Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение высшего образования

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ МОРСКОГО И РЕЧНОГО ФЛОТА имени адмирала С. О. МАКАРОВА

Институт ВОДНОГО ТРАНСПОРТА

Кафедра комплексного обеспечения информационной безопасности

М. Ю. Ястребов
А. П. Ныркова
Г. Б. Чистяков

ВВЕДЕНИЕ В ТЕОРИЮ ЧИСЕЛ

Учебное пособие

Рекомендовано Редакционно-издательской комиссией ГУМРФ имени адмирала С. О. Макарова

Санкт-Петербург
Издательство ГУМРФ имени адмирала С. О. Макарова
2022

УДК 517.5:551.48
ББК 22.171
Я85

Рецензенты:

А. Г. Коробейников, д-р техн. наук, проф.
(Санкт-Петербургский филиал
ФГБУН «Институт земного магнетизма, ионосферы
и распространения радиоволн имени Н. В. Пушкова» РАН);
А. В. Колесниченко, д-р техн. наук, проф.
(ФГБОУ ВО ГУМРФ имени адмирала С. О. Макарова)

Я85 **Ястребов, М. Ю.**
Введение в теорию чисел : учеб. пособие / М. Ю. Ястребов, А. П. Ныркov, Г. Б. Чистяков. — СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2022. — 76 с.

ISBN 978-5-9509-0495-0

Содержание учебного пособия соответствует ФГОС ВО по направлениям подготовки бакалавриата 10.03.01 «Информационная безопасность» и специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Пособие предназначено для студентов 3-го курса очной формы обучения по дисциплине «Основы теории чисел». Может быть использовано как дополнительный методический материал при изучении других дисциплин, направленных на формирование профессиональных компетенций, а также полезно для повышения уровня математического образования для магистров направления 10.04.01 «Информационная безопасность» и аспирантов направления 09.06.01 «Информатика и вычислительная техника».

Рекомендовано к изданию Редакционно-издательской комиссией ГУМРФ имени адмирала С. О. Макарова в качестве учебного пособия. Протокол № 1 от 28 февраля 2022 года.

УДК 517.5:551.48
ББК 22.171

ISBN 978-5-9509-0495-0

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Учебное пособие по дисциплине «Введение в теорию чисел» направлено на формирование общепрофессиональных компетенций в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по уровням бакалавриата и специалитета:

– ОПК-3.1 Применяет соответствующий математический аппарат для решения профессиональных задач.

Учебное пособие предназначено для обучающихся 3-го курса по направлению подготовки бакалавриата 10.03.01 «Информационная безопасность» и специалитета 10.05.03 «Информационная безопасность автоматизированных систем», может быть использовано при изучении других дисциплин, направленных на формирование профессиональных компетенций, а также полезно для повышения уровня математического образования для магистров направления 10.04.01 «Информационная безопасность» и аспирантов направления 09.06.01 «Информатика и вычислительная техника».

В пособии содержится изложение базовых понятий теории чисел. Рассмотрены вопросы делимости, разложения в цепные дроби, свойства и решение сравнений и систем сравнений.

Цель авторов учебного пособия — помочь обучающимся сформировать базовые знания в теории чисел, являющейся основой многих криптографических процедур.

Содержание пособия соответствует рабочей программе дисциплины и основано на классических работах и современных научных и учебно-методических публикациях [1–14].

ГЛАВА 1. ТЕОРИЯ ДЕЛИМОСТИ

Понятие натурального числа наряду с понятиями множества и алгоритма является исходным, интуитивно ясным понятием, не определяемым через более простые понятия. Умение считать, как и умение различать разные количества предметов, — это врожденные способности человеческого интеллекта.

Натуральные числа 1, 2, 3,… имеют двоякое применение в практике: они могут использоваться либо для счета предметов, либо для определения порядкового номера предмета в ряду однородных предметов.

Основополагающими свойствами натуральных чисел («членов натурального ряда») являются их упорядоченность по возрастанию и (теоретическая) возможность неограниченного перехода к следующему, на единицу большему натуральному числу.

Последнее дается нам интуицией «еще одного шага» и формализуется в аксиоме индукции, позволяющей проводить доказательства свойств бесконечных множеств. Одна из возможных формулировок аксиомы индукции имеет следующий вид: если некоторое утверждение $A(n)$ о натуральных числах n справедливо при $n = 1$ и из его справедливости для n следует его справедливость для следующего числа $n + 1$, то утверждение $A(n)$ справедливо для всех натуральных чисел.

Равносильным аксиоме индукции является утверждение о том, что в любой совокупности натуральных чисел имеется наименьший элемент.

Следует указать также на **аксиому Архимеда**: для заданных натуральных чисел m и n существует натуральное число t такое, что $m\,t > n$. Иными словами, двигаясь по числовой оси шагами одинаковой длины, можно уйти на бесконечность, то есть сколь угодно далеко (дальше любого наперед заданного n). Эта аксиома часто используется в доказательствах без явной на нее ссылки.

Методы теории чисел имеют большое значение для криптографии (шифрования, тайнописи) — важного раздела общей задачи защиты информации.

1.1. Исходные понятия и теоремы

Объектом изучения в теории чисел являются множество натуральных чисел $\mathbb{N} = \{1, 2, ..., n, ...\}$ и множество целых чисел $\mathbb{Z} = \{..., -n, ..., -2, -1, 0, 1, 2, ..., n, ...\}$.

Определение. Пусть $a, b \in \mathbb{Z}$. Число a делится на число b (b является делителем a), если для некоторого $t \in \mathbb{Z}$ выполняется $a = bt$. Обозначение: $b|a$. Термины: *b делит* или *делитель a*; *a кратно b*.

Простейшие свойства делимости описываются следующими утверждениями:

Теорема 1. Если $b|a$, $c|b$, то $c|a$.

Доказательство. $a = bt,\ b = ck \Rightarrow a = (ck)t = c(kt)$. ■

Теорема 2. Если имеет место равенство

$$k + ... + m = p + ... + r + t,$$

и обо всех его членах, за исключением одного (например, t), известно, что они делятся на b, то и последний член делится на b.

Доказательство. Имеем по условию:

$$k = k_1 b; ...;\ m = m_1 b;\ p = p_1 b; ...;\ r = r_1 b \Rightarrow$$

$$\Rightarrow t = (k_1 + ... + m_1 - p_1 - ... - r_1)b.$$ ■

NB: В дальнейшем будем рассматривать лишь положительные (то есть натуральные) делители целых чисел.

Теорема 3 (о делении с остатком). Всякое $a \in \mathbb{Z}$ при всяком натуральном b единственным образом представимо в виде:

$$a = bq + r,$$

где $q \in \mathbb{Z}$, $0 \le r < b$ (то есть делится на b с остатком r).

Термины: q— неполное частное; r — остаток.

Доказательство. Для получения указанного представления достаточно взять в качестве q такое целое число, при котором кратное bq является наибольшим, не превосходящим a. Например, при делении с остатком на $b = 4$ числа $a = 9$ имеем $9 = 4 \cdot 2 + 1$, так что $q = 2$, $r = 1$; при делении на 4 числа –9 уже $q = -3$, $r = 3$, поскольку $-9 = 4 \cdot (-3) + 3$.

Убедимся теперь в единственности такого деления. Если $a = bq + r = bq_1 + r_1$, то, вычитая, получим: $0 = b(q - q_1) + (r - r_1)$. Отсюда по теореме 2 (так как 0 делится на любое натуральное b) следует, что $b \mid (r - r_1)$. Ввиду условия $0 \le r, r_1 < b$ это возможно лишь при $r - r_1 = 0$; тогда и $q - q_1 = 0$. ■

Рис. 1 и рис. 2 иллюстрируют деление чисел $a = 9$ и $a = -9$ на $b = 4$ с остатком.

Разумеется, если $b|a$, то остаток $r = 0$.

$$9 = 4 \cdot 2 + 1.$$

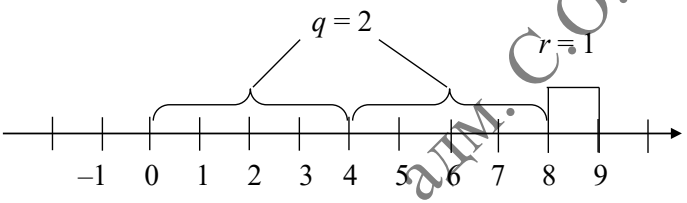

Рис. 1. Деление числа 9 с остатком

$$-9 = 4 \cdot (-3) + 1$$

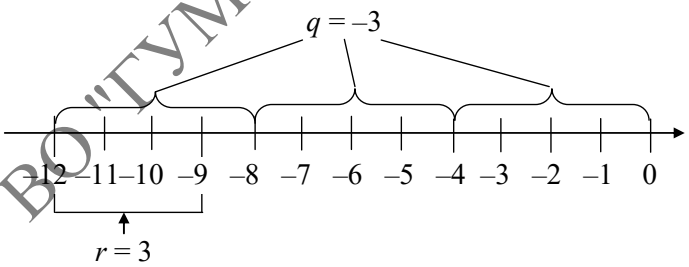

Рис. 2. Деление числа (–9) с остатком

1.2. Наибольший общий делитель

Определение. Натуральное число d называется общим делителем целых чисел $a_1, a_2, \ldots, a_n$, если оно является делителем каждого из этих чисел: $d \mid a_1, ..., d \mid a_n$.

Пример

$d_1 = 2$ и $d_2 = 3$ являются общими делителями чисел –24, –12, 18, 84.

Определение. Наибольший из общих делителей чисел a_1, a_2, … , a_n называется их наибольшим общим делителем (НОД).

Обозначение НОД: $d = (a_1, a_2, ..., a_n)$.

Примеры

1. Наибольшим общим делителем чисел –24, –12, 18, 84 является $d = 6$: (–24, –12, 18, 84) = 6.

2. (21, 22) = 1.

3. (280, 84) = 28.

Обозначим: $D_{x,y}$ — множество общих положительных делителей чисел x и y; D_x — множество положительных делителей числа x.

Замечание. Поскольку 0 делится на любое число, то $D_{b,0} = D_b$.

Теорема 4. Если $b \mid a$, то $D_{a,b} = D_b$, то есть множество общих делителей чисел a и b совпадает с множеством делителей одного b.

Доказательство. Пусть $a = bs$. Докажем оба включения $D_{a,b} \subset D_b$ и $D_b \subset D_{a,b}$.

Если $k \in D_{a,b}$, то $k \in D_b$; таким образом, $D_{a,b} \subset D_b$. Обратно, если $k \in D_b$, то есть $b = kt$, то $a = bs = (kt)s = k(ts)$; тогда $k \in D_{a,b} \Rightarrow$ $\Rightarrow D_b \subset D_{a,b}$. ■

Следствие. Если $b \mid a$, то $(a,b) = b$.

Доказательство. Из совпадения множества общих делителей чисел a и b с множеством делителей числа b следует совпадение наибольших элементов этих множеств, а наибольшим делителем числа b является само b. ■

Теорема 5. Если $a = bq + r$, то $D_{a,b} = D_{b,r}$; в частности, $(a,b) = (b,r)$.

Доказательство. Если $k \in D_{a,b}$, то по теореме 2 из равенства $a = bq + r$ следует, что $k \mid r$, и, значит, $k \in D_{b,r}$. Обратно, если $k \mid b$

и $k \mid r$, то по той же теореме $k \mid a$. Таким образом, множество делителей в обоих случаях одно и то же. Тогда и наибольший элемент в обоих множествах один и тот же. ■

1.3. Алгоритм Эвклида для отыскания НОД

Пусть a и b — натуральные числа. Возможны два случая.

1. Если $b \mid a$, то $(a,b) = b$.

2. Пусть теперь b не является делителем a. Из теоремы 3 о делении с остатком получаем цепочку равенств (если положить $a = r_0,\ b = r_1$, все равенства, включая два первых, примут единообразный вид):

$$
\begin{aligned}
&a = bq_1 + r_2,\ 0 \le r_2 < b \quad \leftrightarrow \quad r_0 = r_1 q_1 + r_2,\ 0 \le r_2 < r_1;\\
&b = r_2 q_2 + r_3,\ 0 \le r_3 < r_2 \quad \leftrightarrow \quad r_1 = r_2 q_2 + r_3,\ 0 \le r_3 < r_2;\\
&r_2 = r_3 q_3 + r_4,\ 0 \le r_4 < r_3;\\
&\ldots \qquad\qquad (1)\\
&r_{n-2} = r_{n-1} q_{n-1} + r_n,\ 0 \le r_n < r_{n-1};\\
&r_{n-1} = r_n q_n + 0.
\end{aligned}
$$

При некотором n обязательно окажется $r_n \mid r_{n-1}$, то есть $r_{n+1} = 0$, поскольку цепочка убывающих натуральных чисел $r_1 = b, r_2, r_3, \ldots$ не может продолжаться неограниченно.

Получение указанной цепочки равенств путем последовательных делений с остатком называется алгоритмом Эвклида.

Теорема 6. 1. Последний ненулевой остаток r_n является наибольшим общим делителем исходных чисел a и b: $(a,b) = r_n$.

2. Множество общих делителей чисел a и b совпадает с множеством делителей их НОД.

Доказательство. 1. По теореме 5 из (1) следуют равенства НОД:

$$(a,b) = (b,r_2) = (r_2,r_3) = \ldots = (r_{n-1},r_n) = r_n$$

(последнее равенство — по следствию из теоремы 4, так как $r_n \mid r_{n-1}$).

2. Из равенств (1) последовательно вытекает, что $D_{a,b} = D_{b,r_2} = D_{r_2,r_3} = ... = D_{r_{n-1},r_n} = D_{r_n,0} = D_{r_n}$. ■

Пример

Найдем $(1113, 504)$. Выполняя последовательные деления с остатком по схеме (1), получаем:

$1113 = 504 \cdot 2 + 105$;

$504 = 105 \cdot 4 + 84$;

$105 = 84 \cdot 1 + 21$;

$84 = 21 \cdot 4 + 0$.

Последний ненулевой остаток равен 21, так что $(1113, 504) = 21$.

Теорема 7 (линейное представление НОД). Пусть $d = (a,b)$. Тогда существуют целые числа M и N, такие что $d = aM + bN$.

Доказательство. Идя по цепочке (1), последовательно получаем:

из первого равенства:

$r_2 = a \cdot 1 + b(-q_1) = aM_1 + bN_1$, где $M_1 = 1, N_1 = -q_1$.

Далее, из второго равенства:

$r_3 = b - r_2 q_2 = b \cdot 1 - (aM_1 + bN_1)q_2 =$

$= a(-M_1 q_2) + b(1 - N_1 q_2) = aM_2 + bN_2$,

где $M_2 = -M_1 q_2$, $N_2 = 1 - N_1 q_2$,

и т. д. вплоть до линейного представления $r_n = (a,b)$.

Следствие. Если $c \mid a$ и $c \mid b$, то $c \mid (a,b)$, то есть общий делитель двух чисел делит и их НОД.

Доказательство. По условию $a = mc$, $b = nc$; отсюда

$d = aM + bN = (mc)M + (nc)N = c(mM + nN) \Rightarrow c \mid d$. ■

1.4. Свойства НОД

Теорема 8. Если m — натуральное число, то $(am, bm) = (a,b)m$, то есть при умножении обоих чисел a и b на m их НОД также умножается на m. Иными словами, общий множитель можно выносить за знак НОД.

Доказательство. Если все равенства в цепочке (1) умножить на m, то получится цепочка, в которой числа $a, b, r_2, ..., r_{n-1}, r_n$ заменяются на $am, bm, r_2m, ..., r_{n-1}m, r_nm$, после чего применяется то же рассуждение, что в теореме 6. ■

Теорема 9. Если $\delta \in D_{a,b}$, то $\dfrac{(a,b)}{\delta} = \left(\dfrac{a}{\delta}, \dfrac{b}{\delta}\right)$.

Доказательство. Поскольку $a = \dfrac{a}{\delta}\delta$, $b = \dfrac{b}{\delta}\delta$, то, применяя предыдущую теорему, получим: $(a,b) = \left(\dfrac{a}{\delta}\delta, \dfrac{b}{\delta}\delta\right) = \delta\left(\dfrac{a}{\delta}, \dfrac{b}{\delta}\right)$, откуда, деля на δ, получаем требуемое равенство. ■

Замечание. Если в последней теореме взять $\delta = (a,b)$, то получим:

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

Теорема 10. Если $(a,b) = 1$, то $(ac,b) = (c,b)$.

Доказательство. Убедимся, что одновременно $(ac,b) \le (c,b)$ и $(ac,b) \ge (c,b)$.

Поскольку (ac,b) делит b, то (ac,b) делит и bc, так что (ac,b), будучи делителем чисел ac и bc, делит их НОД: $(ac,b) \mid (ac,bc) = (a,b)c = 1 \cdot c = c$. Тогда, по следствию к теореме 7, (ac,b), деля c и b, делит (c,b), откуда

$$(ac,b) \le (c,b). \qquad (*)$$

С другой стороны, $(c,b) \mid ac$ и $(c,b) \mid b$, откуда $(c,b) \mid (ac,b)$, так что

$$(ac,b) \ge (c,b). \qquad (**)$$

Из неравенств (*) и (**) теперь следует $(ac,b) = (c,b)$. ■

1.5. Взаимно простые числа

Определение. Целые числа a и b называются взаимно простыми, если их НОД равен единице: $(a,b) = 1$.

1. $(a,b)=1 \Leftrightarrow \exists M, N:\ aM+bN=1$.

Доказательство. Необходимость вытекает из линейного представления НОД. Обратно, пусть $aM+bN=1$, и $\delta=(a,b)$. Тогда по теореме 2 $\delta \mid 1 \Rightarrow \delta=1$. ■

2. Если $(a_1,b)=1$ и $(a_2,b)=1$, то $(a_1a_2,b)=1$.

Доказательство. По предыдущему

$a_1M_1+bN_1=1$,

$a_2M_2+bN_2=1$;

перемножая эти равенства, получаем:

$a_1a_2(M_1M_2)+b(a_1M_1N_2+a_2M_2N_1+N_1N_2)=1$

и применяем предыдущее утверждение. ■

3. Если каждое из чисел $a_1, a_2, ..., a_n$ взаимно просто с b, то их произведение $a_1a_2...a_n$ также взаимно просто с b.

Доказательство. Следует по индукции из предыдущего, поскольку $(a_1a_2...a_n,b)=((a_1a_2...a_{n-1})a_n,b)$. ■

4. Если каждое из чисел $a_1, a_2, ..., a_n$ взаимно просто с каждым из чисел $b_1, b_1, ..., b_k$, то взаимно просты их произведения: $(a_1a_2...a_n, b_1b_2...b_k)=1$.

Доказательство следует из свойства 3.

5. Если $c \mid ab$, и $(a,c)=1$, то $c \mid b$.

Доказательство. По первому свойству при некоторых M и N выполняется равенство $aM+cN=1$, откуда, умножая на b:

$abM+cbN=b$, так что (теорема 2) b делится на c. ■

1.6. Разложение на простые множители

Определение. Натуральное число p, большее 1, называется простым, если у него нет делителей, отличных от 1 и самого p.

В принятых обозначениях это означает, что $D_p=\{1,p\}$. Число, не являющееся простым, называется составным.

Пример

Простыми являются, в частности, числа:

$2, 3, 5, 7, 11, 13, 17,\ 19, 23, ..., 239, ..., 1741, ..., 3677...$.

Отметим, что 2 является единственным четным простым числом.

Теорема 11. Всякое натуральное число $a > 1$ делится на некоторое простое число.

Доказательство. Пусть $p_1, p_2, ..., p_n$ — все делители a, отличные от 1, и p — наименьшее из них. Убедимся, что p простое число. Если $d \mid p$ и $d < p$, то $d \mid a$, откуда $d = 1$, так как p — наименьший делитель, отличный от единицы. ■

Теорема 12 (Евклида). Множество простых чисел бесконечно.

Доказательство. Допустим противное, то есть что все простые числа исчерпываются совокупностью $\{p_1, p_2, ..., p_n\}$. Рассмотрим число $a = p_1 p_2 ... p_n + 1$. При делении на каждое из $p_1, p_2, ..., p_n$, получается в остатке 1, так что либо само a простое, либо (по последней теореме) делится на некоторое простое число, отличное от $p_1, p_2, ..., p_n$. Противоречие. ■

Лемма. Пусть p — простое число, и $d = (a, p)$. Тогда:

$d = 1$, если a не делится на p;

$d = p$, если a делится на p.

Доказательство следует из того, что числа 1 и p являются единственными натуральными делителями p.

Теорема 13. Если произведение натуральных чисел ab $(a > 1, b > 1)$ делится на простое число p, то, по крайней мере, один из множителей, a или b, делится на p.

Доказательство. Пусть $d = (a, p)$ — НОД чисел a и p. По лемме $d = 1$ или $d = p$. Рассмотрим оба случая.

а) если $d = p$, то $p \mid a$, и все доказано;

б) если $d = 1$, то есть a и p взаимно просты, то $p \mid b$ по пятому свойству взаимной простоты. ■

Замечание. По индукции теорема распространяется на любое число сомножителей: если произведение $a_1a_2...a_n$ делится на простое число p, то по крайней один из сомножителей a_i делится на p.

Теорема 14 (основная теорема арифметики). Каждое натуральное число $a>1$ может быть представлено в виде произведения простых множителей:

$$a = p_1p_2...p_s \qquad (2)$$

и притом единственным образом (с точностью до порядка следования сомножителей).

Доказательство. 1. Существование представления. По теореме 11 $a = p_1a_1$, где p_1 простое; при этом $a > a_1$. Если $a_1 > 1$, то $a_1 = p_2a_2 \Rightarrow a = p_1p_2a_2$, $a > a_1 > a_2$ и т. д. На некотором s-м шаге окажется $a_s = 1$, и процесс закончится: $a = p_1p_2...p_s$.

2. Единственность представления. Пусть имеется два разложения на простые множители:

$$p_1p_2...p_s = q_1q_2...q_t. \qquad (*)$$

По теореме 13 одно из чисел q_i должно делится на p_1, и поскольку оно простое, то совпадает с p_1. После возможной перенумерации можно считать $p_1 = q_1$. Сокращая в (*) на p_1, получаем равенство $p_2...p_s = q_2...q_t$ с меньшим количеством множителей и т. д. Если $s<t$, то после очередного сокращения получим: $1 = q_{s+1}...q_t$, что невозможно. Аналогично устанавливается невозможность неравенства $t<s$. Итак, $s=t$, $p_1 = q_1,..., p_s = q_s$. ■

Простые множители в разложении (2) могут повторяться. Записывая их произведения с помощью степени, получаем каноническое разложение:

$$a = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}, \qquad (3)$$

в котором все $p_1, p_2,..., p_n$ различны и все показатели степени α_i положительны.

Если совместно рассматриваются два числа $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$, $b = q_1^{\beta_1} q_2^{\beta_2} ... q_t^{\beta_t}$, то, допуская нулевые показатели степени (то есть множители, равные 1), можно считать, что оба числа раскладываются в произведение степеней одних и тех же простых множителей:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} ... q_k^{\beta_k} \qquad (4)$$
$$(\alpha_i \geq 0,\ b_j \geq 0,\ \alpha_i + b_j > 0).$$

Замечание. В то время как вычисление произведения степеней простых чисел не вызывает затруднений, обратная задача — разложение большого натурального числа a на простые множители в виде (3) — является весьма трудной вычислительной задачей, требующей большого (часто неприемлемо большого) числа операций и неприемлемых затрат машинного времени. На этом основан один из приемов шифрования (см. ниже п. 6.2).

Лемма. Все делители числа $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ имеют вид:

$$d = p_1^{\lambda_1} p_2^{\lambda_2} ... p_k^{\lambda_k},\ 0 \leq \lambda_i \leq \alpha_i. \qquad (*)$$

Доказательство. Очевидно, что все числа вида (*) являются делителями a. Обратно, пусть $d \mid a$. Если бы в разложение d входило простое число q, отличное от $p_1, p_2, ..., p_k$, то оно вошло бы и в разложение a, что противоречит единственности разложения. Итак, в каноническое разложение d входят только степени (возможно нулевые) простых чисел $p_1, p_2, ..., p_k$. Если бы в равенстве (*) было, например, $\lambda_1 \geq \alpha_1$, то $p_1^{\lambda_1}$, будучи делителем d, делило бы и a, что противоречит единственности разложения. ■

Теорема 15 (о разложении НОД на простые множители). Пусть для чисел a и b имеет место разложение (4). Тогда

$$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k};\ \ \gamma_i = \min(\alpha_i, \beta_i),\ i = 1,...,n. \qquad (5)$$

Доказательство. Натуральное число $d = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$ является делителем a и b. Если к нему добавить простой множитель q, отличный от $p_1, p_2, ..., p_n$, то новое произведение не будет являться делите-

лем ни a, ни b (по теореме 13). Если же увеличить хотя бы один из показателей γ_i, то по крайней мере одно из чисел, a или b, не будет делиться на $p_i^{\gamma_i+1}$ (а именно то, которое доставляет минимум γ_i в паре (α_i,β_i). Значит, (5) является каноническим разложением НОД. ■

Пример

$a = 2^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13 = 2202200$,

$b = 2^2 \cdot 5^2 \cdot 13^2 = 16900$.

$(a,b) = 2^2 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13 = 1300$.

Замечание. Взаимная простота a и b означает, что в их разложениях на простые множители нет совпадающих. Действительно, если простое p делит и a, и b, то $p \mid (a,b) = 1$, что невозможно.

1.7. Наименьшее общее кратное

Определение. Наименьшим общим кратным (НОК) чисел $a_1, a_2, ..., a_n$ называется наименьшее положительное число M, которое делится на каждое из этих чисел.

Обозначение: $M = m(a_1, a_2, ..., a_n)$.

Примеры

1. $m(7,8) = 56$.

2. $m(-42, 30) = 210$.

3. $m(-2, 33, 10) = 330$.

Теорема 16 (о разложении НОК на простые множители). Пусть для чисел a и b имеет место разложение (4). Тогда

$$M = m(a,b) = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}; \quad \delta_i = \max(\alpha_i,\beta_i), \ i = 1,...,n. \qquad (6)$$

Доказательство. Поскольку $\delta_i \ge \alpha_i$, $\delta_i \ge \beta_i$, то $a \mid M$ и $b \mid M$, то есть M общее кратное чисел a и b. При этом, если в произведении (6) уменьшить хотя бы один из показателей δ_i, то нарушится делимость на a (если $\delta_i = \alpha_i$), либо на b (если $\delta_i = \beta_i$). ■

Аналогично, если

$$a_1 = p_1^{\alpha_{1,1}} p_2^{\alpha_{1,2}} \dots p_k^{\alpha_{1,k}}, ..., a_n = p_1^{\alpha_{n,1}} p_2^{\alpha_{n,2}} \dots p_k^{\alpha_{n,k}}, \ \alpha_{i,j} \ge 0, \qquad (7)$$

где каждое простое p_j входит в разложение хотя бы одного из $a_1,...,a_n$ в положительной степени, то

$$m(a_1,...,a_n) = p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}; \quad \delta_j = \max(\alpha_{1,j},...,\alpha_{n,j}). \qquad (6')$$

Следствие. Если $m_1 \mid a,..., m_k \mid a$, то $m(m_1,...,m_n) \mid a$.

Доказательство. Пусть $a = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$. Рассмотрим разложения чисел $m_1,...,m_n$ вида (7). Ввиду указанной делимости, для всех показателей при p_j выполняются неравенства: $\alpha_{1,j} \le \beta_j,..., \alpha_{n,j} \le \beta_j$ $(j = 1,...,k)$. Тогда такое же неравенство выполняется и для максимального из них:

$$\delta_j = \max(\alpha_{1,j},...,\alpha_{n,j}) \le \beta_j .$$

Итак, a делится на взаимно простые числа $p_1^{\delta_1},..., p_k^{\delta_k}$, которые тем самым входят в разложение a. Значит, a делится на их произведение, равное $m(m_1,...,m_n)$. ■

Теорема 17 (о связи НОК и НОД). $m(a,b) = \dfrac{ab}{(a,b)}$.

Доказательство. Разложим числа a и b на простые множители в виде (4):

$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$,

так что

$$m(a,b) = p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}; \quad \delta_i = \max(\alpha_i,\beta_i), \ i = 1,...,n,$$

$$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}; \quad \gamma_i = \min(\alpha_i,\beta_i), \ i = 1,...,n.$$

Теперь

$$m(a,b) \cdot (a,b) = p_1^{\gamma_1+\delta_1} p_2^{\gamma_2+\delta_2} ... p_k^{\gamma_k+\delta_k},$$

$$ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} ... p_k^{\alpha_k+\beta_k}.$$

Пусть, например, для некоторого i $\alpha_i \ge \beta_i$, так что в разложениях (5) и (6) $\gamma_i = \beta_i$, $\delta_i = \alpha_i$. Тогда

$$\delta_i + \gamma_i = \max(\alpha_i + \beta_i) + \min(\alpha_i + \beta_i) = \alpha_i + \beta_i . \ ■$$

1.8. Цепные дроби

Определение. Цепной дробью (или непрерывной дробью) называется выражение

$$A = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots}}, \tag{8}$$

где $q_1 \in \mathrm{Z}$, $q_2, q_3, \ldots \in \mathrm{N}$. Числа $q_1, q_2, q_3, \ldots$ называются *элементами непрерывной дроби*.

Если число элементов конечно, то есть непрерывная дробь имеет вид:

$$A = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}, \tag{8'}$$

то A — рациональное число, как результат арифметических операций с рациональными числами.

Разложение числа в непрерывную дробь

Рассмотрим теперь обратный процесс, когда произвольному вещественному числу α сопоставляется однозначно определенная непрерывная дробь A.

I. Если $\alpha \in \mathbb{Z}$, то полагаем $A = q_1 = \alpha$.

II. Пусть $\alpha \notin \mathbb{Z}$. Положим $q_1 = [\alpha]$ — наибольшее целое, не превосходящее α. Тогда

$$0 < \alpha - q_1 < 1 \Rightarrow \alpha = q_1 + (\alpha - q_1) = q_1 + \frac{1}{\alpha_1}, \text{ где } \alpha_1 > 1.$$

Если α_1 оказывается натуральным числом, то полагаем $q_2 = \alpha_1$, так что

$$\alpha = q_1 + \frac{1}{q_2} = A,$$

и процесс заканчивается. Если же $\alpha_1 \notin \mathrm{N}$, то положим $q_2 = [\alpha_1] \Rightarrow$

$\Rightarrow \alpha_1 = q_2 + \dfrac{1}{\alpha_2}$, где $\alpha_2 > 1$. Если α_2 оказывается натуральным числом, то полагаем $q_3 = \alpha_2$, так что

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = A,$$

и процесс заканчивается. Если же α_2 нецелое, то

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}, \quad \alpha_3 > 1,$$

так что

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\alpha_3}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\alpha_4}}} = \ldots$$

и т. д.

II.1. Если α — иррациональное число, то процесс не может закончится за конечное число шагов, поскольку на каждом шаге мы получаем конечную непрерывную дробь, являющуюся рациональным числом. Таким образом, иррациональному числу описанный процесс сопоставляет бесконечную непрерывную дробь.

II.2. Пусть теперь $\alpha = \dfrac{a}{b}$ — рациональное число, причем числа a и b выбраны так, что дробь несократима и $b > 0$. Тогда алгоритм Эвклида последовательных делений с остатком дает разложение числа $\dfrac{a}{b}$ в конечную непрерывную дробь.

Имеем (см. п. 1.3):

1) $a = bq_1 + r_2 \Rightarrow \dfrac{a}{b} = q_1 + \dfrac{r_2}{b}$;

2) $b = r_2 q_2 + r_3 \Rightarrow \dfrac{b}{r_2} = q_2 + \dfrac{r_3}{r_2} \Rightarrow \dfrac{r_2}{b} = \dfrac{1}{q_2 + \dfrac{r_3}{r_2}} \Rightarrow$

$$\Rightarrow \frac{a}{b} = q_1 + \frac{1}{q_2 + \dfrac{r_3}{r_2}};$$

3) $r_2 = r_3 q_3 + r_4 \Rightarrow \dfrac{r_2}{r_3} = q_3 + \dfrac{r_4}{r_3} \Rightarrow \dfrac{r_3}{r_2} = \dfrac{1}{q_3 + \dfrac{r_4}{r_3}} \Rightarrow$

$$\Rightarrow \frac{a}{b} = q_1 + \frac{1}{q_2 + \dfrac{1}{q_3 + \dfrac{r_4}{r_3}}};$$

.
.
.

n-1) $r_{n-2} = r_{n-1} q_{n-1} + r_n \Rightarrow \dfrac{r_{n-2}}{r_{n-1}} = q_{n-1} + \dfrac{r_n}{r_{n-1}} \Rightarrow$

$$\Rightarrow \frac{r_{n-1}}{r_{n-2}} = \frac{1}{q_{n-1} + \dfrac{r_n}{r_{n-1}}} \Rightarrow$$

$$\Rightarrow \frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \dfrac{r_n}{r_{n-1}}}}}};$$

n) $r_{n-1} = r_n q_n \Rightarrow \dfrac{r_{n-1}}{r_n} = q_n \Rightarrow \dfrac{r_n}{r_{n-1}} = \dfrac{1}{q_n} \Rightarrow$

$$\Rightarrow \frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

(здесь r_n — последний ненулевой остаток, даваемый алгоритмом Эвклида; $q_1, q_2, ..., q_n$ — неполные частные, даваемые этим алгоритмом).

Замечание. Требование несократимости дроби $\frac{a}{b}$ однозначно определяет числа a и b, а значит, и указанное представление рационального числа $\frac{a}{b}$ непрерывной дробью.

Подходящие дроби

Определение. Подходящими дробями в сопоставлении числу α цепной дроби (8) описанным способом называются числа

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}, ...$$

Примеры

1. Разложим в непрерывную дробь число $-\frac{38}{15} = \frac{-38}{15}$ (здесь $a = -38,\ b = 15 > 0$). Последовательные деления с положительным остатком дают:

$-38 = 15 \cdot (-3) + 7$. Таким образом, $q_1 = -3;\ r_1 = b = 15;\ r_2 = 7$, и $-\frac{38}{15} = -3 + \frac{7}{15} = -3 + \cfrac{1}{\left(\frac{15}{7}\right)}$.

Далее, $15 = 7 \cdot 2 + 1$, так что $q_2 = 2,\ r_3 = 1,\ \dfrac{15}{7} = 2 + \dfrac{1}{7}$, и $-\dfrac{38}{15} = -3 + \dfrac{1}{2 + \dfrac{1}{7}}$.

Наконец, $7 = 1 \cdot 7 + 0 \Leftrightarrow r_2 = r_3 q_3 + r_4$, так что $q_3 = 7,\ r_4 = 0$, и процесс заканчивается при получении нулевого остатка:

$$-\frac{38}{15} = -3 + \frac{1}{2 + \dfrac{1}{7}}.$$

Подходящие дроби в данном случае имеют вид:

$$\delta_1 = -3;\ \ \delta_2 = -3 + \frac{1}{2} = -\frac{5}{2};\ \ \delta_3 = -3 + \frac{1}{2 + \dfrac{1}{7}} = -\frac{38}{15}.$$

2. Разложим в непрерывную дробь число $\dfrac{105}{38}$ (здесь $a = 105,\ b = 38 = r_1$). Последовательные деления с остатком дают:

$$105 = 38 \cdot 2 + 29 \Rightarrow q_1 = 2,\ r_2 = 29 \Rightarrow \frac{105}{38} = 2 + \frac{29}{38} = 2 + \frac{1}{\left(\dfrac{38}{29}\right)};$$

$$38 = 29 \cdot 1 + 9 \Rightarrow q_2 = 1,\ r_3 = 9 \Rightarrow \frac{38}{29} = 1 + \frac{9}{29} = 1 + \frac{1}{\left(\dfrac{29}{9}\right)} \Rightarrow$$

$$\Rightarrow \frac{105}{38} = 2 + \frac{1}{1 + \left(\dfrac{29}{9}\right)}.$$

$$29 = 9 \cdot 3 + 2 \Rightarrow q_3 = 3,\ r_4 = 2 \Rightarrow \frac{29}{9} = 3 + \frac{2}{9} = 3 + \frac{1}{\left(\dfrac{9}{2}\right)} \Rightarrow$$

$$\Rightarrow \frac{105}{38} = 2 + \frac{1}{1 + \left(\dfrac{29}{9}\right)} = 2 + \frac{1}{1 + \dfrac{1}{3 + \dfrac{1}{\left(\dfrac{9}{2}\right)}}}.$$

$$9 = 2 \cdot 4 + 1 \Rightarrow q_4 = 4,\ r_5 = 1 \Rightarrow \frac{9}{2} = 4 + \frac{1}{2} \Rightarrow$$

$$\Rightarrow \frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

$$2 = 1 \cdot 2 + 0 \ \Rightarrow\ q_5 = 2,\ r_6 = 0.$$

Подходящие дроби:

$$\delta_1 = 2;\ \ \delta_2 = 2 + \frac{1}{1} = 3;\ \ \delta_3 = 2 + \cfrac{1}{1 + \cfrac{1}{3}} = \frac{11}{4};$$

$$\delta_4 = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4}}} = \frac{56}{13};\ \ \delta_5 = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}} = \frac{105}{38}.$$

Замечания.

1. Можно доказать, что для иррационального числа α бесконечная последовательность подходящих дробей δ_n сходится к α: $\lim\limits_{n \to \infty} \delta_n = \alpha$. Таким образом, каждое рациональное число раскладывается в конечную непрерывную дробь, а каждое иррациональное — в бесконечную. Нетрудно увидеть, что такое разложение однозначно, поскольку числа $\alpha_1, \alpha_2, ..., \alpha_n, ...$ на каждом шаге однозначно выражаются через предшествующие значения.

2. При $i \geq 1$ подходящая дробь δ_{i+1} получается из предыдущей δ_i заменой q_i на $q_i + \frac{1}{q_{i+1}}$.

3. Равенство $\delta_i = \alpha$ означает, что α — рациональное число, и δ_i — его последняя подходящая дробь.

Рекуррентные формулы для подходящих дробей

Введем обозначения для числителей и знаменателей подходящих дробей следующим образом.

0) С целью единообразия последующих формул положим $P_0 = 1,\ Q_0 = 0$ и будем считать равенство $\frac{A}{B} = \frac{P_i}{Q_i}$, где A и B — некоторые выражения, определением чисел P_i и Q_i (то есть определением по отдельности числителя P_i и знаменателя Q_i, а не дроби $\frac{P_i}{Q_i}$).

1) $\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}$.

2) $\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2}$.

3) $\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0} = \ldots$ умножаем числитель и знаменатель на q_3 $\ldots = \frac{q_2 q_3 P_1 + P_1 + q_3 P_0}{q_2 q_3 Q_1 + Q_1 + q_3 Q_0} = \frac{q_3 (q_2 P_1 + P_0) + P_1}{q_3 (q_2 Q_1 + Q_0) + Q_1} = \ldots$,

выражения в скобках — это P_2 и Q_2 соответственно $\ldots =$

$$= \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}.$$

Видим, что P_3 и Q_3 получаются из P_2 и Q_2 по той же схеме, по которой P_2 и Q_2 получаются из P_1 и Q_1.

4) Аналогично получаем для числителя и знаменателя каждой подходящей дроби δ_i рекуррентную формулу:

$$P_i = q_i P_{i-1} + P_{i-2};\quad Q_i = q_i Q_{i-1} + Q_{i-2} \tag{9}$$

с начальными значениями

$$P_0 = 1,\ Q_0 = 0 \quad \text{и} \quad P_1 = q_1,\ Q_1 = 1. \tag{10}$$

Свойства подходящих дробей

Свойство 1. При $i \geq 1$ справедлива формула:

$P_iQ_{i-1} - Q_iP_{i-1} = (-1)^i$.

Доказательство. Обозначим: $h_i = P_iQ_{i-1} - Q_iP_{i-1}$. В силу (10):

$h_1 = P_1Q_0 - Q_1P_0 = q_1 \cdot 0 - 1 \cdot 1 = -1$.

Далее, при $i \geq 2$, имеем:

$h_i = P_iQ_{i-1} - Q_iP_{i-1} = (q_iP_{i-1} + P_{i-2})Q_{i-1} - (q_iQ_{i-1} + Q_{i-2})P_{i-1} =$

$= P_{i-2}Q_{i-1} - Q_{i-2}P_{i-1} = -h_{i-1}$.

Значит,

$h_2 = -h_1 = -(-1) = 1$, $h_3 = -h_2 = -1$, $h_4 = -h_3 = -(-1) = 1$

и т. д. ■

Свойство 2. При $i \geq 2$ для разности соседних подходящих дробей справедлива формула:

$$\delta_i - \delta_{i-1} = \frac{(-1)^i}{Q_iQ_{i-1}} . \qquad (11)$$

Доказательство.

$$\delta_i - \delta_{i-1} = \frac{P_i}{Q_i} - \frac{P_{i-1}}{Q_{i-1}} = \frac{P_iQ_{i-1} - Q_iP_{i-1}}{Q_iQ_{i-1}} = \frac{h_i}{Q_iQ_{i-1}} = \frac{(-1)^i}{Q_iQ_{i-1}} . \blacksquare$$

Свойство 3. У подходящей дроби числитель и знаменатель, записанные по рекуррентным формулам (9) и (10), взаимно просты: $(P_i, Q_i) = 1$.

Доказательство. Пусть $d = (P_i, Q_i)$; тогда

$d \mid P_iQ_{i-1} - Q_iP_{i-1} \Rightarrow d \mid (-1)^i \Rightarrow d = 1$. ■

Замечание. Последнее означает, что подходящие дроби, записанные по рекуррентным формулам (9) и (10) несократимы.

Свойство 4. Пусть δ_i — подходящая дробь из разложения числа α , и $\delta_i \neq \alpha$. Тогда знак разности $\delta_i - \alpha$ совпадает со знаком $(-1)^i$.

Доказательство. δ_i получается при разложении α в непрерывную дробь заменой α_i на q_i.

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots + \cfrac{1}{q_{i-1} + \cfrac{1}{\alpha_i}}}}}.$$

При этом $\alpha_n > q_n$. Поскольку при уменьшении знаменателя дробь увеличивается, а при увеличении знаменателя она уменьшается, то:

α_i уменьшится;

α_{i-1} увеличится;

α_{i-2} уменьшится;

.

.

.

α при нечетном индексе i уменьшится, а при четном увеличится.

Следовательно, $\delta_i - \alpha < 0$, если i нечетно; $\delta_i - \alpha > 0$, если i четно. ■

Свойство 5. $\left|\alpha - \delta_{i-1}\right| \le \dfrac{1}{Q_i Q_{i-1}}$.

Доказательство. 1. Если $\delta_i = \alpha$, то это следует из (11) в виде равенства.

2. Если $\delta_i \ne \alpha$, то

$z = \alpha - \delta_{i-1} = (\alpha - \delta_i) + (\delta_i - \delta_{i-1}) = x + y$,

где $x = \alpha - \delta_i$, $y = \delta_i - \delta_{i-1}$. При этом, согласно (11), $\delta_i - \delta_{i-1} = \dfrac{(-1)^i}{Q_i Q_{i-1}}$, и разности $\delta_i - \alpha$ и $\delta_{i-1} - \alpha$ противоположны по

знаку. Возможны следующие варианты взаимного расположения чисел x, y и z на числовой оси:

а) i нечетно, $\Rightarrow i-1$ четно, $z<0$, $x>0$, $y<0$; равенство $z=x+y$ выражается рис. 3:

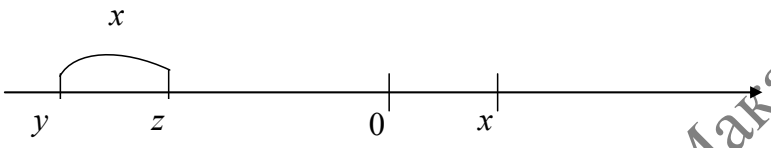

Рис. 3. Вариант взаимного расположения чисел x, y и z

Отсюда $|z|<|y|=\dfrac{1}{Q_iQ_{i-1}}$;

б) i четно, $\Rightarrow i-1$ нечетно, $z>0$, $x<0$, $y>0$; равенство $z=x+y$ выражается рис. 4:

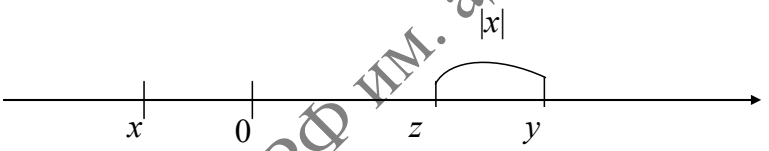

Рис. 4. Другой вариант взаимного расположения чисел x, y и z

Отсюда $0<z<y=\dfrac{1}{Q_iQ_{i-1}}$. ■

ГЛАВА 2. ТЕОРЕТИКО-ЧИСЛОВЫЕ ФУНКЦИИ

2.1. Функции целой и дробной части числа

Определение. Для произвольного вещественного числа x его целой частью $[x]$ называется наибольшее целое число, не превосходящее x.

Примеры

$[-11] = -11;\ [-9,33] = -10;\ [0] = 0;\ [8] = 8;\ [12,5] = 12;$
$[\pi] = 3;\ [e] = 2$.

При всех x выполняется неравенство $x - 1 < [x] \le x$. При этом $[x] = x \Leftrightarrow x \in Z$.

Функция $y = [x]$ является кусочно-постоянной (то есть имеет ступенчатый график), неубывающей и непрерывной справа. Ее график представлен на рис. 5.

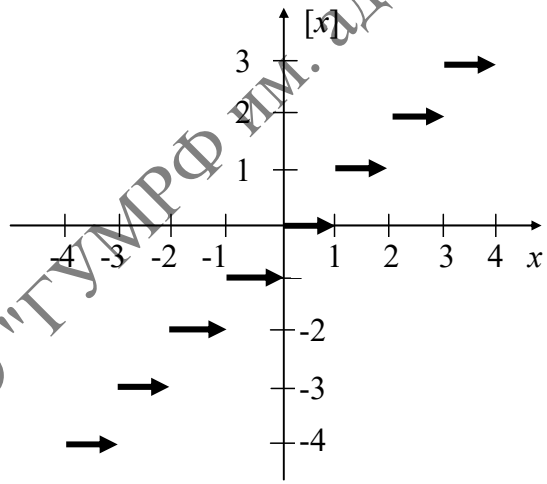

Рис. 5. График функции $[x]$

Определение. Для произвольного вещественного числа x его дробной частью $\{x\}$ называется разность $x - [x]$.

Примеры $\{-11\} = 0;\ \{-9.33\} = 0,67;\ \{0\} = 0;\ \{8\} = 0;\ \{12,5\} = 0,5;$
$\{\pi\} = 0,14159...;\ \{e\} = 0,718281828459045...$.

Очевидно, что $\{x\} = x \Leftrightarrow x \in [0,1)$.

Функция $y = \{x\}$ является периодической с периодом 1, непрерывной справа на всей числовой оси, а также непрерывной на промежутках $[n, n+1)$, $n \in \mathbb{Z}$. Ее график представлен на рис. 6.

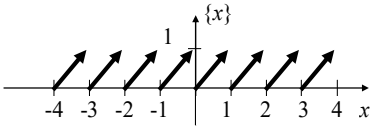

Рис. 6. График функции $\{x\}$

Пример

Рассмотрим $9! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9$. Простое число 2 входит в это произведение в сомножителях 2, 4, 6, 8, количество которых равно $\left[\frac{9}{2}\right] = 4$ (поскольку деление с остатком на 2 дает $9 = 2 \cdot 4 + 1$). Далее, среди этих сомножителей количество тех, которые делятся на $2^2 = 4$ равно $\left[\frac{9}{4}\right] = 2$, (деление с остатком на 4 дает $9 = 4 \cdot 2 + 1$). Наконец, количество множителей, которые делятся на $2^3 = 8$ равно $\left[\frac{9}{8}\right] = 1$, поскольку $9 = 8 \cdot 1 + 1$. В результате $9! = 2^1 \cdot 3^1 \cdot 2^2 \cdot 5^1 \cdot (2^1 \cdot 3^1) \cdot 7^1 \cdot 2^3 \cdot 3^2$, так что суммарный показатель, с которым простое число 2 входит в разложение 9! равно $4 + 2 + 1 = \left[\frac{9}{2}\right] + \left[\frac{9}{2^2}\right] + \left[\frac{9}{2^3}\right] = 7$.

Обобщение этого примера дает следующая теорема.

Теорема 18. Показатель, с которым простой множитель p входит в разложение числа $n! = 1 \cdot 2 \cdot \ldots \cdot n$ равен сумме ряда

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + \ldots . \qquad (12)$$

Замечание. При достаточно больших k $p^k > n \Rightarrow \left[\frac{n}{p^k}\right] = 0$, так что в ряде (12) все члены, начиная с некоторого, равны нулю.

Доказательство. Пусть m таково, что $p^m \le n$, $p^{m+1} > n$. Тогда $0 < \frac{n}{p^{m+1}} < 1$, и $\left[\frac{n}{p^{m+1}}\right] = \left[\frac{n}{p^{m+2}}\right] = \ldots = 0$.

В записи произведения $n!$ количество сомножителей, кратных p, равно $\left[\frac{n}{p}\right]$. Среди них имеется $\left[\frac{n}{p^2}\right]$ сомножителей, кратных p^2. Среди последних имеется $\left[\frac{n}{p^3}\right]$ сомножителей, кратных p^3, и т. д. Наконец, сомножители в записи произведения $n!$, кратные наибольшей степени p^m, встречаются $\left[\frac{n}{p^m}\right]$ раз. В итоге показатель, с которым простое число p входит в каноническое разложение (3) числа $n!$, представляется суммой единиц, общее количество которых дается выражением (12). ■

Пример

Показатель, с которым число 3 входит в произведение 51! равен сумме $\left[\frac{51}{3}\right] + \left[\frac{51}{9}\right] + \left[\frac{51}{27}\right] = 17 + 5 + 1 = 23$.

2.2. Мультипликативные функции

Определение. Функция $\theta(a)$, заданная на множестве натуральных чисел $\mathbb{N}$, называется мультипликативной, если она не является нулевой (то есть $\exists a \in \mathbb{N}: \theta(a) \neq 0$) и для любых взаимно простых a и b выполняется равенство $\theta(ab) = \theta(a)\theta(b)$.

Напомним, что взаимная простота a и b означает, что в их разложениях на простые множители нет совпадающих.

Примеры

1. Функция $\theta(a) = a^n$ при фиксированном n является мультипликативной: $(ab)^n = a^n b^n$.

2. Функция $\theta(n) = \log_2 n$ не является мультипликативной, так как, например, $\log_2(8 \cdot 9) < 3 + 4 = 7$; $\log_2(8) \cdot \log_2(9) > 3 \cdot 3 = 9$.

Общие свойства мультипликативных функций

1. $\theta(1) = 1$.

Действительно, по определению существует a, для которого $\theta(a) \neq 0$. Тогда

$\theta(a) = \theta(1 \cdot a) = \theta(1)\theta(a) \Rightarrow \theta(1) = 1$.

2. Если функции $\theta_1(a)$ и $\theta_2(a)$ мультипликативны, то и функция $\theta(a) = \theta_1(a)\theta_2(a)$ также мультипликативна.

Действительно, при взаимно простых a и b имеем:

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

$= \big(\theta_1(a)\theta_2(a)\big)\big(\theta_1(b)\theta_2(b)\big) = \theta(a)\theta(b)$.

При этом функция θ не равна тождественно нулю, поскольку

$\theta(1) = \theta_1(1)\theta_2(1) = 1 \cdot 1 \neq 0$.

3. Если θ — мультипликативная функция и $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — каноническое разложение, то ввиду взаимной простоты чисел $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$:

$$\theta(a) = \theta(p_1^{\alpha_1})\,\theta(p_2^{\alpha_2}) \ldots \theta(p_k^{\alpha_k}). \qquad (*)$$

Таким образом, все значения мультипликативной функции полностью определяются ее значениями на степенях простых чисел.

Обратно, задавая произвольным образом значения $\theta(p_i^{\alpha_i})$ функции θ на степенях простых чисел, можно с помощью формулы (*) определить мультипликативную функцию θ для всех натуральных аргументов.

Обозначим для мультипликативной функции θ и натурального a через $\eta(a) = \sum_{d|a} \theta(d)$ сумму значений функции θ, взятую по всем делителям d числа a, включая 1 и само a. Пусть, далее, $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ — каноническое разложение на степени простых множителей.

Теорема 19. Для функции $\eta(a)$ справедлива формула

$$\eta(a) = \left(1 + \sum_{i=1}^{\alpha_1} \theta(p_1^i)\right) \cdot ... \cdot \left(1 + \sum_{i=1}^{\alpha_k} \theta\left(p_k^i\right)\right). \qquad (13)$$

Доказательство. Представляя единицу в каждом из скобочных выражений правой части (13), соответственно, как $\theta(p_1^0),..., \theta(p_k^0)$, получим при раскрытии скобок без пропусков и повторений сумму выражений вида

$$\theta(p_1^{i_1})\theta(p_2^{i_2})...\theta(p_k^{i_k}) = \theta(p_1^{i_1} p_2^{i_2} ... p_k^{i_k}),$$

где

$$0 \le i_1 \le \alpha_1,\ 0 \le i_2 \le \alpha_2,...,\ 0 \le i_k \le \alpha_k .$$

Из слагаемых такого вида без пропусков и повторений состоит и сумма в левой части, поскольку все делители d числа a имеют вид $d = p_1^{i_1} p_2^{i_2} ... p_k^{i_k}$. Равенство (13) доказано. ■

Теорема 20. Пусть $\theta(a)$ мультипликативная функция. Тогда функция $\eta(a) = \sum_{d|a} \theta(d)$ также мультипликативна.

Доказательство. Поскольку $d = 1$ — единственный делитель 1, то $\eta(1) = \sum_{d|1} \theta(1) = \theta(1) = 1$, так что функция η отлична от тождественно нулевой. Далее, если $(a,b) = 1$, то есть $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$, $b = q_1^{\beta_1} q2^{\beta_2} ... q_t^{\beta_t}$, где $p_i \ne q_j$ при всех i, j, то по теореме 19:

$$\eta(ab) = \sum_{d|ab} \theta(d) = \prod_{i=1}^{s} (1 + \theta(p_i) + \theta(p_i^2) + ... + \theta(p_i^{\alpha_i})) \times$$

$$\times \prod_{j=1}^{t} (1 + \theta(q_j) + \theta(q_j^2) + ... + \theta(q_j^{\beta_j})) = \eta(a)\eta(b) . \blacksquare$$

Замечание. Беря в качестве θ различные мультипликативные функции, будем получать с помощью конструкции $\eta(a) = \sum_{d|a} \theta(d)$ новые мультипликативные функции.

Примеры

1. Рассмотрим мультипликативную функцию $\theta(a) = a^n$.

Тогда $\theta(d) = d^n$, $\theta(p^i) = p^{in}$, так что из равенства (13) для суммы n-х степеней делителей числа a получаем:

$$\sum_{d|a} d^n = (1 + p_1^n + p_1^{2n} + ... + p_1^{\alpha_1 n})...(1 + p_k^n + p_k^{2n} + ... + p_k^{\alpha_k n}). \qquad (14)$$

При $n = 1$ слева стоит просто сумма $S(a)$ всех делителей числа a, и мы получаем для нее выражение:

$$\sum_{d|a} d = (1 + p_1 + p_1^2 + ... + p_1^{\alpha_1})...(1 + p_k + p_k^2 + ... + p_k^{\alpha_k}). \qquad (15)$$

Каждое скобочное выражение справа есть сумма геометрической прогрессии с начальным членом 1, знаменателем p_i и числом членов $\alpha_i + 1$; она равна $\frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$. Таким образом,

$$S(a) = \sum_{d|a} d = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot ... \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \qquad (15')$$

2. Введем функцию $\tau(a)$ — число делителей натурального числа a (в число делителей входят 1 и само a). При $n = 0$ сумма слева в (14) содержит столько слагаемых, равных единице, сколько делителей имеет число a. Поэтому ее значение равно $\tau(a)$. Поскольку при $n = 0$ каждое скобочное выражение справа в (14) является суммой $\alpha_1 + 1$ единиц, то

$$\tau(a) = (1 + \alpha_1)...(1 + \alpha_k). \qquad (16)$$

В силу теоремы 20 функции $S(a)$ и $\tau(a)$ являются мультипликативными.

2.3. Функция Мёбиуса

Определение. Функция Мёбиуса $\mu(n)$ задается на множестве натуральных чисел $\mathbb{N}$ правилом:

1) $\mu(1) = 1$;

2) если $n > 1$ и n делится на квадрат простого числа, то $\mu(n) = 0$;

3) если все простые сомножители входят в каноническое разложение в первой степени, и количество этих сомножителей равно k, то $\mu(n) = (-1)^k$.

Примеры

$\mu(2) = \mu(13) = \mu(11) = \mu(7 \cdot 11 \cdot 19) = \mu(17 \cdot 103 \cdot 421) = -1$, поскольку все простые сомножители аргументов входят в их разложения в первой степени, и их количество нечетно.

$\mu(3^2) = \mu(5 \cdot 2^3) = \mu(5^2 \cdot 31 \cdot 37) = \mu(7^5) = 0$, поскольку каждый из аргументов делится на квадрат (отличный от единицы).

$\mu(2 \cdot 3) = \mu(7 \cdot 23 \cdot 29 \cdot 101) = 1$, поскольку все простые сомножители аргументов входят в их разложения в первой степени, и их количество четно.

Теорема 21. Функция Мёбиуса является мультипликативной.

Доказательство. Для произведения ab взаимно простых аргументов a и b возможны следующие случаи:

1. В разложение хотя бы одного из сомножителей, например, в a, входит квадрат, так что $\mu(a) = 0 \Rightarrow \mu(a)\mu(b) = 0$; тогда указанный квадрат будет входить и в разложение ab, так что и $\mu(ab) = 0$.

2. Все простые множители входят в a и в b в первой степени, и среди них нет одинаковых (иначе a и b не окажутся взаимно простыми). Если в a количество простых множителей равно k_a, а в b оно равно k_b, то

$$\mu(a) \cdot \mu(b) = (-1)^{k_a} \cdot (-1)^{k_b} = (-1)^{k_a + k_b}.$$

В произведении ab количество простых множителей равно $k_a + k_b$, так что и $\mu(ab) = (-1)^{k_a + k_b}$. ■

Теорема 22. Если каноническое разложение числа $a > 1$ имеет вид $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, и θ — мультипликативная функция, то функция $\sum\limits_{d|a} \mu(d) \cdot \theta(d)$ также мультипликативна, и для нее справедлива формула:

$$\sum_{d|a} \mu(d) \cdot \theta(d) = (1 - \theta(p_1)) \cdot (1 - \theta(p_2)) \cdot \ldots \cdot (1 - \theta(p_k)) \qquad (17)$$

(при $a = 1$ правую часть считаем равной 1).

Доказательство. Функция $\theta_1(a) = \mu(a) \cdot \theta(a)$ мультипликативна, поскольку является произведением мультипликативных функций. Поэтому, в силу теоремы 20, функция $\sum\limits_{d|a} \mu(d) \cdot \theta(d)$ также мультипликативна. Формула (13) дает для нее выражение (17), поскольку $\theta_1(p_i) = (-1)^1 \theta(p_i) = -\theta(p_i))$; $\theta_1(p_i^s) = 0 \cdot \theta(p_i^s) = 0$ при $s > 1$. ■

Следствие 1. Если в (17) положить $\theta(a) = a^0 = 1$ для всех a, то получаем формулу для суммы значений функции Мёбиуса, распространенной на все делители числа:

$$M_0(a) = \sum_{d|a} \mu(d) = \begin{cases} 0, \text{если } a > 1, \\ 1, \text{если } a = 1 \end{cases}. \qquad (18)$$

В силу теоремы 20 функция $M_0(a)$ является мультипликативной.

Примеры

1. Если $a = p$ — простое число, то множество его делителей d имеет вид $\{1, p\}$. На этом множестве функция Мёбиуса принимает значения: $\mu(1) = 1$; $\mu(p) = (-1)^1 = -1$. Сумма этих значений равна нулю: $1 + (-1) = 0$.

2. Если $a = p^2$, где p — простое число, то множество делителей числа a имеет вид $\{1, p, p^2\}$. При этом

$\mu(1) = 1$; $\mu(p) = -1$; $\mu(p^2) = 0$.

Сумма значений равна нулю: $1 + (-1) + 0 = 0$.

3. Если $a = pq$, где p, q — простые, $p \neq q$, то множество делителей имеет вид $\{1, p, q, pq\}$. При этом

$$\mu(1)=1;\ \mu(p)=-1;\ \mu(q)=-1;\ \mu(pq)=(-1)^2=1.$$

Сумма значений равна нулю: $1+(-1)+(-1)+(-1)^2=0$.

4. Если $a=p^2q$, где p,q — простые, то множество делителей имеет вид $\{1,\ p,\ p^2,\ q,\ pq,\ p^2q\}$. При этом

$$\mu(1)=1;\ \mu(p)=-1;\ \mu(p^2)=0;\ \mu(q)=-1;\ \mu(pq)=(-1)^2=1;\ \mu(p^2q)=0.$$

Сумма значений равна нулю: $1+(-1)+0+(-1)+(-1)^2+0=0$.

Следствие 2. Если в (17) положить $\theta(d)=d^{-1}=\dfrac{1}{d}$, то получаем еще одну мультипликативную функцию:

$$a)=\sum_{d|a}\frac{\mu(d)}{d}=\begin{cases}(1-\dfrac{1}{p_1})(1-\dfrac{1}{p_2})...(1-\dfrac{1}{p_k}),\ \text{если } a>1,\\ 1,\ \text{если } a=1\end{cases} \qquad (19)$$

Следствие 3. Примем в формуле (18) в качестве a число $\delta_x=(x,a)$ — НОД чисел x и a.

Если $\delta_x=1$, то есть x и a взаимно просты, то единственным делителем числа δ_x является $d=1$, и $\mu(1)=1$, так что

$$A_x=\sum_{d|\delta_x}\mu(d)=1. \qquad (*)$$

Если же $\delta_x>1$, то есть x и a не взаимно просты, то по (18):

$$A_x=\sum_{d|\delta_x}\mu(d)=0. \qquad (**)$$

Просуммируем числа A_x по всем $x=1,2,...,a-1$. Тогда, в силу (*), число единиц, вошедших в сумму, равно числу $\varphi(a)$ тех x из указанного набора, которые взаимно просты с a; остальные слагаемые, в силу (**), равны нулю. В результате

$$\sum_{x=1}^{a-1}A_x=\varphi(a),$$

или

$$\sum_{x=1}^{a-1}\left(\sum_{d|\delta_x}\mu(d)\right)=\varphi(a). \qquad (20)$$

2.4. Функция Эйлера

Определение. Функция Эйлера $\varphi(n)$ задается на $\mathbb{N}$ правилом: $\varphi(1)=1$; при $n\geq 2$ $\varphi(n)$ есть количество натуральных чисел, меньших n и взаимно простых с n.

Примеры

$\varphi(1)=1,\quad \varphi(2)=1,\quad \varphi(3)=2,$
$\varphi(4)=2,\quad \varphi(5)=4,\quad \varphi(6)=2,$
$\varphi(7)=6,\quad \varphi(8)=4,\quad \varphi(9)=6,$
$\varphi(10)=4,\quad \varphi(11)=10,\quad \varphi(12)=4.$

Если p простое число, то все натуральные числа, ему предшествующие, взаимно просты с p, так что $\varphi(p)=p-1$.

Теорема 23 (формула для функции Эйлера). Если $a=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ — каноническое разложение числа a, то

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right). \qquad (21)$$

Доказательство. Рассмотрим выражение (20). Если $d\,|\,(x,a)$ при некотором $x\in\{1,2,...,a-1\}$, то $d\,|\,a$. Таким образом, в (20) участвуют только такие слагаемые $\mu(d)$, у которых d является делителем a.

Обратно, каждый делитель d числа a появляется в левой части (20) при некоторых $x\in\{1,2,...,a-1\}$, например, при $x=d$, так как $d\,|\,(d,a)=d$.

Остается выяснить, сколько раз каждое слагаемое $\mu(d)$ встречается в левой части (20). Число d является делителем чисел $(d,a),(2d,a),...,(td,a)$, где $t=\frac{a}{d}$.

Следовательно,

$$\varphi(a)=\sum_{d|a}\frac{a}{d}\mu(d)=a\sum_{d|a}\frac{\mu(d)}{d}=a(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$$

(последнее равенство — на основании (19)). ■

Следствие. Если в формуле (21) множитель $p_1^{\alpha_1}$ числа a внести в первую скобку, множитель $p_2^{\alpha_2}$ во вторую скобку и т. д., получим еще одну формулу для $\varphi(a)$:

$$\varphi(a) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1})...(p_k^{\alpha_k} - p_k^{\alpha_k - 1}). \qquad (22)$$

В частности, если $a = p^{\alpha}$ — степень простого числа, то

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}. \qquad (23)$$

Теорема 24. Функция Эйлера мультипликативна.

Доказательство. $\varphi(a) = a\sum\limits_{d|a}\dfrac{\mu(d)}{d} = a\mathrm{M}_{-1}(a)$ — произведение мультипликативных функций. ■

Теорема 25. $\sum\limits_{d|a}\varphi(d) = a$. (24)

Доказательство. Пусть $a = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$. Возьмем в формуле (13) в качестве мультипликативной функции θ функцию Эйлера φ и применим к значениям $\varphi(p_i^j)$ формулу (23):

$$\sum_{d|a}\varphi(d) = \prod_{i=1}^{k}(1 + \varphi(p_i) + \varphi(p_i^2) + ... + \varphi(p_i^{\alpha_i})) =$$

$$= \prod_{i=1}^{k}(1 + (p_i - 1) + (p_i^2 - p_i) + ... + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})) =$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k} = a. \blacksquare$$

Примеры

1. Число $a = 12$ имеет делители $1, 2, 3, 4, 6, 12 \Rightarrow$

$$\Rightarrow \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) =$$

$$= 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

2. Простое число $a = 101$ имеет делители $1, 101 \Rightarrow$

$$\Rightarrow \varphi(1) + \varphi(101) = 1 + (101 - 1) = 101.$$

3. Число $2^6 = 64$ имеет делители $1, 2, 4, 8, 16, 32, 64 \Rightarrow$

$$\Rightarrow \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) + \varphi(16) + \varphi(32) + \varphi(64) =$$

$$= 1 + 1 + 2 + 4 + 8 + 16 + 32 = 64.$$

ГЛАВА 3. СРАВНЕНИЯ

3.1. Исходные понятия и теоремы

Будем рассматривать целые числа $a, b, \ldots$ и остатки от деления их на натуральное число $m > 1$.

Определение. Числа a и b называются сравнимыми по модулю m, если они имеют одинаковые остатки от деления на m.

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

Простейшие свойства сравнений

1. $a \equiv b (\mathrm{mod}\, m) \Leftrightarrow m \mid (a - b)$,

2. $a \equiv b (\mathrm{mod}\, m) \Leftrightarrow a = b + mk$, где $k \in \mathbb{Z}$.

Действительно, пусть $a = mt + r_1,\ b = ms + r_2$. Тогда:

$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow r_1 = r_2 \Leftrightarrow a - b = mt - ms = m(t - s)$; теперь достаточно положить $k = t - s$. ■

Ряд свойств сравнений аналогичен соответствующим свойствам равенств.

3. Пусть $a \equiv c (\mathrm{mod}\, m)$ и $b \equiv c (\mathrm{mod}\, m)$. Тогда $a \equiv b (\mathrm{mod}\, m)$, то есть два числа, сравнимые с третьим, сравнимы между собой.

Действительно, $a = c + mt,\ b = c + ms \Rightarrow a - b = m(t - s)$, то есть $m \mid (a - b)$. ■

4. Сравнения можно почленно складывать:

$a_1 \equiv b_1 (\mathrm{mod}\, m), a_2 \equiv b_2 (\mathrm{mod}\, m) \Rightarrow a_1 + a_2 \equiv (b_1 + b_2) (\mathrm{mod}\, m)$.

Действительно, $a_1 - b_1 = mt_1;\ a_2 - b_2 = mt_2$; сложение этих равенств дает: $(a_1 + a_2) - (b_1 + b_2) = m(t_1 + t_2)$. ■

5. $a \equiv b (\mathrm{mod}\, m) \Rightarrow a + mt \equiv b (\mathrm{mod}\, m),\ t \in \mathbb{Z}$.

Действительно, достаточно сложить сравнения $a \equiv b (\mathrm{mod}\, m)$ и $mt \equiv 0 (\mathrm{mod}\, m)$. ■

6. Сравнения можно почленно перемножать:

$a_1 \equiv b_1 (\mathrm{mod}\, m), a_2 \equiv b_2 (\mathrm{mod}\, m) \Rightarrow a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\, m)$.

Действительно, $a_1 = b_1 + mk_1,\ a_2 = b_2 + mk_2 \ \Rightarrow$

$\Rightarrow a_1 a_2 = (b_1 + mk_1)(b_2 + mk_2) = b_1 b_2 + m(b_1 k_2 + b_2 k_1 + k_1 k_2)$. ■

7. Обе части сравнения можно возводить в степень:

$a \equiv b(\mathrm{mod}\, m) \ \Rightarrow\ a^n \equiv b^n (\mathrm{mod}\, m)$.

Действительно, достаточно взять произведение n экземпляров исходного сравнения. ■

8. Обе части сравнения можно умножить на одно и то же число:

$a \equiv b(\mathrm{mod}\, m) \ \Rightarrow\ ac \equiv bc(\mathrm{mod}\, m)$.

Действительно, достаточно взять произведение исходного сравнения и очевидного сравнения $c \equiv c(\mathrm{mod}\, m)$. ■

9. Обе части сравнения можно сокращать на одно и то же число, взаимное простое с модулем:

Если $(c,m) = 1$ и $ac \equiv bc(\mathrm{mod}\, m)$, то $a \equiv b(\mathrm{mod}\, m)$.

Действительно, $m \mid (ac - bc) \Rightarrow m \mid c(a-b)$. Отсюда (по свойству 5 п. 1.6) $m \mid (a-b)$. ■

10. Если $ak \equiv bk(\mathrm{mod}\, mk)$, то $a \equiv b(\mathrm{mod}\, m)$, то есть, обе части сравнения вместе с модулем можно разделить на одно и то же число.

Действительно, $ak - bk = tmk \ \Rightarrow\ a - b = tm$. ■

11. Пусть $M = m(m_1, m_2, ..., m_n)$ — НОК. Если

$$\begin{cases} a \equiv b(\mathrm{mod}\, m_1), \\ a \equiv b(\mathrm{mod}\, m_2), \\ \cdots \\ a \equiv b(\mathrm{mod}\, m_n), \end{cases}$$

то $a \equiv b(\mathrm{mod}\, M)$, то есть, если сравнение имеет место по нескольким модулям, то оно имеет место по модулю их НОК.

Действительно, по следствию к теореме 16 (п. 1.7), разность $a - b$, делясь на $m_1, ..., m_n$, делится и на их НОК $m(m_1, ..., m_n)$. ■

12. Пусть $a \equiv b(\mathrm{mod}\, m)$ и $d \mid m$. Тогда $a \equiv b(\mathrm{mod}\, d)$, то есть, если сравнение имеет место по модулю m, то оно имеет место по модулю любого его делителя $d > 1$.

Действительно, если $a-b=km$ и $m=td$, то $a-b=(kt)d$. ■

13. Если $a \equiv b(\mathrm{mod}\, m)$, $d \mid a$ и $d \mid m$, то $d \mid b$, то есть, если одна часть сравнения и модуль делятся на d, то и другая часть сравнения делится на d.

Действительно, пусть $a=kd$, $m=td$. Тогда

$b=a+lm=kd+ltd=(k+lt)d$. ■

3.2. Полная и приведенная системы вычетов

Определение. Классом вычетов по модулю m называется совокупность целых чисел, сравнимых по модулю m, то есть имеющих при делении на m одинаковый остаток. Числа, входящие в один и тот же класс, называются вычетами по модулю m.

Пример

Множество

$\overline{4}=\{...,-14,-8,-2,4,10,16,...\}=\{4\pm 6k, k=1,2,3,...\}$

чисел, дающих при деление на 6 остаток 4, образует класс вычетов по модулю 6.

$\overline{0}=\{...,-18,-12,-6,0,6,12,18,...\}=\{0\pm 6k, k=1,2,3,...\}$

чисел, делящихся на 6 (дающих при деление на 6 остаток 0), образует еще один класс вычетов по модулю 6.

При делении на m с остатком возможны остатки $0,1,...,m-1$, количество которых равно m. Поэтому имеется m различных классов вычетов по модулю m. Их объединение дает множество всех целых чисел.

Определение. Полной системой вычетов по модулю m называется набор m чисел, лежащих в разных классах вычетов по этому модулю.

Пример

Числа $\{12, 25, -10, -21, 34, 5\}$ образуют полную систему вычетов по модулю 6, поскольку при делении на 6 они дают 6 различных остатков: соответственно, $0, 1, 2, 3, 4, 5$. В свою очередь, сами эти

остатки от деления также образуют полную систему вычетов $\{0, 1, 2, 3, 4, 5\}$.

Определение. Приведенной системой вычетов называется совокупность всех чисел полной системы, которые взаимно просты с модулем.

Обычно приведенную систему образуют из наименьших положительных остатков от деления на m.

Примеры

1. Приведенная система вычетов по модулю $m = 5$: $\{1, 2, 3, 4\}$.

2. Приведенная система вычетов по модулю $m = 42 = 2 \cdot 3 \cdot 7$ получается исключением из множества: $1, 2, ..., 41$ чисел, кратных простым множителям модуля; в результате получаем систему:

$\{1,5,11,13,17,19,23,25,29,31,37,41\}$.

Замечания. 1. Количество чисел приведенной системы вычетов выражается функцией Эйлера $\varphi(m)$.

2. Числа 1 и m–1 взаимно просты с модулем m и могут быть включены в приведенную систему вычетов.

3. Если модуль p является простым числом, то приведенная система вычетов $\{1, 2, ..., p-1\}$ получается исключением нуля из полной системы вычетов.

4. Любые $\varphi(m)$ попарно не сравнимых по модулю m чисел, взаимно простых с m, образуют приведенную систему вычетов.

Теорема 26. Пусть $(a, m) = 1$.

1. Если x пробегает полную систему вычетов по модулю m, то $ax + b$ 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 модулю m.

Доказательство. 1. Количество чисел $ax + b$ совпадает с количеством чисел x. Остается проверить, что они попарно несравнимы по модулю m. Если x_1 и x_2 — различные числа из полной системы вы-

четов, то из $ax_1 + b \equiv ax_2 + b$ следовало бы, что $m \mid (ax_1 + b) - (ax_2 + b) = a(x_1 - x_2)$; но тогда в силу свойства 5 взаимной простоты (п. 1.5) $m \mid x_1 - x_2$, что невозможно.

2. По свойству 2 взаимной простоты (п. 1.5) из $(a,m) = 1$ и $(x,m) = 1$ следует $(ax,m) = 1$. ■

3.3. Теоремы Эйлера и Ферма

Теорема 27. (Эйлера). Если $m > 1$ и $(a,m) = 1$, то имеет место сравнение

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m). \qquad (25)$$

Доказательство. Положим $c = \varphi(m)$. Пусть $x_1, x_2, ..., x_c$ — приведенная система вычетов по модулю m. По теореме 26 числа $ax_1, ax_2, ..., ax_c$ также образуют приведенную систему вычетов, возможно, в другом порядке. Поэтому

$$ax_1 \equiv x_{j_1} (\mathrm{mod}\, m),\ ax_2 \equiv x_{j_2} (\mathrm{mod}\, m), ..., ax_c \equiv x_{j_c} (\mathrm{mod}\, m).$$

Перемножая почленно эти сравнения, получим:

$$a^c x_1 x_2 ... x_c \equiv x_{j_1} x_{j_2} ... x_{j_c} (\mathrm{mod}\, m), \qquad (*)$$

причем оба произведения значений x совпадают, поскольку содержат одни и те же множители: $x_1 x_2 ... x_c = x_{j_1} x_{j_2} ... x_{j_c} = b$. При этом, по свойству 3 взаимной простоты (п. 1.5), $(b,m) = 1$. Сокращая сравнение (*) на b, получим утверждение теоремы. ■

Следствие 1 (малая теорема Ферма). Если p простое число и $(a,p) = 1$ (то есть a не делится на p), то

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p). \qquad (26)$$

Доказательство. Поскольку $\varphi(p) = p - 1$, то утверждение теоремы следует из (25). ■

Следствие 2. Если p простое число, то при любом целом a (уже без требования взаимной простоты a и p)

$$a^p \equiv a(\mathrm{mod}\, p)\,. \qquad (27)$$

Доказательство. Если $(a, p) = 1$, то (27) следует из (26) при умножении обеих частей сравнения на *a*. Если же *a* делится на *p*, то $a \equiv 0(\mathrm{mod}\, p)$ и $a^p \equiv 0(\mathrm{mod}\, p)$, откуда $a^p \equiv a(\mathrm{mod}\, p)$ по третьему свойству сравнений (п. 3.1). ■

3.4. Китайская теорема об остатках

Теорема 28. Пусть натуральные числа $m_1, m_2, ..., m_n$ попарно взаимно просты. Тогда:

1. Для любых целых чисел $r_1, r_2, ..., r_n$ таких, что $0 \le r_i < m_i$, $i = 1,2,...,n$, найдется число *N*, которое при делении на m_i дает остаток r_i.

2. Если числа N_1 и N_2 обладают указанным свойством, то $N_1 \equiv N_2(\mathrm{mod}\, m_1 m_2 ... m_n)$.

Замечание. Утверждение теоремы означает, что откладывая на числовой оси от начальных точек $r_1, r_2, ..., r_n$ последовательно отрезки длиной $m_1, m_2, ..., m_n$ соответственно, можно получить одну и ту же точку *N* числовой оси (рис. 7).

Доказательство. 1. Проведем индукцию по числу *n*.

При $n = 1$ имеется единственное число m_1 и единственное число r_1. В качестве *N* можно взять любое число вида $m_1 t + r_1$.

Пусть $k \ge 1$ и теорема верна при $n = k$. Докажем, что тогда она верна при $n = k + 1$. По предположению, существует число *M*, дающее при делении на m_i остаток r_i при $i = 1,2,...,k$. Положим $\delta = m_1 m_2 ... m_k$ и рассмотрим числа

$$M, M + \delta, M + 2\delta, ..., M + (m_{k+1} - 1)\delta\ . \qquad (*)$$

Убедимся, что среди чисел (*) найдется число *N*, дающее при делении на m_{k+1} остаток r_{k+1}. Количество чисел в ряду (*) равно m_{k+1}, как и количество возможных неотрицательных остатков при их делении на m_{k+1}. Если бы среди этих остатков нашлись одинаковые, то мы имели бы:

$$M + t\delta = m_{k+1}x + r;\ M + s\delta = m_{k+1}y + r,\ t < s,$$

так что разность $(M + t\delta) - (M + s\delta) = (t - s)\delta$ делилась бы на m_{k+1}. При этом δ взаимно просто с m_{k+1} по свойству 2 взаимной простоты (п. 1.6)). Тогда $t - s$ должно делиться на m_{k+1}, что невозможно, так как из $0 \le t < s < m_{k+1}$, следует $0 < |t - s| < m_{k+1}$.

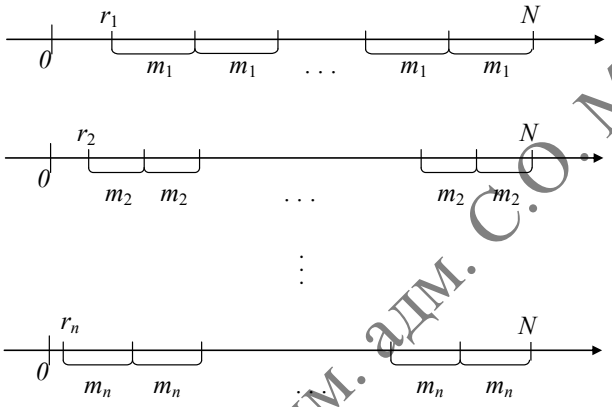

Рис. 7. Иллюстрация замечания к теореме 28 (с. 45)

Итак, числа ряда (*) дают все возможные остатки от деления на m_{k+1}. Значит, одно из этих чисел, N, дает остаток r_{k+1}.

При делении на $m_1, m_2, ..., m_k$ число N, в силу (*), дает те же остатки, что и M, то есть остатки $r_1, r_2, ..., r_k$.

2. Пусть два числа N_1 и N_2 дают при делении на каждое m_i остаток r_i. Тогда $N_1 - N_2 \equiv 0 (\mathrm{mod}\, m_i)$, $i = 1,2,...,n$. По следствию к теореме 16 (п. 1.7) $N_1 - N_2 \equiv 0 (\mathrm{mod}\, m_1 m_2 ... m_n)$. ■

ГЛАВА 4. РЕШЕНИЕ СРАВНЕНИЙ

4.1. Исходные понятия

Пусть $f(x) = ax^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами, и a не делится на m.

Определение. Сравнение

$$f(x) \equiv 0 (\mathrm{mod}\, m) \qquad (28)$$

называется сравнением степени n.

Из свойств сравнений (п. 3.1) следует, что если число x_1 удовлетворяет сравнению (28), и $x_2 \equiv x_1 (\mathrm{mod}\, m)$, то x_2 также удовлетворяет этому сравнению. Таким образом, ему удовлетворяет весь класс вычетов по модулю m.

Определение. Решением сравнения (28) называется класс вычетов по модулю m, которые удовлетворяют этому сравнению.

Последнее будет иметь столько решений, сколько вычетов полной системы ему удовлетворяют.

Определение. Два сравнения $f(x) \equiv 0 (\mathrm{mod}\, m)$ и $g(x) \equiv 0 (\mathrm{mod}\, m)$ называются равносильными, если их решениями являются одни и те же классы вычетов.

Примеры

1. Среди чисел $0, 1, 2, 3, 4, 5, 6$ полной системы вычетов по модулю $m = 7$ сравнению пятой степени $x^5 + 2x + 3 \equiv 0 (\mathrm{mod}\, 7)$ удовлетворяют $x = 3$ и $x = 6$. Сравнение имеет два решения: $x \equiv 3 (\mathrm{mod}\, 7)$ и $x \equiv 6 (\mathrm{mod}\, 7)$.

2. Сравнению $x^5 + x + 1 \equiv 0 (\mathrm{mod}\, 7)$ удовлетворяют $x = 2$ и $x = 4$. Сравнение имеет два решения: $x \equiv 2 (\mathrm{mod}\, 7)$ и $x \equiv 4 (\mathrm{mod}\, 7)$.

Замечание. Можно доказать (см., например, [4, п. IV.4]), что в случае простого модуля p справедлива следующая теорема.

Теорема 29. Если сравнение степени n

$$ax^n + a_1x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\, p)$$

имеет более n решений, то все его коэффициенты кратны p.

Следствие. Сравнение $ax^n + a_1x^{n-1} + ... + a_n \equiv 0(\mathrm{mod}\, p)$ по простому модулю p, где $(a, p) = 1$, имеет не более n решений.

Теорема 30. Пусть p — простое число. Тогда произвольное сравнение $f(x) \equiv 0(\mathrm{mod}\, p)$ степени n равносильно некоторому сравнению, степень которого не превышает $p - 1$.

Доказательство. Если степень $n \geq p$, то, деля многочлен $f(x)$ на многочлен $x^p - x$ с остатком, имеем:

$$f(x) = (x^p - x)q(x) + r(x);$$

при этом $x^p - x \equiv 0(\mathrm{mod}\, p)$ при всех целых x. Отсюда

$f(x) \equiv 0(\mathrm{mod}\, p) \Leftrightarrow r(x) \equiv 0(\mathrm{mod}\, p)$. ■

4.2. Сравнения первой степени

При $n = 1$ сравнение (28) преобразуется к равносильному

$$ax \equiv b(\mathrm{mod}\, m) \qquad (29)$$

путем перенесения свободного члена в правую часть.

1. Пусть сначала $(a, m) = 1$, то есть a и m взаимно просты. Когда x пробегает полную систему вычетов по модулю m, то ax также пробегает полную систему вычетов (п. 3.2, теорема 26). Единственный элемент этой полной системы сравним по модулю m с b. Таким образом, если $(a, m) = 1$, то сравнение (29) имеет единственное решение.

2. Пусть теперь $(a, m) = d > 1$. Если сравнение (29) имеет решение x_1, то по свойству 13 сравнений (п. 3.1) из $d \mid a$ (а значит, и $d \mid ax_1$) и $d \mid m$, следует $d \mid b$. В противном случае сравнение не имеет решений. Пусть $a = a_1d$, $b = b_1d$, $m = m_1d$. Сокращая все члены сравнения (28) на d, получим, что x_1 является единственным решением сравнения $a_1x \equiv b_1(\mathrm{mod}\, m_1)$, где уже $(a_1, m_1) = 1$.

Обратно, если x_1 является решением сравнения

$$a_1x \equiv b_1(\mathrm{mod}\, m_1), \qquad (30)$$

где $(a_1, m_1) = 1$, то, умножая все члены сравнения

$$a_1 x_1 \equiv b_1 (\mathrm{mod}\, m_1)$$

на d, получаем, что x_1 является решением сравнения (29).

Пусть x_1 — наименьший неотрицательный вычет решения сравнения (30) по модулю m_1. Тогда остальные его решения имеют вид:

$$x \equiv x_1 (\mathrm{mod}\, m_1). \qquad (31)$$

В полную систему наименьших неотрицательных вычетов по модулю m, то есть в совокупность $\{0, 1, 2, ..., m-1\}$, из них попадают числа

$$x_1, x_1+m_1, x_1+2m_1, ..., x_1+(d-1)m_1,$$

и их количество равно d. Все они меньше $m = dm_1$ и потому попарно не сравнимы по модулю m. При этом они являются решениями сравнения (29).

Вывод: 1. Если $(a,m) = d$ и b не делится на d, то сравнение (29) не имеет решений. 2. Если $d \mid b$, то сравнение имеет d решений — различных классов вычетов по модулю m; представителями этих классов являются числа

$$x_1, x_1+m_1, x_1+2m_1, ..., x_1+(d-1)m_1,$$

где x_1 — наименьшее неотрицательное число, удовлетворяющее сравнению (30).

Пример

Решим сравнение $25x \equiv 15 (\mathrm{mod}\, 55)$. Здесь $d = (25, 55) = 5$, и свободный член 15 также делится на 5. Деля все члены на 5, приходим к сравнению $5x \equiv 3 (\mathrm{mod}\, 11)$. Подставляя в сравнение последовательно числа из полной системы вычетов $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, находим, что единственный класс вычетов, являющийся его решением, содержит число $x_1 = 5$. Решениями исходного сравнения являются числа

$$5,\ 5+11=16,\ 5+2\cdot 11=27,\ 5+3\cdot 11=38,\ 5+4\cdot 11=49.$$

4.3. Применение непрерывных дробей к решению сравнений первой степени

Единственное решение сравнения $ax \equiv b (\mathrm{mod}\, m)$ в случае взаимной простоты чисел a и m можно найти методом, использующим раз-

ложение рационального числа $\frac{m}{a}$ в конечную непрерывную дробь. Пусть

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

Тогда $\frac{m}{a} = \frac{P_n}{Q_n}$ — последняя подходящая дробь. Ей предшествует подходящая дробь $\frac{P_{n-1}}{Q_{n-1}}$, причем, по свойству 1 подходящих дробей (см. п. 1.8, Г):

$$mQ_{n-1} - aP_{n-1} = (-1)^n \Rightarrow aP_{n-1} \equiv (-1)^{n-1} (\mathrm{mod}\, m).$$

Умножая обе части последнего сравнения на $(-1)^{n-1} b$ и учтя, что $(-1)^{n-1} \cdot (-1)^{n-1} = 1$, получим:

$$a \cdot (-1)^{n-1} P_{n-1} b \equiv b (\mathrm{mod}\, m).$$

Таким образом, решением сравнения является класс вычетов

$$x \equiv (-1)^{n-1} P_{n-1} b (\mathrm{mod}\, m).$$

Пример

Решим сравнение

$$222x \equiv 150 (\mathrm{mod}\, 642). \qquad (*)$$

Имеем $(222, 642) = 6$, причем свободный член 150 также делится на 6. Значит, сравнение имеет шесть решений. Сокращая все члены на 6, приходим к сравнению

$$37x \equiv 25 (\mathrm{mod}\, 107). \qquad (**)$$

Теперь вычислим числители P_i подходящих дробей в разложении $\frac{107}{37}$ в непрерывную дробь с помощью делений с остатком и рекуррентных соотношений (9) и (10).

Имеем: $m = 107,\ a = r_1 = 37$. Свободный член сравнения $b = 25$. Далее:

$$107 = 37 \cdot 2 + 33 \Rightarrow r_1 = 37,\ q_1 = 2,\ P_0 = 1,\ Q_0 = 0, P_1 = 2,\ Q_1 = 1,$$
$$r_2 = 33;$$

$$37 = 33 \cdot 1 + 4 \Rightarrow q_2 = 1,\ r_3 = 4;$$
$$P_2 = q_2 P_1 + P_0 = 1 \cdot 2 + 1 = 3;$$

$$33 = 4 \cdot 8 + 1 \Rightarrow q_3 = 8,\ r_4 = 1;$$
$$P_3 = q_3 P_2 + P_1 = 8 \cdot 3 + 2 = 26;$$

$$4 = 4 \cdot 1 + 0 \Rightarrow q_4 = 1,\ r_5 = 0;$$
$$P_4 = q_4 P_3 + P_2 = 4 \cdot 26 + 3 = 107.$$

Итак, $n = 4,\ n - 1 = 3,\ (-1)^3 = -1$. Числитель предпоследней подходящей дроби $P_3 = 26$. Единственное решение сравнения $37x \equiv 25 (\mathrm{mod}\, 107)$ имеет вид:

$$x \equiv -26 \cdot 25 (\mathrm{mod}\, 107) = -650 (\mathrm{mod}\, 107).$$

Наименьший неотрицательный вычет класса, содержащего (–650) получим при делении (–650) на 107 с остатком:

$$-650 = 107 \cdot (-7) + 99.$$

Окончательная запись решения сравнения (**): $x \equiv 99 (\mathrm{mod}\, 107)$. Остается получить из него решения исходного сравнения (*):

$$x \equiv 99 (\mathrm{mod}\, 642);$$
$$x \equiv 99 + 1 \cdot 107 (\mathrm{mod}\, 642) \Rightarrow x \equiv 206 (\mathrm{mod}\, 642);$$
$$x \equiv 99 + 2 \cdot 107 (\mathrm{mod}\, 642) \Rightarrow x \equiv 313 (\mathrm{mod}\, 642);$$
$$x \equiv 99 + 3 \cdot 107 (\mathrm{mod}\, 642) \Rightarrow x \equiv 420 (\mathrm{mod}\, 642);$$

$x \equiv 99 + 4 \cdot 107 (\mathrm{mod}\, 642) \Rightarrow x \equiv 527 (\mathrm{mod}\, 642)$;

$x \equiv 99 + 5 \cdot 107 (\mathrm{mod}\, 642) \Rightarrow x \equiv 634 (\mathrm{mod}\, 642)$.

4.4. Применение теоремы Эйлера к решению сравнений первой степени

Теорема 31. Если $(a, m) = 1$, то решением сравнения $ax \equiv b (\mathrm{mod}\, m)$ является класс вычетов $x \equiv b a^{\varphi(m)-1} (\mathrm{mod}\, m)$, где φ — функция Эйлера.

Доказательство. По теореме Эйлера $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m) \Rightarrow$

$\Rightarrow a^{\varphi(m)} b \equiv b (\mathrm{mod}\, m) \Rightarrow a a^{\varphi(m)-1} b \equiv b (\mathrm{mod}\, m)$. ■

Пример

Решим сравнение $53x \equiv 7 (\mathrm{mod}\, 6)$. Здесь

$(53, 6) = 1$; $\varphi(6) = 2$; $a^{\varphi(m)-1} = 53$; $x \equiv 7 \cdot 53 (\mathrm{mod}\, 6) \equiv 5 (\mathrm{mod}\, 6)$.

4.5. Системы сравнений первой степени

Пусть модули $m_1, m_2, ..., m_k$ различны и попарно взаимно просты. Рассмотрим систему сравнений

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1) \\ x \equiv b_2 (\mathrm{mod}\, m_2) \\ \ldots \\ x \equiv b_k (\mathrm{mod}\, m_k). \end{cases} \qquad (32)$$

В качестве свободных членов этих сравнений b_i можно взять наименьшие неотрицательные вычеты по соответствующим модулям m_i. Тогда существование решения системы следует из китайской теоремы об остатках (п. 3.4).

Введем числа:

$$M_1 = m_2 m_3 ... m_k, \; M_2 = m_1 m_3 ... m_k, \; ..., \; M_k = m_1 m_2 ... m_{k-1}.$$

Выберем числа $M_1', M_2', ..., M_k'$ так, чтобы при $i = 1, 2, ..., k$ выполнялись сравнения $M_i M_i' \equiv 1 (\mathrm{mod}\, m_i)$. Заметим, что поскольку $(M_i, m_i) = 1$, то M_i' можно получить, решая сравнение $M_i y \equiv 1 (\mathrm{mod}\, m_i)$.

Теорема 32. Пусть $x_0 = M_1M_1'b_1 + M_2M_2'b_2 + ... + M_kM_k'b_k$. Тогда единственным решением системы (32) является класс вычетов $x \equiv x_0 (\mathrm{mod}\, m_1m_2...m_k)$.

Доказательство. Все M_j делятся на m_i при $j \neq i$. Поэтому

$$x_0 \equiv M_iM_i'b_i (\mathrm{mod}\, m_i).$$

Перемножая сравнения $M_iM_i' \equiv 1(\mathrm{mod}\, m_i)$ и $b_i \equiv b_i(\mathrm{mod}\, m)$, получим:

$$M_iM_i'b_i \equiv b_i(\mathrm{mod}\, m_i) \Rightarrow x_0 \equiv b_i(\mathrm{mod}\, m_i).$$

Итак, класс вычетов $x \equiv x_0(\mathrm{mod}\, m_1m_2...m_k)$ является решением системы (32).

Убедимся теперь в единственности решения. Система (32) равносильна системе

$$\begin{cases} x \equiv x_0(\mathrm{mod}\, m_1) \\ x \equiv x_0(\mathrm{mod}\, m_2) \\ ... \\ x \equiv x_0(\mathrm{mod}\, m_k), \end{cases}$$

которой удовлетворяют те и только те x, для которых выполняется $x \equiv x_0(\mathrm{mod}\, m_1m_2...m_k)$ (см. п. 3.1, свойства 11,12). ■

Пример

Решим систему сравнений

$$\begin{cases} x \equiv 1(\mathrm{mod}\, 6) \\ x \equiv 3(\mathrm{mod}\, 5) \\ x \equiv 2(\mathrm{mod}\, 7). \end{cases}$$

Здесь

$M_1 = m_2m_3 = 5 \cdot 7 = 35$, $M_2 = m_1m_3 = 6 \cdot 7 = 42$,

$M_3 = m_1m_2 = 6 \cdot 5 = 30$, $m_1m_2m_3 = 6 \cdot 5 \cdot 7 = 210$.

Решаем сравнения:

$35M_1' \equiv 1(\mathrm{mod}\, 6) \Rightarrow M_1' = 5$;

$42M_2' \equiv 1(\mathrm{mod}\, 5) \Rightarrow M_2' = 3$;

$30M_3' \equiv 1(\mathrm{mod}\, 7) \Rightarrow M_3' = 4$;

$$x_0 = M_1M_1'b_1 + M_2M_2'b_2 + M_3M_3'b_3 =$$
$$= 35 \cdot 5 \cdot 1 + 42 \cdot 3 \cdot 3 + 30 \cdot 4 \cdot 2 = 793 \equiv 163 (\mathrm{mod}\, 210) .$$

Теорема 33. Если свободные члены $b_1, b_2, .., b_k$ системы (32) независимо друг от друга пробегают полные системы вычетов по модулям $m_1, m_2, ..., m_k$ соответственно, то число

$$x_0 = M_1M_1'b_1 + M_2M_2'b_2 + ... + M_kM_k'b_k = x_0(b_1, b_2, ..., b_k)$$

пробегает полную систему вычетов по модулю $m_1m_2...m_k$.

Доказательство. Количество значений x_0 в соответствии с комбинаторным принципом умножения равно $m_1m_2...m_k$, то есть количеству элементов полной системы вычетов по модулю $m_1m_2...m_k$. Остается убедиться, что эти значения попарно не сравнимы по модулю $m_1m_2...m_k$.

Если $x_0(b_1, b_2, ..., b_k) \equiv x_0(b_1', b_2', ..., b_k') (\mathrm{mod} m_1m_2...m_k)$, то, деля модуль сравнения, например, на $m_2...m_k$, получаем:

$$x_0(b_1, b_2, ..., b_k) \equiv x_0(b_1', b_2', ..., b_k') (\mathrm{mod}\, m_1) .$$

Поскольку m_1 делит $M_2, ..., M_k$, то

$$M_1M_1'b_1 \equiv M_1M_1'b_1' (\mathrm{mod}\, m_1) \Rightarrow b_1 \equiv b_1' (\mathrm{mod}\, m_1) .$$

Аналогично получаются остальные сравнения $b_i \equiv b_i' (\mathrm{mod}\, m_i)$. ■

ГЛАВА 5. СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ

5.1. Квадратичные вычеты и невычеты

Определение. Двучленным сравнением второй степени называется сравнение вида:

$$x^2 \equiv a(\mathrm{mod}\, m);\ (a,m)=1. \qquad (33)$$

Будем рассматривать в качестве модуля сравнения (33) простое число p:

$$x^2 \equiv a(\mathrm{mod}\, p);\ (a,p)=1. \qquad (34)$$

Целью дальнейших рассмотрений является исследование вопроса, при каких a сравнение (34) имеет решения. В случае $p=2$ имеется всего два класса вычетов по модулю 2: четные числа, сравнимые с нулем по модулю 2, и нечетные числа, сравнимые с единицей по модулю 2. Поскольку оба числа 0 и 1 являются квадратами ($0=0^2$, $1=1^2$), то оба класса вычетов являются решениями. Поэтому интерес представляет случай, когда простое $p>2$, который мы в дальнейшем и будем рассматривать.

Тогда $p-1$ — четное число, $\frac{p-1}{2}$ — целое положительное число.

Определение. Число a называется квадратичным вычетом по модулю p, если сравнение (34) имеет решения. В противном случае a называется квадратичным невычетом по модулю p.

Заметим, что условие $(a,p)=1$ предполагает, что a не сравнимо с нулем по модулю p, то есть a не кратно p. В качестве a достаточно рассматривать числа из приведенной системы вычетов по модулю p, например, наименьшие положительные вычеты

$$1, 2, \ldots, p-1$$

или отличные от нуля абсолютно наименьшие вычеты

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}.$$

Пример

Определим, какие из чисел $a=1,2,3,4,5,6$ — представителей приведенной системы вычетов — являются квадратичными вычетами по модулю 7. Рассмотрим квадраты всех представителей:

$1^2 = 1 \equiv 1 (\mathrm{mod}\, 7)$

$2^2 = 4 \equiv 4 (\mathrm{mod}\, 7)$

$3^2 = 9 \equiv 2 (\mathrm{mod}\, 7)$

$4^2 = 16 \equiv 2 (\mathrm{mod}\, 7)$

$5^2 = 25 \equiv 4 (\mathrm{mod}\, 7)$

$6^2 = 36 \equiv 1 (\mathrm{mod}\, 7)$

С квадратами оказались сравнимы числа $1, 2, 4$ — они являются квадратичными вычетами по модулю 7, а остальные числа приведенной системы вычетов, то есть $3, 5, 6$ — квадратичными невычетами.

Замечание. Пример показывает:

1) среди классов вычетов по модулю p имеется $\frac{p-1}{2}$ квадратичных вычетов и такое же число невычетов;

2) все квадратичные вычеты проявляются при возведении в квадрат чисел из первой половины набора $1, 2, ..., p-1$;

3) если a оказывается вычетом, то сравнение (34) имеет два решения.

Последнее следует из того, что при условии $x_1^2 \equiv a (\mathrm{mod}\, p)$ также и $(-x_1)^2 = x_1^2 \equiv a (\mathrm{mod}\, p)$; при этом x_1 и $-x_1$ входят в разные классы вычетов по модулю p, действительно:

$$x_1 \equiv -x_1 (\mathrm{mod}\, p) \Rightarrow 2x_1 \equiv 0 (\mathrm{mod}\, p),$$

что противоречит условию $(a, p) = 1$.

Теорема 34. Среди чисел приведенной системы абсолютно наименьших вычетов по модулю p

$$-\frac{p-1}{2}, ..., -2, -1, 1, 2, ..., \frac{p-1}{2}$$

имеется $\frac{p-1}{2}$ квадратичных вычетов, сравнимых с числами $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$, и такое же число квадратичных невычетов.

Доказательство. Те числа приведенной системы

$$-\frac{p-1}{2},...,-2,\ -1,1,2,...,\frac{p-1}{2}, \tag{35}$$

которые сравнимы по модулю p с $1^2, 2^2,..., \left(\frac{p-1}{2}\right)^2$, по определению являются квадратичными вычетами. Они лежат в разных классах вычетов, поскольку из условия

$$u^2 \equiv v^2 (\mathrm{mod}\, p),\ 1 \le u < v \le \frac{p-1}{2}$$

следовало бы

$$u^2 - v^2 \equiv 0(\mathrm{mod}\, p) \Rightarrow (u-v)(u+v) \equiv 0(\mathrm{mod}\, p) \Rightarrow$$

$$\Rightarrow p \mid u+v \ \text{ или } \ p \mid u-v,$$

что невозможно, так как

$$-(p-1) < u \pm v < p-1,\ u \pm v \neq 0. \ \blacksquare$$

Теорема 35 (критерий Эйлера). 1. Для того чтобы a являлось квадратичным вычетом, необходимо и достаточно выполнение условия

$$a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p). \tag{36}$$

2. Для того, чтобы a являлось квадратичным невычетом, необходимо и достаточно выполнение условия

$$a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p). \tag{37}$$

Доказательство. По малой теореме Ферма

$$a^{p-1} \equiv 1(\mathrm{mod}\, p) \Rightarrow\ a^{p-1} - 1 \equiv 0(\mathrm{mod}\, p) \Rightarrow$$

(поскольку $p-1$ — четное число, применима формула разности квадратов)

$$\Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(\mathrm{mod}\, p).$$

На p может делиться только один из сомножителей этого сравнения, так как их разность, равная 2, не делится на p. Следовательно,

каждое a из приведенной системы (35) является либо решением сравнения

$$x^{\frac{p-1}{2}} - 1 \equiv 0 (\mathrm{mod}\, p), \qquad (*)$$

либо решением сравнения

$$x^{\frac{p-1}{2}} + 1 \equiv 0 (\mathrm{mod}\, p), \qquad (**)$$

причем число решений каждого из сравнений не превышает степени сравнения $\frac{p-1}{2}$.

Если теперь a является квадратичным вычетом, то при некотором x имеет место сравнение

$$a \equiv x^2 (\mathrm{mod}\, p) \Rightarrow a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (\mathrm{mod}\, p),$$

последнее в силу малой теоремы Ферма. Таким образом, квадратичные вычеты являются решениями сравнения (*). Количество таких вычетов в приведенной системе (35) равно как раз $\frac{p-1}{2}$. Следовательно, квадратичные невычеты среди решений сравнения (*) находиться не могут. Тогда они и только они удовлетворяют сравнению (37). ■

5.2. Символ Лежандра

Определение. Если $p > 2$ — простое число, a не делится на p, то символ Лежандра $\left(\frac{a}{p}\right)$ («символ a по отношению к p») определяется условиями:

$\left(\frac{a}{p}\right) = 1$, если a — квадратичный вычет;

$\left(\frac{a}{p}\right) = -1$, если a — квадратичный невычет.

При этом a называется числителем символа, а p — знаменателем символа.

Теорема 35 утверждает, что

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \qquad (38)$$

Свойства символа Лежандра

1. Если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Действительно, числа одного класса одновременно являются либо квадратичными вычетами, либо квадратичными невычетами.

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

Действительно, $1 = 1^2 \Rightarrow 1$ — квадратичный вычет.

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

Действительно, достаточно в (38) положить $a = -1$.

4. Нечетное простое число p может иметь вид либо $p = 4m + 1$, либо $p = 4m + 3$. В первом случае $\frac{p-1}{2}$ — четное, и $(-1)^{\frac{p-1}{2}} = 1$, то есть –1 — квадратичный вычет. Во втором случае $\frac{p-1}{2}$ — нечетное, и $(-1)^{\frac{p-1}{2}} = -1$, то есть –1 — квадратичный невычет.

5. Символ Лежандра мультипликативен относительно числителя: $\left(\frac{ab...c}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)...\left(\frac{c}{p}\right)$.

Действительно, в силу (38),

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

6. В числителе символа Лежандра можно отбросить любой множитель, являющийся квадратом:

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

Действительно,

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)^2=\left(\frac{a}{p}\right)\cdot(\pm1)^2=\left(\frac{a}{p}\right).$$

7. Величина, обратная символу Лежандра, совпадает с ним:

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

Действительно, $1/(\pm1)=\pm1$.

Разложение символа Лежандра

Пусть $p_1=\frac{p-1}{2}$ и $(a,p)=1$. Рассмотрим систему S абсолютно наименьших ненулевых вычетов по модулю p:

$$S=\{-p_1,...,-2,\ -1,1,2,...,p_1\}. \qquad (39)$$

и систему $S^+=\{1,2,...,p_1\}$ положительных вычетов из S.

В силу теоремы 26 каждое из чисел $a\cdot1, a\cdot2,..., a\cdot p_1$ сравнимо ровно с одним из абсолютно наименьших вычетов; поэтому

$$a\cdot1\equiv\varepsilon_1 r_1(\mathrm{mod}\,p);$$
$$a\cdot2\equiv\varepsilon_2 r_2(\mathrm{mod}\,p); \qquad (40)$$
$$\ldots$$
$$a\cdot p_1\equiv\varepsilon_{p_1} r_{p_1}(\mathrm{mod}\,p).$$

Здесь ε_i равно +1 либо –1, в зависимости от того, с положительным или с отрицательным абсолютно наименьшим вычетом сравнимо a; $r_i\in S^+$ — модуль соответствующего абсолютно наименьшего вычета.

Приведем пример. Пусть $p=7, a=9$. Абсолютно наименьшие положительные вычеты по мудулю 7 — это числа: 1, 2, 3. Имеем:

$9\cdot1=9\equiv2(\mathrm{mod}\,7);\ \varepsilon_1=+1;\ r_1=2;$

$9\cdot2=18\equiv-3(\mathrm{mod}\,7);\ \varepsilon_2=-1;\ r_2=3;$

$9 \cdot 3 = 27 \equiv -1 (\mathrm{mod}\, 7)$; $\varepsilon_3 = -1$; $r_3 = 1$.

Пусть $s \in S^+$. Если наименьший положительный вычет числа as больше, чем $\frac{p}{2}$, то его абсолютно наименьший вычет отрицателен, и $\varepsilon_s = -1$. В противном случае абсолютно наименьший вычет положителен, и $\varepsilon_s = +1$.

Например, при $p = 7$ для вычета $5 > 3{,}5$ соответствующим абсолютно наименьшим вычетом из этого же класса является $-2 = 5 - 7$; для вычета $3 < 3{,}5$ абсолютно наименьший вычет — это снова 3.

Теорема 36. Для символа Лежандра справедлива формула Гаусса:

$$\left(\frac{a}{p}\right) = \varepsilon_1 \varepsilon_2 ... \varepsilon_{p_1}. \qquad (41)$$

Доказательство. Приведенная система вычетов (39) состоит из p_1 пар чисел $\pm\varepsilon_1 r_1$, $\pm\varepsilon_2 r_2$,..., $\pm\varepsilon_{p_1} r_{p_1}$, причем числа r_1, r_2,..., r_{p_1} — это числа 1, 2,..., p_1 в некотором порядке, так что $1 \cdot 2 \cdot ... \cdot p_1 \equiv r_1 r_2 ... r_{p_1}$. Перемножим сравнения (40):

$$a^{p_1} \cdot 1 \cdot 2 \cdot ... \cdot p_1 \equiv \varepsilon_1 \varepsilon_2 ... \varepsilon_{p_1} r_1 r_2 ... r_{p_1} (\mathrm{mod}\, p).$$

Сократим сравнение на $1 \cdot 2 \cdot ... \cdot p_1 \equiv r_1 r_2 ... r_{p_1}$ и учтем (38):

$$\left(\frac{a}{p}\right) \equiv a^{p_1} \equiv \varepsilon_1 \varepsilon_2 ... \varepsilon_{p_1} (\mathrm{mod}\, p). \blacksquare$$

Квадратичный закон взаимности

Теорема 37. Для символа Лежандра справедлива формула

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{s \in S^+} \left[\frac{2as}{p}\right]}. \qquad (42)$$

Доказательство. Пусть $s \in S^+ = \{1, 2,..., p_1\}$. Имеем:

$$\left[\frac{2as}{p}\right] = \left[2\left(\left[\frac{as}{p}\right] + \left\{\frac{as}{p}\right\}\right)\right] = 2\left[\frac{as}{p}\right] + \left[2\left\{\frac{as}{p}\right\}\right].$$

Первое слагаемое в правой части — четное число. Поэтому вся сумма справа оказывается четной или нечетной вместе со слагаемым $\left[2\left\{\frac{as}{p}\right\}\right]$; последнее определяется тем, будет ли наименьший положительный вычет числа as меньше или больше чем $\frac{p}{2}$. Это, в свою очередь, равносильно условию $\varepsilon_s = 1$ или, соответственно, $\varepsilon_s = -1$. Следовательно, в формуле (41) $\varepsilon_s = (-1)^{\left[\frac{2as}{p}\right]}$. ■

Замечание. Поскольку рассматривается случай нечетного p, то $p^2 - 1 = (p-1)(p+1)$ делится нацело на 8 как произведение двух последовательных четных чисел.

Теорема 38. Для нечетного a справедлива формула:

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{s\in S^+}\left[\frac{as}{p}\right] + \frac{p^2-1}{8}}. \qquad (43)$$

Доказательство. Во-первых, $a + p$ четно. Далее, поскольку $2a \equiv 2a + 2p \pmod p$, то (см. п. 5.2, свойство 1)

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\dfrac{a+p}{2}}{p}\right).$$

Убирая из числителя символа Лежандра квадрат $4 = 2^2$, получаем:

$$\left(\frac{2a}{p}\right) = \left(\frac{\dfrac{a+p}{2}}{p}\right) =$$

(применяем формулу (42))

$$= (-1)^{\sum\limits_{s\in S^+}\left[\frac{(a+p)s}{p}\right]} = (-1)^{\sum\limits_{s\in S^+}\left[\frac{as}{p}\right] + \sum\limits_{s\in S^+} s}.$$

В силу мультипликативности символа Лежандра относительно числителя

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=\left(\frac{2a}{p}\right)=(-1)^{\sum\limits_{s\in S^+}\left[\frac{as}{p}\right]+\sum\limits_{s\in S^+}s}.$$

При этом по формуле суммирования арифметической прогрессии

$$\sum_{s\in S^+}s=\sum_{s=1}^{\frac{p-1}{2}}s=\frac{p^2-1}{8}.\ \blacksquare$$

Следствие. Поскольку $\left(\frac{1}{p}\right)=1$ (из-за $1\equiv 1^2(\mathrm{mod}\,p)$) и $0<\frac{s}{p}<1\Rightarrow\left[\frac{s}{p}\right]=0$, то $\sum\limits_{s\in S^+}\left[\frac{1\cdot s}{p}\right]=0$, и, полагая в (43) $a=1$, получаем:

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.\ \blacksquare \qquad (44)$$

Замечание. Всякое простое число $p>2$, будучи нечетным, имеет вид $p=8n\pm k$, где $k\in\{1,3\}$. Таким образом, для p выполняется ровно одно из четырех сравнений:

$p\equiv\pm1(\mathrm{mod}\,8)$, $p\equiv\pm3(\mathrm{mod}\,8)$.

Теорема 39. 1. Если простое p удовлетворяет условию $p\equiv\pm1(\mathrm{mod}\,8)$, то $\left(\frac{2}{p}\right)=1$. **2.** Если простое p удовлетворяет условию $p\equiv\pm3(\mathrm{mod}\,8)$, то $\left(\frac{2}{p}\right)=-1$.

Доказательство. Значение $(-1)^{\frac{p^2-1}{8}}$ в формуле (44) зависит от четности числа $\frac{p^2-1}{8}$. Поскольку p по условию является нечетным, оно представимо в виде $p=8n+k$, где $k\in\{\pm1,\pm3\}$. Тогда

$$\frac{p^2-1}{8}=\frac{(8n+k)^2-1}{8}=8n^2+2nk+\frac{k^2-1}{8}.$$

Если $k=\pm1$, то $\frac{p^2-1}{8}$ является четным; из (44) следует, что 2 является квадратичным вычетом по модулю p.

Если же $k = \pm 3$, то $\dfrac{p^2-1}{8}$ является нечетным; 2 является квадратичным невычетом по модулю p. ■

В определении символа Лежандра $\left(\dfrac{a}{p}\right)$ знаменатель p предполагается простым числом. Если числитель символа также является простым числом q, то определены оба символа $\left(\dfrac{q}{p}\right)$ и $\left(\dfrac{p}{q}\right)$.

Теорема 40 (квадратичный закон взаимности). Если p и q нечетные простые числа, то

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right). \qquad (45)$$

Доказательство. Обозначим, как и раньше, $p_1 = \dfrac{p-1}{2}$ и, кроме того, $q_1 = \dfrac{q-1}{2}$. Из (43) и (44) для нечетного a следует:

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{s\in S^+}\left[\frac{as}{p}\right]}. \qquad (46)$$

Поэтому дело сводится к вычислению суммы $\sum\limits_{s=1}^{p_1}\left[\dfrac{qs}{p}\right]$ для $\left(\dfrac{q}{p}\right)$ и суммы $\sum\limits_{t=1}^{q_1}\left[\dfrac{pt}{q}\right]$ для $\left(\dfrac{p}{q}\right)$.

Пусть переменные s и t пробегают независимо друг от друга множества значения $\{1, 2, ..., p_1\}$ и $\{1, 2, ..., q_1\}$ соответственно. Тогда $qs \neq pt$. Действительно, $(p,q) = 1$; кроме того, $(t,q) = 1$ из-за $t \le q_1 < q$. Значит, из $qs = pt$ следовало бы $q \mid pt$, что невозможно.

Количество пар (s,t) равно p_1q_1. Множество этих пар B разбивается на два: B_1 — пары, у которых $qs < pt$, и B_2 — пары, у которых $qs > pt$. Обозначим число таких пар через N_1 и N_2 соответственно. $N_1 + N_2 = p_1q_1$.

Имеем при фиксированном $t \in \{1, 2,..., q_1\}$:

$$(s,t) \in \mathrm{B}_1 \Leftrightarrow qs < pt \Leftrightarrow s < \frac{pt}{q} \Leftrightarrow s \le \left[\frac{p}{q} \cdot t\right],$$

так как S является целым числом. При этом $\left[\frac{p}{q} \cdot t\right] \le p_1$, поскольку $t \le \frac{q-1}{2} < \frac{q}{2} \Rightarrow \frac{p}{q} t < \frac{p}{2}$. Таким образом, при данном t в B_1 входят $\left[\frac{p}{q} \cdot t\right]$ пар, а именно, $(1,t), (2,t), ..., (\left[\frac{p}{q} \cdot t\right], t)$. Тогда, суммируя $\left[\frac{p}{q} \cdot t\right]$ по всем $t \in \{1,..., q_1\}$, получим общее число пар (s,t), входящих в B_1:

$$N_1 = \sum_{t=1}^{q_1} \left[\frac{p}{q} t\right].$$

Аналогично

$$N_2 = \sum_{s=1}^{p_1} \left[\frac{q}{p} s\right].$$

Теперь формула (46) дает:

$\left(\frac{p}{q}\right) = (-1)^{N_1}$, $\left(\frac{q}{p}\right) = (-1)^{N_2} \Rightarrow$

$\Rightarrow (-1)^{N_1+N_2} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p_1 q_1}$, и для получения (45) остается разделить последнее равенство на $\left(\frac{p}{q}\right)$, учтя свойство 7 символа Лежандра. ■

5.3. Символ Якоби

Пусть P — нечетное число, $P > 1$. Рассмотрим его разложение на простые множители:

$$P = p_1 p_2 \ldots p_k ,$$

среди которых могут быть и равные.

Определение. Символ Якоби $\left(\frac{a}{P}\right)$ задается равенством с участием символов Лежандра:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_k}\right). \qquad (47)$$

Замечание. Если P — простое число, то символ Якоби совпадает с символом Лежандра, что оправдывает одно и то же обозначение для этих символов.

Свойства символа Якоби

1. Если $a \equiv b(\mathrm{mod}\, P)$, то $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.

Действительно, для каждого простого множителя p_i из (47) имеет место равенство символов Лежандра:

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \quad (i = 1,2,\ldots,k).$$

Перемножая их, получаем требуемое равенство.

2. $\left(\frac{1}{P}\right) = 1$.

Действительно, $\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\ldots\left(\frac{1}{p_k}\right) = 1\cdot 1\cdot\ldots\cdot 1 = 1$.

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

Действительно, по свойству 3 символа Лежандра

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\ldots\left(\frac{-1}{p_k}\right) = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_k-1}{2}}.$$

Убедимся, что сумма показателей справа отличается от $\frac{P-1}{2}$ на четное число $2T$. Имеем:

$$p_i = \frac{2+2p_i-2}{2} = 1+\frac{2p_i-2}{2}.$$

Тогда

$$\frac{P-1}{2} = \frac{p_1p_2...p_k-1}{2} = \frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_1-1}{2}\right)...\left(1+2\frac{p_1-1}{2}\right)-1}{2}.$$

Если в числителе раскрыть все скобки, то получим:

а) сумму слагаемых $2\left(\frac{p_1-1}{2}+\frac{p_2-1}{2}+...+\frac{p_k-1}{2}\right)$, которые получаются при умножении второго слагаемого в одной из скобок на единицы из остальных скобок;

б) 1 – 1 = 0, когда перемножаются единицы из всех скобок;

в) сумму слагаемых вида $2\frac{p_i-1}{2}\cdot 2\frac{p_j-1}{2}...$ — перемножаются вторые слагаемые по крайней мере двух скобок с любыми слагаемыми (с 1 или с $\frac{p_l-1}{2}$) из остальных скобок; эта сумма имеет вид $4T$, поскольку каждое ее слагаемое содержит множитель 4.

Значит,

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+...+\frac{p_k-1}{2}+2T} = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+...+\frac{p_k-1}{2}}.$$

4. Символ Якоби мультипликативен относительно числителя: $\left(\frac{ab...c}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)...\left(\frac{c}{P}\right)$.

Действительно, пользуясь мультипликативностью символа Лежандра, получаем:

$$\left(\frac{ab...c}{P}\right) = \left(\frac{ab...c}{p_1}\right)...\left(\frac{ab...c}{p_k}\right) =$$

$$= \left[\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)...\left(\frac{c}{p_1}\right)\right]...\left[\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right)...\left(\frac{c}{p_k}\right)\right] =$$

(собираем вместе множители с a, множители с b и т. д.)

$$= \left(\frac{a}{p_1 \dots p_k}\right)\left(\frac{b}{p_1 \dots p_k}\right) \dots \left(\frac{c}{p_1 \dots p_k}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right) \dots \left(\frac{c}{P}\right).$$

5. В числителе символа Якоби можно отбросить любой множитель, являющийся квадратом:

$$\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right).$$

Действительно,

$$\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b^2}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)^2 = \left(\frac{a}{P}\right) \cdot (\pm 1)^2 = \left(\frac{a}{P}\right).$$

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

Действительно, пользуясь аналогичной формулой (44) для символа Лежандра, получаем:

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right) \dots \left(\frac{2}{p_k}\right) = (-1)^{\frac{p_1^2-1}{8} + \frac{p_1^2-1}{8} + \dots + \frac{p_1^2-1}{8}}. \qquad (48)$$

Аналогично доказательству свойства 3 можно убедиться, что

$$\frac{P^2-1}{8} = \frac{p_1^2 p_2^2 \dots p_k^2 - 1}{8} =$$

$$= \frac{\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right) \dots \left(1+8\frac{p_k^2-1}{8}\right)}{8} =$$

$$= \frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \dots + \frac{p_k^2-1}{8} + 2T,$$

так что из (48) следует:

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

Теорема (квадратичный закон взаимности для символа Якоби). Если P и Q — натуральные взаимно простые нечетные числа, то символы Якоби $\left(\frac{Q}{P}\right)$ и $\left(\frac{P}{Q}\right)$ связаны равенством:

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

Доказательство. Пусть $P = p_1 p_2 \ldots p_k$, $Q = q_1 q_2 \ldots q_n$, причем $p_i \neq q_j$. Тогда

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\ldots\left(\frac{Q}{p_k}\right) = \prod_{i=1}^{k}\prod_{j=1}^{n}\left(\frac{q_j}{p_i}\right) =$$

(применяем закон взаимности для символов Лежандра)

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

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

$$= (-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\cdot\left(\sum_{j=1}^{n}\frac{q_j-1}{2}\right)}\left(\frac{P}{Q}\right).$$

Аналогично доказательству свойства 3 можно убедиться, что

$$\frac{P-1}{2} = \sum_{i=1}^{k}\frac{p_i-1}{2} + 2T_1;\quad \frac{Q-1}{2} = \sum_{j=1}^{n}\frac{q_j-1}{2} + 2T_2,$$

так что

$$= (-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\cdot\left(\sum_{j=1}^{n}\frac{q_j-1}{2}\right)} = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}. \blacksquare$$

ПРИЛОЖЕНИЯ

Приложение 1

Обзор сведений о простых числах

С более подробным обзором можно ознакомиться, например, в [13, 14]. По мере развития вычислительных мощностей и развития науки подобного рода сведения в значительной своей части быстро устаревают, и «рекорды» долго не держатся.

Пусть n — натуральное число.

1. При $n > 2$ между n и $n!$ содержится, по крайней мере, одно простое число.

2. Постулат Бертрана. При $n > 3$ между n и $2n$ содержится, по крайней мере, одно простое число.

3. Существуют отрезки натурального ряда сколь угодно большой длины, не содержащие простых чисел. Действительно, поскольку $n! = 2 \cdot 3 \cdot ... \cdot n$, то числа

$$n! + 2, n! + 3, ..., n! + n$$

составные, так как у первого из них оба слагаемых делятся на 2, у второго — на 3,…, у последнего — на n.

4. Для каждого n имеется, по крайней мере, три различных простых числа, имеющих в десятичной записи n цифр.

5. Неизвестно, конечно ли число пар простых чисел-близнецов p и $p + 2$, таких как пары {5, 7}, {11, 13}, {17, 19}.

6. Десятичная запись простого числа $p > 10$ может оканчиваться только цифрами из множества $A = \{1, 3, 7, 9\}$.

7. Для любых натуральных s и t, для любой последовательности десятичных цифр $a_1, a_2, ..., a_s$ и для любой последовательности $b_1, b_2, ..., b_t$, где $b_i \in \{1, 3, 7, 9\}$ $(i = 1, ..., t)$, существует простое число, десятичная запись которого начинается первой последовательностью, а заканчивается второй последовательностью (возможно, с промежуточными цифрами).

8. Для всякого n существуют простые числа, десятичная запись которых содержит более n нулей.

9. Обозначим через $\Pi(x)$ количество простых чисел, не превосходящих вещественного x. Функция $\Pi(x)$ описывает распределение простых чисел на числовой оси (см. [5]).

$$\lim_{n\to\infty}\frac{\Pi(x)}{\left(\dfrac{1}{n\ln n}\right)}=1.$$

10. Обозначим через p_k k–е простое число. Существует бесконечно много значений k, для которых $p_k^2 > p_{k-1}^2 p_{k+1}^2$.

11. Числовой ряд $\sum_{k=1}^{\infty}\frac{1}{p_k}$ расходится так, что его частичные суммы S_n превышают с ростом n любое наперед заданное m.

12. Для всех натуральных $k > 3$ множество простых чисел содержит арифметическую прогрессию длины k. Иными словами, существуют арифметические прогрессии любой длины, целиком составленные из простых чисел.

13. Всякая арифметическая прогрессия $\{a, a+d, a+2d, ...\}$, в которой начальный член a и разность прогрессии d взаимно просты, содержит бесконечно много простых чисел.

14. Известно (к 1984 году) 50 миллионов первых идущих подряд простых чисел.

15. Имеется бесконечно много простых чисел каждого из видов $4k+1,\ 4k+3,\ 6k+5$.

16. Теорема Вильсона. Для простого p число $(p-1)!+1$ делится на p.

17. Теорема Лейбница. Для того чтобы натуральное число $p > 2$ было простым, необходимо и достаточно, чтобы $(p-2)!-1$ делилось на p.

18. Имеется бесконечно много троек простых чисел (x, y, z), для которых $z = x + y + 1$.

19. Наибольшее простое число, известное на январь 2016 г., $2^{74207281}-1$. Его десятичная запись содержит 22’338’618 цифр. Оно является числом Мерсенна, то есть числом вида 2^n-1.

В декабре 2017 г. установлена простота еще одного числа Мерсенна — $2^{77232917}-1$. Его десятичная запись состоит из 23’249’425 цифр.

В декабре 2018 г. установлена простота пока (на 22.06.2022) наибольшего числа Мерсенна — $2^{82589933}-1$. Его десятичная запись состоит из 24’862’048 цифр.

Приложение 2

Теорема Эйлера в шифровании с открытым ключом

Процедура шифрования с открытым ключом предполагает использование двух ключей, открытого и секретного, выбранных так, что их последовательное применение к тексту оставляет этот текст без изменений. Шифрование использует открытый ключ, дешифрование — секретный. Дешифрование без знания секретного ключа практически неосуществимо; в частности, практически неразрешима задача вычисления секретного ключа по известному открытому ключу.

Сообщение, предназначенное для конфиденциальной передачи по каналам связи, является двоичным кодом и может быть интерпретировано как двоичная запись натурального числа M. Назовем M исходным текстом.

Пусть p и q большие простые числа, известные только отправителю и адресату. (Обычно используются простые числа порядка 10^{300}). Число $n = pq$ — модуль, который может передаваться открыто, поскольку его разложение на простые множители практически невозможно выполнить за приемлемое время. Тогда практически невозможно вычислить и известное только участникам переписки значение функции Эйлера $\varphi(n) = (p-1)(q-1)$.

Если $M < n$, то M является наименьшим неотрицательным вычетом по модулю n. (Если $M \geq n$, то двоичный код следует разбить на части, каждая из которых представляет число, меньшее n.)

Пусть, далее, натуральное число e (открытая экспонента) выбрано участниками переписки так, что $(e, \varphi(n)) = 1$. Обычно в качестве e выбирается небольшое простое число. Пара чисел $\{e, n\}$ называется открытым ключом и передается открыто вместе с зашифрованным сообщением $C = M^e (\mathrm{mod}\, n)$ — наименьшим положительным остатком от деления M^e на n.

Получатель сообщения C (дешифратор), решая сравнение по из-

вестному ему модулю $\varphi(n)$, вычисляет секретную экспоненту — число d, для которого $de \equiv 1(\mathrm{mod}\,\varphi(n))$. В результате для найденного d получается $de = k \cdot \varphi(n) + 1$.

После этого число C (зашифрованное сообщение) возводится по модулю n в степень d, то есть находится наименьший положительный вычет $C^d(\mathrm{mod}\,n)$. В результате получается исходный текст M.

Действительно, для $\delta = (M, n)$ возможны два случая:

1) Если $\delta = 1$, то применима теорема Эйлера:

$$M^{\varphi(n)} \equiv 1(\mathrm{mod}\,\varphi(n)).$$

Тогда

$$C^d(\mathrm{mod}\,n) \equiv \left(M^e\right)^d(\mathrm{mod}\,n) \equiv M^{ed}(\mathrm{mod}\,n) \equiv$$

$$\equiv M^{k\cdot\varphi(n)+1}(\mathrm{mod}\,n) \equiv \left(M^{\varphi(n)}\right)^k \cdot M(\mathrm{mod}\,n) \equiv$$

$$\equiv 1^k \cdot M(\mathrm{mod}\,n) \equiv M(\mathrm{mod}\,n).$$

2) Если $\delta > 1$, то это возможно лишь при $p \mid \delta$ или $q \mid \delta$, поскольку $n = pq$ и $M < n$. Пусть, например, $p \mid \delta$. Тогда $(M, q) = 1$, и по малой теореме Ферма

$$M^{q-1} \equiv 1(\mathrm{mod}\,q) \Rightarrow \left(M^{q-1}\right)^{k(p-1)} \equiv 1(\mathrm{mod}\,q) \Rightarrow M^{k\varphi(n)} \equiv 1(\mathrm{mod}\,q);$$

умножая обе части сравнения на M, получаем:

$$M^{ed} \equiv M(\mathrm{mod}\,q). \qquad (50)$$

Кроме того,

$$M^{ed} \equiv M(\mathrm{mod}\,p), \qquad (51)$$

так как $M \equiv 0(\mathrm{mod}\,d) \Rightarrow M \equiv 0(\mathrm{mod}\,p)$. Применяя к сравнениям (50) и (51) свойство 11 п. 3.1, и в этом случае заключаем, что имеет место сравнение $C^d \equiv M^{ed} \equiv M(\mathrm{mod}\,pq)$.

Библиографический список

1. Боревич З. И. Теория чисел / З. И. Боревич, И. Р. Шафаревич. — М. : Наука, 1985. — 504 с.
2. Бухштаб А. А. Теория чисел. — М. : Просвещение, 1966. — 384 с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. — М. : МЦНМО, 2003. — 328 с.
4. Виноградов И. М. Основы теории чисел. — Москва-Ижевск : НИЦ «Регулярная и хаотическая динамика», 2003. — 176 с.
5. Дербишир Д. Простая одержимость. Бернхард Риман и величайшая нерешенная проблема в математике. — М. : Астрель, 2010. — 464 с.
6. Коблиц Н. Курс теории чисел и криптографии. — 2001. — 254 с. (электронное издание, www.ph4s/ru).
7. Коутинхо С. Введение в теорию чисел и алгоритм RSA. — М. : Постмаркет, 2001. — 328 с.
8. Кочева А. А. Задачник-практикум по алгебре и теории чисел. Ч. III. — М. : Просвещение, 1984. — 41 с.
9. Маховенко Е. Б. Теоретико-числовые методы в криптографии. — М. : Гелиос АРВ, 2006. — 320 с.
10. Нестеренко Ю. В. Теория чисел. — М. : Академия, 2008. — 272 с.
11. Оре О. Приглашение в теорию чисел / О. Оре. — М. : Едиториал УРСС, 2003. — 128 с.
12. Просветов Г. И. Теория чисел: задачи и решения. — М. : Альфа-Пресс, 2010. — 72 с.
13. Серпинский В. Что мы знаем и чего не знаем о простых числах. — М. : Физматгиз, 1963. — 91 с.
14. Ястребов М. Ю. Основы теории чисел / М. Ю. Ястребов, А. П. Нырков. — СПб. : ГУМРФ имени адмирала С. О. Макарова, 2013. — 92 с.

Учебное издание

Ястребов Михаил Юрьевич, канд. техн. наук
Ырков Анатолий Павлович, д-р техн. наук, проф.
Чистяков Глеб Борисович, канд. техн. наук

Введение в теорию чисел

Учебное пособие

Издательство
ГУМРФ им. адм. С. О. Макарова

198035, Санкт-Петербург, Межевой канал, 2
Тел.: (812) 748-97-19, 748-97-23
E-mail: izdat@gumrf.ru

Редактор *Л. Б. Кожева*
Оригинал-макет *М. Н. Евсюткина*

Подписано в печать 06.07.2022
Формат 60×90/16. Бумага офсетная. Гарнитура Times New Roman
Усл. печ. л. 4,75. Тираж 100 (первый завод — 50) экз. Заказ № 76/22