ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. Лекция 11.

Первообразные корни. Существование первообразных корней по простому модулю.

Механико-математический факультет МГУ
1 поток 1 курса, осень 2026 г.

Согласно малой теореме Ферма для каждого целого числа a взаимно простого с модулем m выполняется сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$. Для некоторых чисел a сравнение $a^d \equiv 1 \pmod{m}$ может выполняться и при $d < \varphi(m)$. Например, $(-1)^2 \equiv 1 \pmod{m}$.

Пусть a – целое число, взаимно простое с модулем m. Напомним, что наименьшее натуральное число d с условием $a^d \equiv 1 \pmod{m}$ называется показателем числа a по модулю m, см. §**??**. Например, при $m > 2$ показатель -1 равен 2. Если два числа сравнимы по модулю m, то их показатели по модулю m одинаковы.

На языке теории групп можно сказать, что показатель числа a по модулю m равен порядку элемента $\overline{a}$ в мультипликативной группе $(\mathbb{Z}/m\mathbb{Z})^*$. Заметим, что порядок этой группы равен $\varphi(m)$.

Определение 1. Целое число a взаимно простое с модулем m называется первообразным корнем по модулю m, если его показатель равен $\varphi(m)$.

Если a – первообразный корень по модулю m, то числа

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

принадлежат различным классам вычетов.

Действительно, если бы нашлись целые числа $0 \leq u < v \leq \varphi(m) - 1$, для которых $a^u \equiv a^v \pmod{m}$, то в силу взаимной простоты чисел a и m мы получили бы

$$1 \equiv a^{v-u} \pmod{m}.$$

Но это невозможно, так как $0 < v - u < \varphi(m)$ и показатель a равен $\varphi(m)$.

Множество (1) состоит из $\varphi(m)$ чисел. Поэтому среди (1) есть представители всех классов вычетов, состоящих из чисел взаимно простых с m.

Другими словами, для каждого целого числа b взаимно простого с модулем m найдется единственное целое k, удовлетворяющее условиям

$$b \equiv a^k \pmod{m}, \qquad 0 \leq k < \varphi(m).$$

Это свойство можно выразить иначе, сказав, что первообразный корень по модулю m существует лишь в случае, когда $(\mathbb{Z}/m\mathbb{Z})^*$ – циклическая группа. Оно выполняется не для всех модулей m. Например, квадрат каждого нечетного числа при делении на 8 дает в остатке 1.

Значит, показатель каждого нечетного числа по модулю 8 может равняться лишь 1 или 2, и всегда отличен от $\varphi(8) = 4$. Первообразных корней по модулю 8 не существует.

Свойства показателей описывает следующая лемма.

Лемма 1. 1. Пусть d – показатель числа a по модулю m. Натуральное число n удовлетворяет условию $a^n \equiv 1 \pmod{m}$ в том и только том случае, когда $d|n$.

2. Пусть a, b – целые числа, взаимно простые с модулем m, показатели их равны соответственно u и v. Если $(u, v) = 1$, то показатель числа ab равен uv.

3. Если показатель числа c равен uv, то показатель c^u равен v.

Доказательство. Заметим, что числа ab и a^u, о которых идет речь в формулировке теоремы, взаимно просты с модулем, поэтому каждое из них имеет некоторый показатель.

Первое утверждение леммы уже доказано нами, см. лемму 2 из лекции 5.

Чтобы доказать второе утверждение, обозначим буквой s показатель числа ab. Так как

$$(ab)^{uv} = (a^u)^v (b^v)^u \equiv 1 \pmod{m},$$

то по первому утверждению леммы имеем $s|uv$. С другой стороны из сравнения $(ab)^s \equiv 1 \pmod{m}$ следует

$$1 \equiv (ab)^{su} = (a^u)^s b^{us} \equiv b^{us} \pmod{m}.$$

С помощью первого утверждения находим $v|us$. Согласно условию числа u, v взаимно просты, поэтому $v|s$. Аналогично доказывается, что $u|s$. Учитывая взаимную простоту чисел u, v, получаем отсюда $uv|s$. Итак, доказано, что $s = uv$.

Для доказательства третьего утверждения обозначим буквой t показатель числа c^u. Так как $1 \equiv c^{uv} = (c^u)^v \pmod{m}$, то $t|v$. А из сравнения $1 \equiv (c^u)^t = c^{tu} \pmod{m}$ следует, в силу первого свойства, что $uv|tu$ и $v|t$. Но тогда $t = v$ и последнее утверждение леммы доказано.

Следствие 1. Если $(a, m) = 1$ и целые числа u, v удовлетворяют сравнению $a^u \equiv a^v \pmod{m}$, то $u \equiv v \pmod{d}$, где d – показатель a по модулю m.

Доказательство. Не уменьшая общности можно считать, что $v > u$. Поскольку a и m взаимно просты, из данного сравнения следует $a^{v-u} \equiv 1 \pmod{m}$. Согласно первому утверждению леммы 1 можно утверждать, что $d|(v - u)$.

В 1801 году К.Ф. Гаусс опубликовал два доказательства следующей теоремы.

Теорема 26. Для каждого простого нечетного числа p существуют первообразные корни по модулю p.

Доказательство. Обозначим буквой d наименьшее общее кратное показателей всех чисел, не делящихся на p. Из малой теоремы Ферма и первого утверждения леммы 1 следует, что $p-1$ делится на показатель каждого числа, не кратного p. Но тогда $p-1$ делится на наименьшее общее кратное этих показателей, т.е. $d|(p-1)$.

Из первого утверждения леммы 1 следует, что каждое целое число, не кратное p, удовлетворяет сравнению $x^d - 1 \equiv 1 \pmod{p}$. Значит, это сравнение имеет $p-1$ решение. С помощью теоремы Лагранжа находим теперь $d \geq p-1$. Таким образом, $d = p-1$.

Пусть $p - 1 = q_1^{k_1} \cdots q_r^{k_r}$ – разложение на простые сомножители. По одному из доказанных ранее следствий основной теоремы арифметики можно утверждать, что для каждого индекса $i, 1 \leq i \leq r$, найдется число a_j, показатель которого равен $q_i^{k_i} v_i$. Положим $a = a_1^{v_1} \cdots a_r^{v_r}$.

По второму утверждению леммы 1 показатель числа $a_i^{v_i}$ равен $q_i^{k_i}$. Из третьего утверждения этой же леммы следует, что показатель числа a равен $q_1^{k_1} \cdots q_r^{k_r} = p - 1$. Итак, построенное число a есть первообразный корень по модулю p. Теорема доказана.