Лекции по курсу
«Элементы теории чисел»

лектор: д.ф.-м.н. Герман О.Н.

Содержание

1 Алгоритм Евклида и его применения **2**
1.1 Деление с остатком . . . 2
1.2 Алгоритм Евклида . . . 2
1.3 Основная теорема арифметики . . . 4
1.4 Линейные диофантовы уравнения от двух неизвестных . . . 6
1.5 Конечные цепные дроби . . . 7
1.6 Линейные диофантовы уравнения от произвольного количества неизвестных . . . 9

2 Арифметические функции **12**
2.1 Формула обращения Мёбиуса . . . 12
2.2 Функция Эйлера . . . 14

3 Сравнения по модулю и классы вычетов **15**
3.1 Сравнения по модулю . . . 15
3.2 Классы вычетов . . . 16
3.3 Обратимые по умножению вычеты . . . 17
3.4 Теорема Эйлера и малая теорема Ферма . . . 18
3.5 Криптографическая система RSA . . . 19
3.6 Цифровая подпись RSA . . . 20

4 Сравнения с одним неизвестным **20**
4.1 Китайская теорема об остатках . . . 20
4.2 Количество решений полиномиального сравнения по простому модулю . . . 22
4.3 Полиномиальные сравнения по модулю, равному степени простого числа . . . 23

5 Квадратичные сравнения **24**
5.1 Символ Лежандра . . . 25
5.2 Символ Якоби . . . 28
5.3 Тест Соловея–Штрассена . . . 31

6 Первообразные корни **33**
6.1 Первообразные корни по простым модулям . . . 34
6.2 Первообразные корни по составным модулям . . . 35
6.3 Протокол Диффи–Хеллмана построения общего ключа шифрования . . . 37
6.4 Криптографическая система Эль-Гамаля . . . 38
6.5 Алгоритм Эль-Гамаля цифровой подписи . . . 39

7 Бесконечные цепные дроби **39**
7.1 Приближение вещественного числа его подходящими дробями . . . 40
7.2 Цепные дроби квадратичных иррациональностей . . . 42

1 Алгоритм Евклида и его применения

1.1 Деление с остатком

Обозначение. Для $a \in \mathbb{Z}$ и $b \in \mathbb{Z}\setminus\{0\}$ свойство *делимости* a на b, то есть существования такого $c \in \mathbb{Z}$, что $a = bc$, записываем как $a \vdots b$ (читается как «a делится на b») или $b \mid a$ (читается как «b делит a»).

Определение 1. Целые числа a и b называются *взаимно простыми*, если у них нет никаких общих натуральных делителей, кроме единицы.

Свойства делимости. Пусть $a, b, c \in \mathbb{Z}$. Тогда

1. $1 \mid a$
2. $a \mid a$ (рефлексивность)
3. $a \mid b,\ b \mid c \implies a \mid c$ (транзитивность)
4. $a \mid b,\ a \mid c \implies a \mid b \pm c$
5. $a \mid b \implies a \mid bc$
6. $a \mid b,\ b \neq 0 \implies |a| \leqslant |b|$

Теорема 1. *Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Тогда существует ровно одна пара целых чисел q и r, такая что*

$$a = qb + r \qquad \text{и} \qquad 0 \leqslant r < b. \tag{1}$$

Доказательство. Рассмотрим множество

$$\{a - bt \mid t \in \mathbb{Z}\}.$$

Это арифметическая прогрессия, бесконечная в обе стороны. Множество её неотрицательных элементов непусто и в нём есть наименьший элемент. Положим

$$q = \max\{t \in \mathbb{Z} \mid a - bt \geqslant 0\} \qquad \text{и} \qquad r = a - bq.$$

Тогда $a = qb + r$, $r \geqslant 0$ и, ввиду максимальности q, $r < b$. Этим доказано существование.

Докажем единственность. Пусть

$$a = q_1 b + r_1 = q_2 b + r_2, \quad q_1, q_2, r_1, r_2 \in \mathbb{Z}, \quad 0 \leqslant r_1 < b, \quad 0 \leqslant r_2 < b.$$

Тогда $(q_1 - q_2)b = r_2 - r_1$, то есть $b \mid r_2 - r_1$. Но $|r_2 - r_1| < b$, откуда ввиду свойства 6 отношения делимости следует, что $r_2 - r_1 = 0$. Стало быть, $r_1 = r_2$ и $q_1 = q_2$. □

Определение 2. Числа q и r из (1) называются соответственно *неполным частным* и *остатком* при делении a на b.

Обозначение.

1. Пусть $a_1, \ldots, a_n \in \mathbb{Z}$, $|a_1| + \ldots + |a_n| \neq 0$. Тогда наибольший общий делитель чисел $a_1, \ldots, a_n$ будем обозначать НОД$(a_1, \ldots, a_n)$ или просто $(a_1, \ldots, a_n)$.

2. Пусть $a_1, \ldots, a_n \in \mathbb{Z}$, $a_1 \cdot \ldots \cdot a_n \neq 0$. Тогда наименьшее общее кратное чисел $a_1, \ldots, a_n$ будем обозначать НОК$(a_1, \ldots, a_n)$ или просто $[a_1, \ldots, a_n]$.

1.2 Алгоритм Евклида

Наибольший общий делитель проще всего вычислять при помощи следующего алгоритма, называемого *алгоритмом Евклида*. Для заданных чисел $a \in \mathbb{Z}$, $b \in \mathbb{N}$ определим последовательность неполных частных $a_0, \ldots, a_n$ и остатков $r_1, \ldots, r_n$ соотношениями

$$\begin{aligned}
&a = a_0 b + r_1, && 0 \leqslant r_1 < b,\\
&b = a_1 r_1 + r_2, && 0 \leqslant r_2 < r_1,\\
&r_1 = a_2 r_2 + r_3, && 0 \leqslant r_3 < r_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-2} = a_{n-1} r_{n-1} + r_n, && 0 \leqslant r_n < r_{n-1},\\
&r_{n-1} = a_n r_n.
\end{aligned} \tag{2}$$

Лемма 1. *Последний ненулевой остаток в алгоритме Евклида для чисел a и b равен (a, b).*

Доказательство. Если целые числа a, b, q, r связаны равенством $a = qb + r$, то множество общих делителей чисел a и b совпадает с множеством общих делителей чисел b и r. В частности, если эти множества конечны (например, это так, если $b \neq 0$), то их максимальные элементы совпадают.

Стало быть, если неполные частные и остатки определяются соотношениями (2), то

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

□

Лемма 2. *Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$ и пусть неполные частные и остатки определяются соотношениями (2). Тогда*

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \ldots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ 0 \end{pmatrix}. \tag{3}$$

Доказательство. Положим $r_0 = b$ и $r_{-1} = a$, а также $r_{n+1} = 0$. Заметим, что для каждого $k = 0, \ldots, n$ справедливо равенство

$$\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}.$$

Отсюда мгновенно следует (3). □

Теорема 2. *Пусть $a, b \in \mathbb{Z}$, $|a| + |b| \neq 0$. Тогда существуют целые числа λ и μ, такие что*

$$(a, b) = \lambda a + \mu b.$$

Доказательство. Пусть $b > 0$ и пусть неполные частные и остатки определяются соотношениями (2). Воспользуемся леммой 2. Домножим равенство (3) на соответствующие обратные матрицы. Получим

$$\begin{pmatrix} 0 & 1 \\ 1 & -a_n \end{pmatrix} \ldots \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_n \\ 0 \end{pmatrix}.$$

Таким образом, существуют целые числа $\lambda, \mu, \nu, \kappa$, такие что

$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda & \mu \\ \nu & \kappa \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{4}$$

В частности, $r_n = \lambda a + \mu b$. Остаётся вспомнить, что $r_n = (a, b)$.

В случае же, когда $b < 0$, по доказанному существуют целые числа λ' и μ', такие что

$$(a, b) = (a, -b) = \lambda' a + \mu'(-b) = \lambda' a - \mu' b.$$

Полагая $\lambda = \lambda'$ и $\mu = -\mu'$, получаем и в этом случае требуемое равенство. □

Замечание. Доказательство теоремы 2 можно проинтерпретировать как «обращение» алгоритма Евклида. То есть r_n представляется в виде линейной комбинации r_{n-1} и r_{n-2}, затем в полученное равенство подставляется представление r_{n-1} в виде линейной комбинации r_{n-2} и r_{n-3} и так далее, пока не дойдём до линейной комбинации чисел r_0 и r_{-1}, которые равны b и a соответственно.

Упражнение. Докажите, что если $(a,b)=1$, то пара чисел ν,κ из (4) совпадает либо с парой $b,-a$, либо с парой $-b,a$.

Следствие (Обобщённая лемма Евклида, она же «Важная лемма»). *Пусть* $a,b,c\in\mathbb{Z}$, $a\mid bc$, $(a,b)=1$. *Тогда* $a\mid c$.

Доказательство. По теореме 2 найдутся целые числа λ и μ, такие что

$$\lambda a+\mu b=1.$$

Домножая обе части на c, получаем

$$\lambda ac+\mu bc=c.$$

Из условия следует, что оба слагаемых в левой части делятся на a. Стало быть, и правая часть делится на a. □

Теорема 3 (Теорема Ламе, 1844). *Пусть* $a,b\in\mathbb{N}$, $a\geqslant b$, $10^{m-1}\leqslant b<10^m$. *Тогда количество делений с остатком в алгоритме Евклида для чисел* a *и* b *не превосходит* $5m$.

Доказательство. Пусть неполные частные и остатки определяются соотношениями (2). Положим, как и прежде, $r_0=b$, $r_{-1}=a$ и $r_{n+1}=0$. Тогда для каждого $k=0,\ldots,n$ имеем

$$r_{k-1}=a_kr_k+r_{k+1},\qquad 0\leqslant r_{k+1}<r_k.$$

Покажем по индукции, что для каждого $k=0,\ldots,n$ справедливо

$$r_{n-k}\geqslant\varphi^k,\tag{5}$$

где $\varphi=\frac{1+\sqrt{5}}{2}$ — золотое сечение. Для $k=0$ имеем $r_n\geqslant 1=\varphi^0$, для $k=1$ имеем $r_{n-1}\geqslant 2>\varphi$. Это даёт нам базу индукции. Возьмём $k\in\mathbb{N}$, $2\leqslant k\leqslant n$. Предположим, что для всех индексов, строго меньших k, неравенство (5) доказано. Тогда

$$r_{n-k}=a_{n-k+1}r_{n-k+1}+r_{n-k+2}\geqslant r_{n-k+1}+r_{n-k+2}\geqslant\varphi^{k-1}+\varphi^{k-2}=\varphi^{k-2}(\varphi+1)=\varphi^{k-2}\varphi^2=\varphi^k.$$

Это даёт нам шаг индукции. В частности, для $k=n$ получаем $r_0\geqslant\varphi^n$ и, поскольку $r_0=b<10^m$, это даёт нам оценку

$$n<m\log_\varphi 10<5m,$$

ибо $\log_\varphi 10=4,78\ldots$. В силу целочисленности n и m получаем $n+1\leqslant 5m$. Остаётся заметить, что количество делений с остатком в алгоритме Евклида для чисел a и b в точности равно $n+1$. □

Замечание. Как нетрудно заметить, проанализировав доказательство неравенства (5), алгоритм Евклида работает «дольше всего», если все неполные частные, кроме последнего, равны 1, а последнее равно 2. То есть в случае, когда a и b суть последовательные числа Фибоначчи.

1.3 Основная теорема арифметики

Определение 3. Пусть $n\in\mathbb{N}$, $n>1$. Если число n имеет только тривиальные делители (тривиальные — это 1 и само n), то n называется *простым*. Если n не простое, то оно называется *составным*.

Замечание. Глубинный смысл того, что 1 не относят ни к простым, ни к составным, заключается в том, что 1 обратимо по умножению.

Лемма 3. *Пусть $n \in \mathbb{N}$, $n > 1$. Пусть p — наименьший делитель n, отличный от 1. Тогда p — простое число.*

Доказательство. Если p — составное, то существует $d \in \mathbb{N}$, такое что $d \mid p$ и $1 < d < p$. Но поскольку $p \mid n$, имеем $d \mid n$ и $1 < d < p$, что противоречит минимальности p. □

Теорема 4 (Теорема Евклида)**.** *Простых чисел бесконечно много.*

Доказательство. Возьмём произвольный набор простых чисел $p_1, \ldots, p_k$. Рассмотрим число

$$N = \prod_{i=1}^{k} p_i + 1.$$

Рассмотрим также p — наименьший делитель N, отличный от 1. По лемме 3 число p является простым. Но $(N, p_i) = 1$ для каждого $i = 1, \ldots, k$. Стало быть, p не равно ни одному из p_i.

Итак, для каждого конечного набора простых чисел мы можем найти простое число, не входящее в этот набор. Следовательно, простых чисел бесконечно много. □

Теорема 5 (Основная теорема арифметики)**.** *Любое натуральное число, большее единицы, однозначно с точностью до перестановки множителей раскладывается в произведение простых.*

Доказательство. Докажем существование по индукции. Для числа 2 всё очевидно, ибо 2 — простое. Это даёт нам базу индукции. Возьмём произвольное $n \in \mathbb{N}$, $n > 2$. Предположим, что для всех чисел, строго меньших n, существование разложения доказано. Если n — простое, разложение получено. Если n — составное, то найдутся $n_1, n_2 \in \mathbb{N}$, такие что $n = n_1 n_2$, $1 < n_1 < n$, $1 < n_2 < n$. По предположению индукции n_1 и n_2 раскладываются в произведение простых. Стало быть, и n раскладывается.

Докажем единственность. Предположим противное. Пусть n — наименьшее натуральное число, допускающее два различных разложения на простые:

$$n = p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_r.$$

Тогда p_1 отлично от каждого q_i, $i = 1, \ldots, r$, ибо иначе на p_1 можно сократить и получить противоречие с минимальностью n. Но тогда $(p, q_i) = 1$, $i = 1, \ldots, r$, откуда по Важной лемме получаем

$$p_1 \mid \prod_{i=1}^{r} q_i \implies p_1 \mid \prod_{i=1}^{r-1} q_i \implies \ldots \implies p_1 \mid q_1 \implies p_1 \mid 1.$$

Но p_1 не делит 1. Получаем противоречие. Стало быть, числа n, допускающего два различных разложения на простые, не существует. □

Определение 4. *Степенью вхождения* простого числа p в натуральное число n называется величина

$$\nu_p(n) = \max\left\{\alpha \in \mathbb{N} \cup \{0\} \,\middle|\, p^\alpha \mid n\right\}.$$

Например, $\nu_2(12) = 2$, $\nu_3(12) = 1$, $\nu_5(12) = 0$.

Из основной теоремы арифметики следует, что каждое натуральное число имеет *каноническое разложение*

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

Здесь произведение берётся по всем простым, делящим n. Отметим, что корректным будет и равенство

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

где произведение берётся по вообще всем простым, ибо в этом произведении лишь конечное количество множителей, отличных от единицы.

Очень полезным бывает следующее наблюдение.

Предложение 1. *Пусть* $a, b \in \mathbb{N}$. *Тогда*

$$a \mid b \iff \nu_p(a) \leqslant \nu_p(b) \text{ для всех простых } p.$$

1.4 Линейные диофантовы уравнения от двух неизвестных

Алгоритм Евклида позволяет также решать *линейные диофантовы уравнения*, то есть решать в целых числах уравнения вида $a_1x_1 + \ldots + a_nx_n = b$ при заданных целых $a_1, \ldots, a_n, b$. В данном параграфе мы рассмотрим самый простой случай — уравнения от двух неизвестных.

Лемма 4. *Пусть* $a, b \in \mathbb{Z}$, $(a, b) = d$. *Тогда общее решение в целых числах уравнения*

$$ax + by = 0 \tag{6}$$

имеет вид

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} b/d \\ -a/d \end{pmatrix} t, \quad t \in \mathbb{Z}.$$

Доказательство. Уравнение (6) равносильно уравнению

$$\frac{a}{d} \cdot x = -\frac{b}{d} \cdot y.$$

Поскольку $(a/d, b/d) = 1$, по Важной лемме x должен делиться на b/d, то есть иметь вид tb/d с некоторым $t \in \mathbb{Z}$. Подставляя $x = tb/d$ и сокращая на b/d, получаем $y = -ta/d$.

Остаётся заметить, что при любом $t \in \mathbb{Z}$ пара чисел $tb/d, -ta/d$ удовлетворяет соотношению (6). □

Теорема 6. *Пусть* $a, b, c \in \mathbb{Z}$, $(a, b) = d$. *Рассмотрим уравнение*

$$ax + by = c. \tag{7}$$

Тогда

а) уравнение (7) *разрешимо в целых числах тогда и только тогда, когда* $d \mid c$;

б) если пара чисел x_0, y_0 *удовлетворяет равенству* (7) *(т.е. является частным решением), то общее решение в целых числах уравнения* (7) *имеет вид*

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \begin{pmatrix} b/d \\ -a/d \end{pmatrix} t, \quad t \in \mathbb{Z}.$$

Доказательство. Если $d \nmid c$, то при любых целых x и y левая часть (7) делится на d, а правая — нет. Стало быть, условие $d \mid c$ является необходимым для разрешимости в $\mathbb{Z}$. Если же $d \mid c$, то поскольку по теореме 2 существуют целые λ и μ, такие что $\lambda a + \mu b = d$, в качестве частного решения уравнения (7) можно взять числа $x_0 = c\lambda/d$, $y_0 = c\mu/d$.

Таким образом, действительно, условие $d \mid c$ является критерием разрешимости уравнения (7) в $\mathbb{Z}$.

Далее, если наряду с x_0, y_0 имеется другое частное решение x_1, y_1, то их покомпонентная разность $x_0 - x_1, y_0 - y_1$ является решением уравнения (6). Это уравнение называется *присоединённым однородным* уравнением.

И обратно, если пара x', y' является частным решением однородного уравнения (6), то пара $x_0 + x', y_0 + y'$ является частным решением уравнения (7).

Итак, прибавив произвольное частное решение уравнения (7) к общему решению однородного уравнения (6), мы получаем общее решение уравнения (7). □

1.5 Конечные цепные дроби

Как мы увидели, однородное уравнение (6) решается совсем просто. И решение уравнения (7) сводится к поиску какого-нибудь частного решения. Один из наиболее простых способов поиска частного решения предоставляется аппаратом цепных дробей.

Рассмотрим соотношения (2), описывающие алгоритм Евклида. Поделим первое соотношение (2) на b, второе — на r_1, третье — на r_2 и так далее. Подставляя каждое следующее из полученных соотношений в предыдущее, получим

$$\frac{a}{b} = a_0 + \frac{1}{b/r_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{r_1/r_2}} = \ldots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

Такие многоэтажные дроби называются *цепными дробями*. Используется также более компактная запись:

$$\frac{a}{b} = [a_0; a_1, a_2, \ldots, a_n].$$

Определение 5. Пусть $a/b = [a_0; a_1, a_2, \ldots, a_n]$. Тогда для каждого $k = 0, \ldots, n$ рациональное число

$$\frac{p_k}{q_k} = [a_0; a_1, a_2, \ldots, a_k]$$

называется *подходящей дробью* числа a/b. При этом p_k и q_k полагаются взаимно простыми, а q_k — положительным.

Лемма 5. *Для подходящих дробей p_k/q_k, p_{k-1}/q_{k-1} цепной дроби $[a_0; a_1, a_2, \ldots]$ справедливо равенство*

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}. \tag{8}$$

Доказательство. Поскольку для каждого k справедливо $(p_k, q_k) = 1$, по лемме 2 имеем

$$\begin{pmatrix} p_k \\ q_k \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad k = 0, 1, 2, \ldots. \tag{9}$$

Отсюда следует, что

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} p_{k-1} \\ q_{k-1} \end{pmatrix}, \quad k = 1, 2, \ldots. \tag{10}$$

Собирая вместе (9) и (10), получаем

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Удаляя в правой части единичную матрицу, приходим к соотношению (8). □

Упражнение. Докажите при помощи соотношения (8) равенство

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0].$$

Теорема 7. *Пусть задана последовательность неполных частных $a_0, a_1, a_2, \ldots$ и соответствующая последовательность подходящих дробей p_k/q_k, $k = 0, 1, 2, \ldots$. Положим*

$$\begin{aligned} p_{-2} &= 0, \qquad p_{-1} = 1, \\ q_{-2} &= 1, \qquad q_{-1} = 0. \end{aligned}$$

Тогда для любого $k = 0, 1, 2, \ldots$ выполняются соотношения

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2}, \\ q_k &= a_k q_{k-1} + q_{k-2}. \end{aligned} \tag{11}$$

Доказательство. Из леммы 5 следует, что для каждого $k = 0, 1, 2, \ldots$ справедливо

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Сравнивая первые столбцы обеих частей этого равенства, получаем (11). □

Следствие. *В обозначениях теоремы 7 справедливо соотношение*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Доказательство.

$$\begin{aligned} p_k q_{k-1} - p_{k-1} q_k = \begin{vmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{vmatrix} = \begin{vmatrix} p_k - a_k p_{k-1} & p_{k-1} \\ q_k - a_k q_{k-1} & q_{k-1} \end{vmatrix} = \begin{vmatrix} p_{k-2} & p_{k-1} \\ q_{k-2} & q_{k-1} \end{vmatrix} = \\ = - \begin{vmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{vmatrix} = \ldots = (-1)^{k+1} \begin{vmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{vmatrix} = (-1)^{k-1}. \end{aligned}$$

□

Предложение 2. *Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $(a, b) = 1$ и пусть $a/b = [a_0; a_1, a_2, \ldots, a_n]$. Рассмотрим предпоследнюю подходящую дробь $p_{n-1}/q_{n-1} = [a_0; a_1, a_2, \ldots, a_{n-1}]$ числа a/b. Тогда пара чисел*

$$(-1)^{n-1} q_{n-1}, \ (-1)^n p_{n-1}$$

является частным решением диофантова уравнения $ax + by = 1$.

Доказательство. По следствию из теоремы 7

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}.$$

Но $(a, b) = 1$ и $b > 0$. Стало быть, $p_n = a$ и $q_n = b$, откуда

$$(-1)^{n-1} \big(a q_{n-1} - b p_{n-1} \big) = 1.$$

□

Замечание. Предложение 2 даёт альтернативное доказательство теоремы 2 о представлении наибольшего общего делителя в виде линейной комбинации. В частности, мы получили ещё один способ доказательства Важной леммы.

1.6 Линейные диофантовы уравнения от произвольного количества неизвестных

Пусть $a_1, \ldots, a_n, b \in \mathbb{Z}$. Рассмотрим упоминавшееся выше линейное уравнение

$$a_1 x_1 + \ldots + a_n x_n = b. \tag{12}$$

Очевидно, что условие

$$(a_1, \ldots, a_n) \mid b \tag{13}$$

является необходимым для разрешимости этого уравнения в целых числах. С другой стороны, зная, как находить представление наибольшего общего делителя двух чисел в виде их линейной комбинации с целыми коэффициентами, несложно понять, как находить аналогичное представление наибольшего общего делителя произвольного набора целых чисел. Таким образом, при выполнении условия (13) частное решение в целых числах уравнения (12) найти достаточно легко. Однако найти общее решение соответствующего однородного уравнения при $n \geqslant 3$ заметно сложнее, чем при $n = 2$ (см. лемму 4 и её доказательство).

Опишем алгоритм решения уравнения (12) в целых числах. В сущности этот алгоритм также базируется на алгоритме Евклида.

Определение 6. Пусть дана матрица с целыми коэффициентами. *Элементарными целочисленными преобразованиями* столбцов этой матрицы называются

(1) перемена двух столбцов местами;

(2) умножение некоторого столбца на -1;

(3) добавление к некоторому столбцу другого, умноженного на целое число.

Замечание. Когда в курсе алгебры обсуждают элементарные преобразования строк матрицы системы линейных уравнений с вещественными коэффициентами, умножение строки допускается на любое ненулевое вещественное число, а прибавлять к строке можно любую другую строку, умноженную на любое вещественное число. Эти операции *обратимы над* $\mathbb{R}$. В нашем же случае коэффициенты обязаны быть целыми числами, а преобразования должны быть *обратимыми над* $\mathbb{Z}$ — отсюда отличие в пунктах (2) и (3).

Определение 7. Пусть A и B — матрицы одинакового размера с целочисленными коэффициентами. Будем говорить, что A эквивалентна B и писать $A \sim B$, если B получается из A при помощи конечного количества элементарных целочисленных преобразований столбцов.

Будем обозначать n-мерные векторы жирным шрифтом и записывать их как столбцы. К примеру, будем писать

$$\mathbf{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \qquad \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Здесь $\mathbf{a}$ — вектор коэффициентов уравнения (12), $\mathbf{x}$ — переменный вектор. Будем также использовать обозначение $\langle \cdot, \cdot \rangle$ для скалярного произведения в $\mathbb{R}^n$. Тогда уравнение (12) переписывается как

$$\langle \mathbf{a}, \mathbf{x} \rangle = b.$$

Наконец, будем обозначать через $\mathbf{e}_1, \ldots, \mathbf{e}_n$ векторы стандартного единичного базиса пространства $\mathbb{R}^n$.

Теорема 8. *Пусть* $a_1, \ldots, a_n, b \in \mathbb{Z}$ *и пусть* $(a_1, \ldots, a_n) = d$, $d \mid b$. *Положим*

$$A = \begin{pmatrix} a_1 & \cdots & a_n \\ \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}.$$

То есть матрица A *образуется приписыванием единичной матрицы* $n \times n$ *снизу к строчке из коэффициентов* $a_1, \ldots, a_n$. *Тогда*

(1) *найдётся матрица* W, *такая что* $W \sim A$ *и*

$$W = \begin{pmatrix} d & 0 & \cdots & 0 \\ \mathbf{w}_1 & \mathbf{w}_2 & \cdots & \mathbf{w}_n \end{pmatrix};$$

(2) *условие на* $\mathbf{x} \in \mathbb{Z}^n$, *задаваемое уравнением* (12), *то есть уравнение* $\langle \mathbf{a}, \mathbf{x} \rangle = b$, *равносильно явному представлению*

$$\mathbf{x} = \frac{b}{d}\mathbf{w}_1 + \sum_{i=2}^{n} t_i \mathbf{w}_i, \qquad t_2, \ldots, t_n \in \mathbb{Z}.$$

Здесь коэффициенты $t_2, \ldots, t_n$ *могут независимо друг от друга принимать произвольные целые значения.*

Для доказательства теоремы 8 нам понадобятся два важных наблюдения, касающихся свойств и соотношений, сохраняющихся при элементарных целочисленных преобразованиях столбцов.

Определение 8. Множество $\mathbb{Z}^n$, то есть множество всех точек пространства $\mathbb{R}^n$ с целыми координатами, называется *целочисленной решёткой.*

Определение 9. Набор векторов $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^n$ называется *базисом* решётки $\mathbb{Z}^n$, если каждый вектор из $\mathbb{Z}^n$ представим в виде линейной комбинации векторов $\mathbf{v}_1, \ldots, \mathbf{v}_n$ с целыми коэффициентами, то есть если $\mathbb{Z}^n = \mathbb{Z}\mathbf{v}_1 + \ldots + \mathbb{Z}\mathbf{v}_n$.

Замечание. Любые n линейно независимых векторов в $\mathbb{R}^n$ образуют базис пространства $\mathbb{R}^n$. Для решётки $\mathbb{Z}^n$ аналогичное утверждение не верно. Например, набор из n линейно независимых векторов с чётными координатами не является базисом $\mathbb{Z}^n$, ибо никакая их линейная комбинация с целыми коэффициентами не даст вектор с нечётными координатами.

Упражнение. Докажите, что векторы $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^n$ образуют базис решётки $\mathbb{Z}^n$ тогда и только тогда, когда определитель матрицы $\begin{pmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{pmatrix}$ равен 1 или -1.

Лемма 6. *Пусть* $V = \begin{pmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{pmatrix}$ *и* $U = \begin{pmatrix} \mathbf{u}_1 & \cdots & \mathbf{u}_n \end{pmatrix}$ — *матрицы* $n \times n$ *с целыми коэффициентами. Пусть* $V \sim U$ *и пусть векторы* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *образуют базис решётки* $\mathbb{Z}^n$. *Тогда векторы* $\mathbf{u}_1, \ldots, \mathbf{u}_n$ *также образуют базис этой решётки.*

Доказательство. Понятно, что элементарные целочисленные преобразования вида (1) и (2) сохраняют свойство столбцов быть базисом $\mathbb{Z}^n$. Покажем, что и преобразование вида (3) сохраняет это свойство. Достаточно рассмотреть случай, когда $\mathbf{u}_1 = \mathbf{v}_1 + q\mathbf{v}_2$, $\mathbf{u}_i = \mathbf{v}_i$, $i = 2, \ldots, n$. В этом случае для любого $\mathbf{v} \in \mathbb{Z}^n$ справедливо

$$\mathbf{v} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \iff \mathbf{v} = \lambda_1 \mathbf{u}_1 + (\lambda_2 - \lambda_1 q)\mathbf{u}_2 + \sum_{i=3}^{n} \lambda_i \mathbf{u}_i,$$

откуда следует, что векторы $\mathbf{u}_1, \ldots, \mathbf{u}_n$, действительно, образуют базис решётки $\mathbb{Z}^n$. $\square$

Лемма 7. *Пусть вектор* $\mathbf{a}$ *и матрица* A *— как в формулировке теоремы 8. Пусть* $B \sim A$,

$$B = \begin{pmatrix} b_1 & \cdots & b_n \\ \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{pmatrix}.$$

Тогда справедливы равенства

$$b_i = \langle \mathbf{a}, \mathbf{v}_i \rangle \qquad i = 1, \ldots, n. \tag{14}$$

Доказательство. Рассмотрим произвольную матрицу C, такую что

$$C = \begin{pmatrix} c_1 & \cdots & c_n \\ \mathbf{u}_1 & \cdots & \mathbf{u}_n \end{pmatrix}$$

и для каждого $i = 1, \ldots, n$ справедливо $c_i = \langle \mathbf{a}, \mathbf{u}_i \rangle$. Достаточно показать, что если

$$\begin{array}{llll} b_1 = c_1 + qc_2, & b_i = c_i, & i = 2, \ldots, n, \\ \mathbf{v}_1 = \mathbf{u}_1 + q\mathbf{u}_2, & \mathbf{v}_i = \mathbf{u}_i, & i = 2, \ldots, n, \end{array} \tag{15}$$

то выполняется (14). Действительно, из (15) следует, что

$$b_1 = c_1 + qc_2 = \langle \mathbf{a}, \mathbf{u}_1 \rangle + q\langle \mathbf{a}, \mathbf{u}_2 \rangle = \langle \mathbf{a}, \mathbf{u}_1 + q\mathbf{u}_2 \rangle = \langle \mathbf{a}, \mathbf{v}_1 \rangle$$

и

$$b_i = c_i = \langle \mathbf{a}, \mathbf{u}_i \rangle = \langle \mathbf{a}, \mathbf{v}_i \rangle$$

при $i = 2, \ldots, n$. Таким образом, равенства (14) имеют место. □

Доказательство теоремы 8. Ввиду возможности применять элементарные целочисленные преобразования вида (1) и (2) (см. определение 6) можно считать, что все a_i неотрицательны и что a_1 — наименьшее из всех ненулевых a_i. Пусть $a_k > 0$ для какого-нибудь $k > 1$. Вычтем из столбца с номером k первый столбец и, если выполнялось условие $0 < a_k - a_1 < a_1$, поменяем полученный k-й столбец с первым столбцом местами. Эта процедура уменьшает сумму чисел в первой строке и сохраняет их наибольший общий делитель. При этом после её выполнения первый элемент первой строки снова будет наименьшим из всех ненулевых элементов этой строки. Будем повторять эту процедуру, пока возможно — то есть пока в первой строке остаются хотя бы два положительных числа. Поскольку уменьшающаяся сумма является числом натуральным, через конечное количество итераций возможность повторить описанную процедуру пропадёт, то есть во всех столбцах, кроме первого, верхние элементы будут равны нулю, а в первом столбце верхний элемент будет равен d. Этим доказано утверждение (1) теоремы.

Далее, из леммы 6 следует, что векторы $\mathbf{w}_1, \ldots, \mathbf{w}_n$ образуют базис решётки $\mathbb{Z}^n$. Тогда для произвольного вектора $\mathbf{w}$ из $\mathbb{Z}^n$ имеет место представление

$$\mathbf{w} = \sum_{i=1}^{n} t_i \mathbf{w}_i, \qquad t_1, \ldots, t_n \in \mathbb{Z}.$$

Учитывая лемму 7, получаем

$$\langle \mathbf{a}, \mathbf{w} \rangle = t_1 d,$$

откуда следует, что равенство $\langle \mathbf{a}, \mathbf{w} \rangle = b$ равносильно тому, что $t_1 = b/d$. Остальные коэффициенты $t_2, \ldots, t_n$ могут принимать произвольные целые значения, что доказывает утверждение (2) теоремы. □

Отметим, что первый абзац доказательства теоремы 8 фактически описывает алгоритм построения матрицы W, то есть алгоритм решения диофантова уравнения (12).

2 Арифметические функции

Определение 10. Отображение из $\mathbb{N}$ в $\mathbb{C}$ называется *арифметической функцией*.

Определение 11. Арифметическая функция f, отличная от тождественного нуля, называется *мультипликативной*, если для любых $a, b \in \mathbb{N}$, таких что $(a, b) = 1$, справедливо $f(ab) = f(a)f(b)$.

Определение 12. Арифметическая функция f, отличная от тождественного нуля, называется *вполне мультипликативной*, если для любых $a, b \in \mathbb{N}$ справедливо $f(ab) = f(a)f(b)$.

Лемма 8. *Если f — мультипликативная функция, то $f(1) = 1$.*

Доказательство. В силу мультипликативности $f(1) = f(1^2) = f(1)^2$, то есть

$$f(1)\big(f(1) - 1\big) = 0,$$

откуда либо $f(1) = 0$, либо $f(1) = 1$. Но если $f(1) = 0$, то для любого $n \in \mathbb{N}$ будет справедливо $f(n) = f(n \cdot 1) = f(n)f(1) = 0$, что противоречит тому, что f не равна тождественно нулю. Стало быть, $f(1) = 1$. □

2.1 Формула обращения Мёбиуса

Лемма 9. *Пусть f и g — мультипликативные функции. Тогда функция h, определяемая равенством*

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

также мультипликативна.

Доказательство. Пусть $(a, b) = 1$. Тогда для любого делителя d числа ab существует единственное разложение $d = d_1 d_2$, такое что $d_1 \mid a$ и $d_2 \mid b$. При этом $(d_1, d_2) = 1$ и $(a/d_1, b/d_2) = 1$. Стало быть,

$$h(ab) = \sum_{d|ab} f(d)g(ab/d) = \sum_{d_1|a}\sum_{d_2|b} f(d_1 d_2)g(ab/d_1 d_2) =$$

$$= \sum_{d_1|a}\sum_{d_2|b} f(d_1)f(d_2)g(a/d_1)g(b/d_2) = \left(\sum_{d_1|a} f(d_1)g(a/d_1)\right)\left(\sum_{d_2|b} f(d_2)g(b/d_2)\right) = h(a)h(b).$$

□

Следствие. *Пусть f — мультипликативная функция. Тогда функция h, определяемая равенством*

$$h(n) = \sum_{d|n} f(d),$$

также мультипликативна и

$$h(n) = \prod_{p|n}\Big(1 + f(p) + f(p^2) + \ldots + f\big(p^{\nu_p(n)}\big)\Big), \tag{16}$$

где произведение берётся по всем простым делителям числа n.

Доказательство. Для доказательства мультипликативности достаточно взять $g(n) = 1$ — тождественную единицу. Раскрывая скобки в правой части (16) и пользуясь мультипликативностью, получаем сумму по всем делителям. Действительно, если каноническое разложение числа n имеет вид

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

то

$$\prod_{p|n}\Big(1+f(p)+f(p^2)+\ldots+f\big(p^{\nu_p(n)}\big)\Big)=\prod_{i=1}^{k}\Big(f(p_i^0)+f(p_i^1)+f(p_i^2)+\ldots+f\big(p_i^{\alpha_i}\big)\Big)=$$

$$=\sum_{\substack{0\leqslant\beta_1\leqslant\alpha_1\\ \ldots\ldots\ldots\\ 0\leqslant\beta_k\leqslant\alpha_k}} f(p_1^{\beta_1})\cdot\ldots\cdot f(p_k^{\beta_k})=\sum_{\substack{0\leqslant\beta_1\leqslant\alpha_1\\ \ldots\ldots\ldots\\ 0\leqslant\beta_k\leqslant\alpha_k}} f(p_1^{\beta_1}\cdot\ldots\cdot p_k^{\beta_k})=\sum_{d|n} f(d).$$

□

Определение 13. Функция

$$\mu(n)=\begin{cases}1, & \text{если } n=1\\ 0, & \text{если для некоторого простого } p \text{ справедливо } p^2\mid n\\ (-1)^k, & \text{если } n=p_1\cdot\ldots\cdot p_k,\quad p_i\neq p_j \text{ при } i\neq j\end{cases}$$

называется *функцией Мёбиуса*.

Теорема 9. *[Формула обращения Мёбиуса] Пусть f — произвольная арифметическая функция и*

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

Тогда

$$f(n)=\sum_{d|n} h(d)\mu(n/d).$$

Лемма 10. *Справедливо равенство*

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

Доказательство. При $n=1$ утверждение очевидно. При $n>1$ по следствию из леммы 9 ввиду мультипликативности функции Мёбиуса имеем

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

□

Доказательство теоремы 9. При $n=1$ утверждение очевидно. Пусть $n>1$. Тогда

$$\sum_{d|n} h(d)\mu(n/d)=\sum_{\substack{c,d\in\mathbb{N}\\ cd=n}} h(d)\mu(c)=\sum_{\substack{c,d\in\mathbb{N}\\ cd=n}}\Big(\sum_{a|d} f(a)\Big)\mu(c)=\sum_{\substack{c,d\in\mathbb{N}\\ cd=n}}\Big(\sum_{\substack{a,b\in\mathbb{N}\\ ab=d}} f(a)\Big)\mu(c)=$$

$$=\sum_{\substack{a,b,c\in\mathbb{N}\\ abc=n}} f(a)\mu(c)=\sum_{a|n} f(a)\Big(\sum_{\substack{b,c\in\mathbb{N}\\ bc=\frac{n}{a}}}\mu(c)\Big)=\sum_{a|n} f(a)\Big(\sum_{c|\frac{n}{a}}\mu(c)\Big)=f(n).$$

По лемме 10 при $a\mid n$ имеем

$$\sum_{c|\frac{n}{a}}\mu(c)=\begin{cases}1, & \text{если } a=n\\ 0, & \text{если } a<n\end{cases}.$$

Стало быть, $\sum_{d|n} h(d)\mu(n/d)=f(n)$. □

Следствие. *Пусть f и h — арифметические функции, связанные соотношением*

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

Тогда функция f мультипликативна в том и только том случае, когда мультипликативна функция h.

2.2 Функция Эйлера

Доказательство. Если функция f мультипликативна, то по следствию из леммы 9 мультипликативна и функция h. Если же функция h мультипликативна, то ввиду мультипликативности функции Мёбиуса из теоремы 9 и леммы 9 следует мультипликативность функции f. □

Определение 14. Для каждого $n \in \mathbb{N}$ положим $\varphi(n)$ равным количеству натуральных чисел, не превосходящих n и взаимно простых с n. Функция φ называется *функцией Эйлера*.

Теорема 10. *Функция Эйлера мультипликативна и*

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

где произведение берётся по всем простым делителям числа n.

Лемма 11. *Справедливо равенство*

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

Доказательство. Рассмотрим множество дробей

$$\mathcal{M} = \left\{ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n} \right\}.$$

После приведения к несократимому виду знаменатель каждой дроби из $\mathcal{M}$ становится каким-то делителем n. Соответственно, для каждого $d \mid n$ можно определить множество

$$\mathcal{M}_d = \left\{ \frac{k}{d} \;\middle|\; 1 \leqslant k \leqslant d,\ (k,d) = 1 \right\}.$$

Эти множества попарно не пересекаются, стало быть,

$$\mathcal{M} = \bigsqcup_{d|n} \mathcal{M}_d \qquad \text{и} \qquad |\mathcal{M}| = \sum_{d|n} |\mathcal{M}_d|.$$

Здесь символ «$\sqcup$» означает дизъюнктное объединение. Остаётся заметить, что $|\mathcal{M}| = n$ и $|\mathcal{M}_d| = \varphi(d)$. □

Доказательство теоремы 10. Тождественная функция $f(n) = n$ мультипликативна, стало быть, по лемме 11 и следствию из теоремы 9 функция φ также мультипликативна. Заметим, что при простом p и натуральном k целое число a взаимно просто с p^k тогда и только тогда, когда $p \nmid a$. Натуральных же чисел, не превосходящих p^k и делящихся на p, ровно p^{k-1}. Стало быть, $\varphi(p^k) = p^k - p^{k-1}$. Пользуясь мультипликативностью, получаем

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

□

Замечание. Для вычисления значений функции Эйлера удобнее пользоваться формулой

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

Упражнение. Докажите, что для любых $a, b \in \mathbb{N}$ справедливо равенство

$$\varphi(ab) = \varphi(a)\varphi(b)\frac{(a,b)}{\varphi\big((a,b)\big)}.$$

3 Сравнения по модулю и классы вычетов

3.1 Сравнения по модулю

Зафиксируем натуральное число m, $m \geqslant 2$. Будем называть его *модулем*.

Определение 15. Пусть $a, b \in \mathbb{Z}$. Говорят, что a *и* b *сравнимы по модулю* m, если $a - b$ делится на m. В случае сравнимости a и b по модулю m пишут $a \equiv b \pmod{m}$.

Отношение сравнимости по модулю является *отношением эквивалентности*, ибо оно *рефлексивно*, то есть

$$a \equiv a \pmod{m},$$

симметрично, то есть

$$a \equiv b \pmod{m} \implies b \equiv a \pmod{m},$$

и *транзитивно*, то есть

$$\begin{array}{l} a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{array} \implies a \equiv c \pmod{m}.$$

Со сравнениями можно работать, как с равенствами: их можно складывать и перемножать.

Лемма 12. *Пусть*

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

Тогда

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

Доказательство. Предположение леммы в точности означает, что

$$m \mid a - b \quad \text{и} \quad m \mid c - d.$$

Стало быть, по свойствам делимости

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

откуда мгновенно следует утверждение леммы. □

Следствие. *Пусть* $f(x) \in \mathbb{Z}[x]$. *Тогда*

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

Сравнения также можно сокращать на общий делитель. Но делать это нужно аккуратно: большую роль играет наличие (или отсутствие) взаимной простоты общего делителя с модулем.

Лемма 13. *Пусть* $(a, m) = 1$. *Тогда*

$$ab \equiv ac \pmod{m} \iff b \equiv c \pmod{m}.$$

Доказательство. Если $m \mid b - c$, то $m \mid ab - ac$. Обратно, если $m \mid a(b - c)$ и $(a, m) = 1$, то по Важной лемме $m \mid b - c$. □

Лемма 14. *Пусть a — произвольное натуральное число. Тогда*

$$ab \equiv ac \pmod{am} \iff b \equiv c \pmod{m}.$$

Доказательство. Достаточно заметить, что $am \mid a(b-c) \iff m \mid b-c$. □

Полезно также понимать, что сравнимые по модулю m числа имеют один и тот же наибольший общий делитель с m.

Лемма 15. *Если $a \equiv b \pmod{m}$, то $(a, m) = (b, m)$.*

Доказательство. Достаточно заметить, что множество общих делителей a и m совпадает с множеством общих делителей b и m. □

3.2 Классы вычетов

Определение 16. Пусть задан модуль m. Тогда для $a \in \mathbb{Z}$ множество

$$\overline{a} = a + m\mathbb{Z} = \left\{a + mt \,\middle|\, t \in \mathbb{Z}\right\}$$

называется *классом вычетов* числа a по модулю m.

Замечание. Сам термин *вычет* нужно понимать следующим образом. *Вычет* — это *элемент класса вычетов*. То есть вычетами называются обыкновенные целые числа *в контексте наличия модуля*. Например, -33, 7 и 117 — вычеты по модулю 10, принадлежащие одному классу вычетов.

Всего при заданном модуле m имеется ровно m классов вычетов. Каждый из них представляет из себя бесконечную в обе стороны арифметическую прогрессию с разностью m. Получаем следующее разбиение $\mathbb{Z}$:

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

Обозначение. Множество всех классов вычетов по модулю m обозначается $\mathbb{Z}_m$.

Таким образом,

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

Определим на множестве $\mathbb{Z}_m$ арифметические операции: «+», «−», «$\cdot$». Для каждых $a, b \in \mathbb{Z}$ положим, при заданном модуле m

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} - \overline{b} = \overline{a-b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$$

Отметим, что использование обозначения $\overline{a}$ «навязывает» выбор представителя этого класса, а именно, числа a. При этом $a + m$ — столь же равноправный представитель этого же класса вычетов. Поэтому необходимо доказывать корректность данного выше определения арифметических операций.

Лемма 16. *Арифметические операции на $\mathbb{Z}_m$ определены корректно. То есть для любых $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, таких что $a_1 \equiv a_2 \pmod{m}$ и $b_1 \equiv b_2 \pmod{m}$, справедливо*

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

Доказательство. По лемме 12 из условий $a_1 \equiv a_2 \pmod{m}$ и $b_1 \equiv b_2 \pmod{m}$ следует, что

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

Что доказывает требуемое утверждение. □

Упражнение. Докажите, что введённые на $\mathbb{Z}_m$ операции сложения и умножения ассоциативны и выполняется закон дистрибутивности.

3.3 Обратимые по умножению вычеты

Как мы увидели, элементы $\mathbb{Z}_m$ можно складывать, вычитать и умножать. На некоторые элементы $\mathbb{Z}_m$ можно ещё и делить.

Лемма 17. *Пусть задан модуль m и пусть a — целое число. Тогда сравнение*

$$ax \equiv 1 \pmod{m} \tag{17}$$

разрешимо относительно x тогда и только тогда, когда $(a, m) = 1$.

Иными словами, условие $(a, m) = 1$ является критерием разрешимости в $\mathbb{Z}_m$ уравнения

$$\overline{a} \cdot \overline{x} = \overline{1}$$

относительно $\overline{x}$.

Доказательство. Разрешимость сравнения (17) равносильна разрешимости линейного диофантова уравнения

$$ax + my = 1.$$

А это уравнение разрешимо ввиду теоремы 6 условию $(a, m) = 1$. □

Определение 17. Вычеты, для которых сравнение (17) разрешимо, называются *обратимыми по умножению* по модулю m.

По лемме 15 вычеты, принадлежащие одному и тому же классу, одновременно обратимы или нет.

Обозначение. Множество всех классов вычетов, обратимых по модулю m, обозначается $\mathbb{Z}_m^*$.

Таким образом,

$$\mathbb{Z}_m^* = \left\{ \overline{a} \in \mathbb{Z}_m \,\middle|\, (a, m) = 1 \right\}.$$

Нетрудно заметить, что количество элементов в $\mathbb{Z}_m^*$ в точности равно $\varphi(m)$.

Теорема 11 (Теорема Вильсона)**.** *Пусть p — простое число. Тогда*

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. Отметим сразу, что для $p = 2$ утверждение теоремы очевидно. Пусть далее $p > 2$.

Для каждого $a \in \{1, \ldots, p-1\}$ по лемме 17 найдётся $b \in \{1, \ldots, p-1\}$, такое что $ab \equiv 1 \pmod{p}$. При этом такое b для заданного a будет определяться однозначно. Действительно, если $ab_1 \equiv ab_2 \pmod{p}$, то $p \mid a(b_1 - b_2)$ и по Важной лемме $p \mid b_1 - b_2$, то есть $b_1 \equiv b_2 \pmod{p}$, откуда $b_1 = b_2$.

Таким образом, все вычеты из набора $\{1, \ldots, p-1\}$ разобьются на пары взаимно обратных вычетов, кроме тех, для которых обратный совпадает с ним самим. Но

$$a^2 \equiv 1 \pmod{p} \iff p \mid (a-1)(a+1) \iff \left[\begin{array}{l} a \equiv 1 \pmod{p} \\ a \equiv -1 \pmod{p} \end{array} \right. .$$

Стало быть, «без пары» среди чисел $\{1, \ldots, p-1\}$ остаются только 1 и -1. Отсюда сразу следует, что $(p-1)! \equiv -1 \pmod{p}$. □

3.4 Теорема Эйлера и малая теорема Ферма

Определение 18. Произвольная система представителей всех m классов вычетов из $\mathbb{Z}_m$ (из каждого класса берётся ровно один представитель) называется *полной системой вычетов по модулю m*.

Определение 19. Произвольная система представителей всех $\varphi(m)$ классов вычетов из $\mathbb{Z}_m^*$ (из каждого класса берётся ровно один представитель) называется *приведённой системой вычетов по модулю m*.

Замечание. Обратите внимание, что полная или приведённая системы вычетов — это наборы целых чисел, а не наборы элементов $\mathbb{Z}_m$. Например, полной системой вычетов по модулю 3 будет как набор $\{0, 1, 2\}$, так и набор $\{-1, 0, 1\}$. Равно как и набор $\{-33, 7, 17\}$, ибо $-33 \in \overline{0}$, $7 \in \overline{1}$, $17 \in \overline{2}$.

Теорема 12 (о полной и приведённой системах вычетов)**.** *Пусть задан модуль m, целое число a, такое что $(a, m) = 1$, и произвольное целое число c.*

(1) *Пусть $b_1, \ldots, b_m$ — произвольная полная система вычетов по модулю m. Тогда числа $ab_1 + c, \ldots, ab_m + c$ также образуют полную систему вычетов по модулю m.*

(2) *Пусть $b_1, \ldots, b_{\varphi(m)}$ — произвольная приведённая система вычетов по модулю m. Тогда числа $ab_1, \ldots, ab_{\varphi(m)}$ также образуют приведённую систему вычетов по модулю m.*

Доказательство. (1) Рассмотрим два произвольных индекса i, j и предположим, что

$$ab_i + c \equiv ab_j + c \pmod{m}.$$

Тогда $m \mid a(b_i - b_j)$ и, поскольку $(a, m) = 1$, по Важной лемме $m \mid b_i - b_j$, то есть $b_i \equiv b_j \pmod{m}$. Таким образом, при $i \neq j$ справедливо

$$ab_i + c \not\equiv ab_j + c \pmod{m}.$$

Следовательно, числа $ab_1 + c, \ldots, ab_m + c$ являются представителями всех m классов вычетов и, стало быть, образуют полную систему вычетов по модулю m.

(2) Рассуждение из пункта (1) при $c = 0$ доказывает, что и в контексте пункта (2) при $i \neq j$ справедливо

$$ab_i \not\equiv ab_j \pmod{m}.$$

Следовательно, числа $ab_1, \ldots, ab_{\varphi(m)}$ являются представителями $\varphi(m)$ попарно различных классов вычетов. Остаётся заметить, что каждое их чисел ab_i взаимно просто с m, ибо в контексте пункта (2) справедливо не только $(a, m) = 1$, но и $(b_i, m) = 1$. □

Теорема 13 (Теорема Эйлера)**.** *Пусть задан модуль m. Пусть $a \in \mathbb{Z}$, $(a, m) = 1$. Тогда*

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

Доказательство. Рассмотрим произвольную приведённую систему вычетов $b_1, \ldots, b_{\varphi(m)}$ по модулю m. Домножим все её элементы на a. Тогда по теореме 12 числа $ab_1, \ldots, ab_{\varphi(m)}$ также образуют приведённую систему вычетов. Следовательно,

$$ab_1 \cdot \ldots \cdot ab_{\varphi(m)} \equiv b_1 \cdot \ldots \cdot b_{\varphi(m)} \pmod{m}.$$

Поскольку все b_i взаимно просты с m, и всё произведение $b_1 \cdot \ldots \cdot b_{\varphi(m)}$ взаимно просто с m. Стало быть, по лемме 13 на это произведение можно левую и правую части сравнения сократить. Получаем $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Теорема 14 (Малая теорема Ферма)**.** *Пусть p — простое число, $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$. Тогда*

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

Доказательство. Достаточно применить теорему Эйлера при $m = p$ и заметить, что для простого p справедливо $\varphi(p) = p - 1$. □

3.5 Криптографическая система RSA

Долгое время теория чисел оставалась одной из наиболее абстрактных областей математики. Однако за последние десятилетия она стала одной из наиболее востребованных для практических приложений областей. В основном эти приложения имеют криптографический характер.

Пусть $x \in \mathbb{N}$ — число, которое абонент $\mathcal{B}$ хочет передать абоненту $\mathcal{A}$ по открытым каналам, не имея возможности предварительно договориться в тайне от всех о некоем шифре. Оказывается, на практике эта задача может быть успешно решена при помощи того факта, что некоторые вычислительные процедуры в одну сторону выполняются достаточно быстро, а в обратную — слишком долго. Эти процедуры называются *односторонними*. Например, если есть два больших простых числа p и q, их произведение $n = pq$ можно вычислить достаточно быстро. Но обратная задача — восстановить p и q по n — является в алгоритмическом смысле намного более сложной.

Вот что придумали в 70-х годах 20-го века Р. Ривест, А. Шамир и Л. Адлеман (именно по первым буквам их фамилий и назван алгоритм).

Абонент $\mathcal{A}$ выбирает большие простые числа p и q, вычисляет

$$n = pq \qquad \text{и} \qquad \varphi(n) = (p-1)(q-1).$$

Числа p и q должны быть настолько большими, чтобы выполнялось неравенство $x < n$ и чтобы задача разложения числа n на множители не могла быть выполнена при помощи имеющихся на данный момент вычислительных средств слишком быстро. Затем $\mathcal{A}$ выбирает $e \in \mathbb{N}$, чтобы выполнялось условие $\big(e, \varphi(n)\big) = 1$, и находит $d \in \mathbb{N}$, такое что

$$ed \equiv 1 \pmod{\varphi(n)}.$$

После этого абонент $\mathcal{A}$ объявляет во всеуслышание числа

$$n,\ e,$$

которые впредь называются *открытой* частью кода, и держит в секрете числа p, q, d, а также $\varphi(n)$, которые, соответственно, называются *закрытой* частью кода. Также используются термины *открытый ключ* и *закрытый ключ*.

Абонент $\mathcal{B}$ находит число $y \in \mathbb{Z}$, $0 \leqslant y < n$, такое что $y \equiv x^e \pmod{n}$ и передаёт по открытым каналам число y абоненту $\mathcal{A}$.

Абонент $\mathcal{A}$ восстанавливает число x возведением y в степень d по модулю n:

$$y^d \equiv \big(x^e\big)^d \equiv x \pmod{n}. \tag{18}$$

Если x удовлетворяет условию $(x, n) = 1$, то сравнение (18) является следствием теоремы Эйлера. Если же $(x, n) > 1$, нужно рассуждать несколько тоньше. При x делящемся на n сравнение (18) тривиально. При x делящемся на p, но не делящемся на q, при некотором целом t по малой теореме Ферма справедливо

$$\begin{cases} x^{ed} \equiv 0 \equiv x \pmod{p} \\ x^{ed} \equiv x^{1+t\varphi(n)} \equiv x \cdot \big(x^{q-1}\big)^{t(p-1)} \equiv x \pmod{q} \end{cases},$$

что равносильно (18). При x делящемся на q, но не делящемся на p, рассуждение аналогично.

Задача выполнена. Чтобы наблюдающему со стороны злоумышленнику взломать эту систему шифрования, ему по сути необходимо научиться раскладывать n на множители. Что на данный момент является чрезвычайно сложной с алгоритмической точки зрения задачей.

Обратите внимание, что ключевую роль в описанном алгоритме играет теорема Эйлера.

3.6 Цифровая подпись RSA

Система RSA позволяет также создавать так называемую *цифровую подпись* сообщения. В рамках схемы, описанной в параграфе 3.5, абонент $\mathcal{A}$ имеет возможность послать абоненту $\mathcal{B}$ сообщение с гарантированным подтверждением своего авторства. Пусть z — натуральное число, $z < n$, которое абонент $\mathcal{A}$ хочет послать абоненту $\mathcal{B}$. Абонент $\mathcal{A}$ находит число $w \in \mathbb{Z}$, $0 \leqslant w < n$, такое что $w \equiv z^d \pmod{n}$ и передаёт по открытым каналам числа z и w абоненту $\mathcal{B}$. Абонент $\mathcal{B}$ удостоверяется в авторстве сообщения z, проверяя выполнение сравнения

$$w^e \equiv \left(z^d\right)^e \equiv z \pmod{n}.$$

Отметим, что в описанной схеме не предполагается шифровка сообщения z. Если есть необходимость его зашифровать, свой набор открытых и закрытых ключей должен создать абонент $\mathcal{B}$.

4 Сравнения с одним неизвестным

Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. Рассмотрим сравнение

$$f(x) \equiv 0 \pmod{m}. \tag{19}$$

Определение 20. Класс вычетов $\overline{a} \in \mathbb{Z}_m$ называется *(частным) решением* сравнения (19), если $f(a) \equiv 0 \pmod{m}$. Такое частное решение называется также *корнем* многочлена $f(x)$ по модулю m.

Напомним, что если $a \equiv b \pmod{m}$, то $f(a) \equiv f(b) \pmod{m}$. Отсюда следует, что определение 20 корректно.

Определение 21. *Количеством решений* сравнения (19) называется величина

$$\mathcal{N}_f(m) = \left|\left\{ \overline{a} \in \mathbb{Z}_m \;\middle|\; f(a) \equiv 0 \pmod{m} \right\}\right|.$$

4.1 Китайская теорема об остатках

Теорема 15 (Китайская теорема об остатках)**.** *Пусть $m_1, \ldots, m_k$ — набор попарно взаимно простых модулей. Пусть $a_1, \ldots, a_k$ — произвольные целые числа. Тогда система сравнений*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{20}$$

имеет ровно одно решение по модулю

$$M = \prod_{i=1}^{k} m_i.$$

В явном виде решение можно находить по формуле

$$x \equiv \sum_{i=1}^{k} M_i b_i \pmod{M},$$

где

$$M_i = M/m_i, \quad i = 1, \ldots, k,$$

а $b_1, \ldots, b_k$ — произвольные целые числа, удовлетворяющие сравнениям

$$M_i b_i \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, k. \tag{21}$$

Доказательство. Определение чисел $b_1, \ldots, b_k$ корректно, ибо каждое из сравнений $M_i x \equiv a_i \pmod{m_i}$ имеет решение ввиду взаимной простоты чисел m_i и M_i при каждом $i = 1, \ldots, k$. Отметим, однако, что числа $b_1, \ldots, b_k$ определены неоднозначно — разрешается брать произвольный элемент соответствующего класса вычетов.

Пусть $b_1, \ldots, b_k$ — произвольные целые числа, удовлетворяющие сравнениям (21). Положим

$$x_0 = \sum_{i=1}^{k} M_i b_i.$$

Из сравнений

$$M_i b_i \equiv \begin{cases} 0 \pmod{m_j} & \text{при } j \neq i \\ a_i \pmod{m_j} & \text{при } j = i \end{cases},$$

следует, что x_0 удовлетворяет системе (20).

При этом очевидно, что при любом целом t число $x_0 + Mt$ также удовлетворяет системе (20), ибо $M \equiv 0 \pmod{m_i}$ для каждого $i = 1, \ldots, k$.

И наоборот, если x_1 — произвольное целое число, удовлетворяющее системе (20), то $x_1 - x_0 \equiv 0 \pmod{m_i}$ для каждого $i = 1, \ldots, k$, откуда ввиду того, что $(m_i, m_j) = 1$ при $i \neq j$, следует, что $x_1 - x_0 \equiv 0 \pmod{M}$. □

Теорема 16. *Пусть $m_1, \ldots, m_k$ — набор попарно взаимно простых модулей и $m = m_1 \cdot \ldots \cdot m_k$. Пусть $f(x) \in \mathbb{Z}[x]$. Тогда*

(1)

$$f(x) \equiv 0 \pmod{m} \iff \begin{cases} f(x) \equiv 0 \pmod{m_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{m_k} \end{cases};$$

(2) $\mathcal{N}_f(m) = \prod_{i=1}^{k} \mathcal{N}_f(m_i)$.

Доказательство. Достаточно доказать оба утверждения для $k = 2$, то есть при

$$m = m_1 m_2, \qquad (m_1, m_2) = 1.$$

Если целое число делится на m, то оно делится и на любой делитель m. Обратно, если целое число делится на m_1 и m_2, то в силу взаимной простоты m_1 и m_2 оно делится на их произведение. Этим доказывается пункт (1).

Далее, пусть $r = \mathcal{N}_f(m_1)$, $s = \mathcal{N}_f(m_2)$, пусть $a_1, \ldots, a_r$ — представители всех r решений сравнения

$$f(x) \equiv 0 \pmod{m_1}$$

(напоминаем, что решением мы называем не число, а класс вычетов) и пусть $b_1, \ldots, b_s$ — представители всех s решений сравнения

$$f(x) \equiv 0 \pmod{m_2}.$$

Тогда

$$f(x) \equiv 0 \pmod{m} \iff \begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \end{cases} \iff \left[\begin{array}{l} \left[\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv a_r \pmod{m_1} \end{array}\right. \\ \left[\begin{array}{l} x \equiv b_1 \pmod{m_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_s \pmod{m_2} \end{array}\right. \end{array}\right..$$

Стало быть, сравнение $f(x) \equiv 0 \pmod m$ равносильно совокупности систем вида

$$\begin{cases} x \equiv a_i \pmod{m_1} \\ x \equiv b_j \pmod{m_2} \end{cases},$$

где i пробегает от 1 до r, а j — от 1 до s. Каждая такая система по китайской теореме об остатках имеет ровно одно решение по модулю $m = m_1 m_2$, а количество систем равно rs. Таким образом, $\mathcal{N}_f(m) = rs = \mathcal{N}_f(m_1)\mathcal{N}_f(m_2)$. Пункт (2) доказан. □

4.2 Количество решений полиномиального сравнения по простому модулю

Теорема 17. *Пусть p — простое число и пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, $p \nmid a_n$. Тогда сравнение*

$$f(x) \equiv 0 \pmod p$$

имеет не более n решений. Иными словами, $\mathcal{N}_f(p) \leqslant \deg f$.

Доказательство. Будем доказывать индукцией по n.

При $n = 0$ имеем сравнение $a_0 \equiv 0 \pmod p$, которое решений относительно x не имеет, ибо по условию $p \nmid a_n = a_0$.

Пусть $n \geqslant 1$. Если сравнение $f(x) \equiv 0 \pmod p$ решений не имеет, то доказывать нечего. Пусть x_0 — некоторое целое число, удовлетворяющее сравнению $f(x_0) \equiv 0 \pmod p$. Заметим, что

$$f(x) - f(x_0) = \sum_{k=0}^{n} a_k (x^k - x_0^k) = (x - x_0) g(x),$$

где $g(x)$ — некоторый многочлен с целыми коэффициентами степени $n-1$, причём его старший коэффициент равен a_n. По предположению индукции $\mathcal{N}_g(p) \leqslant n - 1$. При этом в силу простоты числа p

$$(x - x_0) g(x) \equiv 0 \pmod p \iff \left[\begin{array}{l} x - x_0 \equiv 0 \pmod p \\ g(x) \equiv 0 \pmod p \end{array} \right. .$$

Стало быть, $\mathcal{N}_f(p) \leqslant \mathcal{N}_g(p) + 1 \leqslant n$. □

Следствие 1. *Пусть p — простое число. Рассмотрим многочлены*

$$f(x) = x^p - x \quad \text{и} \quad g(x) = x(x-1)(x-2)\ldots(x-p+1).$$

Тогда все коэффициенты многочлена $f(x) - g(x)$ делятся на p.

Доказательство. Положим $h(x) = f(x) - g(x)$. Тогда $\deg h \leqslant p - 1$. Пусть

$$h(x) = b_{p-1} x^{p-1} + \ldots + b_1 x + b_0.$$

Предположим, что не все b_i делятся на p. Пусть k — наибольший индекс, при котором $p \nmid b_k$. Положим $h_1(x) = b_k x^k + \ldots + b_1 x + b_0$. По малой теореме Ферма для любого $a \in \mathbb{Z}$ справедливо $h_1(a) \equiv h(a) \equiv f(a) - g(a) \equiv 0 \pmod p$. Стало быть, сравнение $h_1(x) \equiv 0 \pmod p$ имеет p решений, тогда как $\deg h_1 = k \leqslant p - 1$. Отсюда по теореме 17 следует, что старший коэффициент многочлена $h_1(x)$ должен делиться на p, что противоречит предположению $p \nmid b_k$. Таким образом, наше предположение неверно, то есть все b_i делятся на p. □

Замечание. Для многочленов из $\mathbb{Z}[x]$ также естественно говорить о делимости и о понятии сравнимости двух многочленов по модулю фиксированного многочлена. В частности, если воспринимать число p как многочлен степени 0, то следствие 1 утверждает, что в $\mathbb{Z}[x]$ выполняется сравнение $f \equiv g \pmod p$.

Следствие 2 (И снова теорема Вильсона)**.** *Пусть p — простое число. Тогда*

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. Достаточно посмотреть на коэффициенты при x многочленов $f(x)$ и $g(x)$ из следствия 1. □

4.3 Полиномиальные сравнения по модулю, равному степени простого числа

Пусть p — простое число и k — натуральное. Пусть $f(x) \in \mathbb{Z}[x]$. Рассмотрим сравнения

$$f(x) \equiv 0 \pmod{p^k} \tag{22}$$

и

$$f(x) \equiv 0 \pmod{p^{k+1}}. \tag{23}$$

Поскольку делимость целого числа на p^{k+1} влечёт его делимость на p^k, для поиска решений сравнения (23) достаточно ограничиться решениями сравнения (22). При этом каждый класс вычетов $a+p^k\mathbb{Z}$ по модулю p^k распадается на p классов вычетов по модулю p^{k+1}:

$$a + p^k\mathbb{Z} = \bigsqcup_{0 \leqslant t \leqslant p-1} \left((a + tp^k) + p^{k+1}\mathbb{Z}\right). \tag{24}$$

Соответственно, если в левой части (24) стоит (частное) решение сравнения (22), возникает естественный вопрос, как определить те классы вычетов по модулю p^{k+1} из правой части (24), которые являются (частными) решениями сравнения (23). В такой ситуации принято говорить о *подъёме* решения от модуля p^k до модуля p^{k+1}. Решается эта задача при помощи следующего утверждения, в котором на удивление большую роль играет значение производной $f'(x)$ в точке a.

Теорема 18 (Лемма Гензеля)**.** *Пусть p — простое число и k — натуральное. Пусть $f(x) \in \mathbb{Z}[x]$. Пусть $f(a) \equiv 0 \pmod{p^k}$. Тогда*

(1) *если $f'(a) \not\equiv 0 \pmod{p}$, то существует ровно одно $t \in \{0, \ldots, p-1\}$, для которого справедливо сравнение $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$;*

(2) *если $f'(a) \equiv 0 \pmod{p}$ и $f(a) \equiv 0 \pmod{p^{k+1}}$, то для каждого $t \in \{0, \ldots, p-1\}$ справедливо сравнение $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$;*

(3) *если $f'(a) \equiv 0 \pmod{p}$ и $f(a) \not\equiv 0 \pmod{p^{k+1}}$, то ни для какого $t \in \{0, \ldots, p-1\}$ не выполняется сравнение $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$;*

Лемма 18. *Пусть $f(x) \in \mathbb{Z}[x]$ и $a \in \mathbb{Z}$. Пусть $f(a+x) = g(x) = b_n x^n + \ldots + b_1 x + b_0$. Тогда $g(x) \in \mathbb{Z}[x]$, $b_0 = f(a)$, $b_1 = f'(a)$.*

Доказательство. После раскрытия скобок в $f(a+x)$ целочисленность коэффициентов сохраняется, поэтому $g(x) \in \mathbb{Z}[x]$. Далее, $b_0 = g(0) = f(a)$. Наконец, $b_1 = g'(0) = f'(a)$. □

Доказательство теоремы 18. Из леммы 18 при $x = tp^k$ следует, что

$$f(a + tp^k) \equiv f(a) + tp^k f'(a) \pmod{p^{k+1}}.$$

Стало быть, поскольку по условию $p^k \mid f(a)$, справедлива цепочка импликаций

$$\begin{aligned} f(a + tp^k) \equiv 0 \pmod{p^{k+1}} &\iff \\ \iff f(a) + tp^k f'(a) \equiv 0 \pmod{p^{k+1}} &\iff \\ \iff \frac{f(a)}{p^k} + f'(a)t \equiv 0 \pmod{p}&. \end{aligned}$$

Таким образом, сравнение $f(a+tp^k) \equiv 0 \pmod{p^{k+1}}$, то есть утверждение, что класс вычетов $(a+tp^k)+p^{k+1}\mathbb{Z}$ является частным решением сравнения (23), равносильно сравнению

$$\frac{f(a)}{p^k} + f'(a)t \equiv 0 \pmod{p}.$$

Остаётся заметить, что при $f'(a) \not\equiv 0 \pmod{p}$ это сравнение имеет ровно одно решение, а при $f'(a) \equiv 0 \pmod{p}$ оно равносильно сравнению $f(a)/p^k \equiv 0 \pmod{p}$, то есть сравнению $f(a) \equiv 0 \pmod{p^{k+1}}$, истинность которого не зависит от t. □

Таким образом, если по заданному простому модулю p корни многочлена $f(x)$ найдены, теорема 18 позволяет достаточно быстро находить корни $f(x)$ по модулю p^k при любом заданном натуральном k.

5 Квадратичные сравнения

В этом параграфе везде будем считать, что p — простое число, $p \geqslant 3$.

Рассмотрим многочлен $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$, $p \nmid a_2$. Тогда ввиду нечётности p

$$f(x) \equiv 0 \pmod{p} \iff 4a_2f(x) \equiv 0 \pmod{p} \iff$$
$$\iff (2a_2x + a_1)^2 \equiv a_1^2 - 4a_2a_0 \pmod{p} \iff y^2 \equiv D \pmod{p},$$

где $y = 2a_2x + a_1$ и $D = a_1^2 - 4a_2a_0$.

Таким образом, любое (нелинейное) квадратичное сравнение равносильно сравнению вида

$$x^2 \equiv a \pmod{p} \tag{25}$$

с некоторым целым a. Отметим, что при выделении полного квадрата мы существенно пользовались нечётностью p.

Определение 22. Целое число a называется *квадратичным вычетом* по модулю p, если сравнение (25) разрешимо. Если же сравнение (25) неразрешимо, то a называется *квадратичным невычетом* по модулю p.

Лемма 19. *Любая приведённая система вычетов по модулю p содержит ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов.*

Доказательство. Для любых целых a и b справедливо

$$a^2 \equiv b^2 \pmod{p} \iff p \mid (a-b)(a+b) \iff \left[\begin{array}{l} p \mid a-b \\ p \mid a+b \end{array}\right. \iff \left[\begin{array}{l} a \equiv b \pmod{p} \\ a \equiv -b \pmod{p} \end{array}\right. .$$

При этом ни для какого a, не делящегося на p, не выполняется сравнение $a \equiv -a \pmod{p}$, ибо $p \neq 2$. Стало быть, элементы любой приведённой системы вычетов разбиваются на пары, которые при возведении в квадрат дают попарно не сравнимые квадратичные вычеты. Остаётся заметить, что множество из $p-1$ элементов разбивается на $\frac{p-1}{2}$ пар. □

Теорема 19 (Критерий Эйлера квадратичности вычета)**.** *Пусть $a \in \mathbb{Z}$, $p \nmid a$. Тогда*

(1) *a — квадратичный вычет по модулю p* $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;

(2) *a — квадратичный невычет по модулю p* $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Доказательство. Пусть a — квадратичный вычет. Тогда для некоторого целого b справедливо $a \equiv b^2 \pmod{p}$, откуда по малой теореме Ферма

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

Рассмотрим многочлен $f(x) = x^{\frac{p-1}{2}} - 1$. Как мы только что показали, если a — квадратичный вычет, то $f(a) \equiv 0 \pmod{p}$. По лемме 19 любая приведённая система вычетов по модулю p содержит ровно $\frac{p-1}{2}$ квадратичных вычетов. Стало быть, квадратичные вычеты дают $\frac{p-1}{2}$ решений сравнения $f(x) \equiv 0 \pmod{p}$. По теореме 17 других решений у этого сравнения нет. Следовательно, если a — квадратичный невычет, то

$$a^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}.$$

Но по малой теореме Ферма

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Таким образом, если a — квадратичный невычет, то $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$, то есть

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

□

Следствие. *Произведение квадратичных невычетов является квадратичным вычетом.*

5.1 Символ Лежандра

При изучении квадратичных сравнений и работе с ними чрезвычайно полезным оказывается так называемый *символ Лежандра*.

Определение 23. Пусть p — нечётное простое число, a — произвольное целое число. *Символ Лежандра a по p* определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } p \mid a \\ 1, & \text{если } p \nmid a \text{ и } a \text{ — квадратичный вычет по модулю } p \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p \end{cases}.$$

Отметим особо, что для модуля 2 символ Лежандра не определён.

Теорема 20 (Элементарные свойства символа Лежандра)**.** *Пусть p — нечётное простое число, a и b — произвольные целые числа. Тогда*

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

(2) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

(4) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{4} \\ -1, & \text{если } p \equiv 3 \pmod{4} \end{cases}$.

Доказательство. Пункт (1) мгновенно следует из критерия Эйлера (см. теорему 19). Пункт (2) следует непосредственно из определения символа Лежандра. Пункты (3) и (4) следуют из пункта (1). □

Теорема 21 (Символ Лежандра для двойки)**.** *Пусть p — нечётное простое число. Тогда*

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

Иными словами,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{если } p \equiv \pm 1 \pmod 8 \\ -1, & \text{если } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Теорема 22 (Квадратичный закон взаимности Гаусса)**.** *Для любых нечётных простых p и q справедливо*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Иными словами, при «переворачивании» символ Лежандра $\left(\frac{p}{q}\right)$ меняет знак тогда и только тогда, когда $p \equiv q \equiv 3 \pmod 4$.

Доказательства теорем 21 и 22 требуют некоторых дополнительных соображений. Одно из наиболее стандартных рассуждений использует следующее наблюдение.

Лемма 20 (Лемма Гаусса)**.** *Пусть p — нечётное простое, $a \in \mathbb{Z}$, $p \nmid a$. Для каждого числа k из набора $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ определим числа $\varepsilon_k \in \{1, -1\}$ и $r_k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ условием*

$$ak \equiv \varepsilon_k r_k \pmod p. \tag{26}$$

Тогда

$$\left(\frac{a}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k = (-1)^t, \tag{27}$$

где t — количество отрицательных чисел среди $\varepsilon_1, \ldots, \varepsilon_{\frac{p-1}{2}}$.

Доказательство. Положим для краткости $s = \frac{p-1}{2}$.

Заметим, что $r_k \neq r_l$ при $k \neq l$. Действительно, если $r_k = r_l$, то $ak \equiv \pm al \pmod p$, то есть $k \equiv \pm l \pmod p$, что возможно лишь при $k = l$, ибо k и l принадлежат множеству $\{1, 2, \ldots, s\}$.

Стало быть, $r_1, \ldots, r_s$ — перестановка чисел $1, \ldots, s$, то есть

$$\prod_{k=1}^{s} r_k = \prod_{k=1}^{s} k = s!,$$

откуда, перемножая сравнения (26) по $k = 1, \ldots, s$, получаем

$$a^{\frac{p-1}{2}} s! \equiv \Big(\prod_{k=1}^{s} \varepsilon_k\Big) s! \mod p.$$

Учитывая пункт (1) теоремы 20 и тот факт, что $(s!, p) = 1$, приходим к сравнению

$$\left(\frac{a}{p}\right) \equiv \prod_{k=1}^{s} \varepsilon_k \mod p.$$

Остаётся заметить, что правая и левая части этого сравнения равны либо 1, либо -1. Разность таких двух чисел по модулю не превосходит 2, стало быть, делиться на нечётное p она может лишь тогда, когда она равна нулю. Получаем равенство (27). □

Следствие 1. *Пусть p — нечётное простое. Тогда*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{если } p \equiv \pm 1 \pmod 8 \\ -1, & \text{если } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Доказательство. Как и в доказательстве леммы 20, положим $s = \frac{p-1}{2}$. По лемме 20

$$\left(\frac{2}{p}\right) = (-1)^t,$$

где t равно количеству чётных чисел, строго больших s и меньших p. Всего чётных чисел на отрезке от 1 до p в точности s. Количество же чётных чисел на отрезке от 1 до s равно $s/2$, если s чётно, и $(s-1)/2$, если s нечётно. Стало быть,

$$t = \begin{cases} \dfrac{s}{2}, & \text{если } s \text{ чётно} \\ \dfrac{s+1}{2}, & \text{если } s \text{ нечётно} \end{cases}.$$

Соответственно, t чётно при $s \equiv 0, 3 \pmod 4$ и нечётно при $s \equiv 1, 2 \pmod 4$. Вспоминая, что $s = \frac{p-1}{2}$, получаем, что t чётно при $p \equiv 1, 7 \pmod 8$ и нечётно при $p \equiv 3, 5 \pmod 8$. □

Доказательство теоремы 21. Заметим сначала, что число $\frac{p^2-1}{8}$ является целым, ибо любой нечётный квадрат сравним с 1 по модулю 8. Далее, среди чисел $p-1$, $p+1$ ровно одно делится на 4. Стало быть, чётность числа $\frac{p^2-1}{8}$ равносильна тому, что то из этих чисел, которое делится на 4, делится и на 8. А это условие равносильно тому, что $p \equiv \pm 1 \pmod 8$. Остаётся воспользоваться следствием 1 из леммы Гаусса. □

Следствие 2. *Пусть p — нечётное простое, a — нечётное число, $p \nmid a$. Положим*

$$S = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ak}{p}\right],$$

где квадратные скобки обозначают целую часть числа. Тогда $\left(\dfrac{a}{p}\right) = (-1)^S$.

Доказательство. Как и прежде, положим $s = \frac{p-1}{2}$. Пусть t, $\varepsilon_1, \ldots, \varepsilon_s$, $r_1, \ldots, r_s$ — из леммы Гаусса. Нужно показать, что

$$S \equiv t \pmod 2. \tag{28}$$

Заметим, что $\left[\frac{ak}{p}\right]$ в точности совпадает с неполным частным при делении ak на p с остатком. Поскольку остаток заключён между 0 и $p-1$, он совпадает либо с r_k, либо с $p - r_k$. Более конкретно, остаток от деления ak на p равен

$$ak - \left[\frac{ak}{p}\right] \cdot p = \begin{cases} r_k, & \text{если } \varepsilon_k = 1 \\ p - r_k, & \text{если } \varepsilon_k = -1 \end{cases}.$$

Поскольку $a \equiv p \equiv \varepsilon_k \equiv 1 \equiv -1 \pmod 2$, справедливо сравнение

$$k + \left[\frac{ak}{p}\right] \equiv \begin{cases} r_k \pmod 2, & \text{если } \varepsilon_k = 1 \\ 1 + r_k \pmod 2, & \text{если } \varepsilon_k = -1 \end{cases}.$$

Просуммируем это сравнение по $k = 1, \ldots, s$. Получим

$$\sum_{k=1}^{s} k + S \equiv t + \sum_{k=1}^{s} r_k \pmod 2.$$

Учитывая, что $r_1, \ldots, r_s$ — перестановка чисел $1, \ldots, s$, то есть

$$\sum_{k=1}^{s} r_k = \sum_{k=1}^{s} k = \frac{s(s+1)}{2},$$

приходим к (28). □

Следствие 2 из леммы Гаусса позволяет довольно изящно вывести квадратичный закон взаимности Гаусса.

Доказательство теоремы 22. Для заданных нечётных простых нам нужно доказать равенство

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{29}$$

Если $p = q$, то обе части этого равенства равны нулю и всё доказано.

Пусть далее $p \neq q$. По следствию 2 из леммы Гаусса

$$\left(\frac{q}{p}\right) = (-1)^{S_1} \qquad \text{и} \qquad \left(\frac{p}{q}\right) = (-1)^{S_2}, \tag{30}$$

где

$$S_1 = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] \qquad \text{и} \qquad S_2 = \sum_{l=1}^{\frac{q-1}{2}} \left[\frac{pl}{q}\right].$$

Покажем, что

$$S_1 + S_2 = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{31}$$

Для этого рассмотрим треугольник $\mathcal{T}_1$ с вершинами в точках $(0,0)$, $\left(\frac{p}{2},0\right)$, $\left(\frac{p}{2},\frac{q}{2}\right)$, треугольник $\mathcal{T}_2$ с вершинами в точках $(0,0)$, $\left(0,\frac{q}{2}\right)$, $\left(\frac{p}{2},\frac{q}{2}\right)$ и их объединение — прямоугольник $\mathcal{P}$ с вершинами в точках $(0,0)$, $\left(\frac{p}{2},0\right)$, $\left(\frac{p}{2},\frac{q}{2}\right)$, $\left(0,\frac{q}{2}\right)$.

Покажем, что количество точек с натуральными координатами, содержащихся в треугольнике $\mathcal{T}_1$, равно S_1. При каждом $k = 1, \ldots, \frac{p-1}{2}$ количество точек в $\mathcal{T}_1$ с натуральными координатами, первая из которых равна k, равно $\left[\frac{qk}{p}\right]$. Стало быть, действительно, суммарное количество точек в $\mathcal{T}_1$ с натуральными координатами равно S_1.

Аналогично, количество точек с натуральными координатами, содержащихся в треугольнике $\mathcal{T}_2$, равно S_2, ибо при каждом $l = 1, \ldots, \frac{q-1}{2}$ количество точек в $\mathcal{T}_2$ с натуральными координатами, вторая из которых равна l, равно $\left[\frac{pl}{q}\right]$.

Остаётся заметить, что количество точек с натуральными координатами, содержащихся в прямоугольнике $\mathcal{P}$, равно $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

Итак, равенство (31), действительно, имеет место. Из него ввиду (30) мгновенно следует (29). □

5.2 Символ Якоби

Определение 24. Пусть P — нечётное число, $P \geqslant 3$. Рассмотрим его каноническое разложение на простые

$$P = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}. \tag{32}$$

Тогда для любого $a \in \mathbb{Z}$ определён *символ Якоби*

$$\left(\frac{a}{P}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}, \tag{33}$$

где справа стоит произведение символов Лежандра.

Замечание. Иногда бывает удобно рассматривать вместо канонического разложения (32) разложение числа P на простые в первых степенях с допускаемыми повторениями (так, например, $72 = 2^3 \cdot 3^2 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$). При таком подходе будем писать

$$P = p_1 \cdot \ldots \cdot p_s,$$

где $s = \alpha_1 + \ldots + \alpha_k$, в соответствии с (32). И в этом случае вместо (33) мы будем использовать эквивалентное равенство

$$\left(\frac{a}{P}\right) = \prod_{i=1}^{s}\left(\frac{a}{p_i}\right).$$

Теорема 23 (Свойства символа Якоби). *Пусть P — нечётное число, $P \geqslant 3$. Пусть a и b — произвольные целые числа и пусть Q — произвольное нечётное число, $Q \geqslant 3$. Тогда*

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

(2) $a \equiv b \pmod P \implies \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$;

(3) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\cdot\left(\frac{b}{P}\right)$;

(4) $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}} = \begin{cases} 1, & \text{если } P \equiv 1 \pmod 4 \\ -1, & \text{если } P \equiv 3 \pmod 4 \end{cases}$;

(5) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = \begin{cases} 1, & \text{если } P \equiv \pm 1 \pmod 8 \\ -1, & \text{если } P \equiv \pm 3 \pmod 8 \end{cases}$;

(6) $\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)\cdot(-1)^{\frac{(P-1)(Q-1)}{4}}$.

Замечание. Как нетрудно заметить, символ Якоби наследует все доказанные нами выше свойства символа Лежандра, кроме пункта (1) теоремы 20, базирующегося на критерии Эйлера. Причина в том, что критерий Эйлера по существу использует простоту модуля, в то время как для составного модуля легко привести контрпример к аналогу утверждения пункта (1) теоремы 20. Например,

$$\left(\frac{2}{15}\right) = 1, \qquad \text{но} \qquad 2^{\frac{15-1}{2}} = 2^7 = 2^4\cdot 2^3 = 16\cdot 8 \equiv 8 \not\equiv 1 \pmod{15},$$

или

$$\left(\frac{3}{15}\right) = 0, \qquad \text{но} \qquad 3^{\frac{15-1}{2}} = 3^7 \not\equiv 0 \pmod{15}.$$

Соответственно, отсутствие аналога критерия Эйлера вызывает трудности уже при доказательстве пункта (3) теоремы 23. Но эти трудности, как мы сейчас увидим, можно преодолеть иначе.

Лемма 21. *Пусть P — нечётное число, $P \geqslant 3$, и пусть $P = p_1\cdot\ldots\cdot p_s$ — его разложение на простые в первых степенях с допускаемыми повторениями (см. замечание к определению 24). Тогда*

(1) $\frac{P-1}{2} \equiv \sum_{i=1}^{s}\frac{p_i-1}{2} \pmod 2$;

(2) $\frac{P^2-1}{8} \equiv \sum_{i=1}^{s}\frac{p_i^2-1}{8} \pmod 2$.

Доказательство. Пусть u и v — произвольные нечётные числа. Тогда

$$\frac{uv-1}{2} - \left(\frac{u-1}{2} + \frac{v-1}{2}\right) = \frac{(u-1)(v-1)}{2} \equiv 0 \pmod 2,$$

то есть числа $\frac{uv-1}{2}$ и $\frac{u-1}{2}+\frac{v-1}{2}$ имеют одинаковую чётность. Отсюда по индукции мгновенно следует пункт (1). Аналогично, пункт (2) следует по индукции из того факта, что

$$\frac{u^2v^2-1}{8}-\left(\frac{u^2-1}{8}+\frac{v^2-1}{8}\right)=\frac{(u^2-1)(v^2-1)}{8}\equiv 0 \pmod 2.$$

□

Доказательство теоремы 23. Пункты (1), (2), (3) мгновенно следуют из определения символа Якоби и соответствующих свойств символа Лежандра.

Первое равенство пункта (4) следует из пункта (1) леммы 21 и известного значения символа Лежандра на -1 (см. пункт (4) теоремы 20). Второе равенство — простое упражнение.

Первое равенство пункта (5) следует из пункта (2) леммы 21 и известного значения символа Лежандра на 2 (см. теорему 21). Второе равенство — немногим более сложное упражнение (если не получается — см. доказательство теоремы 21).

Наконец, докажем пункт (6) при помощи пункта (1) леммы 21.

Для заданных нечётных P, Q, таких что $P,Q\geqslant 3$, нам нужно доказать равенство

$$\left(\frac{P}{Q}\right)=\left(\frac{Q}{P}\right)\cdot(-1)^{\frac{(P-1)(Q-1)}{4}}. \tag{34}$$

Если $(P,Q)\neq 1$, то обе части этого равенства равны нулю и всё доказано.

Пусть далее $(P,Q)=1$ и пусть $P=p_1\cdot\ldots\cdot p_s$, $Q=q_1\cdot\ldots\cdot q_r$ — разложения P и Q на простые в первых степенях с допускаемыми повторениями (опять же, см. замечание к определению 24). Тогда никакое p_i не равно никакому q_j и, стало быть, по квадратичному закону взаимности Гаусса (см. теорему 22)

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=\prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{p_i}{q_j}\right)\cdot\left(\frac{q_j}{p_i}\right)=\prod_{i=1}^{s}\prod_{j=1}^{r}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

Учитывая пункт (1) леммы 21, видим, что

$$\sum_{i=1}^{s}\sum_{j=1}^{r}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}=\left(\sum_{i=1}^{s}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{r}\frac{q_j-1}{2}\right)\equiv\frac{P-1}{2}\cdot\frac{Q-1}{2} \pmod 2.$$

Следовательно,

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

что равносильно (34), ибо все присутствующие множители принимают значения ± 1. □

Замечание. Пункт (5) теоремы 23 можно доказывать без привлечения пункта (2) леммы 21. Достаточно иметь все остальные пункты теоремы 23. Действительно, предположим, что мы уже доказали, что

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

Тогда

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

Так мы доказываем шаг индукции. Базу же индукции предоставляет равенство $\left(\frac{2}{3}\right)=-1$, которое нам уже известно.

5.3 Тест Соловея–Штрассена

Как мы отмечали выше, для символа Якоби, вообще говоря, не выполняется аналог критерия Эйлера. Этот факт можно использовать для тестирования натуральных чисел на непростоту.

Предложение 3. *Пусть N — нечётное число, $N \geqslant 3$. Пусть $a \in \mathbb{Z}$, $1 < a < N$. Тогда*

(1) *если $(a, N) > 1$, то N — составное число;*

(2) *если $(a, N) = 1$ и*

$$\left(\frac{a}{N}\right) \not\equiv a^{\frac{N-1}{2}} \pmod{N}, \tag{35}$$

то N — составное число.

Справедливость этого утверждения очевидна благодаря пункту (1) теоремы 20. Однако в 70-х годах 20-го века это простое наблюдение позволило Р. М. Соловею и Ф. Штрассену описать весьма эффективный вероятностный алгоритм проверки числа на непростоту. Он базируется на следующем результате, который обосновывает тот факт, что если N — составное число, то при случайном выборе целого числа a, такого что $1 \leqslant a \leqslant N - 1$ и $(a, N) = 1$, с вероятностью не менее $1/2$ мы попадём на a, удовлетворяющее условию (35), и стало быть, доказывающее непростоту N.

Теорема 24. *Пусть N — составное нечётное натуральное число. Рассмотрим множество*

$$\mathcal{S}_N = \left\{ \overline{a} \in \mathbb{Z}_N^* \;\middle|\; \left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \pmod{N} \right\}. \tag{36}$$

Тогда

$$|\mathcal{S}_N| \leqslant \frac{\varphi(N)}{2}.$$

Напоминание. Под $\mathbb{Z}_N^*$ мы понимаем множество всех классов вычетов из $\mathbb{Z}_N$, обратимых по умножению. А обратимость по умножению равносильна тому, что класс вычетов состоит из чисел, взаимно простых с модулем.

Лемма 22. *Пусть N и $\mathcal{S}_N$ — как в формулировке теоремы 24 и пусть множество $\mathcal{S}_N$ не совпадает со всем $\mathbb{Z}_N^*$. Тогда*

$$|\mathcal{S}_N| \leqslant \frac{\varphi(N)}{2}.$$

Доказательство. Множество $\mathcal{S}_N$ является подмножеством множества $\mathbb{Z}_N^*$. По условию оно является подмножеством собственным, то есть существует такое $b \in \mathbb{Z}$, что

$$\overline{b} \in \mathbb{Z}_N^* \backslash \mathcal{S}_N.$$

Возьмём такое b. Тогда

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

и для любого $a \in \mathbb{Z}$, такого что $\overline{a} \in \mathcal{S}_N$, справедливо $\overline{ab} \notin \mathcal{S}_N$, ибо

$$\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right) \equiv a^{\frac{N-1}{2}} \left(\frac{b}{N}\right) \not\equiv a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \equiv (ab)^{\frac{N-1}{2}} \pmod{N}.$$

Остаётся заметить, что если $a_1 \not\equiv a_2 \pmod{N}$, в силу взаимной простоты b с N, выполняется также $a_1 b \not\equiv a_2 b \pmod{N}$. Таким образом, множество S_N и «сдвинутое» множество

$$\overline{b} \cdot \mathcal{S}_N = \left\{ \overline{ab} \;\middle|\; \overline{a} \in \mathcal{S}_N \right\}$$

суть два непересекающихся подмножества множества $\mathbb{Z}_N^*$ одинаковой мощности. Отсюда следует, что

$$|\mathcal{S}_N| \leqslant \frac{1}{2} \cdot |\mathbb{Z}_N^*| = \frac{\varphi(N)}{2}.$$

□

Лемма 23. *Пусть N и $\mathcal{S}_N$ — как в формулировке теоремы 24. Пусть $N = M^t$, где $M, t \in \mathbb{N}$ и $t \geqslant 2$. Тогда*

$$\mathcal{S}_N \neq \mathbb{Z}_N^*.$$

Доказательство. Предположим противное, то есть что $\mathcal{S}_N = \mathbb{Z}_N^*$. Тогда для каждого $a \in \mathbb{Z}$, такого что $(a, N) = 1$, имеет место сравнение

$$\left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \pmod{N}. \tag{37}$$

Возьмём $a = 1 + M^{t-1}$. Тогда

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

Учитывая (37), получаем

$$1 = \left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \equiv \left(1 + M^{t-1}\right)^{\frac{M^t-1}{2}} \equiv 1 + \frac{M^t - 1}{2} \cdot M^{t-1} \pmod{M^t}.$$

Стало быть,

$$\frac{M^t - 1}{2} \cdot M^{t-1} \equiv 0 \pmod{M^t},$$

то есть

$$M^t - 1 \equiv 0 \pmod{M},$$

что неверно. Полученное противоречие доказывает, что $\mathcal{S}_N \neq \mathbb{Z}_N^*$. □

Лемма 24. *Пусть N и $\mathcal{S}_N$ — как в формулировке теоремы 24. Пусть N — не полный квадрат и имеет не менее двух различных простых делителей. Тогда*

$$\mathcal{S}_N \neq \mathbb{Z}_N^*.$$

Доказательство. Рассмотрим каноническое разложение $N = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ на простые. Тогда по условию $k \geqslant 2$. Поскольку N — не полный квадрат, не ограничивая общности, можно считать, что α_1 нечётно.

Как и в доказательстве леммы 23, предположим противное, то есть что для каждого $a \in \mathbb{Z}$, такого что $(a, N) = 1$, имеет место сравнение (37).

Возьмём произвольный квадратичный невычет b по модулю p_1 и рассмотрим систему сравнений

$$\begin{cases} a \equiv b \pmod{p_1} \\ a \equiv 1 \pmod{p_2 \cdot \ldots \cdot p_k} \end{cases}.$$

По китайской теореме об остатках такая система имеет решение. Возьмём произвольное целое a, удовлетворяющее этой системе. Тогда

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

Учитывая (37), получаем

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

В частности, $a^{\frac{N-1}{2}} \equiv -1 \pmod{p_2}$, в то время как по построению $a \equiv 1 \pmod{p_2}$. Полученное противоречие доказывает, что $\mathcal{S}_N \neq \mathbb{Z}_N^*$. □

Доказательство теоремы 24. Если N — составное нечётное натуральное число, то оно удовлетворяет либо условию леммы 23, либо условию леммы 24. Применяя эти леммы, получаем, что

$$\mathcal{S}_N \neq \mathbb{Z}_N^*.$$

Остаётся применить лемму 22. □

6 Первообразные корни

Определение 25. Пусть задан модуль m. Пусть $a \in \mathbb{Z}$, $(a, m) = 1$. Величина

$$\operatorname{ord}_m(a) = \min\left\{k \in \mathbb{N} \;\middle|\; a^k \equiv 1 \pmod m\right\}$$

называется *показателем* вычета a по модулю m.

Теорема 25. *Пусть задан модуль m. Пусть $a \in \mathbb{Z}$, $(a, m) = 1$. Пусть k — произвольное целое число, такое что*

$$a^k \equiv 1 \pmod m.$$

Тогда

$$\operatorname{ord}_m(a) \mid k.$$

Доказательство. Обозначим для краткости $\operatorname{ord}_m(a)$ через d. Поделим с остатком k на d:

$$k = qd + r, \qquad 0 \leqslant r < d.$$

Тогда

$$1 \equiv a^k \equiv a^{qd+r} \equiv \left(a^d\right)^q \cdot a^r \equiv a^r \pmod m.$$

Если k не делится нацело на d, то $r \in \mathbb{N}$ и $r < d$. Это противоречит минимальности d. Стало быть, $d \mid k$. □

Следствие. *Пусть задан модуль m. Пусть $a \in \mathbb{Z}$, $(a, m) = 1$. Тогда*

$$\operatorname{ord}_m(a) \mid \varphi(m).$$

Доказательство. Достаточно применить теорему Эйлера и теорему 25. □

Определение 26. Пусть $g \in \mathbb{Z}$, $(g, m) = 1$. Число g называется *первообразным корнем по модулю m*, если $\operatorname{ord}_m(g) = \varphi(m)$.

Очень полезную точку зрения на первообразные корни даёт следующее наблюдение, имеющее в некотором смысле алгебраическую природу.

Предложение 4. *Целое число g является первообразным корнем по модулю m тогда и только тогда, когда числа*

$$1, g, g^2, \ldots, g^{\varphi(m)-1}$$

образуют приведённую систему вычетов по модулю m или, иными словами,

$$\mathbb{Z}_m^* = \left\{\overline{g}^0, \overline{g}^1, \overline{g}^2, \ldots, \overline{g}^{\varphi(m)-1}\right\}.$$

Доказательство. Если g является первообразным корнем по модулю m, то числа

$$1, g, g^2, \ldots, g^{\varphi(m)-1}$$

попарно несравнимы по модулю m, ибо если $g^k \equiv g^l \pmod m$, то $g^{k-l} \equiv 1 \pmod m$, что означает, что $k \equiv l \pmod{\varphi(m)}$. Следовательно, эти числа образуют приведённую систему вычетов по модулю m.

Если же g не является первообразным корнем, то $g^{\operatorname{ord}_m(g)} \equiv 1 \pmod m$, в то время как $\operatorname{ord}_m(g) < \varphi(m)$, то есть никакие степени числа g приведённую систему вычетов не образуют. □

Теорема 26. *Если по модулю m существуют первообразные корни, то в любой приведённой системе вычетов по модулю m содержится ровно $\varphi(\varphi(m))$ первообразных корней по модулю m.*

Доказательство. Пусть g — первообразный корень по модулю m. Достаточно показать, что g^k является первообразным корнем по модулю m тогда и только тогда, когда

$$(k, \varphi(m)) = 1.$$

В свете предложения 4 число g^k является первообразным корнем тогда и только тогда, когда существует целое число l, такое что

$$(g^k)^l \equiv g \pmod{m}.$$

А это в свою очередь равносильно разрешимости сравнения $kl \equiv 1 \pmod{\varphi(m)}$ относительно l. Стало быть, действительно, условие $(k, \varphi(m)) = 1$ является критерием того, что g^k является первообразным корнем по модулю m. □

Упражнение. Пусть g — первообразный корень по модулю m и пусть $k \in \mathbb{N}$. Докажите, что

$$\operatorname{ord}_m(g^k) = \frac{\varphi(m)}{(k, \varphi(m))}.$$

6.1 Первообразные корни по простым модулям

Теорема 27. *По любому простому модулю существуют первообразные корни.*

Лемма 25. *Пусть p — простое число и пусть d — делитель числа $p-1$. Тогда мощность множества*

$$\mathcal{M}_d = \left\{ \overline{a} \in \mathbb{Z}_p^* \;\middle|\; \operatorname{ord}_p(a) = d \right\} \tag{38}$$

не превосходит $\varphi(d)$.

Доказательство. Если $\mathcal{M}_d$ пусто, то $|\mathcal{M}_d| = 0 < \varphi(d)$ и доказывать нечего. Пусть $\mathcal{M}_d$ непусто. Возьмём такое $a \in \mathbb{Z}$, что $\overline{a} \in \mathcal{M}_d$.

Покажем сначала, что

$$\mathcal{M}_d \subseteq \left\{ \overline{a}^k \;\middle|\; k = 0, 1, \ldots, d-1 \right\}. \tag{39}$$

Для этого заметим, что, во-первых, $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$, а во-вторых, классы вычетов $\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{d-1}$ попарно различны. Следовательно, по теореме 17, эти классы вычетов представляют собой *все* решения сравнения

$$x^d \equiv 1 \pmod{p}.$$

То есть целое число может иметь показатель d по модулю p только в том случае, если оно принадлежит одному из классов $\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{d-1}$, что доказывает (39).

Теперь, зная (39), легко показать, что

$$\mathcal{M}_d \subseteq \left\{ \overline{a}^k \;\middle|\; 1 \leqslant k \leqslant d-1,\ (k, d) = 1 \right\}. \tag{40}$$

Действительно, если $(k, d) = l > 1$, то $(a^k)^{d/l} \equiv (a^d)^{k/l} \equiv 1 \pmod{p}$, то есть $\overline{a}^k \notin \mathcal{M}_d$ при таких k. Отсюда мгновенно следует (40). □

Доказательство теоремы 27. Пусть p — простое число. Тогда по следствию из теоремы 25 показатели всех чисел по модулю p являются делителями $p-1$. Определим для каждого $d \mid p-1$ множество $\mathcal{M}_d$ равенством (38). Поскольку при различных d_1 и d_2 множества $\mathcal{M}_{d_1}$ и $\mathcal{M}_{d_2}$ не пересекаются, из леммы 25 следует, что

$$p-1 = \left|\mathbb{Z}_p^*\right| = \sum_{d \mid p-1} |\mathcal{M}_d| \leqslant \sum_{d \mid p-1} \varphi(d). \tag{41}$$

Но по лемме 11 (которую мы использовали для доказательства мультипликативности функции Эйлера)

$$\sum_{d \mid p-1} \varphi(d) = p-1. \tag{42}$$

Легко заметить, что (41) и (42) одновременно выполняются только тогда, когда все неравенства $|\mathcal{M}_d| \leqslant \varphi(d)$ являются равенствами. Стало быть, для любого $d \mid p-1$ справедливо

$$|\mathcal{M}_d| = \varphi(d).$$

В частности, множество $\mathcal{M}_{p-1}$ непусто. □

Замечание. На самом деле мы доказали нечто большее. А именно, мы доказали, что в любой приведённой системе вычетов по простому модулю p количество вычетов с показателем d, где d — произвольный делитель $p-1$, в точности равно $\varphi(d)$. В частности, мы получили ещё одно доказательство теоремы 26 в случае простого модуля.

Следствие (Опять теорема Вильсона)**.** *Пусть p — простое число. Тогда*

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. Пусть g — первообразный корень по модулю p, $p \geqslant 3$. Тогда $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, откуда $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, ибо

$$x^2 \equiv 1 \pmod{p} \iff \left[\begin{array}{l} x \equiv 1 \pmod{p} \\ x \equiv -1 \pmod{p} \end{array}\right. .$$

Стало быть, поскольку по малой теореме Ферма $g^p \equiv g \pmod{p}$,

$$(p-1)! \equiv \prod_{k=1}^{p-1} g^k \equiv g^{\frac{p(p-1)}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

□

Упражнение. Пусть p — нечётное простое число и пусть g — первообразный корень по модулю p. Докажите, что g является квадратичным невычетом по модулю p.

6.2 Первообразные корни по составным модулям

Для проверки свойства числа быть первообразным корнем по модулю m полезен следующий критерий.

Предложение 5. *Пусть задан модуль m. Пусть $g \in \mathbb{Z}$, $(g, m) = 1$. Число g является первообразным корнем по модулю m тогда и только тогда, когда для любого простого делителя q числа $\varphi(m)$ справедливо $g^{\varphi(m)/q} \not\equiv 1 \pmod{m}$.*

Доказательство. Достаточно вспомнить, что показатель g по модулю m является делителем $\varphi(m)$, и заметить, что если $d \mid \varphi(m)$ и $d < \varphi(m)$ (такие делители называются *собственными*), найдётся простое q, делящее $\varphi(m)$, для которого $d \mid \varphi(m)/q$. □

Лемма 26. *Если выполняется хотя бы одно из следующих условий:*

(а) $8 \mid m$;

(б) $4p \mid m$, *где* p — *нечётное простое*;

(в) $pq \mid m$, *где* p *и* q — *различные нечётные простые,*

то по модулю m *первообразных корней не существует.*

Доказательство. Достаточно заметить, что в каждом из трёх случаев теорема Эйлера допускает усиление. А именно, если m удовлетворяет (а), (б) или (в), то для любого целого a, взаимно простого с m, справедливо $a^{\varphi(m)/2} \equiv 1 \pmod m$. □

Лемма 26 указывает модули, по которым не существует первообразных корней. Чтобы показать, что по всем остальным модулям первообразные корни существуют, нам понадобится следующее наблюдение.

Лемма 27. *Пусть* p — *нечётное простое и* $k \in \mathbb{N}$. *Пусть* $a, b \in \mathbb{Z}$, $p \nmid ab$. *Тогда*

$$a \equiv b \pmod{p^k} \iff a^p \equiv b^p \pmod{p^{k+1}}. \tag{43}$$

Доказательство. Справедливо тождество

$$a^p - b^p = (a-b)\sum_{j=0}^{p-1} a^{p-1-j}b^j. \tag{44}$$

Независимо от того, предполагаем мы верным левое или правое сравнение в (43), малая теорема Ферма гарантирует, что $a \equiv b \pmod p$. Возьмём целое число c, такое что $ac \equiv 1 \pmod{p^2}$. Тогда $bc \equiv 1 \pmod p$, то есть $bc = 1 + pt$ с некоторым целым t. Стало быть, для каждого слагаемого из правой части (44) справедливо

$$a^{p-1-j}b^j \equiv a^{p-1}(bc)^j \equiv a^{p-1}(1+pt)^j \equiv a^{p-1}(1+jpt) \pmod{p^2}.$$

Получаем, что

$$\sum_{j=0}^{p-1} a^{p-1-j}b^j \equiv a^{p-1}\Big(p + \frac{p-1}{2}p^2t\Big) \equiv pa^{p-1} \pmod{p^2},$$

то есть данная сумма делится на p, но не делится на p^2. Отсюда ввиду тождества (44) немедленно следует равносильность (43). □

Лемма 28. *Пусть* p — *нечётное простое,* g — *первообразный корень по модулю* p *и* $k \in \mathbb{N}$, $k \geqslant 2$. *Тогда* g *является первообразным корнем по модулю* p^k *в том и только том случае, если*

$$g^{p-1} \not\equiv 1 \pmod{p^2} \tag{45}$$

или, что то же самое,

$$g^p \not\equiv g \pmod{p^2}.$$

Доказательство. Поскольку $\varphi(p^k) = p^{k-1}(p-1)$, есть два типа простых делителей $\varphi(p^k)$ — само p и простые делители $p-1$. Пусть q — простой делитель $p-1$. Тогда ввиду малой теоремы Ферма

$$g^{p^{k-1}(p-1)/q} \equiv (g^{p^{k-1}})^{(p-1)/q} \equiv g^{(p-1)/q} \not\equiv 1 \pmod p,$$

ибо g — первообразный корень по модулю p. В частности, $g^{p^{k-1}(p-1)/q} \not\equiv 1 \pmod{p^k}$. Применяя критерий, предоставляемый предложением 5, получаем, что g является первообразным корнем по модулю p^k тогда и только тогда, когда

$$g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Применяя $k-2$ раза лемму 27, приходим к требуемому утверждению. □

Следствие 1. *Пусть p — нечётное простое, $k \in \mathbb{N}$, $k \geqslant 2$. Пусть g — первообразный корень по модулю p^2. Тогда g — первообразный корень и по модулю p^k.*

Доказательство. Достаточно заметить, что соотношение (45) не зависит от k. □

Следствие 2. *Пусть p — нечётное простое, g — первообразный корень по модулю p, h — целое число и $h \equiv g \pmod{p}$. Тогда h является первообразным корнем по модулю p^2 в том и только том случае, если*

$$h \not\equiv g^p \pmod{p^2}.$$

В частности, среди чисел g, $g+p$, $g+2p$, …, $g+(p-1)p$ ровно $p-1$ являются первообразными корнями по модулю p^2.

Доказательство. Достаточно заметить, что в силу леммы 27 сравнение $h \equiv g \pmod{p}$ равносильно сравнению $h^p \equiv g^p \pmod{p^2}$, и воспользоваться леммой 28. □

Упражнение. Пусть p — нечётное простое, g — первообразный корень по модулю p и $t \in \mathbb{N}$. Докажите, что число $g + tp$ является первообразным корнем по модулю p^2 в том и только том случае, если

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

Замечание. Тот факт, что первообразный корень g по модулю p можно «поднять» до первообразного корня по модулю p^2, следует также из леммы Гензеля (см. теорему 18). Рассмотрим многочлен $f(x) = x^{p-1} - 1$. Его производная $(p-1)x^{p-2}$ обращается в ноль по модулю p только на нулевом классе вычетов. Следовательно, среди чисел g, $g+p$, $g+2p$, …, $g+(p-1)p$ ровно одно даёт корень многочлена $f(x)$ по модулю p^2. Стало быть, все остальные являются первообразными корнями по модулю p^2.

Лемма 29. *Пусть p — нечётное простое, $k \in \mathbb{N}$ и g — первообразный корень по модулю p^k. Тогда ровно одно из чисел g, $g+p^k$ является первообразным корнем по модулю $2p^k$, а именно, то из них, которое нечётно.*

Доказательство. Для любого нечётного a и натурального d справедлива равносильность

$$a^d \equiv 1 \pmod{2p^k} \iff a^d \equiv 1 \pmod{p^k}.$$

Стало быть, если a нечётно и не делится на p, то $\operatorname{ord}_{2p^k}(a) = \operatorname{ord}_{p^k}(a)$. Остаётся заметить, что $\varphi(2p^k) = \varphi(p^k)$. □

Теперь мы готовы описать все модули, по которым существуют первообразные корни.

Теорема 28. *По модулю m существуют первообразные корни тогда и только тогда, когда m равно либо 2, либо 4, либо p^k, либо $2p^k$, где p — нечётное простое и $k \in \mathbb{N}$.*

Доказательство. Достаточно применить лемму 26, следствия 1, 2 леммы 28 и лемму 29. □

6.3 Протокол Диффи–Хеллмана построения общего ключа шифрования

Представим себе, что абоненты $\mathcal{A}$ и $\mathcal{B}$, общаясь по открытым каналам, хотят построить *общий ключ шифрования*, то есть некое целое число, которое будет известно лишь им двоим. Для решения этой задачи можно воспользоваться ещё одной односторонней процедурой. Если для алгоритма RSA мы использовали алгоритмическую сложность

задачи факторизации целых чисел, то в данном случае можно воспользоваться алгоритмической сложностью задачи *дискретного логарифмирования*. Если p — простое число, то, как мы показали выше, по модулю p существуют первообразные корни. Пусть g — первообразный корень по модулю p. Тогда для любого $a \in \mathbb{Z}$, не делящегося на p, найдётся единственное $n \in \mathbb{Z}$, такое что

$$a \equiv g^n \pmod{p}, \qquad 0 \leqslant n < p-1.$$

Такое n называется *дискретным логарифмом* a по основанию g. Вычисление g^n по заданным g и n — задача алгоритмически простая. Например, её можно решить при помощи алгоритма быстрого возведения в степень. Восстановление же n по известным g и g^n — задача алгоритмически сложная. В тех же 70-х годах 20-го века этот факт позволил У. Диффи и М. Хеллману придумать метод выработки общего ключа шифрования. Заключается он в следующем.

Абоненты $\mathcal{A}$ и $\mathcal{B}$, общаясь по открытым каналам, выбирают большое простое число p и ищут какой-нибудь первообразный корень g по модулю p. Затем абоненты строят свои собственные секретные ключи: абонент $\mathcal{A}$ выбирает случайное число $d_{\mathcal{A}}$ из промежутка от 1 до $p-1$, а абонент $\mathcal{B}$ выбирает случайное число $d_{\mathcal{B}}$ из того же промежутка. После этого абонент $\mathcal{A}$ вычисляет остаток от деления $g^{d_{\mathcal{A}}}$ на p и посылает его по открытым каналам абоненту $\mathcal{B}$. Абонент $\mathcal{B}$ в свою очередь вычисляет остаток от деления $g^{d_{\mathcal{B}}}$ на p и посылает его по тем же каналам абоненту $\mathcal{A}$. Наконец, абоненты находят число k из промежутка от 1 до $p-1$, определяемое сравнениями

$$k \equiv (g^{d_{\mathcal{A}}})^{d_{\mathcal{B}}} \equiv (g^{d_{\mathcal{B}}})^{d_{\mathcal{A}}} \pmod{p}. \tag{46}$$

Это число и будет общим ключом шифрования. Поскольку абонент $\mathcal{A}$ держит в секрете ключ $d_{\mathcal{A}}$, а $\mathcal{B}$ держит в секрете ключ $d_{\mathcal{B}}$, злоумышленнику алгоритмически крайне сложно по известным ему классам вычетов $\overline{g}$, $\overline{g}^{d_{\mathcal{A}}}$, $\overline{g}^{d_{\mathcal{B}}}$ восстановить $d_{\mathcal{A}}$, $d_{\mathcal{B}}$ и, соответственно, найти k. Отметим также, что и самим абонентам также алгоритмически сложно найти секретные ключи друг друга.

Как правило, когда используют термин *алгоритм*, подразумевают, что у соответствующей процедуры один исполнитель. В описанной же выше схеме построения общего ключа два исполнителя. В такого рода ситуациях часто вместо термина *алгоритм* используют термин *протокол*.

6.4 Криптографическая система Эль-Гамаля

В начале 80-х годов 20-го века Т. Эль-Гамаль, основываясь на конструкции Диффи–Хеллмана, придумал следующий алгоритм шифрования.

Пусть, как и прежде, абонент $\mathcal{B}$ хочет передать абоненту $\mathcal{A}$ натуральное число x. Они строят по описанной выше схеме общий ключ k. То есть они выбирают большое простое число p (заведомо большее, чем x), ищут какой-нибудь первообразный корень g по модулю p и строят свои собственные секретные ключи $d_{\mathcal{A}}$ и $d_{\mathcal{B}}$, после чего вычисляют k в соответствии со сравнением (46).

Дальнейшее предельно просто. Абонент $\mathcal{B}$ перемножает числа k и x, после чего пересылает абоненту $\mathcal{A}$ по открытым каналам остаток r от деления числа kx на p.

Чтобы восстановить передаваемое сообщение, абоненту $\mathcal{A}$ достаточно найти вычет k^{-1}, обратный вычету k по умножению по модулю p, и вычислить остаток от деления числа rk^{-1} на p, ибо

$$rk^{-1} \equiv xkk^{-1} \equiv x \pmod{p}.$$

Отметим, что для надёжности абоненту $\mathcal{B}$ свой секретный ключ $d_{\mathcal{B}}$ полезно создавать заново для каждого нового сообщения. Ибо если для пересылки двух сообщений

x_1, x_2 абонентом $\mathcal{B}$ используется один и тот же ключ $d_{\mathcal{B}}$, то общий ключ k не меняется и для передаваемых чисел r_1 и r_2 в этом случае справедливо

$$r_1 r_2^{-1} \equiv x_1 x_2^{-1} \pmod{p}.$$

То есть, если злоумышленник узнал число x_1, он без труда сможет узнать и число x_2.

6.5 Алгоритм Эль-Гамаля цифровой подписи

Тот же Т. Эль-Гамаль придумал, как использовать алгоритмическую сложность задачи дискретного логарифмирования для построения алгоритма цифровой подписи.

Допустим, абонент $\mathcal{B}$ хочет передать абоненту $\mathcal{A}$ по открытым каналам натуральное число x. Причём требуется, чтобы абонент $\mathcal{A}$ был уверен, что автором сообщения является именно абонент $\mathcal{B}$. Допустим также, что простое число p и первообразный корень g по модулю p найдены и известны обоим абонентам. Тогда абонент $\mathcal{B}$ придумывает не один, а два секретных ключа: натуральные числа $d_{\mathcal{B}}$ и $c_{\mathcal{B}}$, не превосходящие $p-1$, с условием $(c_{\mathcal{B}}, p-1) = 1$. Передача сообщения x осуществляется, например, по описанной выше схеме. Чтобы подтвердить авторство, абонент $\mathcal{B}$ решает сравнение

$$sc_{\mathcal{B}} + d_{\mathcal{B}} g^{c_{\mathcal{B}}} \equiv x \pmod{p-1} \tag{47}$$

относительно s. Оно разрешимо ввиду условия $(c_{\mathcal{B}}, p-1) = 1$. После этого абонент $\mathcal{B}$, помимо уже переданного остатка от деления $g^{d_{\mathcal{B}}}$ на p, передаёт абоненту $\mathcal{A}$ ещё два числа — остаток от деления $g^{c_{\mathcal{B}}}$ на p и остаток от деления s на $p-1$. Эта пара чисел и есть подпись сообщения x.

Удостовериться в авторстве абонент $\mathcal{A}$ может, убедившись в справедливости сравнения

$$g^x \equiv \left(g^{d_{\mathcal{B}}}\right)^{g^{c_{\mathcal{B}}}} \left(g^{c_{\mathcal{B}}}\right)^s \pmod{p}.$$

Ввиду того факта, что g — первообразный корень по модулю p, это сравнение равносильно сравнению (47).

Впоследствии в этой схеме и в различных её модификациях вместо самого числа x стали использовать значение на нём какой-нибудь *хеш-функции*. Но это уже совсем другая история...

7 Бесконечные цепные дроби

Напоследок вернёмся к цепным дробям. Как нетрудно заметить, неполное частное при делении одного целого числа на другое равно целой части их отношения. Это наблюдение позволяет обобщить идею разложения в цепную дробь на случай иррационального числа.

Пусть $\alpha \in \mathbb{R}$. Определим последовательности (α_k) и (a_k) следующим образом:

$$\alpha_0 = \alpha, \qquad \alpha_{k+1} = \frac{1}{\{\alpha_k\}}, \qquad a_k = [\alpha_k], \qquad k = 0, 1, 2, \ldots, \tag{48}$$

где $[\cdot]$ обозначает целую часть числа, $\{\cdot\}$ — дробную. Если α_k оказывается равно целому числу, последовательности обрываются. Понятно, что такое может быть лишь в случае рациональности α. Если же α иррационально, то все α_k также иррациональны и последовательности, стало быть, будут бесконечными. В любом случае, если α_k

корректно определено, имеет место представление α в виде цепной дроби

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{\alpha_k}}}} = [a_0; a_1, \ldots, a_{k-1}, \alpha_k].$$

Коэффициенты a_k, как и в случае конечных цепных дробей, называются *неполными частными*, а рациональные числа $p_k/q_k = [a_0; a_1, a_2, \ldots, a_k]$ — *подходящими дробями* числа α. Иногда α_k называют *хвостом* цепной дроби.

По теореме 7 для любого $k = 0, 1, 2, \ldots$ выполняются рекуррентные соотношения

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2}, \\ q_k &= a_k q_{k-1} + q_{k-2} \end{aligned} \tag{49}$$

(как и прежде, полагаем $p_{-2} = 0$, $q_{-2} = 1$, $p_{-1} = 1$, $q_{-1} = 0$). Из этих соотношений мы вывели (см. следствие из теоремы 7) равенства

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}. \tag{50}$$

7.1 Приближение вещественного числа его подходящими дробями

Теорема 29. *Для подходящих дробей числа α справедливы неравенства*

(1) $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \ldots < \dfrac{p_{2k}}{q_{2k}} < \ldots \leqslant \alpha \leqslant \ldots < \dfrac{p_{2k-1}}{q_{2k-1}} < \ldots < \dfrac{p_3}{q_3} < \dfrac{p_1}{q_1}$;

(2) $q_k > q_{k-1}$ *при каждом* $k \geqslant 2$;

(3) $\left|\alpha - \dfrac{p_k}{q_k}\right| \leqslant \dfrac{1}{q_k q_{k+1}}$ *при каждом* $k \geqslant 0$.

Доказательство. Для любого вещественного β и положительного γ справедливо очевидное неравенство

$$\beta + \frac{1}{\gamma} > \beta.$$

Отсюда легко вывести все неравенства пункта (1).

Далее, поскольку все знаменатели $q_0, q_1, q_2, \ldots$ и все неполные частные $a_1, a_2, a_3, \ldots$ являются числами натуральными, из рекуррентных соотношений (49) следует, что при $k \geqslant 2$

$$q_k = a_k q_{k-1} + q_{k-2} \geqslant q_{k-1} + q_{k-2} > q_{k-1}.$$

Этим мы доказали пункт (2).

Неравенство из пункта (3) следует из соотношения (50) и того факта, что α находится между p_k/q_k и p_{k+1}/q_{k+1}:

$$\left|\alpha - \frac{p_k}{q_k}\right| \leqslant \left|\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}}\right| = \frac{|p_k q_{k+1} - p_{k+1} q_k|}{q_k q_{k+1}} = \frac{1}{q_k q_{k+1}}.$$

□

Упражнение. Докажите, что для знаменателей подходящих дробей справедлива оценка $q_k \geqslant \varphi^{k-1}$, где $\varphi = \frac{1+\sqrt{5}}{2}$ — золотое сечение.

Следствие 1. *Пусть α иррационально. Тогда подходящие дроби числа α сходятся к α. В частности, корректно равенство $\alpha = [a_0; a_1, \ldots, a_k, \ldots]$ между иррациональным числом и его бесконечной цепной дробью.*

Следствие 2 (Теорема Дирихле)**.** *Пусть α иррационально. Тогда существует бесконечно много рациональных чисел p/q, удовлетворяющих неравенству*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Полученную теорему Дирихле можно усилить.

Теорема 30 (Теорема Гурвица)**.** *Пусть α иррационально. Тогда существует бесконечно много рациональных чисел p/q, удовлетворяющих неравенству*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}. \tag{51}$$

Доказательство. Покажем, что существует бесконечно много значений индекса k, для которых знаменатели соответствующих подходящих дробей удовлетворяют неравенству

$$q_{k+1} > \varphi q_k, \tag{52}$$

где $\varphi = \frac{1+\sqrt{5}}{2}$ — золотое сечение. Пусть для некоторого k справедливо $q_{k+1} < \varphi q_k$. Тогда

$$q_{k+2} = a_{k+2}q_{k+1} + q_k \geqslant q_{k+1} + q_k > q_{k+1}(1 + \varphi^{-1}) = \varphi q_{k+1}.$$

Стало быть, действительно, неравенство (52) выполняется бесконечно много раз.

Рассмотрим произвольное k, для которого верно (52). Как мы уже замечали, α находится между p_k/q_k и p_{k+1}/q_{k+1}. Учитывая вновь соотношение (50), получаем, что

$$\left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| = \left|\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}}\right| = \frac{|p_kq_{k+1} - p_{k+1}q_k|}{q_kq_{k+1}} = \frac{1}{q_kq_{k+1}} =$$
$$= \frac{1}{\sqrt{5}q_k^2} + \frac{1}{\sqrt{5}q_{k+1}^2} - \frac{1}{\sqrt{5}q_{k+1}^2}\left(\frac{q_{k+1}^2}{q_k^2} - \sqrt{5}\frac{q_{k+1}}{q_k} + 1\right) < \frac{1}{\sqrt{5}q_k^2} + \frac{1}{\sqrt{5}q_{k+1}^2},$$

ибо $q_{k+1}/q_k > \varphi$, в то время как φ является бóльшим корнем многочлена $x^2 - \sqrt{5}x + 1$.

Из полученного неравенства следует, что хотя бы одна из подходящих дробей p_k/q_k, p_{k+1}/q_{k+1} удовлетворяет неравенству (51). □

Замечание. По сути мы доказали, что среди любых трёх последовательных подходящих дробей числа α хотя бы одна удовлетворяет неравенству (51).

Упражнение. Пользуясь идеями, на которых основывается доказательство теоремы 30, докажите, что среди любых двух последовательных подходящих дробей числа α хотя бы одна удовлетворяет неравенству

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \tag{53}$$

Данное утверждение называется *теоремой Валена.*

Упражнение. Докажите, что если рациональное число p/q удовлетворяет неравенству (53), то оно является какой-то подходящей дробью числа α. Данное утверждение называется *теоремой Лежандра.*

7.2 Цепные дроби квадратичных иррациональностей

Среди всех бесконечных цепных дробей выделяются цепные дроби квадратичных иррациональностей, ибо они и только они, как оказывается, периодичны.

Определение 27. Иррациональное число называется *квадратичной иррациональностью*, если оно является корнем многочлена второй степени с целыми коэффициентами.

Теорема 31 (Теорема Эйлера–Лагранжа)**.** *Иррациональное число является квадратичной иррациональностью тогда и только тогда, когда его цепная дробь периодична (начиная с какого-то момента).*

Доказательство. Пусть α — иррациональное число и последовательности (α_k) и (a_k) определены соотношениями (48).

Вывести квадратичность α из периодичности его цепной дроби довольно просто. Пусть цепная дробь α периодична. Тогда существуют такие индексы n и m, что $0 < n < m$ и $\alpha_n = \alpha_m$. Это даёт соотношение $\alpha_n = [a_n; a_{n+1}, \ldots, a_{m-1}, \alpha_n]$. Нетрудно заметить, что оно равносильно равенству

$$\alpha_n = \frac{A + B\alpha_n}{C + D\alpha_n}$$

с некоторыми целыми A, B, C, D, которое приводит к квадратному уравнению $Dx^2 + (C - B)x - A = 0$, корнем которого является α_n. При этом $D > 0$, поскольку числа $a_n, a_{n+1}, \ldots, a_{m-1}$ — натуральные. Стало быть, α_n является квадратичной иррациональностью. А значит, и $\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n]$ является квадратичной иррациональностью, ибо для любой квадратичной иррациональности β и любого целого a числа $1/\beta$ и $a + \beta$ также являются квадратичными иррациональностями.

Предположим теперь, что α — квадратичная иррациональность. Тогда все α_k также являются квадратичными иррациональностями. Причём для каждого $k \in \mathbb{N}$ справедливо $\alpha_k > 1$, $a_k \in \mathbb{N}$. Пусть A_0, B_0, C_0 — целые числа, такие что

$$A_0\alpha_0^2 + B_0\alpha_0 + C_0 = 0 \qquad \text{и} \qquad A_0C_0 \neq 0.$$

При заданных A_k, B_k, C_k положим

$$A_{k+1} = A_k a_k^2 + B_k a_k + C_k, \qquad B_{k+1} = 2A_k a_k + B_k, \qquad C_{k+1} = A_k.$$

Тогда, поскольку $\alpha_k = a_k + \alpha_{k+1}^{-1}$ и α_k иррационально, для каждого $k \in \mathbb{N}$ также будет выполняться

$$A_k\alpha_k^2 + B_k\alpha_k + C_k = 0 \qquad \text{и} \qquad A_kC_k \neq 0.$$

Покажем, что для бесконечного количества индексов k имеет место неравенство

$$A_kC_k < 0. \tag{54}$$

Предположим противное, то есть что для всех $k \geqslant t$ при некотором натуральном t коэффициенты A_k и C_k имеют одинаковые знаки. Тогда для всех $k > |B_t|/2$ коэффициенты B_{t+k} будут того же знака, что A_{t+k} и C_{t+k}. Но это значит, что оба корня многочлена $A_{t+k}x^2 + B_{t+k}x + C_{t+k}$ отрицательны, что противоречит неравенству $\alpha_{t+k} > 1$. Стало быть, действительно, неравенство (54) выполняется бесконечное количество раз.

Далее, как нетрудно заметить, значение дискриминанта $D = B_k^2 - 4A_kC_k$ не зависит от k. Следовательно, существует бесконечно много индексов k, для которых

$$0 < B_k^2 - 4A_kC_k = D \qquad \text{и} \qquad A_kC_k < 0.$$

Но тогда существуют такие индексы n и m, что $0 < n < m$, $A_n = A_m$, $B_n = B_m$, $C_n = C_m$ и при этом $A_nC_n < 0$. Тогда $A_nx^2 + B_nx + C_n$ и $A_mx^2 + B_mx + C_m$ — один и тот же многочлен, причём его корни имеют разные знаки. Стало быть, положительный его корень равен и α_n, и α_m. А это значит, что цепная дробь числа α периодична. □