# ТЕОРИЯ ЧИСЕЛ

Ю.В. Нестеренко

# Оглавление

# Введение

Теория чисел имеет своим предметом числа и их свойства, т.е. числа выступают здесь не как средство или инструмент, а как объект исследования. Натуральный ряд

$$1, 2, 3, 4, \ldots, 9, 10, 11, \ldots, 99, 100, 101, \ldots$$

- множество натуральных чисел, является важнейшей областью исследований, необычайно содержательной, важной и интересной.

Начала исследований натуральных чисел были заложены в Древней Греции. Здесь были изучены свойства делимости чисел, доказана бесконечность множества простых чисел и открыты способы их построения (Евклид, Эратосфен). Задачи,связанные с решением неопределенных уравнений в целых числах, были предметом исследований Диофанта, их изучением занимались ученые Древней Индии и Древнего Китая, стран Средней Азии.

В XVII веке П. Ферма и в XVIII Л. Эйлер внесли огромный вклад в наши знания о натуральных числах. И если Ферма оставил лишь свои открытия, не сопроводив их доказательствами, то Эйлер, оказавший большое влияние на развитие всей математики, а также и механики, создал новые методы и приемы, реализовал новые идеи, которые играют важную роль и в современных исследованиях и приложениях теории чисел. В частности, Эйлер был первым, кто предложил использовать средства математического анализа при исследовании проблем теории чисел.

Основные исследования в теории чисел можно условно сгруппировать по нескольким направлениям. Впрочем, обширность содер-

жания не позволяет охватить при этом все многообразие результатов и методов теории чисел, значительную часть их пришлось опустить.

*Исследования свойств простых чисел.* Среди натуральных чисел выделяются так называемые простые числа, т.е. числа, которые невозможно представить в виде произведения меньших натуральных сомножителей. Множество их бесконечно. Асимптотический закон распределения простых чисел утверждает, что их количество в пределах от 1 до заданного числа $x$ асимптотически равно $\frac{x}{\ln x}$. Эта теорема была независимо доказана в 1896г. Ж. Адамаром и Ш.Ж. де ла Валле-Пуссеном. Вопросы распределения простых чисел в различных числовых последовательностях, например, среди значений фиксированного многочлена $f(n)$ составляют одну из проблем этого раздела теории чисел. Для многочленов первой степени она была решена в середине XIX века Г.П. Лежен Дирихле, однако и в настоящее время не доказана бесконечность множества простых чисел в последовательности $n^2 + 1, n \geq 1$. Исследование расстояний между соседними простыми числами в натуральном ряду составляет другой круг проблем этого направления. Среди нерешенных задач отметим, например, утверждение о бесконечности множества пар простых чисел $p, q$ с условием $p - q = 2$, так называемую "проблему близнецов". Эти вопросы, несмотря на их кажущуюся сугубо теоретическую направленность, представляют большой практический интерес. С изучением свойств простых чисел тесно связаны исследования дзета-функции Римана.

*Аддитивные задачи.* Здесь рассматриваются вопросы представимости целых чисел в виде сумм слагаемых определенного вида. Например, в 1770г. Ж. Лагранж установил, что каждое натуральное число представимо в виде суммы четырех квадратов целых чисел. Впоследствии (1909г.) Д.Гильберт обобщил это утверждение, заменив суммы квадратов суммами произвольных фиксированных степеней, решив тем самым знаменитую проблему Варинга. В 1937г. И.М. Виноградов доказал, что каждое достаточно большое целое число представимо в виде суммы трех простых чисел, но так на-

зываемая бинарная проблема Гольдбаха о представимости всякого четного числа $n \geq 2$ в виде суммы двух нечетных простых чисел все еще остается открытой.

*Диофантовы уравнения.* Вопросы разрешимости уравнений в целых числах относятся к древнейшим в теории чисел. В связи с исследованиями в этой области уже упоминались имена Диофанта, Ферма и Эйлера. Теория сравнений, являющаяся важным инструментом исследования диофантовых уравнений была систематически разработана К.Ф.Гауссом, отметим, в частности, его квадратичный закон взаимности. Теория алгебраических чисел, толчком к созданию которой послужили в первую очередь исследования уравнения Ферма $x^n + y^n = z^n, n \geq 3$, и в настоящее время приносит плоды в этой области. Отметим, полученное в 2000г. П. Михайлеску решение проблемы Каталана о существовании у уравнения $x^y - z^t = 1$ единственного решения в целых числах $x > 2, y > 2, z > 2, t > 2$, а именно $3^2 - 2^3 = 1$.

*Диофантовы приближения* – раздел теории чисел о решении неравенств в целых числах, включает в себя теорию цепных дробей и другие алгоритмы построения приближений действительных чисел рациональными, а также ряд вопросов геометрии чисел. Среди наиболее ярких достижений отметим теорему К.Ф. Рота (1954г.) о том, что алгебраические числа не могут слишком хорошо приближаться рациональными. Среди нерешенных вопросов отметим знаменитую проблему Литтлвуда о том, что для любых действительных чисел $\alpha, \beta$ и любого положительного $\varepsilon$ неравенство $|x|\cdot|x\alpha - y_1|\cdot|x\beta - y_2| < \varepsilon$ разрешимо в целых числах $x > 0, y_1, y_2$.

*Трансцендентные числа* – раздел теории чисел, в котором исследуются вопросы иррациональности и трансцендентности действительных чисел. Как правило, это классические постоянные или значения аналитических функций. Неалгебраичность, т.е. трансценденость числа $e$ была доказана в 1873г. Ш. Эрмитом, а трансцендентность числа $\pi$ в 1882г. Ф.Линдеманом. Предполагается, что любое число вида $P(e, \pi)$, где $P(x, y)$ - многочлен с целыми коэффициента-

ми, трансцендентно, однако к настоящему времени не доказана даже иррациональность числа $e + \pi$. Нижние оценки линейных форм от логарифмов алгебраических чисел, доказанные средствами теории трансцендентных чисел (А. Бейкер, 1967г.), играют важную роль при нахождении решений многих диофантовых уравнений.

Теория чисел – один из древнейших математических разделов. Арифметические исследования послужили базой для создания ряда разделов математики и в то же время теория чисел использует аналитические, алгебраические, геометрические и многие другие методы для решения теоретико числовых проблем, ряд из которых ждал и ждет своего решения столетиями. Для доказательства все еще открытой гипотезы Римана о нулях дзета-функции использовались методы, развитые в теории дифференциальных уравнений, теории функций комплексного переменного, функциональном анализе. А доказательство асимптотического закона о распределении простых чисел впервые было получено методами комплексного анализа. Попытки решения проблемы Ферма, проблем распределения простых чисел стимулировали развитие ряда разделов алгебры.

Теория чисел безусловно относится к фундаментальным разделам математики. Вместе с тем ряд ее задач имеет самое непосредственное отношение к практической деятельности. Так, например, благодаря в первую очередь запросам криптографии и широкому распространению ЭВМ, исследования алгоритмических вопросов теории чисел переживают в настоящее время период бурного и весьма плодотворного развития. Криптографические потребности стимулировали исследования классических задач теории чисел, в ряде случаев привели к их решению, а также стали источником постановки новых фундаментальных проблем.

Традиции исследования проблем теории чисел в России идут, вероятно, от Эйлера (1707-1783), который прожил здесь в общей сложности 30 лет и многое сделал для развития науки. Под влиянием его трудов сложилось творчество П.Л. Чебышева (1821-1894), выдающегося ученого и талантливого педагога, издавшего вместе с

В.Я. Буняковским (1804-1889) арифметические сочинения Эйлера. П.Л. Чебышев создал Петербургскую школу теории чисел, представителями которой являлись А.Н. Коркин (1837-1908), Е.И. Золотарев (1847-1878) и А.А. Марков (1856-1922). Г.Ф. Вороной (1868-1908), учившийся в Петербурге у А.А.Маркова и Ю.В.Сохоцкого (1842-1927), основал школу теории чисел в Варшаве. Из нее вышел ряд замечательных специалистов по теории чисел и, в частности, В.Серпинский (1842-1927). Другой воспитанник Петербургского Университета Д.А.Граве (1863-1939) многое сделал для преподавания теории чисел и алгебры в Киевском Университете. Его учениками были О.Ю.Шмидт (1891-1956), Н.Г.Чеботарев (1894-1947), Б.Н.Делоне (1890-1980). Теоретико числовые исследования проводились также в Университетах Москвы, Казани, Одессы. В советский период в теории чисел работали такие выдающиеся ученые, как И.М.Виноградов (1891-1983) (аналитическая теория чисел), А.О.Гельфонд (1906-1968) (трансцендентные числа) , Ю.В.Линник (1915-1972) (аналитическая теория чисел), А.Я.Хинчин (1896-1959) (диофантовы приближения), И.Р.Шафаревич (р. 1923) (алгебраическая теория чисел).

Эта книга представляет собой учебник по элементарной теории чисел. Как видно из оглавления, она в основном включает традиционные темы. Вместе с тем мы доказываем оценки Чебышева для количества простых чисел, разложение числа $e$ в непрерывную дробь, трансцендентность чисел $e$, $\pi$ и невозможность квадратуры круга с помощью циркуля и линейки. Большое внимание уделяется также алгоритмическим вопросам теории чисел.

# Глава 1

# О делимости чисел

Натуральные числа образуют последовательность, ряд чисел, *натуральный ряд*. Под этим подразумевается, что у каждого натурального числа $a$ есть непосредственно следующее за ним, отличное от 1, натуральное число $a+1$. Числа, непосредственно следующие за различными натуральными числами, не могут совпадать. Кроме того, выполняется так называемая

**Аксиома индукции.** *Если некоторое подмножество натурального ряда содержит* 1 *и вместе с каждым натуральным числом содержит непосредственно следующее за ним, то оно содержит все натуральные числа.*

Из этих простейших свойств можно вывести, что

1. *Каждое непустое подмножество натурального ряда содержит наименьший элемент.*

2. *Каждое непустое конечное подмножество натурального ряда содержит наибольший элемент.*

3. *Если известно, что некоторое утверждение о натуральных числах выполняется для числа* $a$*, а также из предположения, что утверждение верно при некотором* $n$ *следует справедливость этого утверждения для числа* $n+1$*, то это утверждение верно для всех натуральных чисел больших или равных* $a$*.*

Про доказательства, основанные на последнем свойстве, говорят, что они выполняются методом математической индукции.

Натуральный ряд бесконечен. Его обозначают буквой $\mathbb{N}$.

В натуральном ряду установлен порядок: из двух разных натуральных чисел меньшим будет то, которое в натуральном ряду стоит раньше. В множестве натуральных чисел определены операции сложения и умножения. Операция вычитания определена не всегда. Вычитать можно лишь меньшее натуральное число из большего.

Натуральные числа составляют множество положительных целых чисел. Если к ним добавить отрицательные числа и ноль, получится множество целых чисел

$$0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots .$$

Это множество принято обозначать буквой $\mathbb{Z}$. С его элементами можно выполнять арифметические операции: сложение и вычитание, умножение и деление. Если первые три операции применимы к любым двум целым числам, то операция деления выполнима не всегда.

## 1.1 Свойства делимости целых чисел

В дальнейшем целые числа будут обозначаться латинскими буквами $a, b, c$ и т.д. Определим важное понятие делимости чисел.

**Определение 1.** *Говорят, что целое число $a$ делится на целое число $b \neq 0$, если найдется целое число $c$, удовлетворяющее равенству*

$$a = b \cdot c.$$

Например, число 111 делится на 37, а 28 делится на $-4$, ведь $111 = 37 \cdot 3$ и $28 = (-4) \cdot (-7)$. Число 5 не делится на 3. Действительно, неравенства $3 \cdot 1 < 5 < 3 \cdot 2$, означают, что целое $c$, для которого $3 \cdot c = 5$, должно удовлетворять неравенствам $1 < c < 2$. Ясно, что такого числа в множестве $\mathbb{Z}$ не существует.

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 $b \nmid a$.

Ноль делится на любое целое число $a \neq 0$. Отметим также следующие свойства делимости.

**Лемма 1.1.** *Пусть $a, b, c$ - целые числа.*

1. *Имеем $1|a$.*
2. *Если $a \neq 0$, то $a|a$.*
3. *Если $a|b$, то $a|bc$.*
4. *Если $a|b$ и $b|c$, то $a|c$.*
5. *Если $a|b$ и $a|c$, то $a|(b+c)$ и $a|(b-c)$.*
6. *Если $a|b$ и $b \neq 0$, то $|a| \leq |b|$.*

*Доказательство.* Справедливы равенства $a = 1 \cdot a = a \cdot 1$, доказывающие первое и второе свойства.

Делимость $a|b$ означает, что с некоторым $u \in \mathbb{Z}$ имеем $b = au$. Но тогда $bc = a(uc)$ и, значит, $a|bc$. Это доказывает третье свойство.

Для доказательства четвертого заметим, что, согласно условию, с некоторыми целыми $u, v$ выполняются равенства $b = au, c = bv$. Отсюда следует, что $c = auv$ и, значит, $a|c$.

В пятом случае, поскольку $a|b$ и $a|c$ имеем $b = au, c = av$ с некоторыми $u, v \in \mathbb{Z}$. Но тогда $b + c = a(u + v)$ и $b - c = a(u - v)$, что завершает доказательство пятого свойства.

Из равенства $b = au$, где $u \in \mathbb{Z}$, и условия $b \neq 0$ следует, что $u \neq 0$ и, значит, $|u| \geq 1$. Но тогда $|b| = |a| \cdot |u| \geq |a|$. □

Как уже отмечалось, не любые два числа связаны отношением делимости. В общем случае используется так называемое деление с остатком.

**Теорема 1.1.** *Для любых целого числа $a$ и натурального $b$ существуют единственным образом определенные целые числа $q, r$, удо-*

*влетворяющие условиям*

$$a = bq + r, \qquad 0 \le r < b. \tag{1.1}$$

*Доказательство.* Докажем существование чисел $q, r$.

Если $b|a$, т.е. $b = au$ с некоторым целым $u$, положим $q = u, r = 0$. При таком выборе условия (1.1), очевидно, будут выполнены.

Далее будем предполагать, что число $a$ не делится на $b$. Множество $M$ натуральных чисел, представимых в виде $a - bk$ с некоторым целым $k$, непусто. Действительно, при $k = -|a| - 1$ имеем

$$a - kb = a + (|a| + 1)b \ge b + |a|(b - 1) \ge 1.$$

Обозначим буквой $r$ – наименьшее из чисел множества $M$. Тогда $r \ge 1$, и с некоторым целым $q$ выполняется равенство $r = a - bq$. Поскольку $a - b(q + 1) = r - b < r$, то $a - b(q + 1) \notin M$, и, значит, выполнено $a - b(q+1) = r - b \le 0$. Учитывая, что равенство $a - b(q + 1) = 0$ невозможно, ведь $b \nmid a$, заключаем $r - b < 0$. Итак, $1 \le r < b$. Существование нужных чисел $q, r$ доказано и в этом случае.

Допустим теперь, что вместе с парой чисел $(q, r)$, удовлетворяющих условиям (1.1), существует еще одна, отличная от неё пара чисел $(u, v)$, для которой

$$a = bu + v, \qquad 0 \le v < b. \tag{1.2}$$

Из равенств (1.1) и (1.2) следует $bq + r = bu + v$. Поэтому $r - v = b(u - q)$, так что $b|(r - v)$. Из неравенств (1.1) и (1.2) находим также $|r - v| < b$. Согласно последнему свойству леммы 1.1 можно утверждать теперь, что $r - v = 0$, т.е. $v = r$. Но тогда $b(u - q) = 0$ и, значит, $u = q$. Получаем, что пары $(q, r)$ и $(u, v)$ должны совпадать, вопреки нашему предположению. Это противоречие завершает доказательство теоремы 1.1. □

Числа $r$ и $q$, определенные в теореме 1.1, называются *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.

Например, справедливо равенство

$$-1234 = 23 \cdot (-54) + 8.$$

Можно сказать, что остаток от деления числа $-1234$ на 23 равен 8, а неполное частное равно $-54$.

Из доказательства теоремы 1.1 следует, что целое число $a$ делится на натуральное $b$ в том и только том случае, когда соответствующий остаток равен нулю.

Числа, делящиеся на 2, называются *четными*, числа, не делящиеся на 2, т.е. имеющие при делении на 2 остаток 1, называются *нечетными*.

Для реального нахождения остатка и неполного частного можно использовать так называемый алгоритм *деления столбиком*. Известны и другие более эффективные алгоритмы.[1]

## 1.2 Наименьшее общее кратное и наибольший общий делитель

Пусть $a_1, \ldots, a_n$ – ненулевые целые числа. Целое число $K$ называется *общим кратным* чисел $a_1, \ldots, a_n$, если оно кратно каждому из этих чисел, т.е. $a_1|K, \ldots, a_n|K$. Например, $|a_1 \cdots a_n|$ есть одно из их общих кратных.

**Определение 2.** *Наименьшее из положительных общих кратных называется наименьшим общим кратным чисел* $a_1, \ldots, a_n$.

Множество общих кратных чисел $a_1, \ldots, a_n$ будет обозначаться символом $\mathcal{M}\{a_1, \ldots, a_n\}$, а их наименьшее общее кратное – символом $\mathbf{НОК}(a_1, \ldots, a_n)$ или $[a_1, \ldots, a_n]$.

**Теорема 1.2.** *1. Любое общее кратное нескольких чисел делится на их наименьшее общее кратное.*

[1] См., например, книгу Ахо А., Хопкрофт Дж., Ульман Дж., Построение и анализ вычислительных алгоритмов, Москва, Мир, 1979.

*2. Для любых отличных от нуля целых чисел $a_1, \ldots, a_n$ выполняется равенство*

$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$

*Доказательство.* Пусть $m = [a_1, \ldots, a_n]$ и $K$ - какое-нибудь общее кратное чисел $a_1, \ldots, a_n$. Разделив с остатком число $K$ на $m$, получим целые $q, r$, удовлетворяющие условиям

$$K = mq + r, \qquad 0 \leq r < m.$$

Из свойств делимости находим, что $r = K - mq$ делится на каждое из целых чисел $a_j$ и потому есть общее кратное чисел $a_1, \ldots, a_n$. Учитывая, что $m$ есть наименьшее из положительных общих кратных, приходим к заключению, что неравенство $r > 0$ невозможно. Поэтому $r = 0$ и $m|K$. Первое утверждение теоремы доказано.

Для сокращения записи в оставшейся части доказательства, мы будем использовать обозначения

$$u = [a_1, \ldots, a_n], \qquad v = [a_1, \ldots, a_{n-1}].$$

Каждое общее кратное чисел $v$ и $a_n$ делится, очевидно, на числа $a_1, \ldots, a_n$, т.е. является их общим кратным. Поэтому

$$\mathcal{M}\{v, a_n\} \subset \mathcal{M}\{a_1, \ldots, a_n\}.$$

С другой стороны, каждое общее кратное чисел $a_1, \ldots, a_n$ делится на числа $a_1, \ldots, a_{n-1}$ и, согласно первому утверждению теоремы, делится на $v$. Вместе с тем оно делится на $a_n$ и потому является общим кратным чисел $v$ и $a_n$. Это доказывает обратное включение

$$\mathcal{M}\{v, a_n\} \supset \mathcal{M}\{a_1, \ldots, a_n\}.$$

Из совпадения множеств следует равенство их наименьших положительных элементов $[v, a_n] = u$. Теорема доказана. □

Множество всех делителей целого отличного от нуля числа $a$ конечно. Действительно, если $d|a$, то, согласно последнему свойству из леммы 1.1, выполняется неравенство $|d| \leq |a|$.

Пусть $a_1, a_2, \ldots, a_n$ – целые числа и $d \in \mathbb{Z}$ – их *общий делитель*, т.е. $d|a_1, d|a_2, \ldots, d|a_n$. Из сказанного выше следует, что если среди чисел $a_1, a_2, \ldots, a_n$ есть не равное нулю, то множество общих делителей этих чисел конечно. Оно всегда содержит $\pm 1$ 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 3.** *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.

Найдем, например, все общие делители чисел $6, 10, 15$. Они содержатся среди делителей 6, т.е. среди чисел $\pm 1, \pm 2, \pm 3, \pm 6$. Учитывая, что $15 = 2 \cdot 7 + 1$ не делится на 2, а, значит, не делится и на 6, из списка возможных делителей следует исключить $\pm 2, \pm 6$. Равенство $10 = 3 \cdot 3 + 1$ означает, что 10 не делится на 3. Поэтому в списке общих делителей остаются лишь числа $\pm 1$, и потому $(6, 10, 15) = 1$. Числа $6, 10, 15$ взаимно просты.

Множество всех общих делителей чисел $a_1, a_2, \ldots, a_n$ будет обозначаться символом $\mathcal{D}\{a_1, \ldots, a_n\}$. Наибольший общий делитель чисел $a_1, a_2, \ldots, a_n$ обозначается символом $\mathbf{НОД}(a_1, \ldots, a_n)$ или просто $(a_1, \ldots, a_n)$.

Выведем из теоремы 1.2 соотношение между наибольшим общим делителем двух чисел и их наименьшим общим кратным.

**Следствие 1.1.** *Для любых двух натуральных чисел $a, b$ справедливо равенство*

$$[a, b] \cdot (a, b) = a \cdot b.$$

*Доказательство.* Произведение $ab$ есть общее кратное чисел $a$ и $b$. Согласно теореме 1.2 оно делится на их наименьшее общее кратное, т.е. $\frac{ab}{[a,b]}$ есть целое число. Из равенств

$$a = \frac{ab}{[a,b]} \cdot \frac{[a,b]}{b}, \qquad b = \frac{ab}{[a,b]} \cdot \frac{[a,b]}{a}$$

следует, что $\frac{ab}{[a,b]}$ есть общий делитель чисел $a$ и $b$.

Пусть теперь $d$ – произвольный общий делитель $a$ и $b$. В силу равенств

$$\frac{ab}{d} = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}$$

заключаем, что $\frac{ab}{d}$ есть общее кратное чисел $a$ и $b$. По теореме 1.2 оно делится на $[a,b]$, т.е. отношение $\frac{ab}{d \cdot [a,b]}$ есть целое число. Поэтому $\frac{ab}{d \cdot [a,b]} \geq 1$ и $\frac{ab}{[a,b]} \geq d$. Следовательно, $\frac{ab}{[a,b]}$ – наибольший из всех общих делителей чисел $a$ и $b$. Это завершает доказательство следствия. □

**Следствие 1.2.** *Если $a|bc$ и $(a,b) = 1$, то $c$ делится на $a$.*

*Доказательство.* Произведение $bc$ есть общее кратное чисел $b$ и $a$. По теореме 1.2 оно делится на $[a,b]$. Согласно условию и следствию 1.1 заключаем, что $[a,b] = ab$, так что $ab|bc$ и, значит, $a|c$. □

**Теорема 1.3.** *1. Наибольший общий делитель нескольких чисел делится на любой их общий делитель.*

*2. Справедливо равенство*

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

*Доказательство.* Пусть $a_1, \ldots, a_n$ некоторый набор целых чисел и $d_1, \ldots, d_m$ все их положительные общие делители. Буквой $d$ обозначим наименьшее общее кратное этих делителей, т.е. $d = [d_1, \ldots, d_m]$. Каждое из чисел $a_1, \ldots, a_n$ есть общее кратное всех делителей $d_1, \ldots, d_m$. Согласно теореме 1.2 можно утверждать, что $d|a_1, \ldots, d|a_n$. Следовательно, $d$ есть один из общих делителей чисел $a_1, \ldots, a_n$. При любом $k$ имеем $d_k|d$, поэтому выполнено неравенство $d_k \leq d$. Итак,

$d$ – наибольший общий делитель данных чисел, он делится на любой другой их общий делитель.

Обозначим для краткости

$$c = (a_1, \ldots, a_{n-1}), \qquad d = (a_1, \ldots, a_n).$$

Так как каждое из чисел $a_1, \ldots, a_{n-1}$ делится на $c$, то по свойствам делимости каждое из этих чисел делится на $(c, a_n)$. Число $a_n$ также делится на $(c, a_n)$. Следовательно, $(c, a_n)$ есть общий делитель всех данных чисел и потому $(c, a_n) \leq d$.

Докажем, что имеет место противоположное неравенство. Так как $d$ есть общий делитель чисел $a_1, \ldots, a_{n-1}$, то по первому утверждению теоремы $d|c$. Вместе с тем $d|a_n$. Следовательно, $d$ есть общий делитель чисел $c$ и $a_n$. Но тогда $d \leq (c, a_n)$. Доказанные неравенства означают, что $(c, a_n) = d$. □

Применяя несколько раз равенства из теорем 1.2 и 1.3 можно свести вычисление наименьшего общего кратного и наибольшего общего делителя нескольких чисел к такой же задаче для двух чисел. В свою очередь следствие 1.1 позволяет свести вычисление наименьшего общего кратного двух чисел к вычислению их наибольшего общего делителя. Эта задача будет рассмотрена в следующем параграфе.

## 1.3 Алгоритм Евклида

Пусть $a \geq b$ - 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. Придуманный в Древней Греции алгоритм, называемый алгоритмом Евклида, достаточно быстро находит наибольший общий делитель и при этом не разлагает числа на множители. В основе его лежит следующее утверждение.

**Лемма 1.2.** *1. Если $a$ – целое, $b$ - натуральное и $b|a$, то множество общих делителей чисел $a$ и $b$ совпадает с множеством делителей $b$. В частности, $(a, b) = b$.*

*2. Если*

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

*то $\mathcal{D}\{a, b\} = \mathcal{D}\{b, r\}$, в частности, $(a, b) = (b, r)$.*

*Доказательство.* Множество общих делителей чисел $a$ и $b$ содержится среди делителей $b$, т.е. $\mathcal{D}\{a, b\} \subset \mathcal{D}\{b\}$. В то же время, каждый делитель числа $b$, в силу условия $b|a$ будет делителем числа $a$, т.е. принадлежит $\mathcal{D}\{a, b\}$. Следовательно, множество общих делителей чисел $a$ и $b$ совпадает с множеством делителей $b$. Это доказывает первое утверждение леммы 1.2.

Для доказательства второго утверждения заметим, что по свойствам делимости каждый общий делитель чисел $b$ и $r$ делит число $bq + r = a$ и, значит, принадлежит множеству $\mathcal{D}\{a, b\}$. Точно так же, каждый общий делитель чисел $a$ и $b$ делит число $a - bq = r$, так что принадлежит множеству $\mathcal{D}\{b, r\}$. Этим доказано равенство $\mathcal{D}\{a, b\} = \mathcal{D}\{b, r\}$. Отсюда следует и совпадение наибольших общих делителей пар чисел $a, b$ и $b, r$. □

Доказанное в лемме 1.2 равенство $(a, b) = (b, r)$ 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, в какой-то момент одно из чисел станет равным 0 и наибольший общий делитель сможет быть найден с помощью первого утверждения леммы 1.2.

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

да. Тогда $r_1 = b$. Таким образом, получаются следующие равенства

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

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

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

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 $(3009, 894) = 3$.

Для реализации алгоритма Евклида на компьютере больше подходит следующая его форма, в которой отсутствуют индексы у делителей и остатков.

**Алгоритм.** 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* $a = bq + r,\ 0 \le r < b$.

*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.*

Примеры показывают, что алгоритм Евклида достаточно быстро находит наибольший общий делитель. Оценку количества делений в нем дает следующая теорема[2].

**Теорема 1.4.** *Количество делений, необходимое для вычисления с помощью алгоритма Евклида наибольшего общего делителя двух положительных целых чисел, не превышает пятикратного количества цифр в десятичной записи меньшего из этих двух чисел.*

*Доказательство.* Пусть $a \geq b$ - натуральные числа и $b$ записывается $m$ цифрами в десятичной системе счисления. Это значит, что $10^{m-1} \leq b < 10^m$. Требуется доказать, что алгоритм Евклида, применённый к числам $a, b$ выполнит не более $5m$ делений с остатком.

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

$$r_{i-1} = q_i r_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i, \quad i = 1, 2, \ldots, n-1, \quad r_n = (a, b).$$

Докажем справедливость неравенств

$$r_{n-i} \geq \lambda^i, \qquad i = 0, 1, \ldots, n-1, \tag{1.4}$$

где $\lambda = \frac{1+\sqrt{5}}{2} = 1,61...$ есть корень квадратного уравнения $\lambda^2 - \lambda - 1 = 0$. Для этого воспользуемся методом математической индукции. При $i = 0$ имеем $r_n \geq 1 = \lambda^0$. При $i = 1$ находим $r_{n-1} \geq r_n + 1 \geq 2 > \lambda$, так что неравенство (1.4) опять справедливо. Предположим теперь, что $1 \leq k < n - 1$ и неравенство (1.4) выполняется при всех $i \leq k$. Имеем следующую цепочку равенств и неравенств

$$r_{n-k-1} = q_{n-k} r_{n-k} + r_{n-k+1} \geq r_{n-k} + r_{n-k+1} \geq \lambda^k + \lambda^{k-1} = \lambda^{k+1}.$$

[2] Это утверждение доказано в 1845г. французским математиком Г. Ламе.

Таким образом, неравенство (1.4) выполняется и при $i = k + 1$. Это доказывает справедливость (1.4) при всех $i = 0, 1, \ldots, n - 1$.

Поскольку $10^m > b$ и $b = r_1 \geq \lambda^{n-1}$, мы видим, что

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

В последнем неравенстве была использована оценка $\lambda > 10^{1/5} = 1,58...$. Таким образом, $n < 5m + 1$, что завершает доказательство теоремы. □

Рассмотрим последовательность целых чисел $u_n, n \geq 0$, определенную рекуррентно

$$u_0 = 0,\ u_1 = 1, \qquad u_n = u_{n-1} + u_{n-2}, \quad n \geq 2.$$

Согласно этому определению $u_2 = u_1 + u_0 = 1, u_3 = u_2 + u_1 = 2$ и так далее. В результате получается ряд чисел: $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$, носящий название последовательности Фибоначчи[3]. Из закона образования этой последовательности видно, что при $n \geq 3$ остаток от деления числа $u_{n+1}$ на $u_n$ всегда равен $u_{n-1}$, неполное частное при этом равно 1. Таким образом, для нахождения наибольшего общего делителя $(u_n, u_{n+1})$ потребуется $n - 1$ деление с остатком. Например, для вычисления наибольшего общего делителя чисел $u_6 = 8$ и $u_7 = 13$ требуется 5 делений с остатком, а для вычисления $(u_{11}, u_{12}) = (89, 144)$ необходимо 10 делений с остатком. Эти примеры показывают, что граница для числа делений, утверждаемая теоремой 1.4 может достигаться.

Для нахождения наибольшего общего делителя нескольких чисел можно использовать так называемый *обобщенный алгоритм Евклида*. Если $a_1, a_2, \ldots, a_n$ – целые неотрицательные числа и $a_2 = a_1 q + r, 0 \leq r < a_1$, то по лемме 1.2 выполняется равенство $\mathcal{D}\{a_1, a_2\} = \mathcal{D}\{r, a_1\}$. Следовательно,

$$\mathcal{D}\{a_1, a_2, a_3, \ldots, a_n\} = \mathcal{D}\{r, a_1, a_3, \ldots, a_n\}$$

[3]Итальянский математик Леонардо Пизанский, 1180-1240, носил прозвище Фибоначчи ("сын Боначчо").

и

$$(a_1, a_2, a_3, \ldots, a_n) = (r, a_1, a_3, \ldots, a_n). \tag{1.5}$$

Наибольший общий делитель совокупности чисел не зависит от того, в каком порядке эти числа записаны, поэтому каждое число в совокупности может быть заменено его остатком от деления на любое другое число из этой же совокупности, причем наибольший общий делитель при такой замене сохранится. Ясно, что операция (1.5) уменьшит сумму чисел в списке, если $a_2 \geq a_1$. И эта сумма не сможет быть уменьшена указанным способом лишь в случае, если все числа списка, кроме одного, равны нулю. Но в таком случае наибольший общий делитель вычисляется легко, $(a_1, 0, \ldots, 0) = a_1$. Эти рассуждения могут быть оформлены в виде алгоритма следующим образом.

**Алгоритм (Обобщенный алгоритм Евклида). Дано:** *Совокупность целых неотрицательных чисел* $\{a_1, \ldots, a_n\}$.

**Найти:** *Наибольший общий делитель* $D = (a_1, \ldots, a_n)$.

*1. Заменить список* $\{a_1, \ldots, a_n\}$, *переставив его элементы так, чтобы число, стоящее на первом месте было наименьшим из положительных чисел списка.*

*2. Если все числа* $a_2, \ldots, a_n$ *равны нулю, положить* $D = a_1$, *СТОП.*

*3. Заменить в списке* $\{a_1, \ldots, a_n\}$ *каждое из ненулевых чисел* $a_2, \ldots, a_n$ *его остатком при делении на* $a_1$. *Перейти в пункт 1 алгоритма.*

Чтобы показать, как работает этот алгоритм рассмотрим пример.

**Пример.** *Вычислить* $D = (10, 6, 15, 24)$.

Имеем

$$\begin{aligned} D = (6, 10, 15, 24) = (6, 4, 3, 0) = (3, 6, 4, 0) = \\ = (3, 0, 1, 0) = (1, 3, 0, 0) = (1, 0, 0, 0) = 1, \end{aligned}$$

т.е. числа $10, 6, 15, 24$ взаимно просты.

Заметим, что числа, равные нулю, могут быть исключены из списка в процессе работы обобщённого алгоритма Евклида. При этом длина списка уменьшится, и на заключительном шаге весь список будет состоять из одного числа - искомого наибольшего общего делителя.

## 1.4 Решение в целых числах линейных уравнений

Уравнения, в которых неизвестные величины выражаются целыми числами, называются диофантовыми по имени древнегреческого ученого Диофанта[4]. Пусть $a, b, c$ – целые числа. Рассмотрим простейшее диофантово уравнение

$$ax + by = c. \tag{1.6}$$

Легко проверить, что уравнение $19x + 12y = 1$ имеет бесконечное множество решений $x = -5 + 12t, y = 8 - 19t, t \in \mathbb{Z}$. Уравнение же $2x - 6y = 3$ решений в целых числах не имеет, ведь при любых целых $x, y$ левая часть этого уравнения делится на 2, т.е. четна, а правая часть 3 есть нечетное число.

**Теорема 1.5.** *1. Уравнение (1.6) разрешимо в целых числах $x, y$ тогда и только тогда, когда $(a, b)|c$.*

*2. В случае разрешимости множество решений бесконечно. Все они имеют вид*

$$x = x_0 + \frac{b}{(a, b)}t, \qquad y = y_0 - \frac{a}{(a, b)}t, \tag{1.7}$$

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

[4]Диофант жил в III веке нашей эры. До нас дошли шесть книг его фундаментального труда "Арифметика", где рассматриваются разнообразные уравнения с целыми и рациональными неизвестными и обсуждаются способы решения таких уравнений.

В приведенных выше примерах имеем $(19, 12) = 1$ и $(2, 6) = 2 \nmid 3$.

*Доказательство.* Предположим, что целые числа $x_0, y_0$ составляют решение уравнения (1.6). Так как $(a, b)|a$ и $(a, b)|b$ то из свойств делимости следует $(a, b)|ax_0+by_0 = c$. Необходимость условия $(a, b)|c$ для разрешимости уравнения (1.6) доказана.

Заметим, что утверждение теоремы в обратную сторону можно доказывать, считая коэффициенты уравнения $a, b$ целыми неотрицательными числами. Общий случай всегда можно свести к этому, сменив, если потребуется, знак у неизвестной.

Предполагая $a \geq 0, b \geq 0$, докажем нужное утверждение методом математической индукции по величине суммы $a + b$.

Если $a+b = 1$, то, скажем, $a = 1, b = 0$. Тогда $(a, b) = 1$ и условие $(a, b)|c$ выполняется при любом $c$. Уравнение также разрешимо при любом $c$. Решением является пара чисел $x = c, y = 0$.

Предположим, что целое $n \geq 1$, и утверждение теоремы выполняется для всех уравнений вида (1.6) с неотрицательными коэффициентами, сумма которых положительна и не превосходит $n$. Пусть также $a, b$ – неотрицательные числа с суммой $a + b = n + 1$. Не уменьшая общности можно считать, что $a \geq b$.

В случае $b = 0$ имеем $(a, b) = a$ и условие $(a, b)|c$ равносильно делимости $a|c$, т.е. равенству $c = au$ с некоторым целым $u$. Уравнение (1.6) имеет решением пару чисел $x = u, y = 0$.

В случае $b \geq 1$ воспользуемся равенством $a = b \cdot 1 + (a - b)$. По второму утверждению леммы 1.2 из него следует $(a, b) = (b, a - b)$ и $(b, a - b)|c$. Учитывая теперь оценку $b + (a - b) = a = n + 1 - b \leq n$, заключаем согласно индуктивному предположению, что существуют целые числа $u, v$, удовлетворяющие равенству $(a - b)u + bv = c$. Это равенство может быть переписано в виде

$$au + b(v - u) = c,$$

откуда следует, что уравнение (1.6) имеет решением целые числа $x = u, y = v - u$. Первое утверждение теоремы полностью доказано.

Для доказательства второго утверждения заметим прежде всего, что числа (1.7) составляют решение уравнения (1.6). Действительно,

$$a\left(x_0 + \frac{b}{(a,b)}t\right) + b\left(y_0 - \frac{a}{(a,b)}t\right) = ax_0 + by_0 = c.$$

Осталось проверить, что каждое решение уравнения (1.6) представимо в виде (1.7). Если $x_1, y_1$ – некоторое решение, то из равенств $ax_1 + by_1 = c$, $ax_0 + by_0 = c$ следует

$$a(x_1 - x_0) = b(y_0 - y_1). \tag{1.8}$$

Числа $a, b$ могут быть представлены в виде $a = (a,b)r, b = (a,b)s$, где $r, s$ – целые взаимно простые числа. Сократив равенство (1.8) на $(a,b)$ получим $r(x_1 - x_0) = s(y_0 - y_1)$ и $s|r(x_1 - x_0)$. Воспользуемся следствием 1.2. С его помощью, учитывая $(r,s) = 1$, заключаем $s|(x_1 - x_0)$ или $x_1 - x_0 = st$ с некоторым целым $t$. Итак,

$$x_1 = x_0 + st = x_0 + \frac{b}{(a,b)}t.$$

Подставляя это выражение в (1.8), находим $\frac{ab}{(a,b)}t = b(y_0 - y_1)$ и $y_1 = y_0 - \frac{a}{(a,b)}t$. Это завершает доказательство теоремы 1.5. □

Приведённое выше доказательство второго утверждения основано на следствии 1.2 из теоремы 1.3. Покажем, как это следствие может быть выведено из первого утверждения теоремы 1.5.

*Второе доказательство следствия 1.2.* По условию числа $a, b$ взаимно просты. Согласно первому утверждению теоремы 1.5 существуют целые числа $x, y$, для которых выполнено равенство $ax+by = 1$. Умножив его на $c$, получим $acx + bcy = c$. Отсюда, так как $ac$ и $bc$ делятся на $b$, заключаем $b|c$. □

Доказательство теоремы 1.5 не позволяет находить решения уравнения (1.6) в целых числах. В силу теоремы 1.5 для этого достаточно найти хотя бы одно его решение. Способ вычисления такого решения основан на алгоритме Евклида.

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 (1.6) будут целые числа $x_0 = \frac{cu}{(a,b)}$, $y_0 = \frac{cv}{(a,b)}$.

Все вычисления удобно оформить в матричном виде. Рассмотрим матрицы

$$A_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}, \qquad i = 1, 2, \ldots, n-1.$$

С их помощью равенства (1.3) могут быть представлены в виде

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = A_i \cdot \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}, \qquad i = 1, 2, \ldots, n-1,$$

и, значит,

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = A_1A_2 \cdots A_{n-1} \cdot \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}.$$

Матрица, обратная к $\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$ имеет вид $\begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$, поэтому

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = B_{n-1} \cdots B_2B_1 \cdot \begin{pmatrix} a \\ b \end{pmatrix},$$

где $B_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$. Обозначив для краткости $B = B_{n-1} \cdots B_1 = \begin{pmatrix} w & t \\ u & v \end{pmatrix}$, из равенства $\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = B \cdot \begin{pmatrix} a \\ b \end{pmatrix}$ найдем $r_n = au + bv$.

Так для примера на стр. 19 имеем

$$B = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 11 & -37 \\ -41 & 138 \end{pmatrix}.$$

Это матричное равенство означает, что уравнение $3009x + 894y = 3$ имеет решение $x = -41, y = 138$.

Обратимся теперь к более общей задаче. Рассмотрим систему диофантовых уравнений

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= b_1, \\ \cdots\cdots\cdots\cdots\cdots & \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n &= b_m, \end{aligned} \tag{1.9}$$

где коэффициенты уравнений $a_{i,j}, b_i$ – целые числа. Неизвестные $x_1, \ldots, x_n$ также предполагаются целыми. С этой системой связываются две матрицы

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} & -b_1 \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} & -b_2 \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots & \cdots\cdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} & -b_m \end{pmatrix}.$$

Первая будет называться матрицей системы, а вторая – расширенной матрицей. В матричном виде эта система уравнений может быть переписана так $\mathbf{A} \cdot \overline{x} = \overline{b}$, где $\overline{b}$ – вектор-столбец размера $m$, состоящий из правых частей системы (1.9). В случае, если все правые части системы (1.9) равны нулю, система называется однородной.

Ниже мы опишем процесс, позволяющий находить все решения системы (1.9) в целых числах.

Составим матрицу $\mathcal{A}$, содержащую $m+n$ строк и $n+1$ столбцов. Первые $m$ строк этой матрицы совпадают со строками матрицы $\mathbf{B}$. Продолжения первых столбцов матрицы $\mathbf{A}$ совпадают со столбцами

единичной $n \times n$ матрицы $\mathbf{E_n}$, а продолжение последнего столбца матрицы $\mathbf{B}$ состоит из нулей. Таким образом, матрица $\mathcal{A}$ имеет вид

$$\mathcal{A} = \begin{pmatrix} \mathbf{A} & -\overline{b} \\ \mathbf{E_n} & 0 \end{pmatrix}. \tag{1.10}$$

Столбцы матрицы $\mathcal{A}$ в порядке следования слева направо обозначим $[\mathcal{A}]_1, \ldots, [\mathcal{A}]_{n+1}$. Часть матрицы $\mathcal{A}$, образованную столбцами $[\mathcal{A}]_1, \ldots, [\mathcal{A}]_n$, будем называть главной частью матрицы $\mathcal{A}$.

Процесс решения системы (1.9) распадается на два этапа. На первом из них выполняются некоторые преобразования, имеющие целью привести $\mathcal{A}$ к специальному виду

$$\mathcal{A}' = \begin{pmatrix} \mathbf{C} & -\overline{b} \\ \mathbf{K} & 0 \end{pmatrix}. \tag{1.11}$$

Здесь $\mathbf{C}$,$\mathbf{K}$ – целочисленные матрицы размера $m \times n$ и $n \times n$ соответственно, и матрица $\mathbf{C}$ имеет трапециевидную форму

$$\mathbf{C} = \begin{pmatrix} c_{1,1} & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ c_{2,1} & c_{2,2} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{r,1} & c_{r,2} & c_{r,3} & \ldots & c_{r,r} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{m,1} & c_{m,2} & c_{m,3} & \ldots & c_{m,r} & 0 & \ldots & 0 \end{pmatrix}, \tag{1.12}$$

причем $c_{1,1} > 0, \ldots, c_{r,r} > 0$.

Для приведения матрицы $\mathcal{A}$ к виду $\mathcal{A}'$ разрешается выполнять преобразования трёх типов (допустимые преобразования):

а) переставить столбцы главной части $\mathcal{A}$;

б) изменить знаки у всех элементов какого-либо столбца главной части;

в) умножить первый столбец главной части на некоторое целое число и вычесть результат из другого столбца главной части.

Опишем последовательность выполняемых преобразований подробнее. По ходу работы алгоритма матрица $\mathcal{A}$ будет меняться, однако для краткости мы будем обозначать замещающие её матрицы

той же буквой $\mathcal{A}$, а для элементов этих матриц по-прежнему будем использовать обозначения $a_{i,j}$. Таким образом, знак $a_{i,j}$ используется для числа, стоящего на пересечении строки с номером $i$ и столбца с номером $j$, меняющегося в процессе вычислений. Сама последовательность вычислений будет похожа на обобщённый алгоритм Евклида:

1. Изменить главную часть матрицы $\mathcal{A}$ с помощью допустимых преобразований вида а) и б) так, чтобы в левом верхнем углу $\mathcal{A}$ стояло положительное число, наименьшее среди абсолютных величин всех ненулевых элементов первой строки главной части.

2. Разделить каждое из чисел $a_{1,j}$ с остатком на $a_{1,1}$, т.е. найти представления

$$a_{1,j} = a_{1,1}d_j + s_j, \quad 0 \leq s_j < a_{1,1}, \qquad j = 2, \ldots, n.$$

Заменить в матрице $\mathcal{A}$ столбцы $[\mathcal{A}]_2, \ldots, [\mathcal{A}]_n$ столбцами

$$[\mathcal{A}]_2 - d_2[\mathcal{A}]_1, \ldots, [\mathcal{A}]_n - d_n[\mathcal{A}]_1$$

соответственно. Вернуться к пункту 1 и снова повторить все операции.

В результате выполнения пунктов 1 и 2, как и в обощённом алгоритме Евклида, будет уменьшаться сумма абсолютных величин элементов первой строки главной части $\mathcal{A}$. Процесс этот завершится лишь тогда, когда все элементы $a_{1,2}, \ldots, a_{1,n}$ станут равными нулю. На этом этапе вычислений определится первый столбец матрицы $\mathcal{A}'$.

Дальнейшая работа происходит со столбцами $[\mathcal{A}]_2, \ldots, [\mathcal{A}]_n$. Заметим, что первые элементы этих столбцов равны нулю, и потому выполнение допустимых преобразований с этими столбцами не будет менять первую строку $\mathcal{A}$. В дальнейшем необходимо выполнить операции указанных выше пунктов 1 и 2 с матрицей, образованной столбцами $[\mathcal{A}]_2, \ldots, [\mathcal{A}]_n$, работая с элементами второй строки этой матрицы (все элементы первой строки равны нулю). В результате матрица $\mathcal{A}$ преобразуется к виду $a_{2,2} = c_{2,2} > 0, a_{2,3} = \cdots = a_{2,n} = 0$.

Ясно, что продолжение подобных действий со столбцами $[\mathcal{A}]_3, \ldots, [\mathcal{A}]_n$ в конечном счете приведет матрицу $\mathcal{A}$ к виду $\mathcal{A}'$.

Во второй части алгоритма происходит работа со всеми столбцами матрицы $\mathcal{A}'$. По-прежнему будем обозначать их $[\mathcal{A}]_1, \ldots, [\mathcal{A}]_{n+1}$.

3. Обозначим $k_1$ и $\ell_1$ неполное частное и остаток от деления первого элемента столбца $[\mathcal{A}]_{n+1}$ на $c_{1,1}$ и заменим столбец $[\mathcal{A}]_{n+1}$ на $[\mathcal{A}]_{n+1} - k_1[\mathcal{A}]_1$. Обозначим далее $k_2$ и $\ell_2$ неполное частное и остаток от деления второго элемента нового столбца $[\mathcal{A}]_{n+1}$ на $c_{2,2}$ и заменим столбец $[\mathcal{A}]_{n+1}$ на $[\mathcal{A}]_{n+1} - k_2[\mathcal{A}]_2$. Продолжим действовать таким же образом, пока столбец $[\mathcal{A}]_{n+1}$ не будет заменен на $[\mathcal{A}]_{n+1} - k_r[\mathcal{A}]_r$. На этом вычисления заканчиваются. Первые $r$ элементов столбца $[\mathcal{A}]_{n+1}$ равны $\ell_1, \ldots, \ell_r$, а остальные обозначим последовательно $\ell_{r+1}, \ldots, \ell_{m+n}$. Заметим, что $0 \leq \ell_j < c_{j,j}$, $j = 1, \ldots, r$.

**Теорема 1.6.** *1. Система уравнений (1.9) разрешима в целых числах тогда и только тогда, когда* $\ell_1 = \cdots = \ell_m = 0$.

*2. В случае разрешимости обозначим* $s = n - r$ *и* $\overline{x}_0 \in \mathbb{Z}^n$ *– вектор с координатами* $\ell_{m+1}, \ldots, \ell_{m+n}$ *в порядке следования. Тогда общее решение системы уравнений (1.9) имеет вид*

$$\overline{x}_0 + t_1[K]_{r+1} + \cdots + t_s[K]_n, \tag{1.13}$$

*где* $t_1, \ldots, t_s$ *пробегают всевозможные наборы целых чисел, а* $[K]_j$ *– соответствующие столбцы матрицы* $\mathbf{K}$*, см. (1.11).*

*Доказательство.* Заметим, что каждый столбец главной части матрицы $\mathcal{A}'$ есть линейная комбинация столбцов главной части исходной матрицы $\mathcal{A}$, отвечающей системе уравнений (1.9). Поэтому равенства $\ell_1 = \cdots = \ell_m = 0$ означают, что столбец $\overline{b}$ есть линейная комбинация столбцов матрицы $\mathbf{A}$ с целыми коэффициентами. Это, конечно, означает разрешимость системы (1.9).

Заметим, что преобразование, обратное к допустимому преобразованию также допустимо. Это значит, что каждый столбец главной части исходной матрицы $\mathcal{A}$ есть линейная комбинация столбцов

главной части матрицы $\mathcal{A}'$. Если система уравнений (1.9) разрешима в целых числах, то вектор $\overline{b}$ есть линейная комбинация с целыми коэффициентами столбцов матрицы $A$. Но тогда, в силу сказанного выше, он есть линейная комбинация столбцов матрицы $C$. Будем использовать обозначение $[C]_1, \ldots, [C]_n$ для столбцов матрицы $C$. Заметим, что все столбцы $[C]_j, j > r$, нулевые. Поэтому для некоторых целых чисел $u_1, \ldots, u_r$ выполняется равенство

$$u_1[C]_1 + \cdots + u_r[C]_r = \overline{b}.$$

Сравнивая в этом равенстве первые координаты, заключаем, что $u_1 c_{1,1} = b_1$. Отсюда следует, что $k_1 = u_1$, и $\ell_1 = 0$. Сравнение вторых координат даёт $u_2 c_{2,2} = b_2 - k_1 c_{2,1}$ и, следовательно, $k_2 = u_2$ и $\ell_2 = 0$. Продолжая эти рассуждения, находим $\ell_1 = \cdots = \ell_r = 0$ и $u_j = k_j, j = 1, \ldots, r$. Но тогда $\overline{b} - k_1[C]_1 - \cdots - k_r[C]_r$ есть нулевой вектор и, значит, $\ell_{r+1} = \cdots = \ell_n = 0$. Это завершает доказательство первого утверждения теоремы.

Любая допустимая операция со столбцами матрицы равносильна умножению справа этой матрицы на некоторую целочисленную матрицу с определителем $\pm 1$. Так изменение знака у всех элементов столбца с номером $k$ равносильно умножению на диагональную матрицу, у которой все элементы главной диагонали равны 1, за исключением, стоящего в $k$-й строке, который равен $-1$. Перестановка столбцов с номерами $\ell$, $k$ равносильна умножению на матрицу, у которой все столбцы, кроме имеющих номера $\ell$ и $k$ совпадают со столбцами единичной матрицы, на пересечении $k$-го столбца с $\ell$ - й строкой и $\ell$-го столбца с $k$-й строкой стоят единицы, а все остальные элементы этих столбцов равны 0. Вычитание первого столбца, умноженного на целое $q$ из столбца с номером $k$ равносильно умножению на матрицу, совпадающую с единичной матрицей, за исключением элемента, стоящего на пересечениии первой строки и $k$-го столбца, где вместо 0 стоит $-q$.

Из сказанного выше следует равенство

$$\begin{pmatrix} \mathbf{C} \\ \mathbf{K} \end{pmatrix} = \begin{pmatrix} \mathbf{A} \\ \mathbf{E_n} \end{pmatrix} \cdot \mathbf{S},$$

где $\mathbf{S}$ – некоторая целочисленная матрица размера $n \times n$ с определителем $\pm 1$. Но тогда $\mathbf{C} = \mathbf{A} \cdot \mathbf{S}$ и $\mathbf{K} = \mathbf{E_n} \cdot \mathbf{S}$, так что $\mathbf{C} = \mathbf{A} \cdot \mathbf{K}$.

Предположим теперь, что система (1.9) разрешима. Тогда из сказанного выше следует равенство

$$\begin{pmatrix} 0 \\ \overline{x}_0 \end{pmatrix} = \begin{pmatrix} -\overline{b} \\ 0 \end{pmatrix} + \begin{pmatrix} \mathbf{A} \\ \mathbf{E_n} \end{pmatrix} \cdot \overline{v},$$

с некоторым вектором $\overline{v} \in \mathbb{Z}^n$. Отсюда находим $\overline{x}_0 = \overline{v}$ и $0 = -\overline{b} + \mathbf{A} \cdot \overline{v}$. Но тогда $0 = -\overline{b} + \mathbf{A} \cdot \overline{x}_0$ и $\overline{x}_0$ есть решение системы (1.9).

Разобъём матрицу $\mathbf{K}$ на две части $\mathbf{K}_1 = ([\mathbf{K}]_1, \ldots, [\mathbf{K}]_r)$ и $\mathbf{K}_2 = ([\mathbf{K}]_{r+1}, \ldots, [\mathbf{K}]_n)$. Последние $s = n - r$ столбцов матрицы $\mathbf{C}$ нулевые, поэтому из установленного выше равенства $\mathbf{C} = \mathbf{A} \cdot \mathbf{K}$ следует $\mathbf{A}\mathbf{K}_2 = \mathbf{0}$. Но это значит, что все столбцы матрицы $\mathbf{K}_2$, т.е. векторы $[\mathbf{K}]_{r+1}, \ldots, [\mathbf{K}]_n$ есть решения однородной системы уравнений, соответствующей (1.9). Тогда с любыми целыми числами $t_1, \ldots, t_s$ выполняется равенство $\mathbf{A} \cdot (\overline{x}_0 + t_1[\mathbf{K}]_{r+1} + \cdots + t_s[\mathbf{K}]_n) = \overline{b}$ и вектор (1.13) есть решение системы (1.9).

Для любого решения $\overline{x} \in \mathbb{Z}^n$ системы (1.9) должно выполняться равенство $\mathbf{A}(\overline{x} - \overline{x}_0) = 0$. По доказанному ранее $\mathbf{K}$ есть целочисленная матрица с определителем $\pm 1$. Поэтому обратная к ней матрица имеет целые элементы. Обозначив $\overline{y} = \mathbf{K}^{-1}(\overline{x} - \overline{x}_0) \in \mathbb{Z}^n$ будем иметь

$$\mathbf{C}\overline{y} = \mathbf{A} \cdot \mathbf{K}\overline{y} = \mathbf{A} \cdot (\overline{x} - \overline{x}_0) = 0.$$

Учитывая теперь вид (1.12) матрицы $\mathbf{C}$, находим, что первые $r$ координат вектора $\overline{y}$ равны 0. Значит $\overline{x} - \overline{x}_0 = \mathbf{K} \cdot \overline{y} = \mathbf{K}_2 \cdot \overline{t}$, где $\overline{t} \in \mathbb{Z}^s$ есть вектор состоящий из последних $s$ координат вектора $\overline{y}$. Если эти координаты есть $t_1, \ldots, t_s$, получаем представление (1.13) для вектора $\overline{x}$.

Теорема полностью доказана. □

Покажем, как работает изложенный выше алгоритм.

**Пример.** *Решить уравнение* $87x_1 + 13x_2 + 6x_3 = 1$.

Выполняя допустимые преобразования, находим

$$\mathcal{A} = \begin{pmatrix} 87 & 13 & 6 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 6 & 13 & 87 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 6 & 1 & 3 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -2 & -14 & 0 \end{pmatrix} \sim$$
$$\begin{pmatrix} 1 & 6 & 3 & -1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ -2 & 1 & -14 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & -6 & -3 & 1 \\ -2 & 13 & -8 & -2 \end{pmatrix}.$$

Данное уравнение разрешимо и его общее решение имеет вид

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -2 \end{pmatrix} + t_1 \begin{pmatrix} 0 \\ -6 \\ 13 \end{pmatrix} + t_2 \begin{pmatrix} 1 \\ -3 \\ -8 \end{pmatrix}, \qquad t_1, t_2 \in \mathbb{Z}.$$

В заключение установим необходимое и достаточное условие разрешимости системы линейных диофантовых уравнений, аналогичное первому утверждению теоремы 1.5. При этом будем предполагать, что уравнения системы (1.9) независимы, т.е. ранг матрицы $\mathbf{A}$ равен $m$. В противном случае некоторые уравнения можно исключить из системы, не изменив множества решений. Чтобы сделать формулировку и доказательство по возможности более короткими, для каждой целочисленной матрицы $\mathbf{M}$ ранга $m$ будем обозначать символом $D\{\mathbf{M}\}$ наибольший общий делитель миноров этой матрицы порядка $m$.

**Теорема 1.7.** *Если уравнения системы (1.9) независимы, то равенство* $D\{\mathbf{A}\} = D\{\mathbf{B}\}$ *необходимо и достаточно для её разрешимости в целых числах.*

*Доказательство.* Мы будем использовать в доказательстве обозначения, введенные в алгоритме решения систем и в доказательстве теоремы 1.6.

При выполнении допустимых преобразований ранги матриц не меняются. Точно так же по второму утверждению леммы 1.2 при выполнении допустимых преобразований не будут меняться наибольшие общие делители миноров максимального ранга. Поэтому $\operatorname{rg}\mathbf{A} = \operatorname{rg}\mathbf{C}$, т.е. $r = m$, и $D\{\mathbf{A}\} = D\{\mathbf{C}\}$, $D\{\mathbf{B}\} = D\{(\mathbf{C}, \overline{\ell})\}$, где $\overline{\ell}$ – вектор-столбец с координатами $\ell_1, \ldots, \ell_m$.

Если система уравнений (1.9) разрешима в целых числах, то по теореме 1.6 имеем $\ell_1 = \ldots = \ell_m = 0$. Но тогда матрица $(\mathbf{C}, \overline{\ell})$ имеет единственный отличный от нуля минор порядка $m$ и он равен определителю матрицы $\mathbf{C}$. Поэтому $D\{\mathbf{C}\} = D\{(\mathbf{C}, \overline{\ell})\}$, и это доказывает необходимость условия теоремы.

Предположим теперь, что выполнено равенство $D\{\mathbf{A}\} = D\{\mathbf{B}\}$. Так как $\operatorname{rg}\mathbf{C} = m$, то система уравнений $\mathbf{C}\overline{x} = \overline{\ell}$ разрешима в рациональных числах. Поэтому существуют целые взаимно простые числа $u_0, \ldots, u_m$, $u_0 > 0$, такие, что

$$u_0\overline{\ell} = u_1[\mathbf{C}]_1 + \cdots + u_m[\mathbf{C}]_m. \tag{1.14}$$

Обозначим $\Delta_j$ определитель матрицы, построенный на столбцах

$$\overline{\ell}, [\mathbf{C}]_\mathbf{1}, \ldots, [\mathbf{C}]_\mathbf{j-1}, [\mathbf{C}]_\mathbf{j+1}, \ldots, [\mathbf{C}]_\mathbf{m}$$

и $\Delta_0 = c_{1,1} \cdots c_{r,r}$ – единственный отличный от нуля минор порядка $m$ матрицы $\mathbf{C}$. Выразим вектор $\overline{\ell}$ с помощью равенства (1.14) через векторы $[\mathbf{C}]_k$ и подставим это выражение в определитель $\Delta_j$. Поскольку определитель линейно зависит от элементов первого столбца, а, кроме того, определитель с двумя совпадающими столбцами равен нулю, находим $u_0\Delta_j = \pm u_j\Delta_0$. Справедливы равенства

$$D\{\mathbf{B}\} = D\{(\mathbf{C}, \overline{\ell})\} = (\Delta_0, \Delta_1, \ldots, \Delta_m).$$

Умножая их на $u_0$ и, пользуясь следствием 2.4, будем иметь

$$u_0 D\{\mathbf{B}\} = (u_0\Delta_0, \ldots, u_0\Delta_m) = (u_0\Delta_0, u_1\Delta_0 \ldots, u_m\Delta_0) = \\ \Delta_0(u_0, u_1, \ldots, u_m) = \Delta_0 = D\{\mathbf{A}\}.$$

Согласно условию выполняется равенство $D\{\mathbf{A}\} = D\{\mathbf{B}\}$, поэтому $u_0 = 1$.

Теперь сравним первые координаты векторов в (1.14). Получившееся при этом равенство $\ell_1 = u_1 c_{1,1}$ и неравенства $0 \leq \ell_1 < c_{1,1}$ означают, что $\ell_1 = 0, u_1 = 0$. Сравнение вторых координат в (1.14) даёт $\ell_2 = u_2 c_{2,2}$, откуда в силу $0 \leq \ell_2 < c_{2,2}$, получаем $\ell_2 = 0, u_2 = 0$. Продолжая действовать точно так же, найдём $\ell_1 = \cdots = \ell_m = 0$. По теореме 1.6 теперь можно утверждать, что система диофантовых уравнений (1.9) разрешима в целых числах. □

# Глава 2

# Простые и составные числа

Натуральное число называется *составным*, если его можно представить в виде произведения двух меньших натуральных чисел. Заметим, что оба множителя при этом отличны от 1. Примеры составных чисел строить очень легко. Для этого нужно взять какие-нибудь два натуральных числа, не равных 1, и перемножить их. Так $2 \cdot 3 = 6$, $23 \cdot 47 = 1081$, $127 \cdot 9721 = 1234567$ – составные числа. Гораздо труднее разложить какое-нибудь заданное число на множители, иногда, как в следующих двух примерах, для этого требуется применение вычислительных средств:

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

Некоторые натуральные числа, отличные от 1, вообще нельзя представить в виде произведения меньших множителей. Такие числа называются *простыми*. Все сомножители в приведенных выше примерах – простые числа. Эта глава посвящена, в основном, обсуждению свойств простых чисел.

## 2.1 Простые числа. Решето Эратосфена. Бесконечность множества простых чисел

Как было сказано выше, отличное от 1 натуральное число называется *простым*, если его нельзя представить в виде произведения

меньших натуральных сомножителей. Всякое простое число $p$ имеет лишь два положительных делителя: 1 и $p$.

Множители, в произведение которых раскладывается составное число, являются его делителями. Поэтому можно сказать, что натуральное число – составное, если оно делится на некоторое меньшее число, отличное от 1. Так все четные числа, превосходящие 2, делятся на 2 и потому все они составные. А 7 не делится ни на одно из чисел $2, 3, 4, 5, 6$ и потому составным не является, т.е. просто. Чтобы проверить, пользуясь указанным правилом, будет составным число 1009 или нет, нужно разделить его на все числа из ряда $2, 3, 4, \cdots, 1007, 1008$. Это утомительное занятие можно значительно сократить, если воспользоваться следующим утверждением.

**Лемма 2.1.** *Пусть $N$ – составное число и $p$ – наименьший из его делителей, удовлетворяющих условию $p > 1$. Тогда $p$ - простое число и $p^2 \leq N$.*

*Доказательство.* Так как $N$ – составное число, то по определению оно может быть представлено в виде $N = u \cdot v$, причем $1 < u < N, 1 < v < N$. Согласно условию леммы имеем $p^2 \leq u \cdot v = N$.

Пусть $d$ – какой-либо отличный от единицы делитель $p$. Свойства $d|p, p|N$ означают, что $d$ есть делитель $N$, и по определению $p$ имеем $d \geq p$. Итак, число $p$ не имеет делителей, удовлетворяющих неравенствам $1 < d < p$. Значит, $p$ – простое число. □

**Следствие 2.1.** *Каждое целое число $N > 1$ имеет простой делитель.*

*Доказательство.* Если $N$ – простое число, то утверждение выполнено, поскольку $N|N$. Если же $N$ – составное число, утверждение имеет место согласно лемме 2.1. □

Лемма 2.1 позволяет утверждать, что если 1009 составное число, то оно имеет простой делитель $p$, удовлетворяющий неравенствам $2 \leq p \leq 31$. Поскольку все четные числа, отличные от 2, не просты, и составными являются делящиеся на 3 числа $9, 15, 21, 27$, а

также число $25 = 5 \cdot 5$, заключаем что возможные делители 1009 содержатся среди чисел

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. \tag{2.1}$$

Теперь уже сравнительно легко обнаружить, что ни одно из них не является делителем 1009, так что это число простое.

Числа (2.1) составляют список всех простых чисел $p$ из промежутка $2 \leq p \leq 31$. Действительно, если среди чисел (2.1) есть составное число, оно должно иметь простой делитель, не превосходящий 5. Но все числа, делящиеся на $2, 3, 5$ уже исключены нами из отрезка $2 \leq x \leq 31$.

Приведенным выше рассуждениям можно придать общую форму, и в результате мы получаем 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 $p_1 < p_2 < \ldots$ до заданной границы $N$].

*1. Выпишем все целые числа* $2, 3, 4, 5, \ldots, N-1, N$. *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* $k \geq 2$ *и уже определены числа* $p_1, \ldots, p_{k-1}$. *Обозначим* $p_k$ *первое невычеркнутое число, следующее за* $p_{k-1}$. *Если* $p_k^2 > N$, *обозначаем* $p_{k+1}, p_{k+2}, \ldots$ *все оставшиеся невычеркнутыми числа, следующие за* $p_k$ *в порядке возрастания. На этом алгоритм завершает свою работу.*

*3. Если* $p_k^2 \leq N$, *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.*

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

Для обоснования корректности алгоритма, заметим, что в процессе его работы вычеркиваются только составные, а все простые числа остаются невычеркнутыми. Предположим теперь, что среди невычеркнутых чисел осталось хотя бы одно составное, обозначим его буквой $a, 2 \leq a \leq N$. По лемме 2.1 это число имеет простой делитель $p$, удовлетворяющий неравенствам $p^2 \leq a \leq N$. Как и всякое простое, число $p$ осталось невычеркнутым по окончании работы алгоритма. Вместе с тем неравенство $p^2 \leq N$ означает, что в результате одного из проходов алгоритма по списку чисел от 2 до $N$ были вычеркнуты, начиная с $p^2$ все числа, делящиеся на $p$. Но тогда и $a$ должно содержаться среди вычеркнутых чисел. Получившееся противоречие доказывает, что алгоритм оставляет невычеркнутыми только простые числа. Это завершает обоснование алгоритма.

Простые числа составляют довольно большую часть натурального ряда. Так среди первых 100 натуральных чисел имеется 25 простых, а среди первых $10^{16}$ натуральных – 279238341033925 простых. Попадаются весьма неожиданные примеры простых чисел. Так простыми будут

$$\underbrace{1\ldots1}_{44}2007\underbrace{1\ldots1}_{44} \qquad \text{и} \qquad 2007\underbrace{1\ldots1}_{275}2007.$$

Наибольшие из известных в настоящее время простых чисел имеют вид

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

Они записываются соответственно $7235733, 7816230$ и $9152052$ десятичными цифрами. Наибольшее из них было найдено в декабре 2005г. Впрочем, пока эта книга готовится к изданию, возможно, рекорд будет побит. Следить за достижениями в этой области можно в Интернет 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 2.1.** *Множество простых чисел бесконечно.*

*Доказательство.* Допустим, что простые числа составляют конечное множество $\{p_1, p_2, \ldots, p_m\}$. Рассмотрим натуральное число $N = p_1 \cdots p_m + 1$. Согласно следствию 2.1 оно имеет простой делитель $p$. Так как $N$ не делится ни на одно из чисел $p_1, \ldots, p_m$, но делится на $p$, то простое число $p$ отлично от каждого из $p_1, \ldots, p_m$. Получившееся противоречие завершает доказательство теоремы Евклида о простых числах. □

## 2.2 Основная теорема арифметики

Целое число 6025729 может быть разложено на множители следующим образом

$$6025729 = 2419 \cdot 2491 = 2173 \cdot 2773. \tag{2.2}$$

Попытки разложить далее каждый из четырех сомножителей требуют некоторых усилий. Тем не менее, согласно теореме, носящей название "основная теорема арифметики", разложения на меньшие сомножители должны существовать.

**Теорема 2.2.** *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. Множители в разложениях (2.2) не могут быть простыми. Более того, каждое простое число, входящее в разложение 2173, должно, согласно теореме 2.2, присутствовать в разложениях 2419 или 2491.

[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.

Но это легко проверить, вычислив наибольшие общие делители. С помощью алгоритма Евклида находим

$$(2173, 2419) = 41, \qquad (2173, 2491) = 53.$$

Теперь, выполняя деления, получаем

$$2173 = 41 \cdot 53, \quad 2419 = 41 \cdot 59, \quad 2491 = 47 \cdot 53, \quad 2773 = 47 \cdot 59,$$

так что $6025729 = 41 \cdot 47 \cdot 53 \cdot 59$, и все сомножители в последнем разложении, как легко проверить, просты.

*Доказательство теоремы 2.2.* Воспользуемся методом математической индукции. Числа $2, 3$, как мы в этом уже убедились, просты, и, значит, утверждение теоремы для них справедливо.

Пусть натуральное $n > 3$ и каждое целое число, меньшее $n$, единственным способом представимо в виде произведения простых.

Докажем сначала, что $n$ может быть разложено в произведение простых чисел. По следствию 2.1 существует простое $p_1$, делящее $n$. В случае $n = p_1$ искомое произведение состоит из одного множителя. Если же $p_1 < n$, то $n = p_1 m$, где $1 < m < n$. Согласно индуктивному предположению найдутся простые числа $p_2, \ldots, p_r$, для которых $m = p_2 \cdots p_r$. Тогда $n = p_1 p_2 \cdots p_r$. Существование разложения доказано.

Предположим теперь, что возможны два разложения

$$n = p_1 \cdots p_r = q_1 \cdots q_s, \tag{2.3}$$

где $p_i, q_j$ – простые числа.

Если $p_1$ совпадает с каким-либо из чисел $q_j$, то, сократив равенство (2.3) на этот общий множитель, получим два различных представления числа $m = p_2 \cdots p_r < n$ в виде произведения простых чисел. Но это согласно индуктивному предположению невозможно.

Значит, $p_1$ отлично от всех чисел $q_j$. Все положительные делители $p_1$ исчерпываются числами $1, p_1$, а все положительные делители $q_1$ исчерпываются числами $1, q_1$. Лишь единица присутствует в обоих

множествах. Значит, $(p_1, q_1) = 1$. Согласно следствию 1.2 из теоремы 1.2 число $u = q_2 \cdots q_s < n$ делится на $p_1$, т.е. $u = p_1 \cdot v$ с $v \in \mathbb{Z}$. Число $v$ согласно индуктивному предположению можно представить в виде произведения простых чисел. Это приводит к новому разложению $u$ на простые сомножители, ведь все числа $q_j$ отличны от $p_1$. Итак, $u$ допускает два различных представления в виде произведения простых чисел, вопреки индуктивному предположению. Получившееся противоречие завершает доказательство теоремы. □

Утверждение о единственности разложения можно доказать и по-другому, не ссылаясь на результаты параграфа 1.2.

*Второе доказательство единственности.* Как и в первом доказательстве будем использовать индукцию по величине раскладываемого числа $n$. Допустим существование двух разложений (2.3). Повторив рассуждения из начала первого доказательства единственности, можно придти к случаю, когда простое число $p_1$ отлично от всех $q_j$ при любых индексах $j$. Не уменьшая общности можно считать при этом, что $p_1 < q_1$. Рассмотрим целое число $a = n - p_1 q_2 \cdots q_s$. Его можно двумя разными способами представить в виде произведения меньших чисел

$$a = (q_1 - p_1) q_2 \cdots q_s = p_1 b < n,$$

где $b = p_2 \cdots p_r - q_2 \cdots q_s$. Оба числа $q_1 - p_1$ и $b$ могут быть разложены в произведения простых множителей, и таким образом будут получены два разложения числа $a < n$ в произведения простых. Докажем, что они различны. В разложение $a = p_1 b$ входит простое число $p_1$. Оно отлично от всех простых чисел $q_2, \ldots, q_s$ в разложении $a = (q_1 - p_1) q_2 \cdots q_s$. Но оно не входит и в разложение числа $q_1 - p_1$, в противном случае мы имели бы $p_1 | q_1$, вопреки простоте $q_1$ и предположению $p_1 \neq q_1$. Получившееся противоречие завершает доказательство. □

*Третье доказательство единственности.* Заметим, что если натуральное число единственным образом раскладывается в произведе-

ние простых чисел, то каждый его простой делитель должен входить в это разложение. Как и ранее можно вести доказательство с помощью индукции по величине раскладываемого числа. Предположив, что существуют два разложения (2.3), не содержащие одинаковых простых в левой и правой частях, можно считать, что $p_1$ – самое маленькое простое среди $p_j$ и точно так же $q_1$ – самое маленькое среди $q_i$. Кроме того, можно предполагать, что $p_1 < q_1$. Поскольку $n$ – составное число, имеем $p_1^2 < q_1^2 \leq n$ и, значит, $p_1 q_1 < n$. Натуральное число $b = n - p_1 q_1$ меньше, чем $n$. Кроме того, оно делится на оба простых числа $p_1, q_1$. Согласно индуктивному предположению оно единственным образом раскладывается в произведение простых чисел и потому оба эти простые числа должны входить в разложение $b$. Но тогда $p_1 q_1 | b$ и $p_1 q_1 | n = q_1 q_2 \cdots q_s$. Следовательно, $p_1 | u = q_2 \cdots q_s$. Но это невозможно, так как $u < n$ и по индуктивному предположению каждый его простой делитель должен входить в его разложение на простые множители. □

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 представление числа 2520 имеет вид $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

Набор различных простых чисел, а также набор показателей степени $\alpha_j$ 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,

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

При таком определении справедливо представление

$$n = \prod_{p|n} p^{\nu_p(n)}. \tag{2.4}$$

В дальнейшем будут использоваться подобные выражения с указанием под знаком произведения тех или иных условий на входящие в него простые числа. Кроме того, иногда удобно бывает формально записывать и бесконечные произведения, если лишь конечное количество, входящих в них сомножителей отлично от единицы. Например, равенство (2.4) может быть записано в виде

$$n = \prod_{p} p^{\nu_p(n)},$$

где произведение берется по бесконечному, согласно теореме 2.1, множеству всех простых чисел. В этом произведении лишь конечное количество сомножителей отлично от единицы, ведь $\nu_p(n) \neq 0$ лишь для простых делителей $p$ числа $n$, а это множество конечно.

При умножении степеней с одинаковым основанием показатели степени складываются, поэтому для любых двух целых чисел $a, b$ и простого числа $p$ выполняется равенство

$$\nu_p(ab) = \nu_p(a) + \nu_p(b). \tag{2.5}$$

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

$$\nu_p(d) \leq \nu_p(n). \tag{2.6}$$

Действительно, равенство $n = d \cdot u$ в силу (2.5) и неравенства $\nu_p(u) \geq 0$ приводит к (2.6). Если же наоборот, для любого простого числа $p$ выполняется неравенство (2.6), то целое число

$$u = \prod_{p} p^{\nu_p(n) - \nu_p(d)}$$

удовлетворяет равенству $n = du$ и, значит, $d|n$.

Еще одно простое, но полезное свойство будет использоваться в дальнейшем. *Если $a$ и $b$ – натуральные числа, причем для каждого простого числа $p$ выполнено равенство $\nu_p(a) = \nu_p(b)$, то $a = b$.*

Определим канонические разложения наименьшего общего кратного и наибольшего общего делителя нескольких натуральных чисел.

**Следствие 2.2.** *Для любых натуральных чисел $a_1, \ldots, a_m$ и любого простого числа $p$ справедливы равенства*

$$\nu_p([a_1, \ldots, a_m]) = \max\{\nu_p(a_1), \ldots, \nu_p(a_m)\} \tag{2.7}$$

$$\nu_p((a_1, \ldots, a_m)) = \min\{\nu_p(a_1), \ldots, \nu_p(a_m)\} \tag{2.8}$$

*Доказательство.* Определим целое число $M$ равенством

$$M = \prod_p p^{\max\{\nu_p(a_1),\ldots,\nu_p(a_m)\}}.$$

Из неравенств $\nu_p(M) \geq \nu_p(a_j)$ следует $a_j|M$, т.е. $M$ – общее кратное чисел $a_1, \ldots, a_m$. Если $K$ - какое-нибудь общее кратное этих чисел, то при любом простом $p$ должны выполняться неравенства

$$\nu_p(K) \geq \nu_p(a_j), \qquad j = 1, \ldots, m,$$

и, значит,

$$\nu_p(K) \geq \max\{\nu_p(a_1), \ldots, \nu_p(a_m)\} = \nu_p(M).$$

Следовательно, $M|K$ и $M \leq K$. Это доказывает, что $M$ есть наименьшее общее кратное данных чисел, и (2.7).

Равенство (2.7) доказывается аналогично. Определим

$$D = \prod_p p^{\min\{\nu_p(a_1),\ldots,\nu_p(a_m)\}}.$$

Из неравенств $\nu_p(D) \leq \nu_p(a_j)$ следует $D|a_j$, т.е. $D$ – общий делитель чисел $a_1, \ldots, a_m$. Если $L$ - какой-нибудь общий делитель этих чисел, то при любом простом $p$ должны выполняться неравенства

$$\nu_p(L) \leq \nu_p(a_j), \qquad j = 1, \ldots, m,$$

и, значит,

$$\nu_p(L) \le \min\{\nu_p(a_1), \dots, \nu_p(a_m)\} = \nu_p(D).$$

Следовательно, $L|D$ и $D \ge L$. Это доказывает, что $D$ есть наибольший общий делитель данных чисел, и (2.8). □

Приведённые рассуждения дают также иные доказательства теорем 1.2 и 1.3.

Равенства (2.7) и (2.8) могут использоваться также и для вычисления наименьшего кратного и наибольшего общего делителя нескольких чисел. Так имеем

$$2737 = 7 \cdot 17 \cdot 23, \quad 9163 = 7^2 \cdot 11 \cdot 17, \quad 9639 = 3^4 \cdot 7 \cdot 17$$

и, значит,

$$[2737, 9163, 9639] = 3^4 \cdot 7^2 \cdot 11 \cdot 17 \cdot 23 = 17070669,$$
$$(2737, 9163, 9639) = 7 \cdot 17 = 119.$$

Этот способ, однако, применим лишь, если числа сравнительно невелики. Разложение на простые сомножители больших чисел – очень трудоёмкая задача, и в таком случае удобнее использовать алгоритмы, приведённые в главе 1.

Приведем еще несколько следствий основной теоремы арифметики. Их можно было бы вывести и из теорем 1.2 и 1.3 в параграфе 1.2. Но приводимые здесь доказательства короче и единообразнее. В дальнейшем предполагается, что $b, a_1, \dots, a_n$ – произвольные натуральные числа.

**Следствие 2.3.** *Если число $b$ взаимно просто с каждым из чисел $a_1, \dots, a_n$, то оно взаимно просто с произведением этих чисел.*

*Доказательство.* Обозначим $d = (b, a_1 \cdots a_n)$. Пусть $p$ – какое-либо простое число. Так как $\nu_p(d) \le \nu_p(b)$, то в случае $\nu_p(b) = 0$ имеем также $\nu_p(d) = 0$. Если же $\nu_p(b) \ge 1$, то в силу взаимной простоты $b$ и $a_j$ имеем $\nu_p(a_j) = 0$, $1 \le j \le n$. Но тогда $\nu_p(d) \le \nu_p(a_1 \cdots a_n) =$

$\nu_p(a_1)+\ldots+\nu_p(a_n) = 0$. Итак, в любом случае выполняется $\nu_p(d) = 0$. Поскольку это верно для любого простого числа $p$, заключаем $d = 1$. Следствие доказано. □

**Следствие 2.4.** *При любом натуральном $b$ выполняется равенство*

$$(ba_1, \ldots, ba_n) = b(a_1, \ldots, a_n).$$

*Доказательство.* Для каждого простого числа $p$, пользуясь равенством (2.5) и следствием 2.2, находим

$$\nu_p((ba_1, \ldots, ba_n)) = \min_{1\le j\le n} \nu_p(ba_j) = \min_{1\le j\le n} (\nu_p(b) + \nu_p(a_j)) =$$
$$\nu_p(b) + \min_{1\le j\le n} \nu_p(a_j) = \nu_p(b) + \nu_p((a_1, \ldots, a_n)) = \nu_p(b(a_1, \ldots, a_n)).$$

Это доказывает нужное равенство. □

**Определение 4.** *Целые числа $a_1, \ldots, a_n$ называются попарно взаимно простыми, если для любых двух индексов $i < j$ выполняется $(a_i, a_j) = 1$.*

Числа $6, 10, 15$ взаимно просты, но не являются попарно взаимно простыми, так как $(6, 10) = 2$. Более того имеем $(6, 15) = 3$, $(10, 15) = 5$.

Попарная взаимная простота означает, что для каждого простого $p$ среди чисел $a_1, \ldots, a_n$ не более, чем одно может делиться на $p$. Иначе это условие можно записать в виде

$$\max_{1\le j\le n} \nu_p(a_j) = \nu_p(a_1) + \ldots + \nu_p(a_n), \quad \textit{для любого простого} \quad p.$$

**Следствие 2.5.** *Наименьшее общее кратное попарно взаимно простых натуральных чисел $a_1, \ldots, a_n$ равно их произведению, т.е.*

$$[a_1, \ldots, a_n] = a_1 \cdots a_n.$$

*Доказательство.* Пусть $p$ – произвольное простое число. Тогда

$$\nu_p([a_1,\ldots,a_n]) = \max_{1\le j\le n} \nu_p(a_j) = \\ \nu_p(a_1)+\ldots+\nu_p(a_n) = \nu_p(a_1\cdots a_n).$$

Поскольку это верно для любого простого числа $p$, получаем требуемое равенство. □

**Следствие 2.6.** *Если число $b$ делится на каждое из попарно взаимно простых чисел $a_1,\ldots,a_n$, то $b$ делится и на их произведение $a_1\cdots a_n$.*

*Доказательство.* По теореме 1.2 число $b$ делится на наименьшее общее кратное $[a_1,\ldots,a_n]$, равное согласно следствию 2.5 произведению $a_1\cdots a_n$.

Можно дать этому утверждению и другое доказательство, основанное на свойствах показателей $\nu_p$. Поскольку при любом $j$ выполнено $a_j|b$, то для любого простого числа $p$ имеем $\nu_p(b)\ge\nu_p(a_j)$ и

$$\nu_p(b) \ge \max_{1\le j\le n} \nu_p(a_j) = \nu_p(a_1)+\ldots+\nu_p(a_n) = \nu_p(a_1\cdots a_n).$$

Поскольку это верно для любого простого числа $p$, заключаем, что $a_1\cdots a_n|b$. □

**Следствие 2.7.** *Для любых натуральных чисел $b,a_1,\ldots,a_n$ имеем*

$$(a_1\cdots a_n,b)\,|\,(a_1,b)\cdots(a_n,b).$$

*Если к тому же числа $a_1,\ldots,a_n$ попарно взаимно просты, то выполняется равенство*

$$(a_1\cdots a_n,b) = (a_1,b)\cdots(a_n,b). \tag{2.9}$$

*Доказательство.* Для любого простого числа $p$ имеем

$$\nu_p((a_1\cdots a_n,b)) = \min\{\nu_p(b),\nu_p(a_1\cdots a_n)\} = \\ = \min\{\nu_p(b)\,,\,\nu_p(a_1)+\ldots+\nu_p(a_n)\} \tag{2.10}$$

и

$$\nu_p((a_1, b) \cdots (a_n, b)) = \sum_{i=1}^{n} \min\{\nu_p(b), \nu_p(a_j)\}. \tag{2.11}$$

Первое утверждение следует теперь из неравенства

$$\min\{y, x_1 + \ldots + x_n\} \leq \sum_{i=1}^{n} \min\{y, x_i\} \tag{2.12}$$

справедливого при всех неотрицательных действительных числах $y, x_1, \ldots, x_n$. Для доказательства (2.12) рассмотрим два случая.

Если при всех индексах $i$ выполнены неравенства $x_i \leq y$, то имеем

$$\min\{y, x_1 + \ldots + x_n\} \leq x_1 + \ldots + x_n = \sum_{i=1}^{n} \min\{y, x_i\}.$$

Если же найдется индекс $j$, для которого $y < x_j$, то

$$\min\{y, x_1 + \ldots + x_n\} \leq y = \min\{y, x_j\} \leq \sum_{i=1}^{n} \min\{y, x_i\}.$$

Это доказывает первое утверждение следствия.

Предположим теперь, что числа $a_1, \ldots, a_n$ попарно взаимно просты. Пусть $p$ – произвольное простое число. Тогда среди чисел $\nu_p(a_j)$ не более одного отлично от нуля. Не уменьшая общности можно считать, что $\nu_p(a_2) = \ldots = \nu_p(a_n) = 0$. Тогда, пользуясь равенствами (2.11) и (2.10), находим

$$\begin{aligned}\nu_p((a_1, b) \cdots (a_n, b)) &= \min\{\nu_p(b), \nu_p(a_1)\} = \\ &= \min\{\nu_p(b)\,,\, \nu_p(a_1) + \ldots + \nu_p(a_n)\} = \nu_p((a_1 \cdots a_n, b)),\end{aligned}$$

и это завершает доказательство следствия. □

В дальнейшем нам понадобятся две функции: целая и дробная части числа. Напомним их определения и свойства.

*Целой частью* действительного числа $x$ называется наибольшее целое число $k$, удовлетворяющее неравенству $k \leq x$. Обозначается

эта функция $[x]$. Так, например, $[2,5] = 2, [\pi] = 3, [-1,3] = -2$. Из определения следует, что при любом $x$ справедливы неравенства $[x] \le x < [x]+1$. Складывая неравенства $[x] \le x$ и $[y] \le y$, получаем $[x] + [y] \le x + y$, и, согласно определению, находим

$$[x] + [y] \le [x + y].$$

Это неравенство справедливо и при любом количестве слагаемых, что легко доказать с помощью метода математической индукции.

Из определения сразу же следует, что для любого целого числа $n$ выполняется $[x + n] = [x] + n$.

При любом действительном $x$ и любом натуральном $a$ выполняется равенство

$$\left[\frac{[x]}{a}\right] = \left[\frac{x}{a}\right], \tag{2.13}$$

Чтобы пояснить его, обозначим $q = \left[\frac{x}{a}\right]$. Тогда $aq \le x < a(q + 1)$ и

$$aq \le [x] \le x < a(q + 1).$$

Разделив эти неравенства на $a$, получаем

$$q \le \frac{[x]}{a} < q + 1,$$

что и доказывает (2.13).

Функция $\{x\} = x - [x]$ называется *дробной частью* числа $x$. Она удовлетворяет неравенствам $0 \le \{x\} < 1$ и имеет период 1. Действительно, $\{x + 1\} = x + 1 - [x + 1] = x - [x] = \{x\}$. Например, $\{-1,3\} = \{0,3\} = 0,3$.

Рассмотрим два, имеющих теоретический интерес, примера, в которых вычисляются кратности вхождения простых в канонические разложения некоторых чисел. Обозначим для каждого действительного числа $x \ge 1$ символом $K(x)$ наименьшее общее кратное всех натуральных чисел, на превосходящих $x$.

**Лемма 2.2.** *Для любого действительного $x \geq 1$ имеем*

$$K(x) = \prod_{p \leq x} p^{\left[\frac{\ln x}{\ln p}\right]}.$$

*Доказательство.* Для каждого простого числа $p$ с помощью (2.7) имеем $\nu_p\big(K(x)\big) = \max_{1 \leq u \leq x} \nu_p(u)$. Если $k = \nu_p(u)$ для некоторого $u \leq x$, то $p^k | u$ и $p^k \leq u \leq x$. Значит, $k \leq \frac{\ln x}{\ln p}$. Но тогда $\nu_p(u) = k \leq \left[\frac{\ln x}{\ln p}\right]$. Из этой оценки и неравенства

$$p^{\left[\frac{\ln x}{\ln p}\right]} \leq p^{\frac{\ln x}{\ln p}} = x$$

следует, что

$$\max_{1 \leq u \leq x} \nu_p(u) = \left[\frac{\ln x}{\ln p}\right].$$

Кроме того, из приведённых рассуждений следует, что при $p > x$ выполняется $\nu_p\big(K(x)\big) = 0$, и это завершает доказательство леммы. □

Далее символом $n!$ обозначается произведение всех целых чисел от 1 до $n$, т.е. $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

**Лемма 2.3.** *Для каждого натурального числа $n$ имеем*

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{k \geq 1} \left[\frac{n}{p^k}\right]. \tag{2.14}$$

Сумма в действительности конечна, так как при $p^k > n$, т.е. при $k > \frac{\ln n}{\ln p}$ слагаемые равны нулю.

*Доказательство.* Среди чисел $1, 2, \ldots n$ на простое $p$ делятся лишь $p, 2p, 3p, \ldots mp$, где $m$ есть наибольшее целое число, удовлетворяющее неравенству $mp \leq n$, т.е. $m = \left[\frac{n}{p}\right]$. Поэтому

$$\nu_p(n!) = \nu_p(p \cdot 2p \cdots mp) = \nu_p(p^m \cdot m!) = m + \nu_p(m!). \tag{2.15}$$

Получившееся равенство позволяет доказать нужную формулу с помощью метода математической индукции.

При $n < p$ обе части равенства (2.14) равны нулю, и оно, конечно, выполняется. Предположим теперь, что $n \geq p$ и это равенство справедливо для любого натурального числа, меньшего $n$. Тогда из (2.15) и (2.13), поскольку $m < n$, находим

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \sum_{\ell \geq 1} \left[\frac{m}{p^\ell}\right] = \left[\frac{n}{p}\right] + \sum_{\ell \geq 1} \left[\frac{\left[\frac{n}{p}\right]}{p^\ell}\right] = \left[\frac{n}{p}\right] + \sum_{\ell \geq 1} \left[\frac{n}{p^{\ell+1}}\right],$$

что и завершает доказательство. □

Как ещё один пример рассмотрим дробь

$$N = \frac{n!}{a_1! \cdot \ldots \cdot a_r!},$$

где $n, a_1, \ldots, a_r$ натуральные числа с условием $a_1 + \ldots + a_r = n$. Докажем, что эта дробь есть целое число.

Пользуясь леммой 2.3 можно написать

$$\nu_p(N) = \sum_{k \geq 1} \left( \left[\frac{n}{p^k}\right] - \left[\frac{a_1}{p^k}\right] - \ldots - \left[\frac{a_r}{p^k}\right] \right) \geq 0.$$

Последнее неравенство выполняется в силу того, что при любом $k$ справедливо

$$\left[\frac{a_1}{p^k}\right] + \ldots + \left[\frac{a_r}{p^k}\right] \leq \left[\frac{a_1 + \ldots + a_r}{p^k}\right] = \left[\frac{n}{p^k}\right].$$

Итак, число $N$ раскладывается в произведение неотрицательных степеней простых чисел, и потому есть целое число.

## 2.3 Теоремы Чебышева

Простые числа распределены в натуральном ряду весьма нерегулярно. Например, можно указать сколь угодно длинные отрезки натурального ряда, не содержащие ни одного простого числа. Выберем с

этой целью некоторое натуральное $n$ и рассмотрим следующие друг за другом числа

$$n! + 2, n! + 3, n! + 4, \ldots, n! + n.$$

Первое из них делится на 2, второе на 3, третье на 4 и так далее. Последнее число делится на $n$. Указанный отрезок натурального ряда не содержит ни одного простого числа. Такие отрезки расположены достаточно далеко в натуральном ряду. Скажем, максимальное расстояние между любыми соседними простыми числами, меньшими $10^{15}$ равно 276.

Вместе с тем существуют сгущения простых чисел. Так как чётные числа, большие 2, делятся на 2, то минимальное расстояние между соседними простыми числами не меньше двух. Простые числа, расположенные на расстоянии 2 друг от друга, называются *близнецами*. Таким образом, любая пара близнецов состоит из нечётных простых чисел $p$ и $p + 2$. Известны достаточно большие примеры близнецов, скажем простыми будут числа

$$156 \cdot 5^{202} \pm 1, \qquad 291 \cdot 2^{1553} \pm 1.$$

Предполагается, что множество таких пар бесконечно, однако этот факт не доказан. С помощью компьютера можно построить достаточно большие пары простых чисел $p, q$, связанных, например, соотношением $p = 2q + 1$ и предполагается, что любое уравнение $ax - by = c$ с натуральными и попарно взаимно простыми коэффициентами имеет бесконечное количество решений в простых числах $p, q$. Но эта проблема не решена и относится к очень трудным.

Несмотря на большие сложности исследования свойств простых чисел, удаётся определить некоторые усреднённые их характеристики. Одной из них является функция $\pi(x)$, равная количеству простых чисел $p$, с условием $p \leq x$. Имеется лишь четыре простых числа, удовлетворяющих неравенству $p \leq 10$. Это $2, 3, 5, 7$. Поэтому $\pi(10) = 4$. Решето Эратосфена позволяет определить, что $\pi(100) = 25$. Известно, что $\pi\left(10^{12}\right) = 37607912018$.

Ясно, что с ростом $x$ функция $\pi(x)$ возрастает. А из теоремы 2.1 следует, что она возрастает до бесконечности, т.е. $\pi(x) \to \infty$.

С помощью решета Эратосфена можно получить и некоторую оценку сверху для функции $\pi(x)$. Для простейшей оценки исключим из множества чисел $2, 3, \ldots, N$, $N \geq 3$, все четные числа. Количество их в этом множестве равно $\left[\frac{N}{2}\right]$. Среди чётных имеется только одно простое число 2. Поэтому

$$\pi(N) \leq N - 1 - \left[\frac{N}{2}\right] + 1 = N - \left[\frac{N}{2}\right] \leq \frac{N+1}{2} \leq \frac{2N}{3}. \qquad (2.16)$$

При $N = 1, 2$ оценка $\pi(N) \leq \frac{2N}{3}$ также справедлива, ведь $\pi(1) = 0$, а $\pi(2) = 1$.

Если использовать для просеивания два простых числа $2, 3$, т.е. исключить все числа, делящиеся на 2 или 3, кроме самих этих чисел, можно таким же способом получить неравенство

$$\pi(N) \leq N - \left[\frac{N}{2}\right] - \left[\frac{N}{3}\right] + \left[\frac{N}{6}\right] + 1 \leq \frac{N+5}{3}.$$

Для произвольного действительного $x \geq 1$ имеем

$$\pi(x) = \pi\big([x]\big) \leq \frac{[x]+5}{3} \leq \frac{x+5}{3}.$$

Отсеивая также числа, делящиеся на $5, 7$ и так далее, можно доказать, что доля простых среди натуральных чисел $n \leq x$ с ростом границы $x$ стремится к нулю, т.е. $\pi(x)/x \to 0$. Этот факт был доказан в 1798г. А. Лежандром[3].

Впервые достаточно точные границы изменения функции $\pi(x)$ были установлены в 1850г. П.Л. Чебышевым[4].

**Теорема 2.3.** *При всех $x \geq 6$ справедливы неравенства*

$$a\frac{x}{\ln x} \leq \pi(x) \leq b\frac{x}{\ln x}, \qquad (2.17)$$

*где $a = \frac{1}{2}\ln 2$, $b = 5\ln 2$.*

[3] Французский математик Антуан Лежандр, 1752-1833

[4] Русский математик Пафнутий Львович Чебышев, 1821-1894

Неравенства (2.17) были доказаны П.Л. Чебышевым с лучшими константами $a = 0,921\ldots, b = 1,105\ldots$, но при достаточно больших $x$. Мы несколько ослабили его результат, упростив при этом вычисления. Заметим также, что в настоящее время известны намного более точные неравенства

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

Для доказательства теоремы 2.3 понадобятся две леммы.

**Лемма 2.4.** *При любом натуральном $n$ наименьшее общее кратное чисел $1, 2, \ldots, 2n+1$ больше, чем $4^n$, т.е.*

$$[1, 2, 3, \ldots, 2n+1] > 4^n.$$

*Доказательство.* Рассмотрим рациональную функцию

$$R_n(x) = \frac{n!}{x(x+1)\cdots(x+n)}.$$

Она может быть представлена в виде суммы простейших дробей

$$\frac{n!}{x(x+1)\cdots(x+n)} = \frac{a_0}{x} + \frac{a_1}{x+1} + \frac{a_2}{x+2} + \cdots + \frac{a_n}{x+n} \qquad (2.18)$$

с целыми коэффициентами $a_k$. Например,

$$R_1(x) = \frac{1}{x(x+1)} = \frac{1}{x} - \frac{1}{x+1},$$

$$R_2(x) = \frac{1}{x(x+1)} - \frac{1}{(x+1)(x+2)} = \frac{1}{x} - \frac{2}{x+1} + \frac{1}{x+2}.$$

В общем случае имеем тождество

$$\begin{aligned} R_n(x) &= \frac{(n-1)!}{x(x+1)\cdots(x+n-1)} - \frac{(n-1)!}{(x+1)(x+2)\cdots(x+n)} \\ &= R_{n-1}(x) - R_{n-1}(x+1), \end{aligned}$$

доказывающее целость коэффициентов в (2.18) с помощью метода математической индукции.

Подставим $x = n + 1$ в тождество (3.14). В результате получится

$$I = \frac{a_0}{n+1} + \frac{a_1}{n+2} + \cdots + \frac{a_n}{2n+1} = \\ = \frac{n!}{(n+1)\cdots(2n+1)} = \frac{n!n!}{(2n+1)!}. \quad (2.19)$$

Обозначим для краткости $K = [1, 2, 3, \ldots, 2n+1]$. Поскольку коэффициенты $a_k$ – целые числа, то $K \cdot I \in \mathbb{Z}$. Учитывая, что $K \cdot I > 0$, заключаем $K \cdot I \geq 1$, так что

$$K \geq I^{-1} = \frac{(2n+1)!}{n!n!}.$$

Докажем с помощью метода математической индукции неравенство

$$\frac{(2n+1)!}{n!n!} > 4^n.$$

При $n = 1$ оно, очевидно, выполняется. Предположив его справедливость для $n-1$, при $n \geq 2$ имеем

$$\frac{(2n+1)!}{n!n!} = \frac{(2n+1)2n}{n^2} \cdot \frac{(2n-1)!}{(n-1)!(n-1)!} > 4 \cdot 4^{n-1} = 4^n.$$

Это завершает доказательство леммы. □

**Лемма 2.5.** *При каждом действительном $x \geq 2$ справедливо неравенство*

$$\prod_{p \leq x} p < 4^x.$$

*Доказательство.* Докажем сначала утверждение для целых значений $x$, воспользовавшись методом математической индукции. При $x = 2$ неравенство, очевидно, выполняется. Пусть $n \geq 3$ и для всех целых $x < n$ неравенство леммы справедливо. Рассмотрим далее два случая.

1. Предположим, что $n = 2m$ чётно. Учитывая, что $n = 2m$ составное число и пользуясь индуктивным предположение для $x = 2m - 1$, находим

$$\prod_{p \le n} p = \prod_{p \le 2m-1} p < 4^{2m-1} < 4^n.$$

В этом случае нужное неравенство доказано.

2. Если $n = 2m - 1$ нечетное число, то $m \ge 2$. Применяя индуктивное предположение для $x = m$, имеем

$$\prod_{p \le n} p = \prod_{p \le m} p \cdot \prod_{m < p \le 2m-1} p < 4^m \cdot \prod_{m < p \le 2m-1} p. \tag{2.20}$$

Чтобы оценить последнее произведение рассмотрим биномиальный коэффициент

$$\binom{2m-1}{m} = \frac{(2m-1)!}{m!(m-1)!},$$

являющийся целым числом. Справедливо равенство

$$(2m-1)! = \binom{2m-1}{m} \cdot m! \cdot (m-1)! \tag{2.21}$$

Пусть $p$ – какое-нибудь простое число, удовлетворяющее неравенствам $m < p \le 2m - 1$. Левая часть (2.21) делится на $p$. Из неравенства $p > m$, простоты $p$ и основной теоремы арифметики следует, что $p$ не может входить в разложения на простые сомножители числа $m! \cdot (m-1)!$ и, значит, $p$ входит в разложение $\binom{2m-1}{m}$. Таким образом, все простые числа $p$ из промежутка $m < p \le 2m-1$ входят в разложение этого биномиального коэффициента. Следовательно

$$\prod_{m < p \le 2m-1} p \le \binom{2m-1}{m}. \tag{2.22}$$

Докажем с помощью метода математической индукции, что при любом целом $k \ge 1$ справедливо неравенство $\binom{2k-1}{k} \le 4^{k-1}$. При $k = 1$

это неравенство, очевидно, выполняется. Если оно верно для $k-1$ при $k \geq 2$, то имеем

$$\binom{2k-1}{k} = \frac{(2k-1)!}{k!(k-1)!} = \frac{2(2k-1)}{k} \cdot \frac{(2k-3)!}{(k-1)!(k-2)!} \leq 4 \cdot 4^{k-2} = 4^{k-1}.$$

Из (2.20) и (2.22), применяя доказанное неравенство с $k = m$, находим

$$\prod_{p \leq n} p < 4^m \cdot \binom{2m-1}{m} \leq 4^m \cdot 4^{m-1} = 4^n.$$

Итак, неравенство леммы 2.5 при любом целом $x$ доказано.

Если же $x$ не целое число, то находим

$$\prod_{p \leq x} p = \prod_{p \leq [x]} p < 4^{[x]} \leq 4^x.$$

Здесь $[x]$ – целая часть числа $x$. Это завершает доказательство леммы. □

*Доказательство теоремы 2.3.* Пусть $x \geq 6$ – произвольное действительное число.

Докажем сначала левое неравенство (2.17). Определим для этого целое число $n$ неравенствами

$$2n+1 \leq x < 2n+3. \tag{2.23}$$

Из лемм 2.4 и 2.2 находим

$$4^n < K(2n+1) = \prod_{p \leq 2n+1} p^{\left[\frac{\ln(2n+1)}{\ln p}\right]} \leq \prod_{p \leq 2n+1} p^{\frac{\ln(2n+1)}{\ln p}} = (2n+1)^{\pi(2n+1)}.$$

Если прологарифмировать это неравенство по основанию 2, получится $\pi(2n+1) > \frac{2n}{\log_2(2n+1)}$. Отсюда, учитывая неравенства (2.23) и монотонность функции $\pi(x)$, получаем

$$\pi(x) \geq \pi(2n+1) > \frac{x-3}{\log_2 x} \geq \frac{1}{2} \cdot \frac{x}{\log_2 x}.$$

Это доказывает левое неравенство (2.17) с $a = \frac{1}{2}\ln 2$.

Перейдём теперь к доказательству правого неравенства (2.17). Справедлива оценка

$$\pi(x) = \sum_{p\le x} 1 = \pi\bigl(x^{2/3}\bigr) + \sum_{x^{2/3}<p\le x} 1 \le \pi\bigl([x^{2/3}]\bigr) + \sum_{x^{2/3}<p\le x} \frac{\log_2 p}{\log_2 x^{2/3}}.$$

Пользуясь (2.16) и неравенством $\sum_{p\le x}\log_2 p \le 2x$, следующим из леммы 2.5, находим

$$\pi(x) \le \frac{2}{3}x^{2/3} + \frac{2x}{\log_2 x^{2/3}} = \frac{2}{3}x^{2/3} + \frac{3x}{\log_2 x}.$$

Как известно, при любом действительном $t > 0$ справедливо неравенство $t \ge \log_2 t$. Взяв здесь $t = x^{1/3}$, находим $x^{2/3} \le 3\frac{x}{\log_2 x}$. И тогда

$$\pi(x) \le 2\frac{x}{\log_2 x} + 3\frac{x}{\log_2 x} = 5\frac{x}{\log_2 x}\,,$$

что завершает доказательство теоремы 2.3. □

**Следствие 2.8.** *Если $2 = p_1 < p_2 < p_3 < \ldots$ последовательность всех простых чисел, то с некоторыми положительными постоянными $\alpha, \beta$ выполняются неравенства*

$$\alpha n\ln n \le p_n \le \beta n\ln n.$$

*Доказательство.* При каждом натуральном $n$ имеем $\pi(p_n) = n$. Подставив $x = p_n$ в неравенства теоремы 2.3, получим при $n \ge 4$

$$a\frac{p_n}{\ln p_n} \le n \le b\frac{p_n}{\ln p_n}.$$

Эти неравенства можно переписать в виде

$$n = c_n\cdot\frac{p_n}{\ln p_n}, \qquad a \le c_n \le b.$$

Из последнего равенства следует

$$\ln n = \ln p_n - \ln\ln p_n + \ln c_n$$

и, значит,

$$\frac{n\ln n}{p_n} = c_n\left(1 - \frac{\ln\ln p_n}{\ln p_n} + \frac{\ln c_n}{\ln p_n}\right).$$

Учитывая, что выражение в скобках с ростом $n$ стремится к единице, в силу неравенств $a \le c_n \le b$, заключаем, что последовательность $\frac{n\ln n}{p_n}$ ограничена снизу и сверху некоторыми положительными постоянными. Это значит, что с некоторыми положительными постоянными $\alpha, \beta$ выполняются неравенства

$$\frac{1}{\beta} \le \frac{n\ln n}{p_n} \le \frac{1}{\alpha},$$

а, значит, и $\alpha n\ln n \le p_n \le \beta n\ln n$. □

Следующее утверждение впервые было доказано Л. Эйлером.

**Следствие 2.9.** *Ряд $\sum_p \frac{1}{p}$, где суммирование происходит по всем простым числам, расходится.*

*Доказательство.* В силу неравенств следствия 2.8 ряды $\sum_{n=2}^{\infty}\frac{1}{n\ln n}$ и $\sum_p \frac{1}{p} = \sum_{n=1}^{\infty}\frac{1}{p_n}$ сходятся или расходятся одновременно.

При всех $t > 0$ справедливо неравенство $\ln(1+t) \le t$. Поэтому для любого целого $n \ge 2$ имеем

$$\ln\ln(n+1) - \ln\ln n = \ln\left(\frac{\ln(n+1)}{\ln n}\right) \le \frac{\ln(n+1)}{\ln n} - 1 = \\ = \frac{1}{\ln n}\cdot\ln\left(1+\frac{1}{n}\right) \le \frac{1}{n\ln n}.$$

Складывая эти неравенства при всех $n = 2, 3, \ldots, N$, находим

$$\sum_{n=2}^{N}\frac{1}{n\ln n} \ge \ln\ln(N+1) - \ln\ln 2 \ge \ln\ln(N+1).$$

Полученная оценка доказывает неограниченность частичных сумм ряда $\sum_{n=2}^{\infty}\frac{1}{n\ln n}$, и тем самым расходимость ряда из чисел, обратных простым. □

В следующем утверждении, носящем название "постулат Бертрана", по-существу содержится оценка сверху расстояния между двумя соседними простыми числами $p_k$ и $p_{k+1}$. Оно, в частности, утверждает, что $p_{k+1} < 2p_k$. Эта, и даже более сильная, теорема впервые была доказана в 1852г. П.Л. Чебышевым.

**Теорема 2.4.** *Для любого натурального $n \geq 2$ существует простое число $p$, удовлетворяющее неравенствам $n < p < 2n$.*

*Доказательство.* Докажем сначала, что утверждение теоремы верно для любого $n \leq 600$. Рассмотрим для этого последовательность простых чисел

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631.$$

Каждое из них меньше удвоенного предыдущего. Пусть $n$ – произвольное целое число из промежутка $2 \leq n \leq 600$. Тогда $n$ содержится между двумя последовательными простыми $q, p$ из выписанного ряда, т.е. $q \leq n < p$. Учитывая, что $p < 2q$, заключаем $p < 2q \leq 2n$. Искомое простое число $p$ найдено.

Поскольку теорема доказана для всех чисел $n \leq 600$, далее будем предполагать выполненным неравенство $n > 600$. Рассмотрим целое число

$$N = \frac{(2n+1)!}{n!n!} = \prod_{p \leq 2n+1} p^{\nu_p(N)}.$$

В доказательстве леммы 2.4 было установлено, что

$$N | K = [1, 2, \ldots, 2n+1] \qquad \text{и} \qquad N > 4^n. \tag{2.24}$$

Докажем справедливость неравенства

$$N \leq (2n+1) \prod_{p \leq 2n-1} p^{\nu_p(N)}. \tag{2.25}$$

Если $2n+1$ простое число, то $\nu_{2n+1}(N) = 1$ и в (2.25) имеет место равенство. Если же $2n+1$ – составное, то $N = \prod_{p \leq 2n-1} p^{\nu_p(N)}$ и (2.25) также выполняется.

Предположим, что утверждение теоремы неверно и интервал $n < x < 2n$ не содержит ни одного простого числа. Тогда из (2.25) следует

$$N \le (2n+1) \prod_{p \le n} p^{\nu_p(N)}. \tag{2.26}$$

Если простое число $p$ удовлетворяет неравенствам $\frac{2n+1}{3} < p \le n$, то $p \le n < \frac{3p-1}{2} < 2p$ и $2p < 2n+1 < 3p$. Значит, $\nu_p(n!) = 1$ и $\nu_p((2n+1)!) = 2$. Таким образом, $\nu_p(N) = \nu_p((2n+1)!) - 2\nu_p(n!) = 0$ и из (2.26) следует

$$N \le (2n+1) \prod_{p \le \frac{2n+1}{3}} p^{\nu_p(N)}. \tag{2.27}$$

Предположим теперь, что $\sqrt{2n+1} < p \le \frac{2n+1}{3}$. Тогда, в частности, $\ln(2n+1) < 2\ln p$. Поскольку $N|K$, то из леммы 2.2 следует $\nu_p(N) \le \nu_p(K) = \left[\frac{\ln(2n+1)}{\ln p}\right] \le 1$. Но тогда из (2.27) находим

$$\begin{aligned} N &\le (2n+1) \cdot \prod_{\sqrt{2n+1} < p \le \frac{2n+1}{3}} p \cdot \prod_{p \le \sqrt{2n+1}} p^{\nu_p(N)} \le \\ &\le \frac{2n+1}{2} \cdot \prod_{p \le \frac{2n+1}{3}} p \cdot \prod_{p \le \sqrt{2n+1}} p^{\nu_p(N)}. \end{aligned} \tag{2.28}$$

Так как $N|K$, то по лемме 2.2 имеем

$$\nu_p(N) \le \nu_p(K) = \left[\frac{\ln(2n+1)}{\ln p}\right] \le \frac{\ln(2n+1)}{\ln p}.$$

Но тогда правое неравенство теоремы 2.3 даёт

$$\prod_{p \le \sqrt{2n+1}} p^{\nu_p(N)} \le (2n+1)^{\pi(\sqrt{2n+1})} \le (2n+1)^{\frac{5\sqrt{2n+1}}{\log_2 \sqrt{2n+1}}} = 4^{5\sqrt{2n+1}}.$$

Воспользовавшись оценкой снизу (2.24) для числа $N$, а также леммой 2.5, из (2.28) находим

$$4^n < N < \frac{2n+1}{2} \cdot 4^{\frac{2n+1}{3}} \cdot 4^{5\sqrt{2n+1}}. \tag{2.29}$$

Легко проверить, что функция $f(x) = x^2 \cdot 2^{-x}$ монотонно убывает на множестве $x \geq 4$. Поскольку $f(4) = 1$, то при любом $x \geq 4$ выполняется неравенство $x^2 \leq 2^x$. В частности, при $x = \sqrt{2n+1}$ находим $2n+1 \leq 2^{\sqrt{2n+1}}$. Теперь из неравенства (2.29) следует

$$2^{2n+1} < 2^{\sqrt{2n+1}} \cdot 4^{\frac{2n+1}{3}} \cdot 4^{5\sqrt{2n+1}}$$

и

$$2n+1 < \frac{2}{3}(2n+1) + 11\sqrt{2n+1}.$$

Из последнего неравенства находим $n < 544$, вопреки условию $n > 600$. Получившееся противоречие доказывает существование простого числа, утверждаемого леммой. □

## 2.4 Дзета-функция Римана и свойства простых чисел

Дзета-функция определяется рядом

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2.30}$$

По историческим причинам её аргумент принято обозначать буквой $s$. Как известно из курсов математического анализа, ряд (2.30) сходится при каждом действительном $s > 1$ и расходится при $s \leq 1$. Такие ряды при различных значениях $s$ изучал Эйлер. Впоследствии дзета-функция стала рассматриваться, как функция действительного переменного $s > 1$. Её свойства тесно связаны со свойствами множества простых чисел, что позволяет использовать для исследования простых чисел методы теории функций. Следующее утверждение называется *тождеством Эйлера*.

**Теорема 2.5.** *При каждом $s > 1$ справедливо тождество*

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{2.31}$$

Правая часть тождества (2.31) содержит бесконечное количество сомножителей. Под таким бесконечным произведением понимается предел конечного произведения

$$P(x) = \prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1}$$

при $x$, стремящемся к бесконечности.

*Доказательство.* Пользуясь формулой для суммы членов бесконечно убывающей геометрической прогрессии, находим

$$\left(1 - \frac{1}{p^s}\right)^{-1} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots. \tag{2.32}$$

Это равенство справедливо при любом простом $p$ и любом $s > 1$.

Выберем некоторое число $x > 2$ и пусть $2 = p_1 < p_2 < \ldots < p_r$ все простые числа, не превосходящие $x$. Перемножим равенства (2.32) для всех простых чисел $p \le x$. В результате получится

$$P(x) = \prod_{j=1}^{r} \left(1 - \frac{1}{p_j^s}\right)^{-1} = \sum_{k_1,\ldots,k_r} \frac{1}{p_1^{k_1 s} \cdot \ldots \cdot p_r^{k_r s}}, \tag{2.33}$$

где справа стоит бесконечная сумма, в которой показатели $k_1, \ldots, k_r$ независимо пробегают множество всех целых неотрицательных чисел. Слагаемые в рядах (2.32) положительны, поэтому согласно теореме о перемножении рядов, равенство (2.33) будет выполняться как бы мы ни упорядочивали слагаемые в его правой части. Упорядочим их по возрастанию знаменателей.

Среди этих знаменателей нет одинаковых, ведь по основной теореме арифметики равенство

$$p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} = p_1^{\ell_1} \cdot \ldots \cdot p_r^{\ell_r}$$

выполняется лишь в случае $k_1 = \ell_1, \ldots k_r = \ell_r$. Поэтому (2.33) можно переписать в виде

$$P(x) = \sum_{k_1,\ldots,k_r} \frac{1}{(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^s} = {\sum_{n \ge 1}}' \frac{1}{n^s}, \tag{2.34}$$

где знак $'$ обозначает, что суммирование происходит по всем натуральным числам, раскладывающимся в произведение простых $p \leq x$. По основной теореме арифметики каждое натуральное число $n$ раскладывается в произведение простых. Ясно также, что в случае $n \leq x$ эти простые не превосходят $x$. Поэтому равенство (2.34) можно переписать в виде

$$P(x) = \sum_{n \leq x} \frac{1}{n^s} + {\sum_{n>x}}' \frac{1}{n^s}. \tag{2.35}$$

Преобразуя его, находим

$$0 < P(x) - \sum_{n \leq x} \frac{1}{n^s} = {\sum_{n>x}}' \frac{1}{n^s} \leq \sum_{n>x} \frac{1}{n^s}. \tag{2.36}$$

Второе неравенство (2.36) выполняется в силу того, что в его правой части суммирование происходит по большему множеству натуральных чисел, а сами слагаемые положительны. Правая часть (2.36) стремится к нулю с ростом $x$, ведь эта сумма есть остаток сходящегося ряда (2.30). Но тогда

$$\lim_{x \to \infty} P(x) = \lim_{x \to \infty} \sum_{n \leq x} \frac{1}{n^s} = \zeta(s).$$

Тождество Эйлера доказано. □

Прежде, чем выводить следствия этого тождества, мы докажем одно вспомогательное утверждение. Оно будет использоваться и в дальнейшем. Поэтому докажем его в несколько большей общности, чем это потребуется здесь.

**Лемма 2.6.** *1. При любом натуральном $N$ справедливы неравенства*

$$\ln(N+1) < \sum_{n=1}^{N} \frac{1}{n} < \ln(2N+1).$$

*2. Существует предел*

$$\lim_{x\to+\infty}\left(\sum_{n\le x}\frac{1}{n}-\ln x\right)=\gamma>0.$$

Численное значение предела равно $\gamma = 0,5772156649\ldots$. Эта математическая константа, такая же как $\pi$ или $e$, носит название постоянной Эйлера. В отличие от двух последних констант, арифметические свойства постоянной Эйлера пока не поддаются исследованиям. Предполагается, что $\gamma$ иррациональна, но это в настоящее время не доказано.

*Доказательство леммы 2.6.* При любом действительном $t > 0$ справедливо неравенство $\ln(1+t) < t$, легко доказываемое, например, с использованием дифференцирования. С его помощью при $t = 1/n$, где $n$ – произвольное натуральное число, находим

$$\ln(n+1)-\ln n=\ln\left(1+\frac{1}{n}\right)<\frac{1}{n}. \tag{2.37}$$

Просуммировав эти неравенства для всех целых $n$ из промежутка $1 \le n \le N$, найдём

$$\sum_{n=1}^{N}\frac{1}{n}>\sum_{n=1}^{N}(\ln(n+1)-\ln n)=\ln(N+1).$$

Точно так же легко проверить, что при любом $t$ из интервала $0 < t < 1$ справедливо

$$\ln(1+t)-\ln(1-t)>2t.$$

Поставляя в это неравенство $t = \frac{1}{2n}$, находим

$$\frac{1}{n}<\ln(2n+1)-\ln(2n-1).$$

Складывая эти неравенства для $n = 1, \ldots, N$ получаем

$$\sum_{n=1}^{N}\frac{1}{n}<\sum_{n=1}^{N}(\ln(2n+1)-\ln(2n-1))=\ln(2N+1).$$

Это завершает доказательство первого утверждения леммы.

Для доказательства второго утверждения обозначим

$$s_N = \sum_{n=1}^{N} \frac{1}{n} - \ln(N+1).$$

С помощью неравенства (2.37) при $N > 1$ получаем

$$s_N - s_{N-1} = \frac{1}{N} - \ln(N+1) + \ln N > 0,$$

т.е. $s_N$ возрастающая последовательность. В то же время из первого утверждения леммы следует неравенство

$$s_N < \ln(2N+1) - \ln(N+1) < \ln 2,$$

так что последовательность $s_N$ ограничена. Как известно, доказанные свойства означают существование предела

$$\gamma = \lim_{N\to\infty} \left( \sum_{n=1}^{N} \frac{1}{n} - \ln(N+1) \right).$$

При любом $N \geq 1$ имеем $s_N \geq s_1 = 1 - \ln 2$. Поэтому $\gamma \geq 1 - \ln 2 > 0$.

Пусть $x > 1$ – действительное число. Тогда

$$\sum_{n\leq x} \frac{1}{n} - \ln x = s_{[x]} + \ln([x]+1) - \ln x = s_{[x]} + \ln\left(1 + \frac{1-\{x\}}{x}\right).$$

С ростом $x$ первое слагаемое в правой части получившегося выражения стремится к $\gamma$, а второе стремится к нулю. Лемма доказана полностью. □

Перейдем теперь к выводу следствий из тождества Эйлера.

**Следствие 2.10.** *При любом $x \geq 2$ справедливо неравенство*

$$\prod_{p\leq x} \left(1 - \frac{1}{p}\right)^{-1} > \ln x.$$

Заметим, что из этого неравенства следует бесконечность множества простых чисел. Ведь, если множество простых конечно, то функция, стоящая в левой части неравенства постоянна при всех достаточно больших $x$, но правая часть этого неравенства стремится к бесконечности.

*Доказательство.* Из (2.35) следует неравенство

$$\prod_{p\le x}\left(1-\frac{1}{p^s}\right)^{-1} > \sum_{n\le x}\frac{1}{n^s},$$

справедливое при любом $s>1$. Переходя в нём к пределу при $s\to 1$ и пользуясь первым утверждением леммы 2.6, находим

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} \ge \sum_{n\le x}\frac{1}{n} = \sum_{n\le [x]}\frac{1}{n} > \ln([x]+1) > \ln x.$$

□

В предыдущем параграфе была доказана расходимость ряда из чисел вида $1/p$, где $p$ - простое число. Докажем несколько более точное утверждение.

**Следствие 2.11.** *При любом $x\ge 2$ справедливо неравенство*

$$\sum_{p\le x}\frac{1}{p} > \ln\ln x - 1.$$

*Доказательство.* Из неравенства $\ln(1+t)\le t$ при $t=1/(p-1)$ следует

$$\ln\left(1-\frac{1}{p}\right)^{-1} = \ln\left(1+\frac{1}{p-1}\right) \le \frac{1}{p-1}.$$

Суммируя эти неравенства при всех простых $p\le x$, находим

$$\ln\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} \le \sum_{p\le x}\frac{1}{p-1} = \sum_{p\le x}\frac{1}{p} + \sum_{p\le x}\left(\frac{1}{p-1}-\frac{1}{p}\right) \le$$

$$\le \sum_{p\le x}\frac{1}{p} + \sum_{n=2}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right) = \sum_{p\le x}\frac{1}{p} + 1.$$

Применяя к левой части оценку из следствия 2.10, получаем требуемое неравенство. □

Эйлер также нашел формулы, связывающие значения дзета - функции в чётных положительных точках с числом $\pi$. Например,

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945}\,.$$

Для значений в нечётных точках подобные соотношения неизвестны. Предполагается, что они не существуют.

Несмотря на то, что ряд (2.30) расходится при $s < 1$, дзета-функцию можно определить и при таких значениях аргумента. Например, при $s > 1$ справедливо тождество

$$(1 - 2^{1-s})\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} - 2\sum_{n=1}^{\infty} \frac{1}{(2n)^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \dots.$$

Последний ряд, как известно, сходится при $s > 0$. Поскольку множитель $1 - 2^{1-s}$ отличен от нуля на множестве $0 < s < 1$, это равенство можно рассматривать как определение дзета-функции в интервале $0 < s < 1$.

В 1859г. Б. Риман[5] определил дзета-функцию при любом комплексном значении $s$ и установил ряд её глубоких свойств. Он также первым использовал обозначение $\zeta(s)$ для функции (2.30), 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 $s = -2, -4, -6, \dots$, а, кроме того, как предположил Риман, имеет бесконечное количество нулей в полосе $0 \le \sigma \le 1$, расположенных симметрично относительно прямой $\sigma = 1/2$ и вещественной

[5] Бернхард Риман, 1826-1866, – немецкий математик, оказавший существенное влияние на развитие теории аналитических функций, геометрии и теории чисел.

оси (этот факт был доказан в 1893г. Ж. Адамаром[6]). Риман высказал без доказательства и приближённую формулу[7] для количества таких нулей в прямоугольнике $0 \le \sigma \le 1, 0 \le t \le T$. Он также предположил, что все нули $\zeta(s)$ в полосе $0 \le \sigma \le 1$ 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[8] установили точный порядок роста функции $\pi(x)$, доказав в 1896г., что

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{при} \quad x \to \infty \quad \text{т.е.} \quad \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1. \tag{2.38}$$

Это утверждение называется *асимптотический закон распределения простых чисел.* Если $\psi(x)$ – натуральный логарифм наименьшего общего кратного всех целых чисел $n$, удовлетворяющих неравенствам $2 \le n \le x$ и $\theta(x) = \sum_{p\le x} \ln p$, то каждая из асимптотических формул

$$\psi(x) \sim x, \qquad \theta(x) \sim x, \qquad \text{при} \quad x \to \infty$$

эквивалентна равенству (2.38).

Валле-Пуссен дал и оценку точности, с которой функция $x/\ln x$ приближает $\pi(x)$. Важную роль в доказательстве сыграло утверждение об отсутствии нулей дзета-функции Римана в некоторой области полосы $0 \le \sigma \le 1$. При этом выяснилось, что для всех достаточно больших $x$ функция $\pi(x)$ лучше приближается интегралом

$$\int_2^x \frac{du}{\ln u},$$

чем отношением $x/\ln x$. Из справедливости недоказанной гипотезы

[6] Жак Адамар, 1865-1963, – французский математик.

[7] Её доказал в 1895г. немецкий математик Ханс фон Мангольдт, 1854-1925.

[8] Шарль Жан де ла Валле-Пуссен, 1866-1962, французский математик.

Римана можно вывести оценку

$$\left|\pi(x) - \int_2^x \frac{du}{\ln u}\right| \leq c\sqrt{x}\ln x,$$

где $c$ – некоторая положительная постоянная.

Наконец, приведём одно элементарное утверждение, эквивалентное гипотезе Римана. Пусть $N$ – натуральное число. Расположим все дроби $a/b$ с условиями

$$0 < a \leq b, \qquad (a,b) = 1, \qquad b \leq N,$$

в порядке возрастания, и обозначим их $r_k, 1 \leq k \leq M$. Такая последовательность называется *рядом Фарея порядка* $N$. Ясно, что количество дробей $M$ в ряде Фарея зависит от $N$. Для справедливости гипотезы Римана необходимо и достаточно, чтобы при каждом $\varepsilon > 0$ существовала, зависящая только от $\varepsilon$, постоянная $C$, при которой для всех $N \geq 1$ выполняется оценка

$$\sum_{k=1}^{M} \left|r_k - \frac{k}{M}\right| \leq CN^{1/2+\varepsilon}.$$

Это неравенство означает, что дроби ряда Фарея не должны слишком сильно отклоняться от соответствующих дробей, полученных делением отрезка $[0;1]$ на $M$ равных частей.

# Глава 3

# Арифметические функции

В теории чисел встречается множество функций. Арифметическими принято называть вообще говоря комплексно значные функции, определённые на множестве натуральных чисел. Свойства некоторых, наиболее важных из них, мы обсудим в этой главе.

## 3.1 Мультипликативные функции и их свойства

Функция $\theta(n)$, определенная на множестве натуральных чисел, называется *мультипликативной*, если для любых двух взаимно простых натуральных чисел $a$ и $b$ выполняется равенство

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

Например, для любого действительного числа $s$ функция $\theta(n) = n^s$ есть мультипликативная функция. Далее мы встретим и другие примеры мультипликативных функций.

Если $\theta(n)$ – не равная тождественно нулю мультипликативная функция, то $\theta(1) = 1$. Действительно, если натуральное число $a$ таково, что $\theta(a) \neq 0$, то имеем $\theta(a) = \theta(a \cdot 1) = \theta(a)\theta(1)$. Сокращая это равенство на $\theta(a)$, находим $1 = \theta(1)$.

Любое натуральное число $a > 1$ единственным образом представляется в виде произведения простых сомножителей, т.е. $a =$

$p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$. Поэтому для мультипликативной функции $\theta(n)$ имеем

$$\theta(a) = \theta(p_1^{k_1}) \cdot \ldots \cdot \theta(p_r^{k_r}) = \prod_{p|a} \theta(p^{\nu_p(a)}), \tag{3.1}$$

так что, любая мультипликативная функция однозначно определяется заданием её значений на степенях простых чисел.

Более того, задав произвольным способом функцию на степенях простых чисел и определив её значения на всех натуральных числах с помощью равенств (3.1), мы получим мультипликативную функцию.

Произведение мультипликативных функций есть мультипликативная функция. Действительно, если $\theta(n) = \theta_1(n) \cdot \theta_2(n)$, где $\theta_1(n)$ и $\theta_2(n)$ – мультипликативные функции, то для любых двух взаимно простых натуральных чисел $a$ и $b$ имеем

$$\theta(ab) = \theta_1(ab)\theta_2(ab) = \theta_1(a)\theta_1(b)\theta_2(a)\theta_2(b) = \theta(a) \cdot \theta(b).$$

Опишем ещё один способ строить мультипликативные функции.

**Лемма 3.1.** *Пусть $\theta(n)$ – мультипликативная функция и функция $f(n)$ определена равенствами*

$$f(n) = \sum_{d|n} \theta(d), \qquad n \geq 1,$$

*где суммирование происходит по всем натуральным делителям числа $n$. Тогда $f(n)$ – мультипликативная функция и*

$$f(n) = \prod_{p|n} (1 + \theta(p) + \theta(p^2) + \ldots + \theta(p^{\nu_p(n)})). \tag{3.2}$$

*Здесь произведение берётся по всем простым делителям числа $n$, а $\nu_p(n)$, как и в параграфе 2.2, есть кратность, с которой $p$ входит в разложение $n$ на простые сомножители.*

*Доказательство.* Для доказательства мультипликативности функции $f(n)$ рассмотрим какие-нибудь два натуральных взаимно простых числа $a$ и $b$. Каждый натуральный делитель $d$ числа $ab$ единственным образом представляется в виде произведения $d = d_1 d_2$, где $d_1|a, d_2|b$. Поэтому имеем

$$f(ab) = \sum_{d|ab} \theta(d) = \sum_{d_1|a} \sum_{d_2|b} \theta(d_1)\theta(d_2) = \left(\sum_{d_1|a} \theta(d_1)\right) \left(\sum_{d_2|b} \theta(d_2)\right) = f(a)f(b).$$

Таким образом, функция $f(n)$ мультипликативна.

Пользуясь мультипликативностью для $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$, находим

$$f(n) = f(p_1^{k_1}) \cdot \ldots \cdot f(p_r^{k_r}) = \prod_{j=1}^{r} (1 + \theta(p_j) + \theta(p_j^2) + \ldots + \theta(p_j^{k_j})).$$

И это завершает доказательство леммы. □

## 3.2 Функция Мёбиуса и формулы обращения

Функцией Мёбиуса[1] $\mu(n)$ называется мультипликативная функция, определённая на степенях простых чисел следующим образом

$$\mu(p) = -1, \qquad \mu(p^k) = 0, \quad k \geq 2.$$

Пользуясь мультипликативностью её можно доопределить на всех натуральных числах следующим образом

1. $\mu(1) = 1$;
2. $\mu(n) = 0$, если $n$ делится на квадрат простого числа;
3. $\mu(p_1 p_2 \ldots p_r) = (-1)^r$, если все простые числа $p_1, p_2, \ldots, p_r$ различны.

[1] А.Ф. Мёбиус, 1790-1868, - немецкий математик и астроном.

Например,

$$\mu(5) = \mu(7) = -1, \quad \mu(6) = \mu(10) = 1, \quad \mu(8) = \mu(9) = 0.$$

Функция $\mu(n)$ по определению является мультипликативной. Поэтому будет мультипликативной и функция $\theta(n) = \frac{\mu(n)}{n^s}$. В дальнейшем мы считаем, что $s > 1$ – фиксированное действительное число. Равенство (3.2) для выбранной функции $\theta(n)$ принимает вид

$$\sum_{d|n} \frac{\mu(d)}{d^s} = \prod_{p|n} \left(1 - \frac{1}{p^s}\right). \tag{3.3}$$

Это равенство справедливо для любого натурального $n$ и любого действительного числа $s$.

Выберем $n = \prod_{p \le x} p$ при некотором достаточно большом $x$ и рассмотрим две суммы $\sum_{d|n} \frac{\mu(d)}{d^s}$ и $\sum_{d \le x} \frac{\mu(d)}{d^s}$. Учитывая, что $\mu(d) = 0$, если $d$ делится на квадрат простого числа, заключаем, что каждое ненулевое слагаемое второй суммы содержится среди слагаемых первой суммы. Поэтому

$$\left| \sum_{d|n} \frac{\mu(d)}{d^s} - \sum_{d \le x} \frac{\mu(d)}{d^s} \right| \le \sum_{d > x} \frac{1}{d^s}$$

и, значит,

$$\left| \prod_{p \le x} \left(1 - \frac{1}{p^s}\right) - \sum_{d \le x} \frac{\mu(d)}{d^s} \right| \le \sum_{d > x} \frac{1}{d^s}.$$

Переходя в этом неравенстве к пределу при $x \to +\infty$ и пользуясь тождеством Эйлера (теорема 2.5), находим

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)}. \tag{3.4}$$

Таким образом, функция Мёбиуса имеет самое непосредственное отношение к дзета-функции Римана. В частности, гипотеза Римана о

нулях дзета-функции эквивалентна оценке

$$\sum_{d\le x}\mu(d)=O\left(x^{1/2+\varepsilon}\right),$$

при любом сколь угодно малом положительном $\varepsilon$.

Можно проверить с помощью тождества Эйлера, что равенство (3.4) эквивалентно следующему утверждению, которое будет доказано независимо от (3.4).

**Лемма 3.2.** *Справедливы равенства*

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{если } n=1,\\ 0 & \text{если } n>1.\end{cases}$$

*Доказательство.* Равенство в случае $n=1$, очевидно, выполняется. Пусть далее $n>1$. Поскольку $\mu(n)$ – мультипликативная функция, то равенство (3.2) и определение функции Мёбиуса дают

$$\sum_{d|n}\mu(d)=\prod_{p|n}(1+\mu(p))=0.$$

Лемма доказана. □

Следующее утверждение называется формулой обращения Мёбиуса.

**Теорема 3.1.** *Пусть $f(n)$ – произвольная функция натурального аргумента и*

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

*Тогда справедливы равенства*

$$f(n)=\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right). \tag{3.5}$$

*Доказательство.* При $n = 1$ имеем $g(1) = f(1)$, и требуемое равенство выполняется.

Пусть далее $n \geq 2$. Согласно определению функции $g(n)$ находим

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) = \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d).$$

По лемме 3.2 сумма $\sum_{d|\frac{n}{c}} \mu(d)$ отлична от нуля лишь в случае $c = n$. Учитывая, что в последнем случае она равна 1, получаем требуемое равенство. □

Укажем теперь несколько более общее тождество, чем (3.5), лежащее в основе так называемых "методов решета". Связь этого тождества с решетом Эратосфена, мотивирующая название, указывается далее в примере 1.

**Теорема 3.2.** *Пусть $a_1, \ldots, a_r$ действительные и $b_1, \ldots, b_r$ натуральные числа. Для любого натурального $d$ положим*

$$c_d = \sum_{j\,:\,d|b_j} a_j,$$

*где суммирование ведется по всем индексам $j$, для которых $b_j$ делится на $d$. Тогда справедливо равенство*

$$\sum_{d} \mu(d) c_d = \sum_{j\,:\,b_j=1} a_j. \tag{3.6}$$

Суммирование в левой сумме равенства (3.6) проводится по всем натуральным $d$, а в правой сумме – по всем индексам $j$ с условием $b_j = 1$. Заметим также, что лишь конечное количество чисел $c_d$ отлично от нуля, ведь множество делителей чисел $b_1, \ldots, b_r$ конечно.

*Доказательство.* С помощью леммы 3.2 находим

$$\sum_{d} \mu(d) c_d = \sum_{d} \mu(d) \sum_{j\,:\,d|b_j} a_j = \sum_{j=1}^{r} a_j \sum_{d|b_j} \mu(d) = \sum_{j\,:\,b_j=1} a_j.$$

□

Теорема 3.1 есть частный случай последнего утверждения. Действительно, пусть $n$ произвольное натуральное число и $1 = b_1 < b_2 < \ldots < b_r$ – все его натуральные делители. Для функции $f(x)$ из теоремы 3.1 положим $a_j = f\,(n/b_j)$. Тогда

$$c_d = \sum_{j\,:\,d|b_j} f\,(n/b_j) = \sum_{c\,|\,n/d} f\,(n/cd) = g\left(\frac{n}{d}\right),$$

где $g$ – функция, определённая в теореме 3.1. Учитывая, что $c_d = 0$ при $d \nmid n$, находим равенства

$$\sum_{j\,:\,b_j=1} a_j = \sum_{j\,:\,b_j=1} f\left(\frac{n}{b_j}\right) = f(n), \qquad \sum_{d} \mu(d)c_d = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

из которых, в силу (3.6) следует равенство (3.5).

С приложениями теоремы 3.1 мы ещё встретимся в дальнейшем. Сейчас же рассмотрим несколько примеров применения теоремы 3.2.

**Пример 1.** Пусть $x \geq 2$ – действительное и $D$ – натуральное числа. Положим в теореме 3.2 $r = [x]$, $a_j = 1$, $b_j = (j, D)$ при $j = 1, \ldots, r$. Тогда

$$c_d = \sum_{j\,:\,d|(j,D)} 1 = \begin{cases} 0 & \text{если } d \nmid D, \\ \left[\frac{x}{d}\right] & \text{если } d|D. \end{cases}$$

Равенство (3.6) приобретает следующий вид

$$\sum_{d|D} \mu(d) \left[\frac{x}{d}\right] = N, \tag{3.7}$$

где $N$ – количество натуральных чисел $n \leq x$, взаимно простых с $D$.

Если выбрать $D = \prod\limits_{p \leq y} p$, число $N$ в формуле (3.5) равняется количеству натуральных $n, 1 \leq n \leq x$, не имеющих простых делителей $p \leq y$. Таким образом, число $N - 1$ равняется в этом случае количеству натуральных чисел $n$ на отрезке $y < n \leq x$, оставшихся

невычеркнутыми, после просеивания решетом Эратосфена с помощью всех простых чисел $p \le y$.

Выберем $D = \prod_{p \le \sqrt{x}} p$. Так как каждое составное число $n \le x$ имеет простой делитель $p \le \sqrt{x}$, то условию $(j, D) = 1$ в рассматриваемом случае удовлетворяют лишь простые числа $p$ из промежутка $\sqrt{x} < p \le x$ и число 1. Поэтому $N = \pi(x) - \pi(\sqrt{x}) + 1$ и равенство (3.7) можно переписать в виде

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_{d|D} \mu(d) \left[\frac{x}{d}\right], \tag{3.8}$$

где $D = \prod_{p \le \sqrt{x}} p$. Получившуюся формулу можно использовать для вычисления значений функции $\pi(x)$. Однако, сумма, стоящая в правой части (3.8) содержит слишком много слагаемых, и это затрудняет вычисления.

Выбрав $D = \prod_{p \le \sqrt[3]{x}} p$, можно получить формулу, требующую значительно меньшего объёма вычислений.

**Пример 2.** Пусть $x \ge 2$ – действительное число и $r = [x]$. Для каждого $j \le x$ определим $b_j$ как наибольшее целое число $s$ с условием $s^2 | j$. Положим также $a_j = 1$. Тогда

$$c_d = \sum_{j\,:\,d|b_j} 1 = \left[\frac{x}{d^2}\right]$$

и по теореме 3.2 находим

$$\sum_d \mu(d) \left[\frac{x}{d^2}\right] = \sum_{j\,:\,b_j = 1} 1 = T(x), \tag{3.9}$$

где $T(x)$ – количество натуральных чисел $n \le x$, не делящихся на квадрат целого, большего 1.

Суммирование в левой части (3.9) проводится по всем натуральным числам $d \le \sqrt{x}$, ведь при $d > \sqrt{x}$ имеем $[x/d^2] = 0$. Отбрасывая

знаки целой части в этой сумме, мы совершим ошибку, не превосходящую $\sqrt{x}$. Поэтому равенство (3.9) может быть переписано в виде

$$T(x) = x \sum_{d \le \sqrt{x}} \frac{\mu(d)}{d^2} + O(\sqrt{x}). \tag{3.10}$$

Сумма в последнем равенстве есть частичная сумма ряда

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Заменяя частичную сумму в (3.10) суммой ряда, мы совершим ошибку не превосходящую остаточного члена и, значит, меньшую, чем

$$\sum_{d > \sqrt{x}} \frac{1}{d^2} < \sum_{d > \sqrt{x}} \left( \frac{1}{d-1} - \frac{1}{d} \right) = \frac{1}{[\sqrt{x}]}. \tag{3.11}$$

Но тогда равенство (3.10) можно переписать в виде

$$T(x) = \frac{6}{\pi^2} \cdot x + O(\sqrt{x}).$$

Получившееся равенство можно интерпретировать сказав, что при случайном выборе натурального числа из множества $n \le x$ с вероятностью близкой при больших $x$ к $6/\pi^2$ мы получим число, не делящееся на квадрат целого числа, отличный от 1.

## 3.3 Функция Эйлера

Для каждого целого числа $n \ge 1$ 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

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

Так определенную функцию натурального аргумента $n$ называют функцией Эйлера.

В частности, имеем $\varphi(1) = 1$. Среди чисел $1, 2, 3, 4, 5, 6$ взаимно простыми с 6 являются лишь 1 и 5. Поэтому $\varphi(6) = 2$. Для каждого простого числа $p$ лишь одно из чисел среди $1, 2, \ldots, p$ не взаимно просто с $p$, а именно само число $p$. Поэтому $\varphi(p) = p - 1$. Если $n = p^r$ есть степень простого числа, то нетривиальный общий делитель с $n$ могут иметь лишь числа, делящиеся на $p$, т.е. числа вида $pk$. Неравенство $pk \leq p^r$ выполняется для целых чисел $k \leq p^{r-1}$ и только для них. Поэтому

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

Свойства функции Эйлера описываются следующей теоремой.

**Теорема 3.3.** *1. Для любого натурального $n \geq 2$ 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*

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

*Первое доказательство.* По лемме 3.2 при любом натуральном $k$ выполняется равенство

$$\sum_{d|(k,n)} \mu(d) = \begin{cases} 1 & \text{если,} \quad (k,n) = 1, \\ 0 & \text{в противном случае.} \end{cases}$$

Поэтому справедливо представление

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(k,n)} \mu(d).$$

Все числа $d$, присутствующие в получившейся двойной сумме, являются делителями числа $n$. Соберем вместе слагаемые этой суммы, отвечающие одному и тому же делителю $d$ числа $n$. Ясно, что они будут появляться при $k$ делящихся на $d$, т.е. при $k = d, 2d, 3d, \ldots$. Последним из них будет число $k = n$, а количество слагаемых, отвечающих фиксированному значению $d$ равно $\frac{n}{d}$. Таким образом,

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \cdot \sum_{d|n} \frac{\mu(d)}{d}. \tag{3.12}$$

Первое утверждение теоремы следует отсюда с помощью равенства (3.3) при $s = 1$.

Второе утверждение теоремы может быть выведено из первого с помощью основной теоремы арифметики. Действительно

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

Другими словами это рассуждение можно пересказать так: из первого утверждения теоремы следует, что функция Эйлера есть произведение двух мультипликативных функций $n$ и $\prod_{p|n} \left(1 - \frac{1}{p}\right)$, а потому она мультипликативна. □

Первое утверждение теоремы 3.3 сразу же следует из теоремы 3.2, если положить в ней $a_j = 1, b_j = (j, n)$ при $1 \leq j \leq n$. Приведенное выше доказательство по-существу повторяет доказательство теоремы 3.2 в этом специальном случае.

Иное доказательство теоремы 3.3 основано на следующей лемме.

**Лемма 3.3.** *Для любого натурального $n$ выполняется равенство*

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

*Доказательство.* Пусть $r$ - делитель числа $n$ и $A_r$ - множество чисел $k$ из совокупности $1, 2, \ldots, n$, удовлетворяющих условию $(k, n) = r$.

Каждый элемент множества $A_r$ делится на $r$ и, значит, имеет вид $k = r\ell$ с некоторым $\ell, 1 \le \ell \le \frac{n}{r}$. По следствию 2.4 из теоремы 1.3 справедливо равенство $(k, n) = r(\ell, n/r)$, из которого следует, что включение $k \in A_r$ выполняется в том и только том случае, когда $(\ell, n/r) = 1$. Поэтому количество элементов в множестве $A_r$ равно $\varphi(n/r)$.

Множества $A_r$ для различных $r|n$, очевидно, не пересекаются, а их объединение совпадает с совокупностью $1, 2, \ldots, n$. Поэтому

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

Если $r$ пробегает все делители числа $n$, то $n/r$ также пробегает все делители $n$. Обозначив $d = n/r$, получаем

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

Это завершает доказательство леммы. □

Первое утверждение теоремы 3.3 получается из равенства леммы 3.3 с помощью формулы обращения Мёбиуса (теорема 3.1), примененной к функциям $f(n) = \varphi(n)$ и $g(n) = n$.

## 3.4 Сумма делителей и число делителей натурального числа

При любом натуральном $s$ функция $n^s$ мультипликативна. Согласно лемме 3.1 мультипликативной будет и функция

$$\sigma_s(n) = \sum_{d|n} d^s.$$

При $s = 0$ так получается функция

$$\tau(n) = \sigma_0(n) = \sum_{d|n} 1$$

- количество делителей $n$, а при $s = 1$ – функция

$$\sigma(n) = \sigma_1(n) = \sum_{d|n} d$$

- сумма делителей числа $n$. Обе эти функции мультипликативны.

Если $n = p_1^{k_1} \cdots p_m^{k_m}$, то по лемме 3.1 имеем

$$\tau(n) = (k_1 + 1) \cdots (k_m + 1)$$

и

$$\sigma(n) = \prod_{j=1}^{m} (1 + p_j + \cdots + p_j^{k_j}) = \prod_{j=1}^{m} \frac{p_j^{k_j+1} - 1}{p_j - 1}.$$

Заметим также, что $\tau(n)$ равно количеству решений в натуральных числах $x, y$ уравнения $x \cdot y = n$.

Древнегреческие математики выделили класс чисел, обладавших с их точки зрения некоторой внутренней гармонией, так называемых *совершенных чисел*. Целое число $N > 1$ называется совершенным, если оно равно сумме своих собственных делителей. Под собственными подразумеваются делители, отличные от самого числа. Так собственными делителями числа 6 являются числа $1, 2, 3$ и, в силу равенства $1+2+3 = 6$, число 6 совершенно. Еще одним совершенным числом является 28. Число 5 "недостаточно", у него сумма собственных делителей равная 1 слишком мала. А число 12 "избыточно", его сумма собственных делителей равна 16.

До сих пор не известно существуют ли нечетные совершенные числа. Это одна из нерешенных древних проблем теории чисел.

Структура четных совершенных чисел описывается результатами Евклида и Эйлера.

**Теорема 3.4.** *Четное число $N > 0$ совершенно тогда и только тогда, когда оно имеет вид $N = 2^n(2^{n+1} - 1)$, причем $2^{n+1} - 1$ простое число.*

Например, $6 = 2 \cdot 3$, причем $3 = 2^2 - 1$ – простое число, а $28 = 2^2 \cdot 7$ и $7 = 2^3 - 1$ также простое число. Простые числа вида $2^k - 1$ называются *простыми числами Мерсенна*[2] Из тождества

$$a^m - 1 = (a-1)(1 + a + \cdots + a^{m-1})$$

следует что число $2^{mk} - 1$ где $m, k$ натуральные числа, делится на $2^k - 1$. Поэтому число $M_p = 2^p - 1$ может быть простым лишь в случае, если $p$ – простое число. Так $M_2 = 3, M_3 = 7, M_5 = 31$ и $M_7 = 127$ – простые числа. С каждым из них связано некоторое совершенное число. Но вот $2^{11} - 1 = 2047 = 23 \cdot 89$ простым не является. Следующие простые числа Мерсенна – $M_{13}, M_{19}, M_{31}$ и $M_{61}$. В параграфе 2.1 указаны самые большие известные в настоящее время простые числа вида $2^p - 1$.

Предполагается, что множество простых чисел Мерсенна, а, значит, и множество четных совершенных чисел бесконечны. Однако этот факт не доказан и является еще одной древней проблемой теории чисел.

*Доказательство теоремы 3.4.* Докажем сначала утверждение Евклида, т.е. совершенность указанных в теореме чисел. Чтобы проверить это воспользуемся выведенной выше формулой для суммы делителей числа. Если $q = 2^{n+1} - 1$ простое число и $N = 2^n \cdot q$, то имеем

$$\sigma(N) = \frac{2^{n+1} - 1}{2 - 1} \cdot \frac{q^2 - 1}{q - 1} = (2^{n+1} - 1)(q + 1) = q \cdot 2^{n+1} = 2N.$$

Одним из слагаемых суммы делителей $\sigma(N)$ является и само число $N$, поэтому сумма собственных делителей $N$ равна $\sigma(N) - N = N$, т.е. $N$ совершенно.

Теперь докажем утверждение Эйлера, что каждое совершенное число имеет вид, указанный в теореме. Пусть $N = 2^n \cdot a$ совершенное число, причем $n \geq 1$ и $a$ нечетно. Так как числа $2^n$ и $a$ взаимно

[2]Мерсенн (1588-1648) - французский математик.

просты, а сумма делителей числа – мультипликативная функция, имеем

$$\sigma(N) = \sigma(2^n) \cdot \sigma(a) = (2^{n+1} - 1)\sigma(a).$$

Учитывая, что $N$ совершенное число, т.е. $\sigma(N) = 2N$, получаем уравнение

$$2^{n+1} \cdot a = (2^{n+1} - 1)\sigma(a).$$

Отсюда, так как $2^{n+1}$ и $2^{n+1} - 1$ взаимно простые числа, заключаем, что $a$ делится на $2^{n+1} - 1$, т.е. $a = (2^{n+1} - 1)b$ с некоторым натуральным $b$ и $\sigma(a) = 2^{n+1}b$. Если $b > 1$, то различные числа $a, b, 1$ являются делителями $a$, так что $\sigma(a) \geq a + b + 1 = \sigma(a) + 1$. Получившееся противоречие означает, что $b = 1$ и $\sigma(a) = a + 1$. Следовательно, $a$ имеет лишь два делителя 1 и $a$. Но тогда $a = 2^{n+1} - 1$ – простое число. □

## 3.5 Оценки среднего значения арифметических функций

Арифметические функции как правило ведут себя очень нерегулярно. Поэтому представляют интерес усредненные характеристики их поведения.

Рассмотрим сначала функцию $\tau(n)$.

**Теорема 3.5.** *При $N \to +\infty$ справедлива следующая асимптотическая формула*

$$\sum_{n=1}^{N} \tau(n) = N \ln N + O(N). \tag{3.13}$$

Поскольку $\tau(n)$ есть количество решений в натуральных числах $x, y$ уравнения $x \cdot y = n$, то сумма из теоремы, для краткости мы обозначим ее символом $U(N)$, равна количеству решений в натуральных числах $x, y$ неравенства $x \cdot y \leq N$. Геометрически эта величина может быть представлена как количество точек первого квадранта

с целыми положительными координатами, лежащих на и под гиперболой $x \cdot y = N$.

*Доказательство.* Из формулы $\tau(n) = \sum_{d|n} 1$ следует

$$U(N) = \sum_{n=1}^{N} \sum_{d|n} 1.$$

Поменяем в этой двойной сумме порядок суммирования, сделав $d$ внешней переменной. При фиксированном значении $d$ переменная $n$ принимает значения кратные $d$, т.е. $d, 2d, \ldots$. Обозначив $n = dk$, получим, что натуральное число $k$ меняется в интервале $1 \leq k \leq N/d$. Таким образом, фиксированному значению $d$ соответствует $[N/d]$ слагаемых двойной суммы, равных 1. Поэтому

$$U(N) = \sum_{d=1}^{N} \left[\frac{N}{d}\right].$$

Отбросив в каждом слагаемом знак целой части, мы совершим ошибку, не превосходящую единицы. Функция же $U(N)$ изменится не более, чем на $N$. Поэтому

$$U(N) = N \sum_{d=1}^{N} \frac{1}{d} + O(N).$$

Из леммы 2.6 следует $\sum_{d \leq N} \frac{1}{d} = \ln N + O(1)$. Поэтому для функции $U(N)$ получаем асимптотическое равенство (3.13). □

Среднее значение функции $\tau(n)$, т.е. величина

$$\frac{\tau(1) + \tau(2) + \ldots + \tau(N)}{N}$$

согласно теореме 3.5 примерно равна $\ln N$.

В настоящее время известны результаты намного более точные, чем формула (3.13). В 1849г. Дирихле доказал, что

$$\sum_{n=1}^{N} \tau(n) = N \ln N + (2\gamma - 1)N + O(N^{\delta}) \tag{3.14}$$

с $\delta = 1/2$. В 1903г. этот результат был усилен Г.Ф. Вороным[3], доказавшим, что формула (3.14) верна при любом $\delta > 1/3$. Этот результат также уточнялся. Но известно, что формула (3.14) при $\delta < 1/4$ уже неверна.

**Теорема 3.6.** *При $N \to +\infty$ справедлива следующая асимптотическая формула*

$$\sum_{n=1}^{N} \sigma(n) = \frac{1}{12}\pi^2 N^2 + O(N \ln N). \tag{3.15}$$

*Доказательство.* Пусть $V(N)$ – сумма из формулировки теоремы. Тогда имеем

$$V(N) = \sum_{n=1}^{N} \sum_{d|n} d.$$

Заменим в получившейся двойной сумме переменную суммирования $n$ новой переменной $k$, положив $n = dk$. Новые переменные суммирования $d, k$ будут пробегать все пары натуральных чисел, удовлетворяющие неравенствам $d \cdot k \leq N$. Тогда

$$V(N) = \sum_{d \cdot k \leq N} d = \sum_{k=1}^{N} \sum_{1 \leq d \leq N/k} d. \tag{3.16}$$

При любом $t > 1$ справедливы равенства

$$\sum_{d \leq t} d = \frac{[t]([t]+1)}{2} = \frac{1}{2}t^2 + O(t). \tag{3.17}$$

[3]Вороной Георгий Федосеевич (1868-1908) - русский математик.

Поэтому из (3.16) находим

$$V(N) = \frac{1}{2}\sum_{k=1}^{N}\frac{N^2}{k^2} + O\left(\sum_{k=1}^{N}\frac{N}{k}\right)$$

Из леммы 2.6 следует, что $\sum_{k=1}^{N}\frac{1}{k} < \ln(2N+1)$, поэтому

$$V(N) = \frac{1}{2}N^2\sum_{k=1}^{N}\frac{1}{k^2} + O(N\ln N).$$

Заменим теперь конечную сумму $\sum_{k=1}^{N}\frac{1}{k^2}$ суммой ряда

$$\sum_{k=1}^{\infty}\frac{1}{k^2} = \zeta(2) = \frac{\pi^2}{6}.$$

При этом будет совершена ошибка, оцениваемая величиной $\sum_{k>N}\frac{1}{k^2} \le \frac{1}{N}$, см. (3.11), что, приводит к нужной ассимптотической формуле. □

Из теоремы 3.6 следует, что среднее значение суммы делителей равно примерно $\frac{1}{12}\pi^2 N$.

**Теорема 3.7.** *При $N \to +\infty$ справедлива следующая асимптотическая формула*

$$\sum_{n=1}^{N}\varphi(n) = \frac{3}{\pi^2}N^2 + O(N\ln N). \tag{3.18}$$

Из определения функции Эйлера следует, что значение $\varphi(n)$ равно количеству несократимых дробей $\frac{m}{n}$ из промежутка $0 \le t \le 1$ со знаменателем $n$, а сумма из формулировки теоремы равна количеству несократимых дробей со знаменателем не большим $N$ на промежутке $[0;1]$. Общее же количество пар целых чисел $m, n$ с условием $1 \le m \le n \le N$ равно

$$\sum_{n=1}^{N} n = \frac{N(N+1)}{2} = \frac{1}{2}N^2 + O(N). \tag{3.19}$$

Поэтому результат теоремы 3.7 можно выразить иначе, сказав, что выбирая случайным образом пару целых чисел $m, n$, удовлетворяющих неравенствам $1 \le m \le n \le N$, можно получить несократимую дробь с вероятностью $\frac{6}{\pi^2} = 0,6079\ldots$.

*Доказательство.* Обозначим сумму из (3.18) символом $S(N)$. Тогда, пользуясь равенством (3.12), находим

$$S(N) = \sum_{n=1}^{N} \varphi(n) = \sum_{n=1}^{N} n \sum_{d|n} \frac{\mu(d)}{d}.$$

Заменим в получившейся двойной сумме переменную суммирования $n$ новой переменной $k$, положив $n = dk$. Новые переменные суммирования $d, k$ будут пробегать все пары натуральных чисел, удовлетворяющие неравенствам $d \cdot k \le N$. Тогда

$$S(N) = \sum_{d \cdot k \le N} k \cdot \mu(d) = \sum_{d=1}^{N} \mu(d) \sum_{1 \le k \le N/d} k. \tag{3.20}$$

Из равенства (3.17) следует, что внутренняя сумма в правой части (3.20) равна $\frac{N^2}{2d^2} + O(N/d)$. Подставляя это выражение в (3.20) и пользуясь тем, что $|\mu(d)| \le 1$, находим

$$S(N) = \frac{N^2}{2} \sum_{d \le N} \frac{\mu(d)}{d^2} + O\left(N \sum_{d \le N} \frac{1}{d}\right). \tag{3.21}$$

Пользуясь оценкой леммы 2.6 заключаем, что

$$S(N) = \frac{N^2}{2} \sum_{d \le N} \frac{\mu(d)}{d^2} + O(N \ln N).$$

Заменим теперь конечную сумму $\sum_{d \le N} \frac{\mu(d)}{d^2}$ суммой ряда

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

При этом будет совершена ошибка, оцениваемая величиной $\sum_{d>N} \frac{1}{d^2} \leq \frac{1}{N}$, см. (3.11), что, наконец, приводит к нужной ассимптотической формуле. $\square$

# Глава 4

# Числовые сравнения

## 4.1 Сравнения и их основные свойства

Пусть $m \geq 2$ целое число.

**Определение 5.** *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* $b \equiv a \pmod{b} \pmod{m}$.
3. *Если* $a \equiv b \pmod{m}$ *и* $b \equiv c \pmod{m}$, *то* $a \equiv c \pmod{m}$.

Например, последнее свойство следует из равенства

$$a - c = (a - b) + (b - c),$$

поскольку оба слагаемых в правой части делятся на $m$.

Если разность $a-b$ не делится на $m$, будем писать $a \not\equiv b \pmod{m}$.

Продолжим список свойств сравнений.

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.*

Доказательства трех указанных сравнений следуют из равенств

$$\begin{aligned} (b + d) - (a + c) &= (b - a) + (d - c), \\ (b - d) - (a - c) &= (b - a) - (d - c), \\ bd - ac &= (b - a)d + (d - c)a \end{aligned}$$

и свойств делимости.

Из свойства 4 следует также, что к любой из частей сравнения можно прибавить любое число кратное модулю, 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.

5. *Если* $ab \equiv ac \pmod m$ *и* $(a, m) = 1$, *то* $b \equiv c \pmod m$.

Действительно, согласно условию $m|(ab - ac) = a(b - c)$ и так как при этом $m$ и $a$ взаимно просты, то по следствию 1.2 из теоремы 1.3 получаем $m \mid (b - c)$, а это и требовалось.

Условие взаимной простоты $(a, m) = 1$ в последнем свойстве существенно: $4 \equiv 0 \pmod 4$, но из этого не следует, что $2 \equiv 0 \pmod 4$.

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* $ad \equiv bd \pmod{md}$.

Из $m|(b-a)$ следует $md|(b-a)d = (bd-ad)$.

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* $a \equiv b \pmod{m}$.

Из $md|(bd-ad) = d(b-a)$, очевидно, следует $m|(b-a)$.

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

Действительно, из условия следует, что $b - a = mc$ с некоторым целым $c$. Но тогда $b = a + mc$ и множество общих делителей чисел $a$ и $m$ совпадает с множеством общих делителей чисел $b$ и $m$. В частности, наибольшие элементы этих множеств совпадают, т.е. $(a,m) = (b,m)$.

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

Согласно условию $b - a = mc$ с некоторым целым $c$. Так как $d|m$, отсюда следует $d|(b-a)$.

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

Действительно, если $a \equiv b \pmod{m_j}$, $j = 1, 2, \ldots, r$, то разность $a - b$ делится на каждое из чисел $m_j$. По теореме 1.2 можно утверждать, что $a - b$ делится на наименьшее общее кратное модулей $m_1, \ldots, m_r$.

Как простейший пример использования сравнений, докажем, что уравнение

$$x^2 - 5y^2 = 3 \tag{4.1}$$

не имеет решений в целых числах. Предположим, что целые числа $a$ и $b$ удовлетворяют данному уравнению, т.е. $a^2-5b^2=3$. Тогда $a^2 \equiv 3 \pmod 5$. Целое число $a$ сравнимо с одним из чисел $0,1,2,3,4$ по модулю 5. Тогда $a^2$ сравнимо по этому же модулю с одним из чисел $0,1,2^2=4,3^2 \equiv 4,4^2 \equiv 1$. Так как 3 не сравнимо по модулю 5 ни с одним из чисел $0,1,4$, приходим к противоречию, доказывающему, что уравнение (4.1) не имеет решений в целых числах.

## 4.2 Классы вычетов. Кольцо классов вычетов по данному модулю

Свойства сравнений 1-3, сформулированные в предыдущем параграфе 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 $m$.

Каждое целое число $a$ представимо в виде

$$a = mq + r, \qquad 0 \le r < m,$$

с целыми $q, r$. Отсюда следует, что $a$ и $r$ лежат в одном классе вычетов и, значит, каждый класс вычетов содержит целое число $r$ из промежутка $0 \le r < m$. Таким образом, количество классов вычетов по модулю $m$ не превосходит $m$. С другой стороны, каждое из чисел $0,1,2,\ldots,m-1$ лежит в некотором классе вычетов и классы эти различны, ведь разность любых двух чисел из указанного списка не делится на $m$. Эти рассуждения доказывают, что *существует ровно $m$ классов вычетов по модулю $m$*. Каждый из них содержит единственное целое число $r$ из промежутка $0 \le r < m$, называемое

*наименьшим неотрицательным вычетом класса* и потому

$$\overline{0}, \quad \overline{1}, \quad \ldots, \quad \overline{m-1}$$

– все классы вычетов по модулю $m$.

На множестве классов вычетов по модулю $m$ можно ввести операции сложения, вычитания и умножения по правилам

$$\overline{a}+\overline{b}=\overline{a+b}, \quad \overline{a}-\overline{b}=\overline{a-b}, \quad \overline{a}\cdot\overline{b}=\overline{a\cdot b}. \tag{4.2}$$

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 $m$. Все аксиомы кольца, а также коммутативность, легко проверяются с помощью свойств делимости. Роль нулевого элемента этого кольца играет класс $\overline{0}$. Действительно, для любого элемента $\overline{a}$ имеем

$$\overline{a}+\overline{0}=\overline{a+0}=\overline{a}, \qquad \overline{0}+\overline{a}=\overline{0+a}=\overline{a}.$$

Роль единичного элемента – класс вычетов $\overline{1}$ :

$$\overline{a}\cdot\overline{1}=\overline{a\cdot 1}=\overline{a}, \qquad \overline{1}\cdot\overline{a}=\overline{1\cdot a}=\overline{a}.$$

Проверка ассоциативности умножения выполняется так

$$\overline{a}\cdot(\overline{b}\cdot\overline{c})=\overline{a}\cdot\overline{bc}=\overline{a\cdot(bc)}=\overline{(ab)\cdot c}=\overline{ab}\cdot\overline{c}=(\overline{a}\cdot\overline{b})\cdot\overline{c}.$$

Доказательство дистрибутивности проводится следующим образом

$$(\overline{a}+\overline{b})\cdot\overline{c}=\overline{a+b}\cdot\overline{c}=\overline{(a+b)\cdot c}=\overline{ac+bc}=\overline{ac}+\overline{bc}=\overline{a}\cdot\overline{c}+\overline{b}\cdot\overline{c}.$$

Остальные аксиомы кольца проверяются столь же несложными преобразованиями.

В кольце $\mathbb{Z}/m\mathbb{Z}$, вообще говоря, могут быть делители нуля. Например, при $m=6$ имеем $\overline{3}\cdot\overline{4}=\overline{12}=\overline{0}$. Пусть $a$ – целое число, $d=(a,m)$, причем $1<d<m$. Тогда с некоторыми целыми числами

$u, v$ выполняются равенства $a = du, m = dv$ и $av = udv = um \equiv 0 \pmod{m}$. Это значит, что $\overline{a} \cdot \overline{v} = \overline{0}$, причем $\overline{v} \neq \overline{0}$, т.е. $\overline{a}$ – делитель нуля в кольце $\mathbb{Z}/m\mathbb{Z}$.

Определим теперь группу обратимых элементов этого кольца.

**Лемма 4.1.** *Пусть $a$ – целое число, взаимно простое с модулем $m$. Тогда найдется целое число $b$, удовлетворяющее сравнению*

$$ab \equiv 1 \pmod{m}. \tag{4.3}$$

*Доказательство.* Рассмотрим числа

$$a, 2a, 3a, \ldots, ma \tag{4.4}$$

Они не сравнимы друг с другом по модулю $m$. Ведь если $ak \equiv a\ell \pmod{m}$, где $k, \ell$ – натуральные числа, не превосходящие $m$, то по свойству 5 сравнений выполняется $k \equiv \ell \pmod{m}$, что возможно лишь в случае $k = \ell$. Итак, числа (4.4) принадлежат различным классам вычетов по модулю $m$. Количество этих чисел равно $m$, поэтому какое-то из них принадлежит классу $\overline{1}$. Если это число равно $ba$, $1 \leq b \leq m$, то $ab \equiv 1 \pmod{m}$. □

Приведенное нами доказательство леммы 4.1 не конструктивно. Оно не позволяет найти число $b$, удовлетворяющее сравнению (4.3). Рассмотрим диофантово уравнение $ax - my = 1$ относительно неизвестных $x, y$. Согласно теореме 1.5 это уравнение разрешимо в целых числах. Действуя так, как это описано в параграфе 1.4 можно найти пару чисел $x = b, y = c$, удовлетворяющую равенству $ab - mc = 1$. Тогда $ab \equiv 1 \pmod{m}$. Эти рассуждения дают еще одно доказательство леммы 4.1.

Если целое число $a$ взаимно просто с модулем $m$, то по лемме 4.1 найдется целое $b$, удовлетворяющее (4.3). Тогда $\overline{a}\overline{b} = \overline{ab} = \overline{1}$ и класс вычетов $\overline{a}$ обратим. Если же $(a, m) > 1$, то по доказанному выше 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 $0 \leq k < m$ и $(k, m) = 1$. Количество таких чисел $k$ равно $\varphi(m)$, т.е. задаётся функцией Эйлера. Итак, доказано следующее утверждение.

**Теорема 4.1.** *Множество классов вычетов по модулю $m$ с операциями, определенными равенством (4.2), образует коммутативное кольцо с единицей. Группа обратимых элементов этого кольца состоит из $\varphi(m)$ классов, наименьшие неотрицательные вычеты которых взаимно просты с модулем.*

В частности, если модуль $m$ есть простое число, т.е. $\varphi(m) = m-1$, то каждый класс вычетов, отличный от $\overline{0}$ имеет обратный в кольце $\mathbb{Z}/m\mathbb{Z}$. Это значит, что кольцо классов вычетов по простому модулю есть поле.

На языке сравнений удобно описывать так называемые признаки делимости чисел. При наличии калькулятора или компьютера, конечно, удобнее воспользоваться техническими средствами, но иногда бывает польза и от вычислений на бумаге. Предположим нам нужно узнать, делится ли данное натуральное число $N$ на некоторое другое число $d$. Идея всех признаков делимости состоит в том, чтобы построить меньшее число $M$, делящееся на $d$ одновременно с $N$.

Следующий общий способ основан на использовании леммы 4.1. Пусть $d$ – натуральное число, взаимно простое с основанием системы счисления 10. Тогда согласно лемме 4.1 найдется число $k$, для которого $10k \equiv 1 \pmod{d}$. Пусть теперь $N = 10u+v$, где $u, v$ целые числа. Тогда справедливо сравнение по модулю $d$

$$N = 10u + v \equiv 10u + 10kv = 10(u + kv) \pmod{d}$$

Обозначим $M = u + kv$. Поскольку числа 10 и $d$ взаимно просты, то из сравнения следует, что $N$ и $M$ одновременно делятся на $d$.

Так что вопрос о делимости $N$ на число $d$ сводится к выяснению, делится ли на $d$ число $M$. Если при этом окажется, что $M < N$, то наша задача упростилась. Рассмотрим некоторые примеры. В них число $v$ равно младшей цифре в десятичной записи числа $N$.

1. $d = 7$. В этом случае справедливо сравнение $10 \cdot (-2) \equiv 1 \pmod 7$ и можно взять $k = -2$. Из сказанного выше следует, что число $N = 10u + v$ делится на 7 одновременно с числом $u - 2v$. Заменяя данное число $N$ меньшими числами по этому правилу мы получаем последовательность убывающих чисел $N_i$. Пусть, например, $N = 22624$. Тогда

$$N_1 = 2262 - 2 \cdot 4 = 2254, \quad N_2 = 225 - 2 \cdot 4 = 217, \quad N_3 = 21 - 2 \cdot 7 = 7.$$

Так как последнее число делится на 7, то 22624 также делится на 7.

2. $d = 13$. Имеем $10 \cdot 4 \equiv 1 \pmod{13}$ и можно взять $k = 4$. Число $N = 10u + v$ делится на 13 одновременно с числом $u + 4v$. Пусть, например, $N = 32721$. Тогда

$$N_1 = 3272 + 4 \cdot 1 = 3276, \quad N_2 = 327 + 4 \cdot 6 = 351, \quad N_3 = 35 + 4 \cdot 1 = 39.$$

Последнее число делится на 13, поэтому 32721 также делится на 13.

3. $d = 17$. Имеем $10 \cdot (-5) \equiv 1 \pmod{17}$ и можно взять $k = -5$. Число $N = 10u + v$ делится на 17 одновременно с числом $u - 5v$. Пусть, например, $N = 39321$. Тогда

$$N_1 = 3932 - 5 \cdot 1 = 3927, \quad N_2 = 392 - 5 \cdot 7 = 357, \quad N_3 = 35 - 5 \cdot 7 = 0.$$

Итак, число 39321 делится на 17.

При $d = 19$ можно взять $k = 2$, при $d = 23$ имеем $k = 7$, и $k = 3$ при $d = 29$.

Для $d = 3$ и $d = 9$ имеем $k = 1$ и, как легко проверить, получается известный признак: *натуральное число делится на* 3 *или* 9, *если сумма его цифр делится на* 3 *или* 9. А в случае $d = 11$ *натуральное число делится на* 11 *в том и только том случае, когда знакочередующаяся сумма его цифр делится на* 11. Для доказательства этих утверждений нужно также использовать индукцию по количеству цифр.

## 4.3 Полная и приведенная системы вычетов.

Совокупность представителей всех классов вычетов по заданному модулю $m \geq 2$ называется *полной системой вычетов* по модулю $m$. Например, числа $-2, -1, 0, 1, 2$ составляют полную систему вычетов по модулю 5. Еще один пример полной системы вычетов по модулю 5 составляют числа $0, 2, 2^2 = 4, 2^3 = 8, 2^4 = 16$. Совокупность наименьших неотрицательных вычетов всех классов, т.е. чисел $0, 1, \ldots, m-1$, составляет полную систему вычетов. *Любые $m$ чисел попарно несравнимые друг с другом по модулю $m$, образуют полную систему вычетов по этому модулю*, ведь они принадлежат различным классам вычетов, а количество их равно числу классов. Набор чисел (4.4) при $a$, взаимно простом с модулем $m$, составляет, как это установлено при доказательстве леммы 4.1, полную систему вычетов. Еще один пример полной системы вычетов – совокупность целых чисел $x$, удовлетворяющих неравенствам $-\frac{m}{2} < x \leq \frac{m}{2}$. Это так называемые *абсолютно наименьшие вычеты* классов по модулю $m$. Так при $m = 5$ имеем уже указанную выше полную систему вычетов $-2, -1, 0, 1, 2$, а при $m = 6$ систему вычетов $-2, -1, 0, 1, 2, 3$.

В предыдущем параграфе было доказано, что существует $\varphi(m)$ классов вычетов по модулю $m$, состоящих из чисел взаимно простых с модулем. Любой набор представителей этих классов вычетов называется *приведенной системой вычетов. Любые $\varphi(m)$ чисел, попарно несравнимые друг с другом по модулю $m$ и взаимно простые с модулем, образуют приведенную систему вычетов по модулю $m$*, действительно, ведь они лежат в различных классах, состоящих из чисел взаимно простых с $m$, а количество их равно количеству таких классов.

**Теорема 4.2.** *Пусть $a, m \geq 2$, – целые взаимно простые числа. Тогда*

*1. если $x$ пробегает полную систему вычетов по модулю $m$, то $ax+b$, где $b$ – любое целое число, также пробегает полную систему вычетов по модулю $m$;*

*2. если $x$ пробегает приведенную систему вычетов по модулю $m$, то $ax$ также пробегает приведенную систему вычетов по этому модулю.*

*Доказательство.* Для доказательства первого утверждения достаточно проверить, что для любых двух чисел $x_1$ и $x_2$, лежащих в различных классах вычетов по модулю $m$, числа $ax_1 + b$ и $ax_2 + b$ также лежат в различных классах вычетов. Предположим противное. Тогда

$$ax_1 + b \equiv ax_2 + b \pmod{m}.$$

Из этого сравнения следует, что $ax_1 \equiv ax_2 \pmod{m}$ и, поскольку числа $a, m$ взаимно просты, по свойству 5 сравнений заключаем, что $x_1 \equiv x_2 \pmod{m}$. Но это невозможно, так как $x_1$ и $x_2$ принадлежат различным классам вычетов по модулю $m$. Первое утверждение теоремы доказано.

Из сказанного выше следует, что для любых двух различных чисел $x_1, x_2$ приведенной системы вычетов числа $ax_1$, $ax_2$ лежат в различных классах вычетов. Осталось доказать, что для $x$, лежащего в приведенной системе вычетов, число $ax$ взаимно просто с $m$. Так как $(a, m) = 1$ и $(x, m) = 1$, то по следствию 2.3 из теоремы 1.3 заключаем, что $(ax, m) = 1$. Теорема доказана полностью. □

## 4.4 Теорема Вильсона

Следующее утверждение, характеризующее простые числа, называется теоремой Вильсона[1].

**Теорема 4.3.** *Для любого простого числа $p$ выполняется сравнение*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

*Доказательство.* Для $p = 2$ утверждение, очевидно выполняется, поэтому далее будем считать, что $p$ нечетно. Пусть $a$ – некоторое

[1] Эта теорема впервые была доказана в 1771г. французским математиком Лагранжем ()

целое число из промежутка $1 \leq a < p$. Так как $(a, p) = 1$, то по лемме 4.1 существует целое число $b$, удовлетворяющее сравнению $ab \equiv 1 \pmod{p}$. При этом можно считать, что $b$ есть наименьший неотрицательный вычет в своем классе. Ясно, что $b \neq 0$, т.е. $1 < b < p$. Кроме того, число $b$ определяется единственным образом. Ведь если $ab_1 \equiv 1 \pmod{p}$, $ab_2 \equiv 1 \pmod{p}$, то $p|a(b_1 - b_2)$ и $p|(b_1 - b_2)$, что при различных $b_1, b_2$ из промежутка $1 < b < p$ невозможно.

Если $b \equiv a \pmod{p}$, то $a^2 \equiv 1 \pmod{p}$ и $p|(a^2-1) = (a-1)(a+1)$. Так как $p$ простое число, это возможно лишь в случае $a = 1$ или $a = p - 1$. Из доказанного следует, что множество целых чисел $a$ из промежутка $1 < a < p - 1$ может быть разбито на пары различных целых чисел $a, b$, удовлетворяющих сравнению $ab \equiv 1 \pmod{p}$. Следовательно,

$$\prod_{k=2}^{p-2} k \equiv 1 \pmod{p}.$$

Умножая это сравнение на $p - 1$, получаем

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}.$$

□

Для составных чисел теорема Вильсона, конечно, нарушается. Ведь если целое число $N$ имеет делитель $d, 1 < d < N$, то $(N-1)!$ делится на $d$. Значит, $(N-1)! + 1$ на $d$ не делится, а потому не делится и на $N$.

## 4.5 Теоремы Эйлера и Ферма

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

**Теорема 4.4.** *Для каждого целого числа $a$ взаимно простого с модулем $m$ выполняется сравнение*

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

*Доказательство.* Пусть $r_1, \ldots, r_h$ – какая-нибудь приведенная система вычетов по модулю $m$. Тогда $h = \varphi(m)$. Согласно теореме 4.2 множество чисел $ar_1, ar_2, \ldots, ar_h$ также составляет приведенную систему вычетов. Это значит, что каждое число второй системы лежит в одном классе с каким-либо единственным числом первой системы вычетов. Поэтому справедливы сравнения

$$ar_1 \cdot ar_2 \cdots ar_h \equiv r_1 \cdot r_2 \cdots r_h \pmod{m}. \tag{4.5}$$

Так как каждое из чисел $r_j$ взаимно просто с модулем, то сравнение (4.5) можно сократить на каждое из $r_j$. В результате получаем сравнение $a^h \equiv 1 \pmod{m}$ или $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Например, для $m = 10$ имеем $\varphi(10) = 4$. В соответствии с теоремой Эйлера можно утверждать, что каждое нечетное число $a$, не делящееся на 5, удовлетворяет сравнению $a^4 \equiv 1 \pmod{10}$, т.е. последняя цифра в десятичной записи числа $a^4$ равна 1. И действительно,

$$1^4 = 1, \quad 3^4 = 81, \quad 7^4 = 2401, \quad 9^4 = 6561.$$

Рассмотрим еще один пример. Определим последние три цифры в десятичной записи числа $3^{2007}$. Для этого достаточно сосчитать $3^{2007} \pmod{1000}$. Так как $\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$, и $(3, 1000) = 1$, то по теореме Эйлера выполняется сравнение $3^{400} \equiv 1 \pmod{1000}$. Отсюда следует

$$3^{2007} = \left(3^{400}\right)^5 \cdot 3^7 \equiv 3^7 \pmod{1000}.$$

Эти сравнения означают, что $3^{2007}$ и $3^7 = 2187$ имеют одинаковые три последние цифры, и десятичная запись числа $3^{2007}$ оканчивается цифрами 187.

Для некоторых чисел $a$ сравнение $a^d \equiv 1 \pmod{m}$ может выполняться и при натуральных $d < \varphi(m)$. Например, для $a = 1$ можно взять $d = 1$. Имеем $3^2 \equiv 1 \pmod{8}$, тогда как $\varphi(8) = 4$. Можно проверить, что $3^{100} \equiv 1 \pmod{1000}$, но выше установлено равенство $\varphi(100) = 400$. Наименьшее натуральное число $d$ с условием $a^d \equiv 1 \pmod{m}$ называется *показателем числа* $a$ по модулю $m$.

**Лемма 4.2.** *Пусть $d$ – показатель 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, $d|\varphi(m)$.*

*Доказательство.* Для каждого $k = ds$ имеем

$$a^k = (a^d)^s \equiv 1 \pmod{m}.$$

Докажем утверждение в обратную сторону. Пусть $a^k \equiv 1 \pmod{m}$. Разделив $k$ на $d$ с остатком, получим $k = dq + r,\ 0 \le r < d$. Тогда

$$a^r \equiv (a^d)^q \cdot a^r = a^k \equiv 1 \pmod{m}.$$

Учитывая, что $d$ – наименьший натуральный показатель с условием $a^d \equiv 1 \pmod{m}$ и $r < d$, заключаем, что $r = 0$. Следовательно, $d|k$. □

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 4.5.** *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 $p$.

## 4.6 Представление рациональных чисел бесконечными десятичными дробями

Как пример использования теоремы Эйлера, рассмотрим представления рациональных чисел $\alpha$ бесконечными десятичными дробями, т.е. в виде рядов

$$\alpha = a_0 + \sum_{k=1}^{\infty} \frac{a_k}{10^k} = a_0, a_1 a_2 \ldots, \tag{4.6}$$

где все $a_k, k \geq 1$, есть цифры $0 \leq a_k \leq 9$, и покажем, что рациональным числам соответствуют периодические разложения.

Прежде всего, существует не более одного представления числа $\alpha$ в виде (4.6), содержащего бесконечное количество цифр, отличных от 9. Это следует из того, что при любом $k \geq 0$ справедливо равенство $a_0 10^k + \ldots + a_{k-1}10 + a_k = [10^k \alpha]$.

Докажем, что сумма ряда, соответствующего бесконечной периодической десятичной дроби есть рациональное число. Это достаточно доказать для чисто периодической дроби $\alpha = 0,(a_1 a_2 \ldots a_m)$. Обозначив $A = a_1 10^{m-1} + \ldots + a_{m-1}10 + a_m$ и пользуясь формулой для суммы геометрической прогрессии, найдем

$$\alpha = \sum_{k=0}^{\infty} 10^{-km} \left( \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_m}{10^m} \right) = \\ = A \sum_{k=1}^{\infty} 10^{-km} = \frac{A}{10^m - 1}. \quad (4.7)$$

Заметим, что если при этом $\alpha = \frac{a}{b}$ – несократимое представление в виде отношения натуральных чисел, то $b|(10^m - 1)$, т.е. $10^m \equiv 1 \pmod{b}$.

Пусть теперь $\alpha = \frac{a}{b}$, где $0 < a < b$ и $(b, 10) = 1$. Обозначим буквой $d$ показатель числа 10 по модулю $b$. Тогда $10^d \equiv 1 \pmod{b}$ и с некоторым натуральным числом $c$ выполняется равенство $10^d - 1 = bc$. Записав теперь $ac$ в десятичной системе счисления $B = ac = b_1 10^{d-1} + \ldots + b_{d-1}10 + b_d$, и пользуясь тождеством (4.7), получим представление $\alpha$ в виде бесконечной периодической дроби

$$\frac{a}{b} = \frac{B}{10^d - 1} = \sum_{k=0}^{\infty} 10^{-kd} \left( \frac{b_1}{10} + \frac{b_2}{10^2} + \ldots + \frac{b_d}{10^d} \right) = 0,(b_1 \ldots b_d).$$

Период в бесконечном десятичном разложении числа $\alpha$ записывается теми же цифрами, что и числитель в представлении $\alpha = \frac{B}{10^d - 1}$. При этом нужно иметь в виду, что период может начинаться с некоторого количества нулей, так $\frac{1}{99} = 0,(01)$.

Если рациональное число $\alpha$ больше единицы, числитель дроби $\alpha = \frac{a}{b}$, $(a, b) = 1$, можно представить в виде $a = bq + r$, $0 \le r < b$ и разложив $\frac{r}{b}$ в бесконечную периодическую дробь, получим $\frac{a}{b} = q, (b_1 \dots b_d)$. При $r = 0$ имеем $\alpha = q = q, (0)$.

Если знаменатель дроби $\frac{a}{b}$ не взаимно прост с 10, т.е. делится на 2 или на 5, то его можно умножить на такое натуральное число $u = 2^s 5^t$, что получится равенство $ub = 10^k v$, где $(v, 10) = 1$ и $k = \max(\nu_2(b), \nu_5(b))$. Тогда

$$\frac{a}{b} = 10^{-k} \frac{ua}{v} = 10^{-k} \cdot c_0, (c_1 \dots c_m).$$

Получившееся представление дает конечную десятичную дробь в случае $v = 1$ и бесконечную периодическую дробь, если $v > 1$.

Заметим также, что в случае $(b, 10) = 1$, длина минимального периода равна показателю 10 по модулю $b$. В силу леммы 4.2 длина периода не превосходит при этом $\varphi(b)$. Минимальную длину периода $\varphi(b)$ имеют, как можно проверить, рациональные числа со знаменателями

$$b = \quad 7,\ 17,\ 19,\ 23,\ 29,\ 47,\ 49,\ 59,\ 61,\ 97.$$

Список исчерпывает все такие $b \le 100$.

Пусть $\alpha = \frac{a}{b}$ – несократимое представление с $(b, 10) = 1$. Пусть также $\frac{a}{b} = 0, (b_1 \dots b_d)$ и $c \equiv 10a \pmod{b}$, $0 < c < b$. Тогда с некоторым целым $q$ имеем

$$\frac{c}{b} = q + 10\frac{a}{b} = q + b_1 + 0, (b_2 \dots b_d b_1) = 0, (b_2 \dots b_d b_1).$$

Период дроби $\frac{c}{b}$ получается из периода $\frac{a}{b}$ циклическим сдвигом на одну позицию. Если допустить в этом случае не чисто периодические разложения, то

$$\frac{c}{b} = 0, b_2 \dots b_d (b_1 b_2 \dots b_d)$$

и можно сказать, что бесконечные разложения дробей $\frac{a}{b}$ и $\frac{c}{b}$ имеют одинаковые периоды.

В частности, если показатель 10 по модулю $b$ равен $\varphi(b)$, то бесконечные десятичные разложения всех дробей $\frac{a}{b}, 1 \leq a < b, (a,b) = 1$ имеют одинаковые периоды. Например,

$$\frac{1}{7} = 0,(142857) \qquad \frac{2}{7} = 0,(285714),$$
$$\frac{3}{7} = 0,(428571) \qquad \frac{4}{7} = 0,(571428),$$
$$\frac{5}{7} = 0,(714285) \qquad \frac{6}{7} = 0,(857142).$$

## 4.7 Проверка на простоту и построение больших простых чисел

Пусть $N$ – натуральное число, вообще говоря большое. Оно может быть либо составным, либо простым. Как определить, к какому из этих двух классов относится данное число?

Можно попробовать разделить $N$ на простые числа из таблицы, составленной с помощью решета Эратосфена и содержащей все простые числа до некоторой границы $B$, определяемой нашими возможностями. Если у $N$ есть маленькие простые делители, мы сможем найти их таким способом и доказать, что $N$ – составное число.

Если же маленькие простые делители не обнаружены и если $B$ сравнительно велико, а именно, $B^2 > N$, можно утверждать, что $N$ простое число. Действительно, если бы $N$ было составным, по лемме 2.1 оно имело бы простой делитель $p \leq \sqrt{N} < B$, содержащийся в нашей таблице. Но таковой отсутствует.

В случае же $N > B^2$ никакого заключения о числе $N$ сделать нельзя.

Далее мы будем считать, что $N$ достаточно велико и не имеет маленьких простых делителей. Выберем целое число $a, 1 < a < N$, и вычислим с помощью алгоритма Евклида наибольший общий делитель $d = (a, N)$. Если оказалось, что $d > 1$, можно утверждать, что $N$ – составное число, ведь оно делится на $d$, причем $1 < d < N$.

Если же оказалось, что $(a, N) = 1$, то о числе $N$ опять никакого заключения сделать нельзя. Если у составного числа $N$ нет маленьких простых делителей, то количество взаимно простых с ним чисел $a$ на интервале $1 < d < N$ равное $\varphi(N) - 1 = N\prod_{p|N}(1 - p^{-1}) - 1$ будет достаточно большим, и маловероятно, что выбранное наугад число $a$, позволит разложить число $N$ на множители.

В этом случае может помочь малая теорема Ферма. Если для числа $N$ и выбранного $a$ с условием $(a, N) = 1$ ее утверждение нарушается, можно утверждать, что $N$ – составное число. Итак, *если*

$$(a, N) = 1, \qquad \textit{и} \qquad a^{N-1} \not\equiv 1 \pmod{N},$$

*то $N$ – составное число.*

Простейший алгоритм для вычисления $a^d \pmod{N}$, состоящий в последовательном умножении на $a$ результата предшествующего вычисления, требует $d - 1$ умножений. В действительности это вычисление можно провести намного быстрее.

Возьмем, например, $N = 437$ и вычислим $2^{436} \pmod{437}$. Поскольку числа не очень большие, это можно сделать на ручном калькуляторе. Используя свойства сравнений (для краткости мы нигде не указываем модуль сравнения, равный 437), получаем:

$$\begin{aligned} 2^3 &\equiv 4 \cdot 2 = 8, & 2^6 &\equiv 8^2 = 64, \\ 2^{13} &\equiv 64^2 \cdot 2 \equiv -111, & 2^{27} &\equiv (-111)^2 \cdot 2 \equiv 170, \\ 2^{54} &\equiv 170^2 \equiv 58, & 2^{109} &\equiv 58^2 \cdot 2 \equiv 173, \\ 2^{218} &\equiv 173^2 \equiv 213, & 2^{436} &\equiv 213^2 \equiv 358. \end{aligned}$$

Проведенные вычисления не раскладывают число 437 на множители, но доказывают, что оно составное. Как легко проверить, $437 = 19 \cdot 23$.

Может показаться, что указанный способ проверки требует слишком много вычислений. Но эти вычисления однотипны. Мы либо возводили в квадрат, либо удваивали число по модулю $N$. И это обстоятельство оказывается очень удобным при реализации алгоритма

на компьютере. А кроме того, как сейчас выяснится, и количество возведений в квадрат мало по сравнению с величиной $N$.

Рассмотренный выше пример есть частный случай общего алгоритма.

**Алгоритм 4.1.** Данные: *Целые числа* $a, N > 1, d > 0$.
Найти: $a^d \pmod N$.

*1. Представить* $d$ *в двоичной системе счисления, т.е. найти такие цифры* $d_j \in \{0,\ 1\}$, *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*

$$a_i \equiv a_{i-1}^2 \cdot a^{d_i} \pmod N. \tag{4.8}$$

*3. Положить* $a^d \equiv a_r \pmod N$.

Таким образом, в случае $d_i = 0$ алгоритм вычисляет $a_i \equiv a_{i-1}^2 \pmod N$, если же $d_i = 1$, то $a_i \equiv a_{i-1}^2 \cdot a \pmod N$. Реализованная выше последовательность вычислений для $d = 436 = 2^8+2^7+2^5+2^4+2^2$ в точности соответствует алгоритму. Докажем теперь, что алгоритм работает правильно, и количество выполняемых им арифметических операций не очень велико.

**Теорема 4.6.** *Алгоритм действительно вычисляет* $a^d \pmod N$. *Он использует для этого не более* $2[\log_2 d]$ *умножений в кольце вычетов* $\mathbb{Z}/N\mathbb{Z}$.

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

$$a_i \equiv a^{d_0 2^i + \cdots + d_i} \pmod N. \tag{4.9}$$

Докажем это индукцией по $i$. При $i = 0$ утверждение выполняется, т.к. $d_0 = 1$. Подставляя (4.9) в равенство $a_{i+1} = a_i^2 \cdot a^{d_{i+1}}$, находим равенство (4.9) для $a_{i+1}$. Это доказывает (4.9) для всех $i$. При $i = r$ получаем $a_r = a^d$, что доказывает правильность алгоритма.

Для доказательства второго утверждения обозначим символом $c(d)$ количество умножений в кольце $\mathbb{Z}/N\mathbb{Z}$, необходимых алгоритму

для вычисления $a^d \pmod N$. Докажем индукцией по $d$ неравенство

$$c(d) \le 2[\log_2 d]. \tag{4.10}$$

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

При $d = 1,\ 2$ неравенство (4.10), очевидно, выполняется. Пусть теперь $d \ge 3$. В силу алгоритма справедливы соотношения

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

доказывающие нужное неравенство. □

Одним из понятий, используемых для сравнения эффективности алгоритмов, является их сложность. Сложность алгоритмов теории чисел обычно принято измерять 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 перемножить 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. Это зависит от рассматриваемой задачи, от целей автора и т.д. Говоря в дальнейшем о сложности, мы будем иметь в виду количество арифметических операций, необходимых для выполнения алгоритмов.

Алгоритмы, в которых количество арифметических операций может быть оценено некоторой степенью числа цифр, необходимых для записи данных, называются *полиномиальными*. Такие алгоритмы, как правило, работают достаточно быстро при их использовании на практике. Алгоритм Евклида требует выполнения $O(\log a)$ арифметических операций, см. теорему 1.2. Для приведенного выше алгоритма возведения в степень согласно теореме 4.6 нужно $O(\log d)$ арифметических операций. Так как целое число $d$ записывается в

двоичной системе счисления не менее чем $\log_2 d$ цифрами, получаем, что как алгоритм Евклида, так и алгоритм возведения в степень относятся к разряду полиномиальных, т.е. быстрых алгоритмов.

Теорема Вильсона также может быть использована для определения, является ли данное натуральное число простым или составным. В отличие от теоремы Ферма быстрые алгоритмы для вычисления факториалов не известны, а использование формулы $k! \equiv k \cdot (k-1)! \pmod{N}$ требует примерно $N$ умножений для нахождения $(N-1)! \pmod{N}$. Основанный на этой формуле алгоритм не является полиномиальным. Его использование на практике требует очень много времени на вычисления, и даже при сравнительно небольших $N$ ответ с помощью этого алгоритма получить не удается.

Сравнительно недавно, в 2000 г., был найден детерминированный алгоритм полиномиальной сложности, позволяющий по заданному натуральному числу $N$ сказать, будут оно простым или составным. Он был предложен индийскими математиками М. Агравалом, Н. Кайалом, Н. Саксеной. Но этот алгоритм не очень удобен на практике, так как требует слишком большого объема памяти при вычислениях на компьютере. Объем необходимой памяти – еще одна характеристика качества алгоритма. Используемые в настоящее время алгоритмы для проверки простоты заданного числа $N$ имеют сложность $O\left((\log N)^{c \log\log\log N}\right)$ с некоторой постоянной $c > 0$. Поскольку функция $\log\log\log x$ растет очень медленно, в пределах важных для практического использования эти алгоритмы работают быстро. Однако знания, необходимые для их описания выходят за рамки настоящей книги.

К сожалению, с помощью малой теоремы Ферма не всегда можно проверить, что испытываемое число $N$ – составное. Существуют составные числа, для которых выполняется сравнение $a^{N-1} \equiv 1 \pmod{N}$ при любом целом $a$ с условием $(a, N) = 1$.

Возьмем, например, $N = 561 = 3 \cdot 11 \cdot 17$. Для каждого целого $a$ взаимно простого с 561 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.

Составное число $N$ называется *числом Кармайкла*[2] если

$$a^{N-1} \equiv 1 \pmod N \qquad \text{при любом} \qquad a \in \mathbb{Z},\ (a,N)=1. \tag{4.11}$$

Числа Кармайкла встречаются в натуральном ряду достаточно редко, но известно, что их множество бесконечно.

Рассмотрим следующий алгоритм, доказывающий для составного числа, что оно является составным, и несколько более точный, чем прямое использование малой теоремы Ферма.

**Алгоритм 4.2.** Данные: *Нечётное натуральное число* $N > 2$. Определить, будет ли $N$ составным числом.

*1. Найти целые числа* $s, t$, *для которых* $N-1 = 2^s t$, *причем* $t$ *нечетно. Выбрать целое число* $a, 1 < a < N$.
*2. Если* $(a,N) > 1$, *то* $N$ *составное число.*
*3. Если* $(a,N) = 1$ *и выполнены условия*

$$a^t \not\equiv 1 \pmod N, \quad a^{2^k t} \not\equiv -1 \pmod N, \quad k = 0,1,\dots,s-1, \tag{4.12}$$

*то* $N$ *составное число.*
*4. Если хотя бы одно из условий пункта 3 нарушается, алгоритм завершает свою работу не дав ответа.*

Очевидно, ответ алгоритма в п. 2 верен. Справедливо разложение на множители

$$a^{N-1} - 1 = (a^t-1)(a^t+1)(a^{2t}+1)\cdots(a^{2^{s-1}t}+1). \tag{4.13}$$

[2] Carmichael – английский математик, доказавший в 1912г., что каждое составное число со свойством (4.11) есть произведение различных нечетных простых чисел, $N = p_1 \cdots p_r$, причем $r \geq 3$ и $(p_j - 1) \mid (N-1)$ при всех $j$. Число 561 обладает этим свойством. Еще один пример $1729 = 7 \cdot 13 \cdot 19$.

Если $N$ – простое число, то по малой теореме Ферма обе части последнего равенства должны делиться на $N$, и, следовательно, хотя бы один из сомножителей в правой части (4.13) должен делиться на $N$. Значит, хотя бы одно из условий (4.12) будет нарушено. Это доказывает, что и в пункте 3 алгоритм дает верный ответ.

Можно доказать, что для составного нечетного $N > 9$ количество взаимно простых с $N$ чисел $a, 1 < a < N$, для которых нарушается хотя бы одно из условий (4.12) сравнительно невелико, а именно, оно не превосходит $\frac{1}{4}\varphi(N)$, где $\varphi(N)$ – функция Эйлера. Это значит, что если алгоритму 4.2 задано составное число $N$, и он выбирает в п. 1 число $a$ на интервале $1 < a < N$ случайным образом, то с вероятностью $\geq \frac{3}{4}$ алгоритм докажет, что $N$ – составное число. А применяя этот алгоритм $r$ раз и выбирая каждый раз число $a$ поновому, мы докажем, что $N$ составное с вероятностью $\geq 1 - 4^{-r}$. Подчеркнем, еще раз, что алгоритм всегда дает правильный ответ, а оценивается лишь вероятность того, что ответ будет получен.

Алгоритм 4.2 дает удобное на практике средство отсеивания составных чисел. Если он сработал достаточно много раз и не дал ответа, можно надеяться, что испытываемое число просто. К сожалению, алгоритм не доказывает это. Рассматриваемая далее теорема позволяет получать некоторую информацию о возможных делителях $N$ и приводит к некоторому достаточному условию простоты.

**Теорема 4.7.** *Пусть $N$ - нечетное и $F$ - натуральное число такие, что для любого простого делителя $q|F$ существует целое $a$ с условиями*

$$a^F \equiv 1 \pmod{N}, \qquad \left(a^{F/q} - 1,\, N\right) = 1. \tag{4.14}$$

*Тогда любой простой делитель $p$ числа $N$ удовлетворяет сравнению*

$$p \equiv 1 \pmod{F}.$$

*Доказательство.* Пусть $p$ - простой делитель $N$, $q$ - простой дели-

тель $F$ и $a$ - число, удовлетворяющее (4.14). Тогда

$$a^F \equiv 1 \pmod{p}, \qquad a^{F/q} \not\equiv 1 \pmod{p}. \tag{4.15}$$

и, в частности, $a$ не делится на $p$. Обозначим буквой $d$ показатель $a$ 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 в силу леммы 4.2 имеем $d|p-1$ и

$$\nu_q(d) \leq \nu_q(p-1). \tag{4.16}$$

Из (4.15) и леммы 4.2 следует, что $d|F$ и $d \nmid F/q$. Это возможно лишь в случае

$$\nu_q(F) = \nu_q(d). \tag{4.17}$$

Из (4.16) и (4.17) находим

$$\nu_q(F) = \nu_q(d) \leq \nu_q(p-1).$$

Последнее неравенство согласно условию справедливо для любого простого делителя $q$ числа $F$, поэтому $F|p-1$ или $p \equiv 1 \pmod{F}$. □

Рассмотрим, пример использования теоремы 4.7, представляющий исторический интерес.

Пусть $a$ и $m$ – натуральные числа. Если $m$ имеет нечетный простой делитель $r$, т.е. $m = rs$, то из равенства

$$a^m + 1 = (a^s)^r + 1 = (a^s + 1)(a^{s(r-1)} - a^{s(r-2)} + \ldots - a^s + 1)$$

следует, что $a^m + 1$ – составное число. Значит, число $a^m + 1$ может быть простым лишь в случае, 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

$$F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537 \tag{4.18}$$

просты.

В 1640г. П. Ферма предположил, что при любом целом $n \geq 1$, число $F_n$ будет простым, но не смог доказать это для $F_5 = 2^{32} + 1$.

Л. Эйлер в 1729г. показал, что $F_5$ делится на 641 и тем опроверг гипотезу Ферма. Короткое доказательство этого факта использует представления

$$641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4.$$

Пользуясь ими, получаем

$$F_5 = 2^{32} + 1 \equiv -5^4 \cdot 2^{28} + 1 \equiv -(5 \cdot 2^7)^4 + 1 \equiv -1 + 1 = 0 \pmod{641}.$$

Позже было доказано, что $F_6, F_7$ - составные. Последнее число было разложено на простые множители в 1970г. Число $F_8$ также составное, но его простые делители неизвестны. В настоящее время неизвестно, будет число $F_{17}$ простым или составным. Не найдено ни одного простого числа Ферма, отличного от чисел (4.18).

В связи с числами Ферма отметим знаменитую теорему Гаусса: правильный $n$-угольник может быть построен с помощью циркуля и линейки лишь в случае $n = 2^k p_1 \cdots p_r$, где $p_j$ - различные простые числа Ферма.

Как же можно было угадать возможный делитель 641 числа Ферма $F_5$? Воспользуемся для этого теоремой 4.7 и выберем

$$N = F_5 = 2^{32} + 1, \qquad F = 128, \qquad a = 2^{16} + 1.$$

Так как

$$a^2 = 2^{32} + 2 \cdot 2^{16} + 1 \equiv 2^{17} \pmod{N},$$

то

$$a^{64} \equiv 2^{17 \cdot 32} \equiv (-1)^{17} = -1 \pmod{N}.$$

Следовательно,

$$a^{128} \equiv 1 \pmod{N}, \qquad (a^{64} - 1, N) = (2, N) = 1.$$

Согласно теореме 4.7 каждый простой делитель $p$ числа $F_5$ должен удовлетворять сравнению $p \equiv 1 \pmod{128}$. Первые простые числа в прогрессии $1 + 128 \cdot k$ есть 257 и 641. Они получаются при $k = 2$ и $k = 5$ соответственно. Второе из них есть делитель числа Ферма $F_5$.

Предположим далее, что нам известна лишь часть $F$ разложения числа $N - 1$ на простые сомножители. Эта информация позволяет сделать некоторые заключения о свойствах делителей числа $N$. А если известная часть разложения $N-1$ достаточно велика, то иногда можно сделать вывод об отсутствии нетривиальных делителей, т.е. о простоте $N$.

Рассмотрим сначала случай, когда $F = N - 1$, т.е. известно полное разложение числа $N - 1$ на простые множители. Этот случай представляют, например, числа Ферма.

**Следствие 4.1.** *Пусть $N$ нечетно и для каждого простого делителя $q$ числа $N - 1$ существует целое $a$ с условиями*

$$a^{N-1} \equiv 1 \pmod{N}, \qquad \left(a^{(N-1)/q} - 1,\, N\right) = 1. \tag{4.19}$$

*Тогда $N$ - простое число.*

*Доказательство.* Применяя теорему 4.7 с $F = N - 1$, заключаем, что каждый простой делитель $p$ числа $N$ удовлетворяет сравнению $p \equiv 1 \pmod{N-1}$ и, значит, $p \geq N$. Но это возможно лишь в случае $p = N$, т.е. когда $N$ простое число. □

К сожалению, чаще всего, если Вам требуется доказать простоту какого-либо числа $N$, разложение $N - 1$ на простые множители удается определить лишь частично. В таком случае может помочь

**Следствие 4.2.** *Пусть $N, F$ нечетны*

$$N - 1 = F \cdot R, \qquad R \leq 4F + 3,$$

*причем для каждого простого делителя $q$ числа $F$ существует целое $b$ с условиями*

$$b^{N-1} \equiv 1 \pmod{N}, \qquad \left(b^{(N-1)/q} - 1,\, N\right) = 1. \tag{4.20}$$

*Тогда $N$ - простое число.*

*Доказательство.* Применим теорему 4.7 к $a = b^R$. Согласно этой теореме каждое простое $p|N$ удовлетворяет сравнению $p \equiv 1 \pmod{F}$ и, поскольку $p - 1$ четно, а $F$ нечетно, удовлетворяет неравенству $p \geq 1 + 2F$. Предположим, что $N$ - составное. Тогда по лемме 2.1

$$(2F + 1)^2 \leq p^2 \leq N = FR + 1 \leq 4F^2 + 3F + 1.$$

Получившееся противоречие завершает доказательство. □

Как правило, необходимость в больших простых числах возникает в связи с различными криптографическими приложениями. Мы коснемся этого вопроса в следующем параграфе. Естественно, к конструируемым числам предъявляются определенные требования. Конструкция простых чисел должна быть массовой, а сами простые числа должны быть в каком-то смысле хорошо распределенными в заданном диапазоне. 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. С другой стороны на практике иногда нужны простые числа $p$, обладающие какими-либо дополнительными особенностями, например $p - 1$ не должно иметь маленьких нечетных простых делителей.

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 покажем, как с помощью следствия 4.2, имея большое простое число $F$, можно построить существенно большее простое число $N$. Выберем для этого случайным образом целое число $Q$ на промежутке $F \leq Q \leq 2F + 1$ и положим $N = 2FQ + 1$. Затем можно проверить число $N$ на отсутствие малых простых делителей. Испытать его некоторое количество раз с помощью алгоритма 4.2. Если при этом выяснится, что $N$ составное

число, следует выбрать новое значение $Q$ и опять повторить вычисления. Так следует делать до тех пор, пока не будет найдено число $N$, выдержавшее испытания алгоритмом 4.2 достаточно много раз. В этом случае появляется надежда на то, что $N$ - простое число, что и следует попытаться доказать с помощью следствия 4.2. Для этого можно случайным образом выбирать число $b, 1 < b < N$, и проверять для него выполнимость условий

$$b^{N-1} \equiv 1 \pmod{N}, \qquad \left(b^{2Q} - 1, N\right) = 1. \tag{4.21}$$

Если при выбранном $b$ эти соотношения выполняются, то, поскольку $2Q \leq 4F + 2 < 4F + 3$, согласно следствию 4.2 можно утверждать, что число $N$ простое.

Если же условия (4.21) 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 (4.21). Заметим, что для простого числа $N$ первое условие (4.21), согласно малой теореме Ферма, будет выполняться всегда. Те же числа $b$, для которых нарушается второе условие (4.21), удовлетворяют сравнению $b^{2Q} \equiv 1 \pmod{N}$. В следующей главе, см. теорему ??? будет доказано, что в промежутке $1 < b < N$ имеется не более $2Q - 1$ чисел, удовлетворяющих сравнению $b^{2Q} \equiv 1 \pmod{N}$. Это означает, что выбирая случайным образом числа $b$ 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 4.2, и тем доказать, что $N$ действительно является простым числом.

Заметим, что построенное таким способом простое число $N$ будет удовлетворять неравенству $N > 2F^2$, т.е. количество цифр в его записи более чем вдвое будет превосходить количество цифр в записи исходного простого числа $F$. Заменив теперь число $F$ на най-

денное простое число $N$ и повторив с этим новым $F$ все указанные выше действия, можно построить еще большее простое число. Начав с какого-нибудь небольшого числа, простоту которого можно проверить, например, делением на маленькие табличные простые числа, и повторив указанную процедуру достаточное число раз, можно построить простые числа нужной величины.

Покажем пример вычислений с помощью описанной схемы. Начнем с простого числа $F_1 = 1223$. Пользуясь следствием 4.2, с $b = 2$, получим по формулам $N_i = 2F_iQ_i + 1, F_{i+1} = N_i$

$$
\begin{aligned}
&Q_1 = 1231, \quad F_2 = N_1 = 3011027,\\
&Q_2 = 3011067, \quad F_3 = N_2 = 18132808071619,\\
&Q_3 = 18132808071644, \quad F_4 = N_3 = 657597457125248955270143273,\\
&Q_4 = 657597457125248955270143281,\\
&N_4 = 864868831235187275941586469515911058724056920216597427.
\end{aligned}
$$

Каждое из чисел $N_i$ просто. При их построении мы выбирали числа $Q_i$ наименьшими $Q_i \geq F_i$, при которых соответствующие числа $N_i$ оказывались простыми. Во всех случаях это удалось доказать с помощью следствия 4.2 при $b = 2$.

В настоящее время никаких теоретических гарантий для существования простого числа $N = 2FQ + 1, Q \leq 2F + 1$ 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 вопрос о расстоянии между соседними простыми числами в арифметической прогрессии. Ведь убедившись, что при некотором $Q$ число $N = 2FQ + 1$ составное, можно заменить $Q$ на $Q + 1$ и продолжить действовать описанным способом до тех пор, пока не будет найдено простое число $N$. И

если расстояние между соседними простыми числами в прогрессии велико, нет надежды быстро построить нужное число $N$. Перебор чисел $Q$ 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 доказано лишь, что $p_{n+1} - p_n = O(p_n^c)$, при любом $c > \frac{38}{61}$. Это очень трудная теорема, но она дает слабую оценку для наших потребностей. Вместе с тем существует так называемая гипотеза Крамера (1936г.), что $p_{n+1} - p_n = O(\ln^2 p_n)$, дающая вполне приемлемую границу. Вычисления на ЭВМ показывают, что простые числа в арифметических прогрессиях расположены достаточно плотно.

Если принять на веру, что наименьшее простое число, а также расстояние между соседними простыми числами в прогрессии $2Fn + 1$ при $F \leq n \leq 2F + 1$ оцениваются величиной $O(\ln^2 F)$ , то описанная схема построения больших простых чисел имеет полиномиальную оценку сложности. И, 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.

## 4.8 Разложение целых чисел на множители и криптографические применения.

Предположим, что задано некоторое составное натуральное число $N$, и требуется разложить его на меньшие множители. Эта задача относится к разряду трудных в вычислительном отношении.

Первые алгоритмы ее решения были предложены Ферма, Эйлером, Гауссом, Лежандром и другими классиками математики. Современные алгоритмы используют вычисления в полях алгебраических чисел, эллиптические кривые и разнообразные технические конструкции. Наилучшая из известных оценок сложности разложе-

ния числа $N$ на множители имеет вид $O(\exp(c(\ln N)^{1/3}(\ln\ln N)^{2/3}))$ с некоторой положительной постоянной $c$. Впрочем, эта оценка количества необходимых арифметических операций условна, так как опирается на ряд недоказанных, но весьма правдоподобных гипотез теории чисел. Установленный в настоящее время рекорд – разложение на два простых множителя числа

$$\begin{aligned} N =& 27997833911221327870829467638722601621070446786955 \\ & 42853756000992932612840010760934567105295536085606 \\ & 18223519109513657886371059544820065767750985805576 \\ & 13579098734950144178863178946295187237869221823983, \end{aligned}$$

записываемого в десятичной системе 200 цифрами. Ему было присвоено имя RSA-200. Работы по разложению были начаты в конце 2003 года и завершились в мае 2005 года. Было найдено разложение на простые множители $N = p \cdot q$, где

$$\begin{aligned} p =& 35324619344027701212726049781984643686711974001976 \\ & 250236493034687761212536794232000585479565280883 49 \end{aligned}$$

и

$$\begin{aligned} q =& 79258699544783330333470858414800596877379758573642 \\ & 199607343303414557678728181521353814093047401854 67. \end{aligned}$$

Вычисления на предварительном этапе выполнялись на многих машинах, работавших параллельно. Оценка общего времени работы, условно приведенная к одному процессору с рабочей частотой 2,2 Ггц, составляет 55 лет. Заключительный этап проводился на кластере, состоявшем из 80 процессоров такой же производительности и занял три месяца. Более подробный отчет об этой работе можно найти на страничке http://www.loria.fr/ zimmerma/records/factor.html в Интернет.

Приведенная информация показывает, насколько больших вычислительных ресурсов требует разложение целых чисел на множители. Она характеризует только внешнюю сторону этой деятельности,

оставляя в тени большой труд математиков, разработавших соответствующие алгоритмы и программистов, сумевших реализовать их оптимальным образом.

Подводя некоторый итог, подчеркнем, что большие простые числа могут быть построены сравнительно легко, например, с помощью алгоритмов предыдущего параграфа. Перемножив, два из них, можно получить большое целое число, разложение которого на множители представляет практически непреодолимые трудности для тех, кто не знает исходные простые числа. На этом обстоятельстве основана одна из используемых систем шифрования информации. Она носит название RSA,[3] была предложена в 1977г., и в течение длительного срока ее использования никто не смог придумать легкий способ распознавать сообщения, зашифрованные с ее помощью.

Любой текст можно записать последовательностью цифр, например, перенумеровав буквы алфавита и знаки, используемые при написаниии текстов: пробелы, точки, запятые, тире и т.д. Заменив каждую букву или знак их номером, мы и получим последовательнось цифр, подлежащую шифрованию. Длинные последовательности можно разбить на блоки, и шифровать каждый блок отдельно. Тот, кто хочет использовать систему RSA, обозначим его буквой A, поступает следующим образом:

*1. выбирает два достаточно больших простых числа* $p, q$ *и третье число* $e$*, взаимно простое с* $(p-1)(q-1)$*;*
*2. вычисляет* $N = pq$*, а также целое число* $d$ *с условием*

$$ed \equiv 1 \pmod{(p-1)(q-1)};$$

*3. публикует в открытой печати числа* $e, N$*.*

Заметим, что простые числа $p, q$ и показатель степени $d$ остаются при этом в секрете.

[3] Сокращение, составленное из первых букв фамилий ее авторов: Rivest R., Shamir A., Adleman L.

Согласно условию числа $e$ и $(p-1)(q-1)$ взаимно просты. Лемма 4.1 утверждает, что число $d$, удовлетворяющее сравнению из пункта 2 существует. Найти его можно, например, решив в целых числах $u, v$ уравнение $eu - (p-1)(q-1)v = 1$ так, как это объяснено в параграфе 1.4, и положив $d = u$. При этом можно считать, что $0 < d < (p-1)(q-1)$.

Блок информации можно представлять себе целым числом $x, 1 < x < N$. Каждый, желающий сообщить пользователю A некоторую секретную информацию $x$, должен зашифровать ее по правилу

$$y \equiv x^e \pmod{N}.$$

После этого он может переслать по открытому каналу связи сообщение $y$.

В соответствии с конструкцией числа $N$ выполняется равенство $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Согласно теореме Эйлера имеем

$$y^d \equiv (x^e)^d \equiv x \pmod{N}.$$

Поэтому пользователю A для расшифровки сообщения достаточно вычислить $y^d \pmod{N}$. Обе операции шифрования и расшифрования выполняются достаточно быстро.

Злоумышленник, чтобы расшифровать сообщение, должен найти целое число $x$, удовлетворяющее сравнению $x^e \equiv y \pmod{N}$. Известные быстрые алгоритмы для решения этой задачи при больших $N$ и $e$ связаны с вычислением секретного числа $d$. Это можно сделать, зная функцию Эйлера $\varphi(N)$. Тот же, кто знает одновременно числа $N$ и $\varphi(N)$, решая систему уравнений $pq = N$, $(p-1)(q-1) = \varphi(N)$ относительно чисел $p, q$, сможет найти простые делители $N$, т.е. разложить число $N$ на множители. Значит, вычисление функции Эйлера $\varphi(N)$ – задача столь же сложная в вычислительном отношении, как и разложение на множители.

Возможно существуют и другие сравнительно быстрые способы найти $d$ по известной информации $e, N$, или другие способы вычисления целого $x$, удовлетворяющего сравнению $x^e \equiv y \pmod{N}$, но за прошедшее время такие обнаружены не были.

# Глава 5

# Сравнения с одним неизвестным

В предыдущей главе мы уже встречались с задачей нахождения целых чисел, удовлетворяющих заданным сравнениям. Так лемма 4.1 есть утверждение об условиях разрешимости в целых числах $x$ сравнения $ax \equiv 1 \pmod{m}$. Уравнение $x^2 - 5y^2 = 3$, см. (4.1), не имеет решений в целых числах потому, что неразрешимо сравнение $x^2 \equiv 3 \pmod{5}$. Из малой теоремы Ферма следует, что для простого $p$ каждое целое число удовлетворяет сравнению $x^p - x \equiv 0 \pmod{p}$. А чтобы прочитать сообщение, зашифрованное с помощью схемы $RSA$, нужно уметь решать сравнения вида $x^e \equiv a \pmod{m}$.

В этой главе мы обсудим некоторые общие вопросы, связанные с решением сравнений, в которые входит одна неизвестная величина, будем обозначать ее буквой $x$. В отличие от уравнений каждое сравнение имеет еще и модуль. Разрешимость сравнений, а также способы нахождения решений, зависят, как мы увидим в дальнейшем, от свойств модуля. Можно также сказать другими словами, что решение сравнений по модулю $m$ есть решение уравнений в кольце классов вычетов $\mathbb{Z}/m\mathbb{Z}$.

## 5.1 Основные определения

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

влетворяет сравнению

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \tag{5.1}$$

если $f(u) \equiv 0 \pmod{m}$. Из результатов параграфа 4.1 следует, что для любого целого числа $v$, сравнимого с $u$ по модулю $m$, выполняется $f(v) \equiv f(u) \equiv 0 \pmod{m}$, другими словами, все числа класса вычетов $x \equiv u \pmod{m}$ удовлетворяют сравнению (5.1). Таким образом, множество, состоящее из всех целых чисел, удовлетворяющих (5.1), если оно не пусто, представляется в виде объединения нескольких непересекающихся классов вычетов по модулю $m$.

Каждый класс вычетов, состоящий из чисел, удовлетворяющих (5.1), называется *решением сравнения* (5.1), а количество таких классов вычетов, называется *числом решений* этого сравнения. Число решений сравнения (5.1) есть число решений уравнения $f(x) = 0$ в кольце $\mathbb{Z}/m\mathbb{Z}$. При этом, если класс вычетов $\overline{k}$ состоит из чисел, удовлетворяющих сравнению $f(x) \equiv 0 \pmod{m}$, то, в соответствии с определением операций, в кольце классов вычетов $\mathbb{Z}/m\mathbb{Z}$ имеет место равенство $f(\overline{k}) = 0$. Здесь мы допускаем некоторую вольность используя одно и то же обозначение $f(x)$ как для многочлена с целыми коэффициентами, присутствующего в сравнении, так и для многочлена в уравнении, коэффициенты которого являются соответствующими классами вычетов. С формальной точки зрения сравнению (5.1) должно соответствовать уравнение

$$\overline{a}_n x^n + \ldots + \overline{a}_1 x + \overline{a}_0 = \overline{0}.$$

Мы и в дальнейшем для краткости записи будем опускать черточки, если из контекста ясно, что речь идет о решении уравнения в кольце классов вычетов.

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 $x$ не делится на $m$, т.е. $m \nmid a_n$, то говорят, что *степень сравнения* (5.1) равна $n$.

Например, сравнение второй степени $x^2 - 1 \equiv 0 \pmod 8$ имеет четыре решения

$$x \equiv 1 \pmod 8, \qquad x \equiv 3 \pmod 8,$$
$$x \equiv 5 \pmod 8, \qquad x \equiv 7 \pmod 8,$$

в иных обозначениях эти классы вычетов по модулю 8 могут быть записаны так $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. Сравнению удовлетворяет каждое нечетное число.

Можно рассматривать и сравнения более общего вида

$$f(x) \equiv g(x) \pmod m, \tag{5.2}$$

где $f(x), g(x)$ – многочлены с целыми коэффициентами. Из свойств сравнений сразу же следует, что множества чисел, удовлетворяющих (5.2) и сравнению $f(x) - g(x) \equiv 0 \pmod m$ совпадают. Так что все вопросы, возникающие в связи со сравнениями (5.2) сразу же сводятся к соответствующим вопросам для сравнений, содержащих 0 в правой части.

## 5.2 Сравнения первой степени

Каждое сравнение первой степени может быть переписано в виде

$$ax \equiv b \pmod m, \qquad m \nmid a. \tag{5.3}$$

Основной результат о таких сравнениях есть

**Теорема 5.1.** *Сравнение (5.3) разрешимо если и только если, $b$ делится на наибольший общий делитель $(a, m)$. Количество решений в этом случае равно $(a, m)$.*

*Доказательство.* Сравнение (5.3) разрешимо в том и только в том случае, когда имеет решение в целых числах $x, y$ уравнение

$$ax + my = b. \tag{5.4}$$

По теореме 1.5 для этого необходимо и достаточно, чтобы $(a, m)|b$.

Предположим теперь, что $b$ делится на $(a, m)$. Из той же теоремы следует, что множество решений уравнения имеет вид

$$x = x_0 + \frac{m}{(a,m)}t, \qquad y = y_0 - \frac{a}{(a,m)}t, \tag{5.5}$$

где пара чисел $x_0, y_0$ есть какое-либо фиксированное решение, а $t$ – произвольное целое число. Итак, множество целых чисел $x$, удовлетворяющих сравнению (5.3) имеет вид

$$x = x_0 + \frac{m}{(a,m)}t, \qquad t \in \mathbb{Z} \tag{5.6}$$

при некотором целом $x_0$. Рассмотрим числа

$$x_k = x_0 + \frac{m}{(a,m)}k, \qquad k = 1, 2, \ldots, (a, m). \tag{5.7}$$

Докажем, что каждое число, удовлетворяющее сравнению (5.3), сравнимо по модулю $m$ с одним из чисел (5.6). Пусть $x$ имеет вид (5.6) и $k$ – то из чисел совокупности $1, 2, \ldots, (a, m)$, которое сравнимо с $t$ по модулю $(a, m)$. Тогда $t = k + q \cdot (a, m)$ с некоторым целым $q$, и

$$x = x_0 + \frac{m}{(a,m)}(k + q \cdot (a, m)) = x_k + qm \equiv x_k \pmod{m}.$$

Для завершения доказательства осталось проверить, что все числа (5.7) лежат в разных классах вычетов по модулю $m$. Предположим, что $x_k \equiv x_\ell \pmod{m}$, где $k, \ell$ – различные числа из набора $1, 2, \ldots, (a, b)$. Тогда

$$\frac{m}{(a,m)}k \equiv \frac{m}{(a,m)}\ell \pmod{m}.$$

Разделив обе части и модуль этого сравнения на целое число $\frac{m}{(a,m)}$ получаем в силу свойства 7 из параграфа 4.1, что $k \equiv \ell \pmod{(a, m)}$. Получившееся противоречие завершает доказательство теоремы. □

Отметим, что лемма 4.1 следует из доказанной теоремы.

Для решения сравнения (5.3) можно решить в целых числах уравнение (5.4), чтобы найти $x_0$ и воспользоваться формулой (5.7) для нахождения представителей всех нужных классов вычетов.

Для упрощения решения сравнения все коэффициенты можно заменить их наименьшими неотрицательными вычетами по модулю $m$.

Заметим, также, что в случае разрешимости, т.е делимости $b$ на $(a, m)$, обе части сравнения и модуль можно разделить на $(a, m)$, что упростит задачу, сведя ее к сравнению с меньшим модулем. Множества чисел, удовлетворяющих новому сравнению и данному совпадают.

Решим, например, сравнение

$$38x \equiv 4 \pmod{26}.$$

Так как $38 \equiv 12 \pmod{26}$, то у данного сравнения те же решения, что и у сравнения $12x \equiv 4 \pmod{26}$. Имеем $(12, 26) = 2$ и 4 делится на 2, поэтому данное сравнение разрешимо и имеет два решения. Кроме того, множество удовлетворяющих ему чисел таково же, как и у сравнения $6x \equiv 2 \pmod{13}$. Заменим получившееся сравнение уравнением $6x + 13y = 2$.

Для решения этого уравнения применим алгоритм Евклида. Уже первый его шаг приводит к равенству $13 = 6 \cdot 2 + 1$, из которого следует, что $1 = 13 - 2 \cdot 6$ и $2 = 13 \cdot 2 - 4 \cdot 6$. Таким образом уравнение имеет решение $x = -4, y = 2$ и $x_0 = -4$. Множество чисел, удовлетворяющих сравнению $6x \equiv 2 \pmod{13}$ состоит из одного класса вычетов по модулю 13, а именно $x \equiv -4 \pmod{13}$. Относительно же модуля 26 имеем два решения. Эти классы вычетов по модулю 26 содержат числа $-4 + \frac{26}{2}k$, $k = 1, 2$, т.е. числа $9, 22$. Итак, решения данного сравнения имеют вид

$$x \equiv 9 \pmod{26}, \qquad x \equiv 22 \pmod{26}.$$

## 5.3 Китайская теорема об остатках

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.

Решим, например, следующую систему сравнений

$$\begin{cases} 3x & \equiv 5 \pmod 4, \\ 5x & \equiv 2 \pmod 7. \end{cases} \tag{5.8}$$

Один из возможных общих способов решения этой задачи состоит в том, чтобы заменить систему сравнений системой уравнений, вводя при этом новые переменные. Так первому сравнению заданной системы удовлетворяют в точности те целые числа $x$, для которых найдется целое число $y$, удовлетворяющее равенству $3x - 4y = 5$. Аналогично, второе сравнение может быть заменено уравнением $5x - 7z = 2$, а вся система сравнений может быть заменена системой уравнений

$$\begin{cases} 3x - 4y & = 5, \\ 5x - 7z & = 2. \end{cases}$$

Эту систему можно решить так, как это объяснялось в параграфе 1.4. Соответствующая матрица (1.10) имеет вид

$$\begin{pmatrix} 3 & -4 & 0 & -5 \\ 5 & 0 & -7 & -2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Поскольку нас в действительности не интересуют переменные $y$ и $z$, две последние строки этой матрицы можно отбросить и все вычисления, указанные в параграфе 1.4 выполнять для более простой

матрицы. С помощью допустимых преобразований находим

$$\begin{pmatrix} 3 & -4 & 0 & -5 \\ 5 & 0 & -7 & -2 \\ 1 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ -5 & 1 & 0 & 0 \\ -1 & -4 & -28 & -113 \end{pmatrix}.$$

Таким образом, все числа, удовлетворяющие заданной системе сравнений имеют вид $x = -113 + 28t, t \in \mathbb{Z}$. Это множество можно записать в виде $x \equiv -113 \pmod{28} \equiv -1 \pmod{28}$.

Конечно, в данном конкретном случае систему сравнений можно было бы решить проще. Умножим каждое из сравнений системы на 3. В результате получаем систему сравнений $\begin{cases} 9x & \equiv 15 \pmod 4, \\ 15x & \equiv 6 \pmod 7, \end{cases}$ или $\begin{cases} x & \equiv -1 \pmod 4, \\ x & \equiv -1 \pmod 7. \end{cases}$ Переписанная в таком виде, система означает, что все искомые числа $x$ таковы, что $x + 1$ делится на 4 и на 7, т.е. делится на 28. В результате находим $x \equiv -1 \pmod{28}$.

Далее мы рассмотрим системы сравнений специального вида

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned} \tag{5.9}$$

где $m_i > 0$, $a_i$ – заданные целые числа. Их решение также может быть сведено к решению систем уравнений. Но в одном важном частном случае решение системы (5.9) может быть получено относительно легко. Следующее утверждение было известно в Китае примерно 2 тысячелетия назад. В настоящее время оно носит название "китайская теорема об остатках".

**Теорема 5.2.** *Если $m_1, \ldots, m_k$ попарно взаимно просты, то система сравнений (5.9) разрешима. Если для целых чисел $M, M_i, b_i$ выполнены соотношения*

$$M = m_1 \cdots m_k, \quad M_i = \frac{M}{m_i}, \quad M_i b_i \equiv a_i \pmod{m_i}, \quad 1 \le i \le k,$$

*и*

$$x_0 = M_1 b_1 + \ldots + M_k b_k, \tag{5.10}$$

*то множество целых чисел, удовлетворяющих системе сравнений (5.9), составляет класс вычетов* $x \equiv x_0 \pmod{M}$.

Поскольку в условиях теоремы $(M_i, m_i) = 1$, то существование чисел $b_i$ следует из теоремы 5.1. Заметим также, что числа $b_i$ определяются не единственным способом. При использовании теоремы 5.2 для решения систем сравнений, следует выбирать те из них, которые дают по возможности меньшие значения $x_0$.

*Доказательство.* Так как $m_i | M_j$ при $j \neq i$, то при любом $i$ выполняются сравнения

$$x_0 \equiv M_i b_i \equiv a_i \pmod{m_i}. \tag{5.11}$$

Это значит, что множества целых чисел, удовлетворяющих системе (5.9) и системе

$$x \equiv x_0 \pmod{m_i}, \qquad 1 \leq i \leq k, \tag{5.12}$$

совпадают. Сравнения (5.12) выполняются в том и только том случае, когда $m_i | (x - x_0)$, $1 \leq i \leq k$. Учитывая попарную взаимную простоту модулей $m_i$, с помощью следствия 2.6 заключаем, что последнее свойство выполняется для тех и только тех чисел $x$, для которых $M | (x - x_0)$, т.е. $x \equiv x_0 \pmod{M}$. □

**Пример.** Решим систему сравнений

$$x \equiv 3 \pmod{7}, \qquad x \equiv 2 \pmod{11}, \qquad x \equiv 1 \pmod{13}, \qquad .$$

В данном случае модули $7, 11, 13$ попарно взаимно просты. Пользуясь соотношениями теоремы 5.2, находим $M = 7 \cdot 11 \cdot 13 = 1001, M_1 = 11 \cdot 13 = 143, M_2 = 7 \cdot 13 = 91, M_3 = 7 \cdot 11 = 77$. Решая вспомогательные сравнения

$$143x \equiv 3 \pmod{7}, \quad 91x \equiv 2 \pmod{11}, \quad 77x \equiv 1 \pmod{13},$$

и выбирая по одному числу, удовлетворяющему каждому из них, находим $b_1 = 1$, $b_2 = -3$, $b_3 = -1$. Далее вычисляем

$$x_0 = 143 \cdot 1 + 91 \cdot (-3) + 77 \cdot (-1) = -207.$$

Ответ: $x \equiv -207 \pmod{1001}$.

**Следствие 5.1.** *Если числа $a_1, \ldots, a_k$ независимо друг от друга пробегают полные системы вычетов по модулям $m_1, \ldots, m_k$ соответственно, то числа $x_0$, определенные для каждого набора $a_1, \ldots, a_k$ с помощью равенств (5.10), пробегают полную систему вычетов по модулю $M = m_1 \cdots m_k$.*

*Доказательство.* Достаточно доказать, что получающиеся указанным в условии способом числа $x_0$ принадлежат различным классам вычетов по модулю $M$. Предположим, что $a_1, \ldots, a_k$ и $a'_1, \ldots, a'_k$ два набора вычетов по модулям $m_1, \ldots, m_k$, причем такие, что хотя бы для одного индекса $i$ выполняется $m_i \nmid (a_i - a'_i)$. Пусть также числа $b_i$, $b'_i$ удовлетворяют сравнениям $M_i b_i \equiv a_i \pmod{m_i}$, $M_i b'_i \equiv a'_i \pmod{m_i}$ и

$$x_0 = M_1 b_1 + \ldots + M_k b_k, \qquad x'_0 = M_1 b'_1 + \ldots + M_k b'_k.$$

Если $x_0 \equiv x'_0 \pmod{M}$, то при любом $i, 1 \le i \le k$, выполняются сравнения $x_0 \equiv x'_0 \pmod{m_i}$. Учитывая, что $m_i | M_j$ при $j \ne i$, заключаем, что $M_i b_i \equiv M_i b'_i \pmod{m_i}$. Но тогда $a_i \equiv a'_i \pmod{m_i}$, т.е. $a_i$, $a'_i$ принадлежат одному классу вычетов по модулю $m_i$. Поскольку это доказано для любого индекса $i$, приходим к противоречию. □

**Следствие 5.2.** *Если числа $a_1, \ldots, a_k$ независимо друг от друга пробегают приведенные системы вычетов по модулям $m_1, \ldots, m_k$ соответственно, то числа $x_0$, определенные для каждого набора $a_1, \ldots, a_k$ с помощью равенств (5.10), пробегают приведенную систему вычетов по модулю $M = m_1 \cdots m_k$.*

*Доказательство.* Все числа $x_0$, полученные согласно условию, принадлежат различным классам вычетов по модулю $M$. Это доказано в следствии 5.1.

С помощью равенства (2.9) и сравнений (5.11) находим

$$(M, x_0) = (m_1, x_0) \cdots (m_k, x_0) = (m_1, a_1) \cdots (m_k, a_k).$$

Значит равенство $(x_0, M) = 1$ выполняется в том и только том случае, когда $(a_i, m_i) = 1$, $1 \leq i \leq k$. Это завершает доказательство следствия. □

Следствие 5.2 дает иное доказательство утверждения теоремы 3.3 о мультипликативности функции Эйлера $\varphi(n)$. Действительно, если числа $a_1, \ldots, a_k$ независимо друг от друга пробегают приведенные системы вычетов по модулям $m_1, \ldots, m_k$, то количество получившихся наборов равно $\varphi(m_1) \cdots \varphi(m_k)$. Согласно следствию 5.2 это число равно количеству классов вычетов по модулю $M$, состоящих из чисел, взаимно простых с $M$, т.е. равно $\varphi(M)$. В результате получается равенство $\varphi(M) = \varphi(m_1) \cdots \varphi(m_k)$ при условии, что числа $m_i$ попарно взаимно просты.

## 5.4 Полиномиальные сравнения по простому модулю

В этом параграфе мы рассмотрим сравнения вида

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}, \qquad p \nmid a_n, \qquad (5.13)$$

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

**Теорема 5.3.** *Сравнение (5.13) имеет не более $n$ решений.*

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

*Доказательство.* Докажем теорему индукцией по степени сравнения $n$. При $n = 1$ справедливость ее утверждения следует из теоремы 5.1.

Предположим теперь, что $n \geq 2$ и утверждение справедливо для всех сравнений степени меньшей $n$. Пусть $x_0$ – целое число, удовлетворяющее сравнению (5.13). Тогда $f(x_0) \equiv 0 \pmod{p}$ и

$$f(x) - f(x_0) = \sum_{k=1}^{n} a_k(x^k - x_0^k) = (x - x_0)g(x),$$

где $g(x) = a_n x^{n-1} + \ldots \in \mathbb{Z}[x]$. Из этого равенства следует, что для каждого целого числа $x_1$, удовлетворяющего сравнению (5.13) будет выполняться сравнение $(x_1 - x_0)g(x_1) \equiv 0 \pmod{p}$. Если при этом $x_0$, $x_1$ лежат в различных классах вычетов по модулю $p$, т.е. $p \nmid (x_1 - x_0)$, то будем иметь $g(x_1) \equiv 0 \pmod{p}$. Итак, каждое целое число, удовлетворяющее сравнению (5.13) и не лежащее в классе вычетов $\overline{x_0}$, будет удовлетворять сравнению $g(x) \equiv 0 \pmod{p}$. Согласно индуктивному предположению это сравнение имеет не более $n - 1$ решений. Отсюда следует, что существует не более $n$ классов вычетов по модулю $p$, элементы которых удовлетворяют сравнению (5.13). □

**Следствие 5.3.** *Для каждого простого числа $p$ справедливо сравнение*

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-p+1) \pmod{p}, \qquad (5.14)$$

*т.е. коэффициенты при одинаковых степенях переменной $x$ в левой и правой частях (5.14) сравнимы между собой по модулю $p$.*

*Доказательство.* Рассмотрим многочлен

$$f(x) = x^p - x - x(x-1)(x-2)\cdots(x-p+1) \in \mathbb{Z}[x].$$

Степень его, как легко видеть, не превосходит $p - 1$. Если $n$ – наибольшее целое число такое, что коэффициент при $x^n$ в многочлене $f(x)$ не делится на $p$, то степень сравнения $f(x) \equiv 0 \pmod{p}$ равна $n$. Для каждого целого числа $a$, $0 \leq a \leq p - 1$, согласно малой теореме Ферма имеем $f(a) = a^p - a \equiv 0 \pmod{p}$. Значит, количество решений сравнения $f(x) \equiv 0 \pmod{p}$ равно $p$. По теореме 5.3

выполняется неравенство $p \leq n$. Поскольку $n \leq p-1$, получаем противоречие, доказывающее, что все коэффициенты многочлена $f(x)$ делятся на $p$. Это завершает доказательство теоремы. □

Сравнивая коэффициенты при $x$ в первой степени слева и справа в сравнении (5.14), получаем теорему Вильсона $-1 \equiv (p-1)! \pmod{p}$.

**Теорема 5.4.** *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*

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

*совпадают. Другими словами, каждое сравнение (5.13) можно заменить равносильным ему сравнением степени не превосходящей* $p-1$.

*Доказательство.* Для каждого целого числа $a$ в силу малой теоремы Ферма имеем

$$f(a) = (a^p - a)g(a) + r(a) \equiv r(a) \pmod{p}.$$

Отсюда сразу же следует нужное утверждение. □

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 $\mathbb{F}_p$. Из следствия 5.3 получаем, что в кольце $\mathbb{F}_p[x]$ 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, как об этом говорилось выше, мы черточки не ставим.

**Пример.** Разделить с остатком многочлен $3x^3 + 2$ на многочлен $2x + 1$ в кольце $\mathbb{F}_5[x]$.

Так как $4 \cdot 2 \equiv 3 \pmod 5$, то в кольце многочленов $\mathbb{F}_5[x]$ справедливо равенство

$$3x^3 + 2 - 4x^2(2x + 1) = x^2 + 2.$$

Поскольку $3 \cdot 2 \equiv 1 \pmod 5$, имеем

$$x^2 + 2 - 3x(2x + 1) = 2x + 2$$

и

$$2x + 2 - (2x + 1) = 1.$$

Итак, в кольце $\mathbb{F}_5[x]$ справедливо равенство

$$3x^3 + 2 = (4x^2 + 3x + 1)(2x + 1) + 1. \tag{5.15}$$

Остаток от деления равен 1. Равенство (5.15), выполняющееся в кольце $\mathbb{F}_5[x]$, может быть переписано как сравнение в кольце многочленов $\mathbb{Z}[x]$

$$3x^3 + 2 \equiv (4x^2 + 3x + 1)(2x + 1) + 1 \pmod 5.$$

Здесь, как и ранее, имеется в виду, что коэффициенты при одинаковых степенях $x$ у многочленов, стоящих слева и справа от знака $\equiv$, сравнимы по модулю 5.

При любом простом $p$ в кольце многочленов $\mathbb{F}_p[x]$, выполняя деление с остатком, можно вычислять наибольший общий делитель двух многочленов. Этот алгоритм подобен алгоритму из параграфа 1.3 и также носит название алгоритм Евклида. Наибольший общий делитель многочленов $f(x)$ и $g(x)$ будет, как и для целых чисел, обозначаться символом $(f(x), g(x))$.

Следующее утверждение позволяет, не нарушая равносильности, понизить степень сравнения больше, чем теорема 5.4.

**Теорема 5.5.** *Пусть $f(x)$ и $d(x)$ многочлены с целыми коэффициентами, причем, если рассматривать их как многочлены из кольца $\mathbb{F}_p[x]$, то $d(x)$ есть наибольший общий делитель $f(x)$ и $x^p - x$. Тогда множества решений сравнений*

$$f(x) \equiv 0 \pmod p, \qquad \text{и} \qquad d(x) \equiv 0 \pmod p \tag{5.16}$$

*одинаковы.*

*Доказательство.* Согласно условию в кольце $\mathbb{F}_p[x]$ выполняется равенство $f(x) = d(x) \cdot h(x)$, где $h(x) \in \mathbb{F}_p[x]$. Заменяя коэффициенты многочлена $h(x)$ их наименьшими неотрицательными вычетами получим многочлен из кольца $\mathbb{Z}[x]$, мы сохраним для него обозначение $h(x)$, для которого выполнено сравнение

$$f(x) \equiv d(x) \cdot h(x) \pmod{p}.$$

Пусть для целого $a$ выполняется сравнение $d(a) \equiv 0 \pmod{p}$. Тогда имеем $f(a) \equiv d(a)h(a) \equiv 0 \pmod{p}$. Таким образом, целое число $a$ удовлетворяет первому из сравнений (5.16).

Подобно теореме 1.5 можно утверждать,что в кольце многочленов $F_p[x]$ найдутся многочлены $u(x), v(x)$, удовлетворяющие равенству $f(x)u(x) + (x^p - x)v(x) = d(x)$. Заменяя эти многочлены соответствующими многочленами из кольца $\mathbb{Z}[x]$, получаем сравнение

$$d(x) \equiv f(x)u(x) + (x^p - x)v(x) \pmod{p}.$$

Если для $a \in \mathbb{Z}$ выполнено сравнение $f(a) \equiv 0 \pmod{p}$, то согласно малой теореме Ферма имеем

$$d(a) \equiv f(a)u(a) + (a^p - a)v(a) \equiv 0 \pmod{p}.$$

Значит, $a$ есть решение второго из сравнений (5.16). Теорема доказана. □

Кольцо $\mathbb{F}_p[x]$ 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 $m(x) \in \mathbb{F}_p[x]$, полагая два многочлена $f(x), g(x) \in \mathbb{F}_p[x]$ 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 4.1.

**Пример.** Упростим сравнение

$$x^3 - 2x - 3 \equiv 0 \pmod{17} \tag{5.17}$$

с помощью теоремы 5.5. Вычислим для этого наибольший общий делитель многочленов $x^3 - 2x - 3$ и $x^{17} - x$ в кольце $\mathbb{F}_{17}[x]$. Имеем в кольце $\mathbb{F}_{17}[x]$ сравнения по модулю многочлена $x^3 - 2x - 3$ (для краткости мы опускаем модуль в обозначениях)

$$\begin{aligned} x^3 &\equiv 2x + 3, \\ x^4 &\equiv 2x^2 + 3x, \\ x^8 &\equiv (2x^2 + 3x)^2 \equiv 2x + 2, \\ x^{16} &\equiv (2x + 2)^2 \equiv 4x^2 + 8x + 4, \\ x^{17} &\equiv x(4x^2 + 8x + 4) \equiv 8x^2 - 5x - 5. \end{aligned}$$

Таким образом, в соответствии с алгоритмом Евклида

$$(x^{17} - x, x^3 - 2x - 3) = (8x^2 - 6x - 5, x^3 - 2x - 3).$$

Продолжая алгоритм Евклида, находим

$$\begin{aligned} x^3 - 2x - 3 + 2x(8x^2 - 6x - 5) &= 5x^2 + 5x - 3, \\ 5x^2 + 5x - 3 - 7(8x^2 - 6x - 5) &= -4x - 2 \end{aligned}$$

и

$$8x^2 - 6x - 5 = (4x + 2)(2x + 6).$$

Таким образом, искомый наибольший общий делитель равен $4x + 2$ или $2x + 1$. В соответствии с теоремой 5.5 сравнение (5.17) имеет те же решения, что и сравнение $2x + 1 \equiv 0 \pmod{17}$. Последнее сравнение имеет единственное решение $x \equiv 8 \pmod{17}$.

Заметим, что в этом примере для вычисления остатка $x^{17}$ по модулю $x^3 - 2x - 3$ использовался алгоритм, подобный алгоритму 4.1. Он может использоваться и в других случаях при больших $p$.

Далее в этом параграфе мы обсудим, как можно находить решения полиномиальных сравнений по простому модулю. Если модуль

$p$ не очень велик, это можно сделать перебором элементов какой-нибудь полной системы вычетов по модулю $p$.

**Пример.** Решить сравнение $x^2 + x + 1 \equiv 0 \pmod 7$. Многочлен $x^2 + x + 1$ при $x = -3, -2, -1, 0, 1, 2, 3$ принимает значения $7, 3, 1, 1, 3, 7, 13$ соответственно. Из них только значения в точках $-3, 2$ делятся на 7.

**Ответ:** Сравнение имеет два решения $x \equiv -3 \pmod 7, x \equiv 2 \pmod 7$.

В общем случае сравнение имеет смысл сначала упростить, пользуясь теоремой 5.5. Далее будем предполагать, что такое упрощение выполнено и многочлен $f(x)$ в сравнении (5.13) есть делитель многочлена $x^p - x = x(x^{p-1} - 1)$ в кольце $\mathbb{F}_p[x]$, а точнее – делитель многочлена $x^{p-1} - 1$. Кроме того, будем предполагать, что $p \geq 3$.

Описываемый ниже алгоритм носит вероятностный характер и эффективен на практике. Он строит множество $\mathcal{M}$, состоящее из различных делителей многочлена $f(x)$ в кольце $\mathbb{F}_p[x]$. При этом количество элементов в множестве $\mathcal{M}$ увеличивается до тех пор, пока оно не станет равным $n = \deg f(x)$.

**Алгоритм 5.1.** Данные: *Многочлен* $f(x) \in \mathbb{F}_p[x]$, $n = \deg f(x) \geq 2$, $f(x) | (x^{p-1} - 1)$. Найти: *Все корни многочлена* $f(x)$.

*1. Положить* $\mathcal{M} = \{f(x)\}$.
*2. Выбрать каким-либо способом элемент* $c \in \mathbb{F}_p$.
*3. Для каждого* $u(x) \in \mathcal{M}$ *с условием* $\deg u(x) > 1$ *выполнить следующие действия:*
*3.1. Если* $u(c) = 0$, *то исключить* $u(x)$ *из множества* $\mathcal{M}$ *и заменить его парой многочленов* $x - c$ *и* $u(x)/(x - c)$.
*3.2. Вычислить*

$$d(x) = (u(x), (x - c)^{\frac{p-1}{2}} - 1).$$

*3.3. Если* $1 \leq \deg d(x) < \deg u(x)$, *то исключить* $u(x)$ *из множества* $\mathcal{M}$ *и заменить его парой многочленов* $d(x)$ *и* $u(x)/d(x)$.

*3.4 Если $\#\mathcal{M} = n$, то алгоритм завершает работу. Множество $\mathcal{M}$ в этом случае состоит из всех многочленов вида $x - \gamma$, где $\gamma \in \mathbb{F}_P$ – корень многочлена $f(x)$.*
*4. Перейти к шагу 2.*

**Пример.** Решим сравнение $x^3 + 2x + 1 \equiv 0 \pmod{17}$.

В начальный момент имеем $\mathcal{M} = \{x^3 + 2x + 1\}$. При $c = -1$ с помощью алгоритма возведения в степень в кольце $\mathbb{F}_{17}[x]$, как и в предыдущем примере, находим сравнения по модулю $x^3 + 2x + 1$

$$(x+1)^4 \equiv 4x^2 - 5x - 3, \qquad (x+1)^8 \equiv 3x^2 + 9x - 2$$

и

$$((x+1)^8 - 1, x^3 + 2x + 1) = x - 3.$$

Разделив многочлен $x^3 + 2x + 1$ на $x - 3$, получаем

$$x^3 + 2x + 1 = (x - 3)(x^2 + 3x - 6).$$

После этого множество $\mathcal{M}$ принимает вид $\mathcal{M} = \{x - 3, x^2 + 3x - 6\}$. Точно так же при $c = 0$ находим

$$(x^8 - 1, x^2 + 3x - 6) = x + 8.$$

Разделив многочлен $x^2 + 3x - 6$ на $x + 8$, получаем

$$x^2 + 3x - 6 = (x + 8)(x - 5).$$

Множество $\mathcal{M}$ становится равным

$$\mathcal{M} = \{x - 3, x - 5, x + 8\}.$$

Множество решений данного сравнения имеет вид

$$x \equiv 3 \pmod{17}, \qquad x \equiv 5 \pmod{17}, \qquad x \equiv -8 \pmod{17}.$$

Конечно, все вычисления лучше выполнять с помощью калькулятора или компьютера.

Следующее утверждение объясняет, почему алгоритм достаточно быстро находит решения сравнения.

**Лемма 5.1.** *Пусть* $u(x) \mid f(x), \deg u(x) \geq 2$. *Вероятность того, что при случайном выборе* $c \in \mathbb{F}_p$, *количество элементов в множестве* $\mathcal{M}$ *в пункте 3 алгоритма увеличится, не меньше* $\frac{1}{2}$.

*Доказательство.* Из условия леммы, поскольку $u(x)|(x^{p-1}-1)$ следует, что $u(x)$ имеет в поле $\mathbb{F}_p$ не менее двух корней, причем все его корни различны. Пусть $\gamma_1, \gamma_2$ – корни многочлена $u(x)$.

Обозначим буквой $\mathcal{D}$ подмножество $F_p$, состоящее из элементов $t$, удовлетворяющих условиям

$$(t-\gamma_1)^{\frac{p-1}{2}} \neq (t-\gamma_2)^{\frac{p-1}{2}}.$$

По теореме Лагранжа многочлен $(x-\gamma_1)^{\frac{p-1}{2}} - (x-\gamma_2)^{\frac{p-1}{2}}$ имеет не более $\frac{p-3}{2}$ корней. Поэтому

$$\#\mathcal{D} \geq p - \frac{p-3}{2} = \frac{p+3}{2}.$$

Докажем, что для каждого $c \in \mathcal{D}$ алгоритм увеличивает количество многочленов в множестве $\mathcal{M}$. Если $c = \gamma_1$ или $c = \gamma_2$, это, очевидно, будет сделано в пункте 3.1. Далее будем считать, что обе разности $c - \gamma_i$ отличны от нуля. Каждый ненулевой элемент $b \in F_p$ согласно малой теореме Ферма удовлетворяет равенству

$$0 = b^{p-1} - 1 = (b^{\frac{p-1}{2}} - 1)(b^{\frac{p-1}{2}} + 1)$$

и, значит, удовлетворяет в точности одному из равенств $b^{\frac{p-1}{2}} = 1$ или $b^{\frac{p-1}{2}} = -1$.

Поскольку $c \in \mathcal{D}$, то

$$(c-\gamma_1)^{\frac{p-1}{2}} \neq (c-\gamma_2)^{\frac{p-1}{2}}$$

и, значит, одно из чисел $\gamma_1, \gamma_2$ будет корнем многочлена $(x-c)^{\frac{p-1}{2}} - 1$, а другое нет. Следовательно, в этом случае $1 \leq \deg d(x) < \deg u(x)$, т.е. $d(x)$ есть собственный делитель $u(x)$. Оцениваемая вероятность не меньше

$$\frac{\#\mathcal{D}}{p} \geq \frac{p+3}{2p} > \frac{1}{2}.$$

□

Лемма 5.1 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 $2^{-k}$.

## 5.5 Полиномиальные сравнения по составному модулю

Рассмотрим сначала случай, когда модуль сравнения есть степень простого числа $p$, т.е. $m = p^k, k \geq 2$. 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* $k \geq 2$ *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* $f(x) \equiv 0 \pmod{p}$*, которому принадлежит* $a$*.*

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, поиску решений по простому модулю. А во-вторых к поиску решений сравнения по модулю $p^k$, принадлежащих фиксированному решению по простому модулю.

Первый шаг обсуждался в предыдущем параграфе. Второй шаг основан на следующем утверждении.

**Теорема 5.6.** *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 $k \geq 1$ существует единственное решение сравнения $f(x) \equiv 0 \pmod{p^k}$, принадлежащее классу вычетов $x \equiv x_1 \pmod{p}$.*

*Доказательство.* Докажем теорему с помощью индукции по степени модуля $k$. При $k = 1$ утверждение, очевидно, выполняется.

Предположим утверждение теоремы справедливо для некоторого $k \geq 1$. Тогда существует единственное целое число $a$, удовлетворяющее условиям

$$f(a) \equiv 0 \pmod{p^k}, \quad 0 \leq a < p^k, \quad a \equiv x_1 \pmod{p}.$$

Найдем все такие целые числа $b$, что

$$f(b) \equiv 0 \pmod{p^{k+1}}, \quad 0 \leq b < p^{k+1}, \quad b \equiv x_1 \pmod{p}. \quad (5.18)$$

Первое из этих условий влечет $p^k | f(b)$ и, значит, наименьший неотрицательный вычет класса $b \pmod{p^k}$ равен $a$. Но тогда $b = a + p^k t$, с некоторым целым $t$, $0 \leq t < p$.

Многочлен

$$f(a + x) = c_0 + c_1 x + c_2 x^2 + \ldots \quad (5.19)$$

имеет целые коэффициенты. Подставляя в это равенство $x = 0$, находим $c_0 = f(a)$. А дифференцируя это равенство и так же подставляя 0 вместо $x$, получаем $c_1 = f'(a)$. При $x = p^k t$ из (5.19) следует сравнение $f(b) \equiv f(a) + f'(a)p^k t \pmod{p^{k+1}}$. Так как $p^k | f(a)$ и $p^{k+1} | f(b)$, то разделив обе части сравнения на $p^k$, получим

$$0 \equiv \frac{f(a)}{p^k} + f'(a)t \pmod{p}.$$

Учитывая теперь, что $a \equiv x_1 \pmod{p}$, заключаем, что $f'(a) \equiv f'(x_1) \pmod{p}$ и

$$f'(x_1)t + \frac{f(a)}{p^k} \equiv 0 \pmod{p}. \quad (5.20)$$

Согласно условию теоремы $p \nmid f'(x_1)$, так что по теореме 5.1 сравнение (5.20) разрешимо относительно $t$ и имеет единственное решение.

Решив это сравнение, мы найдем единственное число $b = a + p^k t$, удовлетворяющее условиям (5.18). Это завершает шаг индукции и вместе с ним доказательство теоремы. □

Приведенное доказательство позволяет находить решения сравнений по модулю, равному степени простого числа.

**Пример.** Решить сравнение $x^3 - 3x^2 - 1 \equiv 0 \pmod{125}$.

Решая сравнение $x^3 - 3x^2 - 1 \equiv 0 \pmod 5$, находим его решения $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 5$.

Найдем теперь числа, удовлетворяющие системе сравнений

$$x^3 - 3x^2 - 1 \equiv 0 \pmod{25}, \qquad x \equiv 2 \pmod 5.$$

Представив $x$ в виде $x = 2 + 5t$ и подставив это выражение в многочлен $f(x) = x^3 - 3x^2 - 1$, как и в доказательстве теоремы 5.6, находим

$$f(2) + f'(2)5t \equiv 0 \pmod{25}$$

или

$$-5 \equiv 0 \pmod{25}.$$

Получившееся сравнение решений относительно $t$ не имеет, поэтому данное сравнение не имеет решений, принадлежащих классу вычетов $x \equiv 2 \pmod 5$. Заметим, что в рассмотренном случае $f'(2) = 0$.

Теперь найдем числа, удовлетворяющие системе сравнений

$$x^3 - 3x^2 - 1 \equiv 0 \pmod{25}, \qquad x \equiv 4 \pmod 5. \tag{5.21}$$

Представив $x$ в виде $x = 4 + 5t$ и подставив это выражение в многочлен $f(x) = x^3 - 3x^2 - 1$, находим

$$15 + 24 \cdot 5t \equiv 0 \pmod{25}.$$

Сократив обе части этого сравнения на 5, получим сравнение $3 + 24t \equiv 0 \pmod 5$, равносильное сравнению $3 - t \equiv 0 \pmod 5$. Таким образом, $t = 3$ и система сравнений (5.21) имеет решение $x \equiv 19 \pmod{25} \equiv -6 \pmod{25}$. Здесь $19 = 4 + 5 \cdot 3$.

Продолжая действовать так же, как и в доказательстве теоремы 5.6, представим искомые $x$ в виде $x = -6 + 25t$. Учитывая, что $f(-6) = -325$ и $f'(-6) = 144$, приходим к сравнению

$$-325 + 144 \cdot 25t \equiv 0 \pmod{125}.$$

Сократив это сравнение на 25, получаем

$$-13 + 144t \equiv 0 \pmod{5}$$

или равносильное сравнение $2 - t \equiv 0 \pmod 5$. Ему удовлетворяет $t = 2$, так что решением исходного сравнения является класс вычетов по модулю 125, содержащий $-6 + 25 \cdot 2 = 44$.

**Ответ:** $x \equiv 44 \pmod{125}$.

Перейдем теперь к решению сравнений по произвольному составному модулю.

**Теорема 5.7.** *Пусть $f(x)$ – многочлен с целыми коэффициентами и $m_1 > 1, \ldots, m_k > 1$ – попарно взаимно простые числа. Множества целых чисел, удовлетворяющих сравнению*

$$f(x) \equiv 0 \pmod{m_1 \cdots m_k} \tag{5.22}$$

*и системе сравнений*

$$f(x) \equiv 0 \pmod{m_1}, \quad \ldots, \quad f(x) \equiv 0 \pmod{m_k} \tag{5.23}$$

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

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

*Доказательство.* Пусть $b$ – целое число, удовлетворяющее сравнению (5.22), т.е. $m_1 \cdots m_k | f(b)$. Тогда при любом $j, 1 \le j \le k$, выполняется $m_j | f(b)$ или $f(b) \equiv 0 \pmod{m_j}$. Значит, $b$ удовлетворяет системе сравнений (5.23).

Докажем обратное утверждение. Если $b$ удовлетворяет системе сравнений (5.23), то $m_j | f(b)$ при любом $j, 1 \le j \le k$. Числа

$m_1, \ldots, m_k$ попарно взаимно просты. Пользуясь следствием 2.6, заключаем, что $m_1 \cdots m_k | f(b)$ и, значит, $b$ удовлетворяет сравнению (5.22).

Пусть $a_1, \ldots, a_k$ – целые числа, удовлетворяющие сравнениям (5.23) соответственно. Согласно теореме 5.2 система сравнений

$$x \equiv a_1 \pmod{m_1}, \quad \ldots, \quad x \equiv a_k \pmod{m_k}$$

разрешима, и целое число $x_0$, определенное равенством (5.10), удовлетворяет этой системе. Тогда при любом $j$ имеем $f(x_0) \equiv f(a_j) \equiv 0 \pmod{m_j}$, т.е. $x_0$ удовлетворяет системе сравнений (5.23), и по доказанному удовлетворяет сравнению (5.22).

Если числа $a_1, \ldots, a_k$ независимо друг от друга пробегают классы вычетов, состоящие из решений соответствующих сравнений (5.23), то по следствию 5.1 числа $x_0$, определенные равенством (5.10), пробегают различные классы вычетов по модулю $m_1 \cdots m_k$. Эти классы вычетов, по доказанному состоят из чисел, удовлетворяющих сравнению (5.22). Значит, число решений этого сравнения не меньше, чем $N(m_1) \cdots N(m_k)$.

По доказанному выше каждое целое число $b$, удовлетворяющее сравнению (5.22) удовлетворяет системе сравнений (5.23) и потому при каждом $j$ класс вычетов $b \pmod{m_j}$ есть решение сравнения $f(x) \equiv 0 \pmod{m_j}$. Это доказывает, что никаких решений, отличных от построенных $N(m_1) \cdots N(m_k)$ решений, сравнение (5.22) не имеет. □

Приведенное выше доказательство теоремы 5.7 позволяет находить решения сравнения (5.22) при составном модуле $m$. А именно, если $m = p_1^{r_1} \cdots p_k^{r_k}$ – разложение в произведение различных простых чисел, то найдя числа, $a_1, \ldots, a_k$, удовлетворяющие сравнениям $f(x) \equiv 0 \pmod{p_j^{r_j}}$ при $1 \leq j \leq k$ и выбрав $x_0$ с помощью равенства (5.10), мы найдем некоторое решение $x_0 \pmod{m}$ сравнения (5.22). Более того, так будут найдены все решения, если каждое из чисел $a_1, \ldots, a_k$ независимо будет пробегать все решения своего сравнения.

**Пример.** Решить сравнение $x^3 - x^2 + 2x + 1 \equiv 0 \pmod{75}$.

Справедливо разложение $75 = 3 \cdot 5^2$. Сравнение $x^3 - x^2 + 2x + 1 \equiv 0 \pmod 3$ имеет два решения $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 3$. Сравнение $x^3 - x^2 + 2x + 1 \equiv 0 \pmod 5$ имеет единственное решение $x \equiv 3 \pmod 5$. Для того, чтобы решить сравнение

$$x^3 - x^2 + 2x + 1 \equiv 0 \pmod{25} \tag{5.24}$$

представим $x$ в виде $x = 3 + 5t$. Для вычисления $t$ получаем, как это было указано выше, сравнение $25 + 23 \cdot 5t \equiv 0 \pmod{25}$. Таким образом, $t = 0$ и сравнение (5.24) имеет единственное решение $x \equiv 3 \pmod{25}$.

В соответствии с теорией для решения исходного сравнения нужно найти решения двух систем сравнений

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 3 \pmod{25}, \end{cases} \qquad \begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod{25}. \end{cases}$$

Первая из них имеет решение $x \equiv 28 \pmod{75}$, а вторая $x \equiv 53 \pmod{75}$. Два найденных класса вычетов и составляют ответ к задаче.

# Глава 6

# Сравнения второй степени

В предыдущей главе решение полиномиальных сравнений по произвольному модулю было сведено к такой же задаче для сравнений по простому модулю. В настоящей главе обсуждаются вопросы, связанные с разрешимостью сравнений второй степени по простому модулю, и приложения доказанных результатов к исследованию некоторых диофантовых уравнений. В дальнейшем считается, что простое число $p$ нечетно.

## 6.1 Сравнения второй степени по простому модулю

Каждое сравнение второй степени

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad p \nmid a, \tag{6.1}$$

можно упростить, изменив его коэффициенты и сделав замену переменной.

Умножив обе части сравнения (6.1) на число $4a$, не делящееся на $p$, получим равносильное сравнение

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}.$$

Его можно переписать в виде $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$ или в виде

$$y^2 \equiv D \pmod{p}, \tag{6.2}$$

где использованы обозначения $y = 2ax + b$ и $D = b^2 - 4ac$.

Так как $p \nmid 2a$, то сравнение

$$2ax + b \equiv y \pmod{p}$$

при любом целом $y$ имеет единственное решение относительно $x$. Это устанавливает взаимно однозначное соответствие между решениями сравнения (6.1) относительно $x$ и сравнения (6.2) относительно $y$.

Из сказанного следует, что в дальнейшем можно рассматривать лишь сравнения вида

$$x^2 \equiv a \pmod{p}. \tag{6.3}$$

По теореме 5.3 сравнение (6.3) имеет не более двух решений. Если это сравнение разрешимо и $a \not\equiv 0 \pmod{p}$, то число решений равно двум. Действительно, вместе с решением $x_0 \pmod{p}$ сравнение будет иметь решением и класс вычетов $-x_0 \pmod{p}$, причем эти классы вычетов различны. В противном случае мы имели бы $x_0 \equiv -x_0 \pmod{p}$ и $p|x_0$. Но тогда $p|a$, что противоречит условию. Таким образом, при $a \not\equiv 0 \pmod{p}$ сравнение (6.3) либо не имеет решений, либо имеет два решения. В случае $a \equiv 0 \pmod{p}$ сравнение имеет единственное решение $x \equiv 0 \pmod{p}$.

Установленное выше взаимно однозначное соответствие между множествами решений сравнений (6.1) и (6.2) позволяет утверждать, что и в общем случае при $p|D = b^2 - 4ac$ сравнение (6.1) имеет единственное решение. Если же $p \nmid D$, то сравнение (6.1) либо имеет два решения, либо не имеет их вовсе.

Легко проверить, что сравнение $x^2 \equiv -1 \pmod{3}$ не имеет решений, а сравнение $x^2 \equiv -1 \pmod{5}$ имеет два решения $x \equiv 2 \pmod{5}$ и $x \equiv 3 \pmod{5}$.

Целое число $a$ называется *квадратичным вычетом* по модулю $p$, если сравнение (6.3) имеет решение. Если же это сравнение не имеет решений, число $a$ называется *квадратичным невычетом* по модулю $p$. Числа, сравнимые между собой, одновременно являются квадратичными вычетами или квадратичными невычетами.

Число $-1$ есть квадратичный невычет по модулю 3. Оно же является квадратичным вычетом по модулю 5.

**Лемма 6.1.** *Любая приведенная система вычетов по модулю $p$ содержит $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов. Целое число $a$, не делящееся на $p$ будет квадратичным вычетов в том и только том случае, когда*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{6.4}$$

*и квадратичным невычетом в том и только том случае, когда*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{6.5}$$

*Доказательство.* Пусть $a$ – квадратичный вычет. Тогда с некоторым целым числом $b$, не делящимся на $p$, выполняется сравнение $b^2 \equiv a \pmod{p}$. Возводя обе части этого сравнения в степень $\frac{p-1}{2}$, и пользуясь малой теоремой Ферма, находим

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

Таким образом, каждый квадратичный вычет удовлетворяет сравнению $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$. Согласно теореме 5.3 можно утверждать, что существует не более $\frac{p-1}{2}$ классов вычетов, состоящих из квадратичных вычетов.

Числа

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2, \tag{6.6}$$

очевидно, являются квадратичными вычетами. Они не сравнимы друг с другом по модулю $p$. В противном случае нашлись бы два числа $k_1, k_2$, удовлетворяющие условиям

$$p|(k_1^2 - k_2^2) = (k_1 - k_2)(k_1 + k_2), \qquad 1 \le k_2 < k_1 \le \frac{p-1}{2}.$$

Но указанная делимость невозможна, ведь сумма $k_1 + k_2$ и разность $k_1 - k_2$ не делятся на $p$, они положительны, но меньше, чем $p - 1$.

Итак, существует не менее $\frac{p-1}{2}$ классов вычетов по модулю $p$, состоящих из квадратичных вычетов.

Из доказанного следует, что квадратичные вычеты образуют ровно $\frac{p-1}{2}$ классов вычетов и удовлетворяют сравнению (6.4).

Но тогда квадратичные невычеты составляют оставшиеся $\frac{p-1}{2}$ классов вычетом, состоящих из чисел, не делящихся на $p$, а каждая приведенная система вычетов по модулю $p$ содержит ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов.

Если $a$ – квадратичный невычет, то по доказанному $p \nmid a^{\frac{p-1}{2}} - 1$. По малой теореме Ферма имеем

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

Следовательно, $p | a^{\frac{p-1}{2}} + 1$ и, значит, выполнено сравнение (6.5). $\square$

## 6.2 Символ Лежандра и его свойства

Символ Лежандра $\left(\frac{a}{p}\right)$ есть функция, принимающая три значения: $-1, 0, 1$. Ее аргументами являются простое нечетное число $p$ и целое число $a$.

**Определение 6.**

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \textit{если } a\textit{-квадратичный невычет по модулю } p \\ 0, & \textit{если } p/a \\ 1, & \textit{если } a\textit{-квадратичный вычет по модулю } p \end{cases}$$

Свойства символа Лежандра описывает следующая теорема.

**Теорема 6.1.** *Пусть $a, b$ – произвольные целые числа. Тогда*

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. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
4. *Кроме того* $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

*Доказательство.* Первое утверждение теоремы совпадает со вторым утверждением леммы 6.1.

Если $a \equiv b \pmod{p}$, то множества решений сравнений $x^2 \equiv a \pmod{p}$ и $x^2 \equiv b \pmod{p}$, очевидно, совпадают. Отсюда следует, что эти сравнения разрешимы или неразрешимы одновременно, что доказывает второе утверждение теоремы.

С помощью первого утверждения находим следующие сравнения по модулю $p$

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

Левая и правая части получившегося сравнения равны $\pm 1$ или 0. Поэтому их разность не превосходит 2 и делится на $p > 2$. Следовательно их разность равна 0. Третье утверждение доказано.

Сравнение $x^2 \equiv 1 \pmod{p}$ при любом простом нечетном $p$ разрешимо.Решением является класс вычетов $x \equiv 1 \pmod{p}$. Поэтому $\left(\frac{1}{p}\right) = 1$.

Из первого утверждения теоремы при $a = -1$ следует

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

Абсолютная величина разности левой и правой частей этого сравнения не превосходит 2 и делится на нечетное простое число $p$. Значит, эта разность равна нулю, что доказывает справедливость последнего утверждения теоремы. □

Из последнего утверждения теоремы 6.1 следует, например, что сравнение $x^2 + 1 \equiv 0 \pmod{p}$, где $p$ – простое нечетное число, разрешимо в том и только том случае, когда $p \equiv 1 \pmod{4}$.

## 6.3 Квадратичный закон взаимности

Утверждение, называемое *квадратичный закон взаимности* впервые сформулировал Эйлер в 1783г, а в 1796г. Гаусс дал первое его

доказательство.

**Теорема 6.2 (Квадратичный закон взаимности).** *Если $p$ и $q$ - различные простые нечётные числа, то*

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

Другими словами,

$$\begin{aligned} \left(\tfrac{p}{q}\right) &= \left(\tfrac{q}{p}\right), \quad \text{если } p \equiv 1 \pmod 4 \text{ или } q \equiv 1 \pmod 4, \\ \left(\tfrac{p}{q}\right) &= -\left(\tfrac{q}{p}\right), \quad \text{если } p \equiv 3 \pmod 4 \text{ и } q \equiv 3 \pmod 4. \end{aligned}$$

Можно также сказать, что в первом случае сравнения $x^2 \equiv a \pmod p$ и $x^2 \equiv b \pmod p$ разрешимы или неразрешимы одновременно, а во втором случае из разрешимости одного из этих сравнений следует неразрешимость другого.

Квадратичный закон взаимности вместе со свойствами из теоремы 6.1 позволяют вычислять символ Лежандра и тем устанавливать разрешимость или неразрешимость квадратичных сравнений. Некоторые примеры будут рассмотрены в конце параграфа.

Перед тем как доказывать теорему 6.2 установим одно вспомогательное утверждение и выведем следствие из него. В этом утверждении используется тот факт, что совокупность чисел

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$$

составляет приведённую систему вычетов по модулю $p$.

**Лемма 6.2 (Лемма Гаусса).** *Пусть $p$ – простое нечетное число и $a$ – целое число, не делящееся на $p$. Для каждого $k = 1, 2 \ldots, \frac{p-1}{2}$, определим $\varepsilon_k = \pm 1$ условиями*

$$k \cdot a \equiv \varepsilon_k \cdot r_k \pmod p, \qquad 0 < r_k \leq \frac{p-1}{2}. \tag{6.7}$$

*Тогда*

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} = (-1)^t,$$

*где* $t$ *- количество отрицательных среди чисел* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{p-1}{2}}$.

*Доказательство.* Докажем сначала, что все числа $r_k$, определенные в (6.7), не сравнимы друг с другом по модулю $p$. Предположим, что для некоторых индексов $k > \ell$ выполняется сравнение $r_k \equiv r_\ell \pmod p$. Тогда согласно определению имеем $ka \equiv \pm\ell a \pmod p$ и, значит, $p|(k \mp l)$. Но этого быть не может, так как $0 < |k \pm l| \leq p-1$. Отсюда следует, что набор чисел $\{r_1, \ldots, r_{\frac{p-1}{2}}\}$ лишь перестановкой отличается от набора $\{1, 2 \ldots, \frac{p-1}{2}\}$. Перемножая все сравнения (6.7), и пользуясь равенством $r_1 \cdots r_{\frac{p-1}{2}} = \left(\frac{p-1}{2}\right)!$, получим:

$$\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \cdot \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} \pmod p.$$

Сократив это сравнение на не кратное $p$ целое число $\left(\frac{p-1}{2}\right)!$ и пользуясь первым утверждением теоремы 6.1, находим $\left(\frac{a}{p}\right) \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} \pmod p$. Учитывая, что разность левой и правой частей этого сравнения по абсолютной величине не превосходит 2, получаем утверждение леммы. □

**Следствие 6.1.** *1)* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

*2) Если* $a$ *нечётно, то* $\left(\frac{a}{p}\right) = (-1)^S$, *где* $S = \sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]$.

*Доказательство.* Неполное частное от деления числа $ak$ на $p$ равно $\left[\frac{ak}{p}\right]$. Поэтому

$$ak - p\left[\frac{ak}{p}\right] = \begin{cases} r_k & , \text{ если } \varepsilon_k = 1 \\ p - r_k & , \text{ если } \varepsilon_k = -1 \end{cases}$$

Суммируем эти равенства при всех $k = 1, 2, \ldots, \frac{p-1}{2}$, учитывая, что $1 + 2 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8}$ и пользуясь обозначениями леммы 6.2. В

результате получим

$$\frac{p^2-1}{8}\cdot a - p\cdot S = t\cdot p + \sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k \cdot r_k.$$

Перейдем в этом равенстве к сравнению по модулю 2. Заметив, что

$$\sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k \cdot r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} r_k = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8} \pmod 2, \qquad p \equiv -1 \pmod 2,$$

получаем $\frac{p^2-1}{8}\cdot a + S \equiv t + \frac{p^2-1}{8} \pmod 2$, то есть

$$t \equiv S + (a-1)\cdot\frac{p^2-1}{8} \pmod 2. \tag{6.8}$$

При $a = 2$ все слагаемые в сумме, определяющей $S$ равны нулю. Поэтому $S = 0$ и $t \equiv \frac{p^2-1}{8} \pmod 2$. В силу леммы Гаусса это доказывает первый пункт следствия.

Если $a$ - нечётно, то согласно (6.8) имеем $t \equiv S \pmod 2$, что в силу леммы Гаусса доказывает второй пункт следствия. □

*Доказательство теоремы 6.2.* По следствию 6.1 выполняются равенства $\left(\frac{q}{p}\right) = (-1)^{S_1}$ и $\left(\frac{p}{q}\right) = (-1)^{S_2}$, где

$$S_1 = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right], \qquad S_2 = \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right].$$

Поэтому

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{S_1+S_2},$$

и достаточно доказать равенство

$$S_1 + S_2 = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

При фиксированном целом $x$ из интервала $0 < x \le \frac{p-1}{2}$ величина $\left[\frac{qx}{p}\right]$ есть количество целых точек $y$ на промежутке $0 < y \le \frac{qx}{p}$ или,

учитывая, что $\frac{qx}{p}$ не есть целое число, – на промежутке $0 < y < \frac{qx}{p}$. Отсюда следует, что $S_1$ равно количеству пар целых чисел $x, y$, удовлетворяющих неравенствам

$$0 < x \leq \frac{p-1}{2}, \qquad 0 < y < \frac{qx}{p}.$$

Поскольку $\frac{p}{2}$ не целое число, и $\frac{qx}{p} < \frac{q}{2}$, заключаем, что $S_1$ есть количество точек $(x, y) \in \mathbb{Z}^2$ с условиями

$$0 < x < \frac{p}{2}, \qquad 0 < y < \frac{q}{2}, \qquad py - qx < 0.$$

Точно так же, число $S_2$ равно количеству точек $(x, y) \in \mathbb{Z}^2$ в прямоугольнике

$$T = \{(x, y) \mid 0 < x < \frac{p}{2}, \quad 0 < y < \frac{q}{2}\}$$

с условием $qx - py < 0$. Последнее условие может быть переписано в виде $py - qx > 0$.

Ни одна из точек $(x, y) \in \mathbb{Z}^2$ прямоугольника $T$ не лежит на прямой линии $py - qx = 0$, поэтому сумма $S_1 + S_2$ равна количеству точек с целыми координатами, лежащих в $T$, т.е. $\frac{p-1}{2} \cdot \frac{q-1}{2}$. □

Рассмотрим несколько примеров.

**Пример.** *Разрешимо ли сравнение* $x^2 \equiv 53 \pmod{233}$ *?*

Так как $53 = 1 + 4 \cdot 13$ и $233 = 4 \cdot 53 + 21$, то, применяя квадратичный закон взаимности и второе свойство из теоремы 6.1, находим

$$\left(\frac{53}{233}\right) = \left(\frac{233}{53}\right) = \left(\frac{21}{53}\right).$$

Пользуясь третьим свойством из теоремы 6.1 и опять применяя квадратичный закон взаимности, получаем

$$\left(\frac{21}{53}\right) = \left(\frac{7}{53}\right) \cdot \left(\frac{3}{53}\right) = \left(\frac{53}{7}\right) \cdot \left(\frac{53}{3}\right).$$

Далее, учитывая, что $53 = 7 \cdot 7 + 4$ и $53 = 3 \cdot 18 - 1$, имеем

$$\left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1, \qquad \left(\frac{53}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1,$$

и, наконец,

$$\left(\frac{53}{233}\right) = 1 \cdot (-1) = -1.$$

Таким образом, данное сравнение не имеет решений.

**Пример.** *Для каких простых чисел $p$ разрешимо сравнение*

$$x^2 + 3 \equiv 0 \pmod{p} \ ?$$

При $p = 2$ решение существует $x \equiv 1 \pmod{p}$. При $p = 3$ решением является класс вычетов $x \equiv 0 \pmod{p}$.
Рассмотрим далее случай $p > 3$. Согласно теоремам 6.1 и 6.2 справедливы равенства

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

Поскольку

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{3}, \\ -1, & \text{если } p \equiv 2 \pmod{3}, \end{cases}$$

заключаем, что равенство $\left(\frac{-3}{p}\right) = 1$ для простых чисел $p > 3$ выполняется лишь при $p \equiv 1 \pmod{3}$. Учитывая, что $p$ нечетно, последнее сравнение можно переписать в виде $p = 6n + 1, n \in \mathbb{Z}$. Итак, данное сравнение разрешимо лишь при $p = 2, 3$ и всех простых числах вида $6n + 1$.

Последний пример может быть обобщен.

**Теорема 6.3.** *Множество всех простых чисел $p$, для которых разрешимо сравнение*

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad p \nmid a, \tag{6.9}$$

*состоит из некоторых делителей числа* $2D$, *где* $D = b^2 - 4ac$, *а также из простых, лежащих в нескольких классах вычетов по модулю* $4|D|$.

*Доказательство.* Достаточно рассматривать только простые числа $p$, не делящие $2D$. Как указывалось выше, существует взаимно однозначное соответствие между решениями сравнения (6.9) и решениями сравнения $x^2 \equiv D \pmod{p}$. Последнее сравнение разрешимо лишь для тех простых чисел $p$, для которых выполняется равенство $\left(\frac{D}{p}\right) = 1$. Для завершения доказательства теоремы достаточно установить, что множество нечетных простых чисел $p$, для которых $\left(\frac{D}{p}\right) = 1$, состоит из нескольких классов вычетов по модулю $4|D|$. Это равносильно утверждению, что для простых из одного класса вычетов по модулю $4|D|$ сравнение $x^2 \equiv D \pmod{p}$ разрешимо или неразрешимо одновременно, т.е. сравнение $p_1 \equiv p_2 \pmod{4|D|}$ влечет за собой $\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right)$.

Пусть $D = (-1)^{\alpha_1} \cdot 2^{\alpha_2} \cdot \prod\limits_q q^{\alpha_q}$ – разложение числа $D$ в произведение простых сомножителей (с учетом знака). Тогда

$$\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right)^{\alpha_1} \cdot \left(\frac{2}{p}\right)^{\alpha_2} \cdot \prod_q \left(\frac{q}{p}\right)^{\alpha_q}. \tag{6.10}$$

Рассмотрим несколько случаев.

1) Так как $p_1 \equiv p_2 \pmod{4}$, то $\frac{p_1-1}{2} \equiv \frac{p_2-1}{2} \pmod{2}$ и по четвертому утверждению теоремы 6.1 выполняется равенство $\left(\frac{-1}{p_1}\right) = \left(\frac{-1}{p_2}\right)$.

2) Допустим, что $\alpha_2 \geq 1$. Тогда $D$ делится на 2, следовательно $p_1 \equiv p_2 \pmod{8}$ и

$$\frac{p_1^2 - 1}{8} - \frac{p_2^2 - 1}{8} = \frac{p_1 - p_2}{8} \cdot (p_1 + p_2) \equiv 0 \pmod{2}.$$

По первому утверждению следствия 6.1 получаем $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right)$ и, значит, при любом $\alpha_2 \geq 0$ выполняется равенство $\left(\frac{2}{p_1}\right)^{\alpha_2} = \left(\frac{2}{p_2}\right)^{\alpha_2}$.

3) Пусть теперь $q|D$. Из сравнения $p_1 \equiv p_2 \pmod{4|D|}$ следует $p_1 \equiv p_2 \pmod{q}$, так что $\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right)$. В то же время $p_1 \equiv p_2 \pmod{4}$, поэтому

$$\frac{p_1-1}{2}\cdot\frac{q-1}{2} - \frac{p_2-1}{2}\cdot\frac{q-1}{2} = (q-1)\cdot\frac{p_1-p_2}{4} \equiv 0 \pmod{2}.$$

Теперь с помощью квадратичного закона взаимности находим

$$\left(\frac{q}{p_1}\right) = \left(\frac{p_1}{q}\right)\cdot(-1)^{\frac{p_1-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{p_2}{q}\right)\cdot(-1)^{\frac{p_2-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{q}{p_2}\right),$$

т.е. $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right)$.

Из равенств, доказанных в пунктах 1)–3) с помощью (6.10) находим $\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right)$. □

Заметим, что во многих случаях модуль $4|D|$ может быть уменьшен. Например, его можно заменить любым числом $4K$ с условием, что $\frac{|D|}{K}$ есть квадрат целого числа.

## 6.4 Символ Якоби и его свойства

Символ Лежандра определен только для пар целых чисел $a, p$, у которых $p$ есть простое нечетное число. Определение можно распространить на большее множество пар целых чисел и построить таким способом функцию, называемую символом Якоби. Одним из важных свойств символа Якоби является возможность вычислять его значения, не используя весьма трудоемкую операцию разложения чисел на множители. В частности это дает быстрый способ вычисления значений символа Лежандра.

Пусть $P$ - положительное нечётное число и $P = p_1 \cdots p_r$ его разложение в произведение простых чисел, не обязательно различных. Определим для каждого целого числа $a$ *символ Якоби* $\left(\frac{a}{P}\right)$ равенством

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

где справа стоит произведение символов Лежандра.

Следует отметить, что символ Якоби не имеет отношения к разрешимости квадратичных сравнений. Например,

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

но сравнение $x^2 \equiv 2 \pmod{15}$ не имеет решений, ведь $\left(\frac{2}{3}\right) = -1$ и, значит, ни при каком целом $x$ число $x^2 - 2$ не делится на 3. Тем более оно не делится на 15.

В дальнейшем буквой $P$ будет обозначаться некоторое положительное нечетное число. Основные свойства символа Лежандра описывает

**Теорема 6.4.** *1) Если целые числа $a, b$ взаимно просты с $P$ и удовлетворяют сравнению $a \equiv b \pmod{P}$, то $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.*
*2) Для любых целых чисел $a, b$, взаимно простых с $P$ выполняется равенство $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right)$.*
*3) Справедливы равенства*

$$\left(\frac{1}{P}\right) = 1, \qquad \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

*4) Для любых двух положительных нечетных взаимно простых чисел $P, Q$ имеет место равенство $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$.*

Заметим, что для каждого нечетного числа $u$ дробь $\frac{u^2-1}{8}$ есть целое число. Действительно $u^2 - 1 = (u-1)(u+1)$ есть произведение двух последовательных целых чисел. Одно из них делится на 4, а другое на 2.

**Лемма 6.3.** *Для любых нечетных целых чисел $u_1, \ldots, u_m$ справедливы сравнения*
*1)* $\frac{u_1 \cdots u_m - 1}{2} \equiv \sum_{i=1}^{m} \frac{u_i - 1}{2} \pmod{2}$
*2)* $\frac{u_1^2 \cdots u_m^2 - 1}{8} \equiv \sum_{i=1}^{m} \frac{u_i^2 - 1}{8} \pmod{8}$.

*Доказательство.* Рассмотрим сначала случай $m = 2$, обозначая для краткости $u = u_1, v = u_2$. Справедливо сравнение

$$uv - 1 - (u-1) - (v-1) = (u-1)(v-1) \equiv 0 \pmod 4.$$

Разделив обе части его и модуль на 2, получаем первое утверждение. Для доказательства второго утверждения разделим обе части и модуль сравнения

$$u^2v^2 - 1 - (u^2-1) - (v^2-1) = (u^2-1)(v^2-1) \equiv 0 \pmod{64}$$

на 8.

По доказанному при любом $m \geq 3$ справедливы сравнения

$$\frac{u_1 \cdots u_m - 1}{2} \equiv \sum_{i=1}^{m-1} \frac{u_1 \cdots u_{m-1} - 1}{2} + \frac{u_m - 1}{2} \pmod 2,$$

$$\frac{u_1^2 \cdots u_m^2 - 1}{8} \equiv \sum_{i=1}^{m-1} \frac{u_1^2 \cdots u_{m-1}^2 - 1}{8} + \frac{u_m^2 - 1}{8} \pmod 8,$$

Оба утверждения леммы следуют отсюда с помощью математической индукции. □

*Доказательство теоремы 6.4.* Пусть $P = p_1 \cdots p_r$ – разложение в произведение простых чисел. Тогда для любых $a \equiv b \pmod P$ имеем $a \equiv b \pmod{p_i}$, $i = 1, \ldots, r$, и согласно определению и теореме 6.1 получаем

$$\left(\frac{a}{P}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right) = \left(\frac{b}{P}\right).$$

Это доказывает первое утверждение.

Справедливы равенства

$$\left(\frac{ab}{P}\right) = \prod_{i=1}^{m} \left(\frac{ab}{p_i}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right) \cdot \left(\frac{b}{p_i}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right),$$

доказывающие второе утверждение.

Пользуясь определением символа Якоби, теоремой 6.1 и леммой 6.3, находим

$$\left(\frac{1}{P}\right) = \prod_{i=1}^{r}\left(\frac{1}{p_i}\right) = 1,$$

$$\left(\frac{-1}{P}\right) = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r}(-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{P-1}{2}},$$

$$\left(\frac{2}{P}\right) = \prod_{i=1}^{r}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{r}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\frac{P^2-1}{8}}.$$

Пусть теперь $P, Q$ – положительные нечетные взаимно простые числа и $P = p_1 \cdots p_r$, $Q = q_1 \cdots q_s$ – их разложения в произведения простых чисел. Пользуясь определением символа Якоби, вторым утверждением теоремы и квадратичным законом взаимности, находим

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}. \qquad (6.11)$$

Согласно лемме 6.3 имеет место сравнение

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

$$\equiv \frac{P-1}{2}\cdot\frac{Q-1}{2} \pmod 2,$$

доказывающее вместе с (6.11) последнее утверждение теоремы. □

Вычислим с помощью теоремы 6.4 символ Якоби $\left(\frac{53}{233}\right)$, совпадающий, поскольку 233 – простое число, с соответствующим символом Лежандра. Имеем, пользуясь утверждениями 1), 3) и 4) этой теоре-

мы,

$$\left(\frac{53}{233}\right) = \left(\frac{233}{53}\right) = \left(\frac{21}{53}\right) = \left(\frac{53}{21}\right) = \left(\frac{11}{21}\right) = \\ = \left(\frac{21}{11}\right) = \left(\frac{-1}{11}\right) = -1,$$

что, конечно, совпадает с результатом предыдущих вычислений.

Способ вычисления символа Якоби, примененный в рассмотренном примере, может быть оформлен в виде общего алгоритма полиномиальной сложности.

## 6.5 Суммы двух и четырех квадратов

Этот параграф посвящен применению сравнений для исследования диофантовых уравнений специального вида. Сначала мы рассмотрим уравнение вида

$$x^2 + y^2 = n, \tag{6.12}$$

где предполагается, что $n$ - заданное целое положительное число. Решения $(x, y)$ этого уравнения также будут предполагаться целыми числами.

Не при всяком натуральном $n$ это уравнение имеет решения. Например, любое решение в целых числах уравнения $x^2+y^2 = 7$ должно удовлетворять неравенствам $|x| \leq 2, |y| \leq 2$. Перебирая последовательно все пары чисел, удовлетворяющих этим неравенствам, можно убедиться, что ни одна из них не есть решение уравнения.

Сначала мы рассмотрим уравнение вида (6.12) в предположении, что его правая часть есть простое число $p$.

**Лемма 6.4.** *Если $p$ – простое число вида $4k + 1$, то уравнение*

$$x^2 + y^2 = p$$

*разрешимо в целых числах $(x, y)$.*

*Доказательство.* Для простого числа $p = 4k + 1$ символ Лежандра $\left(\frac{-1}{p}\right)$ равен 1, и, значит, найдется целое число $a$, удовлетворяющее сравнению $a^2 \equiv -1 \pmod{p}$. Для любых целых чисел $x, y$ справедливы сравнения

$$x^2 + y^2 \equiv x^2 - a^2y^2 = (x - ay)(x + ay) \pmod{p}. \tag{6.13}$$

Рассмотрим всевозможные пары целых чисел $(x, y)$, удовлетворяющие условиям

$$0 \le x \le [\sqrt{p}], \qquad 0 \le y \le [\sqrt{p}], \tag{6.14}$$

и для каждой такой пары найдем класс вычетов $(x + ay) \pmod{p}$. Количество получившихся при этом классов вычетов не превосходит $p$, в то время как количество пар $(x, y)$ равно

$$(1 + [\sqrt{p}]) \cdot (1 + [\sqrt{p}]) > \sqrt{p} \cdot \sqrt{p} = p.$$

Это значит, что найдутся по крайней мере две пары $(x_1, y_1)$, $(x_2, y_2)$, удовлетворяющие условиям (6.14), для которых классы вычетов $(x_i + ay_i) \pmod{p}, i = 1, 2$, совпадают. Таким образом, $x_1 + ay_1 \equiv x_2 + ay_2 \pmod{p}$ или $(x_1 - x_2) + a(y_1 - y_2) \equiv 0 \pmod{p}$. Обозначив для краткости $x_0 = x_1 - x_2, y_0 = y_1 - y_2$, с помощью (6.13) получим

$$x_0^2 + y_0^2 \equiv (x_0 + ay_0)(x_0 - ay_0) \equiv 0 \pmod{p},$$

т.е. число $x_0^2 + y_0^2$ делится на $p$.

Условия (6.14) означают, что числа $x_0, y_0$ не очень велики, а именно,

$$|x_0| = |x_1 - x_2| \le [\sqrt{p}] < \sqrt{p}, \qquad |y_0| = |y_1 - y_2| \le [\sqrt{p}] < \sqrt{p}.$$

Но тогда $x_0^2 + y_0^2 < p + p = 2p$. Учитывая, что пары чисел $(x_1, y_1)$, $(x_2, y_2)$ различны, находим $x_0^2 + y_0^2 > 0$.

Интервал $(0, 2p)$ содержит лишь одно число, делящееся на $p$, а именно $p$. Следовательно $x_0^2 + y_0^2 = p$. □

**Лемма 6.5.** *Если два уравнения*

$$x^2 + y^2 = u, \qquad x^2 + y^2 = v, \qquad u, v \in \mathbb{Z},$$

*разрешимы в целых числах, то и уравнение*

$$x^2 + y^2 = uv \tag{6.15}$$

*имеет целые решения.*

*Доказательство.* Рассмотрим пары целых чисел $(x_1, y_1)$, $(x_2, y_2)$, удовлетворяющие равенствам

$$x_1^2 + y_1^2 = u, \qquad x_2^2 + y_2^2 = v.$$

Раскрыв скобки, легко проверить равенство

$$(x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = uv. \tag{6.16}$$

Таким образом, целые числа $z = x_1x_2 - y_1y_2$, $t = x_1y_2 + y_1x_2$ удовлетворяют равенству $z^2 + t^2 = uv$, т.е. уравнение (6.15) разрешимо в целых числах. □

Рассмотрим комплексные числа

$$\alpha = x_1 + iy_1, \qquad \beta = x_2 + iy_2$$

и их произведение

$$\gamma = \alpha \cdot \beta = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).$$

Равенство (6.16) может быть переписано в виде $|\gamma|^2 = |\alpha|^2|\beta|^2$. Таким образом, оно по-существу равносильно равенству $|\alpha\beta| = |\alpha| \cdot |\beta|$.

**Теорема 6.5.** *Уравнение (6.12) разрешимо в целых числах тогда и только тогда, когда разложение $n$ на простые сомножители содержит каждое простое число вида $4k + 3$ в четной степени.*

*Доказательство.* Докажем разрешимость уравнения (6.12) в условиях теоремы. Если разложение $n$ на простые сомножители содержит каждое простое число вида $4k+3$ в четной степени, то справедливо равенство $n = p_1 \cdots p_\ell \cdot m^2$, где $p_1, \ldots, p_\ell$ – простые числа вида $4k+1$ или 2. Уравнение $x^2 + y^2 = 2$ имеет решение $x = 1, y = 1$. Согласно лемме 6.4 каждое из уравнений $x^2 + y^2 = p_j$ при $p_j > 2$ разрешимо в целых числах. Имеет решения в целых числах также и уравнение $x^2 + y^2 = m^2$. Например, пара чисел $x = m, y = 0$ будет его решением.

Применяя теперь несколько раз лемму 6.5, заключаем, что и уравнение (6.12) при $n = p_1 \cdots p_\ell \cdot m^2$ имеет целые решения.

Предположим теперь, что существуют натуральные числа, представимые в виде суммы двух квадратов, но имеющие в своем разложении на простые сомножители хотя бы одно простое число вида $4k+3$ в нечетной степени. Пусть $n = x_0^2 + y_0^2$ – наименьшее из таких чисел и для $p = 4k+3$ кратность $\nu_p(n)$ нечетна. Справедливы сравнения $x_0^2 + y_0^2 \equiv 0 \pmod{p}$ и

$$x_0^2 \equiv -y_0^2 \pmod{p}. \tag{6.17}$$

Предположим, что $p|x_0$ и, значит, $p|y_0$. Определим целые числа $u, v$ равенствами $x_0 = pu, y_0 = pv$. Тогда $n = p^2(u^2 + v^2)$. Так как $m = u^2+v^2 < n$, то, согласно условию минимальности в определении $n$, кратность $\nu_p(m)$ четна. Но тогда будет четным и число $\nu_p(n) = \nu_p(m) + 2$, вопреки определению $n$. Следовательно $p \nmid x_0$ и $p \nmid y_0$.

Возводя обе части сравнения (6.17) в степень $\frac{p-1}{2} = 2k+1$, находим

$$x_0^{p-1} \equiv -y_0^{p-1} \pmod{p}. \tag{6.18}$$

По малой теореме Ферма выполняются сравнения $x_0^{p-1} \equiv 1 \pmod{p}$, $y_0^{p-1} \equiv 1 \pmod{p}$, так что из (6.18) следует $1 \equiv -1 \pmod{p}$. Последнее сравнение невозможно, ведь $p = 4k+3 > 2$. Это противоречие завершает доказательство теоремы. □

Докажем теорему о представимости натуральных чисел в виде

суммы четырех квадратов. Первое доказательство этой теоремы было опубликовано в 1770г. Лагранжем.

**Теорема 6.6.** *Каждое целое положительное число представимо в виде суммы четырех квадратов целых чисел.*

Иными словами, для каждого натурального $n$ уравнение

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

разрешимо в целых числах.

Сначала мы докажем утверждение, подобное лемме 6.5.

**Лемма 6.6.** *Если натуральные числа $u$ и $v$ представимы в виде суммы четырех квадратов, то их произведение также можно представить в виде суммы четырех квадратов.*

*Доказательство.* Доказательство, как и в случае леммы 6.5 основано на некотором тождестве.

Рассмотрим четыре комплексных числа

$$\alpha = x_1 + ix_2, \quad \beta = x_3 + ix_4, \quad \gamma = y_1 + iy_2, \quad \delta = y_3 + iy_4$$

и матрицы

$$\mathbf{A} = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix}. \tag{6.19}$$

Имеем

$$\det \mathbf{A} = x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad \det \mathbf{B} = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

Справедливо матричное тождество

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} \alpha\gamma - \beta\overline{\delta} & \alpha\delta + \beta\overline{\gamma} \\ -\gamma\overline{\beta} - \overline{\alpha}\overline{\delta} & -\delta\overline{\beta} + \overline{\alpha\gamma} \end{pmatrix},$$

означающее, в частности, что матрица $\mathbf{A} \cdot \mathbf{B}$ имеет такую же структуру, что и матрицы (6.19).

Легко проверить, что

$$\alpha\gamma - \beta\overline{\delta} = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 + i(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3),$$
$$\alpha\delta + \beta\overline{\gamma} = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + i(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1).$$

Поэтому равенство $\det \mathbf{A} \cdot \det \mathbf{B} = \det(\mathbf{A} \cdot \mathbf{B})$ приводит к тождеству

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2, \quad (6.20)$$

где

$$z_1 = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4,$$
$$z_2 = x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3,$$
$$z_3 = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2,$$
$$z_4 = x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1.$$

Тождество (6.20) можно проверить и непосредственно, раскрыв скобки в обеих его частях.

Лемма 6.6 сразу же следует из (6.20). Действительно, если с некоторыми целыми числами $x_i, y_j$ выполняются равенства

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = u, \qquad y_1^2 + y_2^2 + y_3^2 + y_4^2 = v,$$

то определенные выше целые числа $z_i$ согласно тождеству (6.20) дают представление числа $uv$ в виде суммы четырех квадратов

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = uv$$

. □

Лемма 6.6 означает, что для доказательства теоремы 6.6 достаточно установить представимость простых чисел в виде суммы четырех квадратов. Поскольку $2 = 1^2 + 1^2 + 0^2 + 0^2$, далее будем считать, что $p$ – простое нечетное число.

Докажем вспомогательную лемму о сравнениях.

**Лемма 6.7.** *Для каждого простого нечетного числа $p$ существуют целые числа $a$ и $b$, удовлетворяющие сравнению*

$$1 + a^2 + b^2 \equiv 0 \pmod{p}.$$

*Доказательство.* Рассмотрим два множества чисел

$$X_1 = \{k^2 \mid 0 \le k \le \frac{p-1}{2}\}, \qquad X_2 = \{-1 - k^2 \mid 0 \le k \le \frac{p-1}{2}\}.$$

Каждое из них состоит из $\frac{p+1}{2}$ чисел. Поскольку $\frac{p+1}{2} + \frac{p+1}{2} = p+1 > p$, заключаем, что объединение этих множеств $X_1 \cup X_2$ должно содержать два числа, принадлежащие одному классу вычетов по модулю $p$. Но числа множества $X_1$, очевидно, не сравнимы между собой. Точно так же не сравнимы и числа второго множества. Поэтому найдутся целые числа $a, b$ такие, что $a^2 \in X_1$, $-1-b^2 \in X_2$ и $a^2 \equiv -1-b^2 \pmod{p}$. Это завершает доказательство леммы. □

Доказательство следующей леммы напоминает доказательство леммы 6.4.

**Лемма 6.8.** *Каждое простое число есть сумма четырех квадратов.*

*Доказательство.* Пусть $a, b$ – целые числа, определенные в лемме 6.7. Рассмотрим все наборы целых чисел $\overline{x} = (x_1, x_2, x_3, x_4)$, удовлетворяющие условиям

$$0 \le x_i \le [\sqrt{p}], \qquad i = 1, 2, 3, 4, \tag{6.21}$$

и для каждого такого набора найдем пары классов вычетов

$$\Big(x_3 + ax_1 + bx_2 \pmod{p} \quad , \quad x_4 - bx_1 + ax_2 \pmod{p}\Big). \tag{6.22}$$

Количество получившихся при этом пар классов вычетов не превосходит $p^2$, в то время как количество наборов $\overline{x}$ равно

$$(1 + [\sqrt{p}])^4 > (\sqrt{p})^4 = p^2.$$

Значит, найдутся два различных набора $\overline{x} = (x_1, x_2, x_3, x_4)$, $\overline{y} = (y_1, y_2, y_3, y_4)$, удовлетворяющие условиям (6.21), для которых классы вычетов (6.22) совпадают, т.е.

$$\begin{aligned} x_3 + ax_1 + bx_2 \equiv & y_3 + ay_1 + by_2 \pmod{p}, \\ x_4 - bx_1 + ax_2 \equiv & y_4 - by_1 + ay_2 \pmod{p}. \end{aligned}$$

Положим $k_i = x_i - y_i$. Тогда выполняются условия

$$k_3 \equiv -ak_1 - bk_2 \pmod{p}, \quad k_4 \equiv bk_1 - ak_2 \pmod{p}, \quad |k_i| < \sqrt{p}.$$

Отсюда находим сравнение

$$\begin{aligned} k_1^2 + k_2^2 + k_3^2 + k_4^2 \equiv k_1^2 + k_2^2 + (ak_1 + bk_2)^2 + (bk_1 - ak_2)^2 = \\ = (k_1^2 + k_2^2)(1 + a^2 + b^2) \equiv 0 \pmod{p} \end{aligned}$$

и неравенства

$$0 < k_1^2 + k_2^2 + k_3^2 + k_4^2 < 4p.$$

Следовательно,

$$k_1^2 + k_2^2 + k_3^2 + k_4^2 = mp,$$

где $m$ есть одно из чисел $1, 2, 3$.

В случае $m = 1$ утверждение леммы выполняется.

Рассмотрим случай $m = 2$. Сумма $k_1^2 + k_2^2 + k_3^2 + k_4^2$ делится на 2 и, значит, числа $k_1, k_2, k_3, k_4$ могут быть разбиты на пары одинаковой четности. Не уменьшая общности можно считать, что $k_1, k_2$ и $k_3, k_4$ имеют одинаковую четность. Тогда все четыре числа $k_1 - k_2$, $k_1 + k_2$, $k_3 - k_4$, $k_3 + k_4$ четные и из равенств

$$\begin{aligned} \left(\frac{k_1 + k_2}{2}\right)^2 + \left(\frac{k_1 - k_2}{2}\right)^2 + \left(\frac{k_3 + k_4}{2}\right)^2 + \left(\frac{k_3 - k_4}{2}\right)^2 = \\ = \frac{1}{2}(k_1^2 + k_2^2 + k_3^2 + k_4^2) = p, \end{aligned}$$

следует утверждение леммы.

В случае $m = 3$ сумма $k_1^2 + k_2^2 + k_3^2 + k_4^2$ делится на 3. Квадраты целых чисел при делении на 3 дают в остатке 0 или 1. Поэтому одно из чисел $k_i$ делится на 3, а остальные не делятся. Изменив, если необходимо нумерацию этих чисел, можно, не уменьшая общности, считать, что на 3 делится $k_1$. Сменив также в случае необходимости знаки у чисел $k_2, k_3, k_4$ можно считать, что $k_2 \equiv k_3 \equiv k_4 \equiv 1 \pmod 3$. Действительно, если $k \equiv 2 \pmod 3$, то $-k \equiv 1 \pmod 3$.

Воспользуемся тождеством (6.20), положив в нем $x_i = k_i, y_1 = 0, y_2 = y_3 = y_4 = 0$. В результате получим равенство

$$\left(\frac{k_2 + k_3 + k_4}{3}\right)^2 + \left(\frac{k_1 + k_3 - k_4}{3}\right)^2 + \left(\frac{k_1 - k_2 + k_4}{3}\right)^2 + \\ + \left(\frac{k_1 + k_2 - k_3}{3}\right)^2 = \frac{1}{3}(k_1^2 + k_2^2 + k_3^2 + k_4^2) = p. \quad (6.23)$$

Из предположений об остатках чисел $k_i$ при делении на 3 следует, что все дроби в равенстве (6.23) есть целые числа. Это завершает доказательство леммы 6.8, а вместе с тем и теоремы 6.6. □

В виде суммы трех квадратов представимы не все натуральные числа $n$. Исключительное множество составляют числа вида $4^a(8b+7)$ при целых неотрицательных $a, b$ и только они. Так, например, число 7 нельзя представить в виде суммы трех квадратов целых чисел.

Теорему Лагранжа можно обобщить, рассматривая вместо квадратов кубы, четвертые или более высокие степени. Д.Гильберт в 1909г. доказал, что

*для каждого целого $k > 2$ можно найти целое $n > 0$ с условием, что любое натуральное число представимо в виде суммы не более чем $n$ слагаемых вида $x^k$ с целыми $x > 0$.*

При $k = 2$ это утверждение выполняется согласно теореме 6.6 с $n = 4$. Сформулированное утверждение было высказано как гипотеза в 1770г. Варингом.

## 6.6 Представление нуля квадратичными формами от трех неизвестных

В этом параграфе речь пойдет о решении в целых числах $x, y, z$ уравнения

$$ax^2 + by^2 + cz^2 = 0, \tag{6.24}$$

в котором коэффициенты $a, b, c$ предполагаются отличными от нуля целыми числами. Ясно, что при любых коэффициентах уравнение (6.24) имеет решение $x = y = z = 0$. Это решение мы будем называть тривиальным и далее найдем условия, при которых у уравнения имеется хотя бы одно нетривиальное решение.

Уравнение (6.24) имеет нетривиальное решение в целых числах тогда и только тогда, когда оно разрешимо в рациональных числах, среди которых есть отличное от нуля. Действительно, если рациональные числа $\alpha, \beta, \gamma$ удовлетворяют уравнению (6.24), то умножив их на общий знаменатель, можно найти набор целых чисел, также удовлетворяющих этому уравнению.

Сначала мы сделаем несколько упрощающих, но не уменьшающих общности предположений. Коэффициенты $a, b, c$ уравнения (6.24) должны иметь разные знаки. В противном случае уравнение имеет лишь тривиальное решение $x = y = z = 0$. Умножив, в случае необходимости уравнение на $-1$ и сменив, если нужно, обозначения переменных, можно считать, что

$$a > 0, \quad b > 0, \quad c < 0. \tag{6.25}$$

Если какие-либо два коэффициента, скажем $a$ и $b$, имеют общий простой делитель $p$, т.е. $a = pu, b = pv$ при некоторых целых $u, v$, то, умножив уравнение (6.24) на $p$, получаем равенство

$$u(px)^2 + v(py)^2 = pcz^2,$$

из которого следует, что уравнение (6.24) имеет нетривиальное решение в целых числах одновременно с уравнением

$$ux^2 + vy^2 + pcz^2 = 0.$$

Заметим, что $|uvpc| < |abc|$, т.е. абсолютная величина произведения коэффициентов нового уравнения меньше, чем у предшествующего. Если в новом уравнении найдутся два коэффициента, имеющие нетривиальный общий делитель, такое преобразование можно повторить. Ясно, что этот процесс рано или поздно должен завершиться, ведь целые числа $|abc|$ образуют убывающую последовательность, а она не может быть бесконечной. Итак, выясняя разрешимость уравнения (6.24) в целых числах, можно считать, что коэффициенты $a, b, c$ попарно взаимно просты, т.е.

$$(a, b) = (b, c) = (a, c) = 1. \tag{6.26}$$

Наконец, если какой-либо из коэффициентов, скажем $a$, делится на квадрат простого числа, т.е. $a = p^2 w$, где $p$ простое и $w$ целое числа, то уравнение (6.24) может быть переписано в виде

$$w(px)^2 + by^2 + cz^2 = 0,$$

так что уравнение (6.24) имеет нетривиальное решение в целых числах одновременно с уравнением

$$wx^2 + by^2 + cz^2 = 0.$$

Проделав эту операцию несколько раз, можно добиться, чтобы ни один из коэффициентов уравнения не делился бы на квадрат никакого простого числа.

Следующая теорема была впервые доказана Лежандром в 1785г.

**Теорема 6.7.** *Пусть $a, b, c$ целые числа, удовлетворяющие условиям (6.25) и (6.26), а кроме того не делящиеся на квадрат никакого простого. Уравнение (6.24) имеет нетривиальное решение в целых числах в том и только том случае, когда каждое из сравнений*

$$b\lambda^2 + c \equiv 0 (\mathrm{mod}\, a), \quad c\mu^2 + a \equiv 0 (\mathrm{mod}\, b), \quad a\nu^2 + b \equiv 0 (\mathrm{mod}\, c) \tag{6.27}$$

*разрешимо в целых числах $\lambda, \mu, \nu$.*

*Доказательство.* Докажем сначала, что из существования нетривиального решения у уравнения (6.24) следует разрешимость каждого из сравнений (6.27). Покажем это, например, для последнего из сравнений. В остальных случаях доказательства аналогичны.

Предположим, что уравнение (6.24) имеет нетривиальные решения. Выберем среди них решение $(x_0, y_0, z_0)$ с неотрицательными компонентами и наименьшей величиной $|x_0| + |y_0| + |z_0|$.

Проверим, что числа $c$ и $y_0$ взаимно просты. В противном случае они оба делятся на некоторое простое число $p$. Но тогда из равенства

$$ax_0^2 + by_0^2 + cz_0^2 = 0 \tag{6.28}$$

следует, что $p|ax_0^2$. Учитывая взаимную простоту $a$ и $c$, получаем отсюда, что $p|x_0$. Числа $x_0, y_0$ делятся на $p$. Из (6.28) теперь следует $p^2|cz_0^2$ и, так как, согласно условию, $c$ не делится на квадрат $p$, то $p|z_0^2$. Целые числа $u = x_0/p, v = y_0/p, w = z_0/p$ составляют решение уравнения (6.28), причем $|u| + |v| + |w| < |x_0| + |y_0| + |z_0|$. Получившееся противоречие означает, что числа $c$ и $y_0$ взаимно просты.

Из доказанного равенства $(c, y_0) = 1$ следует, в силу теоремы 5.1, что найдется целое число $\nu$, удовлетворяющее сравнению

$$y_0\nu \equiv x_0 \pmod{c}.$$

Далее с помощью равенства (6.28) находим

$$y_0^2(a\nu^2 + b) \equiv ax_0^2 + by_0^2 = -cz_0^2 \equiv 0 \pmod{c},$$

и, в силу $(c, y_0) = 1$, получаем $c|(a\nu^2 + b)$, что равносильно последнему сравнению (6.27).

Теперь докажем, что из разрешимости сравнений (6.27) следует разрешимость уравнения. Пусть $\lambda, \mu, \nu$ – целые числа, удовлетворяющие сравнениям (6.27). Справедливо сравнение по модулю $c$:

$$ax^2 + by^2 + cz^2 \equiv ax^2 - a\nu^2y^2 = (ax - a\nu y)(x + \nu y) \pmod{c}$$

или в иных обозначениях

$$f(x, y, z) \equiv L_1(x, y, z)M_1(x, y, z) \pmod{c}, \tag{6.29}$$

где $f(x,y,z) = ax^2 + by^2 + cz^2$ и $L_1(x,y,z) = ax - a\nu y$, $M_1(x,y,z) = x + \nu y$ линейные формы с целыми коэффициентами.

Точно так же найдутся линейные формы с целыми коэффициентами $L_2(x,y,z), M_2(x,y,z)$, $L_3(x,y,z), M_3(x,y,z)$, для которых

$$f(x,y,z) \equiv L_2(x,y,z)M_2(x,y,z) \pmod{a}, \tag{6.30}$$
$$f(x,y,z) \equiv L_3(x,y,z)M_3(x,y,z) \pmod{b}. \tag{6.31}$$

Рассмотрим далее всевозможные тройки целых чисел $(x,y,z)$, удовлетворяющие условиям

$$0 \le x \le [\sqrt{|bc|}\,], \quad 0 \le y \le [\sqrt{|ac|}\,], \quad 0 \le z \le [\sqrt{ab}\,]. \tag{6.32}$$

Количество их $S$ удовлетворяет неравенству

$$S = (1+[\sqrt{|bc|}\,])(1+[\sqrt{|ac|}\,])(1+[\sqrt{ab}\,]) > \sqrt{|bc|}\cdot\sqrt{|ac|}\cdot\sqrt{ab} = |abc|.$$

Каждой такой тройке $(x,y,z)$ поставим в соответствие набор классов вычетов по модулям $|c|, a, b$, а именно

$$\big(L_1(x,y,z)(\mathrm{mod}\,|c|), \quad L_2(x,y,z)(\mathrm{mod}\,a), \quad L_3(x,y,z)(\mathrm{mod}\,b)\big).$$

Количество различных наборов классов вычетов равно $|abc|$ и, как указано выше, меньше количества $S$ наборов троек $(x,y,z)$. Поэтому найдутся две тройки $(x_1,y_1,z_1)$, $(x_2,y_2,z_2)$, удовлетворяющие сравнениям

$$L_1(x_1,y_1,z_1) \equiv L_1(x_2,y_2,z_2) \pmod{|c|},$$
$$L_2(x_1,y_1,z_1) \equiv L_2(x_2,y_2,z_2) \pmod{a},$$
$$L_3(x_1,y_1,z_1) \equiv L_3(x_2,y_2,z_2) \pmod{b}.$$

Обозначив $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$, $z_0 = z_1 - z_2$, и пользуясь линейностью $L_j$, последние сравнения можно переписать в виде

$$L_1(x_0,y_0,z_0) \equiv 0 \pmod{|c|},$$
$$L_2(x_0,y_0,z_0) \equiv 0 \pmod{a},$$
$$L_3(x_0,y_0,z_0) \equiv 0 \pmod{b}.$$

Теперь из сравнений (6.29), (6.30), (6.31) следует

$$c|f(x_0,y_0,z_0), \quad a|f(x_0,y_0,z_0), \quad b|f(x_0,y_0,z_0).$$

В силу попарной взаимной простоты чисел $a,b,c$ эти делимости означают, что целое число $f(x_0,y_0,z_0)$ делится на $abc$.

Далее из неравенств (6.32) следует, что $|x_0| = |x_1 - x_2| \le [\sqrt{|bc|}]$ и аналогично $|y_0| \le [\sqrt{|ac|}]$, $|z_0| \le [\sqrt{ab}]$. Пользуясь этими неравенствами и (6.25), находим

$$f(x_0,y_0,z_0) \ge cz_0^2 > abc, \qquad f(x_0,y_0,z_0) \le ax_0^2 + by_0^2 < 2|abc|.$$

Здесь использовалось также, что все числа $|bc|, |ac|, ab$ не являются квадратами.

Из этих неравенств, поскольку $abc|f(x_0,y_0,z_0)$ следует, что

$$f(x_0,y_0,z_0) = mabc, \qquad m = 0, -1.$$

Случай $m = 0$ доказывает нужное утверждение, так как по крайней мере одно из чисел $x_0, y_0, z_0$ отлично от нуля.

Если же $ax_0^2 + by_0^2 + cz_0^2 = -abc$, имеем

$$-a(x_0^2 + bc) = by_0^2 + cz_0^2.$$

Умножив последнее равенство на $x_0^2 + bc$, получаем равенства

$$-a(x_0^2+bc)^2 = (by_0^2+cz_0^2)(x_0^2+bc) = b(x_0y_0 - cz_0)^2 + c(x_0z_0 + by_0)^2,$$

означающие, что числа

$$x_0^2 + bc, \quad x_0y_0 - cz_0, \quad x_0z_0 + by_0$$

составляют решение уравнения (6.24). Это решение нетривиально, т.к. $x_0^2 + bc \ne 0$. В противном случае $|bc|$ было бы квадратом целого числа, что неверно. □

Существует алгоритм, позволяющий в случае разрешимости уравнения (6.24) находить все решения в целых числах. Мы не будем

останавливаться здесь на его описании. Рассмотрим некоторые примеры.

**Пример.** Решить в целых числах уравнение

$$3x^2 + 2y^2 - z^2 = 0.$$

Согласно теореме 6.7 данное уравнение имеет нетривиальное решение лишь в случае разрешимости всех трех сравнений

$$2\lambda^2 - 1 \equiv 0 \bmod 3, \quad -\mu^2 + 3 \equiv 0 \bmod 2, \quad 3\nu^2 + 2 \equiv 0 \bmod 1.$$

Первое из этих сравнений равносильно сравнению $\lambda^2 \equiv -1 \bmod 3$ и, так как $\left(\frac{-1}{3}\right) = -1$, оно не имеет решений. Значит, данное уравнение имеет лишь тривиальное решение $x = y = z = 0$.

**Пример.** Найти все простые числа $p$, при которых уравнение

$$x^2 + y^2 = pz^2$$

имеет нетривиальное решение в целых числах.

При $p = 2$ уравнение имеет решение $x = y = z = 1$. Поэтому далее будем считать, что простое число $p$ нечетно.

Согласно теореме 6.7 данное уравнение имеет нетривиальное решение в том и только том случае, когда выполняется сравнение $\nu^2 + 1 \equiv 1 \pmod{p}$. Это условие равносильно равенству $\left(\frac{-1}{p}\right) = 1$. Учитывая, что $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, заключаем, что нетривиальное решение существует лишь для $p = 2$ и простых чисел $p$ из прогрессии $4n + 1$.

# Глава 7

# Первообразные корни и индексы

Теорема 4.1 из главы 4 утверждает, что при любом натуральном $m \geq 2$ группа обратимых элементов кольца $\mathbb{Z}/m\mathbb{Z}$ состоит из $\varphi(m)$ классов, наименьшие неотрицательные вычеты которых взаимно просты с модулем $m$. Мы будем обозначать эту группу символом $(\mathbb{Z}/m\mathbb{Z})^*$. Настоящая глава посвящена изучению ее структуры.

## 7.1 Показатель числа по заданному модулю.

Согласно малой теореме Ферма, см. параграф 4.5, для каждого целого числа $a$ взаимно простого с модулем $m$ выполняется сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$. Для некоторых чисел $a$ сравнение $a^d \equiv 1 \pmod{m}$ может выполняться и при $d < \varphi(m)$. Например, $(-1)^2 \equiv 1 \pmod{m}$.

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 $m$, см. §4.5. Например, при $m > 2$ показатель $-1$ равен 2. Если два числа сравнимы по модулю $m$, то их показатели по модулю $m$ одинаковы.

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 7.** *Целое число $a$ взаимно простое с модулем $m$ на-*

*зывается первообразным корнем по модулю $m$, если его показатель равен $\varphi(m)$.*

Если $a$ – первообразный корень по модулю $m$, то числа

$$1, a, a^2, \ldots, a^{\varphi(m)-1} \tag{7.1}$$

принадлежат различным классам вычетов. Действительно, если бы нашлись целые числа $0 \le u < v \le \varphi(m) - 1$, для которых $a^u \equiv a^v \pmod{m}$, то в силу взаимной простоты чисел $a$ и $m$ мы получили бы

$$1 \equiv a^{v-u} \pmod{m}.$$

Но это невозможно, так как $0 < v - u < \varphi(m)$ и показатель $a$ равен $\varphi(m)$.

Множество (7.1) состоит из $\varphi(m)$ чисел. Поэтому среди (7.1) есть представители всех классов вычетов, состоящих из чисел взаимно простых с $m$. Другими словами, для каждого целого числа $b$ взаимно простого с модулем $m$ найдется единственное целое $k$, удовлетворяющее условиям

$$b \equiv a^k \pmod{m}, \qquad 0 \le k < \varphi(m).$$

Это свойство можно выразить иначе, сказав, что первообразный корень по модулю $m$ существует лишь в случае, когда $(\mathbb{Z}/m\mathbb{Z})^*$ – циклическая группа. Оно выполняется не для всех модулей $m$. Например, квадрат каждого нечетного числа при делении на 8 дает в остатке 1. Значит, показатель каждого нечетного числа по модулю 8 может равняться лишь 1 или 2, и всегда отличен от $\varphi(8) = 4$. Первообразных корней по модулю 8 не существует.

Свойства показателей описывает следующая лемма.

**Лемма 7.1.** *1. Пусть $d$ – показатель числа $a$ по модулю $m$. Натуральное число $n$ удовлетворяет условию $a^n \equiv 1 \pmod{m}$ в том и только том случае, когда $d|n$.*

*2. Пусть $a, b$ – целые числа, взаимно простые с модулем $m$, показатели их равны соответственно $u$ и $v$. Если $(u, v) = 1$, то показатель числа $ab$ равен $uv$.*

*3. Если показатель числа $c$ равен $uv$, то показатель $c^u$ равен $v$.*

*Доказательство.* Заметим, что числа $ab$ и $a^u$, о которых идет речь в формулировке теоремы, взаимно просты с модулем, поэтому каждое из них имеет некоторый показатель.

Первое утверждение леммы уже доказано нами, см. лемму 4.2.

Чтобы доказать второе утверждение, обозначим буквой $s$ показатель числа $ab$. Так как

$$(ab)^{uv} = (a^u)^v (b^v)^u \equiv 1 \pmod{m},$$

то по первому утверждению леммы имеем $s|uv$. С другой стороны из сравнения $(ab)^s \equiv 1 \pmod{m}$ следует

$$1 \equiv (ab)^{su} = (a^u)^s b^{us} \equiv b^{us} \pmod{m}.$$

С помощью первого утверждения находим $v|us$. Согласно условию числа $u, v$ взаимно просты, поэтому $v|s$. Аналогично доказывается, что $u|s$. Учитывая взаимную простоту чисел $u, v$, получаем отсюда $uv|s$. Итак, доказано, что $s = uv$.

Для доказательства третьего утверждения обозначим буквой $t$ показатель числа $c^u$. Так как $1 \equiv c^{uv} = (c^u)^v \pmod{m}$, то $t|v$. А из сравнения $1 \equiv (c^u)^t = c^{tu} \pmod{m}$ следует, в силу первого свойства, что $uv|tu$ и $v|t$. Но тогда $t = v$ и последнее утверждение леммы доказано. □

**Следствие 7.1.** *Если $(a, m) = 1$ и целые числа $u, v$ удовлетворяют сравнению $a^u \equiv a^v \pmod{m}$, то $u \equiv v \pmod{d}$, где $d$ – показатель $a$ по модулю $m$.*

*Доказательство.* Не уменьшая общности можно считать, что $v > u$. Поскольку $a$ и $m$ взаимно просты, из данного сравнения следует $a^{v-u} \equiv 1 \pmod{m}$. Согласно первому утверждению леммы 7.1 можно утверждать, что $d|(v - u)$. □

## 7.2 Существование первообразных корней по простому модулю

В 1801 году К.Ф. Гаусс опубликовал два доказательства следующей теоремы.

**Теорема 7.1.** *Для каждого простого нечетного числа $p$ существуют первообразные корни по модулю $p$.*

*Доказательство.* Обозначим буквой $d$ наименьшее общее кратное показателей всех чисел, не делящихся на $p$. Из теоремы Ферма, см. параграф 4.5, и первого утверждения леммы 7.1 следует, что $p-1$ делится на показатель каждого числа, не кратного $p$. Но тогда $d|(p-1)$, см. параграф 1.2, теорема 1.2.

Из первого утверждения леммы 7.1 следует, что каждое целое число, не кратное $p$, удовлетворяет сравнению $x^d - 1 \equiv 1 \pmod{p}$. Значит, это сравнение имеет $p-1$ решение. С помощью теоремы 5.3 из параграфа 5.4 находим теперь $d \geq p-1$. Таким образом, $d = p-1$.

Пусть $p - 1 = q_1^{k_1} \cdots q_r^{k_r}$ – разложение на простые сомножители. По свойству наименьшего общего кратного, см. следствие 2.2 из параграфа 2.2, можно утверждать, что для каждого индекса $i, 1 \leq i \leq r$, найдется число $a_j$, показатель которого равен $q_i^{k_i} v_i$. Положим $a = a_1^{v_1} \cdots a_r^{v_r}$. По второму утверждению леммы 7.1 показатель числа $a_i^{v_i}$ равен $q_i^{k_i}$. Из третьего утверждения этой же леммы следует, что показатель числа $a$ равен $q_1^{k_1} \cdots q_r^{k_r} = p-1$. Итак, построенное число $a$ есть первообразный корень по модулю $p$. Теорема доказана. □

*Второе доказательство теоремы 7.1.* Как уже указывалось, $p-1$ делится на показатель по модулю $p$ любого числа, не кратного $p$. Для каждого натурального $d$, делящего $p-1$, обозначим символом $\psi(d)$ количество чисел среди $1, 2, \ldots, p-1$, показатель которых по модулю $p$ равен $d$. Тогда $\psi(d) \geq 0$ и

$$\sum_{d|p-1} \psi(d) = p - 1, \tag{7.2}$$

ведь каждое число из набора $1, 2, \ldots, p-1$ имеет некоторый показатель по модулю $p$.

Пусть для какого-то $d$ выполняется $\psi(d) > 0$ и $b$ – некоторое число с показателем $d$. Согласно условию минимальности в определении показателя все числа

$$b^k, \qquad k = 0, 1, \ldots, d-1, \tag{7.3}$$

лежат в различных классах вычетов по модулю $p$ и удовлетворяют сравнению

$$(b^k)^d = (b^d)^k \equiv 1 \pmod{p}.$$

Значит, они являются решениями сравнения $x^d - 1 \equiv 0 \pmod{p}$. Так как это сравнение не может иметь более $d$ корней, все его решения исчерпываются классами вычетов по модулю $p$, содержащими числа (7.3). В частности, каждое число, имеющее показатель $d$ сравнимо с одним из чисел (7.3).

Предположим, что $r = (k, d) > 1$. Тогда

$$(b^k)^{d/r} = (b^d)^{k/r} \equiv 1 \pmod{p},$$

т.е. показатель $b^k$ не превосходит $\frac{d}{r}$. Из этого рассуждения следует, что если показатель какого-либо числа $b^k$ из (7.3) равен $d$, то должно быть выполнено условие $(k, d) = 1$. Значит, при любом $d|p-1$ выполняется неравенство $\psi(d) \leq \varphi(d)$.

Итак, при любом $d|p-1$ выполняется неравенство $\psi(d) \leq \varphi(d)$. Согласно лемме 3.3 из параграфа 3.3 выполняется

$$\sum_{d|p-1} \varphi(d) = p - 1.$$

С помощью (7.2) теперь находим

$$\sum_{d|p-1} (\varphi(d) - \psi(d)) = 0.$$

Все слагаемые в этой сумме неотрицательны, поэтому при любом $d|p-1$ выполняется равенство $\psi(d) = \varphi(d)$. В частности, $\psi(p-1) = \varphi(p-1) > 0$, и это завершает доказательство теоремы. $\square$

**Следствие 7.2.** *Для каждого простого нечетного $p$ существует в точности $\varphi(p-1)$ первообразных корней по модулю $p$.*

*Доказательство.* Согласно определению функции $\psi(d)$ это утверждение следует из равенства $\psi(p-1) = \varphi(p-1)$. □

Для практического нахождения первообразных корней удобно пользоваться следующим утверждением.

**Лемма 7.2.** *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*

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

*Доказательство.* Обозначим буквой $d$ показатель числа $c$ по модулю $p$. Тогда $d|(p-1)$. Если $d < p-1$, то найдется такое простое число $q$, что $qd|(p-1)$ или $d|\frac{p-1}{q}$. Но тогда $c^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, вопреки условию. Значит, $d = p-1$, и это завершает доказательство леммы. □

**Пример.** Найти наименьший первообразный корень по модулю 23.

Справедливы сравнения по модулю 23

$$2^{11} = 2 \cdot (32)^2 \equiv 2 \cdot 9^2 \equiv 1, \qquad 3^{11} = 9 \cdot (27)^3 \equiv 9 \cdot 4^3 \equiv 1.$$

Из них следует, что числа $2, 3$ не являются первообразными корнями по модулю 23. Кроме того, $4^{11} = \left(2^{11}\right)^2 \equiv 1 \pmod{23}$, так что и 4 не является первообразным корнем по модулю 23. Далее

$$5^{11} = 5 \cdot 25^5 \equiv 5 \cdot 2^5 \equiv -1 \pmod{23}$$

и $5^2 \equiv 2 \pmod{23}$. Применяя лемму 7.2 к простому числу $p = 23$ и $c = 5$, заключаем, что 5 есть первообразный корень по модулю 23, т.е. для каждого натурального числа $b$, не делящегося на 23, найдется целое $k$ с условием $b \equiv 5^k \pmod{23}$. Другими словами

класс вычетов $\overline{5}$ есть образующая в группе $(\mathbb{Z}/23\mathbb{Z})^*$. Количество первообразных корней по модулю 23 равно $\varphi(22) = \varphi(2)\varphi(11) = 10$.

**Пример.** Пусть $p, q$ – простые нечетные числа, связанные соотношением $p = 2q+1$. Докажем, что в случае $q = 4n+1$ число 2 есть первообразный корень по модулю $p$, если же $q = 4n+3$, то $-2$ есть первообразный корень по модулю $p$.

Так как $p-1 = 2q$ имеет лишь два простых делителя 2 и $q$, то согласно лемме 7.2 для доказательства того, что $c$ есть первообразный корень, достаточно проверить выполнимость двух условий

$$c^2 \not\equiv 1 \pmod{p}, \qquad c^q \not\equiv 1 \pmod{p}.$$

Для $c = 2$ или $c = -2$ первое из этих условий равносильно $4 \not\equiv 1 \pmod{p}$, что, конечно, выполняется, так как $p \geq 2 \cdot 3 + 1 = 7$.

Для проверки второго условия рассмотрим сначала случай $q = 4n+1$ и $c = 2$. В этом случае имеем

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

Так как в рассматриваемом случае $\frac{p^2-1}{8} = (4n+1)(2n+1)$, заключаем, что $2^q \equiv -1 \pmod{p}$ и, значит, 2 есть первообразный корень по модулю $p$.

В случае $q = 4n+3$ и $c = -2$ находим

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

причем $\frac{p^2-1}{8} = (4n+3)(2n+2)$. Следовательно, $(-2)^q \equiv -1 \pmod{p}$, так что $-2$ есть первообразный корень по модулю $p$.

Если известны все простые делители числа $p-1$, то проверка условий леммы 7.2 выполняется достаточно быстро с помощью алгоритма, изложенного в параграфе 4.7. 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 леммы 7.2.

Существует гипотеза[1], что *для каждого целого числа $a$, отличного от $-1$ и квадратов целых чисел, существует бесконечно много простых чисел $p$, для которых $a$ является первообразным корнем по модулю $p$.* Например, существуют сколь угодно большие простые числа, для которых 2 будет первообразным корнем.

## 7.3 Построение первообразных корней по модулям $p^k$ и $2p^k$

Далее мы докажем существование первообразных корней по модулям вида $p^\alpha$ и $2p^\alpha$, где $p$ – простое нечетное число.

**Теорема 7.2.** *Пусть $p$ – простое нечетное число и $\alpha \geq 1$ – целое. Тогда*

*1. По модулям $p^\alpha$ и $2p^\alpha$ существуют первообразные корни.*

*2. Пусть $g$ – первообразный корень по модулю $p$. Если целое число $g_1$ удовлетворяет условиям*

$$g_1 \equiv g \pmod{p}, \qquad p^2 \nmid g_1^{p-1} - 1, \tag{7.4}$$

*то $g_1$ – первообразный корень по любому модулю вида $p^\alpha$, где $\alpha \geq 1$. По крайней мере одно из чисел $g$ или $g+p$ удовлетворяет условиям (7.4).*

*3. Если $g_2$ нечетно и $g_2 \equiv g_1 \pmod{p^\alpha}$, то $g_2$ – первообразный корень по любому модулю вида $2p^\alpha$, где $\alpha \geq 1$. По крайней мере одно из двух чисел $g_1$ и $g_1 + p^\alpha$ удовлетворяет указанным условиям.*

**Пример.** Доказать, что 2 есть первообразный корень по модулям $37^\alpha$ при любом целом $\alpha \geq 1$. Найти первообразные корни по модулям $2 \cdot 37^\alpha$.

Докажем сначала, что 2 есть первообразный корень по модулю 37. Поскольку для $p = 37$ выполняется $p - 1 = 36 = 2^2 \cdot 3^2$, то в силу

[1] высказана немецким математиком Э. Артином, 1898-1962.

леммы 7.2 достаточно проверить, что $2^{18} \not\equiv 1 \pmod{37}$ и $2^{12} \not\equiv 1 \pmod{37}$. Имеем $2^6 = 64 \equiv -10 \pmod{37}$, поэтому

$$2^{12} \equiv (-10)^2 \equiv 26 \pmod{37}, \quad 2^{18} \equiv (-10)^3 \equiv -1 \pmod{37}.$$

Итак, 2 есть первообразный корень по модулю 37

Предположим теперь, что

$$37^2 | 2^{36} - 1 = (2^{18} - 1)(2^{18} + 1).$$

Так как $2^{18} \equiv -1 \pmod{37}$, то

$$37^2 | (2^{18} + 1) = (2^6 + 1)(2^{12} - 2^6 + 1).$$

Учитывая, что $2^6 + 1 = 65$ не делится на 37, заключаем, что

$$37^2 | 2^{12} - 2^6 + 1 = 4033 = 37 \cdot 109.$$

Получившееся противоречие означает, что $37^2 \nmid 2^{36} - 1$. Согласно теореме 7.2 можно утверждать теперь, что 2 есть первообразный корень по модулю $37^\alpha$ при любом целом $\alpha \geq 2$.

Так как $2+37 = 39$ нечетно, то согласно последнему утверждению теоремы 7.2 число 39 есть первообразный корень по любому модулю вида $2 \cdot 37^\alpha$ при целом $\alpha \geq 1$.

Перейдем теперь к доказательству теоремы 7.2.

*Доказательство.* Первое утверждение теоремы следует из второго и третьего. Поэтому перейдем непосредственно к их доказательству.

Если оба числа $(g+p)^{p-1} - 1$ и $g^{p-1} - 1$ делятся на $p^2$, то

$$p^2 | (g+p)^{p-1} - g^{p-1}$$

и, раскрывая скобки в $(g+p)^{p-1}$ с помощью формулы Ньютона для бинома, находим

$$0 \equiv (g+p)^{p-1} - g^{p-1} \equiv (p-1)g^{p-2}p \pmod{p^2}.$$

Но тогда $p | (p-1)g^{p-2}$, что невозможно. Итак, доказано, что по крайней мере одно из чисел $(g+p)^{p-1} - 1$ и $g^{p-1} - 1$ не делится на $p^2$,

т.е. по крайней мере одно из двух чисел $g$ и $g+p$ удовлетворяет условиям (7.4).

Пусть $g_1$ – произвольное число с условиями (7.4). Докажем, что при любом целом $\beta \geq 0$ выполняется равенство

$$\nu_p\left(g_1^{p^\beta(p-1)} - 1\right) = \beta + 1. \tag{7.5}$$

Воспользуемся для этого математической индукцией по $\beta$. При $\beta = 0$ утверждение следует из условий теоремы (7.4).

Допустим теперь, что равенство (7.5) справедливо для некоторого $\beta \geq 0$ и докажем его для $\beta + 1$. Из (7.5) следует, что

$$g_1^{p^\beta(p-1)} = 1 + cp^{\beta+1}, \qquad p \nmid c.$$

Возводя это равенство в степень $p$, находим

$$g_1^{p^{\beta+1}(p-1)} = \left(1 + cp^{\beta+1}\right)^p = 1 + cp^{\beta+2} + (cp^{\beta+1})^p + \sum_{k=2}^{p-1} \binom{p}{k} (cp^{\beta+1})^k.$$

Поскольку для $k \geq 2$ биномиальный коэффициент $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на $p$ и также выполняются неравенства $k(\beta+1) \geq \beta+2$, $p(\beta+1) \geq \beta+3$, находим

$$g_1^{p^{\beta+1}(p-1)} \equiv 1 + cp^{\beta+2} \pmod{p^{\beta+3}}.$$

Из этого сравнения, поскольку $p \nmid c$ следует (7.5) для $\beta + 1$.

Пусть теперь $\alpha \geq 2$ – некоторое целое число. Докажем, что $g_1$ есть первообразный корень по модулю $p^\alpha$. Обозначим для этого буквой $d$ показатель $g_1$ по модулю $p^\alpha$.

Так как $g_1^d \equiv 1 \pmod{p^\alpha}$ и $g_1 \equiv g \pmod{p}$, то справедливо сравнение $g^d \equiv 1 \pmod{p}$. С помощью леммы 7.1, поскольку $g$ есть первообразный корень по модулю $p$, т.е. показатель $g$ по модулю $p$ равен $p-1$, заключаем, что $(p-1)|d$.

По теореме Эйлера выполняется сравнение $g_1^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$. Опять применяя лемму 7.1, заключаем $d|\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Учитывая установленную ранее делимость $(p-1)|d$, находим, что $d =$

$p^\beta(p-1)$ с некоторым целым $\beta$, удовлетворяющим неравенствам $0 \le \beta \le \alpha - 1$.

Согласно определению $d$ должно выполняться

$$p^\alpha \big| g_1^d - 1 = g_1^{p^\beta(p-1)} - 1.$$

В соответствии с равенством (7.5) отсюда следует, что $\alpha \le \beta + 1$. Сравнивая это неравенство с доказанным ранее, получаем $\beta = \alpha - 1$ и $d = p^{\alpha-1}(p-1) = \varphi(p^\alpha)$. Таким образом, $g_1$ есть первообразный корень по модулю $p^\alpha$.

Для доказательства третьего утверждения теоремы заметим, прежде всего, что оба числа $g_1$ и $g_1 + p^\alpha$ сравнимы с $g_1$ по модулю $p^\alpha$, и в силу нечетности $p^\alpha$, одно из них будет нечетным, т.е. удовлетворяет условиям, определяющим $g_2$.

Из сравнений $g_2 \equiv g_1 \pmod{p^\alpha}$ и $g_2 \equiv 1 \pmod 2$ следует взаимная простота чисел $g_2$ и $2p^\alpha$. Обозначим буквой $s$ показатель $g_2$ по модулю $2p^\alpha$. Так как $g_1^d \equiv g_2^d \equiv 1 \pmod{p^\alpha}$ и $g_1$ есть первообразный корень по модулю $p^\alpha$, то $s \ge \varphi(p^\alpha) = \varphi(2p^\alpha)$. Теперь согласно теореме Эйлера можно утверждать, что $s = \varphi(2p^\alpha)$. Следовательно, $g_2$ есть первообразный корень по модулю $2p^\alpha$. □

Заметим, что любой первообразный корень по модулю $p^n$, где $n \ge 2$ будет также и первообразным корнем по модулю $p$. Действительно, пусть $b$ – первообразный корень по модулю $p^n$. Тогда для любого целого числа $a$, не делящегося на $p$, найдется целое число $k$, удовлетворяющее сравнению $a \equiv b^k \pmod{p^n}$. Но тогда $a \equiv b^k \pmod p$. Так как это справедливо для $a = 1, 2, \ldots, p-1$, показатель числа $b$ по модулю $p$ не может быть менее $p - 1$.

## 7.4 Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, $p^k$ и $2p^k$

В двух предыдущих параграфах были рассмотрены примеры модулей $m = p^\alpha, m = 2p^\alpha$, для которых существуют первообразные

корни и описан алгоритм их вычисления. При $m = 4$ первообразным корнем будет число 3. При $m = 2$ существует единственный класс вычетов, состоящий из чисел взаимно простых с 2, а именно, класс $\overline{1}$, состоящий из нечетных чисел. В этом случае первообразным корнем будет 1. В этом параграфе будет доказано, что указанными примерами исчерпываются все случаи существования первообразных корней.

**Теорема 7.3.** *Пусть $\alpha \geq 3$ – нечетное целое число.*
*1. Каждое нечетное число $a$ удовлетворяет сравнению*

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}. \tag{7.6}$$

*2. Показатель числа 5 по модулю $2^\alpha$ равен $2^{\alpha-2}$.*
*3. Каждое нечетное число сравнимо по модулю $2^\alpha$ с одним из чисел*

$$\pm 5,\ \pm 5^2,\ \pm 5^3,\ \ldots,\ \pm 5^{2^{\alpha-2}}. \tag{7.7}$$

Эта теорема на языке теории групп может быть переформулирована как утверждение о том, что мультипликативная группа $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ равна прямому произведению своих циклических подгрупп, порожденных классами вычетов $\overline{-1}$ и $\overline{5}$.

*Доказательство.* Докажем сначала первое утверждение. При $\alpha = 3$ оно верно, так как для $a = 2b + 1$ выполняется $a^2 - 1 = 4b(b + 1)$, и одно из двух последовательных чисел $b, b + 1$ четно.

Так как $a$ нечетно, то при любом целом $k \geq 0$ число $a^{2^k} + 1$ четно. Из равенства

$$a^{2^{k+1}} - 1 = \left(a^{2^k} - 1\right)\left(a^{2^k} + 1\right), \tag{7.8}$$

следует теперь, что

$$\nu_2\left(a^{2^{k+1}} - 1\right) \geq \nu_2\left(a^{2^k} - 1\right) + 1.$$

Так как по доказанному $\nu_2(a^2 - 1) \geq 3$, заключаем отсюда по индукции, что

$$\nu_2(a^{2^k} - 1) \geq k + 2, \qquad k \geq 1.$$

Это неравенство при $k = \alpha - 2$ дает первое утверждение теоремы.

Так как $5 \equiv 1 \pmod 4$, то при любом целом $k \geq 0$ находим $5^{2^k} + 1 \equiv 2 \pmod 4$ и, значит, $\nu_2\left(5^{2^k} + 1\right) = 1$. Теперь из равенства (7.8) при $a = 5$ следует, что

$$\nu_2\left(5^{2^{k+1}} - 1\right) = \nu_2\left(5^{2^k} - 1\right) + 1.$$

Отсюда же, поскольку $\nu_2(5 - 1) = 2$, находим

$$\nu_2\left(5^{2^k} - 1\right) = k + 2, \qquad k \geq 0. \tag{7.9}$$

Пусть теперь $\alpha \geq 3$ – целое число. Обозначим буквой $d$ показатель числа 5 по модулю $2^\alpha$. Из первого утверждения теоремы следует, что $d | 2^{\alpha-2}$, и, значит, $d = 2^\beta$, $\beta \leq \alpha - 2$. Согласно определению $d$ имеем $2^\alpha | 5^{2^\beta} - 1$, откуда в силу (7.9) следует $\alpha \leq \beta + 2$. Таким образом, $\beta = \alpha - 2$ и $d = 2^{\alpha-2}$. Второе утверждение доказано.

Для доказательства третьего утверждения теоремы достаточно установить, что числа (7.7) составляют приведенную систему вычетов по модулю $2^\alpha$. Поскольку все эти числа нечетны, достаточно установить их попарную несравнимость по модулю $2^\alpha$, см. §4.3.

Предположим, что $5^k \equiv -5^\ell \pmod{2^\alpha}, 1 \leq k, \ell \leq 2^{\alpha-2}$. Тогда $5^k \equiv -5^\ell \pmod 4$ и, значит, $1 \equiv -1 \pmod 4$, что неверно. Итак, числа с разными знаками из набора (7.7) не сравнимы друг с другом по модулю $2^\alpha$. Если предположить, что сравнимы какие-либо два числа (7.7) с одинаковыми знаками, имеем $5^k \equiv 5^\ell \pmod{2^\alpha}, 1 \leq \ell < k \leq 2^{\alpha-2}$. Тогда $5^{k-\ell} \equiv 1 \pmod{2^\alpha}$, $0 < k - \ell < 2^{\alpha-2}$. Но это противоречит второму утверждению теоремы. □

**Теорема 7.4.** *Первообразные корни существуют лишь для модулей*

$$2,\ 4,\ p^\alpha,\ 2p^\alpha, \tag{7.10}$$

*где $p$ – простое нечетное и $\alpha$ – целое положительное числа.*

*Доказательство.* Существование первообразных корней в случаях (7.10) доказано ранее.

Ниже будет показано, что если $m$ отлично от чисел вида (7.10), то для любого целого $a$, взаимно простого с $m$, выполняется сравнение

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}. \tag{7.11}$$

Это сравнение означает, что показатель каждого числа $a$ с условием $(a, m) = 1$ меньше $\varphi(m)$, так что первообразных корней в этом случае не существует.

Итак, пусть $m = 2^{\alpha} \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r}$ отлично от чисел вида (7.10). Тогда возможны следующие три случая:
1) $r = 0, \alpha \geq 3$,
2) $r = 1, \alpha \geq 2$,
3) $r \geq 2$.

В каждом из них выполняется равенство

$$\varphi(m) = \varphi(2^{\alpha}) \cdot \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}). \tag{7.12}$$

В первом случае имеем $m = 2^{\alpha}, \alpha \geq 3$. Тогда сравнение (8.10) совпадает с (7.6), и уже доказано в теореме 7.3.

Во втором и третьем случаях среди чисел

$$\varphi(2^{\alpha}), \quad \varphi(p_1^{\alpha_1}), \quad \dots, \quad \varphi(p_r^{\alpha_r}) \tag{7.13}$$

найдется по крайней мере два четных. Действительно, в третьем случае $r \geq 2$ и таким будет каждое из чисел $\varphi(p_i^{\alpha_i})$, $i = 1, \dots, r$. Во втором же случае, т.е. при $r = 1$, выполняется неравенство $\alpha \geq 2$, так что четным помимо $\varphi(p_1^{\alpha_1})$ будет и $\varphi(2^{\alpha})$.

Поскольку среди чисел (7.13) имеется не менее двух четных, заключаем с помощью равенства (7.12), что

$$2\varphi(2^{\alpha}) \big| \varphi(m), \quad 2\varphi(p_1^{\alpha_1}) \big| \varphi(m), \quad \dots, \quad 2\varphi(p_r^{\alpha_r}) \big| \varphi(m).$$

Но тогда $\frac{\varphi(m)}{2}$ делится на каждое из чисел (7.13) и, следовательно, делится на показатель числа $a$ по каждому из модулей $2^{\alpha}$, $p_i^{\alpha_i}$, $1 \leq i \leq r$. Согласно первому утверждению леммы 7.1 теперь имеем

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{2^{\alpha}}, \qquad a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{p_i^{\alpha_i}}, \quad i = 1, \dots, r.$$

Из этих сравнений, поскольку все числа $2^\alpha$, $p_i^{\alpha_i}$, $1 \le i \le r$, попарно взаимно просты, следует, что разность $a^{\frac{\varphi(m)}{2}} - 1$ делится на их произведение, т.е. делится на число $m$. Сравнение (7.11) доказано во всех случаях.

Оно, как указывалось раньше, означает, что показатель по модулю $m$ каждого числа $a$ взаимно простого с $m$ не превосходит $\frac{\varphi(m)}{2}$ и значит меньше $\varphi(m)$. Поэтому первообразных корней по модулю $m$ не существует. □

## 7.5 Индексы и их свойства

Рассмотрим сначала случаи $m = p^k$ или $m = 2p^k$, где $p$ – простое нечетное число и $k \ge 1$, 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 $\gamma$, удовлетворяющее условиям

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

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

$$a \equiv g^{\operatorname{ind}_g a} \pmod{m}, \qquad 0 \le \operatorname{ind}_g a < \varphi(m). \tag{7.14}$$

Свойства индексов описывает следующая лемма.

**Лемма 7.3.** *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* $(\operatorname{ind}_b a, \varphi(m)) = 1$.

*Доказательство.* Справедливы сравнения

$$g^{\operatorname{ind}_g ab} \equiv ab \equiv g^{\operatorname{ind}_g a} \cdot g^{\operatorname{ind}_g b} = g^{\operatorname{ind}_g a + \operatorname{ind}_g b} \pmod m$$

из которых, так как $g$ – первообразный корень по модулю $m$, получаем первое утверждение леммы, см. следствие из леммы 7.1.

С помощью (7.14) находим

$$b^{\operatorname{ind}_a c \cdot \operatorname{ind}_b a} = \left(b^{\operatorname{ind}_b a}\right)^{\operatorname{ind}_a c} \equiv a^{\operatorname{ind}_a c} \equiv c \equiv b^{\operatorname{ind}_b c} \pmod m.$$

Пользуясь следствием из леммы 7.1 заключаем

$$\varphi(m) | (\operatorname{ind}_a c \cdot \operatorname{ind}_b a - \operatorname{ind}_b c).$$

Это доказывает сравнение из второго утверждения леммы.

Обозначим $d = (\operatorname{ind}_b a, \varphi(m))$. Справедливы сравнения по модулю $m$

$$a^{\frac{\varphi(m)}{d}} \equiv b^{\frac{\varphi(m)}{d} \cdot \operatorname{ind}_b a} = \left(b^{\varphi(m)}\right)^{\frac{\operatorname{ind}_b a}{d}} \equiv 1 \pmod m.$$

Так как $a$ первообразный корень по модулю $m$, это сравнение возможно лишь в случае $d = 1$. □

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

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

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

Заметим, что

$$d \cdot d_0 \cdot d_1 \cdots d_r = 2^{\alpha-1} \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) = \varphi(m) \tag{7.15}$$

при любом $\alpha \geq 0$.

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

Если $a$ – целое число взаимно простое с модулем $m$, то

$$(a, 2^\alpha) = 1, \quad (a, p_1^{\alpha_1}) = 1, \quad \ldots \quad (a, p_r^{\alpha_r}) = 1$$

и согласно теоремам 7.2 и 7.3 существуют целые числа $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_r$, удовлетворяющие сравнениям

$$a \equiv \begin{cases} (-1)^\gamma 5^{\gamma_0} & (\mathrm{mod}\, 2^\alpha), \\ g_1^{\gamma_1} & (\mathrm{mod}\, p_1^{\alpha_1}), \\ \ldots & \ldots \\ g_r^{\gamma_r} & (\mathrm{mod}\, p_r^{\alpha_r}). \end{cases} \tag{7.16}$$

Из теоремы 7.3 и определения первообразного корня следует также, что набор чисел $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_r$ будет определен единственным способом, если наложить дополнительные условия

$$0 \leq \gamma < d, \quad 0 \leq \gamma_0 < d_0, \quad \ldots, \quad 0 \leq \gamma_r < d_r. \tag{7.17}$$

Определенная единственным способом совокупность чисел $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_r$, удовлетворяющая условиям (7.16), (7.17) называется *системой индексов* числа $a$. Каждый элемент системы индексов будет индексом числа $a$, по соответствующему модулю. Систему индексов числа $a$ будем обозначать

$$\gamma(a), \gamma_0(a), \gamma_1(a), \ldots, \gamma_r(a).$$

Числа, лежащие в одном классе вычетов по модулю $m$ и взаимно простые с $m$, очевидно, имеют одинаковые системы индексов. И наоборот, для каждой системы индексов система сравнений (7.16) относительно неизвестного $a$ имеет согласно китайской теореме об остатках, см. §5.3, единственное решение по модулю $m$. Это решение есть класс вычетов по модулю $m$, состоящий из чисел взаимно простых с $m$. Заметим также, что равенства $\gamma(a) = \gamma_0(a) = \cdots = \gamma_r(a) = 0$

выполняются лишь для чисел, сравнимых с 1 по модулю $m$. Установленное взаимно однозначное соответствие между элементами группы $(\mathbb{Z}/m\mathbb{Z})^*$ и системами индексов согласуется с равенством (7.15).

**Лемма 7.4.** *Индексы произведения двух чисел сравнимы по модулям $d, d_0, \ldots, d_r$ с суммами соответствующих индексов сомножителей, т.е. для любых двух чисел $a, b$ взаимно простых с модулем $m$, выполняются сравнения*

$$\begin{aligned} \gamma(ab) &\equiv \gamma(a) + \gamma(b) \pmod{d}, \\ \gamma_0(ab) &\equiv \gamma_0(a) + \gamma_0(b) \pmod{d_0}, \\ &\ldots\ldots\ldots\ldots \\ \gamma_r(ab) &\equiv \gamma_r(a) + \gamma_r(b) \pmod{d_r}. \end{aligned} \tag{7.18}$$

Другими словами сопоставление

$$a(\mathrm{mod}\, m) \mapsto (\gamma(\mathrm{mod}\, d),\ \gamma_0(\mathrm{mod}\, d_0),\ \ldots,\ \gamma_r(\mathrm{mod}\, d_r))$$

является изоморфным отображением мультипликативной группы $(\mathbb{Z}/m\mathbb{Z})^*$ на прямую сумму аддитивных групп $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/d_0\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\mathbb{Z}$.

*Доказательство.* Сравнения (7.18) по модулям $d_k$, $1 \le k \le r$, следуют из первого утверждения леммы 7.3.

Для доказательства первых двух сравнений (7.18) находим, пользуясь первым сравнением (7.16),

$$(-1)^{\gamma(ab)} 5^{\gamma_0(ab)} \equiv ab \equiv (-1)^{\gamma(a)+\gamma(b)} 5^{\gamma_0(a)+\gamma_0(b)} \pmod{2^\alpha}. \tag{7.19}$$

При $\alpha \le 1$ имеем $d = d_0 = 1$ и нужные сравнения (7.18), очевидно выполняются.

Если $\alpha = 2$, то $d = 2$, $d_0 = 1$ и сравнение (7.19) принимает вид $(-1)^{\gamma(ab)} \equiv (-1)^{\gamma(a)+\gamma(b)} \pmod 4$, откуда следует $\gamma(ab) \equiv \gamma(a) + \gamma(b) (\mathrm{mod}\, d)$.

В случае $\alpha \ge 3$, переходя в (7.19) к сравнению по модулю 4 находим $(-1)^{\gamma(ab)} \equiv (-1)^{\gamma(a)+\gamma(b)} \pmod 4$ и, значит, $\gamma(ab) \equiv \gamma(a) +$

$\gamma(b)(\mathrm{mod}\, d)$. Но тогда $5^{\gamma_0(ab)} \equiv 5^{\gamma_0(a)+\gamma_0(b)} \pmod{2^\alpha}$, откуда, согласно второму утверждению теоремы 7.3, находим $\gamma_0(ab) \equiv \gamma_0(a)+\gamma_0(b) \pmod{2^{\alpha-2}}$. Это завершает доказательство леммы. □

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

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

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

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

Из этого определения следует, что для $b = c_{-1}^{\gamma(a)} c_0^{\gamma_0(a)} c_1^{\gamma_1(a)} \cdots c_r^{\gamma_r(a)}$ выполняется сравнение

$$b \equiv \begin{cases} (-1)^{\gamma(a)} 5^{\gamma_0(a)} & (\mathrm{mod}\, 2^\alpha), \\ g_1^{\gamma_1(a)} & (\mathrm{mod}\, p_1^{\alpha_1}), \\ \cdots & \cdots \\ g_r^{\gamma_r(a)} & (\mathrm{mod}\, p_r^{\alpha_r}). \end{cases}$$

Из этого сравнения и (7.16) следует, что разность $b - a$ делится на каждый из модулей $2^\alpha, p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$. Таким образом, для каждого целого числа $a$, взаимно простого с модулем $m$ выполняется сравнение

$$a \equiv c_{-1}^{\gamma(a)} c_0^{\gamma_0(a)} c_1^{\gamma_1(a)} \cdots c_r^{\gamma_r(a)} \pmod{m}. \tag{7.20}$$

Из определения чисел $c_{-1}, c_0, \ldots, c_r$ следует, что их показатели равны соответственно $d_{-1}, d_0, \ldots, d_r$. Отсюда, поскольку системы индексов для чисел, не сравнимых по модулю $m$ различны, следует, что *для каждого взаимно простого с $m$ целого числа $a$ существует единственный набор чисел $k_{-1}, k_0, \ldots, k_r$, удовлетворяющих условиям*

$$a \equiv c_{-1}^{k_{-1}} c_0^{k_0} c_1^{k_1} \cdots c_r^{k_r} \pmod{m}, \tag{7.21}$$

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

другими словами мультипликативная группа $(\mathbb{Z}/m\mathbb{Z})^*$ есть прямое произведение своих циклических подгрупп, порожденных классами вычетов, содержащими числа $c_{-1}, c_0, \ldots, c_r$. При этом набор показателей степени в (7.21) совпадает с системой индексов числа $a$.

## 7.6 Дискретное логарифмирование

Согласно (7.14) и лемме 7.3 свойства индексов напоминают свойства обычных логарифмов от действительных чисел. Поэтому иногда в современной литературе индексы называют дискретными логарифмами, а процесс их нахождения – дискретным логарифмированием.

Далее мы покажем, каким образом задача вычисления $\mathrm{ind}_b(a)$ по модулю $p^{n+1}$, при $n \ge 1$, т.е. вычисления единственного целого числа, удовлетворяющего условиям

$$b^x \equiv a \pmod{p^{n+1}}, \qquad 0 \le x < p^n(p-1), \tag{7.22}$$

где $p$ – нечетное простое число, $b$ – фиксированный первообразный корень по модулю $p^{n+1}$, $(a,p) = 1$, может быть достаточно быстро сведена к аналогичной задаче в случае $n = 0$.

Пусть $p$ – простое нечетное и $n \ge 1$ – целое число. По теореме Эйлера для каждого целого $a$, не делящегося на $p$, число $a^{\varphi(p^n)} - 1$ делится на $p^n$, и потому существует единственное целое число $Q(a)$ такое, что

$$Q(a) \equiv \frac{a^{\varphi(p^n)} - 1}{p^n} \pmod{p^n} \qquad 0 \le Q(a) < p^n. \tag{7.23}$$

Определенная этими условиями функция $Q(a)$ называется *частным Ферма*. Она обладает следующими свойствами.

**Лемма 7.5.** *1) Для любых двух целых чисел $a, b$, не делящихся на $p$, выполняется сравнение*

$$Q(ab) \equiv Q(a) + Q(b) \pmod{p^n}, \tag{7.24}$$

*2) Функция $Q(a)$ имеет период $p^{n+1}$, т.е. для любого целого $a$, не делящегося на $p$, выполняется равенство $Q(a+p^{n+1}) = Q(a)$.*
*3) Если $b$ – первообразный корень по модулю $p^{n+1}$, то $Q(b)$ не делится на $p$.*

*Доказательство.* Из равенства (7.23) следует

$$a^{\varphi(p^n)} \equiv 1 + Q(a)p^n \pmod{p^{2n}}. \tag{7.25}$$

Пользуясь этими сравнениями для $a, b$ и $ab$, находим

$$1 + Q(ab)p^n \equiv (ab)^{\varphi(p^n)} \equiv (1 + Q(a)p^n)(1 + Q(b)p^n) \pmod{p^{2n}}.$$

Раскрывая скобки в правой части, находим сравнение

$$Q(ab)p^n \equiv Q(a)p^n + Q(b)p^n \pmod{p^{2n}}.$$

Разделив обе его части и модуль на $p^n$, приходим к (7.24).

С помощью формулы Ньютона для бинома находим сравнение по модулю $p^{2n}$

$$\begin{aligned}(a + p^{n+1})^{\varphi(p^n)} &= a^{\varphi(p^n)} + \varphi(p^n)a^{\varphi(p^n)-1}p^{n+1} + \ldots \equiv \\ &\equiv a^{\varphi(p^n)} + a^{\varphi(p^n)-1}(p-1)p^{2n} \equiv a^{\varphi(p^n)} \pmod{p^{2n}}.\end{aligned}$$

Благодаря (7.25), получаем

$$1 + Q(a + p^{n+1})p^n \equiv 1 + Q(a)p^n \pmod{p^{2n}}$$

и, $Q(a+p^{n+1}) \equiv Q(a) \pmod{p^n}$. Оба целых числа $Q(a), Q(a+p^{n+1})$ лежат на промежутке $0 \leq x < p^n$ и разность их по доказанному делится на $p^n$. Значит, они равны. Второе утверждение леммы доказано.

Пусть $g_1$ – первообразный корень по модулю $p^{n+1}$, построенный в теореме 7.2. Тогда

$$g_1^{\varphi(p^n)} \equiv 1 + Q(g_1)p^n \pmod{p^{2n}}.$$

Из равенства (7.5) при $\beta = n-1$ следует

$$\nu_p\left(g_1^{\varphi(p^n)} - 1\right) = n.$$

Значит, $\nu_p(Q(g_1)) = 0$ и $p \nmid Q(g_1)$.

Справедливо сравнение $b \equiv g_1^{\operatorname{ind}_{g_1} b} \pmod{p^{n+1}}$. С помощью уже доказанных утверждений 1) и 2) леммы находим

$$Q(b) = Q\left(g_1^{\operatorname{ind}_{g_1} b}\right) \equiv \operatorname{ind}_{g_1} b \cdot Q(g_1) \pmod{p^n}.$$

Из второго утверждения леммы 7.3 следует, что $\operatorname{ind}_{g_1} b$ не делится на $p$. Теперь можно утверждать, что $p \nmid Q(b)$. Лемма полностью доказана. □

Поскольку $b$ есть первообразный корень по модулю $p^{n+1}$, то, как указывалось ранее, $b$ будет первообразным корнем и по модулю $p$. Значит найдется единственное целое число $x_0$, удовлетворяющее условиям

$$a \equiv b^{x_0} \pmod{p}, \qquad 0 \le x_0 < \varphi(p) = p-1.$$

**Теорема 7.5.** *Для каждого целого $a$, не делящегося на $p$, системе сравнений*

$$\begin{cases} Q(b)x & \equiv Q(a) \pmod{p^n}, \\ x & \equiv x_0 \pmod{p-1}. \end{cases} \tag{7.26}$$

*удовлетворяет единственное целое число, принадлежащее промежутку $0 \le x < p^n(p-1)$, оно удовлетворяет также сравнению (7.22).*

*Доказательство.* Так как по лемме 7.5 коэффициент $Q(b)$ не делится на $p$, то первое сравнение системы (7.26) имеет единственное решение $x \equiv x_1 \pmod{p^n}$. Значит, система (7.26) равносильна системе сравнений

$$\begin{cases} x & \equiv x_1 \pmod{p^n}, \\ x & \equiv x_0 \pmod{p-1}, \end{cases}$$

имеющей согласно китайской теореме об остатках единственное решение по модулю $p^n(p-1)$. Итак, каждой из систем условий (7.22), (7.26) удовлетворяет единственное целое число. Докажем их совпадение.

Пусть целое $k$, удовлетворяет (7.22). Тогда $b^k \equiv a \pmod{p^{n+1}}$, и согласно лемме 7.5 имеем

$$Q(a) = Q(b^k) \equiv kQ(b) \pmod{p^n},$$

т.е. $k$ удовлетворяет первому из сравнений (7.26).

Из (7.22) следует, что $b^k \equiv a \equiv b^{x_0} \pmod{p}$. Так как $b$ – первообразный корень по модулю $p$, по следствию из леммы 7.1, находим $k \equiv x_0 \pmod{p-1}$, т.е. выполняется и второе сравнение системы (7.26). Теорема доказана. □

Если известно число $x_0$, то решение системы сравнений может быть найдено достаточно быстро с помощью алгоритмов, изложенных в §§5.2, 5.3. Числа $Q(a), Q(b)$ легко вычисляются, как решения сравнений вида (7.25) при помощи тех же алгоритмов. Вычисление чисел вида $a^{\varphi(p^n)} \pmod{p^{2n}}$ выполняется с помощью алгоритма, описанного в §4.7.

Обсудим теперь задачу дискретного логарифмирования по простому нечетному модулю. Приведем ее формулировку в этом случае.

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

$$b^x \equiv a \pmod{p}. \tag{7.27}$$

Решение этой задачи очень трудоемко в вычислительном отношении. Не случайно в конце практически всех учебников по элементарной теории чисел приводятся таблицы индексов (дискретных логарифмов). 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, но весьма правдоподобных гипотез теории чисел.

В конце 2006 года А.Я.Дорофеев, Д.М.Дугин и Д.В. Матюхин опубликовали в Интернет[2] очередной рекорд дискретного логарифмирования. В качестве модуля было выбрано простое число, записываемое 135 десятичными знаками,

$$p = \left[2^{446}\pi\right] + 63384 = 570857799147913943142073298159453290747376295550451905113865375911865918588022945237020702500203437615419679961659928369778961422486479.$$

Число $g = 7$ является первообразным корнем по этому модулю. Авторы рекорда вычислили

$$\mathrm{ind}_g\, 11 = 263809415442532684357793832777626704483700110050961631240336610545143645723034872275030016383962573841181649388892154031068496007427 12.$$

В случае обычных логарифмов в поле 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 $\mid x \mid < 1$ ряда

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

Логарифмы по произвольному основанию $b$ могут быть вычислены с помощью тождества

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

Подобное ему в дискретном случае доказано в лемме 7.3. Но в случае дискретных логарифмов нет основания, по которому логарифмы вычислялись бы столь же быстро, как натуральные в поле действительных чисел.

Для решения задачи дискретного логарифмирования (7.27) можно вычислять последовательно степени $b^k \pmod p$ при $k = 1, 2, \ldots,$

[2] См. http://www.nabble.com/Discrete-logarithm-in-GF(p)—-135-digits-t2870677.html

$p-1$ пока не будет получено значение, сравнимое с $a$ по модулю $p$. Число $k$, соответствующее этому значению, и будет искомым индексом $a$. Такой способ вычисления индексов требует слишком большого количества арифметических операций. Следующий простой метод, предложенный в 1962г. А.О. Гельфондом, так называемый метод уравнивания, позволяет находить индексы существенно быстрее.[3]

**Алгоритм.** *Пусть $p$ - простое число, $p \geq 3$, $a$ - первообразный корень по модулю $p$, $b \in \mathbb{Z}, p \nmid b$. Требуется решить сравнение (7.27).*

*1. Вычислить $H = [\sqrt{p}] + 1$.*

*2. Положить $c = a^H \pmod{p}$.*

*3. Составить два набора чисел*

$$S = \{c^k \pmod{p}, \quad 1 \leq k \leq H\}$$
$$T = \{b \cdot a^\ell \pmod{p}, \quad 1 \leq \ell \leq H\}.$$

*Имеется в виду, что множества $S$ и $T$ содержат наименьшие неотрицательные вычеты соответствующих классов.*

*4. Упорядочить оба набора $S, T$ по возрастанию и найти совпавшие элементы. Это даст числа $k, \ell$, для которых выполнено*

$$c^k \equiv b \cdot a^\ell \pmod{p}.$$

*5. Положить $x \equiv Hk - \ell \pmod{p-1}$, $0 \leq x < p-1$.*

Найденное алгоритмом число $x$ удовлетворяет сравнению (7.27). Действительно, по малой теореме Ферма, выполняется

$$a^\ell a^x \equiv a^{Hk} \equiv c^k \equiv ba^\ell \pmod{p}.$$

Разделив обе части этого сравнения на $a^\ell$, поскольку $p \nmid a$, находим $a^x \equiv b \pmod{p}$.

Осталось доказать, что при любых числах $a, b$, удовлетворяющих условиям алгоритма, множества $S$ и $T$ имеют общий элемент. Пусть

[3] В зарубежной литературе этот метод называется методом больших и малых шагов

$x$ – целое число, удовлетворяющее сравнению (7.27) и неравенствам $0 \le x < p-1$. Разделив $x$ с остатком на $H$, получим такие целые числа $y, z$, что

$$x = Hy + z, \qquad 0 \le z < H.$$

Тогда $0 \le y \le \frac{x}{H} < \frac{p}{H} < H$, ведь $H = [\sqrt{p}] + 1 > \sqrt{p}$. Положим $k = y + 1, \ell = H - z$. Справедливы неравенства $1 \le k \le H, 1 \le \ell \le H$. Поэтому числа $s = c^k \pmod p$, $0 \le s < p$ и $t \equiv b \cdot a^\ell \pmod p$, $0 \le t < p$ лежат в множествах $S$ и $T$ соответственно. Кроме того,

$$t \equiv ba^\ell \equiv a^{Hy+z+\ell} = a^{H(y+1)} \equiv c^k \equiv s \pmod p,$$

так что $s = t$.

Нетрудно проверить, что выполнение алгоритма уравнивания требует $(\sqrt{p} \ln p)$ арифметических операций и операций перестановки элементов при упорядочении множеств $S$ и $T$. Он существенно быстрее перебора множества всех возможных решений. Однако и этот алгоритм не позволяет находить индексы при больших $p$. Еще одним его недостатком является очень большая память, необходима для хранения в компьютере множеств $S$ и $T$.

Высокая сложность задачи дискретного логарифмирования лежит в основе некоторых ее криптографических применений. Приведем здесь только один пример, связанный с построением так называемого общего ключа для шифрования информации.

Рассмотрим ситуацию, когда два корреспондента, скажем $A$ и $B$ хотели бы обмениваться информацией через Интернет, причем так, чтобы эта информация оставалась недоступной для остальных лиц. Известны методы шифрования, зависящие от так называемого ключа. Тот, кто знает ключ, может раскрыть зашифрованное сообщение, а тот, кому этот ключ неизвестен, если и сможет расшифровать сообщение, то за столь большое время, что раскрытая информация уже потеряет свое значение. Наши корреспонденты, не имея иного сообщения, кроме как через Интернет, хотят выработать общий ключ для шифрования информации. Мы будем представлять себе ключ, как некоторую последовательность цифр, т.е. целое число.

Для решения подобных задач на практике иногда используется такой метод. Корреспонденты $A$ и $B$ обмениваясь информацией через Интернет вырабатывают некоторое большое простое число $p$ и находят первообразный корень $g$ по модулю $p$. После чего каждый из них:
1. *выбирает на промежутке от* 1 *до* $p-1$ *случайное число* $x(A)$ *или* $x(B)$ *соответственно и вычисляет*

$$y(A) \equiv g^{x(A)} \pmod{p}, \quad \textit{или} \quad y(B) \equiv g^{x(B)} \pmod{p};$$

*2. посылает через Интернет своему корреспонденту найденное число* $y(A)$ *или* $y(B)$*:*

$$A \overset{y(A)}{\dashrightarrow} B; \qquad B \overset{y(B)}{\dashrightarrow} A;$$

*3. вычисляет* $(y(B))^{x(A)} \pmod{p}$ *или* $(y(A))^{x(B)} \pmod{p}$*. Ясно, что при этом оба получат одно и то же число*

$$k \equiv (y(B))^{x(A)} \equiv g^{x(B)x(A)} \equiv (y(A))^{x(B)} \pmod{p}, \qquad 0 < k < p,$$

*которое и будет использоваться в качестве секретного общего ключа.*

Через Интернет будут переданы числа $p, g, g^{x(A)} \pmod{p}, g^{x(B)} \pmod{p}$. Попытка определить по ним ключ $k$ связана с необходимостью вычисления $x(A)$ или $x(B)$, т.е. решением задачи дискретного логарифмирования. Даже при сравнительно небольшом $p$ это требует неприемлемо больших вычислительных затрат времени.

Рассмотрим, например, простое число $p = 1000003$. Справедливо разложение на простые множители $p - 1 = 2 \cdot 3 \cdot 166667$. С помощью леммы 7.2 легко проверить, что 2 есть первообразный корень по модулю $p$. Действительно

$$2^6 \equiv 64 (\mathrm{mod}\, p), \quad 2^{500001} \equiv -1 (\mathrm{mod}\, p), \quad 2^{333334} \equiv 499501 (\mathrm{mod}\, p).$$

Выберем, скажем, $x(A) = 394792$, $x(B) = 851982$. Тогда

$$y(A) = 774919 \equiv 2^{394792} (\mathrm{mod}\, p), \quad y(B) = 568356 \equiv 2^{851982} (\mathrm{mod}\, p).$$

Общий ключ, соответствующий указанному выбору чисел $x(A)$ и $x(B)$ равен

$$958970 \equiv 568356^{394792} (\mathrm{mod}\, p), \qquad 958970 \equiv 774919^{851982} (\mathrm{mod}\, p).$$

Итак, в рассматриваемом случае $k = 958970$.

Рассмотрим при том же простом $p$ иной выбор чисел $x(A) = 829267$, $x(B) = 723759$. Тогда

$$y(A) = 58188 \equiv 2^{829267} (\mathrm{mod}\, p), \qquad y(B) = 804734 \equiv 2^{723759} (\mathrm{mod}\, p)$$

и общий ключ $k$ вычисляется так

$$3 \equiv 804734^{829267} \pmod{p}, \qquad 3 \equiv 58188^{723759} \pmod{p}$$

Значит, в этом случае $k = 3$. Такой "секретный"ключ, наверное, неприемлем и наши корреспонденты $A$ и $B$ должны выбрать иные случайные числа.

В последнем примере числа $x(A)$, $x(B)$ подбирались специально. Подобная ситуация встречается крайне редко.

## 7.7 Двучленные сравнения

В этом параграфе мы рассмотрим сравнения вида

$$x^n \equiv a \pmod{m}, \tag{7.28}$$

где $m = p^\alpha$ или $m = 2p^\alpha$, $p$ – простое нечетное и $\alpha$ – целое положительное число. Будем также предполагать, что $a$ – целое, взаимно простое с $m$.

Обозначим буквой $g$ первообразный корень по модулю $m$, и для каждого целого числа $b$, взаимно простого с $m$, символом $\mathrm{ind}\, b$ будем обозначать индекс числа $b$, вычисленный по модулю $m$ при основании $g$. Следующая теорема дает два критерия разрешимости сравнения (7.28).

**Теорема 7.6.** *В указанных выше условиях равносильны следующие три утверждения:*
*1) сравнение (7.28) разрешимо,*
*2) с* $d = (n, \varphi(m))$ *выполняется сравнение*

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}, \tag{7.29}$$

*3)* $d \mid \operatorname{ind} a$.

*В случае разрешимости сравнение (7.28) имеет в точности* $d$ *решений.*

*Доказательство.* 1) $\Rightarrow$ 2) Предположим, что сравнение (7.28) разрешимо и обозначим буквой $c$ некоторое его решение. Тогда $c^n \equiv a \pmod{m}$ и по теореме Эйлера

$$a^{\frac{\varphi(m)}{d}} \equiv c^{\frac{n\varphi(m)}{d}} \equiv \left(c^{\varphi(m)}\right)^{\frac{n}{d}} \equiv 1 \pmod{m}.$$

2) $\Rightarrow$ 3) Если выполняется условие (7.29), то

$$g^{\frac{\varphi(m)}{d}\cdot \operatorname{ind} a} \equiv a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}.$$

Но тогда целое число $\frac{\varphi(m)}{d} \cdot \operatorname{ind} a$ делится на $\varphi(m)$. Следовательно $d \mid \operatorname{ind} a$, т.е. выполняется третье из утверждений.

3) $\Rightarrow$ 1) Допустим, что $a$ удовлетворяет условию $d \mid \operatorname{ind} a$. Рассмотрим сравнение

$$ny \equiv \operatorname{ind} a \pmod{\varphi(m)} \tag{7.30}$$

относительно неизвестной $y$. Согласно теореме 5.1 сравнение (7.30) разрешимо и имеет в точности $d$ решений. Обозначим наименьшие неотрицательные вычеты этих $d$ классов вычетов по модулю $\varphi(m)$ буквами $y_j$, $j = 1, \ldots, d$. И определим также $x_j$ как наименьшие неотрицательные вычеты в классах $g^{y_j} \pmod{m}$, $j = 1, \ldots, d$. Тогда $y_j = \operatorname{ind} x_j$ и

$$x_j^n \equiv g^{n \operatorname{ind} x_j} \equiv g^{\operatorname{ind} a} \equiv a \pmod{m}.$$

Итак, сравнение (7.28) разрешимо и имеет не менее $d$ решений. Это, в частности, завершает доказательство эквивалентности трех утверждений теоремы.

Выше было доказано, что в случае разрешимости сравнение (7.28) имеет не менее $d$ решений. Покажем, что никаких других решений, кроме построенных, это сравнение не имеет. Если $c$ – целое число, удовлетворяющее сравнению (7.28), то $g^{n\operatorname{ind} c} \equiv g^{\operatorname{ind} a} \pmod m$. С помощью следствия из леммы 7.1 заключаем, что $n\operatorname{ind} c \equiv \operatorname{ind} a \pmod{\varphi(m)}$. Но тогда индекс $\operatorname{ind} c$ сравним по модулю $\varphi(m)$ с одним из чисел $y_j$, а число $c$ сравнимо по модулю $m$ с одним из $x_j$. Теорема доказана. □

В частности, получаем

**Следствие 7.3.** *Если $(n, \varphi(m)) = 1$, то сравнение (7.28) при любом $a$, взаимно простом с модулем $m$, имеет единственное решение.*

Целое число $a$, взаимно простое с модулем $m$, называется *$n$-степенным вычетом* или вычетом степени $n$, если сравнение $x^n \equiv a \pmod{p^\alpha}$ разрешимо. В противном случае число $a$ называется *$n$-степенным невычетом*. При $n = 2, 3, 4$ применяется также терминология квадратичный, кубический, биквадратичный вычет или невычет.

Из этого определения следует, что числа, сравнимые по модулю $m$, одновременно являются $n$-степенными вычетами или невычетами.

С помощью введенного понятия первое утверждение теоремы 7.6 может быть переформулировано в виде критерия для отыскания степенных вычетов.

**Следствие 7.4.** *Целое число $a$, взаимно простое с модулем $m$, будет вычетом степени $n \geq 2$, если и только если выполняется сравнение (7.29).*

**Следствие 7.5.** *Если $d = (n, \varphi(m))$, то вычеты степени $n$ по модулю $m$ совпадают с вычетами степени $d$ по тому же модулю.*

Это утверждение выполняется в силу равенства $(n, \varphi(m)) = d = (d, \varphi(m))$ и предыдущего следствия.

**Следствие 7.6.** *Число классов $n$-степенных вычетов по модулю $m$ равно $\frac{\varphi(m)}{d}$, где $d = (n, \varphi(m))$.*

В силу теоремы число $a$, взаимно простое с $m$, будет $n$-степенным вычетом в том и только том случае, когда $d | \operatorname{ind} a$. Но среди чисел $0, \ldots, \varphi(m) - 1$ – возможных значений индексов, имеется в точности $\frac{\varphi(m)}{d}$, делящихся на $d$. Следствие доказано.

# Глава 8

# Цепные дроби

В связи с различными причинами иногда приходится заменять действительные числа их приближенными значениями. Часто при этом хочется обеспечить необходимую точность выбирая рациональное приближение с по возможности меньшим знаменателем.

Вероятно, наиболее известный исторический пример такой замены связан с устройством календарей. В настоящее время считается, что Земля совершает полный оборот вокруг Солнца за 365,24219 суток. Конечно, это число условно. Ведь с течением времени вращение Земли вокруг Солнца замедляется, кроме того Земля вокруг своей оси вращается неравномерно, а это сказывается на продолжительности суток. Так что приведенное выше число, конечно, является усредненным.

Простейшее приближение к продолжительности года $365,25 = 365\frac{1}{4}$ было положено в основу юлианского календаря, созданного александрийскими астрономами во главе с Созигеном. Указом Юлия Цезаря в 46г. до н.э. этот календарь был введен во всей Римской империи. Поскольку год должен содержать целое число суток, то в юлианском календаре на каждые три года продолжительностью в 365 дней приходился один високосный год продолжительностью 366 дней. Так обеспечивается средняя продолжительность года в $365\frac{1}{4}$ суток. Юлианский год чуть длиннее истинной продолжительности обращения Земли вокруг Солнца. Неболь-

шая ошибка (11 минут и 14 секунд за год) по прошествии 128 лет привела к ошибке в одни сутки и продолжала накапливаться. В 1582г. в католических странах специальным распоряжением папы Григория XIII был введен новый календарь. В качестве приближения к истинной продолжительности года было выбрано число $365\frac{97}{400} = 365 + \frac{1}{4} - \frac{3}{400} = 365,2425$, дающее ошибку в одни сутки примерно за 3300 лет. Ценой лучшего приближения стало усложнение календаря. Високосными стали считаться годы, номера которых делятся на 4, но не делятся на 100, а кроме того годы, номера которых делятся на 400. По григорианскому календарю годы с номерами 1700, 1800, 1900 високосными не являлись, в то время, как 2000 год был високосным. В России григорианский календарь был введен в 1918 году.

Наконец, отметим что персидский астроном, математик и поэт Омар Хайям предложил календарь, основанный на приближении $365\frac{8}{33} = 365,242424\ldots$. Этот календарь, введенный в 1079 г. и действовавший в Иране до середины XIX века, содержал 8 високосных лет, повторявшихся с циклом в 33 года. На протяжении цикла между 8 последовательно идущими високосными годами располагались 7 отрезков по 3 обыкновенных года в 365 дней и один отрезок в 4 обыкновенных года. Ошибка в одни сутки накапливалась в этом календаре примерно за 4500 лет.

Заметим, что календарные системы играют важную роль в организации религиозной жизни. Существенной компонентой лунно-солнечных календарей, какими в действительности являются и юлианский, и григорианский календари, является правильная организация не только последовательности солнечных лет в 365 и 366 дней, но и лунных месяцев. Так христианская Пасха по постановлению Никейского Собора 325г. должна праздноваться в первое воскресение после первого полнолуния, следующего за днем весеннего равноденствия. При этом имеются в виду не астрономические полнолуние и равноденствие, а даты, вычисляемые по определенным канонизированным математическим правилам. Если учесть, что сред-

няя продолжительность отрезка времени, за который Луна проходит все фазы от новолуния до новолуния, равна 29,530588 суток, а лунные месяцы поэтому должны содержать по 29 и 30 дней, получается весьма сложная проблема согласования последовательности годов с последовательностью месяцев, так чтобы обе последовательности достаточно точно следовали за движениями Солнца и Луны. В обыденной жизни лунная составляющая юлианского и григорианского календарей не принимается во внимание.

Цепные дроби дают алгоритм, позволяющий находить в некотором смысле наилучшие приближения действительных чисел рациональными.

## 8.1 Теорема Дирихле о приближении действительных чисел рациональными

Рациональные числа расположены на действительной оси всюду плотно, т.е. для любого действительного числа $\alpha$ в любой его $\varepsilon$ окрестности найдется бесконечно много рациональных чисел. Другими словами, при любом $\varepsilon > 0$ неравенство

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon \tag{8.1}$$

имеет бесконечное количество решений в различных рациональных числах $\frac{p}{q}$. Задача усложняется, если интересоваться существованием решения с не очень большим знаменателем, ограничив его в зависимости от $\varepsilon$. Например, ответ на вопрос, существует ли решение с условием $q \leq \varepsilon^{-1/2}$ не очевиден.

В 1842г. Дирихле доказал теорему, позволяющую устанавливать существование решений неравенства (8.1) с ограничением величины знаменателя.

**Теорема 8.1.** *Пусть $\alpha$ и $T$ – действительные числа, причем $T \geq 1$. Тогда существуют целые числа $p, q$, удовлетворяющие неравен-*

*ствам*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qT}, \qquad 1 \le q \le T.$$

*Доказательство.* Как и ранее будем обозначать $[x]$, $\{x\}$ целую и дробную части числа $x$. Положим $N = [T]$ и разобьем отрезок $[0;1]$ на $N+1$ отрезков

$$\frac{u}{N+1} \le x \le \frac{u+1}{N+1}, \qquad u = 0, 1, \ldots, N,$$

длины $\frac{1}{N+1}$.

Рассмотрим $N+1$ чисел

$$\{k\alpha\}, \qquad k = 0, 1, \ldots, N. \tag{8.2}$$

Если хотя бы одно из них попадает в крайний правый из маленьких отрезков, т.е. удовлетворяет неравенствам

$$\frac{N}{N+1} \le \{k\alpha\} < 1,$$

то, получим

$$|k\alpha - [k\alpha] - 1| = 1 - \{k\alpha\} \le \frac{1}{N+1} < \frac{1}{T}.$$

Очевидно выполняется $k \ne 0$, поэтому $1 \le k \le N \le T$. Положив теперь $q = k$, $p = [k\alpha] + 1$, получаем нужное утверждение.

Если же крайний правый отрезок не содержит ни одной из точек (8.2), то все они распределяются между оставшимися $N$ отрезками. Но множество (8.2) состоит из $N+1$ чисел. Значит, по крайней мере один из построенных малых отрезков содержит не менее двух чисел, отвечающих различным значениям $k$. Пусть числа $\{k_1\alpha\}$ и $\{k_2\alpha\}$ принадлежат какому то из малых отрезков. Не уменьшая общности можно считать, что $k_1 > k_2$. Из неравенства $|\{k_1\alpha\} - \{k_2\alpha\}| \le \frac{1}{N+1}$, находим

$$|k_1\alpha - [k_1\alpha] - k_2\alpha + [k_2\alpha]| \le \frac{1}{N+1}.$$

Положив $q = k_1 - k_2 > 0$ и $p = [k_1\alpha] - [k_2\alpha]$, получаем требуемые неравенства

$$1 \le q = k_1 - k_2 \le N \le T, \qquad |q\alpha - p| \le \frac{1}{N+1} < \frac{1}{T}$$

□

**Следствие 8.1.** *Пусть $\alpha$ – иррациональное число. Тогда существует бесконечное множество несократимых дробей $\frac{p}{q}$, удовлетворяющих неравенству*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{8.3}$$

*Доказательство.* Предположим, что множество решений неравенства (8.3) в несократимых дробях конечно. Обозначим все эти решения

$$\frac{p_1}{q_1}\ ,\ \frac{p_2}{q_2}\ ,\ \dots\ ,\ \frac{p_m}{q_m}\ . \tag{8.4}$$

Так как $\alpha$ – иррациональное число, то $\delta = \min_i\{|q_i\alpha - p_i|\} > 0$. Положим $T = \delta^{-1}$. По теореме 8.1 существуют целые числа $p, q$, удовлетворяющие неравенствам

$$|q\alpha - p| < \delta\ , \qquad 1 \le q \le \delta^{-1}. \tag{8.5}$$

Если числа $p, q$ имеют нетривиальный общий делитель, то разделив $p, q$ на него, получим еще одну пару целых чисел, удовлетворяющих неравенствам (8.5). Поэтому можно считать, что $(p, q) = 1$, т.е. дробь $\frac{p}{q}$ несократима.

Первое из неравенств (8.5) означает, что дробь $\frac{p}{q}$ отлична от всех дробей (8.4). Кроме того из (8.5) находим

$$|q\alpha - p| < \delta \le \frac{1}{q},$$

т.е. построенная несократимая дробь $\frac{p}{q}$ есть еще одно, отличное от дробей (8.4), решение неравенства (8.3). Получившееся противоречие завершает доказательство следствия. □

Терема Дирихле неэффективна, т.е. не дает способ строить хорошие рациональные приближения к числам. В следующем параграфе будет рассмотрен алгоритм, позволяющий сравнительно легко находить такие приближения и имеющий вместе с тем важное теоретическое значение.

## 8.2 Конечные цепные дроби

Пусть $a_0, a_1, a_2, \ldots$ – конечная или бесконечная последовательность целых чисел, причем $a_i \geq 1$ при $i \geq 1$. Выражение вида

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \tag{8.6}$$

называется *цепной* или *непрерывной* дробью. Если последовательность $a_i$ конечна, цепная дробь равна некоторому рациональному числу. Если же последовательность бесконечна, выражению (8.6) также можно придать вполне определенное числовое значение, которое в этом случае будет иррациональным. Для краткости записи вместо выражения (8.6) будет использоваться $[a_0; a_1, a_2, \ldots]$ или $[a_0; a_1, a_2, \ldots, a_m]$ при конечной последовательности $a_0, a_1, \ldots, a_m$. В этом параграфе мы изучим некоторые свойства конечных цепных дробей.

Пусть $a, b$ – целые числа, $b > 0$. Рассмотрим последовательность вычислений в алгоритме Евклида при нахождении наибольшего об-

щего делителя $(a, b)$, см. (1.3) :

$$\begin{aligned}
&a = bq_1 + r_2, && 0 \le r_2 < b,\\
&b = r_2q_2 + r_3, && 0 \le r_3 < r_2,\\
&r_2 = r_3q_3 + r_4, && 0 \le r_4 < r_3,\\
&\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots\\
&r_{n-2} = r_{n-1}q_{n-1} + r_n, && 0 \le r_n < r_{n-1},\\
&r_{n-1} = r_nq_n\ . &&
\end{aligned} \tag{8.7}$$

Разделив каждое из выписанных равенств на соответствующий делитель, получим

$$\begin{aligned}
\frac{a}{b} &= q_1 + \frac{1}{(b/r_2)},\\
\frac{b}{r_2} &= q_2 + \frac{1}{(r_2/r_3)},\\
\frac{r_2}{r_3} &= q_3 + \frac{1}{(r_3/r_4)},\\
&\ldots\ldots\ldots\ldots\\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{1}{q_n}.
\end{aligned} \tag{8.8}$$

Подставляя левые части получившихся равенств в правые части предшествующих, найдем представление рационального числа $\frac{a}{b}$ в виде конечной непрерывной дроби $\frac{a}{b} = [q_1; q_2, q_3, \ldots, q_n]$. Таким образом, алгоритм Евклида позволяет находить представление рациональных чисел непрерывными дробями. Заметим, что это представление не единственно:

$$[q_1; q_2, q_3, \ldots, q_n] = \begin{cases} [q_1; q_2, q_3, \ldots, q_n - 1, 1] & \text{если} \quad q_n > 1,\\ [q_1; q_2, q_3, \ldots, q_{n-1} + 1] & \text{если} \quad q_n = 1. \end{cases}$$

Для любого рационального числа существует представление конечной цепной дробью, при этом можно выбирать длину дроби по своему усмотрению так, чтобы она была четной или нечетной.

В дальнейшем используется обозначение $[x_0; x_1, \ldots, x_n]$ для конечной цепной дроби вида (8.6), где вместо целых чисел $a_i$ стоят переменные $x_i$. Конечные цепные дроби такого вида являются рациональными функциями от $x_i$. Следующее утверждение позволяет легко вычислять их.

**Лемма 8.1.** *Пусть $x_0, x_1, \ldots$ – переменные и последовательность многочленов $P_k(x_0, \ldots, x_k), Q_k(x_0, \ldots, x_k)$, $k \geq -1$, определена формулами*

$$\begin{cases} P_k = x_k P_{k-1} + P_{k-2}, & P_{-1} = 1, \quad P_0 = x_0, \\ Q_k = x_k Q_{k-1} + Q_{k-2}, & Q_{-1} = 0, \quad P_0 = 1. \end{cases} \tag{8.9}$$

*Тогда при любом $n \geq 0$ выполняется равенство*

$$[x_0; x_1, \ldots, x_n] = \frac{P_n}{Q_n} = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}} \ . \tag{8.10}$$

*Доказательство.* Воспользуемся индукцией по $n$. При $n = 0, 1$ имеем

$$[x_0] = x_0 = \frac{P_0}{Q_0}, \qquad [x_0; x_1] = x_0 + \frac{1}{x_1} = \frac{x_1 x_0 + 1}{x_1} = \frac{P_1}{Q_1}.$$

Предположим, что $n \geq 1$ и утверждение леммы выполняется для дробей длины $n$, т.е.

$$[x_0; x_1, \ldots, x_n] = \frac{x_n P_{n-1}(x_0, \ldots, x_{n-1}) + P_{n-2}(x_0, \ldots, x_{n-2})}{x_n Q_{n-1}(x_0, \ldots, x_{n-1}) + Q_{n-2}(x_0, \ldots, x_{n-2})}.$$

Подставляя в это тождество $x_n + \frac{1}{x_{n+1}}$ вместо $x_n$, находим

$$[x_0; x_1, \ldots, x_n, x_{n+1}] = [x_0; x_1, \ldots, x_{n-1}, x_n + \frac{1}{x_{n+1}}] =$$

$$\frac{\left(x_n + \frac{1}{x_{n+1}}\right) P_{n-1} + P_{n-2}}{\left(x_n + \frac{1}{x_{n+1}}\right) Q_{n-1} + Q_{n-2}} = \frac{P_n + \frac{1}{x_{n+1}} P_{n-1}}{Q_n + \frac{1}{x_{n+1}} Q_{n-1}} = \frac{x_{n+1} P_n + P_{n-1}}{x_{n+1} Q_n + Q_{n-1}},$$

что завершает доказательство леммы. □

**Следствие 8.2.** *При всех $n \geq 0$ справедливы тождества*

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

*Доказательство.* Воспользуемся индукцией по $n$. При $n = 0$ имеем

$$Q_0 P_{-1} - P_0 Q_{-1} = 1 \cdot 1 - x_0 \cdot 0 = 1.$$

Предположим, что $n \geq 1$ и для всех индексов меньших $n$ нужное тождество справедливо. С помощью (8.9) находим

$$\begin{aligned} Q_n P_{n-1} - P_n Q_{n-1} &= (x_n Q_{n-1} + Q_{n-2}) P_{n-1} - (x_n P_{n-1} + P_{n-2}) Q_{n-1} = \\ &= -(Q_{n-1} P_{n-2} - P_{n-1} Q_{n-2}) = -(-1)^{n-1} = (-1)^n. \end{aligned}$$

Следствие доказано. □

**Следствие 8.3.** *При любом $n \geq 1$ справедливы тождества*

$$Q_n P_{n-2} - P_n Q_{n-2} = (-1)^{n-1} x_n.$$

*Доказательство.* Пользуясь (8.9) и следствием 8.2, находим

$$\begin{aligned} Q_n P_{n-2} - P_n Q_{n-2} &= (x_n Q_{n-1} + Q_{n-2}) P_{n-2} - (x_n P_{n-1} + P_{n-2}) Q_{n-2} = \\ &= x_n (Q_{n-1} P_{n-2} - P_{n-1} Q_{n-2}) = (-1)^{n-1} x_n. \end{aligned}$$

□

Пусть $a_0, a_1, a_2, \ldots$ – последовательность целых чисел, причем $a_i \geq 1$ при $i \geq 1$. Тогда определены целые числа

$$p_n = P_n(a_0, \ldots, a_n), \qquad q_n = Q_n(a_0, \ldots, a_n), \quad n \geq 0,$$

причем $q_n > 0$. Будем также считать $p_{-1} = 1, q_{-1} = 0$. Согласно (8.9) имеем

$$\begin{cases} p_k = a_k p_{k-1} + p_{k-2}, & p_{-1} = 1, \quad p_0 = a_0, \\ q_k = a_k q_{k-1} + q_{k-2}, & q_{-1} = 0, \quad q_0 = 1. \end{cases} \tag{8.11}$$

В частности, отсюда находим $q_1 = a_1 \geq 1$ и при $k \geq 2$ последовательно

$$q_k > a_k q_{k-1} \geq q_{k-1}.$$

Таким образом, $q_n, n \geq 1$, есть строго возрастающая последовательность натуральных чисел. Она стремится к бесконечности, если последовательность $a_i$ бесконечна.

По следствию 8.2 выполняются равенства

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n, \qquad n \geq 0. \tag{8.12}$$

Из них, в частности, следует, что $p_n$ и $q_n$ взаимно просты, а дробь $\frac{p_n}{q_n}$ несократима. Точно так же доказываются равенства

$$q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n, \qquad n \geq 1. \tag{8.13}$$

Согласно лемме 8.1

$$[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Так определенные дроби $\frac{p_n}{q_n}, n \geq 0$, называются *подходящими дробями* цепной дроби $[a_0; a_1, a_2, \ldots]$. Числа $a_j$ называются *неполными частными* этой цепной дроби. Множество подходящих дробей конечной цепной дроби конечно.

Для рационального числа $\frac{a}{b} = [a_0; a_1, \ldots, a_m]$ имеем $\frac{a}{b} = \frac{p_m}{q_m}$.

Равенство (8.12) позволяет решать диофантовы уравнения вида $ax - by = 1$ при взаимно простых $a$ и $b > 0$. Если $\frac{a}{b} = \frac{p_m}{q_m}$, 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 теореме 1.5.

Рассмотрим следующий

**Пример.** Решить диофантово уравнение

$$19x + 15y = 1.$$

Рациональное число $\frac{19}{15}$ имеет следующее разложение в цепную дробь $\frac{19}{15} = [1; 3, 1, 3]$. В данном случае длина цепной дроби $m = 3$ нечетна. В соответствии с указанным правилом находим $[1; 3, 1] = \frac{5}{4}$ и $19 \cdot 4 - 15 \cdot 5 = 1$. Значит, данное уравнение имеет решение $x = 4, y = -5$, а общее его решение имеет вид $x = 4 + 15k, y = -5 - 19k, k \in \mathbb{Z}$.

## 8.3 Цепная дробь действительного числа

В этом параграфе мы рассмотрим бесконечные цепные дроби. Каждой из них будет придано некоторое иррациональное значение и будет доказано, что так устанавливается взаимно однозначное соответствие между бесконечными цепными дробями и ирациональными числами.

**Теорема 8.2.** *Пусть* $[a_0; a_1, a_2, \ldots]$ *– конечная или бесконечная цепная дробь с целыми неполными частными, причем* $a_n \geq 1$ *при* $n \geq 1$. *Тогда*
*1. Последовательность подходящих дробей с четными номерами возрастает, последовательность подходящих дробей с нечетными номерами убывает. При этом любая подходящая дробь нечетного порядка больше любой подходящей дроби четного порядка.*
*2. Если цепная дробь бесконечна, то существует предел*

$$\alpha = \lim_{n \to \infty} \frac{p_n}{q_n},$$

*причем* $\alpha$ *– иррациональное число.*
*3. Справедливы неравенства*

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}, \qquad n \geq 0. \tag{8.14}$$

*Доказательство.* С помощью равенств (8.13) при $n \geq 2$ получаем

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}.$$

Учитывая неравенства $a_n > 0, q_k > 0$, находим что эта разность отрицательна при четном $n$ и положительна при нечетном $n$. Это доказывает первое утверждение теоремы.

Пусть цепная дробь бесконечна. Из равенств (8.12) следует

$$\frac{p_{2k}}{q_{2k}} - \frac{p_{2k+1}}{q_{2k+1}} = \frac{-1}{q_{2k}q_{2k+1}} < 0, \qquad k \geq 0. \tag{8.15}$$

Таким образом, определены отрезки $\left[\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}}, \right]$. По доказанному их левые концы возрастают, а правые убывают. Значит, эти отрезки образуют вложенную последовательность. Согласно (8.15) длины отрезков стремятся к нулю. Поэтому существует единственное число $\alpha$, принадлежащее всем этим отрезкам. Учитывая строгое возрастание левых концов и строгое убывание правых концов, заключаем, что

$$\frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2\ell+1}}{q_{2\ell+1}}, \qquad k \geq 0, \ell \geq 0. \tag{8.16}$$

Отсюда следует, что при любом $n \geq 0$ дроби $\frac{p_n}{q_n}$ и $\frac{p_{n+1}}{q_{n+1}}$ лежат на действительной оси по разные стороны от точки $\alpha$. Поэтому

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}. \tag{8.17}$$

Это доказывает третье утверждение теоремы.

Допустим, что $\alpha$ – рациональное число. Тогда с некоторыми целыми $a, b > 0$ имеем $\alpha = \frac{a}{b}$. Из (8.17) следует, что

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{|aq_n - bp_n|}{bq_n} \geq \frac{1}{bq_n}.$$

Сравнивая получившееся неравенство с (8.17), находим $b > q_{n+1}$, что невозможно при всех $n$, ведь последовательность $q_n$ стремится к бесконечности. Значит, $\alpha$ иррационально, и это завершает доказательство теоремы. □

Число $\alpha$, определенное в теореме 8.2 будем называть значением бесконечной цепной дроби $[a_0; a_1, a_2, \ldots]$ и записывать это в виде

$$\alpha = [a_0; a_1, a_2, \ldots].$$

Соответствующие подходящие дроби будем называть также подходящими дробями числа $\alpha$. Эта терминология будет использоваться и для конечных цепных дробей. В частности, если $\alpha$ – рациональное число, то любая его подходящая дробь, отличная от $\alpha$, удовлетворяет одному из неравенств (8.16).

**Теорема 8.3.** *Пусть* $[a_0; a_1, a_2, \ldots]$ *– конечная или бесконечная цепная дробь с целыми элементами, причем для* $n \geq 1$ *выполняется неравенство* $a_n \geq 1$*, а для конечной дроби ее последнее неполное частное больше* 1*. Тогда для любых двух соседних подходящих дробей к* $\alpha$ *имеем*

$$|q_{n-1}\alpha - p_{n-1}| > |q_n\alpha - p_n|, \qquad n \geq 0. \tag{8.18}$$

*Кроме того*

$$a_{n+1} = \left[\frac{|q_{n-1}\alpha - p_{n-1}|}{|q_n\alpha - p_n|}\right], \qquad n \geq 0, \qquad a_0 = [\alpha]. \tag{8.19}$$

*Различные цепные дроби указанного вида имеют различные значения.*

*Доказательство.* Из равенств (8.11) следует

$$(q_{n+1}\alpha - p_{n+1}) = a_{n+1}(q_n\alpha - p_n) + (q_{n-1}\alpha - p_{n-1}), \qquad n \geq 0.$$

Отсюда, поскольку $q_k\alpha - p_k = (-1)^k|q_k\alpha - p_k|$ при любом $k \geq -1$, находим

$$|q_{n+1}\alpha - p_{n+1}| = -a_{n+1}|q_n\alpha - p_n| + |q_{n-1}\alpha - p_{n-1}|, \qquad n \geq 0,$$

или

$$|q_{n-1}\alpha - p_{n-1}| = a_{n+1}|q_n\alpha - p_n| + |q_{n+1}\alpha - p_{n+1}|, \qquad n \geq 0. \tag{8.20}$$

В случае $q_{n+1}\alpha - p_{n+1} \neq 0$ неравенство (8.18), очевидно, выполняется. Если же $q_{n+1}\alpha - p_{n+1} = 0$, то согласно условию $a_{n+1} \geq 2$, так что (8.18) выполняется и в этом случае.

Будем использовать обозначение $\alpha_j = \frac{|q_{j-2}\alpha - p_{j-2}|}{|q_{j-1}\alpha - p_{j-1}|}$, в случае, если эта величина определена. Из доказанного выше следует, что $\alpha_j > 1$ при $j \geq 1$.

Разделив (8.20) на отличное от нуля число $|q_n\alpha - p_n|$, получим

$$\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}}. \tag{8.21}$$

В случае $q_{n+1}\alpha - p_{n+1} = 0$ дробь в (8.21) отсутствует, так что в любом случае имеем $a_{n+1} \leq \alpha_{n+1} < a_{n+1} + 1$ и $a_{n+1} = [\alpha_{n+1}], n \geq 0$. Это завершает доказательство (8.19) при $n \geq 0$.

Из (8.18) для $n = 0$ и (8.16) для $k = 0$ находим $1 > \alpha - a_0 \geq 0$, следовательно $a_0 = [\alpha_0]$.

Допустим теперь, что существуют две различные цепные дроби, имеющие одно и то же значение

$$\alpha = [a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots].$$

Обозначим $\frac{p_n}{q_n}$ и $\frac{p'_n}{q'_n}$ подходящие дроби этих цепных дробей соответственно и

$$\alpha_n = \frac{|q_{n-2}\alpha - p_{n-2}|}{|q_{n-1}\alpha - p_{n-1}|}, \qquad \beta_n = \frac{|q'_{n-2}\alpha - p'_{n-2}|}{|q'_{n-1}\alpha - p'_{n-1}|}, \qquad n \geq 1. \tag{8.22}$$

По доказанному выше справедливы равенства $a_0 = [\alpha], b_0 = [\alpha]$, так что $a_0 = b_0$. Пусть $r$ – наименьшее целое число, для которого $a_r \neq b_r$. Из рекуррентных уравнений (8.11) следует, что $q_n = q'_n$, $p_n = p'_n$ при $-1 \leq n < r$. Согласно (8.22) при $n = r$ имеем $\alpha_r = \beta_r$, а из (8.19) теперь находим $a_r = [\alpha_r] = [\beta_r] = b_r$. Получившееся противоречие завершает доказательство теоремы 8.3. □

Выше мы доказали, что каждое рациональное число может быть представлено в виде конечной цепной дроби.

Покажем, что и для каждого иррационального числа существует равная ему бесконечная цепная дробь.

**Теорема 8.4.** *Пусть $\alpha$ – действительное иррациональное число. Положим $\alpha_0 = \alpha$ и определим бесконечные последовательности целых чисел $a_n$ и действительных чисел $\alpha_n$ равенствами*

$$a_n = [\alpha_n], \qquad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \qquad n \geq 0. \tag{8.23}$$

*Тогда $a_n \geq 1$ при $n \geq 1$. Если $\left\{\frac{p_n}{q_n}\right\}_{n\geq 0}$ – последовательность подходящих дробей бесконечной цепной дроби $[a_0; a_1, a_2, \ldots]$, то при всех $k \geq 0$ справедливы равенства*

$$\alpha = [a_0; a_1, \ldots, a_k, \alpha_{k+1}] = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}, \tag{8.24}$$

$$q_k\alpha - p_k = \frac{(-1)^k}{\alpha_{k+1}q_k + q_{k-1}}. \tag{8.25}$$

*Цепная дробь $[a_0; a_1, a_2, \ldots]$ равна $\alpha$.*

Числа $\alpha_k$, последовательно вычисляемые с помощью равенств (8.23) называются *остатками непрерывной дроби* числа $\alpha$.

*Доказательство.* Поскольку $\alpha$ иррациональное число, то все числа $\alpha_n$ также иррациональны. Это следует из второго равенства (8.23), поскольку $a_n$ – целые числа. Учитывая, что $0 < \alpha_n - a_n < 1$, заключаем согласно (8.23), что $\alpha_{n+1} > 1$ при $n \geq 0$. Но тогда при $n \geq 0$ выполнены неравенства $a_{n+1} \geq 1$.

Первое равенство (8.24) следует из равенств (8.23), если переписать их в виде $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$. А для доказательства второго равенства (8.24) достаточно подставить в тождество (8.10) при $n = k+1$ следующие значения переменных: $x_j = a_j, 0 \leq j \leq k$, $x_{k+1} = \alpha_{k+1}$.

Теперь равенство (8.25) следует из (8.24) и (8.12) непосредственным вычислением

$$q_k\alpha - p_k = \frac{q_k(\alpha_{k+1}p_k + p_{k-1}) - p_k(\alpha_{k+1}q_k + q_{k-1})}{\alpha_{k+1}q_k + q_{k-1}} = \\ = \frac{q_kp_{k-1} - p_kq_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} = \frac{(-1)^k}{\alpha_{k+1}q_k + q_{k-1}}.$$

Из (8.25) находим

$$\left|\alpha - \frac{p_k}{q_k}\right| \le \frac{1}{q_k(a_{k+1}q_k + q_{k-1})} = \frac{1}{q_k q_{k+1}}, \tag{8.26}$$

откуда следует, что последовательность подходящих дробей $\frac{p_k}{q_k}$ сходится к $\alpha$ и, значит, $\alpha = [a_0; a_1, a_2, \ldots]$. □

Заметим, что равенства (8.23)-(8.25) справедливы и для конечных цепных дробей в пределах тех индексов, для которых существуют неполные частные и подходящие дроби. При этом $\alpha_n = \frac{r_n}{r_{n+1}}$ в формулах (8.8).

Помимо (8.26) из равенства (8.25) можно вывести и оценку снизу для приближения $\alpha$ подходящими дробями. Действительно,

$$|q_k\alpha - p_k| = \frac{1}{\alpha_{k+1}q_k + q_{k-1}} > \frac{1}{(a_{k+1}+1)q_k + q_{k-1}} = \frac{1}{q_{k+1} + q_k}, \tag{8.27}$$

откуда получаем

**Следствие 8.4.** *При любом $k \ge 0$ выполняется неравенство*

$$\left|\alpha - \frac{p_k}{q_k}\right| \ge \frac{1}{q_k(q_{k+1} + q_k)}.$$

Из теорем 8.2-8.4 следует критерий иррациональности числа.

**Следствие 8.5.** *Действительное число $\alpha$ иррационально в том и только том случае, когда его цепная дробь бесконечна.*

Каждая подходящая дробь несократима и в силу неравенств (8.14) удовлетворяет (8.3), что дает еще одно доказательство следствия 8.1.

Равенства (8.23) дают удобный алгоритм для вычисления непрерывной дроби числа. Знание непрерывной дроби позволяет с помощью равенств (8.11) легко вычислять соответствующие подходящие дроби, т.е. находить хорошие рациональные приближения к $\alpha$. В дальнейшем будет показано, что эти приближения являются в некотором смысле наилучшими.

**Пример.** Найти разложение в непрерывную дробь числа $\frac{1+\sqrt{17}}{2}$ и первые пять соответствующих подходящих дробей.

В соответствии с формулами (8.23) находим

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

В формулах (8.23) каждое число $\alpha_{n+1}$ однозначно определяется по числу $\alpha_n$. 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

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

Равенства (8.11) могут быть переписаны в матричном виде

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} a_n \\ 1 \end{pmatrix} = \begin{pmatrix} p_n \\ q_n \end{pmatrix}.$$

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

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \end{pmatrix},$$

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

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

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

## 8.4 Наилучшие приближения

Наилучшие приближения к заданному числу $\alpha$ определяются, как наилучшие среди приближений с заданным ограничением величины знаменателей.

**Определение 8.** *Рациональная дробь $\frac{p}{q}$ называется наилучшим приближением к действительному числу $\alpha$, если для любой другой дроби $\frac{a}{b} \neq \frac{p}{q}$ с условием $1 \leq b \leq q$ выполняется неравенство*

$$|b\alpha - a| > |q\alpha - p|,$$

*другими словами, если система неравенств*

$$\begin{cases} |x - \alpha y| \leq |p - \alpha q| \ , \\ 0 < y \leq q \end{cases} \tag{8.28}$$

*имеет единственное решение в целых числах, а именно*

$$x = p, \qquad y = q.$$

Заметим, что наилучшее приближение всегда есть несократимая дробь. Ведь если $p = ua, q = ub, u > 1$, то $|a - \alpha b| < |p - \alpha q|$ и $0 < b < q$, т.е. система неравенств (8.28) имеет решением и пару чисел $x = a, y = b$.

Следующая теорема описывает связь между наилучшими приближениями к иррациональным числам и подходящими дробями.

**Теорема 8.5.** *Всякое наилучшее приближение к числу $\alpha$ есть подходящая дробь к нему. Всякая подходящая дробь $\frac{p_n}{q_n}$ к $\alpha$ при $n \geq 1$ есть наилучшее приближение к этому числу.*

Заметим, что подходящая дробь $\frac{p_0}{q_0} = \frac{0}{1}$ к числу $\alpha = \frac{2}{3}$ не является наилучшим приближением к нему, так как система (8.28) имеет в этом случае лишнее решение $x = 1, y = 1$.

**Лемма 8.2.** *Пусть $\frac{p_k}{q_k}, \frac{p_{k+1}}{q_{k+1}}$ – соседние подходящие дроби к числу $\alpha$, причем $\frac{p_{k+1}}{q_{k+1}} \neq \alpha$. Тогда система неравенств*

$$\begin{cases} |x - \alpha y| \leq |p_k - \alpha q_k| \ , \\ 0 < y \leq q_{k+1} \end{cases} \tag{8.29}$$

*имеет лишь два решения в целых числах, а именно*

$$x = p_k, \quad y = q_k, \qquad u \qquad x = p_{k+1}, \quad y = q_{k+1}.$$

*Доказательство.* Пусть $(x, y)$ решение системы неравенств (8.29) в целых числах. Рассмотрим систему линейных уравнений

$$\begin{aligned} x &= up_k + vp_{k+1}, \\ y &= uq_k + vq_{k+1} \end{aligned}$$

относительно неизвестных $u, v$. Так как определитель этой системы равен $q_{k+1}p_k - p_{k+1}q_k = (-1)^{k+1}$, то ей удовлетворяют целые числа. Сохраним для них те же обозначения $u, v$. Поскольку $y > 0$, то по крайней мере одно из чисел $u, v$ отлично от нуля.

Рассмотрим несколько случаев.

1. Предположим, что $u = 0$. Тогда $0 < y = vq_{k+1} \leq q_{k+1}$. Значит, $y = q_{k+1}, v = 1$, и $x = p_{k+1}$.

2. Предположим, что $v = 0$. Тогда $x = up_k, y = uq_k, u > 0$, и

$$|p_k - \alpha q_k| \geq |x - \alpha y| = u \cdot |p_k - \alpha q_k|,$$

что возможно лишь при $u = 1$. Но тогда $x = p_k, y = q_k$.

3. Предположим, что $uv \neq 0$. Если числа $u, v$ имеют одинаковые знаки, то условие $y > 0$ означает, что $u > 0, v > 0$. Но тогда $y \geq q_k + q_{k+1}$, что неверно. Итак, $uv < 0$. Имеем

$$x - y\alpha = u(p_k - \alpha q_k) + v(p_{k+1} - \alpha q_{k+1}). \tag{8.30}$$

Учитывая, что числа $p_k - \alpha q_k$ и $p_{k+1} - \alpha q_{k+1}$ также имеют разные знаки, заключаем, что знаки слагаемых в правой части равенства (8.30) одинаковы. Поэтому

$$|x - y\alpha| = |u| \cdot |p_k - \alpha q_k| + |v| \cdot |p_{k+1} - \alpha q_{k+1}| > |p_k - \alpha q_k|,$$

что противоречит условию. Лемма доказана. □

*Докажем теперь теорему* 8.5. Пусть $\frac{p}{q}$ – наилучшее приближение к числу $\alpha$ и $k$ – наибольший индекс, для которого выполнено неравенство $q_k \leq q$. Предположим, что

$$|p - \alpha q| < |p_k - \alpha q_k|.$$

Тогда определена дробь $\frac{p_{k+1}}{q_{k+1}}$, причем $q < q_{k+1}$. Но это невозможно в силу леммы 8.2. Значит выполняется неравенство

$$|p_k - \alpha q_k| \leq |p - \alpha q|.$$

Учитывая теперь, что $\frac{p}{q}$ есть наилучшее приближение к $\alpha$, находим $q = q_k, p = p_k$, т.е. $\frac{p}{q}$ есть одна из подходящих дробей к $\alpha$.

Докажем теперь, что при $k \geq 0$ каждая подходящая дробь $\frac{p_{k+1}}{q_{k+1}}$ к числу $\alpha$, является наилучшим приближением к нему.

Пусть целые числа $x, y$ удовлетворяют неравенствам

$$\begin{cases} |x - \alpha y| \leq |p_{k+1} - \alpha q_{k+1}| \ , \\ 0 < y \leq q_{k+1}. \end{cases}$$

Согласно теореме 8.3 выполняются неравенства

$$\begin{cases} |x - \alpha y| < |p_k - \alpha q_k| \ , \\ 0 < y \leq q_{k+1}, \end{cases}$$

что по лемме 8.2 возможно лишь в случае $x = p_{k+1}, y = q_{k+1}$. Значит, дробь $\frac{p_{k+1}}{q_{k+1}}$ действительно является наилучшим приближением к $\alpha$. Это завершает доказательство теоремы.

**Теорема 8.6.** *Если несократимая дробь $\frac{p}{q}$, $q > 0$, удовлетворяет неравенству*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}, \tag{8.31}$$

*то она есть наилучшее приближение к $\alpha$ и является одной из подходящих дробей к нему.*

*Доказательство.* Предположим, что целые числа $x = a, y = b$ удовлетворяют неравенствам (8.28), т.е.

$$\begin{cases} |a - \alpha b| \le |p - \alpha q| \ , \\ 0 < b \le q \qquad\qquad\quad . \end{cases}$$

Тогда, пользуясь неравенством треугольника, находим

$$|aq - bp| = |q(a - \alpha b) - b(p - \alpha q)| \le$$
$$q|a - \alpha b| + b|p - \alpha q| \le 2q|p - \alpha q| = 2q^2 \left|\alpha - \frac{p}{q}\right| < 1.$$

Следовательно, целое число $aq - bp$ равно нулю. Согласно условию числа $p, q$ взаимно просты. Поэтому из доказанного равенства $aq = bp$ следует $q|b$. По условию $0 < b \le q$, так что $b = q$ и $a = p$. Это доказывает, что $\frac{p}{q}$ есть наилучшее приближение к $\alpha$.

Второе утверждение теоремы следует теперь из теоремы 8.5. □

Покажем теперь, что множество рациональных решений неравенства (8.31) бесконечно.

**Теорема 8.7.** *При $k \ge 1$ по крайней мере одна из двух соседних подходящих дробей $\frac{p_k}{q_k}$, $\frac{p_{k+1}}{q_{q+1}}$ удовлетворяет неравенству (8.31).*

*Доказательство.* Предположим, что выполняются неравенства

$$\left|\alpha - \frac{p_k}{q_k}\right| \geq \frac{1}{2q_k^2}, \qquad \left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| \geq \frac{1}{2q_{k+1}^2}. \tag{8.32}$$

Складывая их и пользуясь тем, что дроби $\frac{p_k}{q_k}$, $\frac{p_{k+1}}{q_{q+1}}$ лежат по разные стороны от $\alpha$, находим

$$\frac{1}{2q_k^2} + \frac{1}{2q_{k+1}^2} \leq \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| = \left|\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}}\right| = \frac{1}{q_k q_{k+1}}.$$

Откуда, выполнив простые преобразования, получаем $(q_{k+1} - q_k)^2 \leq 0$, что невозможно, так как $q_{k+1} > q_k$. Это противоречие доказывает, что предположение (8.32) неверно и утверждение теоремы выполняется. □

Последовательность подходящих дробей для иррационального числа бесконечна. Поэтому находим усиление следствия 8.1.

**Следствие 8.6.** *Пусть $\alpha$ – иррациональное число. Тогда существует бесконечное множество несократимых дробей $\frac{p}{q}$, удовлетворяющих неравенству*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

## 8.5 Эквивалентные числа

На множестве действительных чисел можно ввести отношение эквивалентности. Два действительных числа $\alpha$ и $\beta$ называются *эквивалентными*, если найдутся целые числа $a, b, c, d$, удовлетворяющие равенствам

$$\alpha = \frac{a\beta + b}{c\beta + d}, \qquad ad - bc = \pm 1. \tag{8.33}$$

Это отношение будет обозначаться $\alpha \sim \beta$.

Заметим, что каждое число $\alpha$ эквивалентно самому себе. В этом случае равенство (8.33) выполняется с $a = d = 1, b = c = 0$.

Если $\alpha \sim \beta$, отношение выполняется и в противоположную сторону, т.е. $\beta \sim \alpha$. Действительно, из (8.33) легко найти, что

$$\beta = \frac{-d\alpha + b}{c\alpha - a}.$$

Наконец, если $\alpha \sim \beta$ и $\beta \sim \gamma$, то $\alpha \sim \gamma$. Чтобы проверить это возьмем два представления

$$\alpha = \frac{a\beta + b}{c\beta + d}, \qquad \beta = \frac{p\gamma + q}{r\gamma + s} \qquad ad - bc = \pm 1, \quad ps - qr = \pm 1,$$

и подставим выражение для $\beta$ в первую дробь. В результате получится равенство

$$\alpha = \frac{u\gamma + v}{w\gamma + t},$$

в котором коэффициенты $u, v, w, t$ определяются, как не трудно проверить, матричным равенством

$$\begin{pmatrix} u & v \\ w & t \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Так как определитель произведения матриц равен произведению определителей, отсюда следует, что $ut - vw = \pm 1$. Итак, $\alpha \sim \gamma$.

Из этих трех свойств следует, что множество всех действительных чисел распадается на классы чисел, эквивалентных между собой.

Если при разложении действительного числа $\alpha$ в непрерывную дробь получается равенство $\alpha = [a_0; a_1, \ldots, a_k, \alpha_{k+1}]$, то, см. (8.24),

$$\alpha = [a_0; a_1, \ldots, a_k, \alpha_{k+1}] = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}},$$

где $p_k, q_k, p_{k-1}, q_{k-1}$ – числители и знаменатели подходящих дробей, удовлетворяющие согласно (8.12) равенству

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k, \qquad k \geq 0. \tag{8.34}$$

Но это значит, что $\alpha \sim \alpha_{k+1}$ при любом $k \geq 0$.

Если, например, $\alpha$ – рациональное число, раскладывающееся в непрерывную дробь длины $k+1$, то $\alpha_{k+1}$ – целое число. Но, любые два целых числа, очевидно, эквивалентны. Это доказывает, что *любые два рациональных числа эквивалентны.*

Более обще справедливо утверждение.

**Теорема 8.8.** *Действительные числа $\alpha$ и $\beta$ эквивалентны тогда и только тогда, когда их разложения в непрерывные дроби начиная с некоторого места совпадают.*

*Доказательство.* Предположим сначала, что разложения чисел $\alpha$ и $\beta$ совпадают с некоторого места. Тогда существуют такие индексы $k, \ell$, что

$$\alpha = [a_0; a_1, \ldots, a_k, \alpha_{k+1}], \qquad \beta = [b_0; b_1, \ldots, b_\ell, \beta_{\ell+1}],$$

причем $\alpha_{k+1} = \beta_{\ell+1}$. Из сказанного выше имеем $\alpha \sim \alpha_{k+1} = \beta_{\ell+1} \sim \beta$ и, значит, $\alpha \sim \beta$.

Докажем теперь, что утверждение справедливо в противоположную сторону. Предположим, что $\alpha \sim \beta$. Рассмотрим далее несколько частных случаев. При этом будем использовать запись $\alpha \asymp \beta$ для обозначения того, что разложения в непрерывные дроби чисел $\alpha$ и $\beta$ начиная с некоторого места совпадают.

1) Если, $\beta = \alpha + n$, где $n$ - некоторое целое число, то непрерывные дроби чисел $\alpha$ и $\beta$ совпадают уже начиная с первого места, т.е. $\alpha \asymp \beta$.

2) Пусть $\beta = -\alpha$. Можно предполагать, что $\alpha$ не целое число, ведь этот случай уже разобран в пункте 1). Имеем

$$\alpha = a_0 + \frac{1}{\gamma}\,, \qquad a_0 \in \mathbb{Z}, \qquad a_0 < \alpha < a_0 + 1, \qquad \gamma > 1,$$

т.е. $\alpha = [a_0; \gamma]$. Тогда $-a_0 - 1 < -\alpha < -a_0$ и

$$-\alpha = -a_0 - 1 + \frac{\gamma - 1}{\gamma} = -a_0 - 1 + \frac{1}{1 + \dfrac{1}{\gamma - 1}}\,.$$

При $\gamma > 2$ имеем $-\alpha = [-a_0 - 1; 1, \gamma - 1]$ и, учитывая, что, как доказано в пункте 1), разложения $\gamma$ и $\gamma - 1$ начиная с некоторого места совпадают, получаем $\alpha \asymp \beta$.

При $1 < \gamma < 2$ имеем $\gamma = 1 + \frac{1}{\rho}$ , $\rho > 1$, так что

$$\alpha = [a_0; 1, \rho], \qquad -\alpha = [-a_0 - 1; 1 + \rho].$$

Учитывая, что разложения $\rho$ и $1 + \rho$ начиная с некоторого места совпадают, получаем $\alpha \asymp -\beta = \beta$.

3) Пусть $\beta = \frac{1}{\alpha}$.

а) Рассмотрим сначала случай $\alpha > 1$. Тогда $\beta = [0; \alpha]$ и утверждение $\alpha \asymp \beta$ выполняется.

б) Пусть $0 < \alpha < 1$. Тогда $\alpha = \beta^{-1}, \beta > 1$, т.е. $\alpha = [0; \beta]$ и утверждение $\beta \asymp \alpha$ также выполняется.

в) Если $\alpha < 0$, по доказанному ранее имеем

$$\alpha \asymp -\alpha \asymp \frac{1}{-\alpha} = -\frac{1}{\alpha} \asymp \frac{1}{\alpha}.$$

После рассмотрения трех частных случаев перейдем к общему

$$\beta = \frac{a\alpha + b}{c\alpha + d}, \qquad ad - bc = \pm 1, \tag{8.35}$$

и будем вести доказательство утверждения $\beta \asymp \alpha$ индукцией по $|c|$.

В случае $|c| = 0$ имеем $\beta = \pm\alpha + b$ и утверждение следует из доказанных выше пунктов 1) и 2).

Предположим $|c| = n \geq 1$ и для всех чисел, у которых коэффициент при $\alpha$ в знаменателе представления (8.35) по абсолютной величине меньше $n$, утверждение выполняется. В случае $|a| < n$ находим

$$\frac{1}{\beta} = \frac{c\alpha + d}{a\alpha + b}, \qquad cb - ad = \pm 1,$$

и согласно индуктивному предположению находим $\beta^{-1} \asymp \alpha$, откуда по доказанному выше $\beta \asymp \beta^{-1} \asymp \alpha$. Утверждение выполняется.

В случае $|a| \geq |c|$ можно не уменьшая общности считать $c > 0$. Иначе можно сменить знаки у всех чисел $a, b, c, d$ в представлении

(8.35). Разделив коэффициент $a$ на $c$ с остатком найдем $a = cq + r, 0 \leq r < c$. Тогда

$$\beta - q = \frac{r\alpha + b - qd}{c\alpha + d}$$

и

$$\gamma = \frac{1}{\beta - q} = \frac{c\alpha + d}{r\alpha + b - qd}.$$

Учитывая, что $c(b - qd) - dr = bc - ad = \pm 1$ и $0 \leq r < c \leq n$, заключаем по индуктивному предположению и доказанному ранее

$$\alpha \asymp \gamma \asymp \beta - q \asymp \beta.$$

Теорема доказана. □

## 8.6 Квадратичные иррациональности и цепные дроби

Рациональные числа являются простейшими из действительных чисел. Следующий по сложности подкласс действительных чисел составляют квадратичные иррациональности. Действительное число $\alpha$ называется *квадратичной иррациональностью*, если оно не рационально и есть корень квадратного трехчлена $f(x) = ax^2 + bx + c$ с целыми коэффициентами $a, b, c$. Разделим коэффициенты на общий делитель и, если $a < 0$ умножим трехчлен на $-1$. Так получится многочлен $f(x)$ с целыми коэффициентами, удовлетворяющий условиям

$$f(\alpha) = 0, \qquad (a, b, c) = 1, \qquad a > 0. \tag{8.36}$$

Существует только один такой многочлен. Число $D(\alpha) = b^2 - 4ac$ называется *дискриминантом* $\alpha$. Ясно, что $D(\alpha) > 0$ и отлично от квадрата целого числа.

В этом параграфе мы обсудим свойства цепных дробей, в которые раскладываются квадратичные иррациональности.

Пусть $D$ целое положительное число, отличное от квадратов. Множество чисел вида $x + y\sqrt{D}$ с рациональными $x, y$ обозначается

символом $\mathbb{Q}(\sqrt{D})$. Это множество замкнуто относительно операций сложения и вычитания, умножения и деления. Например, для умножения и деления имеем

$$(x+y\sqrt{D})\cdot(u+v\sqrt{D})=(xu+yvD)+(xv+yu)\sqrt{D}, \tag{8.37}$$

$$\frac{1}{x+y\sqrt{D}}=\frac{x-y\sqrt{D}}{x^2-Dy^2}=\frac{x}{x^2-Dy^2}+\frac{-y}{x^2-Dy^2}\sqrt{D}. \tag{8.38}$$

Значит, множество $\mathbb{Q}(\sqrt{D})$ является полем. Оно содержит множество рациональных чисел. Каждое иррациональное число из $\mathbb{Q}(\sqrt{D})$ есть квадратичная иррациональность.

Для каждого числа $\alpha=x+y\sqrt{D}\in\mathbb{Q}(\sqrt{D})$ с рациональными $x,y$ будем использовать обозначение

$$\alpha'=x-y\sqrt{D}.$$

Ясно, что для иррационального $\alpha$ число $\alpha'$ есть второй корень квадратного трехчлена $f(x)$, удовлетворяющего (8.36). Для рациональных чисел $\alpha$ имеем $\alpha'=\alpha$.

Числа $\alpha$ и $\alpha'$ называются *сопряженными*. Для любых двух чисел $\alpha,\beta\in\mathbb{Q}(\sqrt{D})$ выполняются равенства

$$(\alpha+\beta)'=\alpha'+\beta',\quad (\alpha-\beta)'=\alpha'-\beta',\quad (\alpha\beta)'=\alpha'\beta',\quad \left(\frac{\alpha}{\beta}\right)'=\frac{\alpha'}{\beta'}.$$

В последнем случае предполагается, что $\beta\neq 0$.

Проверим эти равенства для умножения и деления. Для сложения и вычитания они проверяются аналогично. Если $\alpha=x+y\sqrt{D}$, $\beta=u+v\sqrt{D}$, $x,y,u,v\in\mathbb{Q}$, то согласно формулам (8.37), (8.38) находим

$$\alpha'\beta'=(xu+yvD)-(xv+yu)\sqrt{D}=(\alpha\beta)',$$

$$\frac{1}{\beta'}=\frac{u}{u^2-Dv^2}+\frac{v}{u^2-Dv^2}\sqrt{D}=\left(\frac{1}{\beta}\right)'$$

и

$$\left(\frac{\alpha}{\beta}\right)'=(\alpha\cdot\beta^{-1})'=\alpha'(\beta^{-1})'=\alpha'(\beta')^{-1}=\frac{\alpha'}{\beta'}.$$

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 $a_{n+k} = a_n$. Дробь называется *чисто периодической*, если равенство $a_{n+k} = a_n$ выполняется для всех $n \geq 0$. 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. Соответственно чисто периодические дроби обозначаются

$$[\ \overline{a_0, a_1, \ldots, a_{k-1}}\ ].$$

**Теорема 8.9 (Теорема Эйлера-Лагранжа).** *Пусть $\alpha$ – действительное иррациональное число. Цепная дробь $\alpha$ периодична тогда и только тогда, когда $\alpha$ – квадратичная иррациональность.*

Тот факт, что периодические цепные дроби есть разложения квадратичных иррациональностей был доказан в 1737г. Эйлером. Обратное утверждение о периодичности цепной дроби для любой квадратичной иррациональности было установлено в 1770г. Лагранжем. Мы начнем доказательство с первого утверждения.

*Доказательство.* В следующем ниже доказательстве буквы $p_j$, $q_j$ будут обозначать числители и знаменатели подходящих дробей цепной дроби числа $\alpha$.

Предположим, сначала, что цепная дробь $\alpha$ чисто периодическая, т.е. $\alpha = [\ \overline{a_0, a_1, \ldots, a_{k-1}}\ ]$. Тогда $\alpha = [\ a_0; a_1, \ldots, a_{k-1}, \alpha_k]$. Поскольку $\alpha_k = [\ \overline{a_0, a_1, \ldots, a_{k-1}}\ ] = \alpha$, то имеем $\alpha = [\ a_0; a_1, \ldots, a_{k-1}, \alpha]$ или

$$\alpha = \frac{\alpha p_{k-1} + p_{k-2}}{\alpha q_{k-1} + q_{k-2}}\ .$$

Значит, $\alpha$ – корень многочлена $q_{k-1}x^2 + (q_{k-2} - p_{k-1})x - p_{k-2}$. Цепная дробь числа $\alpha$ бесконечна, поэтому $\alpha$ иррационально. Итак, $\alpha$ – квадратичная иррациональность.

В общем случае имеем

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

где $\gamma = [\, \overline{a_{h+1}, a_{h+2}, \ldots, a_{h+k}} \,]$, как установлено выше, – квадратичная иррациональность. Тогда

$$\alpha = \frac{\gamma p_h + p_{h-1}}{\gamma q_h + q_{h-1}}\,, \qquad \gamma = \frac{-\alpha q_{h-1} + p_{h-1}}{\alpha q_h - p_h}\,.$$

Значит, $\alpha$ есть корень многочлена второй степени и иррациональное число. Теорема в одну сторону доказана. □

Докажем теперь, что квадратичные иррациональности раскладываются в периодические цепные дроби. Введем для этого еще одно понятие.

Пусть $\alpha$ – квадратичная иррациональность, $f(x) = ax^2 + bx + c$ – многочлен с целыми коэффициентами, удовлетворяющий условиям (8.36). Второй корень этого многочлена, отличный от $\alpha$, был обозначен ранее символом $\alpha'$. Число $\alpha$ будем называть *приведенным*, если

$$\alpha > 1, \qquad -1 < \alpha' < 0. \tag{8.39}$$

**Пример.** Пусть $D$ – целое положительное, не равное квадрату целого числа. Положим $a_0 = [\sqrt{D}]$ и $\alpha = a_0 + \sqrt{D}$. Тогда $\alpha$ – приведенная квадратичная иррациональность. Действительно, $\alpha' = a_0 - \sqrt{D}$ и неравенства (8.39), очевидно, выполняются.

Для завершения доказательства теоремы 8.9 понадобятся три вспомогательных утверждения.

**Лемма 8.3.** *Пусть $\alpha$, $\beta$ – действительные числа, связанные соотношением $\beta = v + \frac{1}{\alpha}$, где $v$ целое число. Если $\beta$ – квадратичная иррациональность, то таким будет и число $\alpha$, причем $D(\alpha) = D(\beta)$. Если $\beta$ – приведенная квадратичная иррациональность и $v = [\beta]$, то $\alpha$ – приведенная квадратичная иррациональность.*

*Доказательство.* Так как $\alpha = \frac{1}{\beta - v} \in \mathbb{Q}(\sqrt{D(\beta)})$ и $\alpha \notin \mathbb{Q}$, то $\alpha$ квадратичная иррациональность.

Если $\alpha$ – корень многочлена $ax^2 + bx + c$ с целыми коэффициентами, удовлетворяющими условиям $(a, b, c) = 1$, $a > 0$, то число $\beta$ есть корень многочлена

$$c(x - v)^2 + b(x - v) + a = cx^2 + (b - 2cv)x + a - bv + cv^2.$$

Коэффициенты этого квадратного трехчлена взаимно просты в совокупности, поэтому

$$D(\beta) = (b - 2cv)^2 - 4c(a - bv + cv^2) = b^2 - 4ac = D(\alpha).$$

Допустим теперь, что $\beta$ – приведенная квадратичная иррациональность, т.е. $\beta > 1$, $-1 < \beta' < 0$. Так как $v = [\beta]$, то $0 < \beta - v < 1$ и $\alpha = \frac{1}{\beta - v} > 1$.

Из равенства, связывающего числа $\alpha$ и $\beta$, учитывая, что $v = [\beta] \geq 1$, находим

$$-\frac{1}{\alpha'} = v - \beta' > 1.$$

Отсюда следует $0 < -\alpha' < 1$ и $-1 < \alpha' < 0$. Получившиеся неравенства означают приведенность $\alpha$. □

Из этой леммы, в частности следует, что остатки $\alpha_n$, получающиеся при разложении квадратичной иррациональности $\alpha$ в цепную дробь, являются квадратичными иррациональностями, их дискриминанты равны дискриминанту $\alpha$, т.е. $D(\alpha_n) = D(\alpha)$, $n \geq 1$.

**Лемма 8.4.** *Если $\alpha$ – квадратичная иррациональность, то числа $\alpha_n$ – остатки непрерывной дроби $\alpha$, при всех достаточно больших номерах $n$ будут приведенными.*

*Доказательство.* Из определения остатков непрерывной дроби следует, что $\alpha_n > 1$ при любом $n \geq 1$.

Далее из равенства (8.25) следует

$$q_n\alpha' - p_n = \frac{(-1)^n}{\alpha'_{n+1}q_n + q_{n-1}} \tag{8.40}$$

и

$$\alpha'_{n+1}q_n = -q_{n-1} + \frac{1}{q_n} \cdot \frac{(-1)^n}{\alpha' - \frac{p_n}{q_n}}. \tag{8.41}$$

Учитывая, что $\frac{p_n}{q_n} \to \alpha$, и, значит, второе слагаемое в правой части последнего равенства стремится к нулю, получаем, что при всех достаточно больших $n$ выполняется неравенство $\alpha'_{n+1} < 0$.

Из (8.41) также следует

$$(\alpha'_{n+1} + 1)q_n = q_n - q_{n-1} + \frac{1}{q_n} \cdot \frac{(-1)^n}{\alpha' - \frac{p_n}{q_n}}.$$

Поскольку $q_n - q_{n-1} \geq 1$, заключаем отсюда, что при всех достаточно больших $n$ выполняется $\alpha'_{n+1} + 1 > 0$.

Доказанные неравенства означают, что для $n$, превосходящих некоторую границу, все числа $\alpha_n$ будут приведенными. □

**Лемма 8.5.** *Для каждого целого числа $D > 0$ существует лишь конечное число приведенных квадратичных иррациональностей с дискриминантом $D$.*

*Доказательство.* Предположим, что $\alpha$ приведенная квадратичная иррациональность дискриминанта $D$ и $f(x) = ax^2 + bx + c$ – многочлен, удовлетворяющий условиям (8.36). Тогда $b^2 - 4ac = D$ и $c \neq 0$.

Условие приведенности означает, что $c = a\alpha\alpha' < 0$. Значит, $b^2 + 4a|c| = D$ и $|b| \leq \sqrt{D}$, $0 < a < D/4$, $-D/4 < c < 0$, т.е. при фиксированном $D$ каждый из целых коэффициентов $a, b, c$ может иметь лишь конечное число значений. Этим лемма доказана. □

*Завершение доказательства теоремы.* Докажем, что каждая квадратичная иррациональность раскладывается в периодическую цепную дробь.

Пусть $\alpha$ – квадратичная иррациональность. Обозначим $D = D(\alpha)$. Из лемм 8.3 и 8.4 следует, что найдется целое число $n_0$ такое, что при всех $n \geq n_0$ числа $\alpha_n$ будут приведенными квадратичными

иррациональностями дискриминанта $D$. Из леммы 8.5 следует, что среди них может быть лишь конечное число различных. Поэтому найдутся два индекса $m > \ell > n_0$ такие, что $\alpha_m = \alpha_\ell$. Каждый остаток непрерывной дроби однозначно определяется по предшествующему остатку. Поэтому $\alpha_{m+1} = \alpha_{\ell+1}$, $\alpha_{m+2} = \alpha_{\ell+2}$ и т.д. Обозначив $k = m - l > 0$, получившиеся равенства можно записать в виде $\alpha_{n+k} = \alpha_n$ при любом $n \geq \ell$. Требуемая периодичность непрерывной дроби доказана. □

Определим теперь, разложение каких квадратичных иррациональностей в цепную дробь будет чисто периодическим.

**Теорема 8.10.** *Пусть $\alpha$ – квадратичная иррациональность. Цепная дробь $\alpha$ будет чисто периодической в том и только том случае, когда $\alpha$ – приведенная иррациональность.*

*Доказательство.* Если цепная дробь $\alpha$ чисто периодическая, то с некоторым натуральным $k$ при любом $n \geq 0$ выполняются равенства $\alpha_{n+k} = \alpha_n$. В частности, $\alpha = \alpha_0 = \alpha_{rk}$ при любом целом $r \geq 0$. Выбрав $r$ достаточно большим, в соответствии с леммой 8.3 заключаем, что $\alpha$ – приведенная квадратичная иррациональность.

Предположим теперь, что $\alpha$ – приведенная квадратичная иррациональность. По лемме 8.3 можно утверждать, что все числа $\alpha_n$, $n \geq 0$, приведены. Согласно теореме Эйлера-Лагранжа найдутся целые индексы $k$ и $\ell$ такие, что при любом $n \geq \ell$ выполняется неравенство $\alpha_{n+k} = \alpha_n$. Будем считать, что $\ell$ – наименьшее число с этом свойством. Допустим, что $\ell \geq 1$. Из равенств

$$\alpha_{\ell-1} = a_{\ell-1} + \frac{1}{\alpha_\ell}, \qquad \alpha_{\ell+k-1} = a_{\ell+k-1} + \frac{1}{\alpha_{\ell+k}} \tag{8.42}$$

следует

$$-\frac{1}{\alpha_\ell'} = a_{\ell-1} - \alpha_{\ell-1}', \qquad -\frac{1}{\alpha_{\ell+k}'} = a_{\ell+k-1} - \alpha_{\ell+k-1}'.$$

Учитывая, что $\alpha_{\ell-1}$ и $\alpha_{\ell+k-1}$ – приведенные иррациональности, получаем $0 < -\alpha'_{\ell-1} < 1$ и $0 < -\alpha'_{\ell+k-1} < 1$, так что

$$a_{\ell-1} = \left[-\frac{1}{\alpha_\ell{}'}\right], \qquad a_{\ell+k-1} = \left[-\frac{1}{\alpha'_{\ell+k}}\right].$$

Из равенства $\alpha_\ell = \alpha_{\ell+k}$ следует $\alpha_\ell{}' = \alpha'_{\ell+k}$ и $a_{\ell-1} = a_{\ell+k-1}$. Возвращаясь к равенствам (8.42), получаем $\alpha_{\ell-1} = \alpha_{\ell+k-1}$, что противоречит минимальности $\ell$. Следовательно, $\ell = 0$. □

## 8.7 Использование цепных дробей для решения некоторых диофантовых уравнений

Пусть $d$ – натуральное число, не являющееся квадратом какого-либо целого числа. Диофантово уравнение

$$x^2 - dy^2 = 1 \tag{8.43}$$

называется уравнением Пелля. Ясно, что если пара целых чисел $x, y$ есть решение этого уравнения, то числа $\pm x, \pm y$ при любом распределении знаков также будут составлять решение уравнения (8.43). Поэтому, оставив в стороне тривиальное решение $x = \pm 1, y = 0$, далее будем рассматривать решения с условием $x > 0, y > 0$.

Если числа $x, y$ образуют решение уравнения (8.43), то $x^2 > dy^2$ и $x > \sqrt{d}\, y$. Но тогда

$$|x - \sqrt{d}\, y| = \frac{1}{x + \sqrt{d}\, y} < \frac{1}{2\sqrt{d}\, y}$$

и

$$\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{2\sqrt{d}\, y^2} < \frac{1}{2y^2}.$$

С помощью теоремы 8.6 заключаем теперь, что дробь $\frac{x}{y}$ есть подходящая дробь к числу $\sqrt{d}$. Таким образом, задача нахождения решений уравнения Пелля в натуральных числах сводится к поиску

тех из подходящих дробей для $\sqrt{d}$, которые удовлетворяют этому уравнению.

Разложения в цепные дроби чисел вида $\sqrt{d}$ обладают рядом особенностей. К описанию их мы сейчас и перейдем.

**Лемма 8.6.** *Пусть $\alpha$ – приведенная квадратичная иррациональность. Тогда $\beta = -\frac{1}{\alpha'}$ – также приведенная квадратичная иррациональность. Период цепной дроби $\beta$ состоит из чисел периода $\alpha$, записанных в обратном порядке.*

*Доказательство.* Утверждение, что $\beta$ есть квадратичная иррациональность, очевидно, так как $\alpha'$ есть корень того же многочлена второй степени, что и $\alpha$. Приведенность $\beta$ означает выполнение следующих неравенств

$$\beta = -\frac{1}{\alpha'} > 1, \qquad -1 < \beta' = -\frac{1}{\alpha} < 0.$$

Первое из них выполняется, поскольку $-1 < \alpha' < 0$, а второе – в силу того, что $\alpha > 1$.

Пусть $\alpha = [\overline{a_0, a_1, \ldots, a_m}]$ – чисто периодическая в силу теоремы 8.10 цепная дробь числа $\alpha$. Тогда справедливы равенства

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}, \qquad k = 0, \ldots, m, \qquad \alpha_0 = \alpha_{m+1} = \alpha. \tag{8.44}$$

Обозначим $\beta_k = -\frac{1}{\alpha'_{m+1-k}}$, $k = 0, \ldots, m+1$. Из (8.44) следует

$$\alpha_k' = a_k + \frac{1}{\alpha_{k+1}'}$$

или в других обозначениях

$$-\frac{1}{\beta_{m+1-k}} = a_k - \beta_{m-k}. \tag{8.45}$$

Меняя сторонами члены равенства (8.45), находим

$$\beta_{m-k} = a_k + \frac{1}{\beta_{m+1-k}}, \qquad 0 \le k \le m.$$

Введем новую переменную $i = m - k$ для обозначения индексов. Тогда получившиеся равенства могут быть переписаны в виде

$$\beta_i = a_{m-i} + \frac{1}{\beta_{i+1}}, \qquad 0 \le i \le m. \tag{8.46}$$

Согласно лемме 8.3 все числа $\alpha_{m+1-k}$ приведены. Как доказано выше, отсюда следует приведенность чисел $\beta_k$ и, значит, неравенства $\beta_k > 1$. Теперь из (8.46) получаем $[\beta_i] = a_{m-i}$, $0 \le i \le m$.

Из определения чисел $\beta_k$ следует, что $\beta_{m+1} = -\frac{1}{\alpha_0'} = -\frac{1}{\alpha_{m+1}'} = \beta_0$. Поэтому $\beta = [\overline{a_m, \ldots, a_0}]$ и это завершает доказательство леммы. □

**Лемма 8.7.** *Если $d$ – натуральное число, не являющееся квадратом никакого целого числа, то*

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_k, 2a_0}],$$

*где $a_0 = [\sqrt{d}]$, причем упорядоченный набор чисел $a_1, \ldots, a_k$ симметричен, т.е. $a_1 = a_k$, $a_2 = a_{k-1}$ и т.д.*

*Доказательство.* Число $\gamma = a_0 + \sqrt{d}$ приведено. Действительно, оно, очевидно, удовлетворяет неравенству $\gamma > 1$, а кроме того для $\gamma' = a_0 - \sqrt{d}$ в силу $a_0 = [\sqrt{d}]$ выполняется $-1 < \gamma' < 0$. Согласно теореме 8.10 можно утверждать, что $\gamma$ имеет чисто периодическую цепную дробь. Учитывая, что $[\gamma] = 2a_0$, находим

$$\gamma = [\overline{2a_0, a_1, \ldots a_k}] \tag{8.47}$$

с некоторыми целыми $a_1, \ldots, a_k$. Отсюда в силу равенства $\gamma + \gamma' = 2a_0$ и, следовательно,

$$\gamma = 2a_0 + \frac{1}{\left(-\dfrac{1}{\gamma'}\right)},$$

получаем разложение

$$-\frac{1}{\gamma'} = [\overline{a_1, \ldots, a_k, 2a_0}].$$

Согласно лемме 8.6 отсюда следует $\gamma = [\overline{2a_0, a_k, \ldots, a_1}]$. Сравнивая эту цепную дробь с (8.47), получаем утверждение о симметрии. □

**Лемма 8.8.** *Пусть $d$ – натуральное число, не являющееся квадратом никакого целого и $\alpha_n$ – последовательность остатков цепной дроби $\sqrt{d}$, определенная равенствами (7.15). Для каждого $n \geq 0$ выполняется равенство*

$$\alpha_n = \frac{A_n + \sqrt{d}}{B_n}, \qquad A_n \geq 0, \quad B_n > 0, \tag{8.48}$$

*где $A_n, B_n$ – целые числа. При $n \geq 0$ справедливы равенства*

$$A_{n+1} = a_n B_n - A_n, \quad B_{n+1} = \frac{d - A_{n+1}^2}{B_n}, \quad A_0 = 0,\ B_0 = 1. \tag{8.49}$$

*Доказательство.* Докажем равенство (8.48) с помощью индукции по $n$. Для $n = 0$ утверждение выполняется с $A_0 = 0$ и $B_0 = 1$.

Пусть теперь $n \geq 0$ и утверждение верно для числа $\alpha_n$. Из равенств $\alpha_1 = \frac{1}{\sqrt{d}-a_0}$ и $\alpha_1{}' = -\frac{1}{\sqrt{d}+a_0}$ следует $\alpha_1 > 1$, $-1 < \alpha_1 < 0$, так что $\alpha_1$ – приведенное число. Согласно лемме 8.3 можно утверждать, что $\alpha_{n+1}$ – приведенное число. Обозначим

$$ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}, \quad (a, b, c) = 1, \quad a > 0,$$

многочлен, корнем которого является $\alpha_{n+1}$. Из условий приведенности следует, что $\alpha_{n+1} > \alpha'_{n+1}$. Поэтому

$$\alpha_{n+1} = \frac{-b + \sqrt{D(\alpha_{n+1})}}{2a}, \qquad \alpha_{n+1}{}' = \frac{-b - \sqrt{D(\alpha_{n+1})}}{2a},$$

где $D(\alpha_{n+1}) = b^2 - 4ac$ – дискриминант $\alpha_{n+1}$. Все числа $\alpha_j$ при $j \geq 0$, имеют равные дискриминанты, поэтому $b^2 - 4ac = D(\alpha) = 4d$. Отсюда следует, что $b$ четно и с целыми числами $A_{n+1} = -b/2$, $B_{n+1} = a > 0$ справедливо представление

$$\alpha_{n+1} = \frac{A_{n+1} + \sqrt{d}}{B_{n+1}}. \tag{8.50}$$

Число $\alpha_{n+1}$ приведено, поэтому $\frac{2A_{n+1}}{B_{n+1}} = \alpha_{n+1} + \alpha'_{n+1} > 0$ и, значит, $A_{n+1} > 0$.

Равенство $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$ можно переписать в виде $\alpha_{n+1}(\alpha_n - a_n) = 1$. Подставляя сюда представления (8.48), (8.50) и умножая получившееся равенство на $B_nB_{n+1}$, легко находим

$$(A_{n+1} + \sqrt{d})(A_n - a_nB_n + \sqrt{d}) = B_nB_{n+1}. \tag{8.51}$$

Раскрыв скобки в левой части получившегося равенства и приравняв к нулю коэффициент при $\sqrt{d}$, получим $A_n - a_nB_n + A_{n+1} = 0$, так что

$$A_{n+1} = a_nB_n - A_n.$$

Теперь из (8.51) следует $d - A_{n+1}^2 = B_nB_{n+1}$ и

$$B_{n+1} = \frac{d - A_{n+1}^2}{B_n}. \tag{8.52}$$

Лемма полностью доказана. □

**Лемма 8.9.** *Если в условиях предыдущей леммы $\frac{p_n}{q_n}$ – подходящая дробь к $\sqrt{d}$, то*

$$p_n^2 - dq_n^2 = (-1)^{n+1}B_{n+1}, \qquad n \geq -1. \tag{8.53}$$

*Доказательство.* Из (8.24) при $\alpha = \sqrt{d}$ и $k = n$ находим

$$\alpha_{n+1}(q_n\sqrt{d} - p_n) = p_{n-1} - q_{n-1}\sqrt{d}. \tag{8.54}$$

Умножим обе части этого равенства на $q_n\sqrt{d} + p_n$. В результате получится

$$\alpha_{n+1}(q_n^2d - p_n^2) = (p_{n-1} - q_{n-1}\sqrt{d})(q_n\sqrt{d} + p_n).$$

Если подставить в это равенство выражение для $\alpha_{n+1}$ из (8.50) и, воспользовавшись иррациональностью $\sqrt{d}$, сравнить коэффициенты при $\sqrt{d}$, будем иметь

$$\frac{q_n^2d - p_n^2}{B_{n+1}} = p_{n-1}q_n - q_{n-1}p_n = (-1)^n.$$

Последнее равенство выполняется в силу (8.12). Это завершает доказательство леммы. □

Следующая теорема описывает множество всех решений уравнения Пелля (8.43).

**Теорема 8.11.** *Пусть $d$ – натуральное число, не равное квадрату целого, и*

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_k, 2a_0}]$$

*– разложение в цепную дробь с наименьшим периодом. Множество решений уравнения Пелля в натуральных числах состоит из пар $(p_n, q_n)$ числителей и знаменателей подходящих дробей к $\sqrt{d}$ с условием, что $n+1$ четно и делится на $k+1$. Определим целые положительные числа $x_1, y_1$ равенствами*

$$x_1 + y_1\sqrt{d} = \begin{cases} p_k + q_k\sqrt{d}\ , & \text{если } k \text{ нечетно,} \\ (p_k + q_k\sqrt{d})^2\ , & \text{если } k \text{ четно.} \end{cases}$$

*Все решения уравнения Пелля (8.43) в натуральных числах образуют последовательность $(x_m, y_m)$ и получаются по формуле*

$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m, \qquad m = 1, 2, \ldots\ . \tag{8.55}$$

Заметим, что тривиальное решение $x = 1, y = 0$ уравнения (8.43) получается по формуле (8.55) при $m = 0$.

*Доказательство.* Как уже говорилось в начале параграфа, все решения $(x, y)$ уравнения Пелля в натуральных числах содержатся среди числителей и знаменателей подходящих дробей к $\sqrt{d}$. Согласно формуле (8.53) пара чисел $(p_n, q_n)$ будет решением уравнения Пелля лишь в случае, когда выполняются два условия

1) $n$ нечетно,

2) $B_{n+1} = 1$.

Равенство $B_{n+1} = 1$ выполняется в том и только том случае, когда $\alpha_{n+1} = A_{n+1} + \sqrt{d}$. Так как при этом $\alpha_{n+1}$ приведено, то $-1 < A_{n+1} - \sqrt{d} < 0$, и, значит, $A_{n+1} = [\sqrt{d}] = a_0$. Следовательно, равенство $B_{n+1} = 1$ имеет место в том и только том случае, когда $\alpha_{n+1} = a_0 + \sqrt{d} = [\overline{2a_0, a_1, \ldots, a_k}]$, т.е. с некоторым целым $m \geq 1$ выполняется

$n+1 = m(k+1)$. Итак, все решения уравнения Пелля в натуральных числах совпадают с парами чисел $(p_n, q_n)$, номера которых нечетны и удовлетворяют условию $n+1 = m(k+1)$. Это доказывает первое утверждение теоремы.

Чтобы найти формулы для решений докажем сначала с помощью индукции по $n$ справедливость равенств

$$\alpha_1\alpha_2\cdots\alpha_{n+1} = \frac{(-1)^{n+1}}{p_n - q_n\sqrt{d}}, \qquad n \geq 0. \tag{8.56}$$

При $n = 0$ (8.56) следует из равенства $\sqrt{d} = a_0 + \frac{1}{\alpha_1}$. Предположим, что $n \geq 1$ и

$$\alpha_1\alpha_2\cdots\alpha_n = \frac{(-1)^n}{p_{n-1} - q_{n-1}\sqrt{d}}. \tag{8.57}$$

Из (8.54) следует

$$\alpha_{n+1} = -\frac{q_{n-1}\sqrt{d} - p_{n-1}}{q_n\sqrt{d} - p_n}\ , \qquad n \geq 0.$$

Теперь для того, чтобы получить (8.56) достаточно перемножить два последние равенства.

В случае $n+1 = m(k+1)$, пользуясь тем, что цепная дробь $\sqrt{d}$ имеет период длиной $k+1$, т.е. $\alpha_{i+k+1} = \alpha_i$, находим

$$\alpha_1\alpha_2\cdots\alpha_{n+1} = (\alpha_1\cdots\alpha_{k+1})^m = \frac{(-1)^{m(k+1)}}{(p_k - q_k\sqrt{d})^m}.$$

Сравнивая это равенство с (8.56) при $n+1 = m(k+1)$, получаем

$$p_n - q_n\sqrt{d} = (p_k - q_k\sqrt{d})^m$$

и переходя к сопряженным числам –

$$p_n + q_n\sqrt{d} = (p_k + q_k\sqrt{d})^m. \tag{8.58}$$

Если $k$ нечетно, то при любом натуральном $m$ число $n+1 = m(k+1)$ будет четным. Следовательно при любом натуральном $m$ пара целых чисел $(p_n, q_n)$, определенная равенством (8.58) будет решением

уравнения Пелля. Это доказывает второе утверждение теоремы при нечетном $k$.

Если же $k$ четно, то $n+1 = m(k+1)$ будет нечетным лишь в случае, когда $m = 2r$ – четно. Тогда из (8.58) находим

$$p_n + q_n\sqrt{d} = (p_k + q_k\sqrt{d})^{2r} = (x_1 + y_1\sqrt{d})^r.$$

Это завершает доказательство теоремы. □

**Следствие 8.7.** *Решения уравнения Пелля могут быть найдены с помощью рекуррентных соотношений*

$$x_{m+1} = x_1x_m + dy_1y_m,$$
$$y_{n+1} = y_1x_m + x_1y_m,$$

*справедливых при* $m \geq 0$.

Для доказательства этих формул достаточно заметить, что из (8.55) следует равенство

$$x_{m+1} + y_{m+1}\sqrt{d} = (x_m + y_m\sqrt{d})(x_1 + y_1\sqrt{d}),$$

и воспользовавшись иррациональностью $\sqrt{d}$, сравнить соответствующие коэффициенты в левой и правой частях.

**Пример.** Найти все решения в натуральных числах уравнения

$$x^2 - 29y^2 = 1.$$

Следующие вычисления раскладывают $\alpha = \sqrt{29}$ в непрерывную

дробь.

$$\alpha_0 = \sqrt{29}\ , \qquad a_0 = [\alpha_0] = 5,$$
$$\alpha_1 = \frac{1}{\alpha_0 - 5} = \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{4}\ , \qquad a_1 = [\alpha_1] = 2,$$
$$\alpha_2 = \frac{1}{\alpha_1 - 2} = \frac{4}{\sqrt{29} - 3} = \frac{\sqrt{29} + 3}{5}\ , \qquad a_2 = [\alpha_2] = 1,$$
$$\alpha_3 = \frac{1}{\alpha_2 - 1} = \frac{5}{\sqrt{29} - 2} = \frac{\sqrt{29} + 2}{5}\ , \qquad a_3 = [\alpha_3] = 1,$$
$$\alpha_4 = \frac{1}{\alpha_3 - 1} = \frac{5}{\sqrt{29} - 3} = \frac{\sqrt{29} + 3}{4}\ , \qquad a_4 = [\alpha_4] = 2,$$
$$\alpha_5 = \frac{1}{\alpha_4 - 2} = \frac{4}{\sqrt{29} - 5} = 5 + \sqrt{29}\ , \qquad a_5 = [\alpha_5] = 10,$$
$$\alpha_6 = \frac{1}{\sqrt{29} - 5} = \alpha_1.$$

Таким образом $\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$. В данном случае $k = 4$. Последовательность подходящих дробей в рассматриваемом случае такова

$$\frac{p_0}{q_0} = \frac{5}{1}\ , \quad \frac{11}{2}\ , \quad \frac{16}{3}\ , \quad \frac{27}{5}\ , \quad \frac{p_4}{q_4} = \frac{70}{13}\ , \ldots$$

Так как в данном случае $k$ четно, находим в соответствии с теоремой 8.11

$$x_1 + y_1\sqrt{29} = (70 + 13\sqrt{29})^2 = 9801 + 1820\sqrt{29}.$$

Значит, наименьшее решение данного уравнения в натуральных числах имеет вид $x_1 = 9801, y_1 = 1820)$. Последовательность всех решений может быть вычислена по формулам

$$x_{m+1} = 9801x_m + 52780y_m,$$
$$y_{n+1} = 1820x_m + 9801y_m,$$

Например, второе и третье решения имеют вид

$$(192119201, 35675640), \qquad (3765920568201, 699313893460).$$

Из доказательства теоремы 8.11 следует, что уравнение $x^2 - dy^2 = -1$ разрешимо в целых числах лишь в случае, если длина наименьшего периода цепной дроби $\sqrt{d}$ нечетна. Известны лишь немногие случаи, когда можно утверждать, что это уравнение разрешимо, не раскладывая $\sqrt{d}$ в цепную дробь.

**Лемма 8.10.** *Если $p$ – простое число вида $4n+1$, то уравнение*

$$x^2 - py^2 = -1$$

*разрешимо в целых числах, и, значит, наименьший период разложения $\sqrt{p}$ в цепную дробь имеет нечетную длину.*

*Доказательство.* Пусть $(u, v)$ – наименьшее решение уравнения $x^2 - py^2 = 1$ в натуральных числах. Оно существует согласно теореме 8.11. Тогда $u^2 - v^2 \equiv 1 \pmod 4$, и, значит, $u$ – нечетно, а $v$ – четно. Поскольку $\frac{u+1}{2} - \frac{u-1}{2} = 1$, числа $\frac{u+1}{2}$ и $\frac{u-1}{2}$ взаимно просты. Теперь из равенства

$$\frac{u-1}{2} \cdot \frac{u+1}{2} = p\left(\frac{v}{2}\right)^2$$

заключаем, что с некоторыми натуральными числами $s, t$ и $\varepsilon = \pm 1$ выполняются равенства

$$\frac{u+\varepsilon}{2} = t^2, \qquad \frac{u-\varepsilon}{2} = ps^2.$$

Из этих равенств следует

$$t^2 - ps^2 = \varepsilon.$$

Учитывая условие минимальности при выборе решения $(u, v)$ и неравенство $1 \le s < v$, заключаем $\varepsilon = -1$ и, значит, $u^2 - pv^2 = -1$. Из разрешимости уравнения $x^2 - py^2 = -1$ в целых числах следует, что наименьший период разложения $\sqrt{p}$ в цепную дробь имеет нечетную длину. □

Следующее утверждение уже было доказано ранее, см. лемму 6.4. Здесь мы покажем, как с помощью непрерывных дробей можно находить решения соответствующего диофантова уравнения.

**Теорема 8.12.** *Если $p$ – простое число вида $4n+1$, то уравнение*

$$x^2 + y^2 = p$$

*разрешимо в целых числах.*

*Доказательство.* Из леммы 8.10 следует, что длина наименьшего периода цепной дроби $\sqrt{p}$ нечетна. Вместе с утверждением леммы 8.7 это позволяет записать

$$\sqrt{p} = [a_0; \overline{a_1, \ldots, a_r, a_r, \ldots, a_1, 2a_0}].$$

Тогда

$$\alpha_{r+1} = [\ \overline{a_r, \ldots, a_1, 2a_0, a_1, \ldots, a_r}\ ]$$

и по лемме 8.6 заключаем $\alpha_{r+1} = -\frac{1}{\alpha'_{r+1}}$. Значит, $\alpha_{r+1}\alpha'_{r+1} = -1$. Пользуясь теперь представлением (8.48) находим $\frac{A^2_{r+1}-p}{B^2_{r+1}} = -1$ и, следовательно, $A^2_{r+1} + B^2_{r+1} = p$. □

Заметим, что приведенное доказательство дает и способ вычисления решения. Так при $p = 29$ имеем $r = 2$ и $\alpha_3 = \frac{2+\sqrt{29}}{5}$. Пара чисел $(2, 5)$ составляет решение уравнения $x^2 + y^2 = 29$.

*Второе доказательство теоремы 8.12.* Так как $p$ при делении на 4 дает в остатке 1, то по теореме 6.1 найдется целое число $a$, удовлетворяющее условиям

$$a^2 + 1 \equiv 0 \pmod{p}, \qquad 0 < a < p.$$

Разложим рациональное число $\frac{a}{p}$ в цепную дробь, и пусть $\frac{p_k}{q_k}$ подходящая дробь к $\frac{a}{p}$ с наибольшим номером, удовлетворяющим неравенству $q_k < \sqrt{p}$. Тогда $\sqrt{p} < q_{k+1}$. Из неравенства (8.26) следует, что

$$\left|\frac{a}{p} - \frac{p_k}{q_k}\right| \le \frac{1}{q_k q_{k+1}} < \frac{1}{q_k\sqrt{p}}.$$

Умножим обе части последнего неравенства на произведение знаменателей левой части. В результате получится

$$|aq_k - pp_k| < \sqrt{p}.$$

Тогда

$$(aq_k - pp_k)^2 + q_k^2 < 2p.$$

Кроме того имеем $aq_k - pp_k \equiv aq_k \pmod{p}$ и

$$(aq_k - pp_k)^2 + q_k^2 \equiv q_k^2(a^2+1) \equiv 0 \pmod{p}.$$

На интервале $0 < x < 2p$ есть только одно целое число, делящееся на $p$, а именно само $p$. Поэтому $(aq_k - pp_k)^2 + q_k^2 = p$, т.е. уравнению теоремы 8.12 удовлетворяют числа $x = aq_k - pp_k$ и $y = q_k$. □

Например, для решения уравнения $x^2 + y^2 = 29$ заметим, что сравнению $x^2 + 1 \equiv 0 \pmod{29}$ удовлетворяет число $x = 12$. Справедливо разложение в цепную дробь $\frac{12}{29} = [0; 2, 2, 2, 2]$. Числитель и знаменатель подходящей дроби $\frac{p_2}{q_2} = [0; 2, 2] = \frac{2}{5}$ удовлетворяют данному уравнению.

Не трудно доказать, что уравнение из теоремы 8.12 с точностью до перестановки переменных имеет единственное решение.

## 8.8 Разложение числа $e$ в цепную дробь

Классическая постоянная $e$ определяется в курсах математического анализа пределом

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = 2,718281828459045235360287471352662497757\ldots$$

Как мы докажем ниже эта десятичная дробь бесконечна и не имеет периода.

Букву $e$ для обозначения указанного предела впервые стал использовать Л. Эйлер, который доказал также в 1737г. следующее утверждение.

**Теорема 8.13.** *Разложение числа $e$ в цепную дробь имеет вид*

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, \ldots].$$

В отличие от десятичного разложения цепная дробь $e$ устроена регулярно: пары единиц перемежаются последовательно идущими четными числами. Можно представить себе ее неполные частные $a_i$ при $i \geq 1$ иначе, заметив, что их последовательность распадается на отрезки, состоящие из трех чисел и имеющие вид $1, 2m, 1$, где $m$ принимает значения $1, 2, 3, \ldots$. Поэтому цепную дробь для $e$ часто записывают в виде $[2; \overline{1, 2m, 1}]_{m\geq 1}$.

Так как цепная дробь числа $e$ бесконечна, имеем согласно второму утверждению теоремы 8.2

**Следствие 8.8.** *Число $e$ иррационально.*

Для доказательства теоремы 8.13 рассмотрим бесконечную последовательность действительных чисел $I_{-1}, I_0, I_1, I_2, \ldots$, определенную с помощью интегралов

$$I_{3n-2} = \frac{1}{n!}\int_0^1 e^x x^n (1-x)^n dx\ , \quad n \geq 1,$$
$$I_{3n-1} = \frac{1}{n!}\int_0^1 e^x x^{n+1} (1-x)^n dx\ , \quad n \geq 0,$$
$$I_{3n} = \frac{1}{n!}\int_0^1 e^x x^n (1-x)^{n+1} dx\ , \quad n \geq 0.$$

Эти числа связаны между собой рекуррентными соотношениями.

**Лемма 8.11.** *Все числа $I_k, k \geq -1$, неотрицательны и образуют убывающую последовательность. Справедливы равенства*

$$\begin{aligned} I_{3n-2} &= I_{3n-1} + I_{3n}, && n \geq 1, \\ I_{3n-1} &= I_{3n} + I_{3n+1}, && n \geq 0, \\ I_{3n} &= (2n+2)I_{3n+1} + I_{3n+2}, && n \geq 0. \end{aligned}$$

*Доказательство.* Докажем сначала равенства, связывающие числа $I_k$. Имеем

$$I_{3n-2} - I_{3n-1} = \frac{1}{n!}\int_0^1 e^x x^n (1-x)^n (1-x)dx = I_{3n},$$

$$I_{3n+1} = \frac{1}{(n+1)!}\int_0^1 (x-x^2)^{n+1} d(e^x) = \\ = \frac{1}{n!}\int_0^1 e^x (x-x^2)^n (x-(1-x)) = I_{3n-1} - I_{3n}.$$

Второе равенство получено интегрированием по частям. Для доказательства третьего соотношения воспользуемся тем же приемом

$$I_{3n+2} = \frac{-1}{(n+1)!}\int_0^1 (x-x^2)^{n+1} d(e^x(1-x))dx = \\ = \frac{n+1}{(n+1)!}\int_0^1 e^x x^n (1-x)^{n+1}(1-2x)dx = I_{3n} - (2n+2)I_{3n+1}.$$

Доказанные равенства могут быть записаны единообразно в виде

$$I_{k-1} = b_k I_k + I_{k+1}, \qquad k \geq 0, \tag{8.59}$$

где

$$b_k = \begin{cases} 1 & \text{если } k = 3n-1, \\ 1 & \text{если } k = 3n, \\ 2n+2 & \text{если } k = 3n+1. \end{cases} \tag{8.60}$$

Утверждение леммы о положительности чисел $I_k$ следует из того, что все подинтегральные функции непрерывны на отрезке $[0;1]$ и положительны на интервале $(0;1)$. Теперь с помощью равенств (8.59) и (8.60) получаем $I_{k-1} > I_k$, $k \geq 0$. □

Введем обозначения

$$\alpha_k = \frac{I_{k-1}}{I_k}, \qquad k \geq 0.$$

Из леммы 8.11 следует, что $\alpha_k > 1$, а из равенства (8.59) находим

$$\alpha_k = b_k + \frac{1}{\alpha_{k+1}}, \qquad k \geq 0.$$

Но тогда $b_k = [\alpha_k]$, и согласно теореме 8.4 мы получаем разложение в цепную дробь $\alpha_0 = [b_0; b_1, b_2, \ldots] = [1; 2, 1, 1, 4, 1, 1, 6, 1, \ldots]$ .

Поскольку

$$I_{-1} = \int_0^1 e^x x dx = 1, \quad I_0 = \int_0^1 e^x (1-x) dx = e - 2,$$

находим $\alpha_0 = \frac{1}{e-2}$. Отсюда также следует, что $e = 2 + \frac{1}{\alpha_0}$ и, значит, $e = [2; b_0, b_1, \ldots] = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots]$.

# Глава 9

# Алгебраические и трансцендентные числа

## 9.1 Поле алгебраических чисел

В множестве комплексных чисел можно выделить подмножества, удобные в том или другом отношении. Например, для решения диофантовых уравнений иногда привлекаются числа, лежащие в более широких множествах, чем множество рациональных чисел. Так в главе 8 оказалось удобным описывать множество всех решений уравнения Пелля, используя квадратичные иррациональности, т.е. корни квадратных уравнений с рациональными коэффициентами. Попытки доказательства теоремы Ферма о решениях в натуральных числах уравнения $x^n + y^n = z^n, n > 2$, привели к созданию теории, описывающей свойства чисел, зависящих от корней степени $n$ из единицы, а в конечном счете к теории алгебраических чисел. В этом параграфе будут установлены простейшие свойства алгебраических чисел.

**Определение 9.** *1. Комплексное число $\alpha$ называется* алгебраическим*, если найдется отличный от нуля многочлен $f(x) \in \mathbb{Q}[x]$, для которого $f(\alpha) = 0$.*

*2. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен*

*называется* минимальным многочленом $\alpha$. *Его степень называется* степенью $\alpha$ *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 $\alpha$ есть корень некоторого многочлена с целыми коэффициентами $ax^2 + bx + c$. Так как $\alpha$ иррационально, то этот многочлен имеет минимальную степень среди всех, лежащих в кольце $\mathbb{Q}[x]$ и обращающихся в нуль при подстановке $\alpha$ вместо $x$. Поэтому $f(x) = x^2 + \frac{b}{a}x + \frac{c}{a} \in \mathbb{Q}[x]$ – минимальный многочлен $\alpha$ и $\deg \alpha = 2$. Так $i, \sqrt{7}$ – алгебраические числа степени 2.

Укажем некоторые свойства минимального многочлена.

**Лемма 9.1.** *1. Минимальный многочлен любого алгебраического числа неприводим.*

*2. Если $f(x)$ – минимальный многочлен числа $\alpha$, которое также является корнем многочлена $g(x) \in \mathbb{Q}[x]$, то многочлен $g(x)$ делится на $f(x)$.*

*3. Неприводимый многочлен со старшим коэффициентом* 1 *служит минимальным многочленом для каждого из своих корней.*

*4. Все корни минимального многочлена различны.*

*Доказательство.* Пусть $\alpha$ алгебраическое число, и его минимальный многочлен $f(x) \in \mathbb{Q}[x]$ приводим, т.е. может быть разложен на множители меньшей степени в кольце $\mathbb{Q}[x]$. Например, $f(x) = g(x)h(x)$, где $g(x), h(x) \in \mathbb{Q}[x]$ и $\deg g(x) < \deg f(x)$, $\deg h(x) < \deg f(x)$. Из равенства

$$0 = f(\alpha) = g(\alpha)h(\alpha)$$

следует, что либо $g(\alpha) = 0$, либо $h(\alpha) = 0$. В любом случае получаем противоречие, ведь $f(x)$ имеет минимальную степень среди всех

ненулевых многочленов кольца $\mathbb{Q}[x]$, обращающихся в нуль в точке $\alpha$.

Для доказательства второго утверждения разделим многочлен $g(x)$ на $f(x)$ с остатком

$$g(x) = f(x)q(x) + r(x), \qquad \deg r(x) < \deg f(x).$$

Справедливы равенства

$$0 = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Поскольку $r(x) \in \mathbb{Q}[x]$, то из определения минимального многочлена, равенства $r(\alpha) = 0$ и неравенства $\deg r(x) < \deg f(x)$ следует $r(x) = 0$, т.е. многочлен $g(x)$ делится на $f(x)$ без остатка.

Пусть $g(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ – неприводимый многочлен из кольца $\mathbb{Q}[x]$ и $\beta$ – его корень. Обозначим минимальный многочлен числа $\beta$ через $f(x)$. Согласно второму утверждению леммы имеем $f(x)|g(x)$. По условию многочлен $g(x)$ неприводим, значит, $g(x) = cf(x)$, где $c$ – некоторая константа. Старшие коэффициенты многочленов $f(x)$, $g(x)$ равны единице, поэтому $g(x) = f(x)$ и $g(x)$ есть минимальный многочлен $\beta$. Третье утверждение леммы доказано.

Пусть $f(x)$ – минимальный многочлен алгебраического числа $\alpha$ и $\beta$ – кратный корень $f(x)$. По первому утверждению леммы многочлен $f(x)$ неприводим и тогда по третьему утверждению он есть минимальный многочлен $\beta$. Так как $\beta$ есть кратный корень многочлена $f(x)$, то производная $f'(x) \in \mathbb{Q}[x]$ также имеет $\beta$ своим корнем. Согласно второму утверждению леммы имеем $f(x)|f'(x)$, что невозможно, так как $\deg f'(x) < \deg f(x)$. Итак, многочлен $f(x)$ не имеет кратных корней. □

**Определение 10.** *Если $\alpha$ – алгебраическое число степени $n$, то корни $\alpha_1, \ldots, \alpha_n$ его минимального многочлена называются числами,* сопряженными *с $\alpha$.*

Докажем, что множество всех алгебраических чисел замкнуто относительно арифметических операций.

**Теорема 9.1.** *Если $\alpha$ и $\beta$ – алгебраические числа, то числа $\alpha+\beta$, $\beta-\alpha$, $\alpha\beta$, а в случае, если $\alpha\neq 0$, то и $\beta/\alpha$ являются алгебраическими числами.*

Из этой теоремы следует, что множество всех алгебраических чисел является полем. Коммутативность и ассоциативность операций сложения и умножения, а также дистрибутивность умножения выполняются, поскольку они имеют место в поле комплексных чисел. Числа 0 и 1 являются алгебраическими.

Напомним некоторые факты, обычно доказываемые в университетских курсах алгебры и необходимые для доказательства теоремы 9.1.

Пусть $\mathbf{A}$ – некоторое кольцо и $t_1,\ldots,t_n$ – переменные. Многочлен $F(t_1,\ldots,t_n)\in\mathbf{A}[t_1,\ldots,t_n]$ называется *симметрическим*, если он не меняется при любой перестановке переменных. Чтобы привести примеры симметрических многочленов введем еще одну переменную $x$ и рассмотрим многочлен

$$(x-t_1)\cdots(x-t_n)=x^n-\sigma_1x^{n-1}+\sigma_2x^{n-2}-\cdots+(-1)^n\sigma_n.$$

Здесь буквами $\sigma_1,\ldots,\sigma_n$ обозначены многочлены

$$\begin{aligned}
\sigma_1&=t_1+t_2+\cdots+t_n,\\
\sigma_2&=t_1t_2+t_1t_3+\cdots+t_{n-1}t_n,\\
&\cdots\cdots\cdots\cdots\\
\sigma_n&=t_1t_2\cdots t_n.
\end{aligned}$$

Эти многочлены, равные сумме всех переменных, сумме всевозможных произведений по две переменные и т.д., очевидно обладают свойством симметрии и называются *элементарными симметрическими многочленами.*

**Теорема о симметрических многочленах:** *Пусть*

$$F[t_1,\ldots,t_n]\in\mathbf{A}[t_1,\ldots,t_n]$$

*– симметрический многочлен степени $d$. Тогда существует многочлен $G[z_1, \ldots, z_n] \in \mathbf{A}[z_1, \ldots, z_n]$ степени не выше $d$, такой, что*

$$F[t_1, \ldots, t_n] = G[\sigma_1, \ldots, \sigma_n].$$

Например, имеет место тождество

$$t_1^2 + t_2^2 + \ldots + t_n^2 = \sigma_1^2 - 2\sigma_2.$$

Как простое следствие этой теоремы получаем

**Лемма 9.2.** *Пусть $P(x, y) \in \mathbb{Q}[x, y]$ – многочлен от двух переменных с рациональными коэффициентами. Пусть также $\alpha$ – алгебраическое число степени $n$ и $\alpha_1, \ldots, \alpha_n$ – все его сопряженные. Тогда*

$$P(x, \alpha_1) \cdot P(x, \alpha_2) \cdot \ldots \cdot P(x, \alpha_n) = R(x), \tag{9.1}$$

*есть многочлен от переменной $x$ с коэффициентами из поля рациональных чисел $\mathbb{Q}$.*

*Доказательство.* Пусть $\mathbf{A} = \mathbb{Q}[x]$ – кольцо многочленов от переменной $x$. Рассмотрим произведение $P(x, t_1) \cdot P(x, t_2) \cdot \ldots \cdot P(x, t_n)$, где $t_1, \ldots, t_n$ – переменные. Этот многочлен не меняется при любой перестановке переменных $t_1, \ldots, t_n$, в произведении лишь меняются местами сомножители. Так что это произведение есть симметрический многочлен от переменных $t_1, \ldots, t_n$ с коэффициентами из кольца $\mathbf{A} = \mathbb{Q}[x]$. Из теоремы о симметрических многочленах следует теперь, что для некоторого многочлена $Q(x, z_1, \ldots, x_n)$ с рациональными коэффициентами выполняется равенство

$$P(x, t_1) \cdot P(x, t_2) \cdot \ldots \cdot P(x, t_n) = Q(x, \sigma_1, \sigma_2, \ldots, \sigma_n), \tag{9.2}$$

где $\sigma_1, \ldots, \sigma_n$.

Заменим в последнем равенстве переменные $t_1, \ldots, t_n$ числами $\alpha_1, \ldots, \alpha_n$. Тогда левая часть (9.2) примет такой же вид, как и левая часть (9.1). Если $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{Q}[x]$

– минимальный многочлен числа $\alpha$, то согласно теореме Виета выполняются равенства

$$\begin{aligned}
\sigma_1(\alpha_1,\dots,\alpha_n) &= -a_1,\\
\sigma_2(\alpha_1,\dots,\alpha_n) &= a_2,\\
&\dots\dots\dots\dots\\
\sigma_n(\alpha_1,\dots,\alpha_n) &= (-1)^n a_n.
\end{aligned}$$

Поэтому правая часть равенства (9.2) после указанной выше подстановки примет вид $Q(x,-a_1,a_2,\dots,(-1)^n a_n)$. Учитывая, что все числа $a_i$ рациональны, получаем нужное утверждение. □

*Доказательство теоремы 9.1.* Утверждение тривиально, если $\alpha = 0$. Далее будем считать $\alpha \neq 0$. Пусть $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ – числа, сопряженные с $\alpha$, а $g(x)$ – минимальный многочлен числа $\beta$. Определим многочлены

$$\begin{aligned}
P_1(x,y) &= g(x+y), & P_2(x,y) &= g(x-y),\\
P_3(x,y) &= g(xy), & P_4(x,y) &= y^m g(y^{-1}x)
\end{aligned}$$

По лемме 9.2 многочлены

$$\begin{aligned}
R_1(x) &= \prod_{j=1}^{n} g(x+\alpha_j), & R_2(x) &= \prod_{j=1}^{n} g(x-\alpha_j),\\
R_3(x) &= \prod_{j=1}^{n} g(x\alpha_j), & R_4(x) &= \prod_{j=1}^{n} \alpha_j^m g(x\alpha_j^{-1})
\end{aligned}$$

принадлежат кольцу $\mathbb{Q}[x]$. Так как $\alpha = \alpha_1$, то

$$g(\beta-\alpha+\alpha_1) = g(\alpha+\beta-\alpha_1) = g(\beta\alpha^{-1}\cdot\alpha_1) = g(\alpha\beta\cdot\alpha_1^{-1}) = g(\beta) = 0,$$

и, значит, $R_1(\beta-\alpha)=0, R_2(\alpha+\beta)=0, R_3(\beta/\alpha)=0$ и $R_4(\alpha\beta)=0$. Таким образом, каждое из чисел $\beta-\alpha$, $\alpha+\beta$, $\beta/\alpha$ и $\alpha\beta$ есть корень многочлена с рациональными коэффициентами. Поэтому все они – алгебраические числа. Теорема 9.1 доказана. □

Пусть $\xi_1, \ldots, \xi_m$ – алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа $\xi_i$, 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 9.1 следует, что все его элементы являются алгебраическими числами.

Рассмотрим сначала структуру таких полей в случае $m = 1$, т.е. когда они порождаются одним числом.

**Лемма 9.3.** *Пусть $\xi$ алгебраическое число степени $n$. Тогда каждый элемент $\alpha$ поля $\mathbb{Q}(\xi)$ единственным образом представляется в виде*

$$\alpha = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \qquad r_j \in \mathbb{Q}. \tag{9.3}$$

*Доказательство.* Пусть $p(x)$ – минимальный многочлен $\xi$. Согласно определению каждый элемент $\alpha \in \mathbb{Q}(\xi)$ может быть представлен в виде $\alpha = \frac{A(\xi)}{B(\xi)}$, где $A(x), B(x) \in \mathbb{Q}[x]$, причем $B(\xi) \neq 0$. Многочлен $p(x)$ неприводим, поэтому возможны два случая. Либо $B(x)$ делится на $p(x)$, либо эти многочлены взаимно просты. Если $p(x)$ – делитель $B(x)$, то каждый корень $p(x)$ и, в частности, $\xi$, должен быть корнем многочлена $B(x)$. Но это неверно. Значит многочлены $p(x)$ и $B(x)$ взаимно просты. В этом случае можно утверждать, подобно теореме 1.5, что существуют многочлены $u(x), v(x) \in \mathbb{Q}[x]$, для которых выполняется равенство $u(x)p(x) + v(x)B(x) = 1$. Подставляя в него $x = \xi$ и пользуясь тем, что $p(\xi) = 0$, находим $v(\xi)B(\xi) = 1$ и, следовательно, $\alpha = A(\xi)v(\xi)$.

Разделим теперь многочлен $A(x)v(x)$ на $p(x)$ с остатком, т.е. определим многочлены $q(x), r(x) \in \mathbb{Q}[x]$ условиями

$$A(x)v(x) = q(x)p(x) + r(x), \qquad \deg r(x) < \deg p(x) = n.$$

Подставляя $x = \xi$ в последнее равенство, находим $\alpha = r(\xi)$, что доказывает (9.3), поскольку многочлен $r(x)$ имеет вид $r(x) = r_0 + r_1 x + \ldots + r_{n-1}x^{n-1}$ с рациональными коэффициентами $r_j$.

Существование двух многочленов $r(x), s(x) \in \mathbb{Q}[x]$ с условиями

$$\alpha = r(\xi), \quad \alpha = s(\xi), \qquad \deg r(x) < n, \quad \deg s(x) < n,$$

означало бы, что $r(\xi) = s(\xi)$ и, согласно второму утверждению леммы 9.1, что $p(x)|(r(x) - s(x))$. Степень делимого меньше $n = \deg p(x)$, поэтому $r(x) = s(x)$. □

**Теорема 9.2.** *Всякое поле $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, может быть порождено одним числом. Другими словами, существует такое число $\theta \in E$, что $E = \mathbb{Q}(\theta)$.*

Число $\theta$, порождающее поле $E$, называется его *примитивным элементом*.

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

*Доказательство теоремы 9.2.* Докажем сначала нужное утверждение для поля, порожденного двумя алгебраическими числами, т.е. будем считать, что $E = \mathbb{Q}(\alpha, \beta)$. Пусть степени чисел $\alpha, \beta$ равны соответственно $m$ и $n$, а

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0, \qquad g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$$

– их минимальные многочлены. Корни этих многочленов, т.е. числа сопряженные с $\alpha, \beta$, обозначим $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_n$ соответственно. При этом будем считать $\alpha = \alpha_1$, $\beta = \beta_1$. Все числа $\alpha_i$, равно как и числа $\beta_j$, различны между собой.

Выберем $c \in \mathbb{Q}$ так, чтобы

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1, \qquad \text{при} \qquad (i,k) \neq (1,1). \tag{9.4}$$

Это, очевидно, можно сделать, ведь каждое уравнение $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ при $(i,k) \neq (1,1)$ имеет не более одного решения, а поле $\mathbb{Q}$ бесконечно.

Положим $\theta = \alpha + c\beta$ и обозначим $L = \mathbb{Q}(\theta)$. Справедливо включение $L \subset \mathbb{Q}(\alpha, \beta)$. В дальнейших рассуждениях будет использоваться многочлен

$$h(x) = f(\theta - cx) \in L[x].$$

Принадлежащие кольцу $L[x]$ многочлены $g(x)$ и $h(x)$ имеют общий корень $\beta$, ведь $h(\beta) = f(\theta - c\beta) = f(\alpha) = 0$. Если $d(x)$ – их наибольший общий делитель, то как и в случае теоремы 1.5 можно утверждать, что с некоторыми многочленами $u(x), v(x) \in L[x]$ выполняется равенство $g(x)u(x) + h(x)v(x) = d(x)$. Из этого равенства следует, что число $\beta$ является корнем многочлена $d(x) \in L[x]$.

Так как $d(x)$ – делитель неприводимого над полем $\mathbb{Q}$ многочлена $g(x)$, то $d(x)$ не имеет кратных корней. Предположим, что $\deg d(x) > 1$. Тогда многочлен $d(x)$ имеет корень $\gamma$, отличный от $\beta$. Все корни $d(x)$ содержатся среди корней многочлена $g(x)$. Поэтому $\gamma = \beta_k$ с некоторым номером $k > 1$. Учитывая, что $\gamma$ является также корнем многочлена $h(x)$, т.е. $0 = h(\gamma) = f(\theta - c\gamma)$, заключаем, что $\theta - c\gamma = \alpha_i$ с некоторым номером $i$. Но тогда $\theta = \alpha_i + c\beta_k$ вопреки (9.4).

Получившееся противоречие доказывает, что $\deg d(x) = 1$, т.е. $d(x) = ax + b \in L[x]$. Но тогда $\beta = -b/a \in L$ и $\alpha = \theta - c\beta \in L$. Следовательно, $\mathbb{Q}(\alpha, \beta) = L = \mathbb{Q}(\theta)$, чем и завершается доказательство теоремы 9.2 для полей, порожденных двумя числами.

Пусть теперь $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$. Если считать теорему доказанной для полей, порожденных $m-1$ числом, то $\mathbb{Q}(\xi_1, \ldots, \xi_{m-1}) = \mathbb{Q}(\eta)$

для некоторого алгебраического числа $\eta$. Так что $E = \mathbb{Q}(\eta, \xi_m)$. Пользуясь уже доказанным утверждением для полей, порожденных двумя числами, заключаем, что с некоторым $\theta \in E$ будет выполняться равенство $E = \mathbb{Q}(\theta)$. □

**Теорема 9.3.** *Если число $\xi$ – корень многочлена*

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

*с алгебраическими коэффициентами $\alpha_i$, то $\xi$ – 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.

*Доказательство.* Не уменьшая общности можно считать, что $\alpha_m = 1$. Ведь после деления многочлена $\varphi(x)$ на ненулевой старший коэффициент $\alpha_m$ получится многочлен со старшим коэффициентом 1 и остальными коэффициентами – алгебраическими числами, также обращающийся в нуль в точке $\xi$. Согласно теореме о примитивном элементе для некоторого алгебраического числа $\theta$ выполняется равенство $E = \mathbb{Q}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \mathbb{Q}(\theta)$. Обозначим $n = \deg \theta$. По лемме 9.3 существуют такие многочлены $a_j(x) \in \mathbb{Q}[x]$, $0 \leq j < m$, что $\deg a_j(x) < n$ и $\alpha_j = a_j(\theta)$.

Пусть $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ – числа, сопряженные с $\theta$. Обозначим

$$P(x, y) = x^m + a_{m-1}(y)x^{m-1} + \ldots + a_1(y)x + a_0(y) \in \mathbb{Q}[x, y]$$

и

$$R(x) = \prod_{j=1}^{n} P(x, \theta_j).$$

Так как $P(\xi, \theta_1) = 0$, то $R(\xi) = 0$ и, согласно лемме 9.2, $R(x) \in \mathbb{Q}[x]$. Следовательно, $\xi$ – алгебраическое число. □

## 9.2 Приближения алгебраических чисел рациональными. Существование трансцендентных чисел

Множество действительных чисел не исчерпывается только алгебраическими числами. Не алгебраические числа Лейбниц назвал *трансцендентными*. Итак, трансцендентным называется всякое число, которое неспособно удовлетворить никакому алгебраическому уравнению с целыми коэффициентами, т.е. не является корнем никакого многочлена с целыми коэффициентами.

Строгое доказательство существования трансцендентных чисел впервые было дано в 1844г. Лиувиллем. Он установил, что алгебраические числа не допускают слишком хороших приближений рациональными, и это свойство позволило ему построить первые примеры трансцендентных чисел.

Если $\alpha$ – комплексное алгебраическое число, то для любого рационального числа $\frac{p}{q}$ выполняется неравенство $\left|\alpha - \frac{p}{q}\right| \geq |\operatorname{Im}\alpha|$ и ясно, что к числу $\alpha$ из $\mathbb{C} \setminus \mathbb{R}$ нельзя приблизиться рациональным на расстояние меньшее $|\operatorname{Im}\alpha|$. Поэтому далее речь пойдет о рациональных приближениях действительных алгебраических чисел. Следующая теорема о том, что действительные алгебраические числа «плохо» приближаются рациональными была доказана в 1840г. Лиувиллем.

**Теорема 9.4.** *Пусть $\alpha$ – действительное алгебраическое число степени $n \geq 2$. Тогда найдётся константа $c > 0$, зависящая только от $\alpha$, такая, что для любого рационального числа $\frac{p}{q}$, $q > 0$, выполняется неравенство*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}. \tag{9.5}$$

*Доказательство.* Пусть $f(x) \in \mathbb{Q}[x]$ – минимальный многочлен числа $\alpha$ и $d$ – общий знаменатель его коэффициентов. Пусть также $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ – числа, сопряженные с $\alpha$. По лемме 9.1 многочлен $f(x)$ неприводим. Поскольку степень его $n$ не меньше 2, то $f(x)$

не имеет рациональных корней и, значит, $dq^n f(p/q)$ целое отличное от нуля число. Но тогда $dq^n|f(p/q)| \geq 1$. Рассмотрим теперь два случая:

1) Пусть $\left|\alpha - \frac{p}{q}\right| \leq 1$. Тогда

$$\left|\alpha_j - \frac{p}{q}\right| \leq |\alpha_j - \alpha| + \left|\alpha - \frac{p}{q}\right| \leq |\alpha - \alpha_j| + 1, \quad j = 2, \ldots, n.$$

Из этих неравенств следует

$$1 \leq dq^n \left|f(p/q)\right| = dq^n \left|\alpha - \frac{p}{q}\right| \cdot \prod_{j=2}^{n} \left|\alpha_j - \frac{p}{q}\right| \leq$$

$$\leq dq^n \left|\alpha - \frac{p}{q}\right| \cdot \prod_{j=2}^{n} \left(|\alpha - \alpha_j| + 1\right).$$

Обозначив $c = d^{-1} \prod_{j=2}^{n} \left(|\alpha - \alpha_j| + 1\right)^{-1}$, получаем отсюда нужное неравенство.

2) В случае $\left|\alpha - \frac{p}{q}\right| > 1$ можно взять ту же константу $c$, что и в первом случае. Она, очевидно, удовлетворяет неравенству $c < 1$, поэтому

$$\left|\alpha - \frac{p}{q}\right| > 1 \geq \frac{1}{q^n} > \frac{c}{q^n}.$$

□

**Следствие 9.1.** *Если $\alpha \in \mathbb{R}$ и для любого $m \geq 2$ неравенство $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$ имеет бесконечно много решений $\frac{p}{q} \in \mathbb{Q}$, то $\alpha$ трансцендентно.*

*Доказательство.* 1) Докажем сначала, что $\alpha \notin \mathbb{Q}$. Предположим, что это не так, и $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 0$. Возьмём $m = 2$. По условию существует бесконечно много рациональных чисел $p/q$, удовлетворяющих неравенствам $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. Среди них есть, конечно,

решения со сколь угодно большими знаменателями $q$. С другой стороны,

$$\left|\frac{a}{b}-\frac{p}{q}\right| = \left|\frac{aq-bp}{bq}\right| \geq \frac{1}{bq}.$$

Сопоставляя полученные неравенства, заключаем, что $\frac{1}{q^2} > \frac{1}{bq}$ и, значит, $q < b$. Получившееся противоречие доказывает иррациональность $\alpha$.

2) Докажем, что $\alpha$ не есть алгебраическое число степени большей, чем 1. Предположим противное, и пусть $\deg \alpha = n \geq 2$. Положим $m = n + 1$. По условию следствия существует бесконечно много рациональных чисел $\frac{p}{q}$, удовлетворяющих неравенствам $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$. А с другой стороны по теореме 9.4 с некоторой константой $c > 0$, не зависящей от $p$ и $q$, должно выполняться неравенство $\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}$. Сопоставляя эти неравенства, получаем: $\frac{c}{q^n} < \frac{1}{q^{n+1}}$. Но тогда $q < \frac{1}{c}$ вопреки бесконечности множества рациональных решений неравенства из условия следствия. □

Укажем теперь конкретное трансцендентное число.

**Следствие 9.2.** *Число $\alpha$, определенное рядом*

$$\alpha = \sum_{k=0}^{\infty} 2^{-k!},$$

*трансцендентно.*

Члены этого ряда "быстро"стремятся к нулю, а общий знаменатель первых $n$ членов этого ряда растет "не очень быстро". Эти свойства позволяют построить последовательность хороших рациональных приближений к числу $\alpha$, что обеспечивает с помощью следствия 9.1 трансцендентность $\alpha$.

*Доказательство.* Для каждого натурального $n$ определим целые числа

$$q_n = 2^{n!}, \qquad p_n = \sum_{k=0}^{n} 2^{n!-k!}.$$

Рациональное число

$$\frac{p_n}{q_n} = \sum_{k=0}^{n} 2^{-k!}$$

равно частичной сумме ряда, определяющего $\alpha$. Поскольку члены ряда положительны, то

$$\alpha - \frac{p_n}{q_n} = \sum_{k=n+1}^{\infty} 2^{-k!} > 0.$$

Учитывая, что $(k+1)! > k!$, получаем $2^{-(k+1)!}/2^{-k!} < \frac{1}{2}$ и

$$\alpha - \frac{p_n}{q_n} = \sum_{k=n+1}^{\infty} 2^{-k!} < 2^{-(n+1)!}\left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) = \\ = \frac{2}{2^{(n+1)!}} < \frac{1}{2^{n!n}} = \frac{1}{q_n^n}.$$

Из этих неравенств следует, что для любого $m \geq 2$ неравенствам

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$$

удовлетворяет бесконечное количество различных рациональных чисел $\frac{p_n}{q_n}$, $n > m$. В согласии со следствием 9.1 можно утверждать теперь, что $\alpha$ – трансцендентное число. □

Ясно, что таким способом, выбирая вместо 2 другие натуральные основания, можно построить множество примеров трансцендентных чисел. Например, выбрав ряд с членами $10^{-k!}$, получим число, записываемое в десятичной системе нулями и единицами. Причем расстояния между соседними единицами будут возрастать очень быстро. Это число также трансцендентно.

Иное доказательство существования трансцендентных чисел было предложено Г.Кантором, установившим счетность множества алгебраических чисел и несчетность множества действительных чисел. Таким образом, множество действительных чисел не может ис-

черпываться алгебраическими числами. Более того, трансцендентные числа составляют множество большей мощности, чем алгебраические. Впрочем, это рассуждение не позволяет строить примеры трансцендентных чисел.

Утверждение теоремы Лиувилля может быть представлено, как оценка снизу значения в алгебраической точке $\alpha$ многочлена первой степени

$$|q\alpha - p| > \frac{c}{q^{n-1}},$$

см. (9.5). В таком виде теорема Лиувилля допускает обобщение.

**Теорема 9.5.** *Пусть $\alpha$ – алгебраическое число степени $n \geq 1$. Тогда существует постоянная $c > 0$, зависящая только от числа $\alpha$, такая, что для любого многочлена $P(x) \in \mathbb{Z}[x]$ с условием $P(\alpha) \neq 0$ выполняется неравенство*

$$|P(\alpha)| \geq \frac{c^d}{H^{n-1}},$$

*где $d = \deg P$ и $H$ – максимум абсолютных величин коэффициентов многочлена $P$.*

Это утверждение понадобится ниже для доказательства трансцендентности $\pi$.

*Доказательство.* Пусть $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Q}[x]$ – минимальный многочлен числа $\alpha$ и $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ – корни этого многочлена, т.е. числа, сопряженные с $\alpha$. Пусть также $a \in \mathbb{Z}, a > 0$, – наименьший общий знаменатель коэффициентов $f(x)$. Тогда $aa_j \in \mathbb{Z}, 0 \leq j < m$. Согласно теореме о симметрических многочленах, примененной для симметрического многочлена $P(x_1) \cdots P(x_n)$ и кольца $\mathbb{Z}$, найдется многочлен $Q(z_1, \ldots, z_n)$ с целыми коэффициентами, такой, что

$$P(x_1) \cdots P(x_n) = Q(\sigma_1, \ldots, \sigma_n), \tag{9.6}$$

причем $\deg Q \le n \deg P = nd$. Подставляя в тождество (9.6) числа $\alpha_1, \ldots, \alpha_n$ вместо переменных $x_1, \ldots, x_n$ соответственно, и пользуясь теоремой Виета, найдем

$$P(\alpha_1) \cdots P(\alpha_n) = Q(-a_{n-1}, \ldots, (-1)^n a_0). \tag{9.7}$$

Учитывая, что степень многочлена $Q(z_1, \ldots, z_n)$ по совокупности переменных не превосходит $nd$, а коэффициенты его – целые числа, заключаем, что $A = a^{nd} Q(-a_{n-1}, \ldots, (-1)^n a_0)$ есть целое число.

Если $A = 0$, то в силу (9.7) для некоторого индекса $j$ должно выполняться равенство $P(\alpha_j) = 0$. С помощью леммы 9.1 заключаем, что $f(x)$ есть минимальный многочлен числа $\alpha_j$ и $f(x)|P(x)$. Но тогда $P(\alpha) = 0$, вопреки условию теоремы. Таким образом $A \neq 0$. Целое отличное от нуля число не может быть по абсолютной величине меньше единицы, поэтому выполняется неравенство $|A| \ge 1$ или

$$a^{nd} \prod_{j=1}^{n} |P(\alpha_j)| \ge 1. \tag{9.8}$$

Так как коэффициенты многочлена $P(x)$ не превосходят $H$, а степень его равна $d$, имеем неравенства

$$|P(\alpha_j)| \le H(1 + |\alpha_j| + |\alpha_j|^2 + \ldots + |\alpha_j|^d) \le H(1 + |\alpha_j|)^d.$$

Теперь из (9.8) следует

$$1 \le a^{nd} |P(\alpha)| H^{n-1} \prod_{j=2}^{n} (1 + |\alpha_j|)^d.$$

Выбрав $c = a^{-n} \prod_{j=2}^{n} (1 + |\alpha_j|)^{-1}$, получаем отсюда неравенство теоремы 9.5. □

## 9.3 Иррациональность чисел $e^r$ и $\pi$

Иррациональность числа $e$ следует из бесконечности цепной дроби этого числа. Иное доказательство, найденное значительно позже,

использует представление

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}.$$

Допустим, что $e$ рационально и с целыми положительными числами $a, b$ выполняется равенство $e = \frac{a}{b}$. Тогда, определив целые числа

$$q = b!, \qquad p = \sum_{n=0}^{b} \frac{b!}{n!}\,,$$

находим $qe - p = a(b-1)! - p \in \mathbb{Z}$ и

$$qe - p = b! \sum_{n=b+1}^{\infty} \frac{1}{n!} > 0\,.$$

При $n > b+1$ выполняется неравенство $\dfrac{n!}{(b+1)!} = n \cdot \ldots \cdot (b+2) > 2^{n-b-1}$. Поэтому $\dfrac{1}{n!} < \dfrac{2^{-n+b+1}}{(b+1)!}$ и

$$qe - p = b! \sum_{n=b+1}^{\infty} \frac{1}{n!} < \frac{b!}{(b+1)!}\left(1 + \frac{1}{2} + \frac{1}{4} + \ldots\right) = \frac{2}{b+1} \leq 1.$$

Но целое число $qe - p$ не может принадлежать интервалу $0 < x < 1$. Получившееся противоречие доказывает иррациональность $e$.

Легко видеть, что подобные рассуждения не позволяют доказать, например, иррациональность $e^2$. Они должны быть несколько уточнены. Для дальнейшего понадобится одна конструкция, основанная на классическом разложении

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}\,. \tag{9.9}$$

**Лемма 9.4.** *Для каждого целого $n \geq 0$ существуют такие многочлены с целыми коэффициентами*

$$Q(x) = x^n + \ldots \qquad \text{и} \qquad P(x) = (-1)^n x^n + \ldots, \tag{9.10}$$

*что*

$$R(x) = Q(x)e^x - P(x) = \sum_{k=2n+1}^{\infty} \frac{(k-n-1)!}{(k-2n-1)!k!}\, x^k. \tag{9.11}$$

*При этом для каждого комплексного числа $z$ выполняется неравенство*

$$|R(z)| \leq \frac{|z|^{2n+1}}{n!} e^{|z|}. \tag{9.12}$$

Правая часть неравенства (9.12) с ростом $n$ достаточно быстро стремится к нулю. Поэтому, например, при $z = a \in \mathbb{Z}$ целые числа $P(a), Q(a)$ могут служить числителем и знаменателем хорошего рационального приближения к $e^a$.

*Доказательство.* Определим дифференциальный оператор $\delta = x\frac{d}{dx}$ и для каждого многочлена $T(x) = a_n x^n + \ldots + a_1 x + a_0$ будем обозначать символом $T(\delta)$ дифференциальный оператор

$$T(\delta) = a_n \delta^n + \ldots + a_1 \delta + a_0,$$

действующий на функцию $f(x)$ по правилу

$$T(\delta)f(x) = a_n \delta^n f(x) + \ldots + a_1 \delta f(x) + a_0 f(x).$$

Здесь $\delta^k f(x) = \delta(\delta^{k-1} f(x))$ при $k \geq 1$.

Выясним, как оператор $\delta$ действует на степени переменной $x$ и функцию $e^x$. Для любого натурального $r$ имеем $\delta^k x^r = r^k x^r$ и, значит, для любого многочлена $T(x)$ выполняется равенство $T(\delta)x^r = T(r)x^r$.

Докажем, что для каждого целого $k \geq 0$ выполняется равенство

$$\delta^k e^x = A_k(x)e^x, \quad \text{где} \quad A_k(x) \in \mathbb{Z}[x], \quad \deg A_k(x) = k, \tag{9.13}$$

причем коэффициент при $x^k$ в многочлене $A_k(x)$ равен 1. Утверждение легко доказывается с помощью индукции по $k$. При $k = 0$ оно, очевидно, выполняется. Предположим, что $k \geq 1$ и выполняется равенство $\delta^{k-1}e^x = A_{k-1}(x)e^x$ с многочленом $A_{k-1}(x)$, удовлетворяющим сформулированным выше условиям. Тогда

$$\delta^k e^x = \delta\left(\delta^{k-1}e^x\right) = \delta\left(A_{k-1}(x)e^x\right) = A_k(x)e^x,$$

где $A_k(x) = xA_{k-1}(x) + xA'_{k-1}(x)$. Из этого равенства следует справедливость (9.13), а также утверждение о старшем члене $A_k(x)$.

Выберем теперь какое-нибудь целое число $n \geq 0$ и определим многочлен $T(x)$ равенством $T(x) = \prod_{j=n+1}^{2n}(x-j) \in \mathbb{Z}[x]$. Если применить дифференциальный оператор $T(\delta)$ к обеим сторонам равенства (9.9), то по доказанному $T(\delta)e^x = Q(x)e^x$, где $Q(x)$ – многочлен степени $n$ с целыми коэффициентами, его старший коэффициент равен 1. Кроме того

$$T(\delta)e^x = \sum_{k=0}^{\infty} T(k)\frac{x^k}{k!} = P(x) + R(x),$$

где

$$P(x) = \sum_{k=0}^{n} T(k)\frac{x^k}{k!} = (-1)^n \sum_{k=0}^{n} \frac{(2n-k)!}{n!} \cdot \binom{n}{k} \cdot x^k \in \mathbb{Z}[x], \quad (9.14)$$

и $R(x) = \sum_{k=n+1}^{\infty} T(k)\frac{x^k}{k!}$. Учитывая равенства $T(k) = 0$ при $k = n+1, \ldots, 2n$, находим

$$R(x) = \sum_{k=2n+1}^{\infty} T(k)\frac{x^k}{k!} = \sum_{k=2n+1}^{\infty} \frac{(k-n-1)!}{(k-2n-1)!k!}x^k.$$

При $k \geq 2n+1$ выполняется неравенство

$$\frac{k!}{(k-n-1)!} = (k-n)(k-n+1)\cdots k \geq n!\,,$$

поэтому при любом $z \in \mathbb{C}$ имеем

$$|R(z)| \le \frac{1}{n!} \sum_{k=2n+1}^{\infty} \frac{|z|^k}{(k-2n-1)!} = \frac{1}{n!} \sum_{\ell=0}^{\infty} \frac{|z|^{2n+1+\ell}}{\ell!} = \frac{|z|^{2n+1}}{n!} e^{|z|}.$$

Заметим также, что в силу равенства (9.14) старший член многочлена $P(x)$ имеет вид $(-1)^n x^n$. □

**Теорема 9.6.** *Для каждого рационального $r \neq 0$ число $e^r$ иррационально.*

*Доказательство.* Предположим, что $e^r \in \mathbb{Q}$ для некоторого $r = \frac{a}{b}$, где $a, b$ целые, причем $a > 0$. Тогда число $e^a = (e^r)^b$ рационально. Выберем целое $q > 0$, такое, что $q \cdot e^a = p \in \mathbb{Z}$. Согласно (9.11) и (9.12) находим теперь $0 < qR(a) < 1$ для любого достаточно большого $n$. С другой стороны равенство (9.11) влечет

$$qR(a) = q(Q(a)e^a - P(a)) = Q(a)p - P(a)q \in \mathbb{Z}.$$

Так как это противоречит неравенствам $0 < qR(a) < 1$, заключаем, что $e^r \notin \mathbb{Q}$. □

**Теорема 9.7.** *Число $\pi$ иррационально.*

*Доказательство.* Предположим, что $\pi = \frac{a}{b}$, $a, b \in \mathbb{Z}$ и обозначим $z = \pi bi = ai$. Тогда

$$R(z) = Q(ai)e^{\pi bi} - P(ai) = Q(ai)(-1)^b - P(ai) \in \mathbb{Z}[i].$$

Из неравенства (9.12), поскольку $R(z) = u + iv$ с целыми $u, v$, находим $R(z) = 0$ для всех достаточно больших $n$.

Далее используются обозначения $P_n(x) = P(x)$, $Q_n(x) = Q(x)$, $R_n(x) = R(x)$, указывающие на величину параметра $n$, при котором построена тройка $P(x), Q(x), R(x)$. Из (9.11) следует тождество

$$Q_n(x)R_{n+1}(x) - Q_{n+1}(x)R_n(x) = Q_{n+1}P_n - Q_nP_{n+1} = \Delta(x) \quad (9.15)$$

а также неравенство $\operatorname{ord}_{x=0}\Delta(x) \geq 2n+1$, означающее, что разложение многочлена $\Delta(x)$ в ряд Тейлора в окрестности точки $x=0$ начинается по крайней мере со степени $x^{2n+1}$, и оценка $\deg\Delta(x) \leq 2n+1$. Но это возможно лишь в случае $\Delta(x) = \gamma x^{2n+1}$ с некоторой постоянной $\gamma$. Сравнивая при помощи (9.10) старшие коэффициенты в равенстве (9.15), находим $\Delta(x) = 2(-1)^n x^{2n+1}$ и $\Delta(z) \neq 0$, вопреки равенству (9.15) и $R_n(z) = R_{n+1}(z) = 0$. □

## 9.4 Трансцендентность числа $e$

Важной частью доказательства иррациональности чисел вида $e^r$, $r \in \mathbb{Q}$, $r \neq 0$, является конструкция рациональных приближений к этим числам.

В 1873г. Ш. Эрмит предложил при любом $m \in \mathbb{Z}, m > 0$ аналитическую конструкцию целых чисел $b_0, b_1, \ldots, b_m$ таких, что все разности $b_0 e^k - b_k$, $1 \leq k \leq m$, близки к нулю, так называемых совместных приближений. На этой основе он доказал следующую теорему.

**Теорема 9.8.** *Число $e$ трансцендентно.*

В основе конструкции Эрмита лежит тождество

$$\int_0^x e^{-t} f(t)dt = F(0) - F(x)e^{-x}, \tag{9.16}$$

справедливое для любого многочлена $f(x) \in \mathbb{C}[x]$, при

$$F(x) = \sum_{k=0}^{M} f^{(k)}(x), \quad M = \deg f(x), \tag{9.17}$$

и легко доказываемое, например, с помощью дифференцирования (9.16). Действительно, производная левой части равна $e^{-x}f(x)$. А для производной правой части находим

$$\big(F(0) - e^{-x}F(x)\big)' = e^{-x}(F(x) - F'(x)) = e^{-x}f(x).$$

Совпадение производных означает, что разность левой и правой частей (9.16) есть константа. Учитывая, что обе эти функции обращаются в нуль при $x = 0$, заключаем, что они равны.

*Доказательство теоремы 9.8.* Предположим, что $e$ – алгебраическое число. Тогда при некотором натуральном $m$ и с некоторыми целыми коэффициентами $a_0, \ldots, a_m$ выполняется равенство

$$a_m e^m + \ldots + a_1 e + a_0 = 0, \quad a_m > 0. \tag{9.18}$$

Пусть $n$ - натуральное число, впоследствии достаточно большое. Выберем многочлен

$$f(x) = x^{n+r_0}(x-1)^{n+r_1} \cdots (x-m)^{n+r_m},$$

где каждый из параметров $r_0, \ldots, r_m$ в дальнейшем будет выбран равным 0 или 1.

Для любых двух натуральных чисел $k, \ell$ справедливо равенство

$$(x^k)^{(\ell)} = \begin{cases} 0\,, & \text{если} \quad \ell > k \\ \ell! \binom{k}{\ell} x^{k-\ell}\,, & \text{если} \quad \ell \le k. \end{cases} \tag{9.19}$$

Многочлен $f(x)$ имеет целые коэффициенты. Поэтому из (9.19) следует, что коэффициенты многочлена $f^{(\ell)}(x)$ делятся на $\ell!$.

В силу выбора $f(x)$ обладает также свойством

$$f^{(\ell)}(0) = f^{(\ell)}(1) = \ldots = f^{(\ell)}(m) = 0, \quad 0 \le \ell < n,$$

Поэтому при любом $k = 0, 1, 2, \ldots, m$ для многочлена $F(x)$, определенного равенством (9.17), находим

$$F(k) = \sum_{\ell=0}^{M} f^{(\ell)}(k) = \sum_{\ell=n}^{M} f^{(\ell)}(k) = n! b_k,$$

где $b_k$ - целые числа. Из тождества (9.16) при $x = k$ находим

$$b_0 e^k - b_k = \frac{e^k}{n!} \int_0^k e^{-t} f(t) dt. \tag{9.20}$$

Многочлен $f(x)$ есть произведение $\sum_{i=0}^{m}(n+r_i) \leq (m+1)(n+1)$ скобок вида $x-k$, каждая из которых на отрезке $[0,m]$ не превосходит $m$. Поэтому

$$\max_{0\leq x\leq m} |f(x)| \leq c^{n+1}, \qquad c = m^{m+1}. \tag{9.21}$$

Теперь из (9.20) и (9.21) следуют равенства

$$b_0 e^k - b_k = O\left(\frac{c^n}{n!}\right), \quad k = 0, 1, \ldots, m. \tag{9.22}$$

Умножим равенство (9.20) на $a_k$ и просуммируем получившиеся произведения при всех $k = 0, 1, \ldots, m$. В силу (9.18) находим

$$I = a_0 b_0 + \ldots + a_m b_m = -\sum_{k=0}^{m} a_k \frac{e^k}{n!} \int_0^k e^{-t} f(t) dt. \tag{9.23}$$

Равенства (9.22) означают, что

$$I = O\left(\frac{c^n}{n!}\right). \tag{9.24}$$

Определим функции

$$u_k(x) = \begin{cases} 1, & \text{если } x \leq k, \\ 0, & \text{если } x > k, \end{cases}.$$

Тогда равенство (9.23) можно переписать в виде

$$I = -\sum_{k=0}^{m} a_k \frac{e^k}{n!} \int_0^m e^{-t} f(t) u_k(x) dt = -\int_0^m e^{-t} f(t) G(t) dt, \tag{9.25}$$

где

$$G(t) = \frac{1}{n!} \sum_{k=0}^{m} a_k e^k u_k(t).$$

На промежутке $0 < x \leq m$ имеем $G(x) = \frac{1}{n!} a_m e^m > 0$, так что функция $G(x)$ отлична от тождественного нуля. Функция $G(t)$ постоянна

на интервалах между целыми точками. Поэтому она может менять знак лишь при переходе переменной $x$ через целые точки. Выберем теперь показатели $r_1, \ldots, r_{m-1}$, равными 0 или 1 так, чтобы функции $G(t)$ и $f(t)$ при переходе через каждую целую точку $1, \ldots, m-1$ одновременно меняли бы знак или сохраняли его. Параметры $r_0$ и $r_m$ можно взять, например, равными нулю. Тогда под интегралом в правой части равенства (9.25) стоит знакопостоянная функция, что обеспечивает условие $I \neq 0$.

Итак, $I = a_0 b_0 + \ldots + a_m b_m$ есть целое отличное от нуля число, которое в силу (9.24) меньше 1 при достаточно большом $n$. Получившееся противоречие завершает доказательство теоремы 9.8. $\square$

## 9.5 Трансцендентность числа $\pi$

В этом параграфе будет доказана следующая теорема.

**Теорема 9.9.** *Число $\pi$ трансцендентно.*

Начнем с некоторой задачи, относящейся к теории приближения функций. Предположим, что на интервале $(a; b)$ определена функция $f(x)$ и нам известны ее значения в некоторых точках $\alpha_0, \ldots, \alpha_m$ этого интервала. Требуется найти многочлен $P(x)$ по возможности меньшей степени, принимающий в заданных точках $\alpha_j$ те же значения, что и функция $f(x)$. Если количество точек $m$ достаточно велико, а функция достаточно гладкая, значения этого многочлена, называемого интерполяционным, будут близки к значениям функции $f(x)$ и в других точках интервала $(a; b)$. Для решения этой задачи определим многочлены

$$Q(x) = (x - \alpha_0) \cdots (x - \alpha_m), \qquad Q_k(x) = \frac{Q(x)}{x - \alpha_k}, \quad k = 0, \ldots, m,$$

и будем искать многочлен $P(x)$ в виде

$$P(x) = \sum_{k=0}^{m} b_k Q_k(x)$$

с некоторыми постоянными $b_k$, подобрав их так, чтобы выполнялись нужные равенства значений. Учитывая, что при $k \neq j$ выполняется $Q_k(\alpha_j) = 0$, получаем $b_j Q_j(\alpha_j) = P(\alpha_j) = f(\alpha_j)$, $j = 0, 1, \ldots, m$ и, следовательно,

$$P(x) = \sum_{k=0}^{m} \frac{f(\alpha_k)}{Q_k(\alpha_k)} \cdot Q_k(x).$$

Построенный многочлен удовлетворяет условиям

$$P(\alpha_j) = f(\alpha_j), \qquad j = 0, \ldots, m,$$

и, значит, является интерполяционным многочленом.

Для доказательства трансцендентности $\pi$ нам понадобится решить сначала более сложную интерполяционную задачу, в которой требуется совпадение не только значений искомого многочлена со значениями заданной функции, но и совпадение их производных до некоторых порядков. Конструкция этого интерполяционного многочлена задается следующей леммой.

**Лемма 9.5.** *Пусть $\alpha_0, \alpha_1, \ldots, \alpha_m$ – различные числа из интервала $(a; b)$ и $r_0, r_1, \ldots, r_m$ – неотрицательные целые числа. Положим $N = -1 + \sum_{j=0}^{r_m}(r_j + 1)$ и определим многочлены*

$$Q(x) = \prod_{j=0}^{m} (x - \alpha_j)^{r_j+1}, \qquad Q_k(x) = \frac{Q(x)}{(x - \alpha_k)^{r_k+1}}\ , \quad k = 0, 1, \ldots, m.$$

*Пусть также $f(x)$ – функция $N$ раз дифференцируемая в $(a; b)$. Тогда многочлен*

$$P(x) = \sum_{j=0}^{m} Q_j(x) R_j(x), \tag{9.26}$$

*где*

$$R_j(x) = \sum_{i=0}^{r_j} \frac{1}{i!} \left(\frac{d}{dt}\right)^i \left(\frac{f(t)}{Q_j(t)}\right)_{t=\alpha_j} (x - \alpha_j)^i,$$

*имеет степень не выше $N$ и удовлетворяет равенствам*

$$P^{(\ell)}(\alpha_k) = f^{(\ell)}(\alpha_k), \qquad 0 \leq \ell \leq r_k, \quad 0 \leq k \leq m. \tag{9.27}$$

*Доказательство.* Так как $\deg Q_k(x) = N - r_k$, $\deg R_k(x) \le r_k$, и эти неравенства справедливы при любом $k = 0, 1, \ldots, m$, заключаем, что $\deg P(x) \le N$.

Фиксируем некоторое целое число $k, 0 \le k \le m$. Учитывая, что при $j \ne k$ многочлен $Q_j(x)$ делится на $(x - \alpha_k)^{r_k+1}$, получаем

$$P(x) = Q_k(x)R_k(x) + O((x - \alpha_k)^{r_k+1}).$$

Многочлен $R_k(x)$ определен как многочлен Тейлора в точке $x = \alpha_k$ для функции $\dfrac{f(x)}{Q_k(x)}$, поэтому

$$\frac{f(x)}{Q_k(x)} = R_k(x) + O((x - \alpha_k)^{r_k+1}),$$

и, следовательно,

$$f(x) = Q_k(x)R_k(x) + O((x - \alpha_k)^{r_k+1}).$$

Из полученных формул для $P(x)$ и $f(x)$ теперь следует, что $f(x) - P(x) = O((x - \alpha_k)^{r_k+1})$ и, следовательно, $f(x)$ и $P(x)$ имеют одинаковые производные в точке $x = \alpha_k$ до порядка $r_k$ включительно. Поскольку это заключение справедливо для любого целого $k, 0 \le k \le m$, лемма доказана. □

**Следствие 9.3.** *Существует единственный многочлен, удовлетворяющий условиям (9.27) и имеющий степень не выше $N$.*

*Доказательство.* Существование многочлена доказано в лемме 9.5. Если $A(x)$ и $B(x)$ – два многочлена степени не выше $N$, удовлетворяющие условиям (9.27), то $Q(x)|(A(x) - B(x))$. Учитывая, что $\deg Q(x) = N + 1$ и $\deg(A(x) - B(x)) \le N$, заключаем $A(x) = B(x)$. □

**Следствие 9.4.** *В условиях леммы 9.5 на интервале $(a; b)$ существует такая точка $\xi$, что*

$$\sum_{k=0}^{m} \sum_{j=0}^{r_k} \frac{f^{(r_k-j)}(\alpha_k)}{j!(r_k - j)!} \left(Q_k(t)^{-1}\right)^{(j)}_{t=\alpha_k} = \frac{f^{(N)}(\xi)}{N!}. \tag{9.28}$$

*Левая часть этого равенства есть коэффициент при $x^N$ в многочлене $P(x)$ из леммы 9.5.*

*Доказательство.* Коэффициент при $x^N$ в многочлене $P(x)$, как это следует из равенства (9.26), равен сумме старших коэффициентов многочленов $R_j(x)$, т.е. равен

$$\sum_{k=0}^{m} \frac{1}{r_k!} \left(\frac{d}{dt}\right)^{r_k} \left(\frac{f(t)}{Q_k(t)}\right)_{t=\alpha_k} = \sum_{k=0}^{m} \sum_{j=0}^{r_k} \frac{f^{(r_k-j)}(\alpha_k)}{j!(r_k-j)!} \left(Q_k(t)^{-1}\right)^{(j)}_{t=\alpha_k}.$$

Это доказывает второе утверждение следствия. Для доказательства первого утверждения заметим, что функция $F(x) = f(x) - P(x)$, в силу леммы 9.5, имеет в каждой из точек $\alpha_k \in (a;b)$ нули кратности $r_k + 1$. По теореме Ролля, примененной несколько раз, на этом интервале есть точка $\xi$ такая, что $F^{(N)}(\xi) = 0$. Из равенства $F^{(N)}(\xi) = f^{(N)}(\xi) - N!a_N$, где $a_N$ – старший коэффициент многочлена $P(x)$, получаем первое утверждение следствия. □

*Доказательство теоремы 9.9.* Допустим, что $\pi$ – алгебраическое число. Степень его обозначим буквой $m$. Тогда $m \geq 1$. Утверждения леммы 9.5 и её следствий будут применены нами к функции $f(x) = \sin \pi x$ и точкам

$$\alpha_0 = 0, \quad \alpha_1 = 1, \quad \dots \quad , \quad \alpha_m = m.$$

Пусть $N$ – произвольное натуральное число, в дальнейшем оно будет выбрано достаточно большим. Положим

$$r_j = \left[\frac{N-j}{m+1}\right], \qquad j = 0, 1, \dots, m.$$

Если $n$ – частное и $s$ – остаток от деления $N+1$ на $m+1$, т.е. $N+1 = (m+1)n + s$, $0 \leq s \leq m$, то, как легко видеть,

$$r_j = \begin{cases} n & \text{если} j < s, \\ n-1 & \text{если} j \geq s. \end{cases}, \qquad j = 0, 1, \dots, m.$$

Тогда

$$\sum_{j=0}^{m}(r_j+1) = s(n+1) + (m+1-s)n = (m+1)n + s = N+1.$$

Каждому натуральному числу $N$ поставим в соответствие многочлен $P_N(x)$, определенный леммой 9.5 при указанном выборе функции $f(x)$ и чисел $\alpha_0, \ldots, \alpha_m, r_0, \ldots, r_m$.

Если для некоторого $N$ выполняется неравенство $\deg P_{N+1} < N+1$, то по следствию 9.3 можно утверждать, что $P_{N+1}(x) = P_N(x)$. Если бы неравенства $\deg P_N(x) < N$ выполнялись для всех $N$ больших некоторого целого числа $M$, то по доказанному при любом $N > M$ имело бы место равенство $P_N(x) = P_M(x)$ и тогда, в частности,

$$(\sin \pi x)^{(\ell)}_{x=0} = P_M^{(\ell)}(0), \qquad \ell = 0, 1, 2, \ldots.$$

Так как $P_M(x)$ – многочлен, то правая часть последнего равенства равна нулю при всех достаточно больших $\ell$. С другой стороны все нечетные производные функции $\sin \pi x$ в точке 0 отличны от нуля. Получившееся противоречие означает, что существуют сколь угодно большие числа $N$, для которых $\deg P_N(x) = N$.

Выберем какое-нибудь достаточно большое целое число $N$ с условием $\deg P_N(x) = N$. Если $B$ – коэффициент при $x^N$ в многочлене $P_N(x)$, то согласно выбору $N$ выполняется $B \neq 0$. По следствию 9.4 имеем

$$B = \sum_{k=0}^{m}\sum_{j=0}^{r_k} \frac{f^{(r_k-j)}(k)}{(r_k-j)!} \cdot a_{k,j}\ , \tag{9.29}$$

где

$$a_{k,j} = \frac{1}{j!}\left(Q_k(t)^{-1}\right)^{(j)}_{t=k}, \qquad j \geq 0.$$

Справедливы равенства

$$(\sin \pi x)^{(\ell)}_{x=k} = (-1)^k \pi^\ell \sin\frac{\pi\ell}{2}\ , \tag{9.30}$$

из которых следует, что числа $f^{(r_k-j)}(k)$ в равенстве (9.29) либо равны 0, либо с точностью до знака совпадают с некоторой степенью $\pi$, причем показатель степени не превосходит числа $n$. Ниже будет показано, что $a_{k,j} \in \mathbb{Q}$, поэтому $B$ есть многочлен от $\pi$ с рациональными коэффициентами.

Из определения чисел $a_{k,j}$ следует, что

$$\frac{1}{Q_k(t)} = \sum_{j=0}^{\infty} a_{k,j} \cdot (t-k)^j. \tag{9.31}$$

Подставим в это тождество $t = k+dx$, где $d$ – некоторое натуральное, делящееся на все числа $1, 2, \ldots, m$. Например, можно взять $d = m!$. Тогда (9.31) может быть переписано в виде

$$\frac{1}{\prod\limits_{\substack{\ell=0 \\ \ell \neq k}}^{m} (k-\ell+dx)^{r_\ell+1}} = \sum_{j=0}^{\infty} a_{k,j} \cdot d^j \cdot x^j. \tag{9.32}$$

Учитывая, что

$$\frac{d}{k-\ell+dx} = \frac{d}{k-\ell} \cdot \frac{1}{1-\frac{d}{\ell-k}x} = -\sum_{i=0}^{\infty} \left(\frac{d}{\ell-k}\right)^{i+1} x^i,$$

т.е. функция $\frac{d}{k-\ell+dx}$ раскладывается в точке 0 в ряд Тейлора с целыми коэффициентами, заключаем с помощью (9.32), что ряд $d^{N-r_k} \sum\limits_{j=0}^{\infty} a_{k,j} d^j x^j$ имеет целые коэффициенты. Поэтому $d^{N-r_k+j} a_{k,j} \in \mathbb{Z}$ и, значит,

$$d^N \cdot a_{k,j} \in \mathbb{Z}, \qquad 0 \leq j \leq r_k. \tag{9.33}$$

Если $u(x) = \sum_{j=0}^{\infty} u_j x^j$ и $v(x) = \sum_{j=0}^{\infty} v_j x^j$ два степенных ряда, будем обозначать символом $u(x) << v(x)$ тот факт, что каждый коэффициент ряда $u(x)$ по абсолютной величине не превосходит соответствующего коэффициента ряда $v(x)$, т.е. $|u_j| \leq v_j$, $j = 0, 1, \ldots$ .

Так, например, при $k \neq \ell$ имеем

$$\frac{1}{k-\ell+x} = \frac{1}{k-\ell} \cdot \frac{1}{1-\frac{x}{\ell-k}} = -\sum_{j=0}^{\infty} \left(\frac{1}{\ell-k}\right)^{i+1} x^i << \frac{1}{1-x}.$$

Легко проверить, что если степенные ряды связаны соотношениями $u_1(x) << v_1(x)$ и $u_2(x) << v_2(x)$, то $u_1(x)u_2(x) << v_1(x)v_2(x)$. Для этого достаточно лишь сравнить соответствующие коэффициенты степенных рядов. С помощью индукции указанное свойство легко распространяется на любое число сомножителей.

Пользуясь этим свойством, находим

$$\sum_{j=0}^{\infty} a_{k,j} \cdot x^j = \frac{1}{\prod\limits_{\substack{\ell=0 \\ \ell\neq k}}^{m} (k-\ell+x)^{r_\ell+1}} << \frac{1}{(1-x)^{N-r_k}} =$$

$$= \sum_{j=0}^{\infty} \binom{N-r_k-1+j}{j} x^j << \sum_{j=0}^{\infty} 2^{N-r_k-1+j} x^j.$$

Таким образом,

$$|a_{k,j}| \leq 2^N, \qquad k = 0, 1, \ldots, m, \quad j = 0, 1, \ldots, r_k. \tag{9.34}$$

Из (9.29), (9.30) и (9.33) следует, что существует такой многочлен с целыми коэффициентами $A(x)$, что

$$A(\pi) = d^N n! B \neq 0, \qquad \deg A(x) \leq n.$$

При этом, согласно (9.34)

$$L(A) \leq d^N n! \sum_{k=0}^{m} (r_k+1) 2^N \leq n! c_1^{n+1},$$

где $c_1$ положительное число, зависящее только от $m$.

Так как $A(\pi) \neq 0$, а $\pi$ по предположению есть алгебраическое число степени $m$, находим с помощью теоремы 9.5 оценку снизу

$$|A(\pi)| \geq (n! c_1^{n+1})^{1-m} c_2^{-n} \geq \frac{1}{c_3^{n+1} (n!)^{m-1}}, \tag{9.35}$$

где $c_2, c_3$ – положительные числа, зависящие только от $m$.

Оценим теперь $|A(\pi)|$ сверху. Для этого воспользуемся правой частью равенства (9.28). Имеем

$$|A(\pi)| = d^N n! \frac{\left|(\sin \pi x)^{(N)}_{x=\xi}\right|}{N!} \leq d^N n! \frac{\pi^N}{N!} \ .$$

Из определения чисел $r_j$ следует неравенство $N+1 \leq (m+1)(n+1)$. Произведение $(n!)^{m+1}$ состоит из $(m+1)(n-1) \leq N-1$ сомножителей, превосходящих 1, поэтому $(n!)^{m+1} \leq N!$. В результате имеем

$$|A(\pi)| \leq \frac{c_4^{n+1}}{(n!)^m},$$

где $c_4 = (\pi d)^{m+1}$ зависит только от $m$. Сравнивая полученную оценку с (9.35), приходим к неравенству

$$\frac{1}{c_3^{n+1}(n!)^{m-1}} \leq \frac{c_4^{n+1}}{(n!)^m}$$

или

$$1 \leq \frac{(c_3 c_4)^{n+1}}{n!} \ . \tag{9.36}$$

При больших $n$ это неравенство невозможно. С другой стороны имеем $(n+1)(m+1) \geq N+1$, что противоречит выбору числа $N$ достаточно большим.

Получившееся противоречие завершает доказательство трансцендентности $\pi$. □

## 9.6 Невозможность квадратуры круга

Знаменитая проблема квадратуры круга может быть сформулирована так

*построить на плоскости квадрат, площадь которого равнялась бы площади заданного круга.*

При этом "построить"означает построить с помощью циркуля и линейки - инструментов, находившихся в распоряжении древнегреческих геометров. Многочисленные попытки найти требуемое построение продолжались в течение четырех тысячелетий до тех пор, пока в 1882г. Ф.Линдеман не доказал, что такого построения не существует. Это утверждение будет доказано ниже.

Когда говорят о построении с помощью циркуля и линейки, имеют ввиду, что по заданному условиями набору точек, отрезков, окружностей или других геометрических объектов требуется построить некоторый новый отрезок, точку, окружность и т.п., используя только эти инструменты. Причем с их помощью разрешается выполнять лишь две основные операции

1) провести с помощью линейки прямую линию через две заданные или построенные ранее точки;

2) провести циркулем окружность с центром в заданной или построенной ранее точке радиуса, равного расстоянию между двумя заданными или построенными точками.

Любая геометрическая фигура, которая может быть построена, задается совокупностью прямых, окружностей и точек. Например, для построения квадрата достаточно построить четыре его вершины. В результате выполнения в определенном порядке указанных операций на плоскости возникнет множество прямых, окружностей и некоторых точек их пересечения, содержащее искомые точки, прямые или окружности. Не все точки пересечения этих прямых и окружностей в действительности необходимы для построения. Перенумеруем теперь заданные условием точки, прямые и окружности в некотором порядке, а затем прямые, окружности и используемые для построения точки пересечения в порядке их возникновения. Тогда на чертеже появится конечная последовательность прямых, окружностей и точек, содержащая все искомые геометрические объекты. Каким же образом в процессе построения могут возникать

новые прямые, окружности и точки? Перечислим все имеющиеся возможности.

а) Новая прямая может быть построена лишь с помощью линейки, приложенной к двум, построенным ранее точкам.

б) Новая окружность может быть построена лишь с помощью циркуля, помещенного в построенную ранее точку. При этом радиус ее равен расстоянию между двумя построенными ранее точками.

в) Новая точка может быть построена, как пересечение двух построенных прямых.

г) Новая точка может быть построена, как пересечение построенных прямой и окружности.

д) Новая точка может быть построена, как пересечение двух построенных окружностей.

е) Новая точка может быть построена с помощью операции, которую мы назовем "произвольный выбор".

Поясним подробнее, что здесь имеется ввиду. Иногда, при выполнении построения бывает безразлично, где взять необходимую точку. Тогда говорят, "возьмем произвольную точку"на плоскости, на построенной ранее прямой и т.п.. Рассмотрим, например, следующую древнюю и часто возникавшую на практике задачу: *построить с помощью циркуля и линейки центр нарисованной окружности.* Ясно, что построение центра не может начаться ни с одной из перечисленных выше операций а)-д). Одно из классических решений этой задачи начинается с произвольного выбора трех точек $A, B$ и $C$ на окружности с тем, чтобы впоследствии с помощью циркуля и линейки, так как это объясняется в школьном курсе геометрии, построить центр окружности, описанной вокруг треугольника $ABC$, т.е. центр заданной окружности.

Сделав эти вступительные замечания, предположим, что существует построение с помощью циркуля и линейки, решающее проблему квадратуры круга, т.е. позволяющее для любого заданного круга построить равновеликий ему квадрат.

Введем на плоскости систему координат, поместив ее начало в центр заданного круга и выбрав в качестве единицы измерения длины радиус заданного круга. Всякая точка во введенной на плоскости системе координат может быть задана парой чисел $(x; y)$, прямая и окружность уравнениями в канонической форме, соответственно, $ax + by + c = 0$ и $(x - x_0)^2 + (y - y_0)^2 = r^2$, где $(x_0, y_0)$ - координаты центра и $r$ - радиус окружности.

Определим теперь на плоскости класс алгебраических точек, прямых и окружностей. Точку будем называть алгебраической, если ее координаты есть алгебраические числа, прямую - если она может быть задана уравнением с алгебраическими коэффициентами. Окружность будем называть алгебраической, если величина ее радиуса и координаты центра есть алгебраические числа. В частности, заданная окружность имеет уравнение $x^2+y^2 = 1$ и потому является алгебраической.

Покажем, что операции а)-д), примененные к алгебраическим объектам, в результате также дают алгебраические точки, прямые и окружности. В самом деле:

а) Прямая, проведенная через две точки с алгебраическими координатами $(x_1, y_1)$ и $(x_2, y_2)$, задается уравнением

$$(x_2 - x_1)(y - y_1) - (y_2 - y_1)(x - x_1) = 0.$$

Согласно теореме 2 это уравнение в канонической форме имеет алгебраические коэффициенты и потому определяет алгебраическую прямую.

б) Окружность с алгебраическим центром, радиус которой есть алгебраическое число, по определению является алгебраической.

в) Две пересекающиеся прямые, задаваемые уравнениями $a_i x + b_i y + c_i = 0, i = 1, 2$, с алгебраическими коэффициентами $a_i, b_i, c_i$

имеют общую точку с координатами, удовлетворяющими системе уравнений

$$\begin{cases} a_1x + b_1y = c_1, \\ a_2x + b_2y + c_2. \end{cases}$$

Решение этой системы, найденное, например, по формулам Крамера, имеет согласно теореме 2 алгебраические координаты $x, y$. Так что точка пересечения двух алгебраических прямых является алгебраической.

г) Точки пересечения алгебраических прямой и окружности имеют координаты $x, y$, удовлетворяющие системе уравнений

$$\begin{cases} ax + by = c, \\ (x - x_0)^2 + (y - y_0)^2 = r^2, \end{cases}$$

с алгебраическими коэффициентами. Не уменьшая общности можно считать, что $b \neq 0$. Выразив из первого уравнения системы неизвестную $y$ через $x$ и подставив это выражение вместо $y$ во второе уравнение, получим квадратное уравнение относительно $x$, коэффициенты которого согласно теореме 2 будут алгебраическими числами. Но тогда по этой же теореме алгебраическими числами будут оба корня $x_1$ и $x_2$ получившегося квадратного уравнения, а, следовательно, и вторые кординаты $y_i = -(ax_i + c) \cdot b^{-1}$ точек пересечения. Итак, обе точки пересечения $(x_1, y_1)$ и $(x_2, y_2)$ будут алгебраическими.

д) Координаты $x, y$ точек пересечения двух алгебраических окружностей удовлетворяют системе уравнений

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = r_1^2, \\ (x - x_2)^2 + (y - y_2)^2 = r_2^2, \end{cases}$$

с алгебраическими коэффициентами. Вычитая второе уравнение системы из первого, мы, как легко проверить, получим линейное уравнение с алгебраическими коэффициентами. А затем, как и в предыдущем случае, проверяем, что координаты точек пересечения есть алгебраические числа. Этим доказано, что точки пересечения двух алгебраических окружностей будут алгебраическими.

Обсудим теперь ситуацию с операцией е) - "произвольный выбор". Заметим, что точки с алгебраическими (и даже рациональными) координатами всюду плотны на плоскости. Это означает, что сколь угодно близко к любой точке плоскости находятся точки с алгебраическими координатами. Кроме того, согласно теореме 2 они будут всюду плотны на алгебраических прямых и окружностях. Действительно, в любой окрестности точки $(x_1, y_1)$, лежащей, например, на алгебраической окружности, найдется точка $(x_2, y_2)$ с абсциссой $x_2$ - рациональным числом, принадлежащая этой же окружности. Но тогда вторая координата $y_2$ должна быть алгебраическим числом, так что точка $(x_2, y_2)$ будет алгебраической.

Это означает, что если все точки, прямые и окружности, получившиеся в результате операций, предшествовавших "произвольному выбору", были алгебраическими, то и при "произвольном выборе"мы можем построить алгебраическую точку.

Сказанное выше можно резюмировать так. Построение с помощью циркуля и линейки, реализующее квадратуру алгебраического круга $x^2 + y^2 = 1$, может быть выполнено таким образом, что все встречающиеся в нем точки, прямые и окружности будут алгебраическими. В частности, это означает, что алгебраическими будут и все вершины квадрата, получающегося в конце построения, и равновеликого по площади заданному кругу.

Если $(x_1, y_1), (x_2, y_2)$ - соседние вершины квадрата, то его площадь, как легко видеть, равна $(x_2 - x_1)^2 + (y_2 - y_1)^2$ и является алгебраическим числом. Но эта же площадь по условию должна равняться площади заданного круга, т.е. числу $\pi$.

Таким образом, получается противоречие с теоремой Линдемана о трансцендентности числа $\pi$, означающее, что квадратура круга с помощью циркуля и линейки невозможна.

# Литература


[1] Арнольд И.В., Теория чисел, М., Учпедгиз, 1939

[2] Боревич З.И., Шафаревич И.Р., Теория чисел, М., Наука, 1985

[3] Бухштаб А.А., Теория чисел, М., Просвещение, 1966

[4] Венков Б.А., Элементарная теория чисел, ОНТИ НКТП СССР, Москва, Ленинград, 1937

[5] Виноградов И.М., Основы теории чисел, М., Наука, 1981

[6] Гаусс К.Ф. Труды по теории чисел, М., Изд-во АН СССР, 1959

[7] Граве Д.А., Элементарный курс теории чисел, Киев, Университет Св. Владимира, 1913

[8] Диксон Л.Е., Введение в теорию чисел, Тбилиси, 1941.

[9] Диофант, Арифметика, М., Наука, 1974

[10] Егоров Д.Ф., Элементы теории чисел, Госиздательство, Москва-Петроград, 1923

[11] Лежен Дирихле Г.П., Лекции по теории чисел, ОНТИ НКТП СССР, Москва-Ленинград, 1936

[12] Ожигова Е.П., Развитие теории чисел в России, Наука, Ленинград, 1972

[13] Сушкевич А.К., Теория чисел, Изд-во Харьковского Университета, 1956

[14] Чебышев П.Л., Теория сравнений, Полное собрание сочинений, т.1, Изд. АН СССР, Москва, Ленинград, 1946

[15] Ферма П., Исследования по теории чисел и диофантову анализу, М., Наука, 1992

[16] Шидловский А.Б., Диофантовы приближения и трансцендентные числа, М., Физматлит, 2007

[17] Dickson L.E., History of theory of numbers, Washington, I 1919, II 1920, III 1923.