(\sqrt{p})$ арифметических операций. Общее же количество операций в алгоритме Гельфонда равно $O(\sqrt{p} \ln p)$.

6.2 Метод Полига–Хеллмана.

Пусть помимо того, что a — первообразный корень по модулю p, известно еще разложение на простые множители числа $p-1$:

$$p - 1 = \prod_{i=1}^{r} q_i^{k_i}.$$

Излагаемый в данном пункте алгоритм Полига–Хеллмана [1] находит $x \bmod q_i^{k_i}$, $i = 1, \ldots, r$, для x, удовлетворяющего сравнению (6.1). Затем по китайской теореме об остатках восстанавливается x.

Лемма 6.2. *Пусть q — простое число, $q \mid p-1$. Тогда любое решение сравнения*

$$x^q \equiv 1 \pmod{p} \tag{6.4}$$

сравнимо по модулю p с одним из чисел $1, c, c^2, \ldots, c^{q-1}$, где

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

При этом указанные выше числа различны по модулю p.

[1] Этот алгоритм независимо был открыт В.И. Нечаевым.

Доказательство. Каждое из чисел $1, c, c^2, \ldots, c^{q-1}$ является решением сравнения (6.4), так как для любого целого k

$$(c^k)^q \equiv a^{\frac{p-1}{q}kq} \equiv (a^{p-1})^k \equiv 1 \pmod{p}.$$

При этом сравнение (6.4) не может иметь больше, чем q корней по модулю p, поскольку $\mathbb{Z}/p\mathbb{Z}$ — поле. Стало быть, достаточно доказать, что вычеты $c^k \bmod p$, $0 \leqslant k \leqslant q-1$, попарно различны.

Пусть d — порядок c по модулю p. Тогда

$$1 \equiv c^d \equiv a^{\frac{p-1}{q}d} \pmod{p},$$

причем $\frac{p-1}{q}d$ — целое число. Но порядок a по модулю p равен $p-1$, то есть для некоторого целого $v \neq 0$ выполняется равенство $\frac{p-1}{q}d = (p-1)v$. Следовательно, $d = qv \geqslant q$, откуда видим, что вычеты $c^k \bmod p$, $0 \leqslant k \leqslant q-1$, действительно попарно различны. □

Если q невелико, то лемма 6.2 дает быстрый способ нахождения всех решений сравнения (6.4). Число c находится за $O(\ln p)$ арифметических операций, упорядоченный набор решений при известном c — за $O(q \ln q)$ арифметических операций.

Пусть далее $p-1 = q^k h$, $q \nmid h$. Алгоритм Полига–Хеллмана последовательно строит числа u_j, $1 \leqslant j \leqslant k$, такие что

$$(b^h a^{-hu_j})^{q^{k-j}} \equiv 1 \pmod{p}. \tag{6.5}$$

Покажем, что такие числа u_j действительно существуют. При $j = 0$ можно положить $u_0 = 0$, так как в этом случае соотношение (6.5) имеет вид

$$b^{hq^k} \equiv 1 \pmod{p}.$$

Предположим теперь, что при некотором $j \geqslant 0$ число u_j удовлетворяет соотношению (6.5). Тогда по лемме 6.2 найдется такое t, $0 \leqslant t < q$, что выполняется сравнение

$$(b^h a^{-hu_j})^{q^{k-j-1}} \equiv c^t \pmod{p}.$$

Если теперь положить $u_{j+1} = u_j + tq^j$, то получим, что

$$(b^h a^{-hu_{j+1}})^{q^{k-j-1}} \equiv (b^h a^{-hu_j})^{q^{k-j-1}} a^{-thq^{k-1}} \equiv 1 \pmod{p}.$$

Таким образом, числа u_j существуют и их можно находить при помощи леммы 6.2.

При $j = k$ сравнение (6.5) принимает вид

$$b^h a^{-hu_k} \equiv 1 \pmod{p}$$

или, что то же самое,

$$a^{h(\operatorname{Log} b - u_k)} \equiv 1 \pmod{p}.$$

Это значит, что $p - 1 = q^k h \mid h(\operatorname{Log} b - u_k)$, то есть

$$\operatorname{Log} b \equiv u_k \pmod{q^k}.$$

Тем самым мы обосновали следующий алгоритм:

Алгоритм 6.2. Данные: *Простое число $p \geqslant 3$ и простое число q, такое что $p - 1 = q^k h$, $k \geqslant 1$, $q \nmid h$.*
Найти: *Целое число u, такое что $x \equiv u \pmod{q^k}$, где x — решение сравнения* (6.1).
1. Вычислить $c = a^{hq^{k-1}} \bmod p$. Положить $u_0 = 0$, $j = 0$.
2. При помощи леммы 6.2 найти число t, $0 \leqslant t \leqslant q - 1$, удовлетворяющее сравнению

$$(b^h a^{-hu_j})^{q^{k-j-1}} \equiv c^t \pmod{p}. \tag{6.6}$$

3. Положить $u_{j+1} = u_j + tq^j$ и увеличить j на единицу.
4. Если $j < k$, перейти в пункт 2. Если $j = k$, положить $u = u_j$. СТОП.

Предположим, что число $p - 1$ является B–гладким, то есть

$$p - 1 = \prod_{i=1}^{r} q_i^{k_i}, \qquad q_i \leqslant B.$$

Тогда количество арифметических операций, требуемое для решения сравнения (6.1) при помощи алгоритма 6.2 можно оценить следующим образом. Для вычисления $x \bmod q_i^{k_i}$ при фиксированном i требуется $O(\ln p + k_i q_i \ln q_i)$ арифметических операций (один раз находится число c в пункте 1 алгоритма 6.2 и k_i раз решается сравнение (6.6) в пункте 2 алгоритма 6.2). Следовательно, для нахождения всех вычетов $x \bmod q_i^{k_i}$, $i = 1, \ldots, r$, требуется

$$O\left(r \ln p + \sum_{i=1}^{r} k_i q_i \ln q_i\right)$$

арифметических операций, что, в силу неравенств

$$r \leqslant \max_{1 \leqslant i \leqslant r} q_i \leqslant B$$

и

$$\sum_{i=1}^{r} k_i q_i \ln q_i \leqslant B \sum_{i=1}^{r} k_i \ln q_i = B \ln(p-1),$$

оценивается величиной $O(B \ln p)$. Применение китайской теоремы об остатках требует $O(\ln p)$ операций, стало быть, сравнение (6.1) описанным способом решается за $O(B \ln p)$ арифметических операций.

Таким образом, алгоритм Полига–Хеллмана эффективен, если $p-1$ является произведением степеней маленьких простых чисел.

6.3 Линейное решето.

Положим

$$L = \exp((\ln p \ln \ln p)^{1/2}).$$

В данном пункте мы опишем алгоритм Копперсмита–Одлыжко – Шреппеля решения сравнения (6.1), использующий линейное решето. Эвристические соображения позволяют предположить, что данный алгоритм требует $O(L)$ арифметических операций.

Если a_1 и a_2 — два первообразных корня по модулю p, то логарифмы числа b по основаниям a_1 и a_2 связаны соотношением

$$\operatorname{Log}_{a_1} b \equiv \operatorname{Log}_{a_2} a_1 \operatorname{Log}_{a_1} b \pmod{p-1}. \tag{6.7}$$

Если есть алгоритм, вычисляющий дискретные логарифмы по основанию a_2, то формула (6.7) позволяет вычислять логарифмы по основанию a_1. Следовательно, задачу логарифмирования достаточно решить по какому–нибудь основанию. Из расширенной гипотезы Римана следует, что минимальный первообразный корень по модулю p имеет порядок $O(\ln^2 p)$. Поэтому далее в этом пункте мы будем считать, что в сравнении (6.1) число a достаточно мало, а именно,

$$a < L^{1/2}. \tag{6.8}$$

Выберем $\varepsilon > 0$ и положим

$$H = [\sqrt{p}] + 1, \qquad J = H^2 - p.$$

Определим базу множителей $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$:

$$\mathcal{B}_1 = \left\{ q \in \mathbb{Z} \,\middle|\, q \text{ — простое, } q < L^{1/2} \right\},$$
$$\mathcal{B}_2 = \left\{ H + c \in \mathbb{Z} \,\middle|\, 0 < c < L^{1/2+\varepsilon} \right\}.$$

Алгоритм состоит из нескольких этапов.

Этап I. Построение мультипликативных соотношений по модулю p между элементами базы.

Если $H + c_1, H + c_2 \in \mathcal{B}_2$, то

$$(H + c_1)(H + c_2) \equiv J + (c_1 + c_2)H + c_1 c_2 \pmod{p}. \tag{6.9}$$

Величина справа есть $O(p^{1/2+\varepsilon/2})$, так как $L^{1/2+\varepsilon} < p^{\varepsilon/2}$. На данном этапе алгоритма с помощью просеивания по c_2 при каждом фиксированном c_1 находятся такие пары (c_1, c_2), что число $f(c_2) = J + (c_1 + c_2)H + c_1 c_2$ будет $L^{1/2}$–гладким.

Таких пар будет довольно много. Из результатов о распределении чисел заданной гладкости следует, что доля $L^{1/2}$–гладких чисел на интервале $(0, p^{1/2+\varepsilon/2})$, не меньше, чем $L^{-1/2-\varepsilon/2}$. Количество пар (c_1, c_2),

таких что $H+c_1, H+c_2 \in \mathcal{B}_2$, равно $O(L^{1+2\varepsilon})$. Поэтому можно считать, что количество пар (c_1, c_2), для которых величина справа в (6.9) является $L^{1/2}$–гладким числом, равно $O(L^{-1/2-\varepsilon/2}L^{1+2\varepsilon}) = O(L^{1/2+3\varepsilon/2})$.

Для каждой такой пары справедливо соотношение

$$(H + c_1)(H + c_2) \equiv \prod_{q \in \mathcal{B}_1} q^{r_q} \pmod{p}$$

или, что то же самое,

$$\operatorname{Log}_a(H + c_1) + \operatorname{Log}_a(H + c_2) \equiv \sum_{q \in \mathcal{B}_1} r_q \operatorname{Log}_a q \pmod{p-1}.$$

Это однородное линейное соотношение по модулю $p-1$ между логарифмами элементов множества $\mathcal{B}$.

Кроме того, поскольку мы предположили в начале, что $a < L^{1/2}$, то есть a раскладывается по базе $\mathcal{B}_1$, равенство

$$\operatorname{Log}_a a = 1 \tag{6.10}$$

дает неоднородное линейное соотношение между логарифмами элементов множества $\mathcal{B}_1$.

Таким образом, соотношения, получаемые в результате просеивания, вместе с неоднородным соотношением (6.10) образуют неоднородную систему линейных уравнений относительно логарифмов элементов множества $\mathcal{B}$, в которой количество уравнений больше количества переменных (так как $L^{1/2+3\varepsilon/2} > L^{1/2+\varepsilon}$). Эта система заведомо имеет решение и считается, что, как правило, единственное. При этом количество ненулевых коэффициентов в каждом уравнении есть $O(\ln p)$, поскольку количество делителей у любого натурального числа, не превосходящего p, есть $O(\ln p)$. То есть полученная система будет сильно разреженной, что позволяет для ее решения применять специальные методы, намного более эффективные, чем обычный метод исключения Гаусса. Так находятся логарифмы всех элементов базы множителей.

Этап II. Построение мультипликативного соотношения по модулю p между a, b и элементами расширенной базы.

На этом этапе, выбирая случайным образом целое число w, нужно найти такое, что остаток от деления $a^w b$ на p будет L^2–гладким числом, то есть будет справедливо сравнение

$$a^w b \equiv \prod_{q \in \mathcal{B}_1} q^{l_q} \prod_{u \in \mathcal{B}_3} u^{k_u} \pmod{p}, \tag{6.11}$$

где

$$\mathcal{B}_3 = \left\{ q \in \mathbb{Z} \,\middle|\, q \text{ — простое, } L^{1/2} \leqslant q < L^2 \right\}.$$

Из вероятностных соображений и результатов о распределении чисел заданной гладкости следует, что такое w можно найти в среднем не более, чем за $L^{1/4}$ попыток.

Этап III. Вычисление логарифмов элементов расширенной базы.

Пусть u — простое число, $L^{1/2} \leqslant u < L^2$. Для этого u нужно выбрать случайным образом такое число y, что

$$\begin{cases} \left| y - \dfrac{\sqrt{p}}{u} \right| \leqslant L^{1/2} \\ y \text{ является } L^{1/2}\text{–гладким числом.} \end{cases}$$

Затем случайным образом нужно выбрать такое число $v \in \mathcal{B}_2$, что

$$\begin{cases} |v - \sqrt{p}| \leqslant L^{1/2} \\ vyu - p \text{ является } L^{1/2}\text{–гладким числом.} \end{cases}$$

Тогда

$$vyu - p = vu \left| y - \frac{\sqrt{p}}{u} \right| + \sqrt{p}\big(v - \sqrt{p}\big)$$

и

$$|vyu - p| \leqslant |v| L^2 L^{1/2} + p^{1/2} L^{1/2} = O(p^{1/2} L^{5/2}).$$

Вероятности выбрать подходящие y и v также оцениваются при помощи результатов о распределении чисел заданной гладкости.

Для выбранных y и v справедливо равенство

$$vyu - p = \prod_{q \in \mathcal{B}_1} q^{s_q}$$

или, что то же самое,

$$\operatorname{Log}_a v + \operatorname{Log}_a y + \operatorname{Log}_a u \equiv \sum_{q \in \mathcal{B}_1} s_q \operatorname{Log}_a q \pmod{p-1}.$$

Из этого соотношения можно найти $\operatorname{Log}_a u$, так как все остальные логарифмы известны.

Этап IV. Непосредственное вычисление $\operatorname{Log}_a b$.

Из сравнения (6.11) получаем

$$w + \operatorname{Log}_a b \equiv \sum_{q \in \mathcal{B}_1} l_q \operatorname{Log}_a q + \sum_{u \in \mathcal{B}_3} k_u \operatorname{Log}_a u \pmod{p-1}.$$

Данное соотношение позволяет найти $\operatorname{Log}_a b$.

Глава 7

LLL-алгоритм и его применения

7.1 Решетки.

7.1.1 Основные понятия.

В данной главе понятие решетки, основного объекта геометрии чисел, занимает ключевое место.

Определение 7.1. *Подмножество* Λ *пространства* $\mathbb{R}^n$ *называется* k–мерной решеткой, *если*

(а) Λ — *группа по сложению;*

(б) Λ — *дискретное подмножество* $\mathbb{R}^n$, *то есть существует такое* $\varepsilon > 0$, *что расстояние между любыми двумя точками множества* Λ *больше, чем* ε.

(в) минимальное (по включению) подпространство $\mathbb{R}^n$, *содержащее* Λ, *имеет размерность* k.

Примеры:

1. Рассмотрим множество $\mathbb{Z}^n$ точек пространства $\mathbb{R}^n$ с целыми координатами:

$$\mathbb{Z}^n = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_i \in \mathbb{Z},\ i = 1, \ldots, n\}.$$

Это будет решетка, называющаяся *стандартной* n*–мерной целочисленной решеткой.*

2. Пусть $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$ — произвольные n линейно независимых векторов. Тогда множество всех их целочисленных линейных комбинаций

$$\mathrm{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \Big\{ \sum_{i=1}^{n} \lambda_i \mathbf{b}_i \;\Big|\; \lambda_i \in \mathbb{Z},\ i = 1, \ldots, n \Big\}$$

образует n–мерную решетку. Последнее равенство есть определение множества $\mathrm{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

3. Пусть $L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})$ — произвольные n линейно независимых линейных форм на пространстве $\mathbb{R}^n$. Тогда множество

$$\big\{ \big(L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})\big) \in \mathbb{R}^n \;\big|\; \mathbf{x} \in \mathbb{Z}^n \big\}$$

является n–мерной решеткой.

4. Пусть n — некоторое фиксированное целое неотрицательное число. Поставим в соответствие каждому многочлену $a_0 + a_1 x + \ldots + a_n x^n$ с действительными коэффициентами точку $(a_0, a_1, \ldots, a_n)$ пространства $\mathbb{R}^{n+1}$. Тогда прообразом при этом соответствии решетки $\mathbb{Z}^{n+1}$ будет множество

$$\mathbb{Z} + \mathbb{Z}x + \ldots + \mathbb{Z}x^n$$

многочленов над $\mathbb{Z}$ степени, не превосходящей n, которое, таким образом, тоже можно считать $(n+1)$–мерной решеткой.

В дальнейшем, для определенности все рассматриваемые нами векторы будут некоторыми вектор-столбцами.

Определение 7.2. *Набор* $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *линейно независимых векторов решетки* Λ *называется* базисом *этой решетки, если* $\Lambda = \mathrm{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

Теорема 7.1. *Любая* n*–мерная решетка* $\Lambda \subset \mathbb{R}^n$ *обладает базисом, состоящим из* n *векторов.*

Доказательство. Будем доказывать теорему индукцией по n. Для $n = 1$ утверждение очевидно: в качестве $\mathbf{b}_1$ нужно взять самый короткий вектор решетки Λ, существование которого следует из группового свойства и дискретности решетки.

Предположим, что $n \geqslant 2$ и любая $(n-1)$–мерная решетка обладает базисом. Рассмотрим произвольные n линейно независимых векторов $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ решетки Λ. Обозначим через L пространство размерности $(n-1)$, натянутое на вектора $\mathbf{b}'_1, \ldots, \mathbf{b}'_{n-1}$. Множество $\Lambda \cap L$ является $(n-1)$–мерной подрешеткой решетки Λ. По предположению индукции она обладает базисом $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}$.

Рассмотрим подрешетку

$$\Lambda' = \operatorname{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}, \mathbf{b}'_n)$$

решетки Λ и полуоткрытый параллелепипед

$$P = \Big\{ \sum_{i=1}^{n-1} \lambda_i \mathbf{b}_i + \lambda_n \mathbf{b}'_n \;\Big|\; 0 \leqslant \lambda_i < 1,\ i = 1, \ldots, n \Big\}.$$

Решетка Λ' является подгруппой решетки Λ, поэтому Λ распадается в объединение смежных классов по Λ'. Векторы $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}, \mathbf{b}'_n$ образуют базис пространства $\mathbb{R}^n$, следовательно, каждая точка этого пространства принадлежит ровно одному параллелепипеду вида $P + \mathbf{v}$, где $\mathbf{v} \in \Lambda'$. То есть

$$\mathbb{R}^n = \bigsqcup_{\mathbf{v} \in \Lambda'} (P + \mathbf{v}). \tag{7.1}$$

Стало быть, параллелепипед P содержит ровно по одному представителю каждого из смежных классов Λ по Λ'.

Если кроме точки $\mathbf{0}$ в параллелепипеде P точек решетки Λ нет, то количество смежных классов решетки Λ по подрешетке Λ' равно 1 и, стало быть, $\Lambda' = \Lambda$. В этом случае шаг индукции доказан.

Предположим теперь, что в параллелепипеде P есть отличные от 0 точки решетки Λ. При этом

$$P \cap \Lambda \cap L = \{\mathbf{0}\}, \tag{7.2}$$

поскольку векторы $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}$ по предположению индукции образуют базис решетки $\Lambda \cap L$. Параллелепипед P ограничен, поэтому

содержит лишь конечное число точек решетки Λ. Выберем из них ближайшую к пространству L точку $\mathbf{b}_n$, отличную от $\mathbf{0}$. Тогда расстояние от любой точки $\mathbf{a} \in \Lambda \backslash L$ до пространства L не меньше, чем расстояние от $\mathbf{b}_n$ до L, так как иначе в силу (7.1) в множестве $\mathbf{a} + \Lambda'$ найдется точка, лежащая в P и находящаяся ближе к пространству L, чем $\mathbf{b}_n$. Отсюда, учитывая (7.2), получаем, что

$$\Lambda \cap \Big\{ \sum_{i=1}^{n} \lambda_i \mathbf{b}_i \;\Big|\; 0 \leqslant \lambda_i < 1,\ i = 1, \ldots, n \Big\} = \{\mathbf{0}\}.$$

Следовательно, индекс подрешетки $\operatorname{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ решетки Λ равен 1, то есть эти решетки совпадают. □

Базис решетки определен неоднозначно. Более того, имеет место следующее предложение, которое легко вывести из определения 7.2:

Предложение 7.1. *Пусть $\Lambda \subset \mathbb{R}^n$ — решетка с базисом $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Тогда набор векторов $\{\mathbf{b}'_1, \ldots, \mathbf{b}'_n\}$ является базисом решетки Λ в том и только том случае, если он является образом набора $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ при действии некоторого линейного оператора, матрица которого в базисе $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ целочисленна и имеет определитель ± 1.*

Определение 7.3. *Если $\Lambda \subset \mathbb{R}^n$ — решетка с базисом $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, то величина*

$$\det \Lambda = |\det(\mathbf{b}_1, \ldots, \mathbf{b}_n)|$$

называется определителем *решетки Λ.*

Здесь присутствует определитель матрицы, составленной из координат векторов $\mathbf{b}_i$, рассматриваемых как вектор-столбцы.

Из предложения 7.1 видно, что величина $|\det(\mathbf{b}_1, \ldots, \mathbf{b}_n)|$ не зависит от базиса решетки, то есть определение 7.3 корректно. Определитель решетки имеет также очевидный геометрический смысл: он равен объему параллелепипеда

$$\Big\{ \sum_{i=1}^{n} \lambda_i \mathbf{b}_i \;\Big|\; 0 \leqslant \lambda_i \leqslant 1,\ i = 1, \ldots, n \Big\},$$

натянутого на базисные векторы. Все такие параллелепипеды называется *фундаментальными параллелепипедами* решетки. Получаем

Предложение 7.2. *Объем любого фундаментального параллелепипеда решетки равен ее определителю.*

Отметим еще одно свойство определителя решетки, которое нам понадобится в дальнейшем. Пусть, как и прежде, $\Lambda \subset \mathbb{R}^n$ — n–мерная решетка с базисом $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Рассмотрим так называемую *матрицу Грама* векторов $\mathbf{b}_1, \ldots, \mathbf{b}_n$:

$$\Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \begin{pmatrix} \langle \mathbf{b}_1, \mathbf{b}_1 \rangle & \langle \mathbf{b}_1, \mathbf{b}_2 \rangle & \cdots & \langle \mathbf{b}_1, \mathbf{b}_n \rangle \\ \langle \mathbf{b}_2, \mathbf{b}_1 \rangle & \langle \mathbf{b}_2, \mathbf{b}_2 \rangle & \cdots & \langle \mathbf{b}_2, \mathbf{b}_n \rangle \\ \cdots & \cdots & \cdots & \cdots \\ \langle \mathbf{b}_n, \mathbf{b}_1 \rangle & \langle \mathbf{b}_n, \mathbf{b}_2 \rangle & \cdots & \langle \mathbf{b}_n, \mathbf{b}_n \rangle \end{pmatrix},$$

где через $\langle \mathbf{b}_i, \mathbf{b}_j \rangle$ обозначено евклидово скалярное произведение векторов $\mathbf{b}_i, \mathbf{b}_j$.

Теорема 7.2. $\det \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_n) = (\det \Lambda)^2$.

Доказательство. Обозначим через B матрицу базиса $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ (то есть для каждого $i = 1, \ldots, n$ столбец матрицы с номером i состоит из координат вектора $\mathbf{b}_i$). Тогда, как легко видеть, $\Gamma = \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_n) = B^\top B$. Следовательно,

$$\det \Gamma = (\det B)^2 = (\det \Lambda)^2.$$

□

Рассмотрим теперь какую–нибудь k–мерную решетку при $k < n$, к примеру, решетку Λ_k, натянутую на векторы $\mathbf{b}_1, \ldots, \mathbf{b}_k$:

$$\Lambda_k = \mathrm{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_k).$$

Говорить об определителе матрицы, составленной из координат этих векторов нельзя, поскольку она не является квадратной, однако это не мешает нам говорить об определителе решетки Λ_k. Действительно,

можно изометрично отобразить k–мерное подпространство пространства $\mathbb{R}^n$, содержащее Λ_k, на $\mathbb{R}^k$. Тогда образы векторов $\mathbf{b}_1, \ldots, \mathbf{b}_k$ при этом отображении будут k–мерными векторами, модуль определителя которых мы и будем считать определителем решетки Λ_k. Если же теперь воспользоваться предложением 7.2 и тем фактом, что изометрия сохраняет объем, то можно под определителем решетки Λ_k понимать объем k–мерного параллелепипеда, натянутого на векторы $\mathbf{b}_1, \ldots, \mathbf{b}_k$.

С другой стороны, для векторов $\mathbf{b}_1, \ldots, \mathbf{b}_k$ можно также рассмотреть матрицу Грама:

$$\Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_k) = \begin{pmatrix} \langle \mathbf{b}_1, \mathbf{b}_1 \rangle & \langle \mathbf{b}_1, \mathbf{b}_2 \rangle & \cdots & \langle \mathbf{b}_1, \mathbf{b}_k \rangle \\ \langle \mathbf{b}_2, \mathbf{b}_1 \rangle & \langle \mathbf{b}_2, \mathbf{b}_2 \rangle & \cdots & \langle \mathbf{b}_2, \mathbf{b}_k \rangle \\ \cdots & \cdots & \cdots & \cdots \\ \langle \mathbf{b}_k, \mathbf{b}_1 \rangle & \langle \mathbf{b}_k, \mathbf{b}_2 \rangle & \cdots & \langle \mathbf{b}_k, \mathbf{b}_k \rangle \end{pmatrix}.$$

Поскольку изометричное отображение плоскости решетки Λ_k на $\mathbb{R}^k$, рассмотренное выше, сохраняет скалярное произведение, из теоремы 7.2, примененной к образу решетки Λ_k при этом отображении, следует

Теорема 7.3. *Для любой k–мерной решетки*

$$\Lambda_k = \operatorname{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \subset \mathbb{R}^n$$

выполняется $\det \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_k) = (\det \Lambda_k)^2$.

Если рассмотреть все k–мерные подрешетки n–мерной решетки Λ, то окажется, что их определители ограничены снизу некоторой положительной константой, зависящей только от решетки Λ:

Теорема 7.4. *Существует такая константа $c > 0$, зависящая только от Λ, что для любой k–мерной подрешетки Λ' n–мерной решетки Λ выполняется*

$$\det \Lambda' \geqslant c.$$

Доказательство. Пусть Λ' — произвольная k–мерная подрешетка решетки Λ. Поскольку Λ — n–мерная решетка в пространстве $\mathbb{R}^n$, существует такой оператор $A \in \mathrm{GL}_n(\mathbb{R})$, что $A(\Lambda) = \mathbb{Z}^n$. Пусть λ —

максимальное по модулю собственное значение оператора A. Тогда, если P — произвольный фундаментальный параллелепипед решетки Λ', то для объемов k–мерных параллелепипедов P и $A(P)$ имеет место неравенство

$$\mathrm{vol}_k(P) \geqslant |\lambda|^{-k} \mathrm{vol}_k(A(P)),$$

которое следует из того факта, что оператор A растягивает любой отрезок не более, чем в λ раз.

Образ решетки Λ' при действии оператора A — это k–мерная подрешетка решетки $\mathbb{Z}^n$. В силу теоремы 7.3 определитель решетки $A(\Lambda')$ равен корню из некоторого натурального числа, поскольку все элементы матрицы Грама, соответствующей любому базису решетки $A(\Lambda')$, суть целые числа. Стало быть,

$$\det \Lambda' = \mathrm{vol}_k(P) \geqslant |\lambda|^{-k} \mathrm{vol}_k(A(P)) = |\lambda|^{-k} \det(A(\Lambda')) \geqslant |\lambda|^{-k}.$$

Остается положить $c = |\lambda|^{-k}$. □

В случае, когда n–мерная решетка Λ распадается в прямую сумму двух своих подрешеток, ортогональных друг другу, ее определитель равен произведению определителей этих подрешеток:

Теорема 7.5. *Пусть Λ' и Λ'' — подрешетки решетки Λ, содержащиеся в ортогональных друг другу подпространствах $\mathbb{R}^n$, и пусть $\Lambda = \Lambda' \oplus \Lambda''$. Тогда $\det \Lambda = \det \Lambda' \det \Lambda''$.*

Доказательство. Пусть $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ — базис Λ', а $\{\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n\}$ — базис Λ''. Тогда $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ будет базисом решетки Λ, в то время как $\det \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \det \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_k) \det \Gamma(\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n)$, в силу ортогональности векторов $\mathbf{b}_i$ и $\mathbf{b}_j$ при $1 \leqslant i \leqslant k < j \leqslant n$. Остается воспользоваться теоремой 7.3. □

7.1.2 Приведенные базисы.

Пусть задана n–мерная решетка Λ в пространстве $\mathbb{R}^n$. На практике работа с решеткой в большинстве случаев сводится к работе с неко-

торым ее базисом. При этом ясно, что чем меньше по модулю координаты векторов базиса, тем удобнее с ним работать. Самое естественное, что можно сделать в этой ситуации — это ввести какой–нибудь (частичный) порядок на множестве базисов решетки Λ и рассматривать базисы, минимальные относительно этого порядка. Такие базисы называют *приведенными*. Например, можно упорядочить базисы $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ решетки Λ по возрастанию величины $|\mathbf{b}_1|^2 + \ldots + |\mathbf{b}_n|^2$. Базисы, минимальные относительно такого порядка называются *приведенными по Венкову*. Если упорядочивать по возрастанию величины $|\mathbf{b}_1|^2 + \ldots + |\mathbf{b}_n|^2 + |\mathbf{b}_1 + \ldots + \mathbf{b}_n|^2$, получим базисы, *приведенные по Зеллингу*. Однако наиболее часто используемыми являются базисы, приведенные по Минковскому и по Эрмиту. Для того, чтобы дать соответствующие определения, нам понадобится понятие примитивного набора векторов.

Определение 7.4. *Набор* $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ *векторов решетки* Λ, $k \leqslant n$, *называется* примитивным, *если его можно дополнить до базиса решетки* Λ.

Не сложно проверить (см. доказательство теоремы 7.1), что набор $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\} \subset \Lambda$ можно дополнить до базиса решетки тогда и только тогда, когда в полуоткрытом k–мерном параллелепипеде

$$\left\{ \sum_{i=1}^{k} \lambda_i \mathbf{b}_i \;\middle|\; 0 \leqslant \lambda_i < 1,\ i = 1, \ldots, k \right\}$$

нет точек решетки Λ, кроме $\mathbf{0}$. В частности, примитивными векторами решетки Λ называются те векторы, координаты которых в каком–нибудь базисе этой решетки взаимно просты.

Определение 7.5. *Базис* $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *решетки* Λ *называется* приведенным по Минковскому, *если для каждого* $k = 1, \ldots, n$ *и каждого вектора* $\mathbf{b} \in \Lambda$, *такого что набор* $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{b}\}$ *примитивен, выполняется неравенство* $|\mathbf{b}| \geqslant |\mathbf{b}_k|$.

Ясно, что если базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ решетки Λ приведен по Минковскому, то и базис Λ вида $\{\pm\mathbf{b}_1, \ldots, \pm\mathbf{b}_n\}$ также приведен по Минковскому. Однако решетка может иметь существенно различные приведенные по Минковскому базисы. Более того, начиная с размерности $n = 7$, может даже оказаться, что наборы абсолютных величин векторов в этих базисах различны (см. [12], [23]).

Понятие приведенного по Эрмиту базиса вводится при помощи следующего индуктивного определения:

Определение 7.6. 1) *Любой набор, состоящий из одного вектора решетки* Λ*, будем называть* приведенным по Эрмиту*, если этот вектор минимален относительно евклидовой нормы среди всех векторов* Λ*.*

2) *Если* $2 \leqslant k \leqslant n$*, то будем называть примитивный набор* $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ *векторов решетки* Λ приведенным по Эрмиту*, если набор* $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}\}$ *приведен по Эрмиту и для любого примитивного набора векторов* $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{b}\} \subset \Lambda$ *выполняется неравенство* $|\mathbf{b}_k| \leqslant |\mathbf{b}|$*.*

При $k = n$ *получаем* приведенный по Эрмиту *базис решетки* Λ*.*

Как легко видеть, базис решетки Λ, приведенный по Эрмиту, является также приведенным по Минковскому. Обратное, вообще говоря, не верно (см. [12]).

Алгоритмов построения базисов, приведенных по Эрмиту или по Минковскому, сложность которых полиномиально зависит от размерности, на данный момент не существует. Более того, если $\mathcal{P} \neq \mathcal{NP}$, то скорее всего их вообще не существует, ибо если в определениях 7.5 и 7.6 рассматривать не евклидову норму, а норму ℓ_1 или ℓ_∞, то задача построения соответствующих базисов $\mathcal{NP}$–полна (см. пункт 7.3.1).

Однако, как будет показано ниже (в том же пункте 7.3.1), если размерность n фиксирована, то можно за полиномиальное время найти все базисы Λ, приведенные по Минковскому (а, стало быть, и все базисы, приведенные по Эрмиту).

7.1.3 Процесс ортогонализации Грама–Шмидта.

Пусть Λ — n–мерная решетка в $\mathbb{R}^n$ с базисом $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Рассмотрим последовательность подпространств $\{\mathbf{0}\} = L_0 \subset L_1 \subset \ldots \subset L_n = \mathbb{R}^n$, определяемых равенствами

$$\begin{aligned} &L_0 = \{\mathbf{0}\}, \\ &L_i = \operatorname{span}_{\mathbb{R}}(\mathbf{b}_1, \ldots, \mathbf{b}_i), \qquad i = 1, \ldots, n, \end{aligned}$$

где $\operatorname{span}_{\mathbb{R}}(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ означает подпространство, натянутое на векторы $\mathbf{b}_1, \ldots, \mathbf{b}_i$. Будем обозначать через $L_i^{\perp}$ ортогональное дополнение к L_i, а через $\mathbf{b}_i^*$ — ортогональную проекцию вектора $\mathbf{b}_i$ на $L_{i-1}^{\perp}$. Иными словами,

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^* \quad (1 \leqslant i \leqslant n), \tag{7.3}$$

где

$$\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle \quad (1 \leqslant j < i \leqslant n). \tag{7.4}$$

Процесс построения таким образом векторов $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ называется *процессом ортогонализации Грама–Шмидта* базиса $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Набор $\{\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*\}$ является, как легко видеть, ортогональным базисом пространства $\mathbb{R}^n$ с определителем, равным $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Стало быть, имеет место

Теорема 7.6. *Пусть Λ — n–мерная решетка в $\mathbb{R}^n$ с базисом $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ и $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ — векторы, построенные из векторов $\mathbf{b}_1, \ldots, \mathbf{b}_n$ при помощи процесса ортогонализации Грама–Шмидта. Тогда*

$$\det \Lambda = \prod_{i=1}^{n} |\mathbf{b}_i^*|.$$

Из этой теоремы, учитывая, что $|\mathbf{b}_i^*| \leqslant |\mathbf{b}_i|$ для всех i (поскольку $\mathbf{b}_i^*$ — это проекция $\mathbf{b}_i$), получаем неравенство Адамара:

Теорема 7.7 (Неравенство Адамара). *Пусть* Λ *— n–мерная решетка в* $\mathbb{R}^n$ *с базисом* $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. *Тогда*

$$\det \Lambda \leqslant \prod_{i=1}^{n} |\mathbf{b}_i|.$$

Ясно, что в неравенстве Адамара знак равенства можно поставить в том и только том случае, если векторы $\mathbf{b}_1, \ldots, \mathbf{b}_n$ попарно ортогональны. При этом величину $(\prod_{i=1}^{n} |\mathbf{b}_i|)/\det \Lambda$ можно воспринимать как характеристику отклонения базиса $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ решетки Λ от ортогонального. Чем ближе эта величина к единице, то есть чем короче векторы базиса, тем больше базис "похож" на ортогональный. Известно (см. [6], [23]), что для любого n существует такая константа c, зависящая только от n, что у любой n–мерной решетки Λ найдется такой базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, что

$$\prod_{i=1}^{n} |\mathbf{b}_i| \leqslant c \cdot \det \Lambda. \tag{7.5}$$

В следующем параграфе мы приведем алгоритм построения базиса, удовлетворяющего подобному соотношению. А пока сформулируем еще несколько свойств базисов пространства $\mathbb{R}^n$, строящихся при помощи процесса ортогонализации Грама–Шмидта.

Рассмотрим одно из подпространств L_k, определенных выше. Векторы $\mathbf{b}_1, \ldots, \mathbf{b}_k$ образуют базис k–мерной решетки Λ_k в пространстве L_k, а векторы $\mathbf{b}_1^*, \ldots, \mathbf{b}_k^*$ получаются из $\mathbf{b}_1, \ldots, \mathbf{b}_k$ при помощи процесса ортогонализации Грама–Шмидта. Стало быть, применяя к этой решетке теоремы 7.3 и 7.6, получаем следующее утверждение:

Теорема 7.8. *Пусть* $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ *— векторы, построенные из векторов* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *пространства* $\mathbb{R}^n$ *при помощи процесса ортогонализации Грама–Шмидта. Тогда для любого* $k \leqslant n$

$$\det \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_k) = \prod_{i=1}^{k} |\mathbf{b}_i^*|^2,$$

где $\Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_k)$ *— матрица Грама векторов* $\mathbf{b}_1, \ldots, \mathbf{b}_k$.

Решетка Λ_k — это подгруппа группы Λ, поэтому Λ распадается в объединение смежных классов по этой подгруппе. При этом $\Lambda_k = \Lambda \cap L_k$, откуда видим, что каждый из этих смежных классов содержится в соответствующей параллельной копии подпространства L_k. Расстояние между двумя смежными классами оценивается в следующем утверждении:

Теорема 7.9. *Если* $\mathbf{x} \in \Lambda \backslash L_k$, *то расстояние от* $\mathbf{x}$ *до* L_k *не меньше, чем*

$$\min_{k<j\leqslant n} |\mathbf{b}_j^*|.$$

Доказательство. По условию, найдутся такие целые $r_1, \ldots, r_i$, что $r_i \neq 0$, $k < i \leqslant n$ и

$$\mathbf{x} = r_1\mathbf{b}_1 + \ldots + r_i\mathbf{b}_i.$$

Обозначим через $\mathbf{x}^{(k)}$ и $\mathbf{x}^{(i-1)}$ ортогональные проекции вектора $\mathbf{x}$ на подпространства $L_k^\perp$ и $L_{i-1}^\perp$, соответственно. Расстояние от $\mathbf{x}$ до L_k в точности равно $|\mathbf{x}^{(k)}|$, тогда как

$$|\mathbf{x}^{(k)}| \geqslant |\mathbf{x}^{(i-1)}|, \tag{7.6}$$

поскольку $L_{i-1}^\perp \subset L_k^\perp$. С другой стороны, поскольку вектор $\mathbf{b}_i^*$ — это ортогональная проекция вектора $\mathbf{b}_i$ на $L_{i-1}^\perp$, векторы $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$ содержатся в пространстве L_{i-1} и $\mathbf{x} - r_i\mathbf{b}_i \in L_{i-1}$, видим, что

$$\mathbf{x}^{(i-1)} = r_i\mathbf{b}_i^*.$$

Следовательно, в силу (7.6),

$$|\mathbf{x}^{(k)}| \geqslant |r_i\mathbf{b}_i^*| \geqslant |\mathbf{b}_i^*| \geqslant \min_{k<j\leqslant n} |\mathbf{b}_j^*|.$$

□

7.2 LLL–алгоритм.

7.2.1 LLL–приведенные базисы.

Как было сказано ранее, на данный момент не известно ни одного алгоритма построения базиса решетки, приведенного по Минковско-

му, сложность которого полиномиально зависит от размерности. Однако, если ослабить требование минимальности базиса относительно какого–то заданного порядка и искать "почти приведенные" базисы, то есть "почти минимальные", то как показали в 1982–ом году А. К. Ленстра, Х. В. Ленстра и Л. Ловас, такого рода базисы можно строить довольно быстро. Соответствующие базисы носят название *LLL–приведенных базисов*, а алгоритм их построения называется *LLL–алгоритмом*.

Вспомним, что чем короче векторы какого–то базиса, тем больше он "похож" на ортогональный базис (см. рассуждение непосредственно после теоремы 7.7). Поэтому для того, чтобы понять, насколько "близок к минимальности" базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ решетки Λ, можно "сравнивать" его с каким–нибудь ортогональным базисом пространства $\mathbb{R}^n$, например, с базисом $\{\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*\}$, который получается из него методом ортогонализации Грама–Шмидта.

Определение 7.7. *Базис* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *решетки* Λ *называется* LLL–приведенным, *если*

$$|\mu_{i,j}| \leqslant \frac{1}{2} \qquad \textit{при } 1 \leqslant j < i \leqslant n \tag{7.7}$$

и

$$|\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*|^2 \geqslant \frac{3}{4}|\mathbf{b}_{i-1}^*|^2 \qquad \textit{при } 1 < i \leqslant n, \tag{7.8}$$

где $\mathbf{b}_i^*$ *и* $\mu_{i,j}$ *определены равенствами* (7.3) *и* (7.4).

Замечание 1. *Совокупность неравенств* (7.8) *в определении 7.7 называется* условием Ловаса. *Как легко видеть, это условие, в силу попарной ортогональности векторов* $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$, *равносильно тому, что*

$$|\mathbf{b}_i^*|^2 \geqslant \left(\frac{3}{4} - \mu_{i,i-1}^2\right)|\mathbf{b}_{i-1}^*|^2 \qquad \textit{при } 1 < i \leqslant n. \tag{7.9}$$

Вообще говоря, в этих неравенствах число 3/4 *довольно условно и вместо него можно поставить произвольное число* γ, *такое, что*

$1/4 < \gamma < 1$. *Но тогда оценки, которые мы получим ниже, будут выглядеть громоздко, поскольку некоторые двойки нужно будет заменить на* $4/(4\gamma - 1)$. *При этом скорость LLL–алгоритма и "качество" итогового базиса не слишком чувствительны к выбору значения константы* γ. *Поэтому мы ограничимся случаем* $\gamma = 3/4$, *и отметим лишь, что из существования LLL–приведенного базиса для любого* $\gamma : 1/4 < \gamma < 1$ *(которое следует из корректности LLL–алгоритма) можно вывести существование такого базиса решетки, что угол между любыми двумя векторами этого базиса не меньше* 60° *(и не больше* 120°*).*

В следующей теореме доказывается, помимо всего прочего, что LLL–приведенный базис решетки Λ удовлетворяет соотношению (7.5) с константой $c = 2^{n(n-1)/4}$, то есть он не очень сильно отличается от ортогонального.

Теорема 7.10. *Пусть* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *— LLL–приведенный базис решетки* Λ. *Тогда*

(i)
$$\det \Lambda \leqslant \prod_{i=1}^{n} |\mathbf{b}_i| \leqslant 2^{n(n-1)/4} \det \Lambda,$$

(ii)
$$|\mathbf{b}_j| \leqslant 2^{(i-1)/2} |\mathbf{b}_i^*| \qquad \textit{при } 1 \leqslant j \leqslant i \leqslant n,$$

(iii)
$$|\mathbf{b}_1| \leqslant 2^{(n-1)/4} (\det \Lambda)^{1/n},$$

(iv) *для каждого* $\mathbf{x} \in \Lambda$, *отличного от* $\mathbf{0}$,
$$|\mathbf{b}_1| \leqslant 2^{(n-1)/2} |\mathbf{x}|,$$

(v) *или, более общо, для любых линейно независимых векторов* $\mathbf{x}_1, \ldots, \mathbf{x}_k$ *решетки* Λ
$$|\mathbf{b}_j| \leqslant 2^{(n-1)/2} \max(|\mathbf{x}_1|, \ldots, |\mathbf{x}_k|) \qquad \textit{при } 1 \leqslant j \leqslant k.$$

Доказательство. Докажем сначала пункт (ii). Из определения 7.7 следует, что

$$|\mathbf{b}_i^*|^2 \geqslant (3/4 - \mu_{i,i-1}^2)|\mathbf{b}_{i-1}^*|^2 \geqslant \frac{|\mathbf{b}_{i-1}^*|^2}{2} \qquad \text{при } 1 < i \leqslant n,$$

откуда при помощи индукции получаем, что

$$|\mathbf{b}_j^*|^2 \leqslant 2^{i-j}|\mathbf{b}_i^*|^2 \qquad \text{при } 1 \leqslant j \leqslant i \leqslant n.$$

Стало быть, при $1 \leqslant j \leqslant i \leqslant n$

$$|\mathbf{b}_j|^2 = |\mathbf{b}_j^*|^2 + \sum_{k=1}^{j-1} \mu_{j,k}^2 |\mathbf{b}_k^*|^2 \leqslant \frac{2^{j-1}+1}{2}|\mathbf{b}_j^*|^2 \leqslant 2^{j-1}|\mathbf{b}_j^*|^2 \leqslant 2^{i-1}|\mathbf{b}_i^*|^2.$$

Пункт (ii) доказан.

Первое неравенство пункта (i) в точности является неравенством Адамара (см. теорему 7.7). Второе неравенство следует из пункта (ii) и теоремы 7.6:

$$\prod_{i=1}^{n} |\mathbf{b}_i| \leqslant \prod_{i=1}^{n} 2^{(i-1)/2}|\mathbf{b}_i^*| = 2^{n(n-1)/4} \det \Lambda.$$

Подставляя же в пункт (ii) $j = 1$, получаем:

$$|\mathbf{b}_1| \leqslant \Big(\prod_{i=1}^{n} 2^{(i-1)/2}|\mathbf{b}_i^*| \Big)^{1/n} = 2^{(n-1)/4} (\det \Lambda)^{1/n},$$

что доказывает пункт (iii).

Пункт (iv) является частным случаем пункта (v).

Пункт (v) следует из теоремы 7.9 и пункта (ii). Действительно, среди k линейно независимых векторов $\mathbf{x}_1, \ldots, \mathbf{x}_k$ решетки Λ как минимум один не лежит в подпространстве L_{k-1} (порожденном векторами $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$). Стало быть, в силу теоремы 7.9,

$$\min_{k \leqslant i \leqslant n} |\mathbf{b}_i^*| \leqslant \max(|\mathbf{x}_1|, \ldots, |\mathbf{x}_k|).$$

Остается применить пункт (ii). □

7.2.2 Описание LLL–алгоритма.

Не составляет труда по произвольному заданному базису $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ решетки Λ построить базис, для которого будет выполняться условие (7.7) (из определения 7.7). Действительно, нужно просто, перебирая последовательно $k = 2, \ldots, n$, заменять $\mathbf{b}_k$ на

$$\mathbf{b}_k - \sum_{i=1}^{k-1} \lfloor \mu_{k,i} \rceil \mathbf{b}_i,$$

где $\lfloor \mu_{k,i} \rceil$ означает целое число, ближайшее к $\mu_{k,i}$, вычисляя на каждом шаге заново значения коэффициентов $\mu_{i,j}$. Базис решетки Λ удовлетворяющий условию (7.7) из определения 7.7, будем называть μ–*приведенным*.

Для построения LLL–приведенного базиса можно воспользоваться следующей процедурой. Предположим, что базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ μ–приведен, но не LLL–приведен. Рассмотрим минимальный индекс $\varkappa$, для которого не выполняется условие Ловаса:

$$\varkappa = \min \left\{ k \in \{2, \ldots, n\} \;\middle|\; |\mathbf{b}_k^* + \mu_{k,k-1}\mathbf{b}_{k-1}^*|^2 > \frac{3}{4}|\mathbf{b}_{k-1}^*|^2 \right\},$$

и поменяем векторы $\mathbf{b}_\varkappa$ и $\mathbf{b}_{\varkappa-1}$ местами. По получившемуся базису построим μ–приведенный, найдем опять минимальный индекс, для которого нарушается условие Ловаса, поменяем соответствующие векторы местами и будем повторять этот процесс, пока не построим LLL–приведенный базис.

Пока что не вполне понятно, почему данный алгоритм когда–нибудь завершится, ведь индекс $\varkappa$ будет то увеличиваться, то уменьшаться. Однако очевидно, что его можно несколько рационализировать. А именно, μ–приводить базис на каждом этапе полностью не обязательно, ибо предложенный алгоритм при фиксированном значении $\varkappa$ работает лишь с теми $\mu_{k,j}$, у которых $k > \varkappa$. Поэтому мы введем параметр $k_{\max}$, который в каждый момент будет равен максимальному из предыдущих значений $\varkappa$, и будем на каждом шаге

обновлять лишь те $\mu_{k,j}$, у которых $k \leqslant k_{\max}$. Кроме того, в процессе μ–приведения базиса $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ каждый вектор $\mathbf{b}_k$ заменяется на вектор, отличающийся от него на вектор, ортогональный вектору $\mathbf{b}_k^*$. Стало быть, векторы $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ в процессе μ–приведения не меняются, то есть для проверки условия Ловаса из коэффициентов $\mu_{k,j}$ необходимы только коэффициенты $\mu_{k,k-1}$. Поэтому для каждого нового значения индекса k нужно первым делом добиться того, чтобы абсолютное значение коэффициента $\mu_{k,k-1}$ стало не больше, чем $1/2$, затем проверить для этого индекса условия Ловаса, и только в случае его выполнения уменьшать все остальные $\mu_{k,j}$. Наконец, как уже отмечалось в замечании 1, неравенство

$$|\mathbf{b}_k^* + \mu_{k,k-1}\mathbf{b}_{k-1}^*|^2 \geqslant \frac{3}{4}|\mathbf{b}_{k-1}^*|^2$$

равносильно неравенству

$$|\mathbf{b}_k^*|^2 \geqslant \left(\frac{3}{4} - \mu_{k,k-1}^2\right)|\mathbf{b}_{k-1}^*|^2.$$

Поэтому для проверки условия Ловаса, кроме коэффициентов $\mu_{k,k-1}$, достаточно знать величины $|\mathbf{b}_k^*|^2$, которые мы будем обозначать символами B_k.

Получаем следующий алгоритм:

LLL–алгоритм. Данные: *Базис* $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *решетки* Λ.
Найти: *LLL–приведенный базис решетки* Λ.
1. Положить $k = 2$, $k_{\max} = 1$, $\mathbf{b}_1^* = \mathbf{b}_1$, $B_1 = \langle \mathbf{b}_1, \mathbf{b}_1 \rangle$.
2. Если $k \leqslant k_{\max}$, *перейти в пункт 3. Иначе, положить* $k_{\max} = k$ *и вычислить* $\mathbf{b}_k^*$ *и* $\mu_{k,i}$ *для* $i = 1, \ldots, k-1$ *по соответствующим формулам из* (7.3) *и* (7.4). *Положить* $B_k = |\mathbf{b}_k^*|^2$.
3. Если $|\mu_{k,k-1}| > 1/2$, *положить* $q = \lfloor \mu_{k,k-1} \rceil$ *и заменить*

$$\begin{array}{lll} \mathbf{b}_k & \text{на} & \mathbf{b}_k - q\mathbf{b}_{k-1}, \\ \mu_{k,k-1} & \text{на} & \mu_{k,k-1} - q, \\ \mu_{k,i} & \text{на} & \mu_{k,i} - q\mu_{k-1,i} \quad (\text{для всех } i = 1, \ldots, k-2). \end{array}$$

4. Если условие Ловаса для индекса k не выполняется, то есть если

$$B_k < \left(\frac{3}{4} - \mu_{k,k-1}^2\right) B_{k-1},$$

перейти в пункт 7.
5. Для всех $i = 1, \ldots, k-2$ (перебирая их в порядке убывания, от $k-2$ до 1) проделать следующее:
если $|\mu_{k,i}| > 1/2$, положить $q = \lfloor \mu_{k,i} \rceil$ и заменить

$$\begin{aligned}
&\mathbf{b}_k && \text{на} && \mathbf{b}_k - q\mathbf{b}_i, \\
&\mu_{k,i} && \text{на} && \mu_{k,i} - q, \\
&\mu_{k,j} && \text{на} && \mu_{k,j} - q\mu_{i,j} \quad (\text{для всех } j = 1, \ldots, i-1).
\end{aligned}$$

6. Если $k < n$, увеличить k на единицу и перейти в пункт 2. Если же $k = n$, СТОП. Базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ LLL–приведен.
7. Поменять местами векторы $\mathbf{b}_k$ и $\mathbf{b}_{k-1}$. Затем поменять местами (если $k > 2$) коэффициенты $\mu_{k,i}$ и $\mu_{k-1,i}$ для всех $i = 1, \ldots, k-2$. Положить

$$\begin{aligned}
&\mathbf{b} = \mathbf{b}_{k-1}^*, \\
&\mu = \mu_{k,k-1}, \\
&B = B_k + \mu^2 B_{k-1}
\end{aligned}$$

и заменить (в заданном порядке)

$$\begin{aligned}
&\mathbf{b}_{k-1}^* && \text{на} && \mathbf{b}_k^* + \mu\mathbf{b}, \\
&\mu_{k,k-1} && \text{на} && \mu B_{k-1}/B, \\
&\mathbf{b}_k^* && \text{на} && \mathbf{b} - \mu_{k,k-1}\mathbf{b}_{k-1}^*, \\
&B_k && \text{на} && B_{k-1}B_k/B, \\
&B_{k-1} && \text{на} && B.
\end{aligned}$$

Для каждого $i = k+1, k+2, \ldots, k_{\max}$ положить $\nu = \mu_{i,k}$ и заменить (в заданном порядке)

$$\begin{aligned}
&\mu_{i,k} && \text{на} && \mu_{i,k-1} - \mu\nu, \\
&\mu_{i,k-1} && \text{на} && \nu + \mu_{k,k-1}\mu_{i,k}.
\end{aligned}$$

Положить $k = \max(2, k-1)$ и перейти в пункт 3.

Теорема 7.11. *Пусть Λ — n–мерная решетка и $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ — ее базис. Тогда LLL–алгоритм, примененный к векторам $\mathbf{b}_1, \ldots, \mathbf{b}_n$, строит LLL–приведенный базис решетки Λ.*

Доказательство. **1.** Покажем, что после прохождения каждого из пунктов значения $\mathbf{b}_i$, $\mathbf{b}_i^*$, $\mu_{i,j}$, B_i при $1 \leqslant j < i \leqslant k_{\max}$ согласованы, то есть связаны соотношениями

$$\mathbf{b}_i^* = \mathbf{b}_i - \textstyle\sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*,$$
$$B_i = |\mathbf{b}_i^*|^2$$
$$\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / B_j.$$

Для этого достаточно доказать следующие три утверждения:

(а) После выхода из пункта 3 выполняются неравенство $|\mu_{k,k-1}| \leqslant 1/2$ и равенства $\mu_{k,i} = \langle \mathbf{b}_k, \mathbf{b}_i^* \rangle / B_i$ для всех $i : 1 \leqslant i \leqslant k-1$, при условии, что перед входом в этот пункт значения $\mathbf{b}_i$, $\mathbf{b}_i^*$, $\mu_{i,j}$, B_i при $1 \leqslant j < i \leqslant k_{\max}$ были согласованы.

(б) После выхода из пункта 5 выполняются неравенства $|\mu_{k,i}| \leqslant 1/2$ и равенства $\mu_{k,i} = \langle \mathbf{b}_k, \mathbf{b}_i^* \rangle / B_i$ для всех $i : 1 \leqslant i \leqslant k-1$, при условии, что перед входом в этот пункт значения $\mathbf{b}_i$, $\mathbf{b}_i^*$, $\mu_{i,j}$, B_i при $1 \leqslant j < i \leqslant k_{\max}$ были согласованы.

(в) После выхода из пункта 7 выполняются равенства

$$\mathbf{b}_{k-1}^* = \mathbf{b}_{k-1} - \textstyle\sum_{j=1}^{k-2} \mu_{k-1,j}\mathbf{b}_j^*,$$
$$\mathbf{b}_k^* = \mathbf{b}_k - \textstyle\sum_{j=1}^{k-1} \mu_{k,j}\mathbf{b}_j^*,$$
$$B_{k-1} = |\mathbf{b}_{k-1}^*|^2$$
$$B_k = |\mathbf{b}_k^*|^2$$
$$\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / B_j \quad \text{для всех } i,j : \ k-1 \leqslant i \leqslant k_{\max}, \ 1 \leqslant j < i,$$

при условии, что перед входом в этот пункт значения $\mathbf{b}_i$, $\mathbf{b}_i^*$, $\mu_{i,j}$, B_i при $1 \leqslant j < i \leqslant k_{\max}$ были согласованы.

Утверждение (а) легко следует из линейности скалярного произведения и того факта, что перед входом в пункт 3 выполнялось равенство $\langle \mathbf{b}_{k-1}, \mathbf{b}_{k-1}^* \rangle = \langle \mathbf{b}_{k-1}^*, \mathbf{b}_{k-1}^* \rangle$.

Перед входом в пункт 5 также выполняются равенства $\langle \mathbf{b}_i, \mathbf{b}_i^* \rangle = \langle \mathbf{b}_i^*, \mathbf{b}_i^* \rangle$ для всех $i = 1, \ldots, k-2$. Во время выполнения пункта 5 индекс i последовательно принимает значения от $k-2$ до 1. При этом, в силу линейности скалярного произведения, перед каждым уменьшением i на единицу будут выполняться соотношения $|\mu_{k,i}| \leqslant 1/2$ и $\mu_{k,j} = \langle \mathbf{b}_k, \mathbf{b}_j^* \rangle / B_j$ для всех $j \leqslant i$. Коэффициенты же $\mu_{k,j}$ при $j > i$ не меняются, поскольку $\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = 0$. Утверждение (б) доказано.

Для доказательства утверждения (в) обозначим через $\overleftarrow{\mathbf{b}}_i, \overleftarrow{\mathbf{b}}_i^*, \overleftarrow{\mu}_{i,j}, \overleftarrow{B}_i$ значения $\mathbf{b}_i, \mathbf{b}_i^*, \mu_{i,j}, B_i$ перед входом в пункт 7 и через $\overrightarrow{\mathbf{b}}_i, \overrightarrow{\mathbf{b}}_i^*, \overrightarrow{\mu}_{i,j}, \overrightarrow{B}_i$ — их значения после выхода из пункта 7. Тогда

$$\begin{aligned}
&\overrightarrow{\mathbf{b}}_{k-1} = \overleftarrow{\mathbf{b}}_k, \\
&\overrightarrow{\mathbf{b}}_k = \overleftarrow{\mathbf{b}}_{k-1}, \\
&\overrightarrow{\mathbf{b}}_{k-1}^* = \overleftarrow{\mathbf{b}}_k^* + \overleftarrow{\mu}_{k,k-1} \overleftarrow{\mathbf{b}}_{k-1}^*, \\
&\overrightarrow{B}_{k-1} = \overleftarrow{B}_k + \overleftarrow{\mu}_{k,k-1}^2 \overleftarrow{B}_{k-1},
\end{aligned}$$

а также

$$\begin{aligned}
\overrightarrow{\mu}_{k,k-1} &= \overleftarrow{\mu}_{k,k-1} \overleftarrow{B}_{k-1} \Big/ \overrightarrow{B}_{k-1} = \overleftarrow{\mu}_{k,k-1} \langle \overleftarrow{\mathbf{b}}_{k-1}, \overleftarrow{\mathbf{b}}_{k-1}^* \rangle \Big/ \overrightarrow{B}_{k-1} = \\
&= \langle \overrightarrow{\mathbf{b}}_k, \overleftarrow{\mu}_{k,k-1} \overleftarrow{\mathbf{b}}_{k-1}^* \rangle \Big/ \overrightarrow{B}_{k-1} = \langle \overrightarrow{\mathbf{b}}_k, \overrightarrow{\mathbf{b}}_{k-1}^* - \overleftarrow{\mathbf{b}}_k^* \rangle \Big/ \overrightarrow{B}_{k-1} = \\
&= \langle \overrightarrow{\mathbf{b}}_k, \overrightarrow{\mathbf{b}}_{k-1} \rangle \Big/ \overrightarrow{B}_{k-1}, \\
\overrightarrow{\mathbf{b}}_k^* &= \overleftarrow{\mathbf{b}}_{k-1}^* - \overrightarrow{\mu}_{k,k-1} \overrightarrow{\mathbf{b}}_{k-1}^*
\end{aligned}$$

и

$$\begin{aligned}
\overrightarrow{B}_k &= \overleftarrow{B}_{k-1} \overleftarrow{B}_k \Big/ \overrightarrow{B}_{k-1} = \overleftarrow{B}_{k-1} (\overrightarrow{B}_{k-1} - \overleftarrow{\mu}_{k,k-1}^2 \overleftarrow{B}_{k-1}) \Big/ \overrightarrow{B}_{k-1} = \\
&= \overleftarrow{B}_{k-1} - \overleftarrow{\mu}_{k,k-1}^2 \overleftarrow{B}_{k-1} \Big/ \overrightarrow{B}_{k-1} = \overleftarrow{B}_{k-1} - \overrightarrow{\mu}_{k,k-1}^2 \overrightarrow{B}_{k-1} = \\
&= |\overrightarrow{\mathbf{b}}_k^* + \overrightarrow{\mu}_{k,k-1} \overrightarrow{\mathbf{b}}_{k-1}^*|^2 - \overrightarrow{\mu}_{k,k-1}^2 \overrightarrow{B}_{k-1} = |\overrightarrow{\mathbf{b}}_k^*|^2.
\end{aligned}$$

Кроме того,

$$\begin{aligned}
&\vec{\mu}_{k,i} = \overleftarrow{\mu}_{k-1,i} \quad \text{для всех } i = 1, \ldots, k-2,\\
&\vec{\mu}_{k-1,i} = \overleftarrow{\mu}_{k,i} \quad \text{для всех } i = 1, \ldots, k-2.
\end{aligned}$$

Стало быть, перед заменой в пункте 7 индекса k на $\max(2, k-1)$ значения $\mathbf{b}_i$, $\mathbf{b}_i^*$, $\mu_{i,j}$, B_i при $1 \leqslant j < i \leqslant k$ согласованы. Остается заметить, что для всех $i = k+1, k+2, \ldots, k_{\max}$ справедливы соотношения

$$\begin{aligned}
\vec{\mu}_{i,k} &= \overleftarrow{\mu}_{i,k-1} - \overleftarrow{\mu}_{k,k-1}\overleftarrow{\mu}_{i,k} =\\
&= \langle \overleftarrow{\mathbf{b}}_i, \overleftarrow{\mathbf{b}}^*_{k-1} \Big/ \overleftarrow{B}_{k-1} - \overleftarrow{\mu}_{k,k-1}\overleftarrow{\mathbf{b}}^*_k \Big/ \overleftarrow{B}_k \rangle =\\
&= \langle \overleftarrow{\mathbf{b}}_i, \overleftarrow{\mathbf{b}}^*_{k-1} \overleftarrow{B}_k \Big/ \vec{B}_{k-1} - \overleftarrow{\mu}_{k,k-1}\overleftarrow{\mathbf{b}}^*_k \overleftarrow{B}_{k-1} \Big/ \vec{B}_{k-1} \rangle \Big/ \vec{B}_k =\\
&= \langle \overleftarrow{\mathbf{b}}_i, (1 - \overleftarrow{\mu}_{k,k-1}\vec{\mu}_{k,k-1})\overleftarrow{\mathbf{b}}^*_{k-1} - \vec{\mu}_{k,k-1}\overleftarrow{\mathbf{b}}^*_k \rangle \Big/ \vec{B}_k =\\
&= \langle \vec{\mathbf{b}}_i, \vec{\mathbf{b}}^*_k \rangle \Big/ \vec{B}_k
\end{aligned}$$

и

$$\begin{aligned}
\vec{\mu}_{i,k-1} &= \overleftarrow{\mu}_{i,k} + \vec{\mu}_{k,k-1}\vec{\mu}_{i,k} =\\
&= \overleftarrow{\mu}_{i,k} + \overleftarrow{\mu}_{k,k-1}\overleftarrow{B}_{k-1}(\overleftarrow{\mu}_{i,k-1} - \overleftarrow{\mu}_{k,k-1}\overleftarrow{\mu}_{i,k}) \Big/ \vec{B}_{k-1} =\\
&= (\overleftarrow{\mu}_{i,k}\overleftarrow{B}_k + \overleftarrow{\mu}_{k,k-1}\overleftarrow{\mu}_{i,k-1}\overleftarrow{B}_{k-1}) \Big/ \vec{B}_{k-1} =\\
&= \langle \vec{\mathbf{b}}_i, \vec{\mathbf{b}}^*_{k-1} \rangle \Big/ \vec{B}_{k-1}.
\end{aligned}$$

Утверждение (в) доказано.

2. Докажем теперь, что алгоритм завершится. Для этого рассмотрим матрицы Грама $\Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ и их определители

$$d_i = \det \Gamma(\mathbf{b}_1, \ldots, \mathbf{b}_i), \qquad 1 \leqslant i \leqslant n.$$

По теореме 7.8,

$$d_i = \prod_{j=1}^{i} |\mathbf{b}_j^*|^2 = \prod_{j=1}^{i} B_j, \qquad 1 \leqslant i \leqslant n.$$

Стало быть, d_i суть положительные вещественные числа, причем $d_n = (\det \Lambda)^2$, в силу теоремы 7.2. Рассмотрим величину

$$d = \prod_{i=1}^{n-1} d_i.$$

Эта величина изменяется только в том случае, если меняются какие–то из векторов $\mathbf{b}_j^*$, что происходит только тогда, когда выполняется пункт 7 алгоритма, то есть когда для некоторого k вектора $\mathbf{b}_k$ и $\mathbf{b}_{k-1}$ меняются местами. При этом произведение $B_k B_{k-1}$ не меняется. Следовательно, все d_i, кроме d_{k-1}, также не меняются, а d_{k-1} уменьшается более, чем в $4/3$ раза, так как если условие Ловаса для индекса k не выполняется, то

$$\vec{B}_{k-1} = \overleftarrow{B}_k + \overleftarrow{\mu}^2_{k,k-1} \overleftarrow{B}_{k-1} < \frac{3}{4} \overleftarrow{B}_{k-1}.$$

Но из теорем 7.3 и 7.4 следует, что существует такое положительное число c, зависящее только от решетки Λ, что

$$d \geqslant c,$$

то есть алгоритм возвращается в пункт 7 лишь конечное число раз. Стало быть, с какого–то момента условие Ловаса в пункте 4 всегда будет выполняться, что означает, что в какой–то момент алгоритм завершится.

3. Итак, мы показали, что алгоритм закончит работу за конечное время, сохранив согласованность величин $\mathbf{b}_i$, $\mathbf{b}_i^*$, $\mu_{i,j}$, B_i. Алгоритм завершает работу, когда в пункте 6 выполняется условие $k = n$. При этом, как видно из пунктов 3 и 5, будут справедливы неравенства $|\mu_{i,j}| \leqslant 1/2$ для всех $1 \leqslant j < i \leqslant n$, а пункт 4 гарантирует выполнение условия Ловаса. Следовательно, исходный базис в итоге будет преобразован алгоритмом в LLL–приведенный. □

Замечание 2. *Легко видеть, что перед каждым входом в любой пункт LLL–алгоритма векторы* $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ *(для текущего значения индекса* k*) образуют LLL–приведенный базис* $(k-1)$*–мерной решетки* $\operatorname{span}_{\mathbb{Z}}(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}) \subset L_{k-1}$.

В работе [25] проведен подробный анализ количества операций, выполняемых LLL–алгоритмом на каждом шаге и доказана следующая

Теорема 7.12. *Пусть Λ — n–мерная целочисленная решетка (то есть $\Lambda \subseteq \mathbb{Z}^n$) с базисом $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ и пусть величины $|\mathbf{b}_i|$ ограничены некоторой константой $C > 1$ для всех $1 \leqslant i \leqslant n$. Тогда сложность LLL–алгоритма, примененного к этому базису, равна $O(n^4 \ln C)$. При этом двоичная длина чисел, с которыми приходится работать алгоритму, не превосходит $O(n \ln C)$.*

Замечание 3. *Если векторы $\mathbf{b}_1, \ldots, \mathbf{b}_n$ не известны, а известна только их матрица Грама, то LLL–алгоритм можно немного видоизменить так, чтобы он находил координаты векторов соответствующего LLL–приведенного базиса в исходном базисе. При этом, если матрица Грама целочисленная, то при вычислениях можно не выходить за рамки кольца целых чисел. В этом случае справедливы те же оценки для сложности алгоритма, что и в теореме 7.12. Алгоритм можно также применять и для случая, когда коэффициенты матрицы Грама суть рациональные числа, предварительно домножив их на общий знаменатель. Подробнее об этом написано в книге [19].*

7.3 Применения LLL–алгоритма.

7.3.1 Построение коротких векторов решетки.

Задача построения самого короткого ненулевого вектора решетки заведомо является весьма сложной, ибо если ее немного видоизменить и рассматривать вместо евклидовой нормы ℓ_2 норму ℓ_1 или ℓ_∞ (то есть искать такие ненулевые векторы $\mathbf{x}$ решетки $\Lambda \subset \mathbb{R}^n$, на которых достигается минимум величины $|x_1| + \ldots + |x_n|$ или, соответственно, величины $\max_{1 \leqslant i \leqslant n} |x_i|$), то эта новая задача будет $\mathcal{NP}$–полна (см. [26], [14], [24]), то есть, если $\mathcal{P} \neq \mathcal{NP}$, скорее всего, полиномиального алгоритма поиска самого короткого в евклидовой норме ненулевого вектора решетки не существует.

Однако, если размерность n фиксирована, то эта задача решается за полиномиальное время:

Теорема 7.13. *Пусть Λ — подрешетка целочисленной решетки $\mathbb{Z}^n$, заданная каким-то своим базисом $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ и пусть $|\mathbf{v}_i| \leqslant C$, $C > 1$, для любого $i = 1, \ldots, n$. Тогда существует алгоритм, который находит самый короткий (в евклидовой норме) ненулевой вектор решетки Λ за время, полиномиально зависящее от $\ln C$ (но при этом степень многочлена, ограничивающего время работы алгоритма, экспоненциально зависит от n).*

Доказательство. При помощи LLL–алгоритма по базису $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ можно построить LLL–приведенный базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ решетки Λ за $O(n^4 \ln C)$ операций. Если $\mathbf{v}$ — произвольный вектор решетки Λ, то для некоторых целых $\lambda_1, \ldots, \lambda_n$

$$\mathbf{v} = \sum_{i=1}^{n} \lambda_i \mathbf{b}_i.$$

Отсюда, пользуясь правилом Крамера и пунктом (i) теоремы 7.10, для каждого $i = 1, \ldots, n$ получаем:

$$\begin{aligned} |\lambda_i| &= \frac{|\det(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, \mathbf{v}, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n)|}{|\det(\mathbf{b}_1, \ldots, \mathbf{b}_n)|} \leqslant \\ &\leqslant \frac{|\mathbf{b}_1| \cdots |\mathbf{b}_{i-1}| \cdot |\mathbf{v}| \cdot |\mathbf{b}_{i+1}| \cdots |\mathbf{b}_n|}{2^{-n(n-1)/4} |\mathbf{b}_1| \cdots |\mathbf{b}_n|} = 2^{n(n-1)/4} |\mathbf{v}| / |\mathbf{b}_i|. \end{aligned} \tag{7.10}$$

Здесь мы к числителю применили первое неравенство пункта (i) теоремы 7.10, а к знаменателю — второе.

Таким образом, если $\mathbf{v}$ — минимальный вектор решетки Λ, то $|\lambda_i| \leqslant 2^{n(n-1)/4}$ для каждого $i = 1, \ldots, n$. То есть, перебрав элементы множества

$$\Big\{ \sum_{i=1}^{n} \lambda_i \mathbf{b}_i \;\Big|\; \lambda_i \in \mathbb{Z},\ |\lambda_i| \leqslant 2^{n(n-1)/4},\ i = 1, \ldots, n \Big\},$$

мы найдем все минимальные векторы решетки Λ. $\square$

Замечание 4. *Ясно, что такая же теорема имеет место и для ℓ_1, и для ℓ_∞, и вообще для произвольной нормы в $\mathbb{R}^n$, поскольку любые две нормы в $\mathbb{R}^n$ эквивалентны.*

Замечание 5. *С соответствующей поправкой на сложность алгоритма теорема верна и для более общего класса решеток (см. замечание 3).*

Таким образом, LLL–алгоритм *полиномиально сводит* задачу нахождения кратчайшего вектора решетки к перебору элементов некоторого множества, мощность которого зависит лишь от размерности, но зависит экспоненциально.

Соотношение (7.10) можно также использовать и для построения базисов, приведенных по Минковскому. Действительно, из теории последовательных минимумов известен следующий факт (см. [23]):

Теорема 7.14. *Если $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ — приведенный по Минковскому базис решетки Λ, то*

$$\prod_{i=1}^{n} |\mathbf{w}_i| \leqslant \frac{\det \Lambda}{V_n} \cdot 2^n \cdot \left(\frac{3}{2}\right)^{\frac{(n-1)(n-2)}{2}},$$

где V_n — объем n–мерного единичного шара.

Стало быть, если $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ — какой–то приведенный по Минковскому базис решетки $\Lambda \subseteq \mathbb{Z}^n$, то для любого $i = 1, \ldots, n$

$$|\mathbf{w}_i| \leqslant \prod_{j=1}^{n} |\mathbf{w}_j| \leqslant \frac{\det \Lambda}{V_n} \cdot 2^n \cdot \left(\frac{3}{2}\right)^{\frac{(n-1)(n-2)}{2}}.$$

Таким образом, если рассматриваемая решетка Λ является подрешеткой решетки $\mathbb{Z}^n$ и длины всех векторов исходного базиса решетки Λ ограничены некоторой константой C, то при фиксированном n за время, полиномиально зависящее от $\ln C$, можно построить все базисы решетки Λ, приведенные по Минковскому (и, в частности, все приведенные по Эрмиту).

7.3.2 Совместные диофантовы приближения.

Иногда бывает нужно аппроксимировать заданные числа $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ рациональными дробями $p_1/q, \ldots, p_n/q$ с равными знаменателями. При этом желательно, чтобы порядок приближения был как можно больше, а знаменатель — как можно меньше. Самыми "хорошими" такого рода приближениями являются так называемые *наилучшие совместные приближения*:

Определение 7.8. *Пусть заданы отличные от нуля числа* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. *Ненулевой набор* $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$, $q > 0$, *называется* наилучшим совместным приближением *набора* $(\alpha_1, \ldots, \alpha_n)$, *если для любого другого набора* $(p'_1, \ldots, p'_n, q') \in \mathbb{Z}^{n+1}$, $0 < q' \leqslant q$, *выполняются неравенства*

$$\max_{1 \leqslant i \leqslant n} |q\alpha_i - p_i| \leqslant \max_{1 \leqslant i \leqslant n} |q'\alpha_i - p'_i|, \tag{7.11}$$

причем при $q' < q$ *в* (7.11) *имеет место строгое неравенство.*

Ясно, что наилучшие совместные приближения набора $(\alpha_1, \ldots, \alpha_n)$ существуют, причем их число конечно тогда и только тогда, когда $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}^n$. Кроме того, имеет место следующий факт (см. [6]):

Теорема 7.15. *Пусть заданы произвольные числа* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ *и* $\varepsilon \in \mathbb{R}$, $0 < \varepsilon < 1$. *Тогда найдется такой набор* $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$, $q > 0$, *что*

$$\begin{cases} \max\limits_{1 \leqslant i \leqslant n} |q\alpha_i - p_i| \leqslant \varepsilon \\ 0 < q \leqslant \varepsilon^{-n}. \end{cases} \tag{7.12}$$

Отсюда легко получить количественную оценку порядка приближения для наилучших совместных приближений:

Следствие. *Пусть* $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$ — *наилучшее совместное приближение набора* $(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$. *Тогда*

$$\max_{1 \leqslant i \leqslant n} |q\alpha_i - p_i| \leqslant q^{-1/n}.$$

На данный момент не существует алгоритма нахождения наилучших совместных приближений, сложность которого полиномиально зависит от длины входа. Если же ослабить условие (7.12), то для рациональных $\alpha_1, \ldots, \alpha_n$ при помощи LLL–алгоритма можно довольно быстро находить весьма хорошие совместные приближения, хотя, возможно, и не наилучшие. Для этого нужно воспользоваться геометрической интерпретацией аппроксимации вещественных чисел рациональными. Одна из наиболее естественных таких интерпретаций заключается в следующем. Рассмотрим $(n+1)$–мерную решетку Λ, базисные векторы $\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}$ которой суть столбцы матрицы

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\alpha_n \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}. \tag{7.13}$$

Тогда точка $\mathbf{b} = p_1\mathbf{b}_1 + \ldots + p_n\mathbf{b}_n + q\mathbf{b}_{n+1}$ решетки Λ задает "хорошее" совместное приближение $(p_1, \ldots, p_n, q)$ набора $(\alpha_1, \ldots, \alpha_n)$, если она лежит "близко" к прямой, задаваемой вектором $(0, \ldots, 0, 1)^\top$, то есть первые n координат точки $\mathbf{b}$ малы. Для того, чтобы найти такую точку, можно, зная алгоритм поиска относительно коротких векторов решетки (см. пункт (iii) теоремы 7.10), попытаться сжать решетку Λ вдоль вектора $(0, \ldots, 0, 1)^\top$ и применить к ней этот алгоритм. Что и делается в доказательстве следующей теоремы.

Теорема 7.16. *Существует полиномиальный алгоритм, который по заданным числам $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ и $\varepsilon \in \mathbb{Q}$, $0 < \varepsilon < 1$, находит такие числа $p_1, \ldots, p_n, q \in \mathbb{Z}$, $q > 0$, что*

$$\begin{cases} \max\limits_{1 \leqslant i \leqslant n} |q\alpha_i - p_i| \leqslant \varepsilon \\ 0 < q \leqslant 2^{n(n+1)/4}\varepsilon^{-n}. \end{cases} \tag{7.14}$$

Доказательство. Рассмотрим $(n+1)$–мерную решетку $\Lambda \subset \mathbb{R}^{n+1}$,

базисные векторы которой суть столбцы матрицы

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\alpha_n \\ 0 & 0 & \cdots & 0 & c \end{pmatrix},$$

где $c = 2^{-n(n+1)/4}\varepsilon^{n+1}$. Скалярные произведения этих векторов рациональны, поэтому, существует полиномиальный алгоритм (см. замечание 3), который находит LLL–приведенный базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}\}$ решетки Λ. Для вектора $\mathbf{b}_1$ имеет место неравенство (iii) из теоремы 7.10, то есть

$$|\mathbf{b}_1| \leqslant 2^{n/4}(\det \Lambda)^{1/(n+1)} = \varepsilon.$$

Поскольку $\mathbf{b}_1 \in \Lambda$, он выражается с какими–то целыми коэффициентами $p_1, \ldots, p_n, q$ через векторы исходного базиса. То есть

$$\mathbf{b}_1 = (p_1 - q\alpha_1,\, p_2 - q\alpha_2, \ldots, p_n - q\alpha_n,\, 2^{-n(n+1)/4} q\varepsilon^{n+1})^{\top}.$$

Откуда получаем, что

$$\begin{cases} |q\alpha_i - p_i| \leqslant \varepsilon, \quad i = 1, \ldots, n \\ |q| \leqslant 2^{n(n+1)/4}\varepsilon^{-n}. \end{cases}$$

Из того, что $\varepsilon < 1$ и $\mathbf{b}_1 \neq \mathbf{0}$ следует, что $q \neq 0$. Заменяя, если необходимо, $\mathbf{b}_1$ на $-\mathbf{b}_1$, мы можем добиться выполнения неравенства $q > 0$.

Теорема доказана. □

Таким образом, LLL–алгоритм позволяет находить довольно хорошие совместные приближения. Если же считать, как в предыдущем пункте, что n фиксировано, то за полиномиальное время можно найти и наилучшее совместное приближение. Для этого нужно найти кратчайший вектор решетки Λ из доказательства теоремы 7.16, который и даст требуемое приближение. Кратчайший же вектор, как показано в предыдущем пункте, при фиксированном n ищется за полиномиальное время.

7.3.3 Приближения линейной формой нуля.

Как легко видеть, искать точки решетки Λ с базисом (7.13), находящиеся в окрестности прямой, задаваемой вектором $(0,\ldots,0,1)^\top$, — это то же самое, что искать точки решетки $\mathbb{Z}^{n+1}$, находящиеся в окрестности прямой ℓ, задаваемой вектором $(\alpha_1,\ldots,\alpha_n,1)^\top$. Существует классическая задача геометрии чисел, двойственная данной, — задача поиска точек решетки $\mathbb{Z}^{n+1}$ в окрестности ортогонального дополнения к прямой ℓ. Эта задача является естественной геометрической интерпретацией задачи приближения линейной формой нуля, заключающейся в следующем.

Определение 7.9. *Пусть заданы отличные от нуля числа* $\alpha_1,\ldots,\alpha_n\in\mathbb{R}$. *Рассмотрим линейную форму*

$$L(x_1,\ldots,x_n,x_{n+1})=\alpha_1x_1+\ldots+\alpha_nx_n+x_{n+1}.$$

Ненулевой набор $(p_1,\ldots,p_n,q)\in\mathbb{Z}^{n+1}$ *называется* наилучшим приближением линейной формой L нуля, *если для любого другого набора* $(p'_1,\ldots,p'_n,q')\in\mathbb{Z}^{n+1}$, $q'\neq 0$, *такого, что*

$$\max_{1\leqslant i\leqslant n}|p'_i|\leqslant\max_{1\leqslant i\leqslant n}|p_i|,$$

выполняется неравенство

$$|L(p_1,\ldots,p_n,q)|\leqslant|L(p'_1,\ldots,p'_n,q')|, \tag{7.15}$$

причем при

$$\max_{1\leqslant i\leqslant n}|p'_i|<\max_{1\leqslant i\leqslant n}|p_i|$$

в (7.15) *имеет место строгое неравенство.*

Наилучшие приближения линейной формой нуля, очевидно, существуют. Их множество конечно тогда и только тогда, когда числа $1,\alpha_1,\ldots,\alpha_n$ линейно зависимы над $\mathbb{Z}$. Так же, как и для совместных приближений, для приближений линейной формой нуля имеет место следующая

Теорема 7.17. *Пусть заданы произвольные числа* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ *и* $\varepsilon \in \mathbb{R}$, $0 < \varepsilon < 1$. *Тогда найдется такой набор* $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$, $q > 0$, *что*

$$\begin{cases} \left| \sum\limits_{i=1}^{n} \alpha_i p_i - q \right| \leqslant \varepsilon \\ \max\limits_{1 \leqslant i \leqslant n} |p_i| \leqslant \varepsilon^{-1/n}. \end{cases} \tag{7.16}$$

Получаем количественную оценку на порядок приближения нуля для наилучших приближений:

Следствие. *Пусть заданы числа* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ *и* $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$ *— наилучшее приближение нуля линейной формой*

$$L(x_1, \ldots, x_n, x_{n+1}) = \alpha_1 x_1 + \ldots + \alpha_n x_n + x_{n+1}.$$

Тогда

$$|L(p_1, \ldots, p_n, q)| \leqslant \max_{1 \leqslant i \leqslant n} |p_i|^{-n}.$$

Как и в случае совместных приближений, полиномиального алгоритма для построения наилучших приближений линейной формой нуля на данный момент не существует. Однако, если воспользоваться геометрической интерпретацией этой задачи, то для рациональных α_i при помощи LLL–алгоритма можно за полиномиальное время строить весьма хорошие, хоть и не всегда наилучшие, приближения линейной формой нуля. А если считать n фиксированным, то так же, как и в случае совместных приближений, за полиномиальное время можно находить и наилучшие приближения.

Теорема 7.18. *Существует полиномиальный алгоритм, который по заданным числам* $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ *и* $\varepsilon \in \mathbb{Q}$, $0 < \varepsilon < 1$, *находит такие числа* $p_1, \ldots, p_n, q \in \mathbb{Z}$, $q > 0$, *что*

$$\begin{cases} |L(p_1, \ldots, p_n, q)| \leqslant \varepsilon \\ |p_i| \leqslant 2^{(n^2+n+2)/(4n)} \varepsilon^{-1/n}, \quad i = 1, \ldots, n, \end{cases} \tag{7.17}$$

где

$$L(x_1, \ldots, x_n, x_{n+1}) = \alpha_1 x_1 + \ldots + \alpha_n x_n + x_{n+1}.$$

Доказательство. Рассмотрим прямую ℓ в пространстве $\mathbb{R}^{n+1}$, задаваемую вектором $(\alpha_1, \ldots, \alpha_n, 1)^\top$, и ортогональное дополнение к ней — нулевое подпространство формы $L(x_1, \ldots, x_n, x_{n+1})$. Перед нами стоит задача найти точки решетки $\mathbb{Z}^{n+1}$ "вблизи" этого подпространства. Для этого отобразим $\mathbb{R}^{n+1}$ в $\mathbb{R}^{n+2}$ следующим образом:

$$(x_1, \ldots, x_{n+1})^\top \mapsto (x_1, \ldots, x_{n+1}, cL(x_1, \ldots, x_{n+1}))^\top,$$

где

$$c = 2^{-(n^2+n+2)/(4n)} \varepsilon^{-(n+1)/n}.$$

Не ограничивая общности, можно считать, что

$$c^2 \geqslant 1 + \sum_{i=1}^{n} \alpha_i^2. \tag{7.18}$$

Образом решетки $\mathbb{Z}^{n+1}$ будет некоторая $(n+1)$–мерная решетка $\Lambda \subset \mathbb{R}^{n+2}$. Образом единичного базиса решетки $\mathbb{Z}^n$ будет базис решетки Λ, векторы которого суть столбцы матрицы

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n & c \end{pmatrix}.$$

Применим к этому базису LLL–алгоритм. Получим LLL–приведенный базис $\{\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}\}$ решетки Λ. Для вектора $\mathbf{b}_1$ выполняется неравенство (iii) из теоремы 7.10, то есть

$$|\mathbf{b}_1| \leqslant 2^{n/4} (\det \Lambda)^{1/(n+1)} = 2^{n/4} (\det(A^\top A))^{1/(2n+2)}.$$

В последнем равенстве мы воспользовались теоремой 7.3. Нетрудно посчитать $\det(A^\top A)$:

$$\det(A^\top A) = 1 + c^2 + \sum_{i=1}^{n} \alpha_i^2.$$

Таким образом, в силу (7.18),

$$|\mathbf{b}_1| \leqslant 2^{n/4}\Big(1 + c^2 + \sum_{i=1}^{n} \alpha_i^2\Big)^{1/(2n+2)} \leqslant 2^{\frac{n^2+n+2}{4n+4}} c^{1/(n+1)}.$$

Но

$$\mathbf{b}_1 = (p_1, \ldots, p_n, q, cL(p_1, \ldots, p_n, q))^\top$$

для некоторых целых $p_1, \ldots, p_n, q$. Стало быть,

$$\begin{cases} |L(p_1, \ldots, p_n, q)| \leqslant \varepsilon \\ |p_i| \leqslant 2^{(n^2+n+2)/(4n)} \varepsilon^{-1/n}, \quad i = 1, \ldots, n. \end{cases}$$

□

Алгоритмом поиска хороших приближений линейной формой нуля можно пользоваться для нахождения возможных линейных зависимостей заданных ненулевых вещественных чисел $\alpha_0, \alpha_1, \ldots, \alpha_n$ над полем $\mathbb{Q}$. Для этого нужно приближать нуль формой

$$L(x_0, x_1, \ldots, x_n) = x_1 + (\alpha_1/\alpha_0)x_2 + \ldots + (\alpha_n/\alpha_0)x_n.$$

В частности, этим методом можно тестировать заданное вещественное число α на алгебраичность и в случае, если оно является алгебраическим, находить его минимальный многочлен. Для этого нужно исследовать на линейную зависимость над $\mathbb{Q}$ числа $1, \alpha, \alpha^2, \ldots, \alpha^n$. Аналогично, если для заданных вещественных чисел $\alpha_0, \alpha_1, \ldots, \alpha_n$ рассматривать все их произведения степени, не превосходящей некоторой заданной величины, можно, исследуя эти произведения на линейную зависимость над $\mathbb{Q}$, тестировать исходные числа на алгебраическую зависимость.

7.3.4 Факторизация многочленов с рациональными коэффициентами.

Пусть задан произвольный многочлен $f(x) \in \mathbb{Z}[x]$. В данном пункте мы опишем полиномиальный алгоритм разложения многочлена $f(x)$ на неприводимые множители, использующий LLL–алгоритм. Ясно, что достаточно рассмотреть случай, когда $f(x)$ примитивен, то есть когда наибольший общий делитель его коэффициентов равен единице. Именно этот случай мы и будем рассматривать в дальнейшем.

Можно также считать, что наибольший общий делитель $d(x) = (f(x), f'(x))$ многочлена $f(x)$ и его производной $f'(x)$ равен единице. Действительно, если $d(x) \neq 1$, то $1 \leqslant \deg d < \deg f$ и, стало быть, задача сводится к разложению на множители многочленов $d(x)$ и $f(x)/d(x)$, степени которых меньше, чем $\deg f$. При этом все неприводимые делители многочлена $f(x)$ содержатся среди делителей многочлена $f(x)/d(x)$. Более того, последний многочлен равен их произведению.

Поэтому в дальнейшем мы будем считать, что $(f(x), f'(x)) = 1$. Тогда любой неприводимый делитель многочлена $f(x)$ входит в него в первой степени.

Пусть p — минимальное простое число, не делящее результант $R(f(x), f'(x))$ многочленов $f(x)$ и $f'(x)$. Такое число существует, так как в нашем случае результант равен некоторому целому отличному от нуля числу. Результант $R(f(x), f'(x))$ с точностью до знака равен произведению старшего коэффициента многочлена $f(x)$ и его дискриминанта, следовательно, степень многочлена $(f(x) \bmod p)$ равна $\deg f$ и все неприводимые делители $(f(x) \bmod p)$ входят в него в первой степени.

Основная идея предлагаемого ниже алгоритма заключается в сведении данной задачи к задаче нахождения неприводимого делителя многочлена $f(x)$ по модулю p, последующем “поднятии” этого делителя до некоторого делителя $h(x)$ многочлена $f(x)$ по модулю p^k, где k — достаточно большое натуральное число, и построении на основании

$h(x)$ некоторого неприводимого делителя многочлена $f(x)$ над $\mathbb{Z}$.

Для любого многочлена $g(x) = \sum_i a_i x^i \in \mathbb{Z}[x]$ и любого $k \in \mathbb{N}$ мы будем обозначать через $(g(x) \bmod p^k)$ многочлен $\sum_i (a_i \bmod p^k) x^i \in (\mathbb{Z}/p^k\mathbb{Z})[x]$.

Для "поднятия" делителя используется следующее классическое утверждение:

Лемма 7.1 (Лемма Гензеля). *Пусть заданы простое число p и многочлены $f(x), h_0(x), g_0(x) \in \mathbb{Z}[x]$. Пусть*

$$f(x) \equiv h_0(x) g_0(x) \pmod{p}$$

и пусть многочлены $h_0(x) \bmod p$, $g_0(x) \bmod p$ взаимно просты в кольце $F_p[x]$. Тогда для любого целого $k \geqslant 0$ существуют многочлены $h_k(x), g_k(x) \in \mathbb{Z}[x]$, такие что

$$f(x) \equiv h_k(x) g_k(x) \pmod{p^k}, \tag{7.19}$$

$$h_k(x) \equiv h_0(x) \pmod{p}, \tag{7.20}$$

$$g_k(x) \equiv g_0(x) \pmod{p} \tag{7.21}$$

и

$$\deg h_k = \deg h_0.$$

Доказательство. Будем доказывать лемму индукцией по k. При $k = 0$ требуемое утверждение выполняется по условию. Это дает основание индукции. Предположим, что найдены многочлены $h_k(x), g_k(x)$. Покажем, как построить многочлены $h_{k+1}(x), g_{k+1}(x)$. Положим

$$w(x) = (f(x) - h_k(x) g_k(x))/p^k.$$

По условию $w(x) \in \mathbb{Z}[x]$.

Далее, так как $h_k(x) \equiv h_0(x) \pmod{p}$ и $g_k(x) \equiv g_0(x) \pmod{p}$, существуют многочлены $u(x), v(x) \in \mathbb{Z}[x]$, такие что

$$h_0(x) u(x) + g_0(x) v(x) \equiv w(x) \pmod{p}.$$

Пусть $s(x)$ — остаток от деления $u(x)$ на $g_0(x)$ в $F_p[x]$:

$$u(x) \equiv s(x) + t(x) g_0(x) \pmod{p}, \quad \deg s \leqslant \deg g_0 - 1.$$

Положим также $r(x) \equiv v(x) + t(x)h_0(x) \pmod{p}$. Так как

$$\deg w \leqslant \deg f - 1$$

и

$$h_0(x)s(x) + g_0(x)r(x) \equiv w(x) \pmod{p},$$

видим, что

$$\deg(g_0 r) \leqslant \max(\deg h_0 s, \deg w) \leqslant \deg g_0 + \deg h_0 - 1,$$

то есть

$$\deg r \leqslant \deg h_0 - 1.$$

Остается положить

$$h_{k+1}(x) = h_k(x) + p^k r(x), \quad g_{k+1}(x) = g_k(x) + p^k s(x).$$

□

Замечание 6. *Как легко видеть, доказательство леммы 7.1 конструктивно и дает простой алгоритм построения многочленов* $h_{k+1}(x)$ *и* $g_{k+1}(x)$.

LLL–алгоритм в данной задаче применяется для построения неприводимого делителя $f(x)$ после того, как найден многочлен $h(x)$, делящий $f(x)$ по модулю идеала $p^k\mathbb{Z}[x]$. В качестве решетки рассматривается множество всех многочленов из $\mathbb{Z}[x]$ степени, не превосходящей некоторой величины, делящихся на $h(x)$ по модулю идеала $p^k\mathbb{Z}[x]$. При этом длина многочлена $g(x) = \sum_i a_i x^i \in \mathbb{Z}[x]$ как вектора определяется следующим образом:

$$|g| = \Big(\sum_i a_i^2\Big)^{1/2}.$$

Если заданы многочлен $h(x)$ и некоторое натуральное число $m \geqslant \deg h$, то множество Λ многочленов степени, не превосходящей m,

делящихся на $h(x)$ по модулю идеала $p^k\mathbb{Z}[x]$, является подрешеткой решетки

$$\mathbb{Z} + \mathbb{Z}x + \ldots + \mathbb{Z}x^m.$$

Каждый многочлен $g(x) \in \Lambda$ представим в виде $g(x) = h(x)u(x) + p^k v(x)$, $\deg v \leqslant m$, $\deg u \leqslant m - \deg h$, поэтому набор

$$\left\{p^k x^i \,\middle|\, 0 \leqslant i < \deg h\right\} \cup \left\{h(x)x^j \,\middle|\, 0 \leqslant j \leqslant m - \deg h\right\}$$

является базисом решетки Λ, то есть

$$\Lambda = \operatorname{span}_{\mathbb{Z}} \left(\left\{p^k x^i \,\middle|\, 0 \leqslant i < \deg h\right\} \cup \left\{h(x)x^j \,\middle|\, 0 \leqslant j \leqslant m - \deg h\right\}\right). \tag{7.22}$$

Алгоритм 7.1. Данные: *Примитивный многочлен $f(x) \in \mathbb{Z}[x]$ без кратных корней.*
Найти: *Разложение $f(x)$ на неприводимые множители.*
1. Положить $\mathcal{M} = \{f\}$. Найти минимальное простое число p, не делящее $R(f(x), f'(x))$.
2. Если $\deg f = 1$, СТОП. Множество $\mathcal{M}$ содержит все неприводимые делители исходного многочлена.
3. Найти при помощи алгоритма Берлекэмпа какой–нибудь многочлен $h(x) \in \mathbb{Z}[x]$ со старшим коэффициентом 1, неотрицательными коэффициентами, не превосходящими p, и такой, что $(h(x) \bmod p)$ — неприводимый делитель многочлена $(f(x) \bmod p)$ в $F_p[x]$.
4. Положить $n = \deg f$, $l = \deg h$. Если $l = n$, СТОП. Множество $\mathcal{M}$ содержит все неприводимые делители исходного многочлена.
5. Найти наименьшее натуральное k, такое что

$$p^{kl} > 2^{n(n-1)}|f|^{2n-1}.$$

6. При помощи леммы Гензеля (лемма 7.1) так изменить $h(x)$, не меняя многочлена $(h(x) \bmod p)$, чтобы многочлен $(h(x) \bmod p^k)$ делил многочлен $(f(x) \bmod p^k)$ в $(\mathbb{Z}/p^k\mathbb{Z})[x]$ и коэффициенты многочлена $h(x)$ не превосходили p^k.

7. Найти наибольшее натуральное s, такое что $l \leqslant (n-1)/2^s$, и полагая последовательно

$$m = \left[\frac{n-1}{2^s}\right], \left[\frac{n-1}{2^{s-1}}\right], \ldots, \left[\frac{n-1}{2}\right], n-1, \tag{7.23}$$

проделать следующие операции:
7.1 Найти LLL–приведенный базис $\{b_1, \ldots, b_{m+1}\}$ решетки

$$\Lambda = \mathrm{span}_{\mathbb{Z}}\left(\left\{p^k x^i \;\middle|\; 0 \leqslant i < l\right\} \cup \left\{h(x)x^j \;\middle|\; 0 \leqslant j \leqslant m-l\right\}\right).$$

7.2 Если

$$|b_1| \geqslant (p^{kl}/|f|^m)^{1/n} \tag{7.24}$$

и $m < n-1$, то перейти к следующему значению m из (7.23).
7.3 Если справедливо неравенство (7.24), *но $m = n-1$, то СТОП. Множество $\mathcal{M}$ содержит все неприводимые делители исходного многочлена.*
7.4 Если же

$$|b_1| < (p^{kl}/|f|^m)^{1/n}, \tag{7.25}$$

найти максимальный индекс t, такой что $|b_t| < (p^{kl}/|f|^m)^{1/n}$, и вычислить наибольший общий делитель $h_0(x) = (b_1, \ldots, b_t)$ многочленов $b_1, \ldots, b_t$. Исключить $f(x)$ из множества $\mathcal{M}$ и добавить в $\mathcal{M}$ пару многочленов $h_0(x)$, $f(x)/h_0(x)$. Положить $f(x) = f(x)/h_0(x)$ и перейти в пункт 2.

Для того, чтобы доказать корректность этого алгоритма, нам понадобится несколько вспомогательных утверждений. Как и прежде, считаем, что многочлен $f(x) \in \mathbb{Z}[x]$ примитивен и не имеет кратных корней, а p — минимальное простое число, не делящее $R(f(x), f'(x))$.

Лемма 7.2. *Пусть $h(x) \in \mathbb{Z}[x]$ — многочлен со старшим коэффициентом 1, такой, что многочлен $(h(x) \bmod p)$ неприводим в $F_p[x]$, многочлен $(h(x) \bmod p^k)$ делит многочлен $(f(x) \bmod p^k)$ в $(\mathbb{Z}/p^k\mathbb{Z})[x]$, но $(h(x) \bmod p^k)^2$ не делит $(f(x) \bmod p^k)$ в $(\mathbb{Z}/p^k\mathbb{Z})[x]$.*

Тогда существует такой неприводимый делитель $h_0(x) \in \mathbb{Z}[x]$ многочлена $f(x)$, что $(h(x) \bmod p)$ делит $(h_0(x) \bmod p)$, причем

этот делитель определен однозначно с точностью до знака. Кроме того, если $g(x) \in \mathbb{Z}[x]$ *— некоторый делитель многочлена* $f(x)$*, то следующие утверждения эквивалентны:*

(i) $(h(x) \bmod p)$ *делит* $(g(x) \bmod p)$ *в* $F_p[x]$,

(ii) $(h(x) \bmod p^k)$ *делит* $(g(x) \bmod p^k)$ *в* $(\mathbb{Z}/p^k\mathbb{Z})[x]$,

(iii) $h_0(x)$ *делит* $g(x)$ *в* $\mathbb{Z}[x]$.

Доказательство. Существование $h_0(x)$ следует из неприводимости $(h(x) \bmod p)$ и делимости $(f(x) \bmod p)$ на $(h(x) \bmod p)$. Однозначность следует из того факта, что $(h(x) \bmod p)^2$ не делит $(f(x) \bmod p)$.

Импликации (ii) $\Rightarrow$ (i) и (iii) $\Rightarrow$ (i) очевидны.

Предположим теперь, что выполняется утверждение (i). Тогда из того, что $(h(x) \bmod p)^2$ не делит $(f(x) \bmod p)$ следует, что $(h(x) \bmod p)$ не делит $(f(x)/g(x) \bmod p)$. Стало быть, $h_0(x)$ не делит $f(x)/g(x)$ в $\mathbb{Z}[x]$, то есть справедливо утверждение (iii). Далее, в силу неприводимости $(h(x) \bmod p)$, многочлены $(h(x) \bmod p)$ и $(f(x)/g(x) \bmod p)$ взаимно просты в $F_p[x]$. Следовательно, так как F_p — поле, существуют такие многочлены $\lambda_1(x), \mu_1(x), \nu(x) \in \mathbb{Z}[x]$, что

$$\lambda_1(x)h(x) + \mu_1(x)f(x)/g(x) = 1 - p\nu(x).$$

Домножая обе части этого равенства на $1 + p\nu(x) + (p\nu(x))^2 + \ldots + (p\nu(x))^{k-1}$ и на $g(x)$, получаем, что для некоторых многочленов $\lambda_2(x)$, $\mu_2(x) \in \mathbb{Z}[x]$ выполняется сравнение

$$\lambda_2(x)h(x) + \mu_2(x)f(x) \equiv g(x) \pmod{p^k\mathbb{Z}[x]}.$$

Но $(f(x) \bmod p^k)$ делится на $(h(x) \bmod p^k)$. Стало быть, и $(g(x) \bmod p^k)$ делится на $(h(x) \bmod p^k)$, то есть утверждение (ii) также верно. □

Лемма 7.3. *Пусть многочлены* $h(x), h_0(x) \in \mathbb{Z}[x]$ *— такие же, как в лемме 7.2 и пусть* $\deg h = l$*. Пусть* m *— некоторое натуральное число,* $m \geqslant l$*. Пусть* Λ *— решетка вида* (7.22)*. Пусть многочлен* $b(x) \in \Lambda$*, то есть многочлен из кольца* $\mathbb{Z}[x]$*, делящийся на* $h(x)$ *по*

модулю p^k, $\deg b \leqslant m$, *удовлетворяет неравенству*

$$|b|^n |f|^m < p^{kl}. \tag{7.26}$$

Тогда $h_0(x)$ *делит наибольший общий делитель* $(f(x), b(x))$ *многочленов* $f(x)$ *и* $b(x)$. *В частности,* $b(x)$ *делится на* $h_0(x)$.

Доказательство. 1. Положим

$$g(x) = (f(x), b(x)), \quad f_1(x) = f(x)/g(x), \quad b_1(x) = b(x)/g(x).$$

Тогда $(f_1(x), b_1(x)) = 1$ и, стало быть, для любых многочленов $\lambda(x)$, $\mu(x) \in \mathbb{Z}[x]$, таких, что $\deg \lambda < \deg b_1$ и $\deg \mu < \deg f_1$,

$$\lambda(x) f_1(x) + \mu(x) b_1(x) \neq 0. \tag{7.27}$$

Обозначим буквой M решетку, состоящую из многочленов $\lambda(x)f(x) + \mu(x)b(x)$, где $\lambda(x), \mu(x)$ — произвольные многочлены с целыми коэффициентами, удовлетворяющие неравенствам $\deg \lambda < \deg b_1$, $\deg \mu < \deg f_1$.

Очевидно, что все многочлены из M имеют степень меньшую, чем $\deg b + \deg f - \deg g$, и делятся на $g(x)$. В частности, M не содержит ненулевых многочленов степени, меньшей $\deg g$. Далее, очевидно, что решетка M порождается многочленами

$$x^i f(x), \ x^j b(x), \qquad 0 \leqslant i < \deg b_1, \ 0 \leqslant j < \deg f_1.$$

При этом из (7.27) следует, что эти многочлены линейно независимы над $\mathbb{Z}$. Следовательно, они образуют базис решетки M. Применяя неравенство Адамара (теорема 7.7) к решетке M и этому базису, получаем:

$$\det \mathrm{M} \leqslant |f|^{\deg b_1} |b|^{\deg f_1} \leqslant |f|^m |b|^n < p^{kl}. \tag{7.28}$$

Далее в предположении, что $h_0(x) \nmid g(x)$, будет получена оценка снизу величины $\det \mathrm{M}$, противоречащая (7.28). Это завершит доказательство леммы.

2. Предположим теперь, что $h_0(x)$ не делит $g(x)$ в $\mathbb{Z}[x]$. Тогда, по лемме 7.2, $(h(x) \bmod p)$ не делит $(g(x) \bmod p)$ в $F_p[x]$, откуда, в

силу неприводимости $(h(x) \bmod p)$ в $F_p[x]$, следует, что наибольший общий делитель $(h(x) \bmod p)$ и $(g(x) \bmod p)$ равен 1. Стало быть, существуют такие многочлены $\lambda_1(x), \mu_1(x), \nu_1(x) \in \mathbb{Z}[x]$, что

$$\lambda_1(x)h(x) + \mu_1(x)g(x) = 1 - p\nu_1(x).$$

Домножая обе части этого равенства на $1 + p\nu_1(x) + (p\nu_1(x))^2 + \ldots + (p\nu_1(x))^{k-1}$, получаем, что для некоторых многочленов $\lambda_2(x), \mu_2(x)$, $\nu_2(x) \in \mathbb{Z}[x]$

$$\lambda_2(x)h(x) + \mu_2(x)g(x) = 1 - p^k\nu_2(x). \tag{7.29}$$

Рассмотрим две подрешетки

$$\begin{aligned} \mathrm{M}_1 &= \left\{u(x) \in \mathrm{M} \;\middle|\; \deg u < \deg g + \deg h\right\} \subset \mathrm{M}, \\ \mathrm{M}_2 &= \left\{u(x) \in \mathrm{M} \;\middle|\; x^{\deg g + \deg h} \mid u(x)\right\} \subset \mathrm{M}. \end{aligned} \tag{7.30}$$

Из определений этих подрешеток следует, что $\mathrm{M} = \mathrm{M}_1 \oplus \mathrm{M}_2$. Согласно теореме 7.5,

$$\det \mathrm{M} = \det \mathrm{M}_1 \cdot \det \mathrm{M}_2 \geqslant \det \mathrm{M}_1.$$

Рассмотрим произвольный многочлен $u(x) \in \mathrm{M}_1$. Так как $\mathrm{M}_i \subset \mathrm{M}$, имеем $g(x) \mid u(x)$. Домножая равенство (7.29) на многочлен $v(x) = u(x)/g(x) \in \mathbb{Z}[x]$, получаем, что

$$v(x) = \lambda_2(x)v(x)h(x) + \mu_2(x)u(x) + p^k\nu_2(x)v(x). \tag{7.31}$$

Согласно условию леммы 7.2 и соотношению $b(x) \in \Lambda$, многочлены $b(x) \bmod p^k$ и $f(x) \bmod p^k$ делятся в кольце $(\mathbb{Z}/p^k\mathbb{Z})[x]$ на многочлен $(h(x) \bmod p^k)$. Следовательно, в силу определения решетки M, многочлен $(u(x) \bmod p^k)$ делится в кольце $(\mathbb{Z}/p^k\mathbb{Z})[x]$ на $(h(x) \bmod p^k)$. Из равенства (7.31) теперь следует, что в том же кольце многочлен $(v(x) \bmod p^k)$ делится на многочлен $(h(x) \bmod p^k)$. Поскольку

$$\deg v = \deg u \cdot \deg g < \deg h$$

и старший коэффициент $h(x)$ равен 1, из равенства (7.31) следует, что $v(x) \equiv 0 \bmod p^k$. Но тогда $u(x) \equiv 0 \bmod p^k$.

3. Если рассматривать многочлены $f(x)$ и $b(x)$ как многочлены над $\mathbb{Q}$, то их наибольший общий делитель можно представить в виде линейной комбинации $f(x)$ и $b(x)$ с полиномиальными коэффициентами, откуда следует, что для некоторых многочленов $\lambda(x), \mu(x) \in \mathbb{Z}[x]$, таких, что $\deg\lambda < \deg b_1$ и $\deg\mu < \deg f_1$, и некоторого числа $c \in \mathbb{Z}$, отличного от нуля, выполняется равенство

$$\lambda(x)f(x) + \mu(x)b(x) = cg(x).$$

Поэтому $cg(x)x^i \in \mathrm{M}_1$, $i = 0, 1, \ldots, l-1$, где $l = \deg h$, и размерность решетки M_1 равна l. По доказанному, коэффициенты каждого многочлена из M_1 делятся на p^k. Следовательно, $p^{kl} \mid \det \mathrm{M}_1$ и, стало быть,

$$\det \mathrm{M} \geqslant \det \mathrm{M}_1 \geqslant p^{kl},$$

что противоречит неравенству (7.28). То есть предположение, что $h_0(x)$ не делит $(f(x), b(x))$, не верно.

Лемма доказана. □

Если $f(x), g(x)$ — многочлены с целыми коэффициентами и $g(x) \mid f(x)$, то коэффициенты $g(x)$ не могут быть слишком большими по сравнению с коэффициентами $f(x)$. Утверждения подобного рода хорошо известны в теории чисел. Следующий вариант принадлежит М. Миньотту.

Предложение 7.3. *Если $f(x)$ и $g(x)$ — произвольные многочлены из $\mathbb{Z}[x]$, $g(x)$ делит $f(x)$ и $\deg g \leqslant m$, то*

$$|g|^2 \leqslant \binom{2m}{m} |f|^2.$$

Лемма 7.4. *Пусть выполняются условия леммы 7.3. Пусть также $\{b_1(x), \ldots, b_{m+1}(x)\}$ — LLL–приведенный базис решетки Λ и*

$$p^{kl} > 2^{nm/2} \binom{2m}{m}^{1/2} |f|^{m+n}. \tag{7.32}$$

Тогда $\deg h_0 \leqslant m$ *в том и только том случае, если*

$$|b_1| < (p^{kl}/|f|^m)^{1/n}. \tag{7.33}$$

Доказательство. Если справедливо неравенство (7.33), то по лемме 7.3 многочлен $h_0(x)$ делит многочлен $b_1(x)$, степень которого не превосходит m в силу принадлежности решетке Λ. В одну сторону утверждение доказано.

Предположим, что $\deg h_0 \leqslant m$. Тогда $h_0(x) \in \Lambda$ и, в силу пункта (iv) теоремы 7.10, $|b_1| \leqslant 2^{m/2}|h_0|$. Из предложения 7.3 следует, что $|h_0| \leqslant \binom{2m}{m}^{1/2}|f|$. Из (7.32) следует, что

$$2^{nm}\binom{2m}{m}^{n/2}|f|^n < \frac{p^{kl}}{|f|^m}\,.$$

Получаем, что

$$|b_1|^n \leqslant 2^{mn/2}|h_0|^n \leqslant 2^{mn/2}\binom{2m}{m}^{n/2}|f|^n < \frac{p^{kl}}{|f|^m}\,,$$

и это доказывает (7.33). □

Лемма 7.5. *В условиях леммы 7.4 рассмотрим максимальный индекс* t*, такой что*

$$|b_t| < (p^{kl}/|f|^m)^{1/n}. \tag{7.34}$$

Тогда

$$\deg h_0 = m + 1 - t,$$
$$h_0(x) = (b_1(x), \ldots, b_t(x))$$

и

$$|b_j| < (p^{kl}/|f|^m)^{1/n} \quad \text{для всех} \quad j = 1, \ldots, t. \tag{7.35}$$

Доказательство. Обозначим через J множество тех индексов j, для которых справедливо неравенство $|b_j| < (p^{kl}/|f|^m)^{1/n}$. Из леммы 7.3 следует, что $h_0(x)$ делит $b_j(x)$ для каждого $j \in J$. Обозначим через

$h_1(x)$ наибольший общий делитель многочленов $b_j(x)$, индексы которых принадлежат множеству J. Тогда, в силу своей примитивности, $h_0(x)$ делит $h_1(x)$. Каждый многочлен $b_j(x)$ при $j \in J$ делится на $h_1(x)$ и имеет степень не больше m. Следовательно, каждый такой многочлен принадлежит решетке

$$\mathbb{Z}h_1(x) + \mathbb{Z}h_1(x)x + \ldots + \mathbb{Z}h_1(x)x^{m-\deg h_1}.$$

Размерность этой решетки равна $m + 1 - \deg h_1$, а многочлены $b_j(x)$ как векторы линейно независимы, стало быть, если обозначить мощность множества J через $\sharp J$, то

$$\sharp J \leqslant m + 1 - \deg h_1. \tag{7.36}$$

Далее, многочлены $h_0(x)x^i$, $i = 0, 1, \ldots, m - \deg h_0$, линейно независимы и лежат в решетке Λ. Кроме того, $|h_0(x)x^i| = |h_0|$ для всех i. Следовательно, применив пункт (v) теоремы 7.10, предложение 7.3 и неравенство (7.32), получим, что для всех $j = 1, \ldots, m + 1 - \deg h_0$

$$|b_j| \leqslant 2^{m/2}|h_0| \leqslant 2^{m/2}\binom{2m}{m}^{1/2}|f| < (p^{kl}/|f|^m)^{1/n},$$

то есть

$$\{1, \ldots, m + 1 - \deg h_0\} \subseteq J$$

и

$$\sharp J \geqslant m + 1 - \deg h_0.$$

Из (7.36) теперь следует, что $\deg h_1 \leqslant \deg h_0$. Ввиду соотношения $h_0(x) \mid h_1(x)$, получаем, что

$$\deg h_0 = \deg h_1 = m + 1 - t$$

и

$$J = \{1, \ldots, t\}.$$

Остается показать, что $h_0(x)$ совпадает с $h_1(x)$ с точностью до знака, для чего достаточно доказать примитивность $h_1(x)$.

Если $h_1(x)$ не примитивен, то найдется такой индекс $j \in J$, что и $b_j(x)$ не примитивен. Пусть d_j — наибольший общий делитель коэффициентов многочлена $b_j(x)$. Тогда $d_j \neq 1$, но $b_j(x)/d_j$ делится на $h_0(x)$, поскольку последний многочлен примитивен как делитель примитивного многочлена $f(x)$. Имеем $h_0(x) \in \Lambda$. Но тогда и $b_j(x)/d_j \in \Lambda$, чего не может быть, поскольку $b_j(x)$ — элемент базиса решетки Λ. Стало быть, многочлен $h_1(x)$ примитивен. □

Теорема 7.19. *Алгоритм 7.1 находит разложение $f(x)$ на неприводимые множители.*

Доказательство. Из леммы 7.5 следует, что каждый раз, когда при проходе пункта 7.4 выполняется неравенство (7.25), алгоритм для текущего многочлена $f(x)$ вычисляет неприводимый делитель $h_0(x)$, определяемый в лемме 7.2.

Следовательно, в каждый момент работы алгоритма множество $\mathcal{M}$ содержит текущее значение многочлена $f(x)$ и какое–то количество неприводимых над $\mathbb{Z}$ многочленов. При этом произведение всех многочленов, содержащихся в $\mathcal{M}$, всегда равно исходному значению многочлена $f(x)$.

Если алгоритм завершается в пункте 2 или пункте 4, то множество $\mathcal{M}$ в итоге состоит из неприводимых делителей исходного многочлена.

Если перед входом в пункт 7 текущий многочлен $f(x)$ приводим, то многочлен $h_0(x)$, определяемый в лемме 7.2, обязан быть собственным делителем, то есть иметь степень, меньшую n. Тогда, по лемме 7.4, для некоторого m из (7.23) обязано выполняться неравенство (7.25). Следовательно, в этом случае алгоритм вычислит $h_0(x)$, увеличит количество элементов множества $\mathcal{M}$ на единицу и вернется в пункт 2.

Если же перед входом в пункт 7 текущий многочлен $f(x)$ неприводим, то многочлен $h_0(x)$, определяемый в лемме 7.2, с точностью до знака совпадает с $f(x)$. Следовательно, в силу леммы 7.4, неравенство (7.25) не выполняется ни для какого m из (7.23). То есть в этом

случае алгоритм завершится в пункте 7.3 и итоговое множество $\mathcal{M}$ будет также состоять из неприводимых делителей исходного многочлена. □

В работе [25] проведен подробный анализ количества операций, выполняемых алгоритмом 7.1, и доказана следующая

Теорема 7.20. *Алгоритм 7.1 завершит работу за* $O(n^6 + n^5 \log |f|)$ *арифметических операций. Двоичная длина чисел, над которыми эти операции производятся, равна* $O(n^3 + n^2 \log |f|)$.

Глава 8

Криптографические применения

Методы шифрования можно разделить на два типа: на *симметричные* и *асимметричные*.

При симметричном шифровании и для зашифровки, и для расшифровки сообщения применяется один и тот же ключ. Поэтому для безопасности передачи зашифрованного сообщения по открытым каналам необходимо предварительно обеим сторонам в тайне выбрать единый ключ, и лишь после этого начинать обмен информацией. При таком способе шифрования возникают очевидные трудности, связанные с необходимостью либо предварительной встречи, либо поиска надежного курьера, которому можно доверить секретный ключ. В частности, организовать надежный конфиденциальный канал связи для большого числа абонентов при таком способе шифрования довольно затруднительно.

Общая идея асимметричных методов шифрования заключается в том, что для зашифровки сообщения применяется один ключ, а для расшифровки — другой. Ключ для зашифровки открыто передается по любому каналу связи, в то время как ключ для расшифровки держится в секрете. Эти ключи, как правило, являются элементами некоторых алгебраических структур и связаны друг с другом некоторым соотношением. Но параметры этих структур и соотношение подбираются такими, чтобы время, требуемое для построения секретного ключа по открытому, было несравнимо больше того времени,

которое нужно для построения открытого ключа по секретному.

Асимметричные методы шифрования обычно медленнее симметричных. Поэтому, если требуется передать большой объем информации, очень часто тело сообщения шифруют при помощи какого-нибудь симметричного алгоритма, а использующийся при этом ключ — при помощи асимметричного. Подобного рода схемы называются гибридными.

8.1 Алгоритм Диффи–Хеллмана обмена ключами.

Первой работой, в которой была реализована идея асимметричного криптографического преобразования, является работа [21]. Авторы этой работы использовали тот факт, что задача дискретного логарифмирования в мультипликативной группе F_p^* поля F_p, где p — простое число, существенно сложнее задачи возведения в степень.

Отметим, что это обстоятельство можно очень легко использовать для защиты произвольного ресурса, будь то компьютер, или канал связи, от несанкционированного доступа. Для этого нужно выбрать достаточно большое простое число p и какую-нибудь образующую g группы F_p^*. Далее, каждый пользователь "придумывает" себе секретный пароль $t \in \mathbb{Z}$ и вычисляет элемент g^t поля F_p, который система и будет воспринимать как идентификатор данного пользователя. И каждый раз, когда пользователь решает войти в систему, он вводит свой секретный пароль t, система вычисляет g^t и сравнивает результат с идентификатором пользователя. Возможность взлома такой системы зависит от способности злоумышленника вычислять дискретный логарифм по основанию g от идентификатора пользователя, то есть выбор достаточно больших p может обеспечить необходимую безопасность. Отметим однако, что образующую g нужно выбирать не слишком маленькой, чтобы исключить возможность найти g перебором.

Алгоритм же, о котором сейчас пойдет речь, позволяет двум лицам, общающимся по незащищенному каналу связи, без предварительного обмена секретной информацией выработать общий ключ, который будет известен только им двоим. Предположим, абонент A и абонент B выбрали простое число p и образующую g группы F_p^*. Случайным образом абонент A выбирает секретный ключ $a \in \mathbb{Z}$, $2 \leqslant a \leqslant p-2$, а абонент B — секретный ключ $b \in \mathbb{Z}$, $2 \leqslant b \leqslant p-2$.

Алгоритм 8.1. *Данные: Простое число p, первообразный корень g по модулю p, секретный ключ a абонента A и секретный ключ b абонента B.*
Найти: Общий ключ $k \in F_p^*$, известный только абонентам A и B.
1. Абоненту A вычислить $x = g^a$ и передать результат абоненту B.
2. Абоненту B вычислить $y = g^b$ и передать результат абоненту A.
3. Абоненту A положить $k = y^a$,
4. Абоненту B положить $k = x^b$.

Корректность данного алгоритма следует из равенства $k = (g^a)^b = (g^b)^a$. Открытыми ключами здесь являются элементы g^a и g^b. Они передаются по незащищенному каналу связи, поэтому могут стать известными третьим лицам. Но если число p было выбрано достаточно большим, то для того, чтобы по известным g^a и g^b при помощи существующих на данный момент алгоритмов найти секретные числа a и b (и, соответственно, g^{ab}), потребуется очень много времени, что и обеспечивает требуемую безопасность. Аналогично, абоненты A и B не смогут за приемлемое время вычислить секретные ключи друг друга, то есть каждый из них при смене собеседника может не менять свой секретный ключ. Однако стоит отметить уязвимость данной схемы относительно так называемой “атаки посередине”, в которой нарушитель выступает в качестве абонента–посредника между абонентами A и B. Если злоумышленнику удалось убедить абонента A воспринять его как абонента B, а абонента B — соответственно, как A, то наладив

с каждым из них связь при помощи алгоритма Диффи–Хеллмана, он получает полный контроль за перепиской, включая возможность искажения информации и навязывания ложной. Чтобы предотвратить подобную возможность, используют алгоритмы аутентификации (см. пункт 8.3).

Отметим также, что алгоритм 8.1 по своей структуре несколько отличается от изложенных ранее. Обычно предполагается, что у алгоритма ровно один исполнитель, и по этой причине команды имеют безадресный характер. Что же касается алгоритмов типа алгоритма 8.1, то они предполагают как минимум двоих исполнителей. Поэтому такие алгоритмы носят название *протоколов*.

8.2 Алгоритм RSA.

Вскоре после появления алгоритма Диффи–Хеллмана был придуман наиболее популярный на сегодня алгоритм асимметричного шифрования RSA, названный по первым буквам фамилий авторов работы [28], в которой он был описан. Этот алгоритм использует тот факт, что на данный момент не существует слишком быстрых алгоритмов разложения целых чисел на множители.

Процедура построения абонентом секретного и открытого ключей состоит в следующем. Абонент выбирает два простых числа p, q и вычисляет их произведение $n = pq$. Затем абонент случайным образом выбирает два натуральных числа e, d, меньших $\varphi(n) = (p-1)(q-1)$, удовлетворяющих сравнению

$$ed \equiv 1 \pmod{\varphi(n)}. \tag{8.1}$$

Открытым ключом данного абонента будет пара (n, e). Секретным ключом — число d. Числа p и q также должно держать в секрете, но рассматривать всю тройку (p, q, d) в качестве секретного ключа необязательно, потому что числа p, q используются только на стадии генерации чисел n, e, d. Поэтому числа p, q можно уничтожить. Отме-

тим, что любые целые e и d, удовлетворяющие (8.1), взаимно просты с $\varphi(n)$.

Алгоритм 8.2. *Данные: Открытый ключ (n, e) и секретный ключ d абонента A.*
Требуется: Передать абоненту A сообщение $x \in \mathbb{Z}/n\mathbb{Z}$ абонента B.
1. Абоненту B вычислить $y = x^e$ и передать результат абоненту A.
2. Абоненту A положить $x = y^d$.

В кольце $\mathbb{Z}/n\mathbb{Z}$ справедливо тождество $x^{\varphi(n)} = 1$. Поэтому $y^d = x^{ed} = x$. Следовательно, алгоритм корректен.

Как легко видеть, данный алгоритм предлагает простой способ большому числу абонентов обмениваться друг с другом конфиденциальной информацией по незащищенным каналам связи. Для этого каждому абоненту нужно завести секретный и открытый ключи, выложив последний в открытый доступ. Тогда любой другой абонент сможет послать ему сообщение, зашифрованное при помощи этого открытого ключа, расшифровать которое за разумное время сможет только адресат.

Стоит отметить, что не все наборы (p, q, d), пусть даже числа p и q велики, представляются надежными. Например, если число $n + 1$ или число $n - 1$ легко раскладывается на множители (скажем, является степенью двойки), то для числа n можно успешно применить $(N \pm 1)$–методы факторизации, то есть секретный ключ в этом случае найдется довольно быстро. Кроме того, числа p и q не должны быть слишком близкими, так как тогда они будут близки к $\sqrt{n}$ и число n можно будет быстро разложить на множители при помощи метода факторизации Ферма. Необходимо также, чтобы ни $p - 1$, ни $q - 1$ не являлось произведением маленьких простых чисел, ибо в этом случае число n можно будет быстро факторизовать при помощи $(p - 1)$–метода Полларда. В пункте 8.4 мы опишем ряд приемов, позволяющих злоумышленнику в некоторых случаях взломать систему RSA за относительно короткое время.

8.3 Электронная цифровая подпись.

Алгоритм RSA позволяет организовать систему защищенного обмена информацией для большого количества абонентов. Но пользуясь этим алгоритмом в том виде, в котором он пока описан, получатель сообщения, вообще говоря, не может определить, от кого оно было послано. Небольшая модификация алгоритма 8.2 позволяет проверить авторство сообщения. Нам придется рассматривать сравнения по разным модулям, поэтому для удобства через $a \bmod b$ мы будем обозначать минимальное неотрицательное число, сравнимое с a по модулю b (остаток от деления a на b).

Алгоритм 8.3. *Данные: Открытый ключ (n_A, e_A) и секретный ключ d_A абонента A, открытый ключ (n_B, e_B) и секретный ключ d_B абонента B, $n_A \geqslant n_B$.*
Требуется: Передать абоненту A сообщение $x \in \mathbb{Z}$ абонента B с подтверждением авторства.
1. Абоненту B вычислить

$$y = x^{e_A} \bmod n_A \quad \text{и} \quad s = (x^{d_B} \bmod n_B)^{e_A} \bmod n_A,$$

после чего передать пару (y, s) абоненту A.
2. Абоненту A вычислить

$$x = y^{d_A} \bmod n_A \quad \text{и} \quad t = (s^{d_A} \bmod n_A)^{e_B} \bmod n_B.$$

Если $x = t$, считать сообщение достоверным. Если же $x \neq t$, то сообщение недостоверно.

Корректность данного алгоритма следует из сравнений $s^{e_A d_A} \equiv s \pmod{n_A}$, $x^{e_B d_B} \equiv x \pmod{n_B}$ и неравенства $n_A \geqslant n_B$. Действительно, из определения s следует $s^{d_A} \pmod{n_A} = x^{d_B} \pmod{n_b}$. Поэтому

$$t = \left(s^{d_A} (\mathrm{mod} n_A)\right)^{e_B} (\mathrm{mod} n_B) = \\ = \left(x^{d_B} (\mathrm{mod} n_B)\right)^{e_B} (\mathrm{mod} n_B) = x (\mathrm{mod} n_B) = x.$$

"Подписью" в данном случае будет число s. Без особого труда s можно вычислить лишь, зная секретный ключ d_B, поэтому если x и t совпали, то с большой долей уверенности можно говорить о том, что автором сообщения был действительно абонент B. Подпись, как правило, еще усиливают функцией *хеширования* — функцией, ставящей в соответствие произвольному целому числу x некоторое целое число $h(x)$ фиксированного размера. От функции хеширования требуется, чтобы $h(x)$ вычислялось по заданному x достаточно быстро, но чтобы при этом по заданному y было алгоритмически сложно найти такое x, что $h(x) = y$. Часто на функцию хеширования накладывается более сильное требование: чтобы задача поиска для заданного x хотя бы одного элемента в полном прообразе $h(x)$, отличного от x, была алгоритмически сложной, или, более общо, чтобы алгоритмически сложно было найти хотя бы одну пару чисел, на которых функция h дает одинаковые значения. Со встроенной функцией хеширования алгоритм 8.3 будет выглядеть следующим образом:

Алгоритм 8.4. *Данные: Открытый ключ* (n_A, e_A) *и секретный ключ* d_A *абонента* A*, открытый ключ* (n_B, e_B) *и секретный ключ* d_B *абонента* B*,* $n_A \geqslant n_B$*, функция хеширования* h*.*
Требуется: Передать абоненту A *сообщение* $x \in \mathbb{Z}$ *абонента* B *с подтверждением авторства.*
1. Абоненту B *вычислить*

$$y = x^{e_A} \bmod n_A \quad \text{и} \quad s = (h(x)^{d_B} \bmod n_B)^{e_A} \bmod n_A,$$

после чего передать пару (y, s) *абоненту* A*.*
2. Абоненту A *вычислить*

$$x = y^{d_A} \bmod n_A \quad \text{и} \quad t = (s^{d_A} \bmod n_A)^{e_B} \bmod n_B.$$

Если $t = h(x)$*, считать сообщение достоверным. Если же* $t \neq h(x)$*, то сообщение недостоверно.*

8.4 Об уязвимости системы RSA.

Общий модуль. Если пары ключей выдаются пользователям одним центральным распределяющим органом, то может возникнуть желание зафиксировать единый для всех модуль $n = pq$ и генерировать лишь пары чисел e и d. Как оказывается, данный подход нарушает безопасность системы, ибо, как видно из следующей теоремы, любой пользователь, обладающий открытым и секретным ключами, может за короткое время найти разложение $n = pq$ и, таким образом, способен быстро восстанавливать секретный ключ по любому открытому.

Теорема 8.1. *Пусть натуральные числа n, e, d удовлетворяют условиям $ed \equiv 1 \pmod{\varphi(n)}$, $e < \varphi(n)$, $d < \varphi(n)$ и пусть $n = pq$, где p и q — нечетные простые числа. Тогда существует полиномиальный вероятностный алгоритм, при помощи которого, зная числа n, e, d, можно найти разложение числа n. Обратно, зная разложение числа n и число e, можно за полиномиальное время найти d.*

Доказательство. Последнее утверждение теоремы очевидно, зная разложение $n = pq$, можно вычислить $\varphi(n)$ по формуле $\varphi(n) = (p-1)(q-1)$, после чего при помощи алгоритма Евклида найти для числа e соответствующее число d.

Предположим теперь, что известны числа n, e и d. Положим $r = ed - 1$. Тогда r делится на $\varphi(n)$. Но $\varphi(n)$ делится на 4, стало быть, $r = 2^s t$, где $s \geqslant 2$, а t нечетно. Для любого числа g, взаимно простого с n, справедливо сравнение $g^r \equiv 1 \pmod{n}$.

Оценим количество чисел g, взаимно простых с n и удовлетворяющих хотя бы одному из сравнений

$$g^t \equiv 1 \pmod{n}, \qquad g^{2^k t} \equiv -1 \pmod{n}, \qquad 0 \leqslant k < s. \tag{8.2}$$

Обозначим $d = \min(\nu_2(p-1), \nu_2(q-1)) \geqslant 1$. Согласно теоремам 1.16 и 1.17 сравнение $x^t \equiv 1 (\bmod n)$ разрешимо и имеет не более $(t, p-1) \cdot (t, q-1) \leqslant \frac{p-1}{2^d} \cdot \frac{q-1}{2^d}$ решений. Обозначим $T = \frac{(p-1)(q-1)}{4^d}$. В соответствии с теми же теоремами сравнение $x^{2^k t} \equiv -1 (\bmod n)$ разрешимо лишь

для $k < d$ и в этом случае имеет не более $(2^k t, p-1)\cdot(2^k t, q-1) \leqslant 4^k T$ решений. Таким образом, количество чисел g, удовлетворяющих хотя бы одному из сравнений (8.2), может быть оценено сверху величиной

$$T\left(1+\sum_{k=0}^{d-1} 4^k\right) = T\frac{4^d+2}{3} \leqslant T\frac{4^d}{2} = \frac{\varphi(n)}{2}.$$

Таким образом, множество S целых чисел g в промежутке от 1 до n, взаимно простых с n и не удовлетворяющих ни одному из сравнений (8.2), содержит не менее $\frac{\varphi(n)}{2}$ элементов.

Выбрав случайным образом на промежутке $[1; n]$ целое число g, взаимно простое с n, мы с вероятностью, не меньшей $\frac{1}{2}$ получим $g \in S$. Пусть m — наименьшее целое число с условием $g^{2^{m+1}t} \equiv 1 \pmod{n}$. Так как $g \in S$ имеем $0 \leqslant m < s$. Пусть $h = g^{2^m t}$. Согласно определению m имеем $h \not\equiv 1 \pmod{n}$, а, поскольку $g \in S$, заключаем, что $h \not\equiv -1 \pmod{n}$. В то же время из сравнений $h^2 \equiv 1 \pmod{p}$, $h^2 \equiv 1 \pmod{q}$ следует, что $h \equiv \pm 1 \pmod{p}$, $h \equiv \pm 1 \pmod{q}$. По доказанному знаки в правых частях этих двух сравнений различны. Но тогда наибольший общий делитель $(h-1, n)$ отличен от 1 и n. Значит, он будет нетривиальным делителем n, а потому будет равен p или q.

Полиномиальность приведенного вероятностного алгоритма очевидна. □

Мультипликативность. Предположим, злоумышленник хочет, чтобы абонент A, обладающий открытым ключом (n, e) и секретным ключом d, поставил свою подпись под некоторым сообщением x. Если сообщение выглядит подозрительно, абонент не станет его подписывать. В этом случае злоумышленник может сделать следующее. Выбрав случайным образом число r, взаимно простое с n, и положив $x' \equiv r^e x \pmod{n}$, злоумышленник может предложить абоненту A подписать сообщение x'. Если абонент соглашается поставить свою подпись, то злоумышленник получает в свои руки сообщение $y' \equiv (x')^d \pmod{n}$, которое он легко может переделать в нужное ему, положив $y \equiv y' r^{-1} \pmod{n}$, где r^{-1} — число, обратное к r по модулю

n. Действительно,

$$y^e \equiv (x')^{de} r^{-e} \equiv x' r^{-e} \equiv x \pmod{n},$$

то есть y совпадает с сообщением x, подписанным абонентом A.

Таким образом, пользуясь тем, что y зависит от x мультипликативно, злоумышленник может скрыть от абонента истинное содержание подписываемого сообщения. Нарушить мультипликативность можно добавлением какого-нибудь определенного набора нулей и единиц в начало сообщения. Применение функции хеширования также позволяет предотвратить опасность, возникающую при мультипликативной зависимости y от x.

Малый секретный ключ. Поскольку при применении алгоритма RSA требуется возводить в степень d, может возникнуть желание взять в качестве d не очень большое число. Однако, как видно из следующей теоремы, доказанной в [31], при малом d систему можно взломать за весьма короткое время.

Теорема 8.2. *Пусть n, e, d — натуральные числа, $ed \equiv 1 \bmod \varphi(n)$, $e < \varphi(n)$, $d < n^{1/4}/3$ и пусть $n = pq$, где p и q — нечетные простые числа, такие что $q < p < 2q$. Тогда существует полиномиальный алгоритм, при помощи которого, зная числа n и e, можно найти число d.*

Доказательство. Идея состоит в том, чтобы использовать известное число n для приближения неизвестного $\varphi(n)$. При этом можно, конечно, считать $d > 1$.

Поскольку $ed \equiv 1 \pmod{\varphi(n)}$, существует такое целое число $k \geqslant 1$, что

$$ed - k\varphi(n) = 1. \tag{8.3}$$

Согласно условию имеем $q < p < 2q$, так что $q^2 < pq = n$ и $p + q < 3q < 3\sqrt{n}$. Поскольку $\varphi(n) = n - p - q + 1$, то находим

$$0 < n - \varphi(n) = p + q - 1 < 3\sqrt{n} - 1. \tag{8.4}$$

Из (8.3) и (8.4) получаем, что

$$\left|\frac{e}{n}-\frac{k}{d}\right| = \left|\frac{ed-k\varphi(n)-kn+k\varphi(n)}{nd}\right| = \\ = \frac{k(n-\varphi(n))-1}{nd} < \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}}\,.$$

При этом из соотношения $k\varphi(n) = ed-1 < ed$ и неравенства $e < \varphi(n)$ следует, что $k < d < n^{1/4}/3$. Стало быть,

$$\left|\frac{e}{n}-\frac{k}{d}\right| < \frac{3k}{d\sqrt{n}} < \frac{3}{\sqrt{n}} < \frac{1}{2d^2}\,.$$

Из теории цепных дробей известно, что в случае выполнения такого неравенства число k/d является некоторой подходящей дробью числа e/n. В силу неравенства (8.3) числа k и d взаимно просты, поэтому d в точности совпадает со знаменателем одной из подходящих дробей числа e/n. Количество же этих дробей есть величина порядка $O(\ln n)$, то есть число d восстанавливается за линейное время. □

Малый открытый ключ. Для того, чтобы число d не было слишком маленьким, часто в качестве e берут какое-нибудь небольшое число — тогда d будет гарантированно большим. Однако при слишком маленьком e может возникнуть другая проблема. Если сообщение x мало (как элемент $\mathbb{Z}$) по сравнению с n, то получить его из x^e можно при помощи обыкновенного извлечения корня степени e в $\mathbb{Z}$. По этой причине перед возведением в степень сообщение x, как правило, несколько видоизменяют, например, добавляют к его двоичной записи единицу и сколько-то нулей, чтобы итоговое число получилось достаточно большим. Однако и такой прием не всегда может гарантировать безопасность при слишком малом e, ибо злоумышленник может воспользоваться возможностями, которые дает следующая теорема, принадлежащая Копперсмиту. Эта теорема позволяет искать при помощи LLL–алгоритма небольшие корни многочленов с целыми коэффициентами по составному модулю, разложение которого на простые не известно.

Теорема 8.3. *Пусть n — натуральное число и $f(t) \in \mathbb{Z}[t]$ — многочлен степени s со старшим коэффициентом 1. Пусть также фиксировано некоторое число $\varepsilon > 0$. Тогда существует алгоритм, сложность которого полиномиально зависит от величины $\ln n$, при помощи которого можно найти все такие целые числа t_0, что $|t_0| < n^{1/s-\varepsilon}$ и $f(t_0) \equiv 0 \pmod{n}$.*

Доказательство. Положим

$$m = \left[\frac{\ln n}{s}\right], \quad B = \left[n^{1/s-\varepsilon}\right]$$

и рассмотрим многочлены

$$g_{u,v}(t) = n^{m-v} t^u f(t)^v, \quad v = 0, \ldots, m, \quad u = 0, \ldots, s-1.$$

Из равенства $\deg g_{u,v} = u + sv$ следует, что степени всех многочленов $g_{u,v}(t)$ различны и не превосходят $s(m+1) - 1$.

Любое целое число, являющееся корнем многочлена $f(t)$ по модулю n, является корнем каждого из многочленов $g_{u,v}(t)$ по модулю n^m.

Рассмотрим множество Λ всех линейных комбинаций многочленов $g_{u,v}(Bt)$ с целыми коэффициентами. Будем, как и в главе 7, рассматривать многочлены

$$g(t) = \sum_{i=0}^{s(m+1)-1} a_i t^i \in \Lambda$$

как вектора $(a_0, \ldots, a_{s(m+1)-1})$ своих коэффициентов и определять их норму следующим образом:

$$|g| = \left(\sum_{i=0}^{s(m+1)-1} a_i^2 \right)^{1/2}.$$

Тогда множество Λ представляет из себя решетку в пространстве $\mathbb{R}^{s(m+1)}$. Из векторов, сопоставленных $g_{u,v}(Bt)$, упорядочив многочлены по возрастанию степени, можно составить треугольную матрицу.

Откуда видим, что эти вектора образуют базис решетки Λ. Размерность Λ равна $s(m+1)$, а определитель ее равен произведению старших коэффициентов многочленов $g_{u,v}(Bt)$, то есть

$$\det\Lambda = n^{sm(m+1)/2}B^{s(m+1)(s(m+1)-1)/2} = n^{(m+1)\left(\left(1-\frac{s\varepsilon}{2}\right)sm+\frac{(s-1)(1-s\varepsilon)}{2}\right)} \tag{8.5}$$

При помощи LLL–алгоритма, в силу теоремы 7.10, можно найти многочлен $h(t) = \sum_{i=0}^{s(m+1)} b_i t^i \in \mathbb{Z}[t]$, такой что $h(Bt) \in \Lambda$ и такой, что норма многочлена $h(Bt)$ оценивается следующим образом:

$$|h(Bt)| \leqslant 2^{(\dim\Lambda-1)/4}(\det\Lambda)^{1/\dim\Lambda}.$$

Тогда, учитывая (8.5) и равенства $\dim\Lambda = s(m+1)$, $m = [(\ln n)/s]$, получаем, что при достаточно большом n (и фиксированном s)

$$|h(Bt)| < n^{m\left(1-\frac{s\varepsilon}{2}\right)+1} < \frac{n^m}{\sqrt{s(m+1)}}.$$

Отсюда получаем оценку значения многочлена $h(t)$ в любой точке t_0, такой что $|t_0| \leqslant B$:

$$|h(t_0)| = \left|\sum_{i=0}^{s(m+1)-1} b_i t_0^i\right| \leqslant \sum_{i=0}^{s(m+1)-1} \left|b_i B^i\right| \leqslant$$

$$\leqslant \sqrt{s(m+1)}\left(\sum_{i=0}^{s(m+1)-1} \left|b_i B^i\right|^2\right)^{1/2} = \sqrt{s(m+1)}|h(Bt)| < n^m.$$

Здесь мы в предпоследнем неравенстве воспользовались неравенством Коши–Буняковского.

Таким образом, если $h(t_0) \equiv 0 \pmod{n^m}$, то $h(t_0) = 0$. Но многочлен $h(t)$ является линейной комбинацией с целыми коэффициентами многочленов $g_{u,v}(t)$. А, как мы отмечали, любой корень многочлена $f(t)$ по модулю n является корнем каждого из $g_{u,v}(t)$ по модулю n^m. Следовательно, если $f(t_0) \equiv 0 \pmod{n}$ и $|t_0| \leqslant B$, то $h(t_0) = 0$. Остается найти все целые корни многочлена $h(t)$, не превосходящие по

модулю числа B, после чего выбрать из них те, которые являются корнями $f(t)$ по модулю n.

Полиномиальная зависимость сложности алгоритма от $\ln n$ следует из теоремы 7.12. □

В качестве примера применения теоремы Копперсмита опишем следующий прием. Как было сказано в начале данного пункта, сообщения, которые нужно зашифровать, предварительно дополняют некоторым набором нулей и единиц. Предположим, что абонент A обладает открытым ключом (n, e) и секретным ключом d и что он хочет передать абоненту B сообщение $x \in \mathbb{N}$, длина которого в двоичной записи не больше, чем $[\log_2 n] - m$, где

$$m = \left[\frac{\log_2 n}{e^2}\right].$$

Предположим также, что перед тем, как зашифровать сообщение, абонент A приписывает к его двоичной записи случайным образом m нулей и единиц. То есть в степень e возводится число

$$x_1 = 2^m x + r_1,$$

где $0 \leqslant r_1 < 2^m$. Далее, допустим, злоумышленник смог перехватить сообщение $y_1 \equiv x_1^e \pmod{n}$ так, что оно не дошло до абонента B. Абонент A, узнав, что его сообщение не доставлено, может попытаться отправить его еще раз, используя те же ключи, но дополняя сообщение x другим набором нулей и единиц. То есть теперь в степень e будет возводиться число

$$x_2 = 2^m x + r_2$$

с некоторым $r_2 \neq r_1$, $0 \leqslant r_2 < 2^m$. Передаваться, соответственно, будет число $y_2 \equiv x_2^e \pmod{n}$.

Оказывается, если e слишком мало, то злоумышленник в большинстве случаев, зная y_1 и y_2, может при помощи теоремы Копперсмита (теорема 8.3) достаточно быстро восстановить x, вне зависимости от того, чему были равны r_1 и r_2.

Чтобы это доказать, рассмотрим многочлены $g_1(u,t), g_2(u,t) \in \mathbb{Z}[u,t]$,

$$g_1(u,t) = u^e - y_1, \quad g_2(u,t) = (u+t)^e - y_2.$$

Так как $x_2 = x_1 + r_2 - r_1$, то пара чисел $(x_1,\ r_2 - r_1)$ является общим корнем этих многочленов по модулю n. Следовательно, число $r = r_2 - r_1$ является корнем результанта $f(t) = R_u(g_1, g_2)(t) \in \mathbb{Z}[t]$ по модулю n. Степень многочлена $f(t)$ не превосходит e^2. Кроме того, $|r| < 2^m \leqslant n^{1/e^2}$. Стало быть, взяв достаточно малое ε, злоумышленник может при помощи теоремы 8.3 найти число r. После этого ему останется найти общий корень многочленов $g_1(u,r), g_2(u,r) \in \mathbb{Z}[u]$ по модулю n. Для этого он может вычислить наибольший общий делитель этих двух многочленов по модулю n и, если этот делитель линеен, получить число x_1, а по нему — и число x. При $e > 3$ этот делитель иногда оказывается не линейным, и в таких случаях данный подход может не дать искомого результата. Однако в большинстве случаев наибольший общий делитель многочленов $g_1(u,r)$ и $g_2(u,r)$ будет линейным и, соответственно, злоумышленник сможет восстановить исходное число x.

При $e = 3$ данный подход позволяет успешно взламывать систему RSA, если к сообщению перед возведением в степень e добавляется набор из нулей и единиц длины меньшей, чем $1/9$ длины самого сообщения.

Отметим, что часто рекомендуется использовать в качестве e число $F_4 = 2^{2^4} + 1 = 65537$ — наибольшее известное на данный момент простое Ферма. Это число не слишком маленькое, а возводить в эту степень можно очень быстро, так как это степень двойки плюс один.

Упражнения

Квадратичные сравнения.

1. Пусть p — простое нечетное число. Докажите, что среди чисел $1, 2, \ldots, p-1$ ровно $(p-1)/2$ квадратичных вычетов.
2. **Лемма Гаусса.** Пусть p — простое, $a \in \mathbb{Z}$, $p \nmid a$. Докажите, что если среди наименьших по модулю вычетов чисел $a \cdot 1, a \cdot 2, \ldots, a \cdot \frac{p-1}{2}$ ровно μ вычетов отрицательны, то $\left(\frac{a}{p}\right) = (-1)^{\mu}$.
3. Выведите из леммы Гаусса равенство $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
4. Пусть p и q — нечетные простые числа. Докажите квадратичный закон взаимности
$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$
Для этого докажите следующие свойства функции $f(z) = e^{2\pi i z} - e^{-2\pi i z}$:
а)
$$\prod_{k=1}^{\frac{p-1}{2}} f\Big(\frac{kq}{p}\Big) = \left(\frac{p}{q}\right) \prod_{k=1}^{\frac{p-1}{2}} f\Big(\frac{kq}{p}\Big)$$
(*Указание:* воспользуйтесь леммой Гаусса и нечетностью функции $f(z)$);
б)
$$\frac{f(qz)}{f(z)} = \prod_{k=1}^{\frac{q-1}{2}} f\Big(z + \frac{k}{q}\Big) f\Big(z - \frac{k}{q}\Big)$$
(*Указание:* воспользуйтесь тождеством $x^q - y^q = \prod_{k=0}^{q-1} \big(e^{\frac{2\pi i k}{q}} x - e^{-\frac{2\pi i k}{q}} y\big)$);
в)
$$\left(\frac{p}{q}\right) = \prod_{l=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} f\Big(\frac{l}{p} + \frac{k}{q}\Big) f\Big(\frac{l}{p} - \frac{k}{q}\Big).$$

5. Выведите свойства символа Якоби из свойств символа Лежандра.
6. Докажите, что символ Якоби является характером Дирихле (определение характера Дирихле см. в начала параграфа 4.1).
7. Пусть N — нечетное число, большее единицы и свободное от квадратов. Докажите, что ровно половина чисел $a \in \mathbb{Z}$, таких что $1 \leqslant a \leqslant N$ и $(a, N) = 1$, удовлетворяют соотношению $\left(\frac{a}{N}\right) = -1$.
8. Пусть $N = 2^{\alpha_0} p_1^{\alpha_1} \dots p_s^{\alpha_s}$, $a \in \mathbb{Z}$, $(a, N) = 1$. Сколько решений имеет сравнение $x^2 \equiv a \pmod{N}$?
9. Докажите, что число решений сравнения $x^2 - y^2 \equiv a \pmod{p}$ равно $p - 1$ при $p \nmid a$ и $2p - 1$ при $p \mid a$.
10. Пользуясь задачей 9, докажите, что

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{при } p \nmid a, \\ p - 1 & \text{при } p \mid a. \end{cases}$$

11. Пусть p — простое число, $p > 3$. Докажите, что сравнение $x^2 + x + 1 \equiv 0 \pmod{p}$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod{3}$.
12. При помощи алгоритма Шенкса решите сравнения:
    а) $x^2 \equiv 2 \pmod{23}$,
    б) $x^2 \equiv 32 \pmod{41}$,
    в) $x^2 \equiv 108 \pmod{179}$,
    г) $x^2 \equiv 65 \pmod{193}$,
    д) $x^2 \equiv 233 \pmod{353}$,
    е) $x^2 \equiv -10 \pmod{449}$.

Разложение многочленов на множители.

13. При помощи алгоритма Берлекемпа разложите на неприводимые множители многочлен $f(x) \in F_p[x]$, где
    а) $f(x) = x^5 + x^4 + 1$, $p = 2$;
    б) $f(x) = x^8 + x^6 + x^4 + x^3 + 1$, $p = 2$;
    в) $f(x) = x^4 - x^3 - x - 1$, $p = 3$;
    г) $f(x) = x^5 - x + 1$, $p = 3$;
    д) $f(x) = x^5 - x^2 + 1$, $p = 3$;
    е) $f(x) = x^5 - x^3 + 1$, $p = 3$;
    ж) $f(x) = x^4 + 2x^3 - 1$, $p = 5$.
14. Исследуйте, при каких ограничениях на n, k, p, m алгоритм факторизации многочленов, использующий сведение к задаче поиска корней, работает асимптотически быстрее алгоритма Берлекемпа.

15. Пусть $f(x), h(x) \in F_p[x]$ и $h(x)^p - h(x) \equiv 0 \pmod{f(x)}$. Докажите, что при $c \in F_p$ многочлены $f(x)$ и $h(x) - c$ имеют отличный от единицы общий делитель тогда и только тогда, когда c является корнем результанта $R(y)$ многочленов $f(x)$ и $h(x) - y$.

16. Пусть $a \in F_p$, $a \neq 0$, и пусть K — расширение поля F_p, в котором многочлен $f(x) = x^p - x + a$ имеет хотя бы один корень. Докажите, что над полем K многочлен $f(x)$ раскладывается на линейные множители.

17. Пусть $a \in F_p$, $a \neq 0$. Докажите, что многочлен $x^p - x + a$ неприводим над F_p.

18. Пусть F — поле характеристики p и пусть $a \in F$. Докажите, что многочлен $x^p - a$ либо неприводим над F, либо является p-й степенью линейного многочлена из $F[x]$.

19. Докажите, что для любого конечного поля F и любого натурального n существует многочлен степени n, неприводимый над F.

20. Докажите, что над произвольным полем многочлен $x^n - 1$ делит многочлен $x^m - 1$ тогда и только тогда, когда n делит m.

21. Найдите все такие $a \in F_{11}$, что многочлен $x^5 - a$ неприводим над F_{11}.

22. Пусть $f(x), h(x) \in F_p[x]$. Найдите многочлен $g(x) \in F_p[x]$, удовлетворяющий сравнению $h(x)g(x) \equiv 1 \pmod{f(x)}$, если
    а) $f(x) = x^5 + x^4 + x^3 - x + 1$, $h(x) = x^4 - x^2 + x$, $p = 3$;
    б) $f(x) = x^5 - x^4 + x^3 - x - 1$, $h(x) = x^4 - x^2 + x$, $p = 3$;
    в) $f(x) = 3x^5 - 2x^4 + x^3 + 4$, $h(x) = x^4 - 2x^3 + 3x^2 - 4x$, $p = 5$;
    г) $f(x) = x^5 - 2x^4 - 2x^3 - 1$, $h(x) = x^4 - x^3 + 2x^2 + 2x$, $p = 5$.

23. **Еще одна лемма Гаусса.** Многочлен из $\mathbb{Z}[x]$ называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1. Докажите, что произведение примитивных многочленов является примитивным многочленом.

24. Докажите при помощи леммы Гаусса, что если многочлен $f(x)$ с целыми коэффициентами неприводим как элемент $\mathbb{Z}[x]$, то он неприводим и как элемент $\mathbb{Q}[x]$.

25. **Критерий Эйзенштейна.** Докажите, что если $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$ и все a_i делятся на некоторое простое число p, но при этом $p^2 \nmid a_0$, то многочлен $f(x)$ неприводим над $\mathbb{Z}$.

26. Докажите неприводимость над $\mathbb{Q}$ следующих многочленов:
    а) $x^5 - x + 1$,
    б) $x^5 - 5x^4 - 6x - 1$,
    в) $x^5 - x^2 + 1$,

г) $x^4 + x^3 + 1$,
д) $x^4 + 2x^2 + x + 3$.

Круговые поля, многочлены деления круга.

27. Используя критерий Эйзенштейна, докажите, что $\Phi_p(x)$ при простом p неприводим над $\mathbb{Q}$.
28. Докажите, что при $n \geqslant 3$ степень многочлена $\Phi_n(x)$ четна.
29. Докажите, что для нечетных $n \geqslant 3$ справедливо равенство $\Phi_{2n}(x) = \Phi_n(-x)$.
30. Докажите, что для любого простого p справедливо равенство
$$\Phi_{p^{r+1}}(x) = \Phi_p(x^{p^r}).$$
31. Докажите, что для любого простого p, $p \nmid n$, справедливо равенство
$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$
32. Докажите равенство
$$\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)},$$
где $\mu(d)$ — функция Мебиуса.
33. Докажите, что если $n = p_1^{r_1} \dots p_s^{r_s}$ — разложение числа n на простые множители, то
$$\Phi_n(x) = \Phi_{p_1 \dots p_s}\left(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}}\right).$$
34. Докажите, что если $q \in \mathbb{Z}$, $q > 1$, то делимость $\Phi_n(q) \mid (q-1)$ может иметь место только в случае $n = 1$.
35. Разложите многочлен $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$, рассматриваемый как многочлен над $\mathbb{Z}/2\mathbb{Z}$, на неприводимые (над $\mathbb{Z}/2\mathbb{Z}$) множители.
36. Докажите, что при $n \geqslant 3$ поле алгебраических чисел нечетной степени не может содержать примитивный корень n-й степени из единицы.
37. Опишите все подполя поля $\mathbb{Q}(\zeta_n)$.
38. Докажите, что если p — простое число, $p \equiv 3 \pmod 4$, то $\mathbb{Q}(\sqrt{p})$ содержится в круговом поле $\mathbb{Q}(\zeta_{4p})$.
39. Докажите, что любое квадратичное поле содержится в некотором круговом поле.
40. Докажите, что не существует простых чисел, которые оставались бы простыми в круговом поле $\mathbb{Q}(\zeta_n)$.

Суммы Гаусса.

41. Иногда при фиксированном простом q вместо сумм $\tau(\chi)$ рассматривают суммы более общего вида

$$\tau_a(\chi) = \sum_{x=1}^{q-1} \chi(x)\zeta_q^{ax}, \quad a \in \mathbb{Z},$$

которые также называют суммами Гаусса. При $\chi(x) = \left(\frac{x}{q}\right)$ сумму $\tau_a(\chi)$ называют *квадратичной суммой Гаусса* и обозначают τ_a.
Докажите, что $\tau_a = \left(\frac{a}{q}\right)\tau_1$.

42. Пусть p — нечетное простое число. Докажите, что для квадратичных сумм Гаусса поля F_q в кольце целых алгебраических чисел выполняется сравнение $\tau_1^p \equiv \tau_p \pmod{p}$.

43. Докажите, что для квадратичных сумм Гаусса поля F_q верно равенство $\tau_1^2 = (-1)^{(q-1)/2}q$. (*Указание:* вычислите сумму $\sum_{a=0}^{q-1}\tau_a\tau_{-a}$ двумя способами: непосредственно и при помощи задачи 41)

44. Выведите из задач 41, 42, 43 квадратичный закон взаимности.

45. Докажите равенство $|\tau(\chi)| = q^{1/2}$ для сумм Гаусса поля F_q. (*Указание:* вычислите сумму $\sum_{a=0}^{q-1}\tau_a(\chi)\tau_{-a}(\chi^{-1})$ двумя способами)

46. Докажите, что для сумм Якоби поля F_q при $\chi_1 \neq \chi_2^{-1}$ справедливо равенство $|J(\chi_1, \chi_2)| = q^{1/2}$.

47. Пусть χ — неглавный характер по модулю q порядка d. Докажите, что для сумм Гаусса и сумм Якоби поля F_q справедливо равенство

$$\tau(\chi)^d = \chi(-1)q\prod_{j=1}^{d-2} J(\chi, \chi^j).$$

Квадратичные расширения поля $\mathbb{Q}$.

48. Пусть $a, b, c \in \mathbb{Z}$. Докажите, что сравнение $a \equiv b \pmod{c}$ в кольце $\mathbb{Z}$ равносильно сравнению $a \equiv b \pmod{c}$ в кольце целых алгебраических чисел.

49. Пусть d — целое число, отличное от квадрата, и пусть $a, b \in \mathbb{Z}$, $(a, b) = 1$. Докажите, что существует такое целое число t, что в кольце $\mathbb{Z}[\sqrt{d}]$ выполняется сравнение $t \equiv \sqrt{d} \pmod{a + b\sqrt{d}}$.

50. Пусть d — целое число, отличное от квадрата, и пусть $a, b, x, y, t \in \mathbb{Z}$, $(a, b) = 1$, $t \equiv \sqrt{d} \pmod{a+b\sqrt{d}}$. Докажите, что $a+b\sqrt{d}$ делится на $x+y\sqrt{d}$ в кольце $\mathbb{Z}[\sqrt{d}]$ тогда и только тогда, когда $x + yt \equiv 0 \pmod{a^2 - b^2 d}$.

51. Найдите все целые x и y, для которых
а) $x + y\sqrt{2} \equiv 0 \pmod{3 + \sqrt{2}}$ в $\mathbb{Z}[\sqrt{2}]$
б) $x + iy \equiv 0 \pmod{3 + 4i}$ в $\mathbb{Z}[i]$.

52. Докажите, что кольцо $\mathbb{Z}[i]$ евклидово.

53. Сформулируйте и докажите аналог китайской теоремы об остатках для кольца $\mathbb{Z}[i]$.

54. Решите в $\mathbb{Z}[i]$ систему сравнений

$$\begin{cases} (3+2i)x \equiv 7 + 2i \pmod{2 - i} \\ (2-i)x \equiv 5 + 3i \pmod{3 + 2i} \end{cases}$$

55. Докажите, что поля $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$ различны. Выведите отсюда, что степень числа $\sqrt{2} + \sqrt{3}$ равна 4.

56. Пусть $\alpha, \alpha_1, \ldots, \alpha_m \in \mathbb{Q}$. Докажите при помощи индукции по m, что если $\sqrt{\alpha} \in \mathbb{Q}(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$, то существуют такие $\gamma \in \mathbb{Q}$ и $k_1, \ldots, k_m \in \{0, 1\}$, что $\alpha = \gamma_2 \alpha_1^{k_1} \ldots \alpha_m^{k_m}$.

57. Докажите при помощи задачи 56, что для любых попарно различных простых $p_1, \ldots, p_m$ справедливо равенство $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) : \mathbb{Q}] = 2^m$.

58. Докажите, что кольцо целых чисел поля $\mathbb{Q}(\sqrt{d})$ совпадает с кольцом $\mathbb{Z}+\omega\mathbb{Z}$, где

$$\omega = \begin{cases} \sqrt{d} & \text{если} \quad d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{если} \quad d \equiv 1 \pmod 4. \end{cases}$$

59. Докажите, что для поля $K = \mathbb{Q}(\sqrt{d})$ следующие утверждения эквивалентны:
а) кольцо целых чисел $\mathbb{Z}_K$ поля K является кольцом главных идеалов;
б) в кольце $\mathbb{Z}_K$ имеет место единственность разложения на простые сомножители.

60. Докажите, что кольцо $\mathbb{Z}[\sqrt{-3}]$ не является кольцом главных идеалов, в то время как кольцо целых чисел поля $\mathbb{Q}[\sqrt{-3}]$ — является.

61. Докажите, что при $d = -5, -6, -10, -13, -14, -23$ в кольце целых чисел поля $\mathbb{Q}[\sqrt{d}]$ нет единственности разложения на простые сомножители.

62. Разложите числа $2, 3, 5, 7$ в произведение простых идеалов в полях $\mathbb{Q}(\sqrt{d})$ при $d = -1, 2, -3, 5, -7$.

63. Разложите числа $2, 3$ в произведение простых идеалов в поле $\mathbb{Q}(\sqrt{-19})$. Проверьте, что все получившиеся при этом идеалы будут главными.

64. Докажите, что кольцо целых чисел поля $\mathbb{Q}(\sqrt{-19})$ является кольцом главных идеалов.

65. Докажите, что кольцо целых чисел $\mathbb{Z}_K$ поля $K = \mathbb{Q}(\sqrt{-19})$ не является евклидовым.
(*Указание:* в предположении, что для $\mathbb{Z}_K$ существует евклидова норма $\lambda(\cdot)$, рассмотрите число $\alpha \in \mathbb{Z}_K$, отличное от ± 1, с минимальной нормой $\lambda(\alpha)$ и докажите, что в кольце $\mathbb{Z}_K/\alpha\mathbb{Z}_K$ уравнение $x^2 - x + 5 = 0$ не разрешимо)

p-адические числа.

66. Докажите, что любой треугольник в $\mathbb{Q}_p$ является равнобедренным (то есть для любых $a, b, c \in \mathbb{Q}_p$ хотя бы две из величин $|a-b|_p$, $|b-c|_p$, $|a-c|_p$ совпадают)

67. Для всех $a \in \mathbb{Q}_p$ и $r \in \mathbb{R}_{\geqslant 0}$ введем следующие обозначения для шаров и сфер в $\mathbb{Q}_p$:
$$B(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\},$$
$$\overline{B}(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p \leqslant r\},$$
$$S(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p = r\}.$$
Докажите следующие утверждения:
   а) $\mathbb{Z}_p = \overline{B}(0,1) = B(0,p)$, $\quad \mathbb{Z}_p^* = S(0,1) = \bigcup_{k=1}^{p-1}(k + p\mathbb{Z}_p)$;
   б) если $r > 0$ и r не является целой степенью числа p, то $S(a,r) = \varnothing$ и $B(a,r) = \overline{B}(a,r)$ для любого $a \in \mathbb{Q}_p$.
   в) для любых $a \in \mathbb{Q}_p$ и $r > 0$ множества $B(a,r), \overline{B}(a,r), S(a,r)$ открыты и замкнуты в $\mathbb{Q}_p$;
   г) если B — произвольный шар в $\mathbb{Q}_p$, то любая точка $a \in B$ является его центром;
   д) если B — произвольный шар в $\mathbb{Q}_p$ положительного радиуса, то у B нет границы (то есть нет точек, в любой открытой окрестности которых есть точки как принадлежащие B, так и не принадлежащие);
   е) если B_1 и B_2 — произвольные шары в $\mathbb{Q}_p$, то либо $B_1 \cap B_2 = \varnothing$, либо один из этих шаров содержится в другом;
   ж) в $\mathbb{Q}_p$ счетное число шаров.

68. Найдите канонические p-адические разложения чисел
   а) -3, $1/2$, $3/10$, $-5/6$, $2/9$ при $p = 5$,
   б) -2, $1/3$, $-3/7$, $7/6$, $3/5$ при $p = 7$.

69. Докажите, что каноническое p-адическое разложение числа $a \in \mathbb{Q}_p$ периодично, начиная с какого-то места, тогда и только тогда, когда a является рациональным числом (то есть в соответствующем классе эквивалентности последовательностей Коши есть последовательность, в которой все члены равны).

70. Докажите, что каноническое p-адическое разложение числа $a \in \mathbb{Q}_p$ конечно (то есть все цифры, начиная с какого-то момента, равны нулю) тогда и только тогда, когда a является положительным рациональным числом, знаменатель которого равен степени числа p.

71. Найдите рациональное число, имеющее следующее каноническое p-адическое разложение:
а) $(1, \overline{1})$ при $p = 2$,
б) $(3, \overline{0, 1, 2, 4, 3, 2})$ при $p = 5$,
в) $(2, \overline{4, 5, 2, 1})$ при $p = 7$.

72. Найдите рациональное число, имеющее следующее *не*каноническое p-адическое разложение:
а) $\sum_{k=0}^{\infty} -2^k$ при $p = 2$,
б) $\sum_{k=0}^{\infty} (-3)^k$ при $p = 3$.

73. Докажите, что если $p \neq 2$, то число $a = (a_0, a_1, a_2, \ldots) \in \mathbb{Z}_p^*$ является квадратом в $\mathbb{Z}_p$ тогда и только тогда, когда a_0 является квадратичным вычетом по модулю p.

74. Приведите пример ряда в $\mathbb{Q}_p$, который сходится, но не сходится абсолютно.

75. Докажите, что ряд
$$E_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$
сходится в шаре $B(0, p^{-1/(p-1)})$.

76. Пусть $B = B(0, p^{-1/(p-1)})$. Докажите, что отображения
$$E_p : B \to 1 + B \quad \text{и} \quad L_p : 1 + B \to B$$
взаимно обратны и задают изоморфизм аддитивной группы B и мультипликативной группы $1 + B$.

77. Докажите, что изоморфизм из задачи 76 является изометрией.

Литература

[1] Ахо А., Хонкрофт Дж., Ульман Дж., Построение и анализ вычислительных алгоритмов, Москва, Мир, 1979.

[2] Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В., Математические и компьютерные основы криптологии, Минск, Новое знание, 2003.

[3] ван дер Варден, Б.Л., Современная алгебра, М., Наука, 1976.

[4] Василенко О.Н., Теоретико-числовые алгоритмы в криптографии, Москва, МЦНМО, 2003.

[5] Виноградов И.М., Основы теории чисел, М., Наука, 1972.

[6] Дж.В.С. Касселс. Введение в геометрию чисел. Москва, Мир, 1965.

[7] Кнут Д., Искусство программирования для ЭВМ, Т.2, Получисленные алгоритмы, М., Мир, 1977.

[8] Монтгомери Г., Мультипликативная теория чисел, Перев. с англ.-М.: Мир, 1974.

[9] Нечаев В.И., Элементы криптографии, М., Высшая школа, 1999.

[10] Ноден П., Китте К., Алгебраическая алгоритмика, М., Мир, 1999.

[11] Прахар К., Распределение простых чисел, Москва, Мир, 1967.

[12] С.С Рышков. О приведении положительных квадратичных форм от n переменных по Эрмиту, по Минковскому и по Венкову. ДАН СССР, т.207, №5, с.1054–1056, 1972.

[13] Черемушкин А.В., Лекции по арифметическим алгоритмам в криптографии, М., МЦНМО, 2002.

[14] L.M. Adleman, K.S. McCurley. Open problems in number theoretic complexity, II. Proceedings of ANTS–1, Lecture Notes in Computer Science, vol.877, pp. 291–322, Springer–Verlag, NY, 1994.

[15] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers, Ann. Math., 1994, v.140, p.703-722.

[16] E.R. Berlekamp, Factoring polynomials over finite fields, Bell System Tech. J., 1967, v.46, p. 1853-1859.

[17] D.G. Cantor, H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, Math. Comput., 1981, v.36, p. 587-592.

[18] R.D. Carmichael, On composite numbers p which satisfy the Fermat congruence $a^{p-1} \equiv 1 \pmod{p}$, Amer. Math. Monthly, 1912, v. 19, p. 22-27.

[19] H. Cohen. A Course in Computational Algebraic Number Theory, volume 138 of Graduate Texts in Mathematics. Springer–Verlag, 2000.

[20] R. Crandall, C. Pomerance. Prime Numbers: a computational perspective. Springer, NY, 2005.

[21] W. Diffie, M. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, vol.22, pp.644–654, 1976.

[22] M. Fürer. Faster integer multiplication. Proceedings of the 39th ACM STOC 2007, pp. 57–66.

[23] P.M. Gruber, C.G. Lekkerkerker. Geometry of Numbers. Amsterdam, 1987.

[24] J.C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. SIAM Journal of Computing, vol.14, pp.196–209, 1985.

[25] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovasz. Factoring polynomials with rational coefficients. Math. Ann., vol.261, pp.515–534, 1982.

[26] H.W. Lenstra, Jr. Integer programming with a fixed number of variables. Mathematics of operations research, vol.8, No.4., pp.538–548, 1983.

[27] M. Rabin, Probabilistic algorithms for testing primality, J. Number Theory, 1980, v.12, p. 128-138.

[28] R. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM, vol.21, pp.120–126, 1978.

[29] A. Schönhage, V. Strassen. Schnelle Multiplikation grosser Zahlen. Computing (Arch. Elektron. Rechnen), vol.7, pp.281–292, 1971.

[30] R. Solovay, V. Strassen, A fast Monte-Carlo test for primality, SIAM J. Comput., 1977, v.6, p. 84-85, Errata in: 1978, v.7, p. 117.

[31] M. Wiener. Cryptanalysis of short RSA secret exponents. IEEE Trans. Inform. Theory, vol.36, pp.553–558, 1990.