Высшее профессиональное образование

БАКАЛАВРИАТ

О. Н. ГЕРМАН, Ю. В. НЕСТЕРЕНКО

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Учебник
для студентов учреждений
высшего профессионального образования,
обучающихся по направлениям подготовки
«Информационная безопасность»
и «Математика»

ACADEMIA

Москва
Издательский центр «Академия»
2012

УДК 003.26(075.8)
ББК 81.2-8я73
Г 38

Рецензенты:
д-р физ.-мат. наук, проф., действительный член Академии криптографии РФ *М. М. Глухов*;
канд. техн. наук, доц. *А. Б. Лось* (зав. кафедрой «Информационная безопасность» факультета прикладной математики Московского института электронного машиностроения)

Герман О. Н.

Г38 Теоретико-числовые методы в криптографии : учебник для студ. учреждений высш. проф. образования / О. Н. Герман, Ю. В. Нестеренко. — М. : Издательский центр «Академия», 2012. — 272 с. — (Сер. Бакалавриат).

ISBN 978-5-7695-6786-5

Учебник создан в соответствии с Федеральным государственным образовательным стандартом по направлениям подготовки «Информационная безопасность» и «Математика» (квалификация «бакалавр»).

В учебнике описаны элементы теории чисел, быстрые алгоритмы решения ряда важных задач с числами (возведение в степень, вычисление символов Лежандра, отсеивание составных чисел и др.) и многочленами над конечными полями (разложение на множители и нахождение корней); алгоритмы проверки чисел на простоту, разложения чисел на множители, дискретного логарифмирования, построения приведенного базиса решетки; даны также криптографические приложения теоретико-числовых алгоритмов (криптосхема RSA, открытое распределение ключей, электронная цифровая подпись, криптосхемы, основанные на теории решеток).

Для студентов учреждений высшего профессионального образования. Может быть полезен студентам других специальностей, связанных с информационной безопасностью, а также всем, кто интересуется алгоритмическими и прикладными аспектами теории чисел.

УДК 003.26(075.8)
ББК 81.2-8я73

ISBN 978-5-7695-6786-5

ПРЕДИСЛОВИЕ

Настоящая книга представляет собой учебник по алгоритмической теории чисел, ориентированный на вопросы, связанные с различными криптографическими применениями. В гл. 1 дается обзор некоторых результатов теории чисел, в основном элементарных, нужных для последующих глав. Здесь изложение ограничивается определениями, формулировками утверждений и разбором примеров. Глава 2 содержит описание ряда быстрых алгоритмов теории чисел. Обсуждаются детерминированные, условные и вероятностные алгоритмы. В конце главы рассказывается о дискретном преобразовании Фурье и его использовании для построения быстрых алгоритмов умножения и деления целых чисел. В гл. 3 — 6 рассматриваются вопросы факторизации многочленов над конечными полями, проверки чисел на простоту и построения больших простых чисел, факторизации целых чисел, дискретного логарифмирования. Глава 7 содержит описание так называемого LLL-алгоритма, с помощью которого можно находить короткие векторы в заданной решетке и, в частности, решать задачи построения совместных диофантовых приближений чисел. В гл. 8 обсуждаются важные для криптографии система шифрования информации RSA, приложения задачи дискретного логарифмирования, цифровая подпись. В конце книги предложен ряд упражнений, направленных на то, чтобы дать возможность читателю поближе познакомиться с объектами, лежащими в основе описываемых алгоритмов.

Эта книга написана на основе курса алгоритмической теории чисел, читавшегося авторами в течение ряда лет на механико-математическом факультете МГУ им. М. В. Ломоносова. Авторы благодарны А. В. Устинову, И. П. Рочеву и А. Ю. Нестеренко за ряд полезных замечаний. Наша особая балгодарность рецензентам книги — М. М. Глухову и А. Б. Лосю.

ВВЕДЕНИЕ

Теория чисел начала широко применяться в криптографии примерно 30 лет назад. Это было вызвано необходимостью обмена большими массивами конфиденциальной информации (не только государственной и военной, но и банковской, экономической, медицинской, юридической и т. п.), а также возможностью такого обмена в связи с появлением доступных и эффективных компьютерных средств обработки этой информации. Любая информация может быть закодирована последовательностью чисел. Например, букве «а» можно сопоставить число 1, букве «б» — число 2 и так далее, букве «я» — число 33. Можно сопоставить числа пробелам, точке, другим знакам препинания. После этого процессы зашифрования и расшифрования информации представятся как некоторые алгоритмы, перерабатывающие одни массивы целых чисел в другие.

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

Сложность алгоритмов теории чисел обычно измеряют количеством арифметических операций (сложений, вычитаний, умножений и делений с остатком), необходимых для выполнения всех действий, предписанных алгоритмом. Впрочем, это определение не учитывает величины чисел, участвующих в вычислениях. Ясно, что 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. оцениванию количества необходимых операций с цифрами 0 и 1 в двоичной записи чисел (битовая сложность). Это зависит от рассматриваемой задачи, от целей автора и т. д.

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

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

Для многих задач алгоритмы полиномиальной сложности не известны. Сложной, например, является следующая фундаментальная задача.

Пример В.1. *Дано простое число p. Для заданных чисел $a, b \in \mathbb{Z}$ требуется решить сравнение*

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

Эта задача носит название дискретного логарифмирования. Как известно, мультипликативная группа $(\mathbb{Z}/p\mathbb{Z})^*$ циклична. Если a — её образующая, то сравнение (B.1) при $p \nmid b$ всегда разрешимо. Однако нахождение решения при большом p является весьма трудоемкой в вычислительном отношении задачей. Неслучайно в конце практически всех учебников по элементарной теории чисел приводятся таблицы индексов — так традиционно назывались дискретные логарифмы. Лучшие из

известных алгоритмов дискретного логарифмирования, использующие вычисления в полях алгебраических чисел, требуют $O(\exp(c(\ln p)^{1/3}(\ln\ln p)^{2/3}))$ арифметических операций. Впрочем, эта оценка условна, ибо опирается на ряд недоказанных гипотез теории чисел.

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

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

Логарифмы по произвольному основанию a могут быть вычислены с помощью тождества

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

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

Следующая задача также важна в криптографических приложениях и является сложной.

Пример B.2. *Дано составное натуральное число N. Требуется разложить его на нетривиальные множители.*

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

Глава 1. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Числа

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

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

В данной главе представлен обзор необходимых в дальнейшем сведений из теории чисел.

1.1. Делимость целых чисел. Алгоритм Евклида

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

$$a = b \cdot c.$$

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

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

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

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

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

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

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

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

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

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

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

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

Пусть $a \geq b$ — 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. Известный в Древней Греции алгоритм, называемый алгоритмом Евклида, достаточно быстро находит наибольший общий делитель и при этом не разлагает числа на множители.

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

совпадение наибольших общих делителей пар чисел a, b и b, r, т. е. равенство

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

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

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

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

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

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

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

Пример 1.1. *Найти наибольший общий делитель чисел* 3 009 *и* 894.

Пользуясь алгоритмом Евклида, находим

$$\begin{aligned}
3\,009 &= 894 \cdot 3 + 327, && 894 = 327 \cdot 3 + 240,\\
327 &= 240 \cdot 1 + 87, && 240 = 87 \cdot 2 + 66,\\
87 &= 66 \cdot 1 + 21, && 66 = 21 \cdot 21 + 3,\\
21 &= 3 \cdot 7.
\end{aligned}$$

Последний ненулевой остаток равен 3, поэтому $(3\,009, 894) = 3$.

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

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

где a, b, c — целые числа.

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

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

Для доказательства достаточности рассмотрим еще раз равенства (1.3).

Первое из них даёт $r_2 = a - bq_1$. Подставляя это выражение во второе равенство, находим

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

Далее, из третьего —

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

Продолжив вычисления, можно найти представление $r_n = au + + bv$ с некоторыми целыми u, v. Но это равенство означает, что уравнение $ax + by = (a, b)$ имеет решение $x = u, y = v$. А поскольку $(a, b)|c$, решениями уравнения (1.4) будут целые числа $x_0 = \dfrac{cu}{(a, b)}$, $y_0 = \dfrac{cv}{(a, b)}$. ■[1]

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

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

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

[1]Здесь и далее знак ■ означает конец доказательства.

1.2. Простые числа, основная теорема арифметики

Натуральное число $N > 1$ называется *составным*, если его можно представить в виде произведения двух меньших натуральных чисел. Если такое представление невозможно, число N называется *простым*. Например, числа 1 111 111 и 11 111 111 111 составные. Это следует из равенств

$$1\,111\,111 = 239 \cdot 4\,649, \quad 11\,111\,111\,111 = 21\,649 \cdot 513\,239.$$

Все сомножители в этих равенствах — простые числа.

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

Решето Эратосфена [Этот алгоритм находит список всех простых чисел $p_1 < p_2 < \ldots$ 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 через* p_k *первое невычеркнутое число, следующее за* p_{k-1}. *Если* $p_k^2 > N$, *обозначаем через* $p_{k+1}, p_{k+2}, \ldots$ *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.*

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

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

[1] Эратосфен (276 — 196 гг. до н. э.) — древнегреческий математик, географ и астроном.

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

Более сложный алгоритм позволил найти, что среди первых 10^{16} натуральных имеется 279 238 341 033 925 простых чисел. Наибольшие из известных в настоящее время простых чисел имеют вид

$$2^{43\,112\,609} - 1, \quad 2^{42\,643\,801} - 1, \quad 2^{37\,156\,667} - 1, \quad 2^{32582657} - 1.$$

Большее из них записывается 12 978 189 цифрами. Оно было найдено в августе 2008 г. Следить за достижениями в этой области можно в Интернете по адресу http://primes.utm.edu/largest.html.

Утверждение о существовании сколь угодно больших простых чисел или, что то же самое, о бесконечности множества простых чисел называется теоремой Евклида[1].

Теорема 1.2. Множество простых чисел бесконечно.

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

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

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

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

Такое представление числа называется *каноническим разложением* на простые сомножители. Например, каноническое разложение числа 2 520 имеет вид $2\,520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

[1] Теорема о простых числах содержится в IX книге «Начал» Евклида. По некоторым косвенным данным, предполагается, что он жил в Александрии в III в. до н. э.

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

$$\nu_2(2\,520) = 3, \quad \nu_3(2\,520) = 2, \quad \nu_{11}(2\,520) = 0.$$

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

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

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

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

Разложение на простые сомножители больших чисел — очень трудоемкая задача, в гл. 5 приведены некоторые алгоритмы её решения.

Обозначим символом $\pi(x)$ количество простых чисел p, с условием $p \le x$. Ранее с помощью решета Эратосфена установлено, что $\pi(100) = 25$. Ясно, что с ростом x функция $\pi(x)$ возрастает. Теорема 1.2 равносильна утверждению $\pi(x) \to \infty$ при $x \to \infty$.

Впервые достаточно точные границы изменения функции $\pi(x)$ были установлены в 1850 г. П. Л. Чебышёвым[1].

Теорема 1.4. При всех достаточно больших x справедливы неравенства

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

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

В настоящее время известны намного более точные неравенства

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

1.3. Функция Эйлера и ее свойства

Для каждого целого числа $n \ge 1$ обозначим символом $\varphi(n)$ количество натуральных чисел, не превосходящих n и взаимно

[1] Пафнутий Львович Чебышёв (1821 — 1894) — русский математик.

простых с n. Другими словами, $\varphi(n)$ есть количество целых чисел k, удовлетворяющих условиям

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

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

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

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

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

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

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

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

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

3. Для любого натурального n выполняется равенство

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

1.4. Сравнения

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

Отношение сравнимости обозначается символом $a \equiv b (\mathrm{mod}\, m)$ и обладает следующими легко проверяемыми свойствами:

1) $a \equiv a (\mathrm{mod}\, m)$ *для любого целого* a;
2) *если* $a \equiv b (\mathrm{mod}\, m)$, *то* $b \equiv a (\mathrm{mod}\, m)$;
3) *если* $a \equiv b (\mathrm{mod}\, m)$ *и* $b \equiv c (\mathrm{mod}\, m)$, *то* $a \equiv c (\mathrm{mod}\, m)$;
4) *если* $a \equiv b (\mathrm{mod}\, m)$, $c \equiv d (\mathrm{mod}\, m)$, *то*

$$a + c \equiv b + d (\mathrm{mod}\, m);$$
$$a - c \equiv b - d (\mathrm{mod}\, m);$$
$$a \cdot c \equiv b \cdot d (\mathrm{mod}\, m),$$

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

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

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

$$P(a) \equiv P(b) (\mathrm{mod}\, m).$$

Подобное свойство выполняется и для многочленов от нескольких переменных.

Отметим еще несколько свойств сравнений:

5) *если* $ab \equiv ac (\mathrm{mod}\, m)$ *и* $(a, m) = 1$, *то* $b \equiv c (\mathrm{mod}\, m)$;

6) *обе части сравнения и модуль можно умножить на любое отличное от нуля число, т. е. из сравнения* $a \equiv b (\mathrm{mod}\, m)$ *при* $d \neq 0$ *следует* $ad \equiv bd (\mathrm{mod}\, md)$;

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

8) *если* $a \equiv b (\mathrm{mod}\, m)$, *то* $(a, m) = (b, m)$;

9) *если* $a \equiv b (\mathrm{mod}\, m)$ *и* $d | m$, *то* $a \equiv b (\mathrm{mod}\, d)$;

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

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

Существует ровно m классов вычетов по модулю m. Каждый из них содержит единственное целое число r из промежутка

$0 \le r < m$, называемое *наименьшим неотрицательным вычетом класса*. На множестве классов вычетов по модулю m можно ввести операции сложения, вычитания и умножения по правилам

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

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

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

$$ab \equiv 1 (\mathrm{mod} m). \tag{1.10}$$

Тогда $\overline{a}\overline{b} = \overline{ab} = \overline{1}$ и класс вычетов $\overline{a}$ обратим. Если же $(a, m) > 1$, то, как легко видеть, класс вычетов $\overline{a}$ есть делитель нуля в кольце $\mathbb{Z}/m\mathbb{Z}$ 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 $0 \le k < m$ и $(k, m) = 1$. Количество таких чисел k равно $\varphi(m)$, т. е. задаётся функцией Эйлера.

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

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

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