Глава 1
Теория делимости

Тот факт, что целое число a *делится* на целое число b будем обозначать $b|a$ (b делит a) или $a{:}b$ (a делится на b). Верны следующие утверждения:

- если $a|b$, $a|c$, то $a|b \pm c$;
- если $a|b$, то $a|bc\ \forall c \in \mathbb{Z}$;
- если $a|b$, $b|a$, то $a = \pm b$.

Теорема 1.1. *Пусть a – целое, b – натуральное. Тогда существуют однозначно определенные $q, r \in \mathbb{Z}$, $0 \leq r < b$ такие, что $a = bq + r$.*

Доказательство. Возьмем наибольшее q такое, что $bq \leq a$. Пусть $r = a - bq$. Очевидно, при этом $r < b$. Допустим также, что $a = bq_1 + r_1$ для некоторых $r_1 < b_1$. Тогда $b(q - q_1) + (r - r_1) = 0$ и делится на b. Значит, $r - r_1{:}b$. Но $|r - r_1| < b$, так что делиться на b оно может быть только будучи равным 0. Но если $r = r_1$, то и $q = q_1$. □

Аналогичная теорема верная для целых $b \neq 0$, если заменить $r < b$ на $r < |b|$.

Наибольшим общим делителем чисел $a_1, \ldots, a_n$ называется наибольшее целое число d такое, что $d|a_i$ для всех $i = \overline{1, n}$. Наибольший общий делитель будем обозначать НОД$(a_1, \ldots, a_n)$ или $(a_1, \ldots, a_n)$.

НОД обладает следующими свойствами:

- если $b|a$, то $(a, b) = b$;
- если $a = bq + c$, то $(a, b) = (b, c)$.

Эти свойства лежат в основе алгоритма Евклида, позволяющего найти наибольший общий делитель двух чисел.

Алгоритм 1.1. (Алгоритм Евклида)
Даны натуральные числа $a > b$. Требуется найти (a, b).

1. Пока $r_j > 0$, выполнять деления с остатком:

$$a = bq_1 + r_1, 0 \leq r_1 < b$$
$$b = r_1q_2 + r_2, 0 \leq r_2 < r_1$$
$$r_1 = r_2q_3 + r_3, 0 \leq r_3 < r_2$$
$$\ldots$$

2. Наибольший общий делитель найти как r_n в последнем делении $r_{n-1} = r_n q_{n+1}$.

В силу свойств НОД, приведенных выше, имеем

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

Сложность алгоритма.

Сложностью алгоритма называется количество выполняемых им операций – как правило битовых, хотя иногда может идти речь, например, о числе операций в группе, индивидуальная сложность которых может зависеть от группы. Сложность должна быть выражена некоторой функцией о длины входа. В нашем случае вход обычно будет характеризоваться какими-то натуральными числами, и под их длиной понимается длина их записи в двоичной системе счисления. Т.е. длина n – это $\log_2 n = \log n$.

Для примера приведем сложности базовых арифметических операций.

1. Сложение и вычитание n-значных (в двоичном представлении) чисел требует $O(n)$ двоичных операций.

2. Умножение в столбик n-значных чисел требует $O(n^2)$ двоичных операций. Действительно, каждый разряд одного числа перемножается с каждый разрядом другого – $n^2 = O(n^2)$ операций, после чего производится сложение n не более чем $(n+1)$-значных чисел – каждое сложение за $O(n)$ операций.

3. Деление в столбик n-значных чисел требует $O(n^2)$ двоичных операций.

Для больших чисел, однако, существуют и более быстрые алгоритмы. Например алгоритм умножения Карацубы имеет сложность всего лишь $O(n^{\log 3})$, алгоритм Шёнхаге-Штрассена – $O(n \log n \log\log n)$. Оптимизация деления может осуществляться в том числе за счет использования более быстрого алгоритма умножения.

Говорят, что перечисленные выше действия обладают *полиномиальной* сложностью. Кроме полиномиальных выделяют экспоненциальные и субэкспоненциальные алгоритмы.

Теорема 1.2. *Алгоритм Евклида для нахождения НОД чисел $a > b$ требует $O(\log^3 a)$ бинарных операций.*

Доказательство. Для начала оценим количество делений, которые потребуется выполнить. Для этого покажем, что $r_{j+2} < r_j/2$. Если $r_{j+1} \le r_j/2$, то, очевидно $r_{j+2} < r_{j+1} \le r_j/2$. Иначе, $r_j = 1 \cdot r_{j+1} + r_{j+2}$, а значит, $r_{j+2} = r_j - r_{j+1} < r_j - r_j/2 = r_j/2$.

Итак, если $r_{j+2} < r_j/2$, т.е. остаток уменьшается хотя бы в 2 раза за каждые 2 шага, потребуется не больше $2\log a = O(\log a)$ шагов прежде чем будет получен 0.

Само деление чисел, не превосходящих a, может быть выполнено за $O(\log^2 a)$ двоичных операций. Таким образом, весь алгоритм, требует $O(\log^3 a)$ двоичных операций. $\square$

Очевидно, при одном и том же a число операций может сильно различаться в зависимости от b. Определим худший возможный вход для алгоритма Евклида. Под этим будем понимать наименьшие значения a и b, для которых алгоритм должен будет сделать n шагов, в зависимости от n. Т.к. a и b – пара чисел, не очень понятно, как она может быть меньше или больше другой пары. Будем говорить, что пара a, b (где $a > b$) меньше пары a', b' если $a < a'$ или $a = a'$ и $b < b'$. Покажем, что худшими значениями для a и b являются числа Фибоначчи.

Теорема 1.3. *Пусть $a > b > 0$, алгоритм Евклида выполняет n шагов для нахождения (a, b), и это наименьшая пара, обладающая данным свойством. Тогда $a = F_{n+2}$, $b = F_{n+1}$.*

Доказательство. Для начала покажем, что $a \geq F_{n+2}$, $b \geq F_{n+1}$ с помощью индукции по n. При $n = 1$ в алгоритме должно произойти всего одно деление, $r_{-1} = a = bq_1 = r_0 q_1$, и раз $a > b$, то наименьшая возможная пара это 2 и 1.

Пусть утверждение верно для всех $j < n$. Тогда на первом шаге алгоритма устанавливается, что $r_{-1} = r_0 q_1 + r_1$ и (r_0, r_1) находится за $n - 1$ шаг. Тогда $r_0 \geq F_{n+1}$, $r_1 \geq F_n$ по предположению индукции. Но из этого следует, что $r_{-1} \geq r_0 + r_1 \geq F_{n+2}$.

Осталось показать, что если $a = F_{n+2}$, $b = F_{n+1}$, алгоритму действительно потребуется n шагов. Заметим, что $F_{n+2} = F_{n+1} \cdot 1 + F_n$, где $0 < F_n < F_{n+1}$ – т.е. получено разложение из теоремы 1.1, которое является единственным. Это означает, что остаток, находимый на каждом следующем шаге алгоритма Евклида, будет равен предыдущему числу Фибоначчи, а неполное частное – единице (за исключением последнего шага, т.к. $2 = 2 \cdot 1$, т.е. остаток равен 0, а частное 2). Если в ходе алгоритма деление выполняется для всех чисел Фибоначчи между F_{n+2} и $F_3 = 2$ включительно, то было выполнено как раз n делений. $\square$

Теорема 1.4. *Пусть $a, b, c \in \mathbb{Z}$. Уравнение $au + bv = c$ имеет целые решения тогда и только тогда, когда $(a, b)|c$. Число этих*

решений бесконечно и они имеют вид

$$\begin{aligned} x &= x_0 + \frac{b}{(a,b)}t, \\ y &= y_0 - \frac{a}{(a,b)}t, \end{aligned} \tag{1.1}$$

где $t \in \mathbb{Z}$, а (x_0, y_0) – какое-то частное решение.

Доказательство. Утверждение о существовании решений довольно очевидно. Если левая часть делится на (a, b), то и правая должна делиться на (a, b), из чего следует необходимость. Если же $(a, b)|c$, то хотя бы одно решение можно получить с помощью расширенного алгоритма Евклида. Пусть $au + bv = (a, b)$, тогда частным решением уравнения будут $x_0 = \frac{uc}{(a,b)}$, $y_0 = \frac{vc}{(a,b)}$.

Теперь покажем, что все решения представимы в виде (1.1). Рассмотрим сначала однородное диофантово уравнение $ax + by = 0$. Пусть $(a, b) = d$, $a = a_1 d$, $b = b_1 d$. Т.к. $x = -\frac{by}{a} = -\frac{b_1 y}{a_1}$, то, чтобы он был целым, y должен иметь вид $a_1 t$. Можно убедиться, что при любом $t \in \mathbb{Z}$ пара $x = -b_1 t$, $y = a_1 t$ является решением.

Перейдем к неоднородному случаю. Пусть x_0, y_0 – частное решение, x', y' – любое другое решение. Тогда имеем

$$(ax_0 + by_0) - (ax' + by') = a(x_0 - x') + b(y_0 - y') = 0.$$

Полученное можно рассмотреть как однородное диофантово уравнение, все решения которого находятся как $x_0 - x' = -b_1 t$, $y_0 - y' = a_1 t$, $t \in \mathbb{Z}$. Таким образом, любое решение $ax + by = c$ представимо в виде $x' = x_0 + \frac{b}{(a,b)}t$, $y' = y_0 - \frac{a}{(a,b)}t$. Легко убедиться, что эта пара действительно является решением при любом целом t. $\square$

Взаимно простыми называются числа, чей НОД равен 1.

Следствие 1.1 Целые числа a и b взаимно просты тогда и только тогда, когда уравнение $au + bv = 1$ разрешимо в целых числах.

Расширенный алгоритм Евклида позволяет найти u и v, для которых $au + bv = (a, b)$. Одновременно с остатками и неполными частными для этого вычисляются две вспомогательные последовательности.

Алгоритм 1.2. (Расширенный алгоритм Евклида)

Пусть $a > b > 0$, и на n-ом шаге алгоритма Евклида получено $r_{n-2} = q_n r_{n-1} + (a, b)$. Положим

$$r_{-1} = a, r_0 = b;$$
$$x_{-1} = 1, y_{-1} = 0;$$
$$x_0 = 0, y_0 = 1.$$

Остальные члены вычисляются рекуррентно следующим образом:

$$r_i = r_{i-2} - q_i r_{i-1},$$
$$x_i = x_{i-2} - q_i x_{i-1},$$
$$y_i = y_{i-2} - q_i y_{i-1}.$$

Тогда $ax_n + by_n = (a, b)$.

Наименьшим общим кратным чисел $a_1, \ldots, a_n$ называется наименьшее целое число m такое, что $m \vdots a_i$ для всех $i = \overline{1, n}$. Наименьшее общее кратное будем обозначать НОК$(a_1, \ldots, a_n)$ или $[a_1, \ldots, a_n]$.

НОК обладает следующими свойствами:

- любое общее кратное чисел a и b делится на $[a, b]$;
- $[a, b] = \frac{ab}{(a,b)}$.

Приведенные определения НОД и НОК работают для натуральных чисел и задают НОД и НОК однозначно. В дальнейшем однако эти понятия будут обобщены на кольца, в которых элементы могут быть и не упорядочены, из-за чего понятия «наибольший» и «наименьший» теряют смысл. Максимальность и минимальность будет устанавливаться в первую очередь по включению, и НОД и НОК уже не будут определены однозначно.

Натуральное число n называется *простым*, если его натуральными делителями являются лишь 1 и само число n. Другие натуральные числа, большие 1, называются *составными*. Простые числа обладают следующими свойствами:

- если $(p, a) \neq 1$, то $a \vdots p$;
- если $p | a_1 \ldots a_n$, то одно из a_i делится на p.

Теорема 1.5. (Основная теорема арифметики) *Всякое натуральное число, большее 1, раскладывается в произведение простых множителей, и это разложение единственно с точностью до порядка следования множителей.*

Доказательство. Если a не простое, то $a = p_1 a_1$, где p_1 – наименьший простой делитель a. Если и a_1 – не простое, то $a_1 = p_2 a_2$. При этом $a_{i+1} < a_i$, а значит, эта процедура не может продолжаться вечно. Следовательно, существует разложение $a = p_1 p_2 \dots p_n$. Пусть есть еще одно разложение: $a = q_1 q_2 \dots q_m$. Тогда

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

Значит, p_1 делит хотя бы одно из чисел в правой части – например, q_1. Но т.к. все они простые, из этого следует $p_1 = q_1$. Сократим на них и повторим те же рассуждения для равенства

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

и так далее. Сократив по очереди все множители, получим тождественность двух разложений. $\square$

Каноническое разложение – запись разложения на простые множители, где повторяющиеся множители объединены под степенью:

$$a = p_1^{k_1} \dots p_n^{k_n}$$

Глава 2
Сравнения

2.1. Классы вычетов

Будем рассматривать остатки от деления целых чисел на некоторое число m, которое назовем *модулем*. Если числа a и b имеют один и тот же остаток при делении на m, они называются *сравнимыми* по модулю m. Сравнимость обозначается как

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

Сравнимость является отношением эквивалентности:

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

Приведем еще несколько свойств сравнений

1. если $a \equiv b \pmod{m}$, то $ca \equiv cb \pmod{m}$;
2. если $ca \equiv cb \pmod{m}$, $(c, m) = 1$, то $a \equiv b \pmod{m}$;
3. если $c \neq 0$, то сравнение $a \equiv b \pmod{m}$ выполняется тогда и только тогда, когда $ca \equiv cb \pmod{cm}$;
4. если $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$;
5. если $a \equiv b \pmod{m}$, то $a^k \equiv b^k \pmod{m}$ для любого натурального k;
6. если $a \equiv b \pmod{m}$, то $f(x)$ – многочлен с целыми коэффициентами, то $f(a) \equiv f(b) \pmod{m}$;
7. $a \equiv b \pmod{m_1}, \ldots, a \equiv b \pmod{m_k}$, тогда и только тогда, когда $a \equiv b \pmod{[m_1, \ldots, m_k]}$;
8. если $a \equiv b \pmod{m}$ и $d|m$, то $a \equiv b \pmod{d}$;

9. если $a^k \equiv b^k \pmod m$ и $k|n$, то $a^n \equiv b^n \pmod m$, где k, n – натуральные числа.

Для $a \in Z$, обозначим через $\overline{a}$ множество $\{a+mt|t \in \mathbb{Z}\}$, которое будем называть *классом вычетов по модулю* m. Очевидно, $\overline{a} = \overline{b}$ тогда и только тогда, когда $a \equiv b \pmod m$. Далее будем также писать

$$a = b \pmod m,$$

имея в виду, что a – остаток при делении b на m (т.е. наименьший неотрицательный вычет из класса $\overline{b}$).

Множество всех классов вычетов $\{\overline{a}|a = 0, \ldots, m-1\}$ называется *полной системой вычетов по модулю* m и обозначается $\mathbb{Z}_m$. На множестве $\mathbb{Z}_m$ вводятся операции сложения и умножения классов по правилам:

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

Подмножество множества $\mathbb{Z}_m$, которое состоит из классов вычетов $\overline{a}$ таких, что $(a, m) = 1$, называется *приведенной системой вычетов* и обозначается через $\mathbb{Z}_m^*$. Иногда вместо классов вычетов будем выбирать по одному их представителю, и полученные множества также называть полной и приведенной системами вычетов.

Утверждение 2.1. *Если* $(a, m) = 1$ *и* x *пробегает полную систему вычетов по модулю* m*, то* $ax + b$ *тоже пробегает полную систему вычетов по модулю* m

Доказательство. Как и x, $ax + b$ принимает m разных значений. Значит остается показать, что эти значения несравнимы по модулю m. Действительно, если $ax_1 + b \equiv ax_2 + b \pmod m$, то $ax_1 \equiv ax_2 \pmod m$ (свойство 7), откуда $x_1 \equiv x_2 \pmod m$ (свойство 5) – противоречие. □

Утверждение 2.2. *Если* $(a, m) = 1$ *и* x *пробегает приведенную систему вычетов по модулю* m*, то* ax *тоже пробегает приведенную систему вычетов по модулю* m*.*

Доказательство. Различных значений ax будет столько же, сколько различных значений x, и остается показать, что все ax будут несравнимы по модулю m и взаимно просты с этим модулем. Первое снова следует из свойства 5, второе – из того что $(a, m) = 1$ и $(x, m) = 1$. □

2.2. Функция Эйлера

Функция Эйлера $\varphi(m)$ – количество натуральных чисел, меньших m, и взаимно простых с ним. Также $\varphi(1)$ принимается равным 1.

Очевидно, для простого числа $\varphi(p) = p - 1$. Для составных чисел значение функции Эйлера позволяют вычислить следующие утверждения.

Утверждение 2.3. *Пусть p – простое. Тогда $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Доказательство. Числа, не взаимно простые с p^α – это ровно те числа, которые делятся на p. В промежутке от 1 до p^α таких $p^{\alpha-1}$, т.е. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. $\square$

Утверждение 2.4. *(Мультипликативность) Если $(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$.*

Доказательство. Числа от 1 до mn запишем в таблицу с m строками и n столбцами, помещая числи от 1 до n по порядку в первую строку, от $n + 1$ до $2n$ – во вторую, и т.д. Число, стоящее в i-ой строке, j-ом столбце, равно $n(i-1)+j$, и оно взаимно просто с n тогда и только тогда, когда j взаимно просто с n. Таким образом, взаимно простым с n будет весь столбец целиком, и таких столбцов существует $\varphi(n)$. Согласно утверждению 2.1, остатки при делении на m в одном таком столбце различны. Значит, среди чисел в одном столбце ровно $\varphi(m)$ будут взаимно просты с m, и всего получаем $\varphi(m)\varphi(n)$ чисел. $\square$

Таким образом, имея каноническое разложение, можем записать явную формулу для функции Эйлера:

$$\varphi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = p_1^{\alpha_1-1} \dots p_k^{\alpha_k-1}(p_1 - 1) \dots (p_k - 1).$$

Утверждение 2.5. *Сумма $\varphi(d)$, где d пробегает все различные делители числа n, равна n.*

Доказательство. Пусть $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Рассмотрим выражение

$$(\varphi(1) + \varphi(p_1) + \dots + \varphi(p_1^{\alpha_1})) \dots (\varphi(1) + \varphi(p_k) + \dots + \varphi(p_k^{\alpha_k})). \quad (2.1)$$

После раскрытия скобок имеем все возможные $\prod_{i=1}^{k} \varphi(p^{\beta_i})$, где $0 \le \beta_i \le \alpha_i$. Заменяя каждое произведение на $\varphi\left(\prod_{i=1}^{k} p^{\beta_i}\right)$ в соответствии со свойством мультипликативности, получаем как раз $\sum_{d|n} \varphi(n)$ из условия теоремы.

Однако

$$\begin{aligned} &\varphi(1) + \varphi(p) + \dots + \varphi(p^\alpha) = \\ &= 1 + p - 1 + p^2 - p + \dots + p^\alpha - p^{\alpha-1} = p^\alpha, \end{aligned}$$

и подставляя этот результат в (2.1), получаем n. $\square$

Теорема 2.1. *(Теорема Эйлера) При $m > 1$ и $(a, m) = 1$ имеем*

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

Доказательство. Пусть x пробегает приведенную систему вычетов $r_1, \ldots, r_{\varphi(m)}$, $0 < r_i < m$. Тогда, согласно утверждению 2.2, остатки при делении ax на m пробегают ту же систему вычетов, но в другом порядке. Перемножая почленно все сравнения $ar_i \equiv r_k \pmod{m}$, получим

$$a^{\varphi(m)} r_1 \ldots r_{\varphi(m)} \equiv r_1 \ldots r_{\varphi(m)} \pmod{m}.$$

Т.к. $(r_1 \ldots r_{\varphi(m)}, m) = 1$, можем на него разделить и получить $a^{\varphi(m)} \equiv 1 \pmod{m}$. $\square$

Частным случаем теоремы Эйлера для простых модулей является теорема Ферма.

Теорема 2.2. *(Теорема Ферма) При простом p и a, не делящемся на p, имеем*

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

2.3. Линейные сравнения

Пусть a, m – ненулевые целые числа. Рассмотрим сравнение

$$ax \equiv b \pmod{m}. \tag{2.2}$$

Говорят, что сравнение имеет столько решений, сколько вычетов полной системы ему удовлетворяет. Пусть $(a, m) = 1$. Тогда если x пробегает полную систему вычетов, то и ax пробегает полную систему вычетов. Следовательно, только одно ax_i может быть сравнимо с b.

Пусть теперь $(a, m) = d$. В таком случае чтобы сравнение вообще имело решения, необходимо, чтобы и b делилось на d. Тогда пусть $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. По свойству 3 сравнение (2.2) равносильно сравнению

$$a_1 x \equiv b_1 \pmod{m_1}, \tag{2.3}$$

которое, как уже установлено, имеет единственное решение. Но нас интересуют x по модулю m, а не m_1. Пусть x_1 – наименьший неотрицательный вычет решения (2.3). Тогда все остальные вычеты имеют вид $x = m_1 t + x_1$, $t \in \mathbb{Z}$. Однако по модулю m некоторые из них

различаются, а именно – те, у которых $0 \leq t < d$. Т.е. сравнение (2.2) имеет d решений:

$$x_1, x_1 + m_1, \ \ldots, x_1 + (d-1)m_1.$$

Таким образом, доказана следующая теорема.

Теорема 2.3. *Пусть $(a, m) = d$. Если b не делится на d, то сравнение $ax \equiv b \pmod{m}$ не имеет решений. В противном случае сравнение имеет d решений.*

Из определения сравнения следует, что существует такой $y \in \mathbb{Z}$, что

$$ax - ym = b.$$

Тогда для нахождения частного решения сравнения 2.2 можно воспользоваться расширенным алгоритмом Евклида **??**. Находим линейное разложение НОД $(a, m) = a\alpha + m\beta$ и полагаем $x_0 = \frac{\alpha b}{(a,m)}$. Все решения находим как

$$\left\{ x_0 + \frac{mt}{(a,m)} | t = \overline{0, d-1} \right\}.$$

Решение линейного сравнения также можно находить используя свойства сравнений.

2.4. Системы линейных сравнений

Пусть $a_1, \ldots, a_k$, $M_1, \ldots, M_k$ – целые ненулевые числа. Систему сравнений

$$\begin{cases} a_1 x \equiv b_1 \pmod{M_1} \\ \ldots \\ a_k x \equiv b_k \pmod{M_k} \end{cases}$$

можно свести к системе вида

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ \ldots \\ x \equiv c_r \pmod{m_r} \end{cases}, \tag{2.4}$$

где модули m_i попарно взаимно простые, с помощью решения каждого отдельного уравнения по своему модулю и используя свойства сравнений.

Теорема 2.4. (Китайская теорема об остатках) *Решение системы 2.4 задается следующим образом:*

$$x \equiv c_1 x_1 \frac{m}{m_1} + \ldots + c_r x_r \frac{m}{m_r} \pmod{m},$$

где $m = m_1 \ldots m_r$, x_i *– произвольные целые числа, удовлетворяющее сравнению* $x_i \frac{m}{m_i} \equiv 1 \pmod{m_i}$, $i = 1, \ldots, r$.

Доказательство. Обозначим $x_0 = c_1 x_1 \frac{m}{m_1} + \ldots + c_r x_r \frac{m}{m_r}$. Т.к. все $\frac{m}{m_i}$, $i \neq j$, делятся на m_j, то действительно имеем $x_0 \equiv c_j x_j \frac{m}{m_j} \equiv c_j \pmod{m_j}$. Отсюда следует, что система (2.4) равносильна системе

$$\begin{cases} x \equiv x_0 \pmod{m_1} \\ \ldots \\ x \equiv x_0 \pmod{m_r} \end{cases}, \tag{2.5}$$

Согласно свойству 7, этой системе удовлетворяют только $x \equiv x_0 \pmod{m}$. $\square$

Пример 2.1. Найти решение системы сравнений

$$\begin{cases} 5x \equiv 8 \pmod{12} \\ 7x \equiv 16 \pmod{18} \\ 11x \equiv 8 \pmod{42} \end{cases}$$

Прибавим 12 к правой части первого сравнения и сократим обе части на 5, получим

$$x \equiv 4 \pmod{12}.$$

Прибавим 54 к правой части второго сравнения и сократим обе части на 7, получим

$$x \equiv 10 \pmod{18}.$$

Найдем решение сравнения $11x \equiv 8 \pmod{42}$ с помощью расширенного алгоритма Евклида (алгоритм 1.2).

$$\begin{aligned} 42 &= 3 \cdot 11 + 9 \\ 11 &= 1 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

Из разложения $42x'+11y' = 1$ нас интересует только y. Вычислим его рекурсивно

$$\begin{aligned} &y_{-1} = 0,\\ &y_0 = 1,\\ &y_1 = 0 - 3 = -3,\\ &y_2 = 1 - (-3) = 4,\\ &y_3 = -3 - 4 \cdot 4 = -19. \end{aligned}$$

Таким образом,

$$x \equiv -19 \cdot 8 \equiv 16 \pmod{42}.$$

Итого получаем систему

$$\begin{cases} x \equiv 4 \pmod{12} \\ x \equiv 10 \pmod{18} \\ x \equiv 16 \pmod{42} \end{cases}$$

Сведем эту систему к системе с *примарными* (т.е. вида p^α) модулями

$$\begin{cases} x \equiv 4 \pmod{3} \\ x \equiv 4 \pmod{4} \\ x \equiv 10 \pmod{2} \\ x \equiv 10 \pmod{9} \\ x \equiv 16 \pmod{2} \\ x \equiv 16 \pmod{3} \\ x \equiv 16 \pmod{7} \end{cases}$$

Третье и пятое сравнения вытекают из второго, поэтому их можно удалить. Аналогично первое и шестое сравнения можно удалить как следствия четвертого сравнения. Убираем избыточные сравнения и берем по модулю правые части сравнений

$$\begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 2 \pmod{7} \\ x \equiv 1 \pmod{9} \end{cases}$$

Решение полученной системы найдем с помощью китайской теоремы об остатках. Найдем числа x_2, x_3 из сравнений

$$\begin{aligned} &4 \cdot 9 \cdot x_2 \equiv 1 \pmod{7},\\ &4 \cdot 7 \cdot x_3 \equiv 1 \pmod{9}. \end{aligned}$$

Получаем $x_2 = x_3 = 1$. Заметим, что x_1 нет надобности находить, поскольку правая часть первого сравнения равна нулю. Окончательно получаем

$$x \equiv 2 \cdot 1 \cdot 4 \cdot 9 + 1 \cdot 1 \cdot 4 \cdot 7 \pmod{4 \cdot 9 \cdot 7} \equiv 100 \pmod{252}.$$

2.5. Полиномиальные сравнения

Пусть p – простое. В силу теоремы Ферма сравнение вида

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

равносильно некоторому сравнению

$$b_{p-1} x^{p-1} + \cdots + b_1 x + b_0 \equiv 0 \pmod{p}.$$

Чтобы привести его к этому виду, надо найти остаток от деления исходного многочлена на $x^p - x \equiv 0 \pmod{p}$.

Теорема 2.5. *Сравнение n-ой степени по простому модулю p имеет не более n решений, или все его коэффициенты кратны p.*

Заметим, что для составного модуля это неверно: например $x^2 - 1 \equiv 0 \pmod{8}$ имеет 4 решения: 1, 3, 5, 7. Дело в том, что для доказательства этой теоремы используется отсутствие в $\mathbb{Z}_p$ делителей нуля. Например, если $(x-1)(x+1) \equiv 0 \pmod{7}$, это значит, что или $x-1$, или $x+1$ делится на 7, что дает только 2 решения – не больше, чем скобок в разложении. Если же модуль составной, то вовсе не обязательно один из множителей, полученный при разложении многочлена, делится на этот модуль целиком.

В дальнейшем нам понадобится следующее утверждение, доказательство которого как раз использует теорему о числе решений.

Теорема 2.6. (Критерий простоты Вильсона) *Число p простое тогда и только тогда, когда*

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

Доказательство. Для $p = 2$ теорема очевидна. Пусть $p > 2$ – простое. Рассмотри сравнение

$$(x-1)\ldots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Его степень $p-2$, но оно имеет хотя бы $p-1$ решение – все ненулевые вычеты по модулю p. Значит, все его коэффициенты делятся на p, включая свободный член $(p-1)! + 1$.

Обратно, допустим $(p-1)! \equiv -1 \pmod{p}$. Если бы $p > 3$ было составным, то среди чисел от 1 до $p-1$ нашелся бы его нетривиальный делитель, однако -1 ни на какой такой делитель не делится. $\square$

Теорема 2.7. *Сравнение $f(x) \equiv 0 \pmod{m}$, где $m = m_1 \dots m_k$, m_i попарно взаимно простые, эквивалентно системе*

$$\left\{ f(x) \equiv 0 \pmod{m_1} \dots f(x) \equiv 0 \pmod{m_k} \right. .$$

При это если число решений i-ого сравнения системы равно T_i, то число решений исходного сравнения равно $T_1 \dots T_k$.

Таким образом, решение сравнения по модулю $m = p_1^{\alpha_1} \dots p_l^{\alpha_k}$ сводится к решению сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}. \tag{2.6}$$

В свою очередь сравнение (2.6) сводится к сравнениям по простому модулю.

Как известно, многочлен $f(x)$ можно разложить по степеням $(x-a)$, воспользовавшись формулой Тейлора или делением на $x-a$ с остатком. Из второго способа следует, что в нашем случае все коэффициенты будут целыми. Следующий способ основан на последовательном решении сравнения для все больших степеней p с использованием этого разложения.

Если выполняется сравнение (2.6), то выполняется и

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

Предположим, что мы знаем, как найти решения сравнения по простому модулю, и в данном случае эти решения – x_1, ..., x_k. Тогда решение (2.6) должно записываться в виде $x = x_i + tp$, $i = \overline{1,k}$.

Если выполняется сравнение (2.6) и решение имеет вид $x_i + tp$, то выполняется и

$$f(x_i + tp) \equiv 0 \pmod{p^2}.$$

Разложим многочлен по степеням $x - x_i = tp$:

$$f(x_i+tp) = \left(\left(\dots \left(\frac{f^{(n)}}{n!} tp + \frac{f^{(n-1)}}{(n-1)!} \right) \dots \right) tp + \frac{f'(x_i)}{1!} \right) tp + f(x_i).$$

Заметим, что если рассматривать его как многочлен от t, то коэффициенты при всех степенях выше первой делятся на p^2. Поэтому

по модулю p^2 у нас остается сравнение

$$f(x_i) + tpf'(x_i) \equiv 0 \pmod{p^2}.$$

Т.к. $f(x_i) \vdots p$, его можно свести к сравнению

$$\frac{f(x_i)}{p} + tf'(x_i) \equiv 0 \pmod{p}.$$

Это линейное сравнение может иметь единственное решение, не иметь их вовсе или выполняться при любом t. Если решений нет, то их нет и у сравнения (2.6), в противном случае для каждого решения $t_{i,j}$ представляем решение исходного сравнения в виде

$$x = x_i + t_{i,j}p + sp^2 = x_{i,j} + sp^2$$

Если выполняется сравнение (2.6), то выполняется и

$$f(x_{i,j} + sp^2) \equiv 0 \pmod{p^3}.$$

Снова разложим многочлен по степеням – на этот раз $x - x_{i,j}$ – и получим, что все коэффициенты, кроме первых двух должны быть кратны p^3. Таким образом, остается сравнение

$$f(x_{i,j}) + sp^2 f'(x_{i,j}) \equiv 0 \pmod{p^3},$$

которое, в силу $f(x_{i,j}) \vdots p^2$, равносильно линейному сравнению по простому модулю:

$$\frac{f(x_{i,j})}{p^2} + sf'(x_{i,j}) \equiv 0 \pmod{p}.$$

Находим решения этого сравнения и переписываем наше общее решение в виде

$$x = x_{i,j} + s_{i,j,l}p^2 + rp^3 = x_{i,j,l} + rp^3.$$

Алгоритм продолжается, пока не дойдет до p^α.

Пример 2.2. Решить сравнение

$$x^{10} - 51x^9 + 3x^5 - 6001x - 81 \equiv 0 \pmod{675}.$$

Разложим на множители модуль: $675 = 5^2 \cdot 3^3$. Таким образом, сравнение сводится к системе:

$$\begin{cases} x^{10} - 51x^9 + 3x^5 - 6001x - 81 \equiv 0 \pmod{25} \\ x^{10} - 51x^9 + 3x^5 - 6001x - 81 \equiv 0 \pmod{27} \end{cases}.$$

Начнем с решения первого сравнения. Согласно описанному методу, сначала надо решить его по модулю 5. Используя теорему Ферма и заменяя коэффициенты их остатками при делении на 5, получим $x^2 + x - 1 \equiv 0 \pmod{5}$. Отметим, что теорему Ферма применять можно только если $x \not\equiv 0 \pmod{5}$ – можно проверить, что это так, и $x = 0$ не является решением. Перебором находим, что у этого сравнения единственное решение: $x_1 = 2$. Тогда решение по модулю 25 имеет вид $x = 2 + 5t$.

Для решения по модулю 25 вычислим $\frac{f(2)}{5} + tf'(2) \equiv 120 + 3055t \pmod{5}$. Это сравнение верно при любом t, поэтому получаем 5 различных значений для x: 2, 7, 12, 17 и 22.

Перейдем теперь ко второму сравнению в системе. Запишем его по модулю 3 – снова используя теорему Ферма и заменяя коэффициенты их остатками. Получим $1 - x \equiv 0 \pmod{3}$, т.е. $x = 1$ – решение. Однако в этот раз $x = 0$, для которого теорему Ферма использовать нельзя, тоже удовлетворяет сравнению. Т.е. имеем два решения по модулю 3: $x_1 = 0$, $x_2 = 1$.

Переходя к модулю 9, находим

$$\frac{f(0)}{3} + tf'(0) \equiv -7t \pmod{3}$$

и

$$\frac{f(1)}{3} + tf'(1) \equiv 45t \pmod{3}.$$

В первом случае 0 будет получаться только при $t = 0$, таким образом $x_{1,1} = 0 + 3 \cdot 0 = 0$. Во втором все вычеты по модулю 3 дают 0, поэтому $x_{2,1} = 1 + 0 = 1$, $x_{2,2} = 1 + 3 = 4$, $x_{2,3} = 1 + 6 = 7$.

Наконец, для перехода к модулю 27 вычисляем

$$\frac{f(0)}{9} + sf'(0) \equiv -7s \pmod 3$$
$$\frac{f(1)}{9} + sf'(1) \equiv -7s \pmod 3$$
$$\frac{f(4)}{9} + sf'(4) \equiv 204228 + 4394745s \equiv 0 \pmod 3$$
$$\frac{f(7)}{9} + sf'(7) \equiv 44842938 + 559221705s \equiv 0 \pmod 3$$

В первых двух сравнениях 0 получится только при $s = 0$, в оставшихся двух – при любом s. Таким образом, можем записать все решения второго сравнения исходной системы: 0, 1, 4, 13, 22, 7, 16, 25.

Чтобы найти решения исходного сравнения, нужно взять все возможные пары решений по модулям 25 и 27 и составить из них систему линейных уравнений, которая решается с помощью китайской теоремы об остатках. Например,

$$\begin{cases} x \equiv 2 \pmod{25} \\ x \equiv 0 \pmod{27} \end{cases}$$

дает решение $x \equiv 27 \pmod{675}$ для исходного сравнения. Приведем для проверки все множество решений:

$$27, 432, 162, 567, 297, 652, 382, 112, 517, 247, 202, 607, 337, 67,$$
$$472, 427, 157, 562, 292, 22, 277, 7, 412, 142, 547, 502, 232, 637,$$
$$367, 97, 52, 457, 187, 592, 322.$$

2.6. Сравнения второй степени

2.6.1. Квадратичные вычеты по простому модулю

В этой главе подробно остановимся на решении сравнений вида

$$x^2 \equiv a \pmod m, (a, m) = 1 \tag{2.7}$$

Говорят, что a – *квадратичный вычет* по модулю m, если такое сравнение имеет решение. Аналогично вводится понятие вычета степени n. В противном случае a называется невычетом.

Начнем с рассмотрения случая, когда $m = p$ – простое нечетное. Тогда если a – квадратичный вычет по модулю p, сравнение (2.7) имеет ровно 2 решения. Действительно, пусть x_0 – одно известное решение. Тогда $a \equiv x_0^2 \pmod{p}$ и сравнение можно переписать в виде

$$(x - x_0)(x + x_0) \pmod{p}.$$

Очевидно, его решениями будут только x_0 и $-x_0$, причем в силу нечетности модуля они различны.

Утверждение 2.6. *Приведенная система вычетов по простому нечетному модулю p имеет $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов.*

Доказательство. Рассмотрим приведенную систему вычетов

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

Можно видеть, что существует $\frac{p-1}{2}$ вычетов по модулю p, являющихся квадратичными вычетами и сравнимых с $1, 2, \ldots, \left(\frac{p-1}{2}\right)^2$. При этом никакие два из этих квадратов не сравнимы друг с другом, ведь если $k^2 \equiv l^2 \pmod{p}$, $1 \leq k < l \leq \frac{p-1}{2}$, то сравнение $x^2 \equiv k^2 \pmod{p}$ имеет уже не 2, а 4 решения $k, -k, l, -l$. $\square$

Для числа квадратичных вычетов по составному модулю тоже существует формула, хотя весьма громоздкая – формула Стангла.

Теорема 2.8. *Если a – квадратичный вычет по модулю p, то*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{2.8}$$

Если a – квадратичный невычет по модулю p, то

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{2.9}$$

Доказательство. Т.к. по малой теореме Ферма $a^{p-1} \equiv 1 \pmod{p}$, можем записать

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

Оба множителя правой части не могут одновременно делиться на p, ведь тогда на p должна была бы делиться их разность, равная 2. Значит, имеет место только одно из сравнений (2.8), (2.9). Но если a – квадратичный вычет, то

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

При этом у сравнения (2.8) всего $\frac{p-1}{2}$ решений, поэтому квадратичными вычетами они исчерпываются. Для квадратичных невычетов в таком случае должно выполняться сравнение (2.9). $\square$

2.6.2. Символ Лежандра

Символ Лежандра $\left(\frac{a}{p}\right)$ определяется для всех a, не делящихся на p. Он равен 1, если a является квадратичным вычетом по модулю p, и -1, если a является квадратичным невычетом. Таким образом,

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

Иногда также говорят, что символ Лежандра равен 0 для a, кратных p.

Приведем несколько простых свойств символа Лежандра.

1. Если $a_1 \equiv a_2 \pmod{p}$, то $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right)$;
2. $\left(\frac{a_1 \ldots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \ldots \left(\frac{a_n}{p}\right)$;
3. $\left(\frac{a_1 a_2^2}{p}\right) = \left(\frac{a_1}{p}\right)$.

Теорема 2.9. (Квадратичный закон взаимности) *Если p и q – различные нечетные простые числа, то*

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

Доказательство. Из китайской теоремы об остатках следует, что существует биекция из множества $\mathbb{Z}_{pq}^*$ во множество $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$, определяемая как $f(a) = (a, a)$.

Пусть A – подмножество приведенной системы вычетов a по модулю pq, таких, что $1 \leq a < \frac{pq}{2}$, а B – множество таких пар (b, c), что b принадлежит приведенной системе вычетов по модулю p, c принадлежит приведенной системе вычетов по модулю q, $1 \leq c < \frac{q}{2}$. Мощности A и B одинаковы. Заметим теперь, что для каждого $(b, c) \in B$ существует единственное $a \in A$ такое, что $f(a) = \pm(b, c)$. Действительно, существуют единственные вычеты b', c' в приведенных системах такие, что $b' \equiv a \pmod{p}$, $c' \equiv a \pmod{q}$. Тогда , если $c' < \frac{q}{2}$, то $b = b'$ и $c = c'$. В противном случае $b = -b'$, $c = -c'$.

Для пар (b, c) определим сложение и умножение как поэлементные операции по соответствующему модулю. Таким образом, имеем

$$\prod_{a\in A}(a, a) = \varepsilon \prod_{(b,c)\in B}(b, c),$$

где $\varepsilon = \pm 1$.

Упростим обе части. Для краткости обозначим $p_1 = \frac{p-1}{2}$, $q_1 = \frac{q-1}{2}$. Начнем с вычислений первой компоненты произведения, выполняемых по модулю p.

$$\prod_{a\in A} a = \left(\prod_{a<pq/2, p\nmid a} a\right) \Bigg/ \left(\prod_{a<pq/2, q|a} a\right) =$$

$$= \left(\prod_{0<a<p} a\right)\left(\prod_{p<a<2p} a\right)\ldots\left(\prod_{q_1p<a<pq/2} a\right) \Bigg/ \left(\prod_{a<pq/2, q|a} a\right) \equiv$$

$$\equiv \frac{(p-1)!^{q_1}p_1!}{q\cdot 2q\ldots p_1q} \equiv \frac{(-1)^{q_1}}{q^{p_1}} \equiv (-1)^{q_1}\left(\frac{q}{p}\right).$$

Аналогично, для второй компоненты по модулю q получаем

$$\prod_{a\in A} a = \frac{(-1)^{p_1}}{p^{q_1}} \equiv (-1)^{p_1}\left(\frac{p}{q}\right).$$

С другой стороны

$$\prod_{(b,c)\in B}(b, c) = \prod_{0<b<p, 0<c<q/2}(b, c) = ((p-1)!^{q_1}, q_1!^{2p_1}).$$

По соответствующим модулям упростим эти выражение:

$$(p-1)!^{q_1} \equiv (-1)^{q_1} \pmod p,$$
$$q_1!^{2p_1} \equiv ((q-1)!(-1)^{q_1})^{p_1} \equiv (-1)^{p_1}(-1)^{p_1q_1} \pmod q.$$

Таким образом,

$$\left((-1)^{q_1}\left(\frac{q}{p}\right), (-1)^{p_1}\left(\frac{p}{q}\right)\right) = \varepsilon\left((-1)^{q_1}, (-1)^{p_1}(-1)^{p_1q_1}\right).$$

То есть имеем два сравнения:

$$\left(\frac{q}{p}\right) = \varepsilon \pmod{p},$$
$$\left(\frac{p}{q}\right) = \varepsilon(-1)^{p_1 q_1} \pmod{q}.$$

Подставляя ε из первого во второе, получаем квадратичный закон взаимности. $\square$

Квадратичный закон взаимности позволяет быстрее вычислять символы Лежандра. Кроме того, в далее мы докажем аналогичное утверждение для составных модулей. Квадратичный закон взаимности можно сформулировать также следующим образом.

Теорема 2.10. (Квадратичный закон взаимности) *Пусть p и q – нечетные простые числа. Тогда если хотя бы одно из них имеет вид $4k+1$, то сравнения $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ одновременно являются разрешимыми (или неразрешимыми). Если же оба числа имеют вид $4k+3$, то только одно из этих сравнений разрешимо.*

2.6.3. Символ Якоби

Для еще большего упрощения вычисления символа Лежандра вводят *символ Якоби*, определяемый для $n = p_1 \dots p_k$ и a, взаимно простого с n, как

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_n}\right).$$

Для символа Якоби верны те же элементарные свойства, что были перечислены для символа Лежандра. Кроме того, для него верен квадратичный закон взаимности. Прежде чем перейти к его доказательству, докажем следующую лемму.

Лемма 2.1. *Пусть $n = p_1 \dots p_k$ – нечетное положительное число. Тогда*

$$\frac{n-1}{2} \equiv \sum_{i=1}^{k} \frac{p_i - 1}{2} \pmod{2}$$

Доказательство. Число $\frac{n-1}{2}$ четно, если n имеет вид $4k+1$, и нечетно, если n имеет вид $4k+3$. Т.к. произведение двух чисел вида $4k+3$ – это число вида $4k+1$, то для того, чтобы $\frac{n-1}{2}$ было нечетным, в разложении n должно содержаться нечетное количество множителей вида $4k+3$. Остальные множители имеют вид $4k+1$.

Посмотрим теперь на правую часть. Ее нечетность равносильна тому, что в ней нечетное количество нечетных слагаемых, то есть нечетным должно быть количество p_i вида $4k+3$, а это совпадает с условием нечетности $\frac{n-1}{2}$. $\square$

Теорема 2.11. *Пусть m и n – положительные нечетные взаимно простые числа. Тогда*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Доказательство. Пусть $m = q_1 \dots q_l$, $n = p_1 \dots p_k$. Тогда

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{k}\left(\frac{m}{p_i}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right) =$$

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

Для степени -1 важна только четность, поэтому в соответствии с доказанной ранее леммой, имеем

$$(-1)^{\frac{m-1}{2}\frac{n-1}{2}}\prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right). = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right),$$

что завершает доказательство. $\square$

Замечание 2.1. Символ Якоби не характеризует разрешимость соответствующего квадратичного сравнения так, как символ Лежандра. Например, $\left(\frac{2}{15}\right) = 1$, однако можно проверить перебором, что сравнение $x^2 \equiv 2 \pmod{1)5}$ не имеет решений. Тем не менее, если $\left(\frac{a}{n}\right) = -1$, то сравнение $x^2 \equiv a \pmod{n}$ не имеет решений.

Пример 2.3. Выяснить, имеет ли решения сравнение

$$x^2 = 235 \pmod{311}$$

Проверив, что 311 – простое число, вычисляем:

$$\left(\frac{235}{311}\right) = \left(\frac{76}{235}\right) = \left(\frac{2^2\cdot 19}{235}\right) = \left(\frac{19}{235}\right) = \left(\frac{7}{19}\right) =$$
$$= -\left(\frac{5}{7}\right) = -\left(\frac{2}{5}\right) = 1.$$

Таким образом, сравнение имеет решения.

2.6.4. Решение квадратичных сравнений

В прошлом параграфе мы показали, что полиномиальное сравнение по составному модулю сводится к системе сравнений по модулям вида p^k, которые, в свою очередь, сводятся к сравнениям по простому модулю. Поэтому начнем с решения квадратичных сравнений по простому модулю.

Пусть $p = 4k + 3$. Тогда, если $x \equiv a^{\frac{p+1}{4}}$, то

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

при условии, что a является квадратичным вычетом.

Для $p = 4k+1$ все намного сложнее и готовой формулы не известно. Рассмотрим распространенный алгоритм для поиска решения в этом случае.

Алгоритм 2.1. (Тонелли-Шенкса)

Вход: модуль $p = 4k + 1$, a – квадратичный вычет по модулю p

1. Записать $p - 1$ в виде $2^s q$, q – нечетное.

2. Найти случайный квадратичный невычет z (для этого можно выбирать случайное $0 < z < p$ и проверять его, вычисляя символ Лежандра).

3. Пусть $M = s$, $c = z^q \pmod{p}$, $t = a^q \pmod{p}$, $r = a^{\frac{q+1}{2}} \pmod{p}$. Пока не будет получено $t = 1$, вычислять:

   - наименьшее i, $0 < i < M$ такое, что $t^{2^i} \equiv 1 \pmod{p}$;
   - $b = c^{2^{M-i-1}} \pmod{p}$;
   - $M = i$;
   - $c = b^2 \pmod{p}$;
   - $t = tb^2 \pmod{p}$;
   - $r = rb \pmod{p}$;

4. Как только $t = 1$, вернуть $x = r$ и второе решение $x = -r$.

Утверждение 2.7. *Алгоритм Тонелли-Шенкса корректен*

Доказательство. Заметим, что на момент начала цикла выполняются следующие соотношения:

$$\begin{aligned} c^{2^{M-1}} &\equiv z^{2^{s-1}q} \equiv z^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \\ t^{2^{M-1}} &\equiv a^{2^{s-1}q} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \\ r^2 &\equiv a^{q+1} \equiv ta \pmod{p}. \end{aligned}$$

Более того, они продолжают выполняться на любой следующей итерации алгоритма:

$$\begin{aligned} c'^{2^{M'-1}} &\equiv b^{2^{M'}} \equiv c^{2^{M-i-1}2^i} \equiv c^{2^{M-1}} \equiv -1 \pmod{p}, \\ t'^{2^{M'-1}} &\equiv t^{2^{i-1}} b^{2^i} \equiv -1 \cdot c^{2^{M-1}} \equiv 1 \pmod{p}, \\ r'^2 &\equiv r^2 b^2 \equiv tab^2 \equiv t'a \pmod{p}. \end{aligned}$$

Во втором сравнении $t^{2^{i-1}} \equiv -1 \pmod{p}$ т.к. i – наименьшее число, для которого $t^{2^i} \equiv 1 \pmod{p}$. Следовательно $t^{2^{i-1}}$ должно быть сравнимо с 1 или -1, но не может быть сравнимо с 1.

Обратим внимание на второй инвариант. Проверка $t \neq 1$ перед очередной итерацией вместе с этим равенством гарантирует, что i ($0 < i < M$), для которого t^{2^i}, всегда найдется. При этом с каждой итерацией M уменьшается. То есть алгоритм сходится, и однажды будет получено $t = 1$. Т.к. $r^2 \equiv ta \pmod{p}$, r в этот момент будет являться решением сравнения. □

Наконец, остается случай $p = 2$. Сравнение $x^2 \equiv a \pmod{2}$ имеет решение 1 (оно же -1), если a нечетно. Сравнение $x^2 \equiv a \pmod{4}$ имеет решение только при $a \equiv 1 \pmod{4}$ – эти решения 1 и 3.

Теорема 2.12. *Сравнение $x^2 \equiv a \pmod{2^k}$, $k \geq 3$, имеет 4 решения, если $a \equiv 1 \pmod{8}$ и не имеет решений в противном случае.*

Доказательство. Легко проверить, что 1, 3, 5 и 7 являются решениями сравнения $x^2 \equiv 1 \pmod{8}$. Поскольку сравнения для $k > 3$ подразумевают также выполнение некоторого сравнения для модуля 8, получаем условие на a для общего случая.

Для $k \geq 3$ рассмотрим сравнение

$$x^2 \equiv a \pmod{2^{k+1}}, \tag{2.10}$$

предполагая, что нам известно некоторое решение сравнения $x^2 \equiv a \pmod{2^k}$, которое мы обозначим x_k. Тогда $a - x_k^2 = 2^k t$. Если t четно,

то

$$x_k^2 - a \equiv 0 \pmod{2^{k+1}},$$

т.е. $x_{k+1} = x_k$ является решением (2.10). В противном случае

$$(x_k + 2^{k-1})^2 - a \equiv 2^k t + 2^k + 2^{2k-2} \equiv 0 \pmod{2^{k+1}},$$

т.е. $x_{k+1} = x_k + 2^{k-1}$ будет искомым решением. Еще три отличных от него решения – это $-x_{k+1}$, $x_{k+1} + 2^k$ и $-x_{k+1} - 2^k$.

Таким образом, по индукции мы получили, что у каждого разрешимого сравнения существует хотя бы 4 решения. Покажем, что их не может быть больше. Т.к. сравнения разрешимы только для $a \equiv 1 \pmod 8$, существует 2^{k-3} квадратичных вычета по модулю 2^k. При этом x может принимать только 2^{k-1} различных (нечетных) значений и каждое x является решением только для одного a. Тогда наличие у какого-то сравнения более чем 4 решений приведет к тому, что у какого-то другого их меньше 4. $\square$

Пример 2.4. Решить сравнение $x^2 \equiv 4945 \pmod{289 \cdot 32}$.

Данное сравнение равносильно системе

$$\begin{cases} x^2 \equiv 17 \pmod{2^5} \\ x^2 \equiv 15 \pmod{17^2} \end{cases}.$$

Начнем с первого сравнения. Нам известны решения $x^2 \equiv 17 \pmod 8$ – это 1, 3, 5 и 7. Чтобы найти решения по модулю 16, вычисляем:

$17 - 1^2 = 8 \cdot 2$, 2 – четно, т.е. $x = 1$ – решение,

$17 - 3^2 = 8 \cdot 1$, 1 – четно, т.е. $x = 3 + 4 = 7$ – решение.

Два оставшихся решения противоположны найденным – это 9 и 15.

Перейдем к модулю 32. Нам известны решения 1, 7, 9, 15 сравнения $x^2 \equiv 17 \pmod{16}$. Тогда:

$17 - 1^2 = 16 \cdot 1$, 1 – нечетно, т.е. $x = 1 + 8 = 9$ – решение,

$17 - 7^2 = -16 \cdot 2$, -2 – четно, т.е. $x = 7$ – решение.

Таким образом, первое сравнение в системе имеет следующие решения: 7,9, -7, -9.

Второе сравнение рассмотрим сначала по модулю 17:

$$x^2 \equiv 15 \pmod{17}.$$

Т.к. это число вида $4k+1$, можем применить алгоритм Тонелли-Шенкса. Найдем невычет по модулю 17, т.е. такое z, что $z^8 \equiv -1 \pmod{17}$ – подойдет, например, $z = 3$.

Запишем $17 - 1 = 2^4 \cdot 1$. Тогда начальные параметры:

$$\begin{aligned} M &= 4, \\ c &= 3^1 \pmod{17} = 3, \\ t &= 15^1 \pmod{17} = 15, \\ r &= 15^1 \pmod{17} = 15. \end{aligned}$$

Т.к. $15^2 \equiv 4 \pmod{17}$, $15^4 \equiv 16 \pmod{17}$, $15^8 \equiv 1 \pmod{17}$, на первом шаге выбираем $i = 3$. Теперь вычисляем остальные параметры:

$$\begin{aligned} b &= 3^1 \pmod{17} \\ M &= 3, \\ c &= 3^2 \pmod{17} = 9, \\ t &= 15 \cdot 9 \pmod{17} = 16, \\ r &= 15 \cdot 3 \pmod{17} = 11. \end{aligned}$$

Для второго шага имеем $16^2 \equiv 1 \pmod{17}$, т.е. $i = 1$. Вычислим остальные параметры:

$$\begin{aligned} b &= 9^2 \pmod{17} = 13 \\ M &= 1, \\ c &= 13^2 \pmod{17} = 16, \\ t &= 16 \cdot 16 \pmod{17} = 1, \\ r &= 11 \cdot 13 \pmod{17} = 7. \end{aligned}$$

Т.к. $t = 1$, можем остановиться. Найденные корни: $x_1 = r = 7$ и $x_2 = -7$.

Теперь перейдем к модулю 17^2. Начнем со случая, когда $x = 7 + 17t$. Для поиска t решаем сравнение

$$\frac{7^2 - 15}{17} + 2 \cdot 7t = 2 + 14t \equiv 0 \pmod{17}.$$

Получаем $t = 12$ и, следовательно, $x = 211$.

Для случая $x = -7 + 17t$ решаем сравнение

$$2 - 14t \equiv 0 \pmod{17}.$$

Очевидно, теперь $t = 5$, а $x = 78$. Это решение можно было найти и как $-211 \pmod{17}$.

Итак, первое сравнение в системе имеет решения 7, 9, -9, -7, а второе – решения 78 и -78. Для всех возможных пар решений находим решение системы с помощью китайской теоремы об остатках и получаем следующее множество:

$$7303, 5991, 7881, 6569, 2679, 1367, 3257, 1945.$$

2.7. Первообразные корни и индексы

2.7.1. Показатели

По теореме Эйлера при $(a, m) = 1$, $m > 1$ существуют такие положительные g, что $a^g \equiv 1 \pmod{m}$ – например, $g = \varphi(m)$. Наименьшее из них, $g = \gamma$, называется *показателем, которому принадлежит a по модулю m*. Далее приведем основные свойства показателей.

Утверждение 2.8. *Числа* $1, a, ..., a^{\gamma-1}$ *попарно не сравнимы по модулю* m.

Доказательство. Если $a^k \equiv a^l \pmod{m}$ для некоторых $0 \leq k < l < \gamma$, то $a^{l-k} \equiv 1 \pmod{m}$. При этом $0 < l - k < \gamma$ – получено противоречие. □

Утверждение 2.9. $a^k \equiv a^l \pmod{m}$ *тогда и только тогда, когда* $k \equiv l \pmod{\gamma}$.

Доказательство. Пусть r и q – наименьшие неотрицательные вычеты k и l по модулю γ. Тогда $k = x\gamma + r$, $l = y\gamma + q$. Используя то, что $a^\gamma \equiv 1 \pmod{m}$, находим

$$a^k \equiv (a^\gamma)^x a^r \equiv a^r \pmod{m},$$

$$a^l \equiv (a^\gamma)^y a^q \equiv a^q \pmod{m}.$$

Из утверждения 2.14 следует, что $a^r \equiv a^q \pmod{m}$ тогда и только тогда, когда $r = q$, т.е. $k \equiv l \pmod{\gamma}$. □

В частности при $k = 0$, $l = \varphi(m)$ получаем следствие

Следствие 2.1 $\varphi(m)$ делится на γ.

Утверждение 2.10. *Если число a принадлежит показателю $\gamma\delta$ по модулю m, то число a^γ принадлежит показателю δ по модулю m*

Доказательство. Очевидно, $(a^\gamma)^\delta \equiv 1 \pmod m$. Если бы существовало $\delta' < \delta$, для которого $(a^\gamma)^{\delta'} \equiv 1 \pmod m$, то и a принадлежало бы меньшему показателю $\gamma\delta'$. $\square$

Утверждение 2.11. *Если a принадлежит показателю γ по модулю m, а b принадлежит показателю δ по модулю m, и $(\gamma, \delta) = 1$, то ab принадлежит показателю $\gamma\delta$ по модулю m.*

Доказательство. Очевидно, $(ab)^{\gamma\delta} = (a^\gamma)^\delta (b^\delta)^\gamma \equiv 1 \pmod m$. Если предположить, что реальный показатель ab меньше, то $\gamma\delta$ делится на этот показатель. Пусть показатель равен $d = d_\gamma d_\delta$, где $\gamma = \gamma' d_\gamma$ и $\delta = \delta' d_\delta$. Тогда

$$(ab)^{d_\delta \gamma} = (a^\gamma)^{d_\delta} b^{d_\delta \gamma} \equiv b^{d_\delta \gamma} \equiv 1 \pmod m.$$

Тогда в соответствии с утверждением 2.9, $d_\delta \gamma \vdots \delta$. Следовательно, $d_\delta = \delta$. Аналогично показывается, что $d_\gamma = \gamma$. Таким образом, показатель ab все-таки оказывается равным $\delta\gamma$. $\square$

Утверждение 2.12. *Если a принадлежит показателю γ по модулю m, то a^δ, $\delta \in \mathbb{N}$ принадлежит показателю $\frac{\gamma}{(\gamma,\delta)}$ по модулю m.*

Доказательство. Пусть $\gamma = \gamma'(\gamma, \delta)$, $\delta = \delta'(\gamma, \delta)$. По утверждению 2.10 число $a^{(\gamma,\delta)}$ принадлежит показателю γ'. Пусть a^δ принадлежит показателю β. Тогда $(a^\delta)^\beta = (a^{(\gamma,\delta)})^{\delta'\beta} \equiv 1 \pmod m$ означает, что $\delta'\beta \vdots \gamma'$. Но $(\gamma', \delta') = 1$, поэтому $\beta \vdots \gamma'$, и, следовательно, $\beta \geq \gamma'$. Легко видеть, что для $\beta = \gamma' = \frac{\gamma}{(\gamma,\delta)}$ сравнение выполняется. $\square$

2.7.2. Первообразные корни

Если a принадлежит показателю $\varphi(m)$ по модулю m, а называется *первообразным корнем* по модулю m. Первообразные корни существуют не для каждого модуля.

Утверждение 2.13. *Существуют первообразные корни по модулю p, если p – простое.*

Доказательство. Очевидно, 1 является первообразным корнем по модулю 2. Пусть теперь p – нечетное простое. Обозначим τ наименьшее общее кратное тех показателей γ_i, которым принадлежат числа $i = \overline{1, p-1}$ по модулю p. Пусть $\tau = q_1^{\alpha_1} \dots q_k^{\alpha_k}$ – каноническое разложение числа τ. Тогда при каждом j существует некое γ_i, делящееся на $q_j^{\alpha_j}$, которое можно записать как $\gamma_i = a q_j^{\alpha_j}$. Согласно утверждению 2.10, если i – число, принадлежавшее показателю $a q_j^{\alpha_j}$, то $x_j = i^a$ принадлежит показателю $q_j^{\alpha_j}$. Таким образом, получено k чисел x_j, принадлежащих попарно взаимно простым показателям

$q_j^{\alpha_j}$. Тогда из утверждения 2.11 получаем, что $\tau = q_1^{\alpha_1} \dots q_k^{\alpha_k}$ – это показатель, которому принадлежит $g = x_1 \dots x_j$ по модулю p.

В свою очередь показатели γ_i должны быть делителями τ. Тогда все числа от 1 до $p-1$ удовлетворяют сравнению $x^\tau \equiv 1 \pmod p$, т.е. у этого сравнения есть хотя бы $p-1$ корень. Значит, $\tau \geq p-1$. Одновременно с этим τ является делителем $p-1$. Следовательно, $\tau = p-1$, и g – первообразный корень. $\square$

Теорема 2.13. *Существуют первообразные корни по модулям 2, 4, p^α, $2p^\alpha$, где p – простое нечетное, $\alpha \geq 1$.*

Доказательство. Легко видеть, что 1 и 3 – первообразные корни по модулям 2 и 4. Пусть g – первообразный корень по модулю p. Тогда $g^{p-1} = 1 + pq$ для некоторого целого q. Покажем, что существует такое x, что $g' = g + px$ является первообразным корнем по модулю p^α. Вычислим его $(p-1)$-ую степень:

$$(g+px)^{p-1} = g^{p-1} + (p-1)g^{p-2}px + \dots + (px)^{p-1} =$$

$$= 1 + p((p-1)g^{p-2}x + \dots + p^{p-2}x^{p-1}).$$

Заметим, что, во-первых, $(g')^{p-1} \equiv 1 \pmod p$. Кроме того, $(p-1)g^{p-2}$ не делится на p в отличие от остальных коэффициентов при x в скобках, т.е. x можно выбрать так, чтобы вся сумма не делилась на p. Таким образом, при некотором x имеем $(g')^{p-1} = 1 + py$, $p \nmid y$.

Предположим, что показатель, которому g' принадлежит по модулю p^α, равен γ. Тогда $\varphi(p^\alpha) = p^{\alpha-1}(p-1) \vdots \gamma$. С другой стороны, $g \equiv g' \pmod p$, т.е. оба являются первообразными корнями по модулю p. Т.к. $(g')^\gamma \equiv 1 \pmod p$, то γ делится на $p-1$. Таким образом, γ имеет вид $p^k(p-1)$, $k < \alpha$.

Теперь заметим, что, т.к. $(y,p) = 1$ и при простом p все биномиальные коэффициенты C_p^l, кроме крайних, делятся на p, то:

$$(1+py)^p = 1 + p^2y + \dots + p^py^p = 1 + p^2z_1, (z_1,p) = 1,$$
$$(1+p^2z_1)^p = 1 + p^3z_1 + \dots + p^{2p}z_1^p = 1 + p^3z_2, (z_2,p) = 1,$$
$$\dots (1+p^kz_{k-1})^p = 1 + p^{k+1}z_k, (z_k,p) = 1$$

Таким образом, $(g')^\gamma = (1+py)^{p^k} = 1 + p^{k+1}z$, где $(z,p) = 1$. Это значит, что $p^{k+1} \equiv 0 \pmod{p^\alpha}$, т.е. $k = \alpha - 1$. Тогда $\gamma = p^{\alpha-1}(p-1) = \varphi(p^\alpha)$, и g' – первообразный корень по модулю p^α.

Наконец, рассмотрим $2p^\alpha$. Заметим, что $\varphi(2p^\alpha) = \varphi(p^\alpha)$. Тогда выбрав из чисел g' и $g'+p^\alpha$ нечетное, получим первообразный корень по модулю $2p^\alpha$. $\square$

Теорема 2.14. *Не существует первообразных корней по остальным модулям.*

Доказательство. Пусть m – не степень 2. Тогда его можно представить в виде $m_1 m_2$, где $m_1, m_2 > 2$ и $(m_1, m_2) = 1$. При этом $\varphi(m_1)$ и $\varphi(m_2)$ оказываются четными, поэтому для a из приведенной системы вычетов имеем

$$a^{\varphi(m)/2} = (a^{\varphi(m_1)})^{\varphi(m_2)/2} \equiv 1 \pmod{m_1},$$
$$a^{\varphi(m)/2} \equiv 1 \pmod{m_2}.$$

Тогда $a^{\varphi(m)/2} \equiv 1 \pmod{m}$, и a не может быть первообразным корнем. Если же $m = 2^k$, то для a из приведенной системы вычетов имеем $a^2 \equiv 1 \pmod{8}$. Рассмотрим

$$a^{2^{k-2}} - 1 = (a^2 - 1)(a^2 + 1) \dots (a^{2^{k-3}} + 1).$$

Первый множитель делится на 8, каждый из $k - 3$ оставшихся делится на 2, следовательно, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$, в то время как $\varphi(2^k) = 2^{k-1}$. $\square$

Для поиска первообразного корня по модулю m можно воспользоваться следующими соображениями. Пусть $q_1, \dots, q_k$ – простые делители $\varphi(m)$. Рассмотрим сравнения

$$x^{\frac{\varphi(m)}{q_1}} \equiv 1 \pmod{m}, \dots, x^{\frac{\varphi(m)}{q_k}} \equiv 1 \pmod{m}. \tag{2.11}$$

Если x – первообразный корень, то он принадлежит показателю $\varphi(m)$, и потому ни одному из этих сравнений удовлетворять не может. С другой стороны, пусть x не удовлетворяет ни одному из сравнений и принадлежит показателю γ по модулю m. Если $\gamma < \varphi(m)$, то можно записать $\varphi(m) = \gamma q u$, дл некоторого натурального u и простого q. Тогда $\frac{\varphi(m)}{q} = \gamma u$ и

$$x^{\frac{\varphi(m)}{q}} \equiv (x^{\gamma})^u \equiv 1 \pmod{m}.$$

Но это противоречит нашему предположению о том, что не выполняется ни одно из сравнений (2.11). Таким образом, доказана следующая теорема.

Теорема 2.15. *Число x является первообразным корнем по модулю m тогда и только тогда, когда не выполняется ни одно из сравнений (2.11).*

Пусть p – нечетное простое, $m = p^\alpha$ или $2p^\alpha$, g – первообразный корень по модулю m.

Утверждение 2.14. *Числа 1, g, ..., $g^{\varphi(m)-1}$ образуют приведенную систему вычетов по модулю m.*

Доказательство. Числа 1, g, ..., $g^{\varphi(m)-1}$ взаимно просты с m и, согласно утверждению , попарно не сравнимы по модулю m. □

Теорема 2.16. *Если по модулю m существует первообразный корень g, то по нему существует ровно $\varphi(\varphi(m))$ попарно несравнимых первообразных корней. Эти корни имеют вид $g^k \pmod m$, где $(k, \varphi(m)) = 1$.*

Доказательство. Очевидно, первообразный корень должен быть взаимно прост с модулем, поэтому имеет рассматривать только приведенную систему вычетов, а она может быть представлена как 1, g, ..., $g^{\varphi(m)-1}$.

Из утверждения 2.12 имеем, что т.к. g принадлежит показателю $\varphi(m)$ по модулю m, то g^k принадлежит показателю $\frac{\varphi(m)}{(\varphi(m),k)}$. Следовательно, первообразным корнем оно будет тогда и только тогда, когда $(\varphi(m), k) = 1$, а количество таких $k < \varphi(m)$ как раз и есть $\varphi(\varphi(m))$. □

Аналогичным образом вычисляется количество чисел, принадлежащих показателю γ по модулю m – оно равно $\varphi(\gamma)$.

2.7.3. Индексы

Пусть g – первообразный корень по модулю m, тогда в виду утверждения 2.14, если γ пробегает полную систему вычетов по модулю $\varphi(m)$, то g^γ действительно пробегает приведенную систему вычетов по модулю m. Поэтому для чисел a, взаимно простых с m, можно ввести понятие, аналогичное понятию логарифма для действительных чисел. Целое неотрицательное число δ называется *индексом*, или *дискретным логарифмом* a по модулю m при основании g, если $g^\delta = a \pmod m$. Индекс будем обозначать $\log_g a$ (иногда встречается $\mathrm{ind}_g a$ или $\mathrm{ind} a$; отсутствие основания подразумевает произвольный, но фиксированный первообразный корень g).

Индекс, вообще говоря, не определен однозначно, но все индексы принадлежат одному классу вычетов по модулю $\varphi(m)$. Для определенности будем, как правило, использовать наименьшее натуральное значение индекса.

Индексы обладают свойствами, аналогичными свойствам логарифмов:

- $\log_g(a_1 \dots a_k) \equiv \log_g a_1 + \dots + \log_g a_k \pmod{\varphi(m)}$;
- $\log_g a^n \equiv n \log_g a \pmod{\varphi(m)}$.

Число a называется *вычетом степени* n по модулю m если сравнение

$$x^n \equiv a \pmod{m} \tag{2.12}$$

разрешимо.

Теорема 2.17. *Пусть* $(n, \varphi(m)) = d$. *Тогда*

1. a *является вычетом степени* n *по модулю* m *тогда и только тогда когда* $\log a$ *делится на* d;

2. *в приведенной системе вычетов по модулю* m *существует ровно* $\frac{\varphi(m)}{d}$ *вычетов степени* n.

Доказательство. Сравнение (2.12) равносильно сравнению

$$n \log x \equiv \log a \pmod{\varphi(m)},$$

которое разрешимо тогда и только тогда, когда $\log a$ делится на $(n, \varphi(m)) = d$, и в случае разрешимости имеет как раз d решений – среди вычетов по модулю $\varphi(m)$.

Для доказательства второй части заметим, что вся приведенная система вычетов разбивается на классы по d элементов, для которых x^n сравнимы по модулю m. Следовательно, $x^n \pmod{m}$ принимает ровно $\frac{\varphi(m)}{d}$ различных значений, которые и являются вычетами степени n. $\square$

Утверждение 2.15. *Число* a *является вычетом по модулю* m *тогда и только тогда, когда* $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$.

Доказательство. Это условие равносильно $\frac{\varphi(m)}{d} \log a \equiv 0 \pmod{\varphi(m)}$, что, в свою очередь, равносильно тому, что $\log a$ делится на d. $\square$

Следующее утверждение связывает показатель, которому принадлежит число, с дискретным логарифмом. Отметим, что оно остается верным независимо от того, какой первообразный корень используется для вычисления логарифма, хотя значения логарифма при этом оказываются различными.

Утверждение 2.16. *Показатель* γ, *которому* a *принадлежит по модулю* m, *равен* $\frac{\varphi(m)}{(\varphi(m), \log a)}$.

Доказательство. Действительно, γ – наименьший делитель $\varphi(m)$, для которого верно $a^\gamma \equiv 1 \pmod{m}$. Логарифмируя, получаем

$$\gamma \log a \equiv 0 \pmod{\varphi(m)},$$

что равносильно

$$\log a \equiv 0 \pmod{\frac{\varphi(m)}{\gamma}}.$$

То есть γ – наименьший делитель $\varphi(m)$, при котором $\frac{\varphi(m)}{\gamma}$ делит $\log a$. Тогда $\frac{\varphi(m)}{\gamma}$ – наибольший делитель $\varphi(m)$, делящий $\log a$. Таким образом, $\frac{\varphi(m)}{\gamma} = (\varphi(m), \log a)$. $\square$

В частности это дает критерий того, является ли a первообразным корнем: $\varphi(m)$ и $\log a$ должны быть взаимно просты.

Для поиска индексов могут использоваться таблицы индексов. Однако построение таблиц обладает высокой вычислительное сложностью. Существуют специальные алгоритмы дискретного логарифмирования, однако ни один из них не является полиномиальным в общем случае. На сложности задачи дискретного логарифмирования опираются некоторые криптосистемы, например, криптосистема Эль-Гамаля.

Оглавление