Теория чисел: учебное пособие

А. А. Илларионов

01.02.2016

Оглавление

Глава I
Теория делимости

Будем использовать следующие обозначения:

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ — множество целых,

$\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных,

$\mathbb{R}$ — множество вещественных чисел.

Если не указано противное, то все рассматриваемые числа считаются целыми.

§ 1. Делители, кратные и алгоритм Евклида

Определение. Пусть $a, b \in \mathbb{Z}$. Если $\dfrac{a}{b}$ целое число, то говорят, что a *делится* на b (a *кратно* b), а число b называют *делителем* a Символически это записывается так: $b \mid a$.

Согласно определению

$$b \mid a \quad \Longleftrightarrow \quad \exists q \in \mathbb{Z} : \ a = bq.$$

Пример. Делителями 28 являются $1, 2, 4, 7, 14, 28$.

Лемма 1.1. *Справедливы следующие свойства.*

1. *Если* $a \mid b$, *то* $a \mid bc$.
2. *Если* $a \mid b$, $b \mid c$, *то* $a \mid c$.
3. *Если* $a \mid b$, $a \mid c$, *то* $a \mid (b \pm c)$.
4. *Если* $a \mid b$ *и* $b \neq 0$, *то* $|a| \leq b$.

Доказательство вытекает из определения и оставляется читателю.

Теорема 1.1. *Пусть* $d \in \mathbb{N}$. *Любое целое* a *единственным образом представимо в виде:*

$$a = dq + r, \tag{1.1}$$

где $0 \leq r < d$.

Доказательство. Докажем, что a можно представить в виде (1.1). Выберем целое q так, чтобы dq было наибольшим числом, не превосходящим a. Положим $r = a - dq$. Тогда

$$\begin{aligned} &r \geq 0, \quad \text{т.к. } dq \leq a, \\ &r < d, \quad \text{т.к. в противном случае } d(q+1) \leq a. \end{aligned}$$

Докажем единственность представления (1.1). Предположим, что $a = dq' + r'$, где $0 \leq r' < 0$. Тогда

$$0 = d(q - q') + (r - r').$$

Значит, d делит $(r - r')$. Кроме того, $|r - r'| < d$. Поэтому $(r - r') = 0$ и, следовательно, $(q - q') = 0$. □

Числа q и r, входящие в формулу (1.1), называют *неполным частным* и *остатком* при делении a на d.

Определение. Целое d, делящее $a_1, a_2, \ldots a_n$, называется их *общим делителем*. Наибольшее d, делящее $a_1, a_2, \ldots a_n$, называется их *наибольшим общим делителем* и обозначается нод $(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$.

Пример. нод $(28, 21) = 7$, нод $(48, 36) = 12$.

Алгоритм Евклида нахождения наибольшего общего делителя основывается на следующем простом результате.

Лемма 1.2. *Если* $a = bq + r$, *то* $(a, b) = (b, r)$.

Доказательство. Если $d \mid a$ и $d \mid b$, то $d \mid r$. Аналогично, если $d \mid b$ и $d \mid r$, то $d \mid a$. Значит, множество общих делителей a и b совпадает с множеством общих делителей b и r. □

Алгоритм Евклида. Дано $a, b \in \mathbb{N}$, $a > b > 0$. Найти нод (a, b).

1. Делим a на b с остатком:
$$a = bq + r \qquad (0 \leq r < b)$$
(Тогда нод $(a, b) =$ нод (b, r)).

2. Если $r > 0$, то заменяем пару (a, b) на пару (b, r) и переходим к шагу 1.

3. Полагаем нод $(a, b) = b$. СТОП.

Алгоритм сходится за конечное число шагов, т.к. на каждом шаге уменьшается максимальное из рассматриваемой пары чисел.

Пример. Найти нод $(6188, 4709)$. Имеем

$$\begin{aligned} 6188 = 4709 + 1479 \quad &\Longrightarrow \quad (6188, 4709) = (1479, 4709), \\ 4709 = 1479 \cdot 3 + 272 \quad &\Longrightarrow \quad (1479, 4709) = (1479, 272), \\ 1479 = 272 \cdot 51 + 47 \quad &\Longrightarrow \quad (1479, 272) = (47, 272) \\ 272 = 47 \cdot 5 + 37 \quad &\Longrightarrow \quad (47, 272) = (47, 37) = (10, 37) = (10, 7) = (3, 7) = (3, 1) = 1. \end{aligned}$$

Ответ: нод $(6188, 4709) = 1$.

Определение. Целое M, которое делится на $a_1, a_2, \ldots, a_n$, называется *общим кратным* $a_1, a_2, \ldots, a_n$. Наименьшее натуральное M, которое делится на $a_1, a_2, \ldots, a_n$, называется *наименьшим общим кратным* и обозначается через нок $[a_1, \ldots, a_n]$ либо $[a_1, \ldots, a_n]$.

Пример. $[2, 3] = 6, \quad [4, 6] = 12.$

Теорема 1.2. *Любое общее кратное нескольких чисел делится на их наименьшее общее кратное (если $\hat{M}$ — общее кратное $a_1, \ldots, a_n$, то $\hat{M}$ делится на* нок $[a_1, \ldots, a_n]$*).*

Доказательство. Пусть $M =$ нок $[a_1, \ldots, a_n]$. Тогда $M < \hat{M}$ и поэтому

$$\hat{M} = M \cdot q + r,$$

где $0 \leq r < M$. Согласно свойствам делимости число $r = (\hat{M} - Mq)$ делится на каждое из чисел $a_1, \ldots, a_n$, т.е. r есть их общее кратное. Если $r > 0$, то приходим к противоречию с условием $M = [a_1, \ldots, a_n]$. Поэтому $r = 0$ и $\hat{M} = qM$. □

Следствие 1.1. *Для любых натуральных a и b*

$$[a, b] = \frac{a \cdot b}{(a, b)}. \tag{1.2}$$

Доказательство. Произведение ab есть общее кратное a и b. Значит, по теореме 1.2 найдется такое $d \in \mathbb{N}$, что $ab = d \cdot [a, b]$. Так как

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

то d делит a. Аналогичным образом получаем, что d делит b. Значит, d является общим делителем a и b. Поэтому $d \leq (a, b)$. Кроме того, $ab/(a, b)$ есть общее кратное a и b. Поэтому

$$\frac{ab}{(a, b)} \geq [a, b] = \frac{ab}{d}.$$

Следовательно, $(a, b) \leq d$. Значит, $d = (a, b)$. □

§ 2. Простые и составные числа

Число 1 имеет только один делитель 1. Все другие натуральные числа имеют, как минимум, два делителя.

Определение. Натуральное $p > 1$ называется *простым,* если оно делится только на 1 и на p. Целое $a > 1$, имеющее другие делители, кроме a и 1 называется *составным.*

Одна из важнейших задач современной теории чисел[1] заключается в следующем: *определить является ли данное N простым числом или нет?*

Тривиальное решение заключается в проверке делимости N на все целые от 2 до $N-1$. Следующий результат показывает, что достаточно рассмотреть целые от 2 до $\sqrt{N}$.

[1] имеющая важное значение, например, в криптографии

Лемма 2.1. *Пусть N — составное. Возьмем наименьшее p такое, что $p \mid N$, $p > 1$. Тогда p — простое, причем $p \leq \sqrt{N}$.*

Доказательство. Если p составное, то существует такой $d \in (1, p)$, что $d \mid p$. Но тогда $d \mid N$ и $d < p$, что противоречит условию леммы. Поэтому p простое.

Положим $d = N/p$. Тогда $d \mid N$ и поэтому $d \leq p$. Значит, $N = dp \geq p^2$. □

Следствие 2.1. *Любое составное N имеет простой делитель $p \leq \sqrt{N}$.*

Для составления таблицы простых, не превосходящих заданного N, существует метод, называемый *решетом Эратосфена*, который заключается в следующем. Выписываем все натуральные от 2 до N. Первое число есть 2. Оно простое. Вычеркиваем все остальные числа нашего ряда, которые кратны 2. Первое следующее за 2 невычеркнутое число есть 3. Оно не делится на 2, поэтому также простое. Вычеркиваем все числа, кратные 3, кроме самого 3. Следующее за 3 невычеркнутое число есть 5 оно не делится на 2 и 3 и, значит, является простым. Вычеркиваем все числа, кратные 5, кроме самого 5 и так далее.

Алгоритм (решето Эратосфена)**.** Дано $N \in \mathbb{N}$. Нужно вычислить все простые, не превосходящие N.

1. Полагаем $p = 2$.
2. Вычеркиваем все $a \in [p^2, N]$, которые кратны p.
3. Следующее за p не вычеркнутое число обозначаем через p'.
4. Если $p'^2 \leq N$, то полагаем $p = p'$ и переходим к шагу 2.
5. Невычеркнутые числа из $\{2, 3, \ldots, N\}$ образуют искомое множество простых. Конец.

Теорема 2.1. *Числа, которые останутся невычеркнутыми после окончания вышеприведенного алгоритма, образуют множество простых из отрезка $[1, N]$.*

Доказательство. Вычеркнутые числа являются составными. Осталось доказать, что мы вычеркнули все составные числа. Возьмем любое составное $a \in [1, N]$. По следствию 2.1 существует простое p такое, что $p \mid a$, $p \leq \sqrt{a}$. Все числа, которые кратны простым отрезка $[2, \sqrt{N}]$ вычеркнуты. Значит, a вычеркнуто. □

Пример. Проверить число 1009 на простоту. Предположим, что 1009 составное. Тогда пол лемме 2.1 оно имеет простой делитель p, причем $2 \leq p \leq \sqrt{1009} = 31.7\ldots$. Выпишем все простые из отрезка $[2, 31]$ с помощью решета Эратосфена. Для этого мы должны вычеркнуть все составные кратные 2, 3, 5. В результате, получим

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31.$$

Ни одно из этих чисел не делит 1009. Поэтому число 1009 простое.

Теорема 2.2 (Евклид)**.** *Простых чисел бесконечно много.*

Доказательство. Предположим, что множество простых конечное и состоит из $p_1, p_2, \ldots, p_n$. Рассмотрим число $p = p_1 \cdot \ldots \cdot p_n + 1$. Если оно составное, то должно иметь простой делитель. Однако p не делится ни на одно из p_j. Получили противоречие. □

Замечание 2.1. Издавна ведутся записи, отмечающие наибольшие известные на то время простые числа. Один из рекордов поставил в свое время Эйлер, доказав, что простым является $2^{31} - 1 = 2\,147\,483\,647$. Наибольшим известным простым числом по состоянию на февраль 2013 года является $2^{57885161} - 1$. Оно содержит 17 425 170 десятичных цифр и является простым числом Мерсенна.[2] За нахождение простых чисел из более чем 10^8 и 10^9 десятичных цифр американская организация EFF назначила денежные призы соответственно в 150 и 250 тыс. долларов США.

§ 3. Основная теорема арифметики

Лемма 3.1. *Пусть p — простое*

а) для любого $a \in \mathbb{Z}$ либо нод $(a, p) = 1$, *либо $p \mid a$;*

б) если $p \mid ab$, то либо $p \mid a$, либо $p \mid b$;

в) если $p \mid (a_1 \cdot \ldots \cdot a_n)$, то найдется хотя бы один a_j, который кратен p.

Доказательство. Докажем а). Так как нод $(a, p) \mid p$, то либо нод $(a, p) = 1$, либо нод $(a, p) = p$, т.е. $p \mid a$.

Докажем б). Если $p \mid a$, то утверждение выполнено. Пусть $p \nmid a$. Тогда нод $(p, a) = 1$. Так как ab кратно p и кратно a, то

$$ab \text{ делится на нок } [a, p] = \frac{a \cdot p}{\text{нод } (a, p)} = ap.$$

Поэтому b делится на p.

Докажем в). Предположим, что $p \nmid a_i$, $i \geq 2$. Так как

$$p \mid (a_1 \cdot \ldots a_{n-1})a_n, \quad p \nmid a_n,$$

то согласно б), $p \mid (a_1 \cdot \ldots a_{n-1})$. Так как

$$p \mid (a_1 \cdot \ldots a_{n-2})a_{n-1}, \quad p \nmid a_{n-1},$$

то $p \mid (a_1 \cdot \ldots a_{n-2})$. И так далее. В итоге, получаем $p \mid a_1$. □

Теорема (Основная теорема арифметики)**.** *Любое целое $a > 1$ разлагается в произведение простых чисел, причем единственным образом с точностью до порядка следования сомножителей.*

Доказательство. Докажем существование искомого разложения. Случай a — простое является тривиальным. Пусть a — составное. Тогда оно имеет простой делитель p_1, т.е. $a = p_1 \cdot a_1$. Если a_1 — простое, то процесс закончен. Если нет, то $a_1 = a_2 p_2$, т.е.

$$a = p_1 p_2 a_2.$$

[2] Числа Мерсенна имеют вид $2^n - 1$, где $n \in \mathbb{N}$. Существует эффективный алгоритм проверки чисел Мерсенна на простоту. Поэтому простые числа Мерсенна давно удерживают лидерство, как самые большие из известных простых.

Если a_2 — простое, то процесс закончен. Продолжая процесс, мы за конечное число шагов получим

$$a = p_1 p_2 \dots p_n, \tag{3.1}$$

где p_j — (возможно повторяющиеся) простые.

Докажем, что разложение (3.1) единственно (с точностью до нумерации p_j). Предположим, что

$$a = q_1 q_2 \dots q_m,$$

где q_j — простые. Тогда

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m.$$

Левая часть делится на p_1. Значит, и правая делится на p_1. Согласно лемме 3.1 в) найдется q_j, кратный p_1. Пусть, например, $j = 1$. Так как q_1 — простое, то $q_1 = p_1$. Сокращая левую и правую части на p_1, получаем

$$p_2 \dots p_n = q_2 \dots q_m.$$

Аналогичным образом сокращая на p_2, p_3, $\dots p_n$, приходим к соотношению

$$1 = Q,$$

где Q — произведение оставшихся после сокращений q_j. Значит, все q_j должны сократиться. Это означает, что $n = m$ и произведения $p_1 \dots p_n$ и $q_1 \dots q_m$ отличаются только нумерацией сомножителей. □

Согласно основной теореме арифметики любое целое $a > 1$ единственным образом представимо в виде

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, \tag{3.2}$$

где p_j — попарно различные простые (простые делители), причем $p_1 < p_2 < \dots < p_s$, а $\alpha_j \in \mathbb{N}$ (показатели).

Определение. Соотношение (3.2) называется *каноническим разложением* целого $a > 1$.

Задача *факторизации* заключается в нахождении канонического разложения заданного натурального N. Она относится к числу важнейших задач теории чисел, имеющих прикладной значение (например, в криптографии). С вычислительной точки зрения, самым трудным является случай, когда N есть произведение двух простых. Такие N называют еще полупростыми. В 1991–2007 гг. RSA Laboratory проводила конкурс «RSA Factoring Challenge» для поощрения исследований в области вычислительной теории чисел и практической сложности факторизации больших целых чисел. Был опубликован список из 54 полупростых числа длиной от 100 до 617 десятичных знаков. За факторизацию некоторых из них предлагались денежные призы. Например, премия за факторизацию RSA-1536 (1536 битов) составляла 150 тыс. долларов. Наименьшее RSA-число было разложено за несколько дней. Большинство чисел до сих пор не разложены и предполагается, что многие из них останутся неразложенными еще довольно долгое время до значительного улучшения вычислительных мощностей и продвижений в факторизации целых чисел.

§ 4. Следствия из основной теоремы арифметики

Следствие 4.1. *Справедливы следующие свойства.*

а) Пусть (3.2) есть каноническое разложение числа a. Тогда множество его делителей состоит из чисел d вида

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s},$$

где $0 \le \beta_j \le \alpha_j$.

б) Наибольший общий делитель нескольких чисел равен произведению степеней вида p^α, где p — общий простой делитель этих чисел, а α — наименьший из показателей, с которыми p входит в их канонические разложения.

в) Любой общий делитель нескольких чисел делит их наибольший общий делитель.

г) Общее наименьшее кратное нескольких чисел равно произведению степеней вида p^α, где p — простой делитель хотя бы одного из этих чисел, а α — наибольший из показателей, с которыми p входит в их канонические разложения.

Доказательство. Докажем а). Пусть $d \mid a$, причем каноническое разложение d имеет вид

$$d = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}.$$

Возьмем любое $i \in \{1, \dots, l\}$. Так как $q_i \mid d$, $d \mid a$, то $q_i \mid a$. Согласно лемме 3.1 в) отсюда вытекает, что q_i делит какое-нибудь из простых $p_1, \dots, p_s$. Это возможно только в случае, когда q_i равен одному из $p_1, \dots, p_s$. Пусть, для определенности, $q_i = p_1$. Осталось доказать, что $\beta_i \le \alpha_1$. Имеем

$$p_1^{\beta_i} \mid d, \quad d \mid a \quad \Longrightarrow \quad p_1 \mid a \quad \Longrightarrow \quad p_1^{\beta_i} \mid (p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}).$$

Если $\beta_i > \alpha_1$, то $p_1 \mid (p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s})$. Последнее невозможно согласно лемме 3.1. Значит, $\beta_i \le \alpha_1$. Ввиду произвольности i, свойство а) доказано.

Утверждения б), в) являются очевидными следствиями из а). Свойство г) доказывается по такой же схеме, что и а). □

Пример. Выпишем канонические разложения следующих чисел

$$1\,089\,000 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 11^2, \quad 720 = 2^4 \cdot 3^2 \cdot 5, \quad 67\,914 = 2 \cdot 3^2 \cdot 7^3 \cdot 11.$$

Число 67 914 имеет следующие делители

$$2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 7^{\alpha_3} \cdot 11^{\alpha_4},$$

где $\alpha_1 \in \{0, 1\}$, $\alpha_2 \in \{0, 1, 2\}$, $\alpha_3 \in \{0, 1, 2, 3\}$, $\alpha_4 \in \{0, 1\}$. Кроме того,

$$(1\,089\,000,\ 720,\ 67\,914) = 2 \cdot 3^2 = 18,$$
$$[1\,089\,000,\ 720,\ 67\,914] = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7^3 = 3\,087\,000$$

Следствие 4.2. *Пусть* нод $(a, b) = 1$. *Тогда*

а) нод (a, bc) = нод (a, c);

б) если $a \mid bc$, *то* $a \mid c$.

Доказательство. Так как нод $(a, b) = 1$, то a, b не имеют общих простых делителей и требуемые утверждения вытекают из следствия 4.1 а), б). □

Следствие 4.3. *Пусть* нод $(a_i, b_j) = 1$, $i = \overline{1,n}$, $j = \overline{1,k}$. *Тогда*

$$\text{нод}\ \left(\prod_{i=1}^{n} a_i,\ \prod_{j=1}^{k} b_j\right) = 1.$$

Доказательство. Числа $\prod a_i$ и $\prod b_j$ не имеют общих простых делителей. □

Используя следствие 4.1, можно также вывести следующие формулы

$$\text{нод}\ (ba_1, ba_2, \ldots, ba_n) = b \cdot \text{нод}\ (a_1, a_2, \ldots, a_n), \tag{4.1}$$
$$\text{нок}\ [ba_1, ba_2, \ldots, ba_n] = b \cdot \text{нок}\ [a_1, a_2, \ldots, a_n], \tag{4.2}$$
$$\text{нод}\ (a_1, a_2, \ldots, a_{n-1}, a_n) = \text{нод}\ (\text{нод}\ (a_1, a_2, \ldots, a_{n-1}),\ a_n), \tag{4.3}$$
$$\text{нок}\ [a_1, a_2, \ldots, a_{n-1}, a_n] = \text{нок}\ [\text{нок}\ [a_1, a_2, \ldots, a_{n-1}],\ a_n], \tag{4.4}$$

Упражнение 4.1. Пусть $a/b = c/d$ и нод $(c, d) = 1$. Докажите, что тогда $a = c$, $b = d$ либо $a = -c$, $b = -d$.

Численные упражнения к главе I

1. Найдите наибольшие общие делители

$$(385, 781), \quad (1234, 56789), \quad (53357, 70303), \quad (2^{21} - 1, 2^{27} - 1), \quad (2^{100} \cdot 1221,\ 3333)$$

2. Найдите наименьшие общие кратные

$$[33, 35], \quad [34, 38], \quad [30, 165], \quad [8192, 32768], \quad [6, 10, 55].$$

3. Используя решето Эратосфена, выпишите все простые, не превосходящие 100.

4. Исследуйте следующие числа на простоту: 131, 133, 233, 237, 311, 319, 419.

5. Найдите множество общих делителей чисел 385, 781.

Глава II
Алгоритм Евклида и непрерывные дроби

§ 1. Сложность алгоритма Евклида. Обобщенный алгоритм Евклида

Одним из древнейших математических алгоритмов является античный алгоритм Евклида нахождения наибольшего общего делителя. Он основывается на следующем элементарном результате (см. лемму I.1.2): если $a = bq + r$, то нод $(a, b) =$ нод (b, r).

Алгоритм Евклида. Дано $a > b > 0$. Нужно найти $d =$ нод (a, b).

1. Представим a в виде $a = bq + r$, где $0 \leq r < b$. Тогда $(a, b) = (b, r)$.
2. Если $r > 0$, то заменяем пару (a, b) на (b, r) и переходим к шагу 1.
3. Полагаем $d = b$. СТОП.

Запишем алгоритм в виде следующей цепочки соотношений (деления с остатком)

$$\begin{array}{ll} a = bq_0 + r_1, & 0 < r_1 < b, \\ b = r_1 q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 = r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ \dots & \dots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_n q_n, & \end{array} \tag{1.1}$$

которая заканчивается при $r_{n+1} = 0$.

Лемма 1.1. *Для любых натуральных a, b*

$$\text{нод } (a, b) = r_n,$$

где r_n — последний ненулевой остаток в алгоритме Евклида.

Доказательство. Используя (1.1) и лемму I.1.2, получаем

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = (r_n q_n, r_n) = r_n,$$

□

Пример. Вычислим нод $(525, 231)$. Имеем $a = 525$, $b = 231$,

$$\begin{array}{lll} 525 = 231 \cdot 2 + 63, & q_1 = 2, & r_2 = 63, \\ 231 = 63 \cdot 3 + 42, & q_2 = 3, & r_2 = 63, \\ 63 = 42 \cdot 1 + 21, & q_3 = 1, & r_4 = 21, \\ 42 = 21 \cdot 2, & q_4 = 2, & r_5 = 21. \end{array}$$

Ответ: нод $(525, 231) = 21$.

Время работы алгоритма Евклида зависит от числа делений (т.е. от n). Получим оценку для этой величины.

Определение. *Золотым сечением* называется константа

$$\varphi = \frac{1 + \sqrt{5}}{2} = 1.61803398\ldots$$

Она является положительным решением квадратного уравнения

$$\varphi^2 - \varphi - 1 = 0. \tag{1.2}$$

Теорема 1.1. *Пусть $a, b \in \mathbb{N}$, причем $b < a$. Количество делений, необходимых для вычисления* нод (a, b) *с помощью алгоритма Евклида не больше, чем* $\log_\varphi b + 1$.

Доказательство. Будем использовать соотношения (1.1). Для удобства положим $r_0 = b$. Число делений в алгоритме Евклида равно $n + 1$. Поэтому достаточно доказать, что $n \le \log_\varphi b$. Получим следующую оценку неполных частных:

$$r_{n-i} \ge \varphi^i, \quad i = \overline{1, n}, \tag{1.3}$$

используя метод математической индукции по $i = 1, 2, \ldots, n$.

База индукции. Так как $r_{n-1} > r_n \ge 1$, то $r_{n-1} \ge 2 > \varphi$. Неравенство (1.3) выполнено при $i = 1$.

Индукционный переход от $(i - 1)$ к i. Пусть неравенство (1.3) выполняется для всех $i < j$. Нужно доказать, что оно справедливо и при $i = j$. Полагая $i = j - 1$ и $i = j - 2$, получаем

$$r_{n-j+1} \ge \varphi^{j-1}, \quad r_{n-j+2} \ge \varphi^{j-2}.$$

Используя (1.1) и равенство $\varphi + 1 = \varphi^2$, имеем

$$r_{n-j} = q_{n-j+1} r_{n-j+1} + r_{n-j+2} \ge r_{n-j+1} + r_{n-j+2} \ge \varphi^{j-1} + \varphi^{j-2} = \varphi^{j-2}(1 + \varphi) = \varphi^{j-2} \cdot \varphi^2 = \varphi^j.$$

Неравенство (1.3) доказано. Из него вытекает, что $\varphi^n \le r_0 = b$, т.е. $n \le \log_\varphi b$. □

Замечание 1.1. Пусть N — количество разрядов в двоичной записи числа b (количество битов, требуемых для хранения b в памяти компьютера). Тогда $b < 2^N$. Поэтому количество делений в алгоритме Евклида не превосходит

$$\log_\varphi b + 1 = \log_2^{-1} \varphi \cdot \log_2 b + 1 < \log_2^{-1} \varphi \cdot N + 1 < 1.45 \cdot N + 1.$$

Если мы попытаемся найти нод (a, b) путем перебора всех возможных чисел от 2 до b, то количество пробных делений примерно равно $b/2 \approx 2^N$. Например, при $N = 100$ алгоритм Евклида потребует не более, чем 146 делений, а количество делений в методе перебора будет

$$2^{100} = 10^{100/\log_2 10} > 10^{33}.$$

Отметим также, что количество делений в алгоритме Евклида не превосходит пятикратного количества цифр в десятичной записи b.

Алгоритм Евклида нетрудно обобщить для нахождения наибольшего общего делителя нескольких чисел.

Обобщенный алгоритм Евклида. Дан набор целых неотрицательных чисел $A = \{a_1, a_2, \ldots, a_n\}$. Нужно найти $d = \text{нод}\ (a_1, a_2, \ldots, a_n)$.

1. Вычеркиваем все нулевые числа набора A. Наименьшее из оставшихся ставим на первое место. Получаем новый набор $A = \{a_1, a_2, \ldots\}$.
2. Если A содержит только a_1, то $d = a_1$. Конец.
3. Заменяем каждое a_j $(j \geq 2)$ на его остаток от деления на a_1. Переходим к шагу 1.

Корректность алгоритма следует из следующей леммы.

Лемма 1.2. *Пусть* $a_j \geq 0$, $j = \overline{1,n}$, *причем* $a_1 > 0$. *Пусть*

$$a_j = q_j a_1 + r_j, \quad j = \overline{2,n},$$

где $0 \leq r_j < a_1$. *Тогда* $\text{нод}\ (a_1, a_2, \ldots, a_n) = \text{нод}\ (a_1, r_2, \ldots, r_n)$.

Доказательство совпадает с доказательством леммы I.1.2 и оставляется читателю.

Пример. Используя обобщенный алгоритм Евклида, получаем

$$\text{нод}\ (10, 6, 15, 24) = (6, 10, 15, 24) = (6, 4, 3, 0) = (3, 6, 4) = (3, 0, 1) = (1, 3) = 1.$$

Числа $10, 6, 15, 24$ взаимно просты.

§ 2. Конечные непрерывные дроби

Пусть $a, b \in \mathbb{N}$, $a > b$. Запишем цепочку соотношений (1.1) алгоритма Евклида следующим образом (первое равенство делим на b, второе на r_1, третье на r_2,...)

$$\begin{aligned}
\frac{a}{b} &= q_0 + \frac{1}{b/r_1}, \\
\frac{b}{r_1} &= q_1 + \frac{1}{r_1/r_2}, \\
\frac{r_1}{r_2} &= q_2 + \frac{1}{r_2/r_3}, \\
&\vdots \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{1}{r_{n-1}/r_n}, \\
\frac{r_{n-1}}{r_n} &= q_n.
\end{aligned}$$

Следовательно,

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}. \tag{2.1}$$

Подчеркнем, что $q_n \geq 2$ (т.к. $q_n = r_{n-1}/r_n > 1$), за тривиальным исключением $a/b = 1$.

Определение. Равенство (2.1) называется разложением рационального a/b в *непрерывную (цепную) дробь*. Натуральные $q_0, \ldots, q_n$ называются *неполными частными*. Символически равенство (2.1) записывается следующим образом:

$$\frac{a}{b} = [q_0; q_1, q_2, \ldots, q_n].$$

Пример.

$$\begin{aligned}
\frac{31}{7} &= 4 + \frac{3}{7} = 4 + \frac{1}{7/3} = 4 + \frac{1}{2 + \frac{1}{3}} = [4; 2, 3], \\
\frac{8}{5} &= 1 + \frac{3}{5} = 1 + \frac{1}{5/3} = 1 + \frac{1}{1 + 2/3} = 1 + \frac{1}{1 + \frac{1}{3/2}} = 1 + \frac{1}{1 + \frac{1}{1+1/2}} = [1; 1, 1, 2].
\end{aligned}$$

Непосредственно из определений вытекает следующий результат.

Теорема 2.1. *Любое рациональное положительное число a/b единственным образом разлагается в непрерывную дробь (2.1), где $q_0 \geq 0$, $q_j \in \mathbb{N}$, причем $q_n \geq 2$ (за исключением тривиального случая $a/b = 1$).*

Определение. Пусть $a/b = [q_0; q_1, \ldots, q_n]$. Несократимые дроби

$$\frac{P_k}{Q_k} = [q_0; q_1, \ldots, q_k], \quad k = \overline{0, n}$$

называются *подходящими дробями*. Числители и знаменатели подходящих дробей называются *подходящими числителями и подходящими знаменателями* соответственно.

Подчеркнем, что последняя подходящая дробь совпадает с исходным числом, т.е.

$$\frac{P_n}{Q_n} = \frac{a}{b},$$

Однако, в общем случае, $P_n \neq a$, $Q_n \neq b$.

Пример. Найдем подходящие дроби для $\frac{210}{76}$. Имеем

$$\begin{aligned}
&\frac{210}{76} = 2 + \frac{29}{38}, \quad \frac{38}{29} = 1 + \frac{9}{29}, \quad \frac{29}{9} = 3 + \frac{2}{9}, \quad \frac{9}{2} = 4 + \frac{1}{2}, \quad \frac{2}{1} = 2; \\
&\frac{210}{76} = [2; 1, 3, 4, 2]. \\
&\frac{P_0}{Q_0} = [2] = \frac{2}{1}, \quad \frac{P_1}{Q_1} = [2; 1] = 2 + \frac{1}{1} = \frac{3}{1}, \quad \frac{P_2}{Q_2} = [2; 1, 3] = 2 + \frac{1}{1 + \frac{1}{3}} = \frac{11}{4}, \\
&\frac{P_3}{Q_3} = [2; 1, 3, 4] = 2 + \frac{1}{1 + \frac{1}{3+1/4}} = \frac{47}{17}, \quad \frac{P_4}{Q_4} = [2; 1, 3, 4, 2] = \frac{105}{38}.
\end{aligned}$$

Подходящими дробями являются $\frac{2}{1}$, $\frac{3}{1}$, $\frac{11}{4}$, $\frac{47}{17}$, $\frac{105}{38}$.

Для изучения дальнейших свойств, нам понадобится один вспомогательный результат. Для любого вещественного $x_0 \geq 0$ и положительных вещественных $x_1, x_2 \ldots, x_k$ определим

$$[x_0; x_1, x_2, \ldots, x_k] = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ldots + \cfrac{1}{x_k}}}.$$

Сразу отметим, что

$$[x_0; x_1, \ldots, x_{k-1}, \alpha] = [x_0; x_1, \ldots, x_{k-1} + 1/\alpha]. \tag{2.2}$$

Лемма 2.1. *Определим многочлены* $f_k = f_k(x_0, x_1, \ldots, x_k)$ *и* $g_k = g_k(x_0, x_1, \ldots, x_k)$ *по следующим реккурентным соотношениям*

$$\begin{array}{llll} f_{-1} = 1, & f_0 = x_0, & f_k = x_k f_{k-1} + f_{k-2}; & \\ g_{-1} = 0, & g_0 = 1, & g_k = x_k g_{k-1} + g_{k-2}, & k = 1, 2, 3, \ldots \end{array}$$

Тогда для любого $k \geq 0$

$$\frac{f_k}{g_k} = [x_0; x_1, \ldots, x_k]. \tag{2.3}$$

Доказательство. Применим метод математической индукции по $k = 0, 1, 2, \ldots$.

База индукции. Так как

$$\frac{f_0(x_0)}{g_0(x_0)} = x_0 = [x_0],$$

то утверждение леммы выполняется при $k = 0$.

Индукционный переход от k к $(k+1)$. Пусть формула (2.3) выполняется при всех $k \leq n$. Нужно доказать, что она справедлива и при $k = (n+1)$. Используя (2.2) и предположение индукции, получаем

$$\begin{aligned} &[x_0; x_1, \ldots, x_n, x_{n+1}] = [x_0; x_1, \ldots, x_n + 1/x_{n+1}] = \frac{f_n(x_0, x_1, \ldots, x_n + 1/x_{n+1})}{g_n(x_0, x_1, \ldots, x_n + 1/x_{n+1})} = \\ &= \frac{(x_n + 1/x_{n+1}) \cdot f_{n-1} + f_{n-2}}{(x_n + 1/x_{n+1}) \cdot g_{n-1} + g_{n-2}} = \frac{(x_n f_{n-1} + f_{n-2}) + f_{n-1}/x_{n+1}}{(x_n g_{n-1} + g_{n-2}) + g_{n-1}/x_{n+1}} = \frac{f_n + f_{n-1}/x_{n+1}}{g_n + g_{n-1}/x_{n+1}} = \\ &= \frac{x_{n+1} f_n + f_{n-1}}{x_{n+1} g_n + g_{n-1}} = \frac{f_{n+1}}{g_{n+1}}. \end{aligned}$$

□

Используя лемму, мы можем изучить дальнейшие свойства подходящих дробей.

Теорема 2.2. *Пусть* $a/b = [q_0; q_1, \ldots, q_n]$ *и* $P_k/Q_k = [q_0; q_1, \ldots, q_k]$ $(k = \overline{0, n})$ *— подходящие дроби для* a/b. *Справедливы следующие свойства.*

а) Числители и знаменатели определяются реккурентными соотношениями

$$\begin{array}{llll} P_{-1} = 1, & P_0 = q_0, & P_k = q_k P_{k-1} + P_{k-2}, & \\ Q_{-1} = 0, & Q_0 = 1, & Q_k = q_k Q_{k-1} + Q_{k-2}. & \end{array} \tag{2.4}$$

б) Для любого $k \in \{0, \ldots, n\}$ *справедлива формула*

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k+1}. \tag{2.5}$$

в) Последовательность подходящих дробей с четными номерами возрастает, а с нечетными убывает.

г) Подходящая дробь с четным номером меньше любой подходящей дроби с нечетным.

Доказательство. Определим натуральные P'_k и Q'_k по реккурентным соотношениям

$$\begin{array}{lll} P'_{-1}=1, & P'_0=q_0, & P'_k=q_kP'_{k-1}+P'_{k-2}, \\ Q'_{-1}=0, & Q'_0=1, & Q'_k=q_kQ'_{k-1}+Q'_{k-2}. \end{array}$$

Используя математическую индукцию, докажем формулу

$$P'_kQ'_{k-1}-P'_{k-1}Q'_k=(-1)^{k+1}. \tag{2.6}$$

База индукции. При $k=0$

$$P'_0Q'_{-1}-P'_{-1}Q'_0=q_0\cdot 0-1\cdot 1=-1=(-1)^{0+1}.$$

Индукционный переход от k к $(k+1)$. Используя предположение индукции, получаем

$$\begin{array}{rcl} P'_{k+1}Q'_k-P'_kQ'_{k+1} & = & (P'_kq_{k+1}+P'_{k-1})Q'_k-P'_k(Q'_kq_{k+1}+Q'_{k-1})=P'_{k-1}Q'_k-P'_kQ'_{k-1}= \\ & = & -(P'_kQ'_{k-1}-P'_{k-1}Q'_k)=-(-1)^{k+1}=(-1)^{k+2}. \end{array}$$

Соотношение (2.6) доказано. Из него вытекает, что дробь P'_k/Q'_k несократимая. Действительно, $d=$ нод (P'_k,Q'_k) делит правую часть (2.6) и поэтому $d=1$.

Согласно лемме 2.1

$$\frac{P'_k}{Q'_k}=\frac{f_k(q_0,\ldots,q_k)}{g_k(q_0,\ldots,q_k)}=[q_0;q_1,\ldots,q_k]=\frac{P_k}{Q_k}.$$

Так как дроби P'_k/Q'_k и P_k/Q_k несократимые, то $P'_k=P_k$, $Q'_k=Q_k$. Отсюда вытекает выполнение а) и б).

Докажем в). Используя а), б), получаем для любого $k\geq 0$

$$\begin{array}{rcl} \dfrac{P_{k+2}}{Q_{k+2}}-\dfrac{P_k}{Q_k} & = & \dfrac{P_{k+2}Q_k-P_kQ_{k+2}}{Q_{k+2}Q_k}=\dfrac{(q_{k+2}P_{k+1}+P_k)Q_k-P_k(q_{k+2}Q_{k+1}+Q_k)}{Q_{k+2}Q_k}= \\ & = & q_{k+2}\dfrac{P_{k+1}Q_k-P_kQ_{k+1}}{Q_{k+2}Q_k}=q_{k+2}\dfrac{(-1)^k}{Q_{k+2}Q_k}. \end{array}$$

Поэтому выполняется в).

Докажем г). Пусть n — нечетное. Согласно б)

$$\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^{n+1}}{Q_nQ_{n-1}}>0.$$

Учитывая в), имеем

$$\frac{P_0}{Q_0}<\frac{P_2}{Q_2}<\ldots<\frac{P_{n-1}}{Q_{n-1}}<\frac{P_n}{Q_n}<\frac{P_{n-2}}{Q_{n-2}}<\ldots<\frac{P_1}{Q_1}.$$

Следовательно, г) справедливо при нечетном n. Случай четного n рассматривается аналогично. □

Подходящие дроби удобнее находить по формулам (2.4), чем по определению.

Пример. Найдем подходящие дроби для $\frac{210}{76} = [2; 1, 3, 4, 2]$. Используя (2.4), получаем

$$\begin{array}{ll} P_{-1} = 1, & Q_{-1} = 0, \\ P_0 = 2, & Q_0 = 1, \\ P_1 = 1 \cdot 2 + 1 = 3, & Q_1 = 1 \cdot 1 + 0 = 1, \\ P_2 = 3 \cdot 3 + 2 = 11, & Q_2 = 3 \cdot 1 + 1 = 4, \\ P_3 = 4 \cdot 11 + 3 = 47, & Q_3 = 4 \cdot 4 + 1 = 17, \\ P_4 = 2 \cdot 47 + 11 = 105, & Q_4 = 2 \cdot 17 + 4 = 38. \end{array}$$

Подходящие дроби имеют вид $\frac{2}{1}$, $\frac{3}{1}$, $\frac{11}{4}$, $\frac{47}{17}$, $\frac{105}{38}$. Результаты вычислений удобно записывать в следующую таблицу

k	-1	0	1	2	3	4
q_k		2	1	3	4	2
P_k	1	2	3	11	47	105
Q_k	0	1	1	4	17	38

§ 3. Решение линейного диофантового уравнения

Уравнения, решаемые в целых числах, называются диофантовыми. Мы рассмотрим простейшее линейное уравнение

$$ax + by = c \tag{3.1}$$

относительно неизвестных $x, y \in \mathbb{Z}$. Здесь и далее считаем, что a, b, c — заданные целые. Вместе с (3.2) будем рассматривать соответствующее однородное уравнение

$$ax_0 + by_0 = 0. \tag{3.2}$$

Следующая лемма отражает хорошо известный факт о том, что *общее решение линейного неоднородного уравнения есть сумма частного решения неоднородного и общего решения однородного уравнений.*

Лемма 3.1. *Пусть пара (u, v) есть решение неоднородного уравнения (3.1), т.е. $au+bv = c$. Тогда пара (x, y) является решением (3.1), если и только если*

$$x = u + x_0, \quad y = v + y_0, \tag{3.3}$$

где (x_0, y_0) — решение однородного уравнения (3.2).

Доказательство. Если x, y имеет вид (3.3), то

$$ax + by = a(u + x_0) + b(v + y_0) = (au + bv) + (ax_0 + by_0) = c + 0 = c.$$

Возьмем теперь любое решение x, y уравнения (3.1). Положим $x_0 = x - u$, $y_0 = y - v$. Тогда

$$ax_0 + by_0 = (ax + by) - (au + bv) = 0,$$

т.е. пара (x_0, y_0) является решением однородного уравнения (3.2). □

Однородное уравнение (3.2) решается довольно просто.

Лемма 3.2. *Пусть* $d = \text{нод}\,(a, b)$. *Тогда множество решений однородного уравнения (3.2) состоит из пар* (x_0, y_0) *вида*

$$x_0 = t \cdot \frac{b}{d}, \quad y_0 = -t \cdot \frac{a}{d}, \qquad t \in \mathbb{Z}. \tag{3.4}$$

Доказательство. Очевидно, что пара (x_0, y_0) вида (3.4) есть решения (3.2). Возьмем теперь любое решение (x_0, y_0) уравнения (3.2). Положим $t = \text{нод}\,(x_0, y_0)$. Тогда

$$\frac{a}{b} = -\frac{y_0}{x_0} \quad \Longleftrightarrow \quad \frac{a/d}{b/d} = \frac{-y_0/t}{x_0/t}.$$

Так как целые y_0/t, x_0/t взаимно простые и целые a/d, b/d взаимно простые, то

$$a/d = -y_0/t, \quad b/d = x_0/t \quad (\text{либо} \quad a/d = y_0/t, \quad b/d = -x_0/t).$$

Учитывая, что $t \in \mathbb{N}$, приходим к (3.4). □

Найдем теперь какое-нибудь частное решение неоднородного уравнения (3.1).

Лемма 3.3. *Пусть* $b > 0$, $d = \text{нод}\,(a, b)$. *Пусть* P_k/Q_k *— подходящие дроби для* $a/b = [q_0; q_1, \ldots, q_n]$. *Тогда*

$$a \cdot Q_{n-1} - P_{n-1} b = (-1)^{n+1} \cdot d.$$

Доказательство. Согласно (2.5)

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

Кроме того,

$$\frac{P_n}{Q_n} = \frac{a}{b} = \frac{a/d}{b/d}.$$

Поэтому $P_n = a/d$, $Q_n = b/d$ и утверждение леммы становится очевидным. □

Лемма 3.4. *Пусть* $b > 0$ *и* $d = \text{нод}\,(a, b)$ *делит* c. *Пусть* P_k/Q_k *— подходящие дроби для* $a/b = [q_0; q_1, \ldots, q_n]$. *Положим*

$$u = (-1)^{n+1} Q_{n-1} \cdot \frac{c}{d}, \quad v = (-1)^n P_{n-1} \cdot \frac{c}{d}.$$

Тогда целые $x = u$, $y = v$ *удовлетворяют (3.1).*

Доказательство. Согласно предыдущей лемме

$$au + bv = \frac{c}{d}(-1)^{n+1}(aQ_{n-1} - bP_{n-1}) = \frac{c}{d}(-1)^{n+1}(-1)^{n+1} d = c.$$

□

Результаты этого параграфа можно сформулировать следующим образом.

Теорема 3.1. *Пусть* $d = \text{нод}\,(a, b)$ *и* $b > 0$.

а) Если d не делит c, то уравнение (3.1) не имеет решений.

б) Если $d \mid c$, то уравнение (3.1) имеет бесконечно много решений и они определяются формулами

$$x = u + \frac{b}{d} \cdot t, \quad y = v - \frac{a}{d} \cdot t, \quad t \in \mathbb{N},$$

где u, v такие же, как и в лемме 3.4.

Доказательство. Предположим, что уравнение (3.1) имеет решение. Тогда d делит левую часть (3.1). Значит, $d \mid c$. Утверждение а) доказано.

Утверждение б) вытекает из лемм 3.1, 3.2, 3.4. □

Пример. Решим уравнение

$$7x + 11y = 13.$$

Имеем $a = 7, \quad b = 11, \quad c = 13$. Сначала мы найдем нод (a, b), разложим $a/b = 7/11$ в непрерывную дробь, вычислим P_{n-1}, Q_{n-1} и определим частное решение u, v нашего уравнения. Имеем

$$\frac{11}{7} = 1 + \frac{4}{7}, \quad \frac{7}{4} = 1 + \frac{3}{4}, \quad \frac{4}{3} = 1 + \frac{1}{3}.$$

$$d = \text{нод}\,(11, 7) = (1, 3) = 1, \quad \frac{11}{7} = [1; 1, 1, 3], \quad \frac{a}{b} = \frac{7}{11} = [0; 1, 1, 1, 3].$$

q_k		0	1	1	1	3
P_k	1	0	1	1	2	7
Q_k	0	1	1	2	3	11

, $\quad n = 4, \quad P_{n-1} = 2, \quad Q_{n-1} = 3.$

$$u = (-1)^{n+1} Q_{n-1} c = -3 \cdot 13 = -39, \quad v = (-1)^n P_{n-1} c = 2 \cdot 13 = 26.$$

Теперь находим общее решение однородного уравнения. Так как $d = 1$, то

$$x_0 = 11 \cdot t, \quad y_0 = -7 \cdot t, \quad t \in \mathbb{Z}.$$

Ответ: $x = -39 + 11 \cdot t$, $y = 26 - 7 \cdot t$, $t \in \mathbb{Z}$.

§ 4. Бесконечные непрерывные дроби

4.1 Сходимость бесконечной непрерывной дроби

Определение. Пусть $q_0 \in \mathbb{N} \cup \{0\}$, $q_1, q_2, \ldots \in \mathbb{N}$. Следующее (формальное) выражение

$$[q_0; q_1, q_2, \ldots] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots}}$$

называется *бесконечной непрерывной дробью с неполными частными* $q_0, q_1, q_2, \ldots$. Несократимые дроби

$$\frac{P_k}{Q_k} = [q_0; q_1, q_2, \ldots, q_k]$$

называют *подходящими дробями.*

Подчеркнем, что подходящие дроби определяются через *конечные* непрерывные дроби. Поэтому для них остаются в силе утверждения теоремы 2.2. В частности,

$$Q_{-1} = 0, \quad Q_0 = 1, \quad Q_k = q_k Q_{k-1} + Q_{k-2}, \tag{4.1}$$

$$\left| \frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} \right| = \frac{1}{Q_k Q_{k+1}}. \tag{4.2}$$

Получим сначала нижнюю оценку скорости роста подходящих знаменателей.

Определение. *Числа Фибоначчи* $\{F_k\}_{k=0}^{\infty}$ определяются реккурентными соотношениями:

$$F_0 = 0, \quad F_1 = 1, \quad F_{k+1} = F_k + F_{k-1}.$$

Лемма 4.1. *Справедлива оценка* $Q_k \geq F_{k+1}$, $k = -1, 0, 1, 2, 3, \ldots$.

Доказательство. По определениям, $Q_{-1} = F_0$, $Q_0 = F_1$. При $k \geq 2$, используя метод математической индукции, имеем $Q_k = q_k Q_{k-1} + Q_{k-2} \geq Q_{k-1} + Q_{k-2} \geq F_k + F_{k-1} = F_{k+1}$. □

Нетрудно получить следующие оценки

$$F_k \geq \varphi^{k-2}, \qquad Q_k \geq \varphi^{k-1}, \quad k = 1, 2, \ldots \quad (\varphi \text{ — золотое сечение}).$$

Напомним, что любая *конечная* непрерывная дробь равна рациональному числу.

Теорема 4.1. *Для любой бесконечной непрерывной дроби* $[q_0; q_1, q_2, \ldots]$ *существует предел*

$$\alpha = \lim \frac{P_k}{Q_k},$$

причем число α *является иррациональным и имеет место оценка*

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k Q_{k+1}}, \quad k = 0, 1, 2, \ldots \tag{4.3}$$

Доказательство. Положим $\beta_k = P_k/Q_k$. Используем теорему 2.2. Согласно в) последовательность β_{2k} строго возрастает, а согласно г) она ограничена сверху. Значит,

$$\exists \alpha' \in \mathbb{R} : \qquad \lim_{k \to +\infty} \beta_{2k} = \sup_{k \in \mathbb{N}} \beta_{2k} = \alpha'.$$

Аналогичным образом, доказывается, что существует предел

$$\lim_{k \to +\infty} \beta_{2k+1} = \inf_{k \in \mathbb{N}} \beta_{2k+1} = \alpha''.$$

В силу теоремы 2.2 г), числа α' и α'' лежат между β_k и β_{k+1} при любом выборе номера k. Поэтому, учитывая (4.2), получаем

$$|\alpha' - \alpha''| \leq |\beta_k - \beta_{k+1}| = \frac{1}{Q_k Q_{k+1}} \to 0.$$

Следовательно, $\alpha' = \alpha'' \alpha$, последовательность β_k сходится.

Докажем (4.3). Так как $\alpha = \sup \beta_{2k} = \inf \beta_{2k+1}$, то α лежит между β_k и β_{k+1}. Поэтому

$$\left|\alpha - \frac{P_k}{Q_k}\right| = |\alpha - \beta_k| < |\beta_{k+1} - \beta_k| = \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k Q_{k+1}}.$$

Осталось доказать, что α иррациональное. Предположим противное: $\alpha = a/b$, $a, b \in \mathbb{N}$. Последовательность $\{Q_k\}_{k=2}^{\infty}$ возрастает. Поэтому для всех k, кроме возможно одного

$$\frac{a}{b} \neq \frac{P_k}{Q_k}, \quad aQ_k - bP_k \neq 0, \quad |aQ_k - bP_k| \geq 1,$$
$$\left|\alpha - \frac{P_k}{Q_k}\right| = \left|\frac{a}{b} - \frac{P_k}{Q_k}\right| = \left|\frac{aQ_k - bP_k}{Q_k}\right| \geq \frac{1}{bQ_k}.$$

Сравнивая последнюю оценку и (4.3), получаем $1/(bQ_k) < 1/(Q_k Q_{k+1})$, т.е. $b > Q_{k+1}$. Это невозможно, т.к. $Q_k \to +\infty$. □

Определение. Число $\alpha = \lim \dfrac{P_k}{Q_k}$ называют *значением непрерывной дроби* $[q_0; q_1, q_2, \ldots]$ и пишут $\alpha = [q_0; q_1, q_2, \ldots]$.

4.2 Разложение произвольного вещественного в непрерывную дробь

Определение. Для любого вещественного α определим

$$[\alpha] = \max\{k \in \mathbb{Z} : k \leq \alpha\} \quad \text{— целая часть } \alpha,$$
$$\{\alpha\} = \alpha - [\alpha] \quad \text{— дробная часть } \alpha.$$

Таким образом, $\alpha = [\alpha] + \{\alpha\}$. Подчеркнем, что $\{\alpha\} \in [0, 1)$.

Пример. $[2.7] = 2$, $\{2.7\} = 0.7$; $[1/5] = 0$, $\{1/5\} = 1/5$; $[\pi] = 3$, $\{\pi\} = 0.14\ldots$; $[e] = 2$, $\{e\} = 0.71\ldots$; $[-1.5] = -2$, $\{-1.5\} = 0.5$.

Рассмотрим теперь вопрос: *каким образом произвольное α разложить в бесконечную непрерывную дробь?* Другими словами, для заданного $\alpha \in (0, +\infty)$ нужно найти такие $q_0 \in \mathbb{Z}$ и $q_1, q_2, \ldots \in \mathbb{N}$, что

$$\alpha = [q_0; q_1, q_2, \ldots] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots}}.$$

Случай рационального α рассмотрен в § 2. Далее будем считать, что α иррациональное. Выбор q_0 очевиден: $q_0 = [\alpha]$. Тогда

$$\alpha = [\alpha] + \{\alpha\} = q_0 + \frac{1}{\alpha_1} = [q_0; \alpha_1], \tag{4.4}$$

где $\alpha_1 = \frac{1}{\{\alpha\}} > 1$. Вещественное α_1 можно разложить аналогичным образом

$$\alpha_1 = q_1 + \frac{1}{\alpha_2} = [q_1; \alpha_2],$$

где $q_1 = [\alpha_1] > 0$, $\alpha_2 = \frac{1}{\{\alpha_1\}} > 1$. Учитывая (4.4), получаем

$$\alpha = q_1 + \frac{1}{\alpha_2} = q_1 + \frac{1}{q_1 + \dfrac{1}{\alpha_2}} = [q_0; q_1, \alpha_2].$$

Далее мы точно таким же образом представляем α_2, α_3, ... В итоге, получаем

$$\alpha = [q_0; q_1, \ldots, q_k, \alpha_{k+1}], \quad k = 0, 1, 2, \ldots, \tag{4.5}$$

где последовательности α_k и q_k определяются реккурентными соотношениями

$$\begin{aligned} &\alpha_0 = \alpha, \quad \alpha_{k+1} = \frac{1}{\{\alpha_k\}}; \\ &q_k = [\alpha_k], \quad k = 0, 1, 2, \ldots \end{aligned} \tag{4.6}$$

Т.к. α — иррациональное, то $\alpha_k > 1$, $q_k \in \mathbb{N}$ при $k \geq 1$.

Определение. Вещественные α_k, определенные формулами (4.6), называют *остатками* непрерывной дроби числа α.

Теорема 4.2. *Пусть α — иррациональное вещественное. Определим целые q_k по формулам (4.6). Тогда $[q_0; q_1, q_2, \ldots] = \alpha$, причем*

$$\frac{1}{Q_k(Q_{k+1} + Q_k)} < \left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}}, \quad k = 0, 1, 2, \ldots \tag{4.7}$$

Доказательство. Используя (4.5) и лемму 2.1, получаем

$$\alpha = [q_0; q_1, \ldots, q_k, \alpha_{k+1}] = \frac{f_{k+1}(q_0; q_1, \ldots, q_k, \alpha_{k+1})}{g_{k+1}(q_0; q_1, \ldots, q_k, \alpha_{k+1})}.$$

Вспоминая определение функций f_{k+1}, g_{k+1} и учитывая, что

$$f_k(q_0; q_1, \ldots, q_k) = P_k, \quad g_k(q_0; q_1, \ldots, q_k) = Q_k,$$

приходим к равенству

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

Из последнего соотношения и (2.5) вытекает

$$\begin{aligned} &Q_k \alpha - P_k = \frac{(-1)^k}{\alpha_{k+1} Q_k + Q_{k-1}}. \\ &\left|\alpha - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k(\alpha_{k+1} Q_k + Q_{k-1})} \to 0. \end{aligned}$$

Поэтому $\alpha = [q_0; q_1, q_2, \ldots]$. Осталось доказать (4.7). Так как $q_{k+1} = [\alpha_{k+1}]$, то

$$\begin{aligned} &\alpha_{k+1} < q_{k+1} + 1, \\ &\alpha_{k+1} Q_k + Q_{k-1} < (q_{k+1} + 1) Q_k + Q_{k-1} = Q_{k+1} + Q_k, \\ &\left|\alpha - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k(\alpha_{k+1} Q_k + Q_{k-1})} \geq \frac{1}{Q_k(Q_{k+1} + Q_k)}. \end{aligned}$$

Первое неравенство из (4.7) доказано. Второе неравенство следует из (4.3). □

Замечание 4.1. Любое вещественное *единственным образом* разлагается в непрерывную дробь. Полного доказательства этого факта мы не приводим. Из изложенного выше вытекает, что q_0 и q_1 определяется единственным образом.

Следствие 4.1. *Вещественное положительное α является иррациональным числом тогда и только тогда, когда оно раскладывается в бесконечную непрерывную дробь.*

Доказательство является очевидным следствием теорем 4.1, 4.2. □

Неравенства (4.7) дают оценки погрешности приближенной формулы

$$\alpha \approx \frac{P_k}{Q_k}.$$

Подходящие дроби дают очень хорошие приближения вещественных чисел дробями с небольшими знаменателями[1]. Это послужило одной из причин интереса к конструкции непрерывных дробей.

4.3 Примеры

Квадратичные иррациональности. Найдем разложение $\alpha = \sqrt{2}$ в непрерывную дробь. Имеем

$$\begin{aligned}
&\alpha_0 = \sqrt{2}, \quad q_0 = [\sqrt{2}] = 1,\\
&\alpha_1 = \frac{1}{\{\alpha_0\}} = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1, \quad q_1 = [\alpha_1] = 2,\\
&\alpha_2 = \frac{1}{\{\alpha_1\}} = \frac{1}{\sqrt{2}-1} = \alpha_1.
\end{aligned}$$

Каждый α_j однозначно определяется предыдущим α_{j-1}. Поэтому из условия $\alpha_2 = \alpha_1$ следует, что все α_j равны α_1 при $j \geq 2$ и все q_j равны $q_1 = 2$ при $j \geq 2$. Значит, разложение в непрерывную дробь будет обладать периодичностью:

$$\sqrt{2} = [1; 2, 2, \ldots] = [1; \overline{2}].$$

Отметим, что согласно теореме Лагранжа (которую мы не будем доказывать) *непрерывная дробь иррационального α является периодической тогда и только тогда, когда α имеет вид (квадратичная иррациональность)*

$$\alpha = \frac{a+\sqrt{d}}{b}, \quad a, d, b \in \mathbb{N},\ \sqrt{d} \notin \mathbb{N}.$$

Другие иррациональности. Для некоторых чисел, не являющихся квадратичными иррациональностями, удается найти закономерность образования неполных частных. Например,

$$\begin{aligned}
e &= [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots],\\
\operatorname{tg} 1 &= [1; 1, 1, 3, 1, 5, 1, 7, 1, 9, \ldots].
\end{aligned}$$

[1] наилучшие в некотором смысле

Однако таких примеров крайне мало. Для числа π соответствующая закономерность неизвестна. Найдем первые три подходящие дроби для π. Имеем

$$\alpha_0 = \pi = 3.14159+, \quad q_0 = [\pi] = 3,$$
$$\alpha_1 = \frac{1}{\{\alpha_0\}} = \frac{1}{\pi - 3} = 7.0625+, \quad q_1 = [\alpha_1] = 7,$$
$$\alpha_2 = \frac{1}{\{\alpha_2\}} = \frac{1}{0.0625+} = 15.996+, \quad q_2 = [\alpha_2] = 15.$$
$$\pi = [3; 7, 15, \ldots]$$

q_k		3	7	15
P_k	1	3	22	333
Q_k	0	1	7	106

Подходящими дробями являются

$$\frac{P_0}{Q_0} = 3, \quad \frac{P_1}{Q_1} = \frac{22}{7}, \quad \frac{P_2}{Q_2} = \frac{333}{106}.$$

Согласно (4.7)

$$\left|\pi - \frac{22}{7}\right| = \left|\pi - \frac{P_1}{Q_1}\right| \le \frac{1}{Q_1 Q_2} = \frac{1}{7 \cdot 106} < 1.4 \cdot 10^{-4};$$
$$\left|\pi - \frac{333}{106}\right| = \left|\pi - \frac{P_2}{Q_2}\right| \le \frac{1}{Q_2 Q_3} < \frac{1}{Q_2^2} = \frac{1}{106^2} < 8.9 \cdot 10^{-5}.$$

Численные упражнения к главе II

1. Найти наибольшие общие делители

$$(28, 12, 60, 100), \quad (255, 123, 211, 190), \quad (1024, 26871031131)$$

2. Найти разложение в непрерывную дробь и выписать подходящие дроби для следующих рациональных чисел

$$\frac{147}{13}, \quad \frac{129}{111}, \quad \frac{1135}{129}, \quad \frac{1024}{7013}.$$

3. Решить уравнения

$$11x + 23y = 24, \quad 15x + 19y = 1, \quad 15x + 19y = 1,$$
$$253x - 449y = 1, \quad 53x + 47y = 11, \quad 81x - 48y = 33,$$
$$258x - 172y = 112, \quad 38x + 114y = 209, \quad 122x + 129y = 2.$$

4. Найти разложения в непрерывную дробь чисел $\sqrt{5}$, $\sqrt{17}$, $\sqrt{19}$.

5. Выписать первые подходящие дроби к e и $\operatorname{tg} 1$, пока не будет найдено рациональное приближение с погрешностью 10^{-4}. Для оценки погрешности используйте теорему 4.2.

6. У какого числа подходящие знаменатели самые маленькие?

7. Вычислить значение непрерывной дроби $[1; \overline{1, 2}] = [1; 1, 2, 1, 2, 1, 2, \ldots]$.

Глава III
Важнейшие функции теории чисел

Функция, определенная на множестве натуральных чисел $\mathbb{N}$, называется *арифметической* (числовой). В этой главе мы рассмотрим некоторые основные арифметические функции, возникающие в теории чисел.

§ 1. Мультипликативные функции

Определение. Арифметическая функция θ называется *мультипликативной*, если

1) $\theta(1) = 1$;

2) для любых взаимно простых a и b выполняется равенство: $\theta(ab) = \theta(a) \cdot \theta(b)$.

Пример. Функция $\theta(a) = a^s$ $(s \in \mathbb{R})$ является мультипликативной.

Лемма 1.1. *Пусть функция θ мультипликативная. Тогда*

а) если $a_1, \ldots, a_s$ — натуральные попарно взаимно простые, то

$$\theta(a_1 \cdot \ldots \cdot a_s) = \theta(a_1) \cdot \ldots \cdot \theta(a_s).$$

б) если $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — каноническое разложение натурального n, то

$$\theta(n) = \theta(p_1^{\alpha_1}) \cdot \theta(p_1^{\alpha_1}) \cdot \ldots \cdot \theta(p_s^{\alpha_s}). \tag{1.1}$$

Доказательство. Каждое a_j взаимно просто с произведением любых из оставшихся a_i. Поэтому

$$\theta(a_1 \cdot \ldots \cdot a_{s-1} a_s) = \theta(a_1 \cdot \ldots \cdot a_{s-1}) \cdot \theta(a_s) = \theta(a_1 \cdot \ldots \cdot a_{s-2}) \cdot \theta(a_{s-1)}) \cdot \theta(a_s) = \ldots = \theta(a_1) \cdot \ldots \cdot \theta(a_s).$$

Утверждение б) следует из а), так как нод $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ при $i \neq j$. □

Лемма 1.2. *Любая арифметическая функция θ, удовлетворяющая (1.1) и условию $\theta(1) = 1$, является мультипликативной.*

Доказательство. Если натуральные a и b взаимно просты, то они не имеют общих простых делителей и согласно (1.1) $\theta(ab) = \theta(a)\theta(b)$. □

Таким образом, *мультипликативная функция однозначно опредяляется своими значениями в точках вида p^α.*

Лемма 1.3. *Произведение мультипликативных функций является мультипликативной функцией.*

Доказательство. Пусть $\theta = \theta_1 \cdot \ldots \cdot \theta_s$, где θ_j — мультипликативные функции. Тогда $\theta(1) = 1$. Пусть нод $(a, b) = 1$. Тогда

$$\theta(ab) = \prod_{i=1}^{s} \theta_i(ab) = \prod_{i=1}^{s} \theta_i(a)\theta_i(b) = \left(\prod_{i=1}^{s} \theta_i(a)\right)\left(\prod_{i=1}^{s} \theta_i(b)\right) = \theta(a)\theta(b).$$

□

Всюду ниже в выражениях вида

$$\sum_{d|n}(\ldots)$$

суммирование ведется по всем *натуральным* делителям целого n.

Теорема 1.1. *Пусть функция θ мультипликативная. Определим $f : \mathbb{N} \to \mathbb{R}$ по формуле*

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

Тогда функция f также является мультипликативной, причем

$$f(n) = \prod_{i=1}^{s} \left(1 + \theta(p_i) + \theta(p_i^2) + \ldots + \theta(p_i^{\alpha_i})\right), \tag{1.2}$$

где $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — каноническое разложение натурального n.

Доказательство. Докажем, что f мультипликативная. Очевидно, что $f(1) = \theta(1) = 1$. Осталось проверить выполнение условия 2).

Возьмем любые взаимно простые $a, b \in \mathbb{N}$. Докажем сначала, что

$$d \mid ab \quad \Longleftrightarrow \quad \exists d_1, d_2 \in \mathbb{N} : \ \ d = d_1 d_2,\ d_1 \mid a,\ d_2 \mid b. \tag{1.3}$$

Действительно, если $d_1 \mid a$, $d_2 \mid b$, то $d_1 d_2 \mid ab$. Возьмем теперь любой $d \mid ab$. Положим $d_1 = $ нод (a, d) и $d_2 = d/d_1$. Тогда $d = d_1 d_2$. Кроме того,

$$d_2 \mid ab, \quad \text{нод } (d_2, a) = \text{нод } \left(\frac{d}{\text{нод } (a, d)}, a\right) = 1.$$

Поэтому $d_2 \mid b$. Утверждение (1.3) доказано. Из условия нод $(a, b) = 1$ дополнительно следует, что нод $(d_1, d_2) = 1$. Поэтому

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

Осталось доказать (1.2). Используя (1.1), получаем

$$f(n) = \prod_{i=1}^{s} f(p_i^{\alpha_i}).$$

Возьмем любой i. Все делители числа $p_i^{\alpha_i}$ имеют вид $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$. Значит,

$$f(p_i^{\alpha_i}) = \sum_{d|p_i^{\alpha_i}} \theta(d) = \theta(1) + \theta(p_i) + \theta(p_i^2) + \ldots + \theta(p_i^{\alpha_i}).$$

Из двух последних соотношений и равенства $\theta(1) = 1$ вытекает (1.2). □

§ 2. Число делителей и сумма делителей

Определим

$\tau(n)$ — число положительных делителей натурального n,

$\sigma(n)$ — сумма положительных делителей натурального n.

Пример. Делителями числа 6 являются $1, 2, 3, 6$. Поэтому $\tau(6) = 4, \sigma(6) = 1+2+3+6 = 12$.

Пусть $n = p^\alpha$, где p — простое, $\alpha \in \mathbb{N}$. Тогда множество делителей n состоит из чисел $1, p, p^2, \ldots, p^\alpha$. Поэтому

$$\tau(p^\alpha) = \alpha + 1, \qquad \sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}. \tag{2.1}$$

Теорема 2.1. *Функции $\tau, \sigma : \mathbb{N} \to \mathbb{N}$ являются мультипликативными. Кроме того, если $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — каноническое разложение натурального n, то*

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_s + 1), \tag{2.2}$$

$$\sigma(n) = \prod_{i=1}^{s} \left(1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}\right) = \prod_{i=1}^{s} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \tag{2.3}$$

Доказательство. Функции $\theta \equiv 1$ и $\theta(n) = n$ мультипликативные. Поэтому функции

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} \theta(n),$$

являются мультипликативными по теореме 1.1. Формулы (2.2), (2.3) следуют из (1.1), (2.1). □

Пример. Так как $720 = 2^4 \cdot 3^2 \cdot 5$, то

$$\tau(720) = (4+1)(2+1)(1+1) = 30, \quad \sigma(720) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 2418.$$

§ 3. Функция Мебиуса

Определение. *Функцией Мебиуса* называется мультипликативная функция μ, которая на степенях простых определяется следующим образом

$$\mu(p^\alpha) = \begin{cases} -1, & \alpha = 1, \\ 0, & \alpha \geq 2 \end{cases}.$$

Согласно определению

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^s, & \text{если } n = p_1 p_2 \ldots p_s, \\ 0 & \text{в противном случае.} \end{cases}$$

Здесь p_i попарно различные простые.

Пример.

$$\mu(1)=1,\quad \mu(2)=-1,\quad \mu(3)=-1,\quad \mu(4)=0,\quad \mu(5)=-1,\quad \mu(6)=1,$$
$$\mu(7)=-1,\quad \mu(8)=0,\quad \mu(9)=0,\quad \mu(10)=1,\quad \mu(11)=-1,\quad \mu(12)=0.$$

Всюду ниже $\prod\limits_{p|n}(\dots)$ — произведение по всем простым делителям $p \mid n$.

Лемма 3.1. *Пусть θ — мультипликативная функция. Тогда для любого $n>1$*

$$\sum_{d|n}\mu(d)\theta(d)=\prod_{p|n}(1-\theta(p)). \tag{3.1}$$

Доказательство. Пусть $n=p_1^{\alpha_1}\dots p_s^{\alpha_s}$ (каноническое разложение). Произведение μ и θ есть мультипликативная функция. Поэтому согласно теореме 1.1

$$\sum_{d|n}\mu(d)\theta(d)=\prod_{i=1}^{s}\Big(1+\theta(p_i)\mu(p_i)+\theta(p_i^2)\mu(p_i^2)+\dots+\theta(p_i^{s_i})\mu(p_i^{s_i})\Big)=\prod_{i=1}^{s}(1-\theta(p_i)).$$

□

Лемма 3.2. *Для любого натурального n*

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1,\\ 0, & n>1.\end{cases} \tag{3.2}$$

Доказательство. При $n=1$ требуемая формула очевидна. При $n>1$ она вытекает из соотношения (3.1), в котором $\theta\equiv 1$. □

Теорема 3.1 (формула обращения Мебиуса)**.** *Пусть $f,g:\mathbb{N}\to\mathbb{R}$. Тогда*

$$g(n)=\sum_{d|n}f(d)\quad\Longleftrightarrow\quad f(n)=\sum_{d|n}\mu(n)\cdot g(n/d). \tag{3.3}$$

Доказательство. Пусть выполняется первая формула из (3.3). Так как

$$d\mid n,\ r\mid(n/d)\quad\Longleftrightarrow\quad rd\mid n\quad\Longleftrightarrow\quad r\mid n,\ d\mid(n/r),$$

то, используя определение g, получаем

$$\sum_{d|n}\mu(d)\cdot g(n/d)=\sum_{d|n}\mu(d)\cdot\sum_{r|(n/d)}f(r)=\sum_{rd|n}\mu(d)f(r)=\sum_{r|n}\left(f(r)\cdot\sum_{d|(n/r)}\mu(d)\right).$$

Согласно (3.2)

$$\sum_{d|(n/r)}\mu(d)=\begin{cases}1, & r=n,\\ 0, & r<n.\end{cases}$$

Поэтому справедлива вторая формула из (3.3).

Пусть теперь выполняется вторая формула из (3.3). Тогда

$$f(d) = \sum_{r|d} \mu(r) g(d/r), \quad \sum_{d|n} f(d) = \sum_{d|n} \sum_{r|d} \mu(r) g(d/r).$$

Условие $r \mid d$ эквивалентно $d = qr$, где $r \in \mathbb{N}$. Поэтому

$$\sum_{d|n} \sum_{r|d} \mu(r) g(d/r) = \sum_{qr|n} \mu(r) g(q) = \sum_{q|n} g(q) \sum_{r|(n/q)} \mu(r) = g(n).$$

Поэтому справедлива первая формула из (3.3). □

Примеры.

1. Обращением формулы $\tau(n) = \sum\limits_{d|n} 1$ является $\sum\limits_{d|n} \mu(n)\tau(n/d) = 1$.

2. Обращением формулы $\sigma(n) = \sum\limits_{d|n} d$ является $\sum\limits_{d|n} \mu(n)\sigma(n/d) = n$.

§ 4. Функция Эйлера

Определение. *Функция Эйлера* φ — это арифметическая функция. Значение $\varphi(n)$ равно количеству целых от 1 до n, которые взаимно просты с n.

Пример. $\varphi(6) = 2$, $\varphi(10) = 4$.

Рассмотрим простейшие свойства функции Эйлера. По определению

$$\varphi(1) = 1, \quad 1 \le \varphi(n) \le n - 1.$$

Любое простое p взаимно просто со всеми числами из $\{1, 2, \ldots, p-1\}$. Поэтому

$$\varphi(p) = p - 1.$$

Вычислим $\varphi(p^\alpha)$. Подсчитаем числа от 1 до p^α, которые не взаимно просты с p^α. Такие числа делятся на p и имеют вид kp, где $k = 1, 2, \ldots, p^{\alpha-1}$. Их количество равно $p^{\alpha-1}$. Поэтому

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right). \tag{4.1}$$

Теорема 4.1. *Для любого натурального* n

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{4.2}$$

Доказательство. Используя (3.2), получаем

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

Условие $d \mid \text{нод } (k,n)$ эквивалентно тому, что $d \mid k$ и $d \mid n$. Поэтому

$$\varphi(n) = \sum_{d \mid n} \left(\sum_{k \in [1,n]:\ d \mid k} \mu(d) \right) = \sum_{d \mid n} \mu(d) \cdot f_n(d),$$

где $f_n(d)$ — количество целых от 1 до n, которые кратны d. Такие целые имеют вид jd, где $j = 1, 2, \ldots, n/d$. Поэтому $f_n(d) = n/d$. □

Следствие 4.1. *Функция Эйлера является мультипликативной, причем при* $n > 1$

$$\varphi(n) = \prod_{i=1}^{s} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p} \right), \tag{4.3}$$

$$n = \sum_{d \mid n} \varphi(d), \tag{4.4}$$

где $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ *— каноническое разложение* n.

Доказательство. Функция $d \in \mathbb{N} \to \mu(d)/d$ является мультипликативной (как произведение двух мультипликативных функций). Поэтому мультипликативность φ вытекает из (4.2) и теоремы 1.1. Формула (4.3) следует из (1.1) и (4.1). Для доказательства (4.4) достаточно воспользоваться (4.2) и формулой обращения Мебиуса, где $g(x) = x$, $f = \mu$. □

Замечание 4.1. Формулу (4.3) также можно вывести из (1.2), (4.2) и мультипликативности μ.

Численные упражнения к главе III

1. Вычислить $\tau(n)$, $\sigma(n)$, $\varphi(n)$ при $n = 100$, $n = 1000$, $n = 550$.
2. Вычислить $\tau(n)$, $\sigma(n)$, $\varphi(n)$ при $n = 2^{100} \cdot 7^2 \cdot 11^{10}$.

Глава IV
Сравнения

Всюду в этой главе считаем, что m целое и $m \geq 2$.

§ 1. Сравнения и их основные свойства

Определение. Целые a и b называются *сравнимыми по модулю* m, если $m \mid (a-b)$. Отношение сравнимости записывается следующим образом

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

Эквивалентное определение. Целые a и b называются *сравнимыми по модулю* m, если существует такой $k \in \mathbb{Z}$, что $a = b + km$, т.е. a и b дают одинаковые остатки от деления на m.

Пример. $-8 \equiv -1 \equiv 6 \equiv 13 \pmod{7}$.

Рассмотрим простейшие свойства сравнений, которые вытекают из теории делимости.

1. $a \equiv a \pmod{m}$.
2. Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$
3. Если $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

   Доказательство. Первые два свойства очевидны. Для доказательства 3-го достаточно заметить, что $(a-c) = (a-b) + (b-c)$. □

4. Сравнения (по одинаковому модулю) можно почленно складывать, вычитать и умножать, т.е. если $a_i \equiv b_i \pmod{m}$, $i = 1, 2$, то

   $$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}, \quad a_1 a_1 \equiv b_1 b_2 \pmod{m}.$$

   Доказательство первых двух соотношений оставим читателю. Докажем последнее:

   $$a_i = b_i + k_i m,\ i = 1, 2 \quad \Longrightarrow \quad a_1 a_2 = (b_1 + k_1 m)(b_2 + k_2 m) \equiv b_1 \cdot b_2 \pmod{m}.$$

   □

5. Пусть $x \equiv y \pmod m$, а $P(x)$ — многочлен с целыми коэффициентами. Тогда
$$P(x) \equiv P(y) \pmod m.$$

Доказательство. Пусть $P(x) = a_0 + a_1x + \ldots + a_nx^n$. Согласно свойству 4
$$x^2 \equiv y^2 \pmod m, \quad x^3 \equiv y^3 \pmod m, \ldots, x^n \equiv y^n \pmod m.$$
$$a_kx^k \equiv a_ky^k \pmod m, \quad k = 0, 1, \ldots, n,$$
$$a_0 + a_1x + \ldots a_nx^n \equiv a_0 + a_1y + \ldots a_ny^n \pmod m.$$
□

6. Обе части сравнения и модуль можно умножить на натуральное, либо разделить на их общий делитель, то есть для любого $d \in \mathbb{N}$
$$a = b \pmod m \iff ad \equiv bd \pmod{md}.$$

7. Обе части сравнения можно делить на общий делитель, если он взаимно прост с модулем, т.е.
$$ad \equiv bd \pmod m, \quad (d, m) = 1 \implies a \equiv b \pmod m.$$

Доказательство. Так как $m \mid d(a - b)$ и нод $(m, d) = 1$, то $m \mid (a - b)$ по следствию I.4.2 б). □

Отметим, что условие $(d, m) = 1$ выбросить нельзя. Например, $9 \equiv 6 \pmod 3$, однако $3 \not\equiv 2 \pmod 3$.

8. Если $a \equiv b \pmod m$, то нод $(a, m) =$ нод (b, m).

Доказательство. Так как $a \equiv b \pmod m$, то $a = mk + b$. □

9. Если $a \equiv b \pmod m$ и $d \mid m$, то $a \equiv b \pmod d$.

Доказательство. Так как $d \mid m$, $m \mid (a - b)$, то $d \mid (a - b)$. □

10. Если $a \equiv b \pmod{m_i}$, $i = \overline{1, n}$, то $a \equiv b \pmod M$, где $M =$ нок $(m_1, \ldots, m_n)$

Доказательство. По условию $(a - b)$ есть общее кратное $m_1, \ldots, m_n$. Поэтому $a - b$ делится на нок $(m_1, \ldots, m_n)$ по теореме I.1.2. □

Пример. Докажем, что уравнение
$$x^2 - 3y^2 = 2 \tag{1.1}$$
не имеет решений в целых числах. Действительно, если решение существует, то
$$x^2 \equiv 2 \pmod 3.$$
Любоей целое x сравнимо с одним из чисел $0, 1, 2$ по модулю 3. Так как
$$0^2 \equiv 0 \pmod 3, \quad 1^2 \equiv 1 \pmod 3, \quad 2^2 \equiv 1 \pmod 3,$$
то $x^2 \equiv 0 \pmod 3$ либо $x^2 \equiv 1 \pmod 3$. Значит, сравнение $x^2 \equiv 2 \pmod 3$ не имеет решений. Поэтому и исходное уравнение (1.1) не имеет решений в целых числах.

§ 2. Классы вычетов

Определение. Для любого $a \in \mathbb{Z}$ множество чисел

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$$

называется *классом вычетов по модулю* m.

По определению $\overline{a} = \{a + km : k \in \mathbb{Z}\}$.

Пример. Пусть $m = 3$. Тогда

$$\begin{aligned} \overline{0} &= \{0, \pm 3, \pm 6, \pm 9, \ldots\}, \\ \overline{1} &= \{1, 4, 7, 10, \ldots\} \cup \{-2, -5, -8, -11 \ldots\}, \\ \overline{2} &= \{2, 5, 8, 11, \ldots\} \cup \{-1, -4, -7, -10\}. \end{aligned}$$

Лемма 2.1. *Справедливы следующие свойства.*

а) Если $a \equiv b \pmod{m}$, *то* $\overline{a} = \overline{b}$. *Если* $a \not\equiv b \pmod{m}$, *то* $\overline{a} \cap \overline{b} = \emptyset$.

б) Существует ровно m *классов вычетов по модулю* m, *причем*

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{(m-1)}.$$

Доказательство. Пусть $a \equiv b \pmod{m}$. Согласно свойству 3 (из § 1) $x \equiv a \pmod{m}$ тогда и только тогда, когда $x \equiv b \pmod{m}$. Поэтому $\overline{a} = \overline{b}$.

Пусть $a \not\equiv b \pmod{m}$. Возьмем любой $x \in \overline{a}$. Тогда $x \equiv a \pmod{m}$ и поэтому $x \not\equiv b \pmod{m}$, т.е. $x \notin \overline{b}$. Значит, $\overline{a} \cap \overline{b} = \emptyset$.

Докажем б). Возьмем любое $x \in \mathbb{Z}$. Его можно представить в виде

$$x = km + r, \quad 0 \le r < m - 1.$$

Значит, $x \in \overline{r}$, где $0 \le r < m-1$. Осталось заметить, что все числа множества $\{0, 1, \ldots, m-1\}$ попарно несравнимы по модулю m. □

Определение. Элементы множества $\overline{a}$ называются *вычетами класса* $\overline{a}$.

Класс вычетов однозначно определятся любым своим элементов (представителем). В качестве этого представителя часто берут *наименьший неотрицательный вычет.*

Пример. Пусть $m = 5$. Тогда 3 есть наименьший неотрицательный вычет класса $\overline{8}$.

Напомним одно определение из курса алгебры.

Определение. Непустое множество K называется *кольцом*, если на нем определены две бинарные операции:

сложение каждой паре $x, y \in K$ ставит в соответствие элемент $z = (x + y) \in K$;

умножение каждой паре $x, y \in K$ ставит в соответствие элемент $z = x \cdot y \in K$.

При этом для любых $x, y, z \in K$ выполняются условия

1) $x + y = y + x$ (коммутативность сложения);

2) $(x + y) + z = x + (y + z)$ (ассоциативность сложения);

3) $\exists 0 \in K: \quad x + 0 = x$ (существование нулевого элемента);

4) $\forall x \in K \quad \exists(-x) \in K: \ x+(-x) = 0$ (существование обратного элемента по сложению);

5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (ассоциативность умножения);

6) $(x + y) \cdot z = x \cdot z + y \cdot z$, $z \cdot (x + y) = z \cdot x + z \cdot y$ (дистрибутивность).

Если дополнительно $x \cdot y = y \cdot x$, то K называется *коммутативным кольцом*. Если существует такой элемент $1 \in K$, что $x \cdot 1 = 1 \cdot x = x$, то K называется *кольцом с единицей*.

Условие 4) позволяет определить операцию вычитания следующим образом

$$x - y = x + (-y).$$

Таким образом элементы кольца можно складывать, вычитать и умножать.

В рассматриваемых ниже примерах операции сложения и умножения определяются «обычным» образом.

Примеры.

1. Множество вещественных чисел $\mathbb{R}$, рациональных $\mathbb{Q}$ и целых $\mathbb{Z}$ являются коммутативными кольцами с единицами.
2. Множество натуральных $\mathbb{N}$ не является кольцом.
3. Множество $\mathbb{Z}_+ = \mathbb{Z} \cap [0, +\infty)$ не является кольцом.
4. Множество $\mathrm{M}_n(\mathbb{R})$, состоящее из матриц размера $n \times n$ с вещественными элементами, есть кольцо с единицей. Однако кольцо $\mathrm{M}_n(\mathbb{R})$ не является коммутативным (умножение матриц не коммутативно).

Определение. Через $\mathbb{Z}_m$ будем обозначать множество классов вычетов по модулю m[1].

В силу вышеизложенного,

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

На множестве $\mathbb{Z}_m$ можно определить операции сложения и умножения следующим образом

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}. \tag{2.1}$$

Пример. Пусть $m = 5$. Тогда $\overline{2} + \overline{3} = \overline{0}$, $\overline{2} - \overline{3} = \overline{4}$.

Нетрудно проверить, что результаты операций (2.1) не зависят от выбора представителей классов $\overline{a}$ и $\overline{b}$, Действительно, пусть $a_1, a_2 \in \overline{a}$ и $b_1, b_2 \in \overline{b}$. Тогда $a_1 \equiv a_2 \pmod m$, $b_1 \equiv b_2 \pmod m$. Поэтому по свойству 4 сравнений

$$a_1 + b_1 \equiv a_2 + b_2 \pmod m, \quad a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod m.$$

Следовательно,

$$\overline{a_1 + b_1} = \overline{a_2 + b_2}, \qquad \overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}.$$

[1] Часто вместо $\mathbb{Z}_m$ пишут $\mathbb{Z}/m\mathbb{Z}$.

Лемма 2.2. *Множество $\mathbb{Z}_m$ с операциями сложения и умножения (2.1) является коммутативным кольцом с единицей $\overline{1}$. Нулевым элементом является $\overline{0}$. Обратный по сложению элемент определяется формулой $-(\overline{a}) = \overline{(-a)}$.*

Доказательство. Достаточно воспользоваться тем, что множество $\mathbb{Z}$ есть коммутативное кольцо с единицей 1 и нулем 0. Например, коммутативность сложения проверяется так

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}.$$

Оставшиеся условия доказываются аналогичным образом. □

Замечание 2.1. Кольцо $\mathbb{Z}_m$ можно рассматривать как множество $\{0, 1, 2, \ldots, m-1\}$, в котором сумма и произведение определены, как остаток от деления «обычной» суммы и произведения на модуль m. Например, $2 \cdot 3 = 2$, $2 + 3 = 1$, $2 - 3 = 3$ в кольце $\mathbb{Z}_4$.

Определение. Пусть K — кольцо с единицей. Элемент $x^{-1} \in K$ называется *обратным к* x, если $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Определение. Элементы $x, y \in K$ называются *делителями нуля*, если $x, y \neq 0$ и $x \cdot y = 0$.

Примеры.

1. Любой ненулевой элемент кольца $\mathbb{Q}$ имеет обратный. Делителей нуля нет.
2. Элементы кольца $\mathbb{Z}$, кроме 1, не имеют обратных. Делителей нуля нет.
3. Любая невырожденная матрица из $\mathrm{M}_n(\mathbb{R})$ имеет обратную. Кольцо $\mathrm{M}_n(\mathbb{R})$ имеет делители нуля. Например,
$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = 0.$$

Делители нуля не могут быть обратимыми. Действительно, если $x \cdot y = 0$ и существует x^{-1}, то $y = x^{-1}xy = 0$.

Кольцо $\mathbb{Z}_m$ может иметь делители нуля. Например, $\overline{2} \cdot \overline{3} = \overline{0}$ в $\mathbb{Z}_6$. Поэтому не все элементы кольца $\mathbb{Z}_m$ обратимы. Выведем необходимое и достаточное условие обратимости.

Лемма 2.3. *Сравнение*

$$ax \equiv 1 \pmod{m} \tag{2.2}$$

имеет решение $x \in \mathbb{Z}$ тогда и только тогда, когда нод $(a, m) = 1$.

Доказательство. Целое x удовлетворяет (2.2), если и только если существует такой $y \in \mathbb{Z}$, что $ax + my = 1$. Полученное диофантовое уравнение исследовано в § II.3. По теореме II.3.1 уравнение разрешимо, если и только если нод $(a, m) \mid 1$, т.е нод $(a, m) = 1$. □

Определение. Коммутативное кольцо с единицей, у которого каждый ненулевой элемент обратим, называется *полем*.

В поле мы можем определить операцию деления на ненулевой элемент по формуле: $\frac{x}{y} = x \cdot y^{-1}$. Таким образом, элементы поля можно складывать, вычитать, умножать и делить на ненулевой элемент.

Пример. Кольца $\mathbb{Q}$, $\mathbb{R}$ являются полями. Кольца $\mathbb{Z}$, $\mathrm{M}(\mathbb{R})$ не являются полями.

Теорема 2.1. *Справедливы свойства*

а) элемент $\overline{a} \in \mathbb{Z}_m$ *является обратимым, если и только если* нод $(a, m) = 1$;

б) количество обратимых элементов кольца $\mathbb{Z}_m$ *равно* $\varphi(m)$;

в) кольцо $\mathbb{Z}_m$ *является полем тогда и только тогда, когда* m *есть простое число.*

Доказательство. Утверждение а) является эквивалентной формулировкой леммы 2.1. Утверждения б) следует из а) и определения функции Эйлера. Докажем в). Согласно а), кольцо $\mathbb{Z}_m$ является полем, если и только если нод $(a, m) = 1$ при всех $a \in \{1, \ldots, m-1\}$. Это эквивалентно тому, что m — простое. □

§ 3. Полная и приведенная системы вычетов

Определение. Выберем по одному элементу из каждого класса вычетов по модулю m. Полученное множество называется *полной системой вычетов* по модулю m.

Пример. Следующие множества образуют полные системы вычетов по модулю 5

$$\{0, 1, 2, 3, 4\}, \quad \{-2, -1, 0, 1, 2\}, \quad \{0, 2, 4, 8, 16\}.$$

Набор $\{0, 1, \ldots, m-1\}$, составленный из всех наименьших неотрицательных вычетов, образуют полную систему вычетов по модулю m. Еще одним очевидным примером полной системы вычетов по модулю m является множество

$$\{x \in \mathbb{Z} : -m/2 < x \leq m/2\}.$$

Оно состоит из так называемых *абсолютно наименьших вычетов.* Рассмотрим какие еще множества образуют полные системы вычетов.

Теорема 3.1. *Справедливы следующие свойства.*

а) Любой набор из m *попарно несравнимых по модулю* m *чисел образует полную систему вычетов по модулю* m.

б) Пусть $a, b \in \mathbb{Z}$, *причем* нод $(a, m) = 1$. *Если* $\{x_j\}_{j=1}^m$ *образуют полную систему вычетов по модулю* m, *то*

$$\{ax_j + b\}_{j=1}^m$$

также есть полная система вычетов по модулю m.

Доказательство. Докажем а). Пусть $x_1, \ldots, x_m \in \mathbb{Z}$, причем $x_i \not\equiv x_j \pmod m$ при $i \neq j$. Тогда x_i принадлежат разным классам вычетов. Так как количество x_i равно m, то они образуют полную систему вычетов.

Докажем б). Согласно а) достаточно доказать, что числа $(ax_i + b)$ попарно несравнимы по модулю m. Действительно, если

$$ax_i + b \equiv ax_j + b \pmod m,$$

то $ax_i \equiv ax_j \pmod m$, а т.к. нод $(a, m) = 1$, то по свойству 6 сравнений $x_i \equiv x_j \pmod m$. Следовательно, $i = j$. □

Согласно свойству 8) сравнений числа одного и того же класса вычетов по модулю m имеют с модулем один и тот же наибольший общий делитель. Особенно важны классы, для которых этот делитель равен 1, т.е. классы, состоящие из чисел взаимно простых с m.

Определение. Выберем по одному элементу из каждого класса вычетов по модулю m, состоящего из чисел взаимно простых с m. Полученное множество называется *приведенной системой вычетов* по модулю m.

Пример.

Модуль	6	5	10
Пример приведенной системы	$\overline{1}, \overline{5}$	$\overline{1}, \overline{2}, \overline{3}, \overline{4}$	$\overline{1}, \overline{2}, \overline{3}, \overline{7}, \overline{9}$

Для любого m числа из $1, 2, \ldots, m-1$, которые взаимны простые с m, образуют приведенную систему вычетов по модулю m. Любая приведенная система вычетов по модулю m состоит из $\varphi(m)$ элементов.

Теорема 3.2. *Справедливы следующие свойства.*

а) Любой набор из $\varphi(m)$ попарно несравнимых по модулю m чисел, которые взаимно простые с m, образует приведенную систему вычетов по модулю m.

б) Пусть $a \in \mathbb{Z}$, причем нод $(a, m) = 1$. *Если $\{x_j\}_{j=1}^{\varphi(m)}$ является приведенной системой вычетов по модулю m, то $\{ax_j\}_{j=1}^{\varphi(m)}$ также есть приведенная система вычетов.*

Доказательство. Свойство а) доказывается также, как и утверждение а) теоремы 3.1. Докажем б). Согласно теореме 3.1 б) числа ax_j попарно несравнимые по модулю m. Так как нод $(a, m) = 1$, нод $(x_j, m) = 1$, то нод $(ax_j, m) = 1$. Осталось воспользоваться а). □

§ 4. Теоремы Эйлера и Ферма

Теорема 4.1 (Эйлер). *Если $a \in \mathbb{Z}$, $m \in \mathbb{N}$, причем* нод $(a, m) = 1$, *то*

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

Доказательство. Пусть $\varphi = \varphi(m)$ и $\{x_i\}_{i=1}^{\varphi}$ — приведенная система вычетов по модулю m. Тогда $\{ax_i\}_{i=1}^{\varphi}$ также является приведенной системой вычетов по модулю m согласно теореме 3.2 б). Значит, каждое число первой системы сравнимо по модулю m с одним и только одним числом второй системы. Другими словами для любого номера $i \in \{1, \ldots, \varphi\}$ существует единственный номер $k_i \in \{1, \ldots, \varphi\}$ такой, что

$$x_i \equiv ax_{k_i} \pmod{m}.$$

Следовательно, $\prod\limits_{i=1}^{\varphi} x_i \equiv \prod\limits_{i=1}^{\varphi} (ax_{k_i}) \pmod{m}$. Так как $\prod\limits_{i=1}^{\varphi} (ax_{k_i}) = a^{\varphi} \prod\limits_{i=1}^{\varphi} x_i$, то

$$\prod_{i=1}^{\varphi} x_i \equiv a^{\varphi} \prod_{i=1}^{\varphi} x_i \pmod{m}.$$

Каждое из чисел x_i взаимно просто с модулем m. Значит, их произведение также взаимно просто с модулем. Поэтому мы можем сократить на $\prod_{i=1}^{\varphi} x_i$. В итоге, получаем

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

□

Пример. Пусть $m = 1000$. Тогда $m = 2^3 \cdot 5^3$, $\varphi(m) = \varphi(2^3)\varphi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$. Следовательно, если нод $(a, 1000) = 1$, то

$$a^{400} \equiv 1 \pmod{1000}.$$

Условие нод $(a, 1000) = 1$ означает, что последняя цифра в десятичной записи числа a не равна $0, 2, 5$. Например, $17888885671^{400} \equiv 1$, $3^{400} \equiv 1 \pmod{1000}$.

Теорема 4.2 (малая теорема Ферма)**.** *Если целое a не делится на простое p, то*

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

Доказательство. Так как a не делится на p, а p простое, то нод $(a, p) = 1$. Осталось применить теорему Эйлера в которой $m = p$ и учесть, что $\varphi(p) = p - 1$. □

Следствие 4.1. *Для любого целого a и простого p*

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

Доказательство. Если $p \mid a$, то утверждение следствия тривиально. Если $p \nmid a$, то мы можем применить малую теорему Ферма. Умножая сравнение $a^{p-1} \equiv 1 \pmod{p}$ на a, получаем требуемый результат. □

§ 5. Алгоритм быстрого возведения в степень

Одним из основных действий арифметики вычетов, возникающих, например, в криптографии, является вычисление $a^x \pmod{m}$, то есть нахождение такого y, что

$$y = a^x \pmod{m}, \tag{5.1}$$

где a, x, m — заданные натуральные. Далее считаем, что $a < m$. Запись $y = b \pmod{m}$ означает, что $y \equiv b \pmod{m}$ и $0 \leq y < m$, т.е. y — наименьший неотрицательный вычет по модулю m, лежащий в том классе, что и b.

Если вычислять «в лоб», т.е. последовательно находить

$$a^2 = a \cdot a \pmod{m}, \quad a^3 = a^2 \cdot a \pmod{m}, \ldots, a^x = a^{x-1} \cdot a \pmod{m},$$

то нужно выполнить $(x - 1)$ умножение в кольце $\mathbb{Z}_m$. Если n — количество разрядов в двоичной записи x, то число умножений не меньше, чем 2^{n-1}.

Лемма 5.1. *Пусть $x, m, a \in \mathbb{N}$. Пусть $x = (x_0 x_1 \ldots x_{n-1})_2$, т.е.*

$$x = x_0 + 2x_1 + 2^2 x_2 + \ldots + 2^{n-1} x_{n-1} \qquad (x_j \in \{0, 1\}).$$

Определим целые a_j по реккурентным формулам

$$a_0 = a; \qquad a_j = a_{j-1}^2 \pmod{m}, \quad j = \overline{1, n-1}. \tag{5.2}$$

Тогда $a^x \equiv a_0^{x_0} a_1^{x_1} \ldots a_{n-1}^{x_{n-1}} \pmod{m}$.

Доказательство. По определению чисел a_j

$$a_0 = a \pmod m, \quad a_1 = a^2 \pmod m, \quad a_2 = a^4 \pmod m, \quad a_3 = a^8 \pmod m, \dots$$

В общем случае $a_j = a^{2^j} \pmod m$, $\quad j = \overline{0, n-1}$. Следовательно,

$$a_0^{x_0} a_1^{x_1} \dots a_{n-1}^{x_{n-1}} \equiv a^{x_0} \left(a^2\right)^{x_1} \left(a^4\right)^{x_2} \dots \left(a^{2^{n-1}}\right)^{x_{n-1}} = a^{x_0 + 2x_1 + 2^2 x_2 + \dots + 2^{n-1} x_{n-1}} = a^x \pmod m.$$

□

Алгоритм (быстрого возведения в степень)**.** Даны натуральные a, m и $x = (x_{n-1} x_{n-2} \dots x_0)_2$. Нужно вычислить $y = a^x \pmod m$.

1. Вычисляем a_j $(0 \le j \le n-1)$ по формулам (5.2).
2. Вычисляем $y = a_0^{x_0} a_1^{x_1} \dots a_{n-1}^{x_{n-1}} \pmod m$.

Лемма 5.2. *Пусть n — число разрядов в двоичной записи x. Тогда приведенный выше алгоритм требует выполнения не более, чем $2(n-1)$ умножений в кольце $\mathbb{Z}^m$.*

Пример. Вычислим $2^{1000} \pmod{100}$. Имеем

$$a = 2, m = 100, x = 1000,$$
$$x = 1024 - 24 = 2^{10} - 2^4 - 2^3 = (10000000000)_2 - (11000)_2 = (10111101000)_2, \quad n = 10.$$

Вычислим a_j. Все действия выполняем по модулю 100 (запись $\pmod{100}$ опускаем).

$$\begin{aligned}
a_0 &= 2, \quad a_1 = 2^2 = 4, \quad a_2 = 4^2 = 16, \quad a_3 = 16^2 = (10+6)^2 = 2 \cdot 6 \cdot 10 + 6^2 = 56, \\
a_4 &= 56^2 = (50+6)^2 = 6^2 = 36, \quad a_5 = 36^2 = (50-14)^2 = 14^2 = (10+4)^2 = 80 + 16 = 96, \\
a_6 &= 96^2 = (100-4)^2 = 4^2 = 16, \quad a_7 = 16^2 = 56, \\
a_8 &= 56^2 = 36, \quad a_9 = 36^2 = 96, \quad a_{10} = 96^2 = 16.
\end{aligned}$$

Вычисления удобно записывать в таблицу

j	0	1	2	3	4	5	6	7	8	9	10
x_j	0	0	0	1	0	1	1	1	1	0	1
a_j	2	4	16	56	36	96	16	56	36	96	16

Следовательно,

$$\begin{aligned}
2^{1000} &= 16 \cdot 36 \cdot 56 \cdot 16 \cdot 96 \cdot 56 = 16^2 \cdot 56^2 \cdot 36 \cdot 96 = 56 \cdot 36 \cdot 36 \cdot 96 = 56 \cdot 96^2 = 56 \cdot 16 = \\
&= (50+6) \cdot 16 = 6 \cdot 16 = 96.
\end{aligned}$$

§ 6. Криптографические приложения (шифр RSA)

Описание RSA

Предположим, что два абонента хотят обмениваться информацией по общедоступному каналу связи (например, через интернет). Чтобы обеспечить конфеденциальность переписки

можно воспользоваться шифрованием сообщений. Одним из самых популярных алгоритмов шифрования является шифр RSA[2]. Он заключается в следующем.

Подготовка. Абонент A выбирает два простых числа p и q и вычисляет

$$m = pq, \quad \varphi = \varphi(m) = (p-1)(q-1).$$

Далее он выбирает натуральное d, удовлетворяющее условию

$$\text{нод } (d, \varphi) = 1.$$

После этого A находит $e \in [1, m]$ (обратный к d по модулю m), как решение сравнения

$$ed \equiv 1 \pmod{\varphi}. \tag{6.1}$$

Такое e существует, т.к. нод $(d, \varphi) = 1$. Для его вычисления можно использовать алгоритм непрерывных дробей. Подготовка закончена.

Число m называют *модулем*, а e — *экспонентой шифрования* (открытой экспонентой). Абонент A *публикует* (помещает в открытом доступе) пару (m, e).

Натуральное d называют *экспонентой расшифрования* (секретной экспонентой). Абонент A держит число d в строгой тайне.

Натуральные p, q, φ можно «забыть». Они были нужны только для вычисления d. Однако их значения не должны быть доступны никому, кроме A.

Алгоритм шифрования. Пусть абонент B хочет написать секретное сообщение для A. Он знает только m и e, которые находятся в открытом доступе (в справочнике, на web-странице абонента A и.т.д.). Сообщение разбивается на блоки, каждый из которых кодируется целым неотрицательным числом x так, чтобы $x < m$ (каждый блок представляется на компьютере в виде последовательности нулей и единиц, которую можно рассматривать как запись некоторого неотрицательного целого в двоичной системе исчисления).

Блок x шифруется следующим образом

$$y = x^e \pmod{m}. \tag{6.2}$$

Абонент B посылает y абоненту A по любому каналу связи.

Алгоритм дешифровки. Абонент A, зная секретное d, расшифровывает блок y:

$$x = y^d \pmod{m}.$$

Доказательство корректности процедуры расшифровки. Ограничимся случаем, когда нод $(x, m) = 1$. Используя условие $ed \equiv 1 \pmod{\varphi}$ и теорему Эйлера, получаем

$$ed = 1 + k\varphi \quad \Longrightarrow \quad y^d \equiv (x^e)^d = x^{ed} = x^{1+k\varphi} = x \cdot (x^\varphi)^k \equiv x \cdot 1^k = x \pmod{m}.$$

□

О стойкости алгоритма RSA

Предположим, что злоумышленник может перехватывать шифрованные сообщения (т.е. y). Он знает e и m. Параметры d, p, q, φ ему неизвестны. Расшифровка блока y сводится к нахождению решения x сравнения

$$x^e \equiv y \pmod{m}, \tag{6.3}$$

где y — заданное число. Рассмотрим проблемы, возникающие у злоумышленника.

[2] его создателями являются Rivest R., Shamir A., Adleman L.

1. Все существующие нетривиальные методы решения (6.3) требуют знания разложения модуля m на простые сомножители:

$$m = pq. \tag{6.4}$$

2. Сравнение (6.3) легко решается, если известен секретный ключ d. Для его нахождения из (6.1) нужно знать φ. Задача нахождения значения функции Эйлера $\varphi(m)$ эквивалентна решению задачи факторизации (6.4).

3. Можно попытаться найти секрет d следующим образом. Возьмем любое a и вычислим $b = a^e \pmod m$. Тогда согласно корректности алгоритма расшифровки

$$a = b^d \pmod m, \tag{6.5}$$

т.е. d есть решение задачи (6.5). Все существующие нетривиальные методы решения (6.5) требуют знания разложения (6.4). Отметим, что даже в случае простого модуля m не существует эффективных алгоритмов решения (6.5), а сложность существующих алгоритмов примерно соответствует сложности решения задачи факторизации.

Возможно существуют методы решения сравнения (6.3), не использующие решение задачи факторизации. Однако они неизвестны. Поэтому на сегодняшний день *криптостойкость алгоритма RSA определяется сложностью решения задачи факторизации (6.4).*

Самые эффективные из известных методы решения задачи факторизации (6.4) требуют выполнения порядка

$$c \cdot \exp(2n^{1/3} \ln^{2/3} n)$$

элементарных операций (сложение, вычитание, умножение, деление) в кольце $\mathbb{Z}_m$. Здесь n — количество разрядов в двоичной записи модуля m, а c — некоторая положительная абсолютная постоянная. Вспоминая результаты предыдущего параграфа заключаем: количество действий в $\mathbb{Z}_m$, необходимых для шифрования (6.2) блока x не больше, чем $2n$, а количество операций, необходимых для взлома шифра (т.е. решения задачи факторизации (6.4)) пропорционально $\exp(2n^{1/3} \ln^{2/3} n)$. Функция $\exp(2n^{1/3} \ln^{2/3} n)$ растет гораздо быстрее, чем n. Поэтому, независимо от возможностей ЭВМ, мы можем выбрать такое (большое) n, чтобы шифрование занимало, грубо говоря, секунды, а взлом шифра — тысячелетия. В настоящий момент, выбирают n в пределах примерно от 1024 до 2048, то есть

$$2^{1024} \ll m \ll 2^{2048}.$$

Если $n = 1024$, то $\exp(2n^{1/3} \ln^{2/3} n) > 10^{168}$.

Ситуация может измениться, если появятся принципиально новые методы решения задач (6.4) или (6.3). В частности, изобретение эффективного алгоритма факторизации целых чисел приведет к краху шифра RSA, который используется повсеместно.

RSA и простые числа

Реализация шифра RSA в сетях с многими абонентами (например, банк и его клиенты) приводит к следующей проблеме. Каждый абонент должен иметь свой уникальный модуль $m = pq$. В настоящий момент, безопасным считается использование модулей, не меньших, чем 2^{1024} или даже $2^{2048} \approx 3 \cdot 10^{616}$. Шифры, использующие модули меньшей длины, могут быть взломаны (небольшое число можно разложить на множители простым перебором

возможных делителей). В целях безопасности, параметры абонентов должны регулярно меняться. Вопрос: каким образом мы можем генерировать большие простые числа? Единственный (пока) ответ заключается в следующем: выбирается некоторое большое случайное число и проверяется является оно простым или нет. Если нет, то выбираем другое случайное число и т. д. Это приводит к следующей задаче: каким образом проверить заданное n на простоту? Можно конечно проверить делимость n на все натуральные, не превосходящие $\sqrt{n}$. Однако такой алгоритм является неэффективным для больших n. Например, при $n \approx 2^{1024}$ количество пробных делений будет порядка $2^{512} \approx 1,3 \cdot 10^{154}$.

Тесты на простоту делят на *детерминированные* и *вероятностные*. Первые дают однозначный ответ на вопрос о простоте тестируемого числа. Вероятностные тесты заключаются в многократной проверке некоторых условий. Чем больше проверок выдержало число, тем выше вероятность того, что оно является простым. В приложениях, как правило, используются вероятностные тесты, которые являются более быстрыми, чем детерминированные.

Тест простоты Ферма. Дано $n \in \mathbb{N}$. Нужно проверить является n простым или нет.

1. Случайным образом выбираем натуральное a.
2. Если нод $(n, a) > 1$, то n — составное.
3. Если $a^{n-1} \not\equiv 1 \pmod{n}$, то n — составное.
4. Возвращаемся к шагу 1.

Чем больше проверок выдержало n, тем выше вероятность того, что n — простое.

Существуют «быстрые» алгоритмы вычисления нод (a, n) (алгоритм Евклида) и $a^{n-1} \pmod{m}$. Тем не менее тест Ферма имеет ряд недостатков[3] и на практике не используется. Он является основой для ряда эффективных тестов. Описания реально используемых тестов на простоту выходит за рамки настоящего курса. Их можно найти в [?].

Численные упражнения к главе IV

1. Используя свойства сравнений, выведите критерии делимости натурального числа, записанного в 10-ичной системе исчисления, на 3, 7, 9, 11.
2. Исследовать вопрос о разрешимости диофантовых уравнений
$$y^2 = 5 + 9x, \quad y^3 = 1 + 7x, \quad 3x^9 - 2y^2 = 1.$$
3. Вычислить $7 \cdot 8^{-1} - 10$ в $\mathbb{Z}_{11}$; $\dfrac{11+7}{6}$ в $\mathbb{Z}_{13}$.
4. Используя свойства сравнений, а также теоремы Эйлера и Ферма, вычислить
$$1000000^{18} \pmod{19}, \quad 71701^{19} \pmod{19}, \quad 1111^{172} \pmod{17}, \quad 300^{100} \pmod{11},$$
$$333^{1003} \pmod{10}, \quad 2^{500} \pmod{7}, \quad 3^{1151} \pmod{100}.$$
5. Вычислить $52^{100} \pmod{50}$, $5^{1151} \pmod{100}$.

[3] Например, существует бесконечно много составных чисел n (числа Кармайкла) таких, что для любого a, которое взаимно просто с n, $a^n \equiv 1 \pmod{n}$.

Глава V
Полиномиальные сравнения

§ 1. Основные определения

Мы будем изучать сравнения следующего вида

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}. \tag{1.1}$$

Если a_n не делится на m, то n называется *степенью* сравнения.

Решить сравнение — значит найти все целые значения x, ему удовлетворяющие. Если x удовлетворяет (1.1), то согласно свойству 5 сравнений (см. § IV.1) этому же сравнению удовлетворяют все целые, сравнимые с x по модулю m, т.е. все числа класса вычетов $\overline{x}$.

Определение. *Решением сравнения* (1.1) называется класс вычетов по модулю m, состоящий из целых, удовлетворяющих (1.1). *Количество решений сравнения* (1.1) — это количество классов вычетов, удовлетворяющих (1.1).

Из определений вытекают следующие очевидные свойства.

1. *Количество решений сравнения* (1.1) равно количеству чисел 0 до $m-1$, удовлетворяющих (1.1).

2. *Количество решений сравнения* (1.1) равно количеству чисел $x_1, \ldots, x_k$ таких, что

   1) $x_1, \ldots, x_k$ удовлетворяют (1.1),

   2) $x_1, \ldots, x_k$ попарно несравнимы по модулю m,

   3) любое целое, удовлетворяющее (1.1), сравнимо с одним из x_i по модулю m.

Пример. Решим сравнение

$$x^5 + x + 1 \equiv 0 \pmod{7}. \tag{1.2}$$

Достаточно найти числа из $0, 1, 2, \ldots, 6$, которые удовлетворяют (1.2). Таких чисел только два $x = 2$ и $x = 4$. Значит, сравнение имеет два решения: $x \equiv 2$ и $x \equiv 4 \pmod{7}$. Это означает, что x удовлетворяет (1.2), если и только если $x \equiv 2$ либо $x \equiv 4 \pmod{7}$.

§ 2. Сравнения первой степени

Любое сравнение первой степени можно записать в следующем виде

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

Теорема 2.1. *Пусть* $d = \text{нод}\,(a, m)$. *Тогда*

а) сравнение (2.1) разрешимо, если и только если $d \mid b$;

б) если $d \mid b$, *то сравнение (2.1) имеет равно* d *решений:*

$$x \equiv u + \frac{m}{d}k, \quad k = 0, 1, \ldots, d-1, \tag{2.2}$$

где u *— любое такое целое, что* $au \equiv b \pmod m$.

Доказательство. Целое x удовлетворяет сравнению (2.1) в том и только том случае, когда существует такое целое y, что

$$ax + my = b. \tag{2.3}$$

Согласно теореме II.3.1, уравнение (2.3) имеет решение, если и только если $d \mid m$. Утверждение а) доказано. Согласно этой же теореме все решения (2.3) определяются формулой

$$x = u + \frac{m}{d} \cdot t, \quad y = v - \frac{a}{d} \cdot t, \quad t \in \mathbb{N},$$

где u, v такие целые, что $au + mv = b$. Тогда $au \equiv b \pmod m$ и множество x, удовлетворяющих (2.1), имеет вид

$$x = u + \frac{m}{d}t, \qquad t \in \mathbb{Z}. \tag{2.4}$$

Рассмотрим следующие числа

$$x_k = u + \frac{m}{d}k, \quad k = 0, 1, \ldots, d-1.$$

Докажем, что любое x, удовлетворяющее (2.1), сравнимо с одним из чисел x_k по модулю m. Действительно, x имеет вид (2.4). Пусть k — наименьшее неотрицательное, сравнимое с t по модулю d. Тогда $k \in \{0, 1, \ldots, d-1\}$ и

$$x - x_k = \frac{m}{d}(t-k) = \frac{t-k}{d}m \equiv 0 \pmod m.$$

Докажем, что числа x_k попарно несравнимы по модулю m. Действительно, если $x_k \equiv x_j \pmod m$, то $\frac{m}{d}k \equiv \frac{m}{d}j \pmod m$. Сокращая на m/d, имеем $k \equiv j \pmod d$, т.е. $k = j$.

Таким образом, числа $x_0, \ldots, x_{d-1}$ удовлетворяют (2.1), попарно несравнимы по модулю m и любое другое целое, удовлетворяющее (2.1), сравнимо с одним из $x_0, \ldots, x_{d-1}$. Значит, количество решений (2.1) равно d и все решения имеют вид (2.2). □

Пусть $d \mid b$. Согласно теории непрерывных дробей (см. § II.3), если Q_{n-1} — предпоследний подходящий знаменатель для a/m, то целое

$$u = \frac{b}{d} \cdot Q_{n-1}(-1)^{n-1},$$

удовлетворяет сравнению $au \equiv b \pmod m$.

Пример. Решим сравнение

$$111x \equiv 75 \pmod{321}. \tag{2.5}$$

Решение. Найдем $d = (111, 321)$, разложим $111/321$ в непрерывную дробь и вычислим подходящие знаменатели. Получаем

$$d = (111, 321) = (111, 99) = (12, 99) = (12, 3) = 3,$$
$$\frac{111}{321} = [0; 321/111] = [0; 2, 111/99] = [0; 2, 1, 99/12] = [0; 2, 1, 8, 12/3] = [0; 2, 1, 8, 4].$$

q_k		0	2	1	8	4
Q_k	0	1	2	3	26	107

, $\qquad n = 4, \qquad Q_{n-1} = 26.$

Значит,

$$u = \frac{75}{3} \cdot 26 \cdot (-1)^3 = -25 \cdot 26 \equiv 99 \pmod{107}, \qquad \frac{m}{d} = \frac{321}{3} = 107.$$

Ответ: сравнение (2.5) имеет три решения

$$x \equiv 99 \pmod{321},$$
$$x \equiv 99 + 107 \equiv 206 \pmod{321},$$
$$x \equiv 99 + 107 \cdot 2 \equiv 313 \pmod{321},$$

Если нод $(a, m) = 1$, то существует целое a^{-1} такое, что $a^{-1}a \equiv 1 \pmod{m}$ и решение сравнения (2.1) имеет следующий вид

$$x \equiv a^{-1}b \pmod{m}.$$

Эта формула удобна для решения несколько сравнений с одинаковыми a и m.

Пример. Выпишем формулу для решения сравнения

$$7x \equiv b \pmod{57}.$$

Так как $(7, 57) = 1$, то существует целое $y = 7^{-1}$, удовлетворяющее сравнению

$$7 \cdot 7^{-1} \equiv 1 \pmod{57}.$$

Найдем его с помощью алгоритма непрерывных дробей. Имеем

$$\frac{7}{57} = [0; 8, 7]; \qquad \begin{array}{|c|c|c|c|c|}\hline q_k & & 0 & 8 & 7 \\ \hline Q_k & 0 & 1 & 8 & 57 \\ \hline \end{array}; \quad n = 2, \quad Q_1 = 8, \quad 7^{-1} = 8 \cdot (-1)^1 = -8.$$

Ответ: $x \equiv -8b \pmod{57}$.

§ 3. Алгоритм Евклида решения линейного сравнения

Пронумерованные шаги алгоритма Евклида вычисления нод (a, m) имеют вид

$$\begin{aligned} m &= aq_1 + r_2 && (0 < r_2 < a),\\ a &= r_2q_2 + r_3 && (0 < r_3 < r_2),\\ r_2 &= r_3q_3 + r_4 && (0 < r_4 < r_3),\\ &\dots && \dots\\ r_{n-2} &= r_{n-1}q_{n-1} + r_n && (0 < r_n < r_3),\\ r_{n-1} &= r_nq_n. \end{aligned}$$

В этом случае нод $(a,m) = (a,r_2) = (r_2,r_3) = (r_3,r_4) = \ldots = (r_{n-1},r_n) = r_n$. Для нахождения решения u сравнения $au \equiv b \pmod m$ нужно дополнительно вычислять значения некоторой вспомогательной переменной S_i:

$$S_{-1} = 0, \quad S_0 = 1; \quad S_i = -q_i S_{i-1} + S_{i-2} \pmod m, \quad i = \overline{1, n-1}.$$

Лемма 3.1. *Справедлива формула*

$$aS_{n-1} \equiv \text{нод}\,(a,m) \pmod m.$$

Доказательство. Используя определение S_i и формулы алгоритма Евклида, получаем

$$\begin{aligned}
&S_1 = -q_1, \quad S_2 = -S_1 q_2 + 1, \quad S_3 = -S_2 q_3 + 2,\\
&r_2 \equiv -aq_1 = aS_1 \pmod m,\\
&r_3 = a - r_2 q_2 \equiv a - aS_1 q_2 = a(-S_1 q_2 + 1) = aS_2 \pmod m,\\
&r_4 = r_2 - r_3 q_3 \equiv aS_1 - aS_2 q_3 = a(-S_2 q_3 + S_1) = aS_3 \pmod m.
\end{aligned}$$

Поэтому (строгое обоснование проводится с помощью метода математической индукции)

$$r_i \equiv aS_{i-1} \pmod m, \quad i = \overline{2, n}.$$

Следовательно, $aS_{n-1} \equiv r_n = \text{нод}\,(a,m) \pmod m$. □

Алгоритм. (Расширенный алгоритм Евклида) Дано: $a, m \in \mathbb{N}$. Найти $d = \text{нод}\,(a,m)$ и целое u_0 такое, что

$$au_0 \equiv d \pmod m. \tag{3.1}$$

1. Полагаем $S_0 = 0$, $S_1 = 1$.
2. Делим m на a с остатком: $m = aq + r, \quad 0 \le r < a$.
3. Если $r = 0$, то $d = a$, $u_0 = S_1$. Конец.
4. Заменяем пару (S_0, S_1) на $(S_1, \ -qS_1 + S_0)$, а пару (m,a) на (a,r) и переходим к шагу 2.

Пусть $d \mid b$, а u_0 удовлетворяет (3.1). Положим

$$u \equiv \frac{b}{d} u_0 \pmod m.$$

Тогда

$$au \equiv b \pmod m.$$

Пример. Найти хотя бы одно целое, удовлетворяющее сравнению $111x \equiv 75 \pmod{321}$. Используя алгоритм Евклида, получаем

			$S_0 = 0,$	$S_1 = 1,$
$(m,a) = (321,111),$	$321 = 111 \cdot 2 + 99,$	$q = 2,\ r = 99,$	$S_0 = 1,$	$S_1 = -q = -2;$
$(m,a) = (111,99),$	$111 = 99 \cdot 1 + 12,$	$q = 1,\ r = 12,$	$S_0 = -2,$	$S_1 = -q \cdot (-2) + 1 = 3;$
$(m,a) = (99,12),$	$99 = 12 \cdot 8 + 3,$	$q = 8,\ r = 3,$	$S_0 = 3,$	$S_1 = -q \cdot 3 - 2 = -26;$
$(m,a) = (12,3),$	$12 = 3 \cdot 4,$	$q = 4,\ r = 0.$		

Значит,

$$\text{нод}\,(321,111) = 3; \quad 111 \cdot (-26) \equiv 3 \pmod{321}; \quad x \equiv \frac{75}{3} \cdot (-26) = -650 \equiv -8 \pmod{321}.$$

Ответ: $x = -8$.

§ 4. Система сравнений первой степени. Китайская теорема об остатках

Рассмотрим следующую систему сравнений первой степени относительного неизвестного x

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, n. \tag{4.1}$$

При $n = 2$ ее решение не представляет труда. Действительно по определению

$$x = a_1 + k_1 m_1, \quad x = a_2 + k_2 m_2,$$

где k_1, k_2 — некоторые целые. Они должны удовлетворять диофантовому уравнению

$$k_1 m_1 - k_2 m_2 = a_2 - a_1,$$

которое исследовано в § II.3. Необходимое и достаточно условие разрешимости имеет вид: нод $(m_1, m_2) \mid (a_2 - a_1)$. Рассмотрим теперь общий случай.

Лемма 4.1. *Предположим, что существует решение $x_0 \in \mathbb{Z}$ системы (4.1). Тогда множество целых чисел, удовлетворяющих (4.1), совпадает с классом вычетов*

$$x \equiv x_0 \pmod{M},$$

где $M =$ нок $[m_1, \ldots, m_n]$

Доказательство. Докажем, что если $x \equiv x_0 \pmod{M}$, то x удовлетворяет (4.1). Действительно, т.к. $x = x_0 + kM$, а M кратно любому m_i, то

$$x \equiv x_0 \equiv a_i \pmod{m_i}.$$

Пусть теперь x удовлетворяет (4.1). Осталось доказать, что $x \equiv x_0 \pmod{M}$. Так как

$$x \equiv a_i \equiv x_0 \pmod{m_i}, \quad i = \overline{1, n},$$

то $(x - x_0)$ кратно любому m_i, т.е. $(x - x_0)$ есть общее кратное $m_1, \ldots, m_n$. Согласно теореме I.1.2 $(x - x_0)$ делится на M, т.е. $x \equiv x_0 \pmod{M}$. □

Таким образом, достаточно найти хотя бы одно частное решение системы (4.1). Эта задача легко решается в случае, когда модули m_i попарно взаимно простые.

Теорема 4.1 (китайская теорема об остатках)**.** *Пусть m_i попарно взаимно простые. Тогда система (4.1) имеет решение и оно определяется следующим образом. Положим*

$$M = m_1 \cdot \ldots \cdot m_n, \quad M_i = \frac{M}{m_i}, \quad i = \overline{1, n}.$$

Найдем целые b_i, удовлетворяющие сравнениям

$$M_i b_i \equiv a_i \pmod{m_i}, \quad i = \overline{1, n} \tag{4.2}$$

Тогда множество целых чисел, удовлетворяющих (4.1), совпадает с классом вычетов

$$x \equiv (M_1 b_1 + \ldots + M_n b_n) \pmod{M}.$$

Доказательство. Так как модули m_i попарно взаимно простые, то $M = \text{нок}\,[m_1, \ldots, m_n]$. Поэтому достаточно доказать, что $x_0 = M_1 b_1 + \ldots + M_n b_n$ удовлетворяет (4.1).

Так как модули m_i попарно взаимно простые, то $\text{нод}\,(M_i, m_i) = 1$. Значит, существуют b_i, удовлетворяющие (4.2). Возьмем любое $i \in \{1, \ldots, n\}$. Так как $m_i \mid M_j$ при $j \neq i$, то

$$x_0 \equiv M_i b_i \equiv a_i \pmod{m_i},$$

т.е. $x = x_0$ есть решение (4.1). □

Пример. Решим следующую систему

$$x \equiv 4 \pmod 3, \quad x \equiv 5 \pmod{11}, \quad x \equiv 2 \pmod{13}.$$

Так как модули взаимно простые, то можно применить китайскую теорему об остатках:

$$M = 2 \cdot 11 \cdot 13 = 429, \quad M_1 = 11 \cdot 13 = 143, \quad M_2 = 2 \cdot 13 = 39, \quad M_3 = 3 \cdot 11 = 33.$$
$$143 b_1 \equiv 4 \pmod 3 \quad \Leftrightarrow \quad 2 b_1 \equiv 1 \pmod 3 \quad \Leftrightarrow \quad b_1 \equiv 2 \pmod 3;$$
$$39 b_2 \equiv 5 \pmod{11} \quad \Leftrightarrow \quad 6 b_2 \equiv 5 \pmod{11} \quad \Leftrightarrow \quad b_2 \equiv -1 \pmod{11};$$
$$33 b_3 \equiv 2 \pmod{13} \quad \Leftrightarrow \quad 7 b_3 \equiv 2 \pmod{13} \quad \Leftrightarrow \quad b_3 \equiv 4 \pmod{13}.$$
$$x_0 = M_1 b_1 + M_2 b_2 + M_3 b_3 = 143 \cdot 2 + 39 \cdot (-1) + 33 \cdot 4 = 379.$$

Ответ: $x \equiv 379 \pmod{429}$.

Если нужно решить несколько систем с одинаковыми наборами модулей вычисления лучше проводить следующим образом.

Следствие 4.1. *Пусть модули m_i попарно взаимно простые. Вычислим*

$$M = m_1 \cdot \ldots \cdot m_n, \quad M_i = \frac{M}{m_i}, \quad i = \overline{1, n}$$

и найдем целые b'_i, удовлетворяющие сравнениям

$$M_i b'_i \equiv 1 \pmod{m_i}, \quad i = \overline{1, n}.$$

Тогда множество целых чисел, удовлетворяющих (4.1), совпадает с классом вычетов

$$x \equiv (M_1 b'_1 a_1 + \ldots + M_n b'_n a_n) \pmod M.$$

Доказательство следствия тривиально и оставляется читателю.

Пример. Решить систему

$$x \equiv a_1 \pmod 7, \quad x \equiv a_2 \pmod{11}, \quad x \equiv a_3 \pmod{13}.$$

Решение. Модули попарно взаимно простые, поэтому применяем следствие 4.1:

$$M_1 = 11 \cdot 13 = 143, \quad M_2 = 7 \cdot 13 = 91, \quad M_3 = 7 \cdot 11 = 77, \quad M = 1001.$$
$$143 b'_1 \equiv 1 \pmod 7, \quad 3 b'_1 \equiv 1 \pmod 7, \quad b'_1 \equiv -2 \pmod 7;$$
$$91 b'_2 \equiv 1 \pmod{11}, \quad 3 b'_2 \equiv 1 \pmod{11}, \quad b'_2 \equiv 4 \pmod{11};$$
$$77 b'_3 \equiv 1 \pmod{13}, \quad -b'_3 \equiv 1 \pmod{13}, \quad b'_3 \equiv -1 \pmod{13}.$$

Ответ: $x \equiv (-2 \cdot 143 a_1 + 4 \cdot 91 a_2 - 77 a_3) = (-286 a_1 + 364 a_2 - 77 a_3) \pmod{1001}$.

§ 5. Сравнения любой степени по простому модулю

Рассмотрим следующее сравнение

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}, \tag{5.1}$$

где p — простое, причем $a_n \not\equiv 0 \pmod{p}$.

Теорема 5.1. *Сравнение (5.1) имеет не более, чем n решений.*

Доказательство. Прежде всего отметим, что для любых x, x_0

$$x^k - x_0^k = (x - x_0) \cdot \left(x^{k-1} + x^{k-2}x_0 + x^{k-3}x_0^2 + \ldots + x x_0^{k-2} + x_0^{k-1}\right),$$

$$f(x) - f(x_0) = \sum_{k=1}^{n} a_k (x^k - x_0^k) = (x - x_0) \cdot g(x), \tag{5.2}$$

где $g(x)$ — многочлен с целыми коэффициентами (зависящими от a_i и x_0) степени $(n-1)$ со старшим коэффициентом равным a_n.

Докажем теорему, используя математическую индукцию по $n = 1, 2, \ldots$.

База индукции. При $n = 1$ требуемое утверждение следует из теоремы 2.1.

Индукционный переход от $(n-1)$ к n. Пусть утверждение теоремы справедливо для всех сравнений степени не выше, чем $(n-1)$. Возьмем любое решение $\overline{x_0}$ сравнения (5.1). Нужно доказать, что количество оставшихся решений не более, чем $(n-1)$. Пусть $\overline{x_1}$ – еще одно решение. Используя (5.2), получаем

$$f(x_1) - f(x_0) = (x_1 - x_0) g(x_1),$$

где g — многочлен степени $(n-1)$. Поэтому

$$f(x_1) \equiv (x_1 - x_0) \cdot g_0(x_1) \equiv 0 \pmod{p}.$$

Так как $(x_1 - x_0)$ не кратно p, то число $(x_1 - x_0)$ взаимно простое с модулем p. Значит,

$$g(x_1) \equiv 0 \pmod{p}.$$

Так как g — многочлен степени $(n-1)$ и его старший коэффициент не кратен p, то согласно предположению индукции число решений сравнения

$$g(x) \equiv 0 \pmod{p}$$

не превышает $(n-1)$. Поэтому (5.1) имеет не более $(n-1)$ решений, кроме $\overline{x_0}$. □

Замечание 5.1. В случае составного модуля p утверждение теоремы может не выполняться даже при $n = 1$ (см. теорему 2.1).

Следствие 5.1. *Пусть количество решений сравнения (5.1) больше, чем n. Тогда все коэффициенты a_i многочлена f делятся на p.*

Доказательство. Предположим противное. Тогда существует коэффициент a_i, который не кратен p, причем все коэффициенты с номерами большими i делятся на p. Тогда сравнение (5.1) эквивалентно следующему

$$a_i x^i + \ldots + a_1 x + a_0 \equiv 0 \pmod{p},$$

которое согласно теореме 5.1 имеет не более, чем i решений. □

Теорема 5.2 (теорема Вильсона). *Пусть $p > 1$. Тогда p простое, если и только если*

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{5.3}$$

Доказательство. Докажем необходимость. Пусть p — простое. Рассмотрим многочлен

$$f(x) = (x-1)(x-2)\cdot\ldots\cdot(x-(p-1)) - (x^{p-1}-1).$$

Его степень равна $p-2$. Рассмотрим сравнение

$$f(x) \equiv 0 \pmod{p}.$$

Его решениями являются $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. Действительно, согласно малой теореме Ферма

$$\forall a \in \{1, 2, \ldots, p-1\} \qquad f(a) = -(a^{p-1}-1) \equiv 0 \pmod{p}.$$

Таким образом, число решений больше степени многочлена. Значит, все коэффициенты многочлена кратны p. Так как свободный член равен $(1-(p-1)!)$, то выполняется (5.3).

Докажем достаточность. Пусть выполняется (5.3). Если p составное, то существует простой делитель q числа p. Так как $1 < q \leq p-1$, то q делит $(p-1)!$. Поэтому $(p-1)!+1$ не делится на q. Но тогда $(p-1)! + 1 \not\equiv 0 \pmod{p}$ (т.к. p кратно q). □

Согласно следующей лемме сравнение (5.1) можно свести к сравнению степени меньшей p.

Лемма 5.1. *Пусть $f(x) = (x^p - x)g(x) + r(x)$, где g и r — многочлены с целыми коэффициентами. Тогда (5.1) эквивалентно сравнению $r(x) \equiv 0 \pmod{p}$.*

Доказательство. По малой теореме Ферма $x^p \equiv x \pmod{p}$. Поэтому $f(x) \equiv r(x) \pmod{p}$. □

Пример. Решим сравнение $x^{18} - 2x + 1 \equiv 0 \pmod{7}$. Так как

$$x^{18} - 2x + 1 = (x^7 - x)(x^{11} + x^5) + x^6 - 2x + 1,$$

то оно эквивалентно $x^6 - 2x + 1 \equiv 0 \pmod{7}$. Перебирая целые $0, 1, \ldots, 6$, получаем единственное решение $x \equiv 1 \pmod{7}$.

§ 6. Сравнения любой степени по модулю p^α

Пусть f — многочлен степени n с целыми коэффициентами. Рассмотрим сравнение

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{6.1}$$

где p — простое, а α — натуральное. Если x удовлетворяет (6.1), то

$$f(x) \equiv 0 \pmod{p^k}, \quad k \in \{1, 2, \ldots, \alpha\}. \tag{6.2}$$

Поэтому целые, удовлетворяющие (6.1), нужно искать среди решений сравнения

$$f(x) \equiv 0 \pmod{p}. \tag{6.3}$$

Лемма 6.1. *Для любых* $x, m, t \in \mathbb{Z}$

$$f(x + tm) \equiv f(x) + f'(x)tm \pmod{m^2}. \tag{6.4}$$

Доказательство. Возьмем любое $k \in \mathbb{N}$ и положим $g(x) = x^k$. Тогда

$$g(x + tm) = (x + tm)^k \equiv x^k + kx^{k-1}tm = g(x) + g'(x)tm \pmod{m^2}.$$

Из полученной формулы вытекает (6.4). □

Теорема 6.1. *Пусть* $x_1 \in \mathbb{Z}$, *причем*

$$f(x_1) \equiv 0 \pmod{p}. \tag{6.5}$$
$$f'(x_1) \not\equiv 0 \pmod{p}. \tag{6.6}$$

Тогда существует единственное решение сравнения (6.1), удовлетворяющее условию

$$x \equiv x_1 \pmod{p}. \tag{6.7}$$

Доказательство. Согласно (6.7) неизвестное x нужно искать в виде:

$$x = x_1 + t_1 p, \quad t_1 \in \mathbb{Z}.$$

Нужно подобрать параметр t_1 так, чтобы выполнялось (6.1). Последнее эквивалентно (6.2).

Так как $x \equiv x_1 \pmod{m}$, $f(x_1) \equiv 0 \pmod{m}$, то $f(x) \equiv 0 \pmod{p}$ при любом t_1.

Подберем t_1 так, чтобы $f(x) \equiv 0 \pmod{p^2}$. Согласно (6.4)

$$f(x_1 + t_1 p) \equiv f(x_1) + t_1 p f'(x_1) \pmod{p^2}.$$

Поэтому

$$f(x) \equiv 0 \pmod{p^2} \iff f(x_1) + t_1 p f'(x_1) \equiv 0 \pmod{p^2}.$$

Так как $f(x_1)$ делится на p, то последнее эквивалентно

$$\frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0 \pmod{p} \iff t_1 f'(x_1) = -\frac{f(x_1)}{p} \pmod{p}.$$

Так как p простое, то ввиду (6.6), нод $(f'(x_1), p) = 1$. Поэтому последнее сравнение имеет ровно одно решение $t_1 \equiv t_1' \pmod{p}$. Значит, $t_1 = t_1' + t_2 p$. Таким образом,

$$x = x_1 + t_1 p = x_1 + (t_1' + t_2 p)p = x_1 + t_1' p + t_2 p^2 = x_2 + t_2 p^2,$$

где $x_2 = x_1 + t_1' p$, а $t_2 \in \mathbb{Z}$. Отметим, что при любом выборе t_2

$$f(x_2) \equiv 0 \pmod{p^2}.$$

Подберем t_2 так, чтобы $f(x) \equiv 0 \pmod{p^3}$. Подставляя $x = x_2 + t_2 p^2$ в сравнение

$$f(x) \equiv 0 \pmod{p^3}$$

и используя (6.4), получаем следующее сравнение для t_2:

$$f(x_2) + t_2 p^2 f'(x_2) \equiv 0 \pmod{p^3} \iff t_2 f'(x_2) = -\frac{f(x_2)}{p^2} \pmod{p}. \tag{6.8}$$

Так как $x_1 \equiv x_2 \pmod{p}$, $f'(x_1) \not\equiv 0 \pmod{p}$, то $f'(x_2) \not\equiv 0 \pmod{p}$. Поэтому $f'(x_2)$ не делится на p. Значит, нод $(p, f'(x_2)) = 1$, следовательно, сравнения (6.8) имеют единственное решение $t_2 \equiv t_2' \pmod{p}$. Поэтому t_2 можно единственным образом представить в виде:

$$t_2 = t_2' + t_3 p,$$

Таким образом,

$$x = x_2 + t_2 p^2 = x_2 + t_2' p^2 + t_3 p^3 = x_3 + t_3 p^3,$$

где $x_3 = x_2 + t_2' p^2$, а $t_3 \in \mathbb{Z}$. Отметим, что при любом выборе t_3

$$f(x_3) \equiv 0 \pmod{p^3}.$$

Подставляя $x = x_3 + t_3 p^3$ в $f(x) \equiv 0 \pmod{p^4}$, приходим к $t_3 = t_3' + t_4 p$. И так далее. В итоге, получаем, что

$$x = x_1 + t_1' p + t_2' p^2 + \ldots + t_{\alpha-1}' p^{\alpha-1} + t_\alpha p^\alpha,$$

где коэффициенты $t_1', \ldots, t_{\alpha-1}' \in [0, p-1)$ определяются единственным образом. Значит,

$$x \equiv x_1 + t_1' p + t_2' p^2 + \ldots + t_{\alpha-1}' p^{\alpha-1} \pmod{p^\alpha}$$

является единственным решением сравнения (6.1), удовлетворяющим (6.7). □

Напомним, что для любого целого x, удовлетворяющего (6.1), выполняется и сравнение (6.3). Поэтому для любого такого x существует решение x_1 сравнения (6.3) такое, что $x \equiv x_1 \pmod{p}$

Пример. Решить сравнение

$$x^3 - 3x^2 - 1 \equiv 0 \pmod{125}. \tag{6.9}$$

Решение. По условию $f(x) = x^3 - 3x^2 - 1$, $f'(x) = 3x^2 - 6x$, $125 = 5^3$, $p = 5$.

Сначала находим решения сравнения по простому модулю: $x^3 - 3x^2 - 1 \equiv 0 \pmod{5}$. Их ровно два: $x \equiv 2 \pmod{5}$ и $x \equiv -1 \pmod{5}$.

1. Ищем решение исходного сравнение, удовлетворяющее условию $x \equiv 2 \pmod{5}$, т.е. $x = 2 + 5t_1$. Подставляя в сравнение $f(x) \equiv 0 \pmod{p^2}$, получаем

$$f(2) + pf'(2)t_1 \equiv 0 \pmod{p^2}, \quad -5 \equiv 0 \pmod{25}.$$

Полученное сравнение не имеет решений. Значит (6.9) не имеет решений, удовлетворяющих условию $x \equiv 2 \pmod{5}$. Отметим, что $f'(2) = 0$ (вырожденный случай).

2. Ищем решение, удовлетворяющее условию $x \equiv -1 \pmod{5}$, т.е. $x = -1 + 5t_1$. Подставляя в сравнение $f(x) \equiv 0 \pmod{p^2}$, получаем

$$f(-1)+5t_1 f'(-1) \equiv 0 \pmod{5^2} \Rightarrow -5+5\cdot 9t_1 \equiv 0 \pmod{25} \Rightarrow 9t_1 \equiv 1 \pmod{5}.$$

Следовательно, $t_1 \equiv -1 \pmod{5}$, $t = -1 + 5t_2$,

$$x = -1 + 5 \cdot (-1 + 5t_2) = -6 + 25t_2.$$

Подставляя последнее выражение в сравнение $f(x) \equiv 0 \pmod{p^3}$, получаем

$$f(-6) + 25t_2 f'(-6) \equiv 0 \pmod{125} \Rightarrow -325 + 25 \cdot 144t_2 \equiv 0 \pmod{125} \Rightarrow$$
$$-t \equiv -2 \pmod{5} \Rightarrow t_2 \equiv 2 \pmod{5} \Rightarrow x = -6 + 25t_2 = -6 + 25 \cdot 2 = 44.$$

Ответ: существует единственное решение $x \equiv 44 \pmod{125}$.

§ 7. Сравнения любой степени по произвольному модулю

Пусть f — многочлен степени n с целыми коэффициентами. Рассмотрим сравнение

$$f(x) \equiv 0 \pmod{m}. \tag{7.1}$$

Теорема 7.1. *Пусть $m = m_1 \cdot m_2 \cdot \ldots \cdot m_s$, где $m_i > 1$ попарно взаимно простые. Тогда сравнение (7.1) эквивалентно системе*

$$f(x) \equiv 0 \pmod{m_j}, \quad 1 \le j \le s. \tag{7.2}$$

Доказательство. Если целое x удовлетворяет (7.1), то для любого j

$$m_j \mid m, \quad m \mid f(x) \quad \Longrightarrow \quad m_j \mid f(x) \quad \Longleftrightarrow \quad f(x) \equiv 0 \pmod{m_j}.$$

Пусть целое x удовлетворяет (7.2). Тогда $f(x)$ есть общее кратное всех m_j. Значит, $f(x)$ делится на нок $[m_1, \ldots, m_s] = m$, т.е. $f(x) \equiv 0 \pmod{m}$. □

Замечание 7.1. Если $N_f(n)$ — количество решений сравнения $f(x) \equiv 0 \pmod{n}$, то

$$N_f(m_1 \cdot \ldots \cdot m_s) = N_f(m_1) \cdot \ldots \cdot N_f(m_s),$$

если модули m_i попарно взаимно простые. Полное доказательство мы опускаем.

Любой модуль m можно представить в виде (каноническое разложение)

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

Поэтому, согласно теореме 7.1, исследование и решение сравнения (7.1) сводится к исследованию и решению системы, состоящей из сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}.$$

Пример. Решить сравнение $x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$. Так как $35 = 5 \cdot 7$, то оно эквивалентно следующей системе

$$x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{5}, \quad x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{7}.$$

Первое сравнение имеет два решения: $x \equiv 1$, $x \equiv 4 \pmod{5}$.
Второе сравнение имеет три решения: $x \equiv 3$, $x \equiv 5$, $x \equiv 6 \pmod{7}$.
Значит, исходное сравнение сводится к решению следующих систем

$$x \equiv a_1 \pmod{5}, \quad x \equiv a_2 \pmod{7}, \tag{7.3}$$

где $a_1 \in \{1, 4\}$, $a_2 \in \{3, 5, 6\}$. Используем китайскую теорему об остатках. Имеем

$$\begin{aligned} &M = 35, \quad M_1 = 7, \quad M_2 = 5, \\ &7b_1 \equiv a_1 \pmod{5}, \quad b_1 = 3a_1, \\ &5b_2 \equiv a_2 \pmod{7}, \quad b_2 = 3a_2. \end{aligned}$$

Следовательно, решение (7.3) имеет вид

$$x \equiv M_1 b_1 a_1 + M_2 b_2 a_2 \equiv 21a_1 + 15a_2 \pmod{35}.$$

Подставляя вместо a_1, a_2, указанные выше значения, получаем 6 решений исходной задачи

$$x \equiv 21 \cdot 1 + 15 \cdot 3 \equiv 31, \quad x \equiv 21 \cdot 1 + 15 \cdot 5 \equiv 26, \quad x \equiv 21 \cdot 1 + 15 \cdot 6 \equiv 6 \pmod{35},$$
$$x \equiv 21 \cdot 4 + 15 \cdot 3 \equiv 24, \quad x \equiv 21 \cdot 4 + 15 \cdot 5 \equiv 19, \quad x \equiv 21 \cdot 4 + 15 \cdot 6 \equiv 34 \pmod{35}.$$

Ответ: сравнение имеет шесть решений $x = 31;\ 26;\ 6;\ 24;\ 19;\ 34 \pmod{35}$.

В заключение, отметим, что в некоторых частных случаев существует довольно простые и эффективные методы решения полиномиальных сравнений по простому модулю. Например, пусть нод $(n, p-1) = 1$. Тогда, если сравнение

$$x^n \equiv a \pmod{p}$$

имеет решение, то оно единственно и определяется формулой

$$x \equiv a^{n^*} \pmod{p},$$

где n^* — обратный к n по модулю $p-1$, т.е. $n \cdot n^* \equiv 1 \pmod{p-1}$. Доказательство повторяет рассуждения, использованные при обосновании корректности алгоритма дешифровки шифра RSA. Тем не менее, нет универсальных методов решения произвольных полиномиальных сравнений большой степени.

Численные упражнения к главе V

1. Решить сравнения

   а) $11x \equiv 45 \pmod{37}$; б) $26x \equiv 19 \pmod{31}$;
   в) $899x \equiv 7 \pmod{2166}$; г) $32x \equiv 4 \pmod{60}$.

   Ответы: а) -6; б) 21; в) 359; г) $2, 17, 32, 47$.

2. Решить системы сравнений

   а) $\begin{cases} x \equiv 7 \pmod{11}, \\ x \equiv 13 \pmod{63}; \end{cases}$ б) $\begin{cases} x \equiv 3 \pmod{29}, \\ x \equiv 13 \pmod{21}, \\ x \equiv -5 \pmod{32}; \end{cases}$

   в) $\begin{cases} 11x \equiv 1 \pmod{2}, \\ x \equiv 7 \pmod{21}, \\ x \equiv 3 \pmod{17}; \end{cases}$ г) $\begin{cases} x \equiv 9 \pmod{17}, \\ x \equiv 16 \pmod{19}, \\ x \equiv 29 \pmod{41}. \end{cases}$

   Ответы: а) $139 \pmod{693}$; б) $7195 \pmod{19488}$; в) $343 \pmod{714}$; г) $111 \pmod{13243}$.

3. Решить сравнения

   а) $x^3 + 2x + 2 \equiv 0 \pmod{125}$; б) $x^4 + 7x + 4 \equiv 0 \pmod{27}$;
   в) $x^5 + x^4 + 1 \equiv 0 \pmod{1024}$; г) $x^3 + 2x + 9 \equiv 0 \pmod{216}$;
   д) $x^4 + 7x + 4 \equiv 0 \pmod{189}$.

   Ответы: а) -12; б) -5; в) решений нет; г) 85, 117, 149; д) 101, 76.

Глава VI
Сравнения второй степени

На протяжении всей главы считаем, что p — нечетное простое ($p \neq 2$).

§ 1. Сравнения второй степени по простому модулю

Лемма 1.1. *Если* $a \equiv 0 \pmod{p}$, *то сравнение*

$$x^2 \equiv a \pmod{p}. \tag{1.1}$$

имеет ровно одно решение $x \equiv 0 \pmod{p}$. *Если* $a \not\equiv 0 \pmod{p}$, *то либо сравнение (1.1) не имеет решений, либо имеет ровно два решения.*

Доказательство. Пусть $a \equiv 0 \pmod{p}$ и $x \equiv x_0 \pmod{p}$ — решение (1.1). Тогда $x_0^2 \equiv a \equiv 0 \pmod{p}$. Следовательно, $x_0 \equiv 0 \pmod{p}$.

Пусть $a \not\equiv 0 \pmod{p}$ и сравнение (1.1) имеет решение $x \equiv x_1 \pmod{p}$. Тогда $x \equiv -x_1 \pmod{p}$ также удовлетворяет (1.1). Если $x_1 \equiv -x_1 \pmod{p}$, то $2x_1 \equiv 0 \pmod{p}$. Поэтому $p \mid 2$ либо $p \mid x_1$. Так как $p > 2$, то $p \mid x_1$. Но тогда

$$p \mid x_1^2 \quad \Longrightarrow \quad x_1^2 \equiv 0 \pmod{p} \quad \Longrightarrow \quad x_1^2 \equiv a \equiv 0 \pmod{p}.$$

Получили противоречие с условием. Поэтому $x_1 \not\equiv -x_1 \pmod{p}$ и сравнение (1.1) имеет два решения $x \equiv \pm x_1 \pmod{p}$. Больше решений нет согласно теореме V.5.1. □

Определение. Пусть $a \not\equiv 0 \pmod{p}$. Тогда a называется *квадратичным вычетом по модулю* p, если сравнение (1.1) имеет решение и *квадратичным невычетом*, если не имеет.

Пример. Сравнение $x^2 \equiv -1 \pmod{3}$ не имеет решений, а сравнение $x^2 \equiv -1 \pmod{5}$ имеет два решения $x \equiv \pm 2 \pmod{5}$. Поэтому -1 есть квадратный невычет по модулю 3 и квадратный вычет по модулю 5.

Напомним, что приведенная система вычетов по модулю p, состоит из $(p-1)$ попарно несравнимых чисел по модулю p, которые не делятся на p (например, $1, 2 \ldots, p-1$).

Теорема 1.1. *Любая приведенная система вычетов по модулю* p *содержит ровно* $(p-1)/2$ *квадратичных вычетов и столько же невычетов.*

Если $a \not\equiv 0 \pmod{p}$, *то* p *есть квадратичный вычет тогда и только тогда, когда*

$$a^{(p-1)/2} \equiv 1 \pmod{p} \tag{1.2}$$

и квадратичный невычет тогда и только тогда, когда

$$a^{(p-1)/2} \equiv -1 \pmod{p}. \tag{1.3}$$

Доказательство.

1. Докажем, что если $a \not\equiv 0 \pmod p$, то имеет место одно (и только одно) из сравнений

$$a^{(p-1)/2} \equiv 1 \pmod p \quad \text{либо} \quad a^{(p-1)/2} \equiv -1. \tag{1.4}$$

Действительно, используя малую теорему Ферма, получаем

$$\left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) = a^{p-1} - 1 \equiv 0 \pmod p.$$

Значит, простое p делит один из множителей, стоящих в левой части последнего сравнения, то есть выполняется (1.4). Если выполнены оба сравнения из (1.4), то складывая их, получаем $2a^{(p-1)/2} \equiv 0 \pmod p$, то есть $a \equiv 0 \pmod p$.

2. Докажем, что любая приведенная система вычетов по модулю p содержит не менее, чем $(p-1)/2$ квадратичных вычетов. Для этого рассмотрим целые

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

Они являются квадратичными вычетами. Кроме того, они принадлежат разным классам вычетов. Действительно, если $k, m \in \{1, 2, \ldots, (p-1)/2\}$, $k^2 \equiv m^2 \pmod p$, то

$$k^2 - m^2 = (k-m)(k+m) \equiv 0 \pmod p.$$

Значит, $p \mid (k-m)$, либо $p \mid (k+m)$. Так как $|k \pm m| < p$, то $k = m$.

3. Докажем, что любой квадратичный вычет a удовлетворяет (1.2). По определению, найдется такой x, что $x^2 \equiv a \pmod p$. Т.к. $a \not\equiv 0 \pmod p$, то $x \not\equiv 0 \pmod p$. Используя малую теорему Ферма, получаем

$$a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod p.$$

4. Согласно теореме V.5.1 сравнение (1.2) имеет, не более чем $(p-1)/2$ решений a. Учитывая вышедоказанное, получаем, что любая приведенная система вычетов по модулю p содержит ровно $(p-1)/2$ квадратичных вычетов и они образуют множество решений сравнения (1.2).

5. Осталось доказать, что любой квадратичный невычет a удовлетворяет (1.2). Это вытекает из (1.4) и того, что любое решение (1.2) есть квадратичный вычет. □

Так как p нечетное, то $p \equiv 1$ либо $p \equiv 3 \pmod 4$. В случае $p \equiv 3 \pmod 4$ сравнение (1.1) можно легко решить следующим образом.

Следствие 1.1. *Пусть $p \equiv 3 \pmod 4$ и $a^{(p-1)/2} \equiv 1 \pmod p$. Тогда, сравнение (1.1) разрешимо и его решения определяются формулами*

$$x \equiv \pm a^{(p+1)/4} \pmod p.$$

Доказательство. $x^2 \equiv a^{(p+1)/2} = a^{(p-1)/2} a \equiv 1 \cdot a = a \pmod p$. □

Пример. Решения сравнения $x^2 \equiv 11 \pmod{19}$ имеют вид $x \equiv \pm 11^5 \equiv \pm 7 \pmod{19}$.

Рассмотрим теперь произвольное сравнение второй степени

$$ax^2 + bx + c \equiv 0 \pmod p, \tag{1.5}$$

где $a \not\equiv 0 \pmod p$. Оно сводится к сравнения вида

$$y^2 \equiv D \pmod p. \tag{1.6}$$

Действительно, т.к. $4a \not\equiv 0 \pmod p$, то умножая (1.5) на $4a$, получаем эквивалентное сравнение

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p \iff (2ax+b)^2 \equiv b^2 - 4ac \pmod p.$$

Полагая $D = b^2 - 4ac$ и $y = 2ax + b$, приходим к (1.6). Отметим, что т.к. $2a$ и p взаимно просты, то для любого y существует единственное решение x сравнения

$$2ax + b \equiv y \pmod p,$$

т.е. существует взаимно однозначное соответствие между решениями (1.5) и (1.6).

Решение (1.6) можно определить следующими формулами

$$x \equiv \frac{-b \pm \sqrt{D}}{2a} \pmod p,$$

где под «делением» на $2a$ понимается умножение на обратный к $2a$ по модулю p, а $\sqrt{D} = y$, где y — наименьшее положительное решение сравнения $y^2 \equiv D \pmod p$.

Следствие 1.2. *Пусть $D = b^2 - 4ac$. Тогда сравнение (1.5) имеет единственное решение при $D \equiv 0 \pmod p$, имеет два решение, если D квадратичный вычет по модулю p и не имеет решений, если D квадратичный невычет по модулю p.*

Примеры.

1. Решить сравнение $x^2 + x + 2 \equiv 0 \pmod 7$.

Решение:

$$4x^2 + 4x + 8 \equiv 0 \pmod 7, \quad (2x+1)^2 - 1 + 8 \equiv 0 \pmod 7,$$
$$(2x+1)^2 \equiv 0 \pmod 7, \quad 2x + 1 \equiv 0 \pmod 7, \quad x \equiv 3 \pmod 7.$$

Ответ: $x \equiv 3 \pmod 7$.

2. Решить сравнение $x^2 + x - 2 \equiv 0 \pmod{11}$.

Решение. $D = 1 - 4(-2) \equiv 9 \pmod 7$. Так как сравнение $y^2 \equiv 2 \pmod 7$ имеет решение $y = 3$, то

$$x = \equiv \frac{-1 \pm 3}{2} \equiv (-1 \pm 3) \cdot 4 = -16,\ 8$$

Ответ: $x \equiv -2 \pmod 7$ и $x \equiv 1 \pmod 7$.

§ 2. Символ Лежандра

Определение. Для любого целого a и нечетного простого p символ Лежандра $\left(\frac{a}{p}\right)$ определяется формулой

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{если } a \text{ — квадратичный невычет по модулю } p, \\ 0, & \text{если } p \mid a, \\ 1, & \text{если } a \text{ — квадратичный вычет по модулю } p. \end{cases}$$

Символ Лежандра есть функция двух аргументов a и p, где a — целое, а p — нечетное простое. Она может принимать три значения: ± 1 и 0.

Пример. Найдем $\left(\frac{a}{3}\right)$.

Пусть $a \equiv 1 \pmod 3$. Тогда сравнение $x^2 = a \pmod 3$ эквивалентно $x^2 \equiv 1 \pmod 3$ и имеет решения $x \equiv \pm 1 \pmod 3$, следовательно, $\left(\frac{a}{3}\right) = 1$.

Пусть $a \equiv 2 \pmod 3$. Тогда сравнение $x^2 = a \pmod 3$ эквивалентно $x^2 \equiv 2 \pmod 3$ и не имеет решений, следовательно, $\left(\frac{a}{3}\right) = -1$.

Ответ:

$$\left(\frac{a}{3}\right) = \begin{cases} -1, & a \equiv 2 \pmod 3, \\ 0 & a \equiv 0 \pmod 3, \\ 1, & a \equiv 1 \pmod 3. \end{cases} \tag{2.1}$$

Теорема 2.1. *Справедливы следующие свойства символа Лежандра*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p, \tag{2.2}$$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \qquad \textit{при } a \equiv b \pmod p, \tag{2.3}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \tag{2.4}$$

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \qquad \textit{при } b \not\equiv 0 \pmod p, \tag{2.5}$$

$$\left(\frac{1}{p}\right) = 1, \tag{2.6}$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{2.7}$$

Доказательство. Формула (2.2) вытекает из определения и теоремы 1.1.

Если $a \equiv b \pmod p$, то сравнения $x^2 \equiv a \pmod p$ и $x^2 \equiv b \pmod p$ эквивалентны. Значит, они одновременно разрешимы либо неразрешимы. Поэтому имеет место (2.3).

Используя (2.2), получаем

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

Абсолютная величина разности левой и правой части последнего сравнения меньше p. Поэтому левая и правая части равны, т.е. выполняется (2.4).

Докажем (2.5). Так как b не кратно p, то $\left(\frac{b}{p}\right) \cdot \left(\frac{b}{p}\right) = 1$. Используя (2.4), получаем

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

Сравнение $x^2 \equiv 1 \pmod p$ имеет решения $x \equiv \pm 1 \pmod p$. Поэтому справедливо (2.6).

Докажем (2.7). Согласно (2.2)

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

Так как модуль разности левой и правой части сравнения меньше p, то получаем (2.7). □

Замечание 2.1. Формула (2.7) означает следующее: уравнение $x^2 + 1 \equiv 0 \pmod{p}$ имеет решение в том и только том случае, когда $p = 4k + 1$ (т.е. $p \equiv 1 \pmod 4$).

Теорема 2.2 (квадратичный закон взаимности)**.** *Если p и q — различные простые нечетные, то*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{2.8}$$

Доказательство теоремы мы опустим. Его можно найти в [].

Так как $\left(\frac{q}{p}\right) = \pm 1$, то умножая (2.8) на $\left(\frac{q}{p}\right)$, получаем

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

Квадратичный закон взаимности и теорему 2.1 можно использовать для вычисления символа Лежандра и исследования вопросов о разрешимости квадратичных уравнений.

Примеры.

1. Исследовать вопрос о разрешимости сравнения $x^2 \equiv 53 \pmod{233}$.

Решение. Числа 53 и 233 простые. Поэтому для вычисления $\left(\frac{53}{233}\right)$ можно применять квадратичный закон взаимности. Так как $233 \equiv 21 \pmod{53}$, то согласно (2.3), (2.4), (2.9)

$$\left(\frac{53}{233}\right) = \left(\frac{233}{53}\right)(-1)^{\frac{232}{2}\frac{52}{2}} = \left(\frac{233}{53}\right) = \left(\frac{21}{53}\right) = \left(\frac{7\cdot 3}{53}\right) = \left(\frac{7}{53}\right)\cdot\left(\frac{3}{53}\right) = \left(\frac{53}{7}\right)\cdot\left(\frac{53}{3}\right).$$

Так как $53 \equiv 4 \pmod 7$, $53 \equiv -1 \pmod 3$, то

$$\left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1, \quad \left(\frac{53}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1, \quad \left(\frac{53}{233}\right) = -1.$$

Ответ: решений нет.

2. Выяснить для каких простых p разрешимо сравнение $x^2 + 3 \equiv 0 \pmod{p}$.

Решение. Если $p = 2$, то решение существует $x \equiv \pm 1 \pmod 2$. Если $p = 3$, то решением является $x \equiv 0 \pmod 3$.

Рассмотрим теперь случай $p > 3$. Используя теоремы 2.1, 2.2, получаем

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

Если $p \equiv 1 \pmod 3$, то $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Так как $p \equiv 1 \pmod 2$, то условие $p \equiv 1 \pmod 3$ означает, что $p = 6n + 1$, $n \in \mathbb{N}$.

Если $p \equiv 2 \pmod 3$, то $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$.

Ответ: сравнение разрешимо при $p = 2, 3$ и всех простых вида $p = 6n + 1$.

Приведем без доказательства еще одну важную формулу

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{2.10}$$

Отметим, что $(p^2 - 1) = (p - 1)(p + 1)$ есть произведение двух последовательных четных чисел. Поэтому одно из них кратно 4. Следовательно, $p^2 - 1 \equiv 0 \pmod 8$.

§ 3. Символ Якоби

Определение. Пусть $N > 2$ — натуральное нечетное и $N = p_1 \cdot \ldots \cdot p_s$ — его разложение в произведение простых, не обязательно различных. Для каждого целого a, которое взаимно просто с N, *символ Якоби* $\left(\frac{a}{N}\right)$ определяется формулой

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_s}\right),$$

где в правой части стоит произведение символов Лежандра.

Отметим, что для простого N символ Якоби $\left(\frac{a}{N}\right)$ равен символу Лежандра $\left(\frac{a}{N}\right)$. Поэтому для них используют одинаковое обозначения. Функция «символ Лежандра» есть сужение функции «символ Якоби» на более узкую область определения.

Символ Якоби $\left(\frac{a}{N}\right)$ *не имеет отношения к разрешимости квадратичного сравнения* $x^2 \equiv a \pmod N$ *в случае составного* N.

Пример. Сравнение $x^2 \equiv 2 \pmod 3$ не имеет решений. Поэтому сравнение $x^2 \equiv 2 \pmod{15}$ также не имеет решений. Однако

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3 \cdot 5}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = -1 \cdot (-1)^{\frac{5^2-1}{8}} = 1.$$

Мы будем использовать символ Якоби для построения эффективного алгоритма вычисления символа Лежандра. Для этого нам понадобятся некоторые свойства.

Лемма 3.1. *Пусть* $u_1, \ldots, u_s$ *— целые нечетные. Тогда*

$$(u_1 \cdot \ldots \cdot u_s) - 1 \equiv (u_1 - 1) + \ldots + (u_s - 1) \pmod 4, \tag{3.1}$$
$$(u_1^2 \cdot \ldots \cdot u_s^2) - 1 \equiv (u_1^2 - 1) + \ldots + (u_s^2 - 1) \pmod{64}. \tag{3.2}$$

Доказательство. Так как u_i — нечетное, то $u_i - 1 \equiv 0 \pmod 2$. Поэтому

$$\begin{aligned}(u_i-1)(u_j-1) &\equiv 0 \pmod 4,\\ (u_1\cdot\ldots\cdot u_s)-1 &= \Big(1+(u_1-1)\Big)\cdot\Big(1+(u_2-1)\Big)\cdot\ldots\Big(1+(u_s-1)\Big)-1\equiv\\ &\equiv 1+(u_1-1)+\ldots+(u_s-1)-1 \pmod 4.\end{aligned}$$

Сравнение (3.1) доказано. Так как u_i нечетно, то $u_i^2-1=(u_i-1)(u_i+1)$ есть произведение двух последовательных четных. Одно из них кратно 4. Значит, $u_i^2-1\equiv 0 \pmod 8$. Поэтому

$$\begin{aligned}(u_i^2-1)(u_j^2-1) &\equiv 0 \pmod{64},\\ (u_1^2\cdot\ldots\cdot u_s^2)-1 &= \Big(1+(u_1^2-1)\Big)\cdot\Big(1+(u_2^2-1)\Big)\cdot\ldots\Big(1+(u_s^2-1)\Big)-1\equiv\\ &\equiv 1+(u_1^2-1)+\ldots+(u_s^2-1)-1 \pmod{64}.\end{aligned}$$

□

Величины в обеих частях сравнения (3.1) кратны 2, а (3.2) — кратны 8. Поэтому эти сравнения можно переписать в следующем виде

$$\frac{u_1\cdot\ldots\cdot u_s-1}{2}\equiv\frac{(u_1-1)+\ldots+(u_s-1)}{2} \pmod 2, \tag{3.3}$$

$$\frac{u_1^2\cdot\ldots\cdot u_s^2-1}{8}\equiv\frac{(u_1^2-1)+\ldots+(u_s^2-1)}{8} \pmod 8. \tag{3.4}$$

Еще раз напомним, что мы определили символ Якоби $\left(\frac{a}{N}\right)$ для нечетного $N>2$ и целого a, который взаимно простой с N. Ниже везде считаем выполненными эти условия.

Теорема 3.1. *Справедливы следующие свойства символа Якоби*

$$\left(\frac{a}{N}\right)=\left(\frac{b}{N}\right) \qquad \text{при } a\equiv b \pmod N, \tag{3.5}$$

$$\left(\frac{ab}{N}\right)=\left(\frac{a}{N}\right)\cdot\left(\frac{b}{N}\right), \tag{3.6}$$

$$\left(\frac{1}{N}\right)=1, \tag{3.7}$$

$$\left(\frac{-1}{N}\right)=(-1)^{\frac{N-1}{2}}, \tag{3.8}$$

$$\left(\frac{2}{N}\right)=(-1)^{\frac{N^2-1}{8}}. \tag{3.9}$$

Кроме того, если P,Q положительные нечетные и нод $(P,Q)=1$, *то*

$$\left(\frac{P}{Q}\right)=\left(\frac{Q}{P}\right)(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}. \tag{3.10}$$

Доказательство. Считаем, что $N = p_1 \cdot \ldots \cdot p_s$, где p_i — простые.

Пусть $a \equiv b \pmod N$. Тогда $a \equiv b \pmod{p_i}$, $i = \overline{1,s}$. Поэтому, согласно (2.3)

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

Докажем (3.6). Ввиду (2.4),

$$\left(\frac{ab}{N}\right) = \prod_{i=1}^{s}\left(\frac{ab}{p_i}\right) = \prod_{i=1}^{s}\left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \left(\prod_{i=1}^{s}\left(\frac{a}{p_i}\right)\right)\left(\prod_{i=1}^{s}\left(\frac{b}{p_i}\right)\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right).$$

Формула (3.7) вытекает из (2.6). Докажем (3.8). Используя (2.6), имеем

$$\left(\frac{-1}{N}\right) = \prod_{i=1}^{s}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{s}(-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{(p_1-1)+\ldots+(p_s-1)}{2}}.$$

Согласно (3.3) найдется такое целое k, что

$$\frac{(p_1-1)+\ldots+(p_s-1)}{2} = \frac{(p_1\cdot\ldots\cdot p_s)-1}{2} + 2k = \frac{N-1}{2} + 2k.$$

Поэтому $\left(\dfrac{-1}{N}\right) = (-1)^{\frac{N-1}{2}+2k} = (-1)^{\frac{N-1}{2}}$.

Докажем (3.9). Ввилу (2.10),

$$\left(\frac{2}{N}\right) = \prod_{i=1}^{s}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{s}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\frac{(p_1^2-1)+\ldots+(p_s^2-1)}{8}}.$$

Согласно (3.3) найдется такое целое k, что

$$\frac{(p_1^2-1)+\ldots+(p_s^2-1)}{8} = \frac{(p_1^2\cdot\ldots\cdot p_s^2)-1}{8} + 8k = \frac{N^2-1}{8} + 8k.$$

Поэтому $\left(\dfrac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}+8k} = (-1)^{\frac{N^2-1}{8}}$.

Осталось доказать (3.10). Пусть $P = p_1 \cdot \ldots \cdot p_s$ и $Q = q_1 \cdot \ldots \cdot q_r$ — разложения P и Q в произведение простых. Так как нод $(P,Q) = 1$, то $p_i \neq q_j$ для любых i и j. Используя (3.6), квадратичный закон взаимности, свойство (2.4) и формулу (3.3), получаем

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{r}\left(\frac{p_1\cdot\ldots\cdot p_s}{q_j}\right) = \prod_{j=1}^{r}\prod_{i=1}^{s}\left(\frac{p_i}{q_j}\right) = \prod_{j=1}^{r}\prod_{i=1}^{s}\left(\frac{q_i}{p_j}\right)(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \left(\frac{Q}{P}\right)(-1)^T,$$

где

$$\begin{aligned} T &= \sum_{j=1}^{r}\sum_{i=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2} = \left(\sum_{j=1}^{r}\frac{q_j-1}{2}\right)\cdot\left(\sum_{i=1}^{s}\frac{q_i-1}{2}\right) \equiv \\ &\equiv \frac{q_1\cdot\ldots q_r-1}{2}\cdot\frac{p_1\cdot\ldots p_s-1}{2} = \frac{Q-1}{2}\frac{P-1}{2} \pmod 2. \end{aligned}$$

Поэтому $(-1)^T = (-1)^{\frac{Q-1}{2}\frac{P-1}{2}+2k} = (-1)^{\frac{Q-1}{2}\frac{P-1}{2}}$. □

Свойства символа Якоби (3.5), (3.10) позволяют сводить вычисление символа Лежандра к случаям вида (3.7), (3.8) и (3.9). Главная особенность заключается в следующем: квадратичный закон взаимности для символа Лежандра применим только при нечетных *простых* P и Q. Поэтому, если P составное, то его нужно разлагать на простые сомножители. Это сложная задача. Тогда как формула (3.10) для символа Якоби справедлива для *произвольных* нечетных взаимно простых P, Q.

Вычисление символа Якоби $\left(\frac{a}{b}\right)$ сводится к многократному повторению шагов следующих трех видов.

1. Если $a \in \{1, -1, 2\}$, то $\left(\frac{a}{b}\right)$ вычисляется по формулам (3.7), (3.8), (3.9).

2. Если $a > b$, то $\left(\frac{a}{b}\right) = \left(\frac{r}{b}\right)$, где r — остаток от деления a на b.

3. Пусть a — четное и $a > 2$. Тогда $a = 2^k \cdot \tilde{a}$, где $\tilde{a}$ — нечетное. Согласно (3.6)
$$\left(\frac{a}{b}\right) = \left(\frac{\tilde{a}}{b}\right)\left(\frac{2}{b}\right)^k.$$

4. Если $a < b$, a, b — положительные нечетные и $a > 2$, то $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.

Замечание 3.1. Количество шагов вида 2 не больше, чем количество делений в алгоритме Евклида нахождения нод (a, b), то есть оно оценивается величиной $1.45 \cdot \log_2 a$. Количество шагов вида 3 не больше, чем $\log_2 a$.

Примеры.

1. Вычислим символ Лежандра $\left(\frac{53}{233}\right)$ с помощью свойств символа Якоби:

$$\begin{aligned}\left(\frac{53}{233}\right) &= \left(\frac{233}{53}\right)(-1)^{\frac{233-1}{2}\frac{53-1}{2}} = \left(\frac{233}{53}\right) = \left(\frac{21}{53}\right) = \left(\frac{53}{21}\right)(-1)^{\frac{53-1}{2}\frac{21-1}{2}} = \left(\frac{53}{21}\right) = \\ &= \left(\frac{11}{21}\right) = \left(\frac{21}{11}\right) = \left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = -1.\end{aligned}$$

2. Исследовать вопрос о разрешимости сравнения $x^2 \equiv 219 \pmod{383}$.

Решение. Вычислим символ Лежандра $\left(\frac{219}{383}\right)$ с помощью свойств символа Якоби:

$$\begin{aligned}\left(\frac{219}{383}\right) &= -\left(\frac{383}{219}\right) = -\left(\frac{164}{383}\right) = -\left(\frac{383}{164}\right) = -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) = \\ &= -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = 1.\end{aligned}$$

Ответ: сравнение имеет два решения.

3. Исследовать вопрос о разрешимости сравнения $x^2 \equiv 871 \pmod{1009}$.

Решение. Вычислим символ Лежандра $\left(\frac{871}{1009}\right)$ с помощью свойств символа Якоби:

$$\begin{aligned}
\left(\frac{871}{1009}\right) &= \left(\frac{1009}{871}\right)(-1)^{\frac{871-1}{2}\frac{1009-1}{2}} = \left(\frac{1009}{871}\right) = \left(\frac{138}{871}\right) = \left(\frac{2\cdot 69}{871}\right) = \\
&= \left(\frac{2}{871}\right)\cdot\left(\frac{69}{871}\right) = (-1)^{\frac{871^2-1}{8}}\left(\frac{69}{871}\right) = \left(\frac{69}{871}\right) = \left(\frac{871}{69}\right)(-1)^{\frac{871-1}{2}\frac{69-1}{2}} = \\
&= \left(\frac{871}{69}\right) = \left(\frac{43}{69}\right) = \left(\frac{69}{43}\right)(-1)^{\frac{69-1}{2}\frac{43-1}{2}} = \left(\frac{69}{43}\right) = \left(\frac{26}{43}\right) = \left(\frac{2\cdot 13}{43}\right) = \\
&= \left(\frac{2}{43}\right)\cdot\left(\frac{13}{43}\right) = (-1)^{\frac{43^2-1}{8}}\left(\frac{43}{13}\right)(-1)^{\frac{43-1}{2}\frac{13-1}{2}} = (-1)\cdot\left(\frac{4}{13}\right) = \\
&= -\left(\frac{2}{13}\right)\cdot\left(\frac{2}{13}\right) = -1.
\end{aligned}$$

Ответ: сравнение не имеет решений.

В заключение отметим, что в случае нод $(a, N) > 1$ полагают $\left(\frac{a}{N}\right) = 0$.

Численные упражнения к главе VI

1. Среди вычетов приведенной системы по модулю 23 найти все квадратичные вычеты и квадратичные невычеты.

2. Среди вычетов приведенной системы по модулю 37 найти все квадратичные вычеты и квадратичные невычеты.

3. Решить сравнения $x^2 \equiv 2$ и $x^2 \equiv 5 \pmod{23}$.

4. Вычислить а) $\left(\frac{111}{541}\right)$, б $\left(\frac{529}{601}\right)$, в) $\left(\frac{2108}{2003}\right)$, г) $\left(\frac{19525}{1847}\right)$.

5. Исследовать вопрос о разрешимости сравнений

   а) $x^2 \equiv 68 \pmod{113}$, б) $x^2 \equiv 219 \pmod{383}$,
   в) $x^2 + 7x + 45 \equiv 0 \pmod{409}$, г) $5x^2 + 11x - 91 \equiv 0 \pmod{379}$.

6. Найти все простые p, для которых разрешимо сравнение $x^2 \equiv 5 \pmod{p}$.

7. Найти все простые p для которых разрешимо сравнение $x^2 - 2 \equiv 0 \pmod{p}$.

8. Найти все простые p для которых разрешимо сравнение $x^2 + 2 \equiv 0 \pmod{p}$.

Ответы. 3. а) нет; б) $x \equiv \pm 5$. **4.** а) -1; б) 1; в) 1; г) -1. **5.** а) нет; б) да; в) да; г) нет. **6.** $p = 2, 5$ и $p \equiv \pm 1 \pmod{5}$. **7.** $p = 2$, $p \equiv \pm 1 \pmod{8}$. **8.** $p = 2$ и $p \equiv \pm 1 \pmod{8}$, $p \equiv \pm 3 \pmod{8}$.

Глава VII
Первообразные корни и индексы

§ 1. Показатели чисел и их основные свойства

Возьмем любое натуральное $m > 2$. Если нод $(a, m) = 1$, то по теореме Эйлера

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \tag{1.1}$$

где $\varphi(m)$ — функция Эйлера. Для некоторых a сравнение

$$a^u \equiv 1 \pmod{m} \tag{1.2}$$

может выполняться для натурального u, которое меньше, чем $\varphi(m)$.

Пример. $\varphi(8) = 4$, $3^2 \equiv 1 \pmod{8}$.

Определение. Наименьшее натуральное u, удовлетворяющее (1.2), называется *показателем числа a по модулю m.*

Пример. Пусть $a = 2$, $m = 7$. Тогда $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1 \pmod{7}$. Значит, показатель 2 по модулю 7 равен 3.

Подчеркнем, что любой показатель по модулю m удовлетворяет неравенствам

$$1 \leq u \leq \varphi(m).$$

Случай $m = 2$ исключают из рассмотрению, ввиду тривиальности. Если нод $(a, m) > 1$, то не существует u, удовлетворяющего (1.2). Поэтому показатели определяются только для целых взаимно простых с модулем и ниже это условие считается всюду выполненным.

Теорема 1.1. *Пусть u — показатель целого a по модулю $m > 2$.*

а) Если $n \in \mathbb{N}$ и $a^n \equiv 1 \pmod{m}$, то $u \mid n$.

б) Целые

$$1, \quad a, \quad a^2, \quad \ldots, \quad a^{u-1} \tag{1.3}$$

являются попарно несравнимыми по модулю m. Любое число вида a^k, $k \in \mathbb{N}$ сравнимо по модулю m с одним из чисел (1.3).

в) Если v — показатель целого b по модулю m, причем нод $(u, v) = 1$, *то показатель ab равен uv.*

г) Если $k \in \mathbb{N}$, то показатель a^k равен u/d, где $d = \text{нод}\,(k, u)$.

Доказательство. Докажем а). Пусть $n = uq + r$, где $0 \le r < u$. Так как

$$1 \equiv a^n = a^{uq} \cdot a^k = (a^u)^q \cdot a^r \equiv a^r \pmod{m},$$

то $a^r \equiv 1 \pmod{m}$, причем $r < u$. По определению показателя u, это возможно только при $r = 0$. Следовательно, n делится на u.

Докажем б). Пусть $a^k \equiv a^j \pmod{m}$, где $k, j \in \{0, \dots u-1\}$, $j \le k$. Так как a и m взаимно простые, то нод $(a^j, m) = 1$. Поэтому обе части сравнения $a^k \equiv a^j \pmod{m}$ можно сократить на a^j. Получаем

$$a^{k-j} \equiv 1 \pmod{m}.$$

Так как $(k-j) < u$, то это возможно только при $k = j$. Возьмем теперь любое $k \in \mathbb{N}$ и представим его в виде $k = qu + r$, где $0 \le r < u$. Тогда

$$a^k = a^{qu+r} = (a^u)^q \cdot a^r \equiv a^r \pmod{m},$$

т.е. a^k сравнимо с одним из чисел (1.3).

Докажем в). Пусть w – показатель ab. Так как

$$(ab)^{uv} = (a^u)^v \cdot (b^v)^u \equiv 1^v \cdot 1^u = 1 \pmod{m},$$

то, ввиду а), $w \mid uv$. С другой стороны, поскольку $(ab)^w \equiv 1 \pmod{m}$, то

$$1 \equiv ((ab)^w)^u = (a^u)^w \cdot b^{wu} \equiv b^{wu} \pmod{m}.$$

Согласно а), $v \mid wu$. Так как нод $(v, u) = 1$, то $v \mid w$. Аналогичным образом доказывается, что $u \mid w$. Значит, $(uv) \mid w$. Получили $w \mid uv$ и $(uv) \mid w$. Поэтому $uv = w$.

Докажем г). Используем такие же рассуждения как и при доказательстве в). Пусть w — показатель a^k. Тогда

$$\text{нод}\left(\frac{u}{d}, \frac{k}{d}\right) = 1,$$
$$(a^k)^{u/d} = (a^u)^{k/d} \equiv 1 \pmod{m}.$$

Значит, w делит u/d. С другой стороны,

$$1 \equiv (a^k)^w = a^{kw} \pmod{m}.$$

Значит, u делит kw. Поэтому $\frac{u}{d}$ делит $\frac{k}{d} \cdot w$. Так как нод $(u/d, k/d) = 1$, то $\frac{u}{d} \mid w$. Получили $\frac{u}{d} \mid w$ и $w \mid \frac{u}{d}$. Значит, $w = u/d$. □

§ 2. Первообразные корни и их основные свойства

Определение. Целое a называется первообразным корнем по модулю m, если его показатель равен $\varphi(m)$.

Пример. Пусть $m = 7$. Имеем $\varphi(m) = 6$,

$$3^2 = 9 \equiv 2 \pmod 7, \quad 3^3 = 9 \cdot 3 \equiv 2 \cdot 3 = 6 \pmod 7, \quad 3^4 = 9^2 \equiv 2^2 = 4 \pmod 7,$$
$$3^5 = 9^2 \cdot 3 \equiv 2^2 \cdot 3 = 5 \pmod 7, \quad 3^6 \equiv 1 \pmod 7.$$

Значит, 3 является первообразным корнем по модулю 7.

Если a — первообразный корень по модулю m, то его простейшие свойства вытекают из теоремы 1.1, в которой полагаем $u = \varphi(m)$.

Теорема 2.1.

а) Натуральное a является первообразным корнем по модулю m тогда и только тогда, когда числа

$$1, \quad a, \quad a^2, \quad \ldots, \quad a^{\varphi(m)-1}, \tag{2.1}$$

образуют приведенную систему вычетов по модулю m.

б) Пусть m — простое. Натуральное a является первообразным корнем по модулю m тогда и только тогда, когда числа

$$0, \quad 1, \quad a, \quad a^2, \quad \ldots, \quad a^{m-2} \tag{2.2}$$

образуют полную систему вычетов по модулю m.

Доказательство. Докажем а). Пусть a — первообразный корень. Согласно теореме 1.1 б), числа (2.1) попарно несравнимы по модулю m. Количество этих чисел равно $\varphi(m)$. Значит, (2.1) образуют приведенную систему вычетов. Пусть числа (2.1) образуют приведенную систему вычетов. Пусть u — показатель a. Тогда

$$a^u \equiv 1 \pmod m.$$

Так как числа (2.1) попарно несравнимы, то $u > \varphi(m) - 1$, т.е. $u \geq \varphi(m)$, $u = \varphi(m)$.

Утверждение б) вытекает из а), т.к. $\varphi(m) = m - 1$ для простого m. □

Замечание 2.1. Если p — простое, a — любой первообразный корень по модулю p, то

$$\mathbb{Z}_p \setminus \{0\} = \left\{a^k \pmod p : \quad k = 0, 1, \ldots, p-2\right\}.$$

Подчеркнем, что *не для всех модулей существуют первообразные корни.*

Пример. Пусть $m = 12$. Тогда $\varphi(12) = 4$. Из чисел $\{2, 3, \ldots, 11\}$ взаимно простыми с модулем 12 будут 5, 7 и 11 (только они могут быть первообразными). Однако

$$5^2 = 25 \equiv 1 \pmod{12}, \quad 7^2 \equiv (-5)^2 \equiv 1 \pmod{12}, \quad 11^2 \equiv (-1)^2 = 1 \pmod{12}.$$

Поэтому первообразных корней по модулю 12 не существует.

Вопрос о том для каких модулей существуют первообразные корни будет рассмотрен в следующем параграфе.

Если известны простые делители $\varphi(m)$, то первообразные корни можно находить с помощью следующего результата.

Лемма 2.1. *Пусть* нод $(a, m) = 1$. *Тогда a является первообразным корнем по модулю m, если и только если для любого простого p, делящего $\varphi(m)$,*

$$a^{\varphi(m)/p} \not\equiv 1 \pmod{m}. \tag{2.3}$$

Доказательство. Если a — первообразный корень, то (2.3) вытекает из определений.

Пусть выполняется (2.3). Пусть u — показатель a по модулю p. Так как $a^{\varphi(m)} \equiv 1 \pmod{m}$, то по теореме 1.1 а), $u \mid \varphi(m)$. Если $u < \varphi(m)$, то существует простое p, делящее $\varphi(m)/u$, т.е. найдется такое $k \in \mathbb{N}$, что

$$\frac{\varphi(m)}{u} = kp, \qquad a^{\varphi(m)/p} = a^{uk} \equiv 1 \pmod{m}.$$

Получили противоречие с условием (2.3). Значит, $u = \varphi(m)$. □

Пример. Найдем первообразные корни $a \in \{1, \ldots, 10\}$ по модулю 11.
Решение. Так как $\varphi(11) = 10 = 2 \cdot 5$, то a есть первообразный корень, если и только если

$$a \not\equiv 0 \pmod 2, \quad a \not\equiv 0 \pmod 5, \quad a^2 \not\equiv 1 \pmod{11}, \quad a^5 \not\equiv 1 \pmod{11}.$$

Имеем

$$\begin{array}{ll}
3^2 \equiv 9 \pmod{11}, & 3^5 = 3 \cdot 81 \equiv 3 \cdot 4 \equiv 1 \pmod{11}, \\
4^2 \equiv 5 \pmod{11}, & 4^5 = 4 \cdot 64 \equiv 5 \cdot 9 \equiv 1 \pmod{11}, \\
6^2 \equiv (-5)^2 \equiv 4 \pmod{11}, & 6^5 \equiv (-5)^5 \equiv -1 \pmod{11}, \\
7^2 \equiv (-4)^2 \equiv 5 \pmod{11}, & 7^5 \equiv (-4)^5 \equiv -1 \pmod{11}, \\
8^2 \equiv (-3)^2 \equiv 9 \pmod{11}, & 8^5 \equiv (-3)^5 \equiv -1 \pmod{11}, \\
9^2 \equiv (-2)^2 \equiv 4 \pmod{11}, & 9^5 \equiv (-2)^5 \equiv 1 \pmod{11}, \\
10^2 \equiv (-1)^2 \equiv 1 \pmod{11}. &
\end{array}$$

Ответ: 2, 6, 7, 8.

§ 3. Результаты о существовании первообразных корней

Сначала мы докажем теорему о существовании первообразных корней по простому нечетному модулю p. Для этого нам понадобятся две вспомогательные леммы.

Лемма 3.1. *Пусть p — простое нечетное, $a \in \mathbb{Z}$, причем показатель a по модулю p равен u. Тогда любое целое с показателем u сравнимо по модулю p с одним из чисел*

$$1, \quad a, \quad a^2, \quad \ldots, \quad a^{u-1}. \tag{3.1}$$

Доказательство. Любое целое x с показателем u удовлетворяет сравнению

$$x^u \equiv 1 \pmod{p}. \tag{3.2}$$

По теореме V.5.1 сравнение (3.1) имеет не более, чем u решений. Числа (3.1) удовлетворяют (3.2), они попарно несравнимы по модулю p (см. теорему 1.1 б)) и их ровно u штук. Поэтому любое x, удовлетворяющее (3.2), сравнимо с одним из чисел (3.1). □

Лемма 3.2. *Пусть p — простое нечетное; $\omega(u)$ — количество таких $a \in \{1, 2, \ldots, p-1\}$, что показатель a по модулю p равен u. Тогда для любого $u \mid (p-1)$*

$$\omega(u) = \varphi(u). \tag{3.3}$$

Доказательство. Рассмотрим сначала случай, когда $\omega(u) > 0$. Тогда существует такой $a \in \{1, 2, \ldots, p-1\}$, что показатель a равен u. Возьмем любое другое целое $b \in \{1, 2, \ldots, p-1\}$ с показателем u. По лемме 3.1 существует единственное $k \in \{0, 1, \ldots, u-1\}$ такое, что $b \equiv a^k \pmod{p}$. Показатель a^k равен b и равен u. Согласно теореме 1.1 г) показатель a^k равен u, если и только если нод $(k, u) = 1$. Поэтому $\omega(u)$ совпадает с количеством таких $k \in \{1, \ldots, u-1\}$, что нод $(k, u) = 1$, т.е. равно $\varphi(u)$. Формула (3.3) доказана при $\omega(u) > 0$.

Рассмотрим теперь общий случай. Пусть $\Omega(u)$ состоит из чисел $a \in \{1, 2, \ldots, p-1\}$ таких, что показатель a равен u. Тогда

$$\bigcup_{u=1}^{p-1} \Omega(u) = \{1, \ldots, p-1\},$$

причем $\omega(a)$ есть количество элементов множества $\Omega(u)$. Так как $a^{p-1} \equiv 1 \pmod{p}$, то по теореме 1.1 г), любой показатель является делителем $(p-1)$. Значит,

$$\bigcup_{u \mid (p-1)} \Omega(u) = \{1, \ldots, p-1\}.$$

Так как $\Omega(u) \cap \Omega(v) = \emptyset$ при $u \neq v$, то

$$\sum_{u \mid (p-1)} \omega(u) = p - 1.$$

Согласно формуле (III.4.4)

$$\sum_{u \mid (p-1)} \varphi(u) = p - 1.$$

Следовательно,

$$\sum_{u \mid (p-1)} (\varphi(u) - \omega(u)) = 0.$$

Поскольку $\varphi(u) = \omega(u)$ при $\omega(u) > 0$, то $\varphi(u) - \omega(u) \geq 0$. Значит, выполняется (3.3). □

Теорема 3.1. *Пусть p — простое нечетное. Тогда существует ровно $\varphi(p-1)$ первообразных корней по модулю p.*

Доказательство. Пусть функция ω такая же, как и в предыдущей лемме. Тогда количество первообразных корней по модулю p равно $\omega(\varphi(p)) = \omega(p-1) = \varphi(p-1)$. □

Пример. Пусть $p = 1009$. Тогда

$$p - 1 = 1008 = 2^4 \cdot 3^2 \cdot 7, \quad \varphi(p-1) = \varphi(2^4)\varphi(3^2)\varphi(7) = (2^4 - 2^3)(3^2 - 3)(7 - 1) = 288.$$

Следовательно, существует 288 первообразных корней по модулю 1009.

Приведем теперь все случаи, в которых первообразные корни существуют.

Теорема 3.2. *Первообразные корни существуют только для следующих модулей*

$$2, \quad 4, \quad p^\alpha, \quad 2p^\alpha,$$

где p — простое нечетное, а $\alpha \in \mathbb{N}$.

Доказательство теоремы мы опускаем. Его можно найти в [].

§ 4. Индексы (дискретные логарифмы)

Определение. Целое x, удовлетворяющее сравнению

$$a^x \equiv b \pmod m, \tag{4.1}$$

называется *индексом (дискретным логарифмом)* числа b по модулю m при основании a и обозначается $\operatorname{ind}_a b$.

По определению

$$a^{\operatorname{ind}_a b} \equiv b \pmod m.$$

Очевидно, что индексы существуют не для любых a, b, m. Например, сравнение (4.1) заведомо не имеет решений, если нод (a, m) не делит b. Простота модуля m также не гарантирует разрешимость (4.1).

Пример. Уравнение $2^x \equiv b \pmod 7$ имеет решение только при $b \in \{1, 2, 4\}$.

Рассмотрим сначала вопрос о структуре множества возможных решений (4.1).

Лемма 4.1. *Пусть* нод $(a, m) = 1$ *и существует такое* x_0, *что* $a^{x_0} \equiv b \pmod m$. *Тогда множество целых, удовлетворяющих сравнению (4.1), совпадает с классом вычетов* $x \equiv x_0 \pmod u$, *где* u — *показатель целого* a *по модулю* m.

Доказательство. Пусть $x \equiv x_0 \pmod u$. Тогда существует такой k, что

$$x = x_0 + ku, \qquad a^x = a^{x_0} \cdot (a^u)^k \equiv b \cdot (1)^k = b \pmod u,$$

т.е. любое число из класса вычетов $x \equiv x_0 \pmod u$ удовлетворяет (4.1).

Возьмем любое целое x, удовлетворяющее (4.1). Пусть, например, $x > x_0$. Так как нод $(a, m) = 1$, то нод $(a^{x_0}, m) = 1$. Поэтому обе части сравнения $a^x \equiv a^{x_0} \pmod m$ можно сократить на a^{x_0}. В итоге, получаем

$$a^{x-x_0} \equiv 1 \pmod m.$$

Значит, $u \mid (x - x_0)$ по теореме 1.1. □

Рассмотрим теперь вопрос о разрешимости сравнения (4.1). Следующая теорема является эквивалентной формулировкой теоремы 1.1 б).

Теорема 4.1. *Пусть* нод $(a, m) = 1$ *и* u — *показатель целого* a *по модулю* m. *Сравнение (4.1) имеет решение только для целых* b *вида*

$$b \equiv a^k \pmod m, \quad k \in \{0, 1, \ldots, u-1\}. \tag{4.2}$$

В частности, количество $b \in \mathbb{Z}_m$ *для которых сравнение (4.1) имеет решение равно* u.

Доказательство. Если существует x, удовлетворяющий (4.1), то по теореме 1.1 б) найдется такое $k \in \{0, 1, \ldots, u-1\}$, что $a^x \equiv a^k \pmod m$. Поэтому имеет место (4.2). Если выполняется (4.2), то $x = k$ удовлетворяет (4.1). □

Если нод $(a, m) = 1$, то условие нод $(b, m) = 1$ является необходимым для разрешимости сравнения (4.1). Рассмотрим вопрос о том, когда это условие является не только необходимым, но и достаточным.

Следствие 4.1. *Пусть* нод $(a, m) = 1$. *Следующие утверждения эквивалентны.*

а) Решение сравнения (4.1) существует, если нод $(b, m) = 1$;

б) Число a является первообразным корнем по модулю m.

Доказательство. Пусть выполняется а). Тогда согласно теореме 4.1 $u = \varphi(m)$, т.е. a есть первообразный корень. Пусть выполняется б). Тогда по теореме 2.1 а) числа $1, a, \ldots, a^{u-1}$ образуют приведенную систему вычетов. Утверждение а) следует из теоремы 4.1. □

Следствие 4.2. *Пусть* нод $(a, m) = 1$. *Следующие утверждения эквивалентны.*

а) сравнение (4.1) имеет решение для любого b, не кратного m;

б) m — простое число, a — первообразный корень по модулю m.

Доказательство. Пусть выполняется а). Согласно теореме 4.1 это означает, что $u = m-1$. Так как $u \le \varphi(m) \le m - 1$, то $u = \varphi(m) = m - 1$, т.е. имеет место б).

Пусть выполняется б). Тогда согласно следствию 4.1 количество $b \in \mathbb{Z}_m$ для которых сравнение (4.1) имеет решение равно $u = \varphi(m) = m - 1$. Отсюда вытекает а). □

Таким образом, индекс $\mathrm{ind}_a b$ по модулю m существует, если a — первообразный корень по модулю m и $(b, m) = 1$. Ниже предполагаем, что все рассматриваемые индексы существуют. Следующие свойства индексов похожи на свойства логарифмов.

Лемма 4.2. *Пусть u — показатель a по модулю m. Тогда*

$$\mathrm{ind}_a(xy) \equiv \mathrm{ind}_a x + \mathrm{ind}_a y \pmod{u},$$
$$\mathrm{ind}_a x \equiv (\mathrm{ind}_b x) \cdot (\mathrm{ind}_a b) \pmod{u}.$$

Доказательство. По определению индекса

$$a^{\mathrm{ind}_a(xy)} \equiv xy \equiv a^{\mathrm{ind}_a x} a^{\mathrm{ind}_a y} = a^{\mathrm{ind}_a x + \mathrm{ind}_a y} \pmod{m}.$$
$$a^{\mathrm{ind}_b x \, \mathrm{ind}_a b} = (a^{\mathrm{ind}_a b})^{\mathrm{ind}_b x} \equiv b^{\mathrm{ind}_b x} \equiv x \equiv a^{\mathrm{ind}_a x} \pmod{m}.$$

Осталось воспользоваться леммой 4.1. □

Численные упражнения к главе VI

1. Найти показатель 7 по модулю 43.
2. Найти первообразные корни по модулю 7.
3. Найти наименьшие первообразные корни по модулям 13, 17, 23.
4. Выяснить для каких $b \in \{0, 1, \ldots, 19\}$ разрешимо сравнение $3^x \equiv b \pmod{20}$.

Ответы: 1) 6; 2) 3 и 5; 3) 2, 3, 3; 4) 1, 3, 7, 9.

Вариант 1

Контрольная работа по главе I.

1. Указать какие из чисел 233, 237 простые. Обосновать ответ с помощью решета Эратосфена.
2. Найти множество общих делителей чисел a, b, где $a = 1000$, $b = 550$.
3. Найти нод (a, b, c), где $a = 2^{100}3^{99}7^{40}$, $b = 2^{50} \cdot 3 \cdot 5^2 \cdot 7^5$, $c = 2 \cdot 3^{21} \cdot 5^{10} \cdot 7$.

Контрольная работа по главе II.

1. Найти нод $(28, 12, 60, 102)$.
2. Разложить в непрерывную дробь число $25/9$ и найти все подходящие дроби.
3. Решить уравнение $61x + 17y = 1$.

Контрольная работа по главе III.
Вычислить $\tau(n)$, $\sigma(n)$ и $\varphi(n)$ при 1) $n = 1000$, 2) $n = 3^3 \cdot 7 \cdot 11^2$.

Ответы:
КР 1: 2) $1, 2, 5, 10, 25, 50$. 3) 42
КР 2: 1) 2. 2) $[2; 1, 3, 2]$; $\frac{2}{1}, \frac{3}{1}, \frac{11}{4}, \frac{25}{9}$. 3) $x = -5 + 17t$, $y = 18 - 61t$.
КР 3: $\tau(1000) = 16$, $\sigma(1000) = 12 \cdot 13 \cdot 15 = 2340$, $\varphi(1000) = 400$;
$\tau(3^3 \cdot 7 \cdot 11^2) = 24$, $\sigma(\ldots) = 40 \cdot 8 \cdot 33 = 42560$, $\varphi(\ldots) = 17820$.

Вариант 2

Контрольная работа по главе I.

1. Указать какие из чисел 281, 283 простые. Обосновать ответ с помощью решета Эратосфена.
2. Найти множество общих делителей чисел 1100 и 450.
3. Найти нод (a, b, c), где $a = 2^5 3^{10} 7^4$, $b = 2^{50} \cdot 3 \cdot 5^3 \cdot 7^2$, $c = 2^2 \cdot 3^{31} \cdot 5^{20} \cdot 7$.

Контрольная работа по главе II.

1. Найти нод $(66, 42, 18, 54)$.
2. Разложить в непрерывную дробь число $111/40$ и найти все подходящие дроби.
3. Решить уравнение $15x + 19y = 1$.

Контрольная работа по главе III.
Вычислить $\tau(n)$, $\sigma(n)$ и $\varphi(n)$ при 1) $n = 900$, 2) $n = 2^5 \cdot 3^3 \cdot 5$.

Ответы:
КР 1: 2) $2^{\alpha_1} 5^{\alpha_2} 11^{\alpha_3}$, $\alpha_{1,2} = 0, 1, 2$, $\alpha_3 = 0, 1$. 3) $2^2 \cdot 3 \cdot 7 = 84$.
КР 2: Ответы: 1) 6. 2) $[2; 1, 3, 2, 4]$; $\frac{2}{1}, \frac{3}{1}, \frac{11}{4}, \frac{25}{9}, \frac{111}{40}$. 3) $x = -5 - 19t$, $y = 4 + 15tt$.
КР 3:
$\tau(900) = 27$, $\sigma(900) = 7 \cdot 31 \cdot 13 = 2821$, $\varphi(900) = 240$;
$\tau(3^5 \cdot 3^3 \cdot 5) = 48$, $\sigma(\ldots) = 64 \cdot 40 \cdot 20 = 51200$, $\varphi(\ldots) = 32 \cdot 18 \cdot 4 = 2304$.