Первообразные корни

Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, н.о.д.$(a, m) = 1$. *Показатель* числа a по модулю m — наименьшее $d \in \mathbb{N}$, такое что $a^d \equiv 1 \pmod m$. (*Почему такое d существует?*) Обозначение: $\operatorname{ord}_m a = d$.

Контрольный вопрос (в голову): $\operatorname{ord}_{13} 5 = ?$

Некоторые свойства показателя $\operatorname{ord}_m a = d$:

- $1, a, a^2, \ldots, a^{d-1}$ попарно различны по модулю m.
- $a^n \equiv 1 \pmod m \iff d \mid n$; в частности, $d \mid \varphi(m)$.
- $a^u \equiv a^v \pmod m \iff u \equiv v \pmod d$.

Если $\operatorname{ord}_m g = \varphi(m)$, то g называется *первообразным корнем* по модулю m. Это эквивалентно тому, что $1, g, g^2, \ldots, g^{\varphi(m)-1}$ — приведённая система вычетов по модулю m.

Пусть $m = 100 = 4 \cdot 25$. Если н.о.д.$(a, 100) = 1$, то

$$\begin{cases} a^2 \equiv 1 \pmod 4, \\ a^{20} \equiv 1 \pmod{25} \end{cases} \implies \begin{cases} a^{20} \equiv 1 \pmod 4, \\ a^{20} \equiv 1 \pmod{25} \end{cases} \implies a^{20} \equiv 1 \pmod{100},$$

поэтому $\operatorname{ord}_{100} a \leqslant 20$. Следовательно, не существует п. к. mod 100. (*Почему?*)

Первообразные корни существуют только для модулей $1, 2, 4, p^\alpha, 2p^\alpha$ (здесь и всюду далее $p > 2$ — простое, $\alpha \in \mathbb{N}$). (На лекциях обычно считают $m > 1$.)

Для простого модуля п. к. ищется методом проб и ушибов. Для проверки используется критерий (для небольших простых можно пользоваться определением).

Критерий. *Пусть $g \in \mathbb{Z}$,* н.о.д.$(g, p) = 1$. *Тогда g — п. к.* mod p, *если и только если для всякого* простого $q \mid (p-1)$ *выполнено*

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod p.$$

При этом для делителя $q = 2$ удобно воспользоваться символом Лежандра:

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

Утверждение 1. *Если g — п. к.* mod p, $g_1 \equiv g \pmod p$, *причём*

$$g_1^{p-1} \not\equiv 1 \pmod{p^2},$$

то g_1 — п. к. mod p^2. *При этом среди чисел $g, g+p, g+2p, \ldots, g+(p-1)p$ все, кроме ровно одного, годятся в качестве g_1.* (*И таким образом получаются все п. к.* mod p^2.)

Утверждение 2. *Если g_1 — п. к.* mod p^2, *то g_1 — п. к.* mod p^α *для любого α.*

Утверждение 3. *Если g_1 — п. к.* mod p^α, *то нечётное из двух чисел $g_1, g_1 + p^\alpha$ является п. к.* mod $2p^\alpha$.

Задача 1. Проверьте, что 2 — п. к. mod 101.

Задача 2. Проверьте, что 12 — п. к. mod 125.

Задача 3. Решите сравнения:

1) $2^{15x-26} \equiv 16 \pmod{101}$.
2) $x^6 \equiv 16 \pmod{101}$. (*Подсказка.* Сделайте замену $x \equiv 2^y \pmod{101}$, $0 \leqslant y \leqslant 99$.)
3) $x^{10} \equiv 16x^4 \pmod{101}$.

Задача 4. Пусть p — простое число, $p \equiv 5 \pmod 6$, $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $p \nmid a$. Докажите, что сравнение $x^3 \equiv a \pmod{p^n}$ имеет единственное решение.

Резерв. Как, зная один п. к. mod m, найти все? Сколько их всего (различных mod m)?

Домашнее наказание

Задача 1. Найдите наименьшие положительные п. к. по (простым) модулям 19, 31, 41.

Задача 2. Найдите (какой-нибудь) п. к. по модулю 343.

Задача 3. Убедитесь, что 3 — п. к. по модулю 257, и с помощью этого знания решите сравнения:

1) $3^{6x+8} \equiv 9 \pmod{257}$;
2) $x^{10} \equiv 9x^4 \pmod{257}$.

(Число 257 простое.)

Ответы

1: 2, 3, 6 соответственно.
2: например, 3.
3: 1) $x = 128t - 1$, $t \in \mathbb{N} \cup \{0\}$; 2) $x \equiv 0, 3^{43}, 3^{171} \equiv 0, 110, 147 \pmod{257}$.