Домашнее задание на 7.03 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

№1 Рассмотрим модуль $m = 11$. Тогда функция Эйлера даёт

$$\varphi(11) = 10.$$

Пусть $g \in \mathbb{Z}$ с $(g, 11) = 1$. По критерию первообразности, g является первообразным корнем по модулю 11, если и только если для каждого простого делителя q числа $\varphi(11) = 10$ выполняются неравенства:

$$g^{\frac{10}{q}} \not\equiv 1 \pmod{11}.$$

Так как простые делители 10 — это 2 и 5, условие эквивалентно:

$$g^5 \not\equiv 1 \pmod{11} \quad \text{и} \quad g^2 \not\equiv 1 \pmod{11}.$$

Переберём все g из множества $\{1, 2, \ldots, 10\}$:

- $g = 1$:

$$1^2 \equiv 1 \pmod{11}, \quad 1^5 \equiv 1 \pmod{11} \quad \Rightarrow \quad \text{не является первообразным.}$$

- $g = 2$:

$$2^2 = 4 \not\equiv 1 \pmod{11}, \quad 2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11}$$

$$\Rightarrow \quad 2 \text{ — первообразный корень.}$$

- $g = 3$:

$$3^2 = 9 \not\equiv 1 \pmod{11}, \quad 3^5 = 243 \equiv 1 \pmod{11} \quad \Rightarrow \quad 3 \text{ не подходит.}$$

- $g = 4$:

$$4^5 = 1024 \equiv 1 \pmod{11} \quad \Rightarrow \quad 4 \text{ не подходит.}$$

- $g = 5$:

$$5^5 = 3125 \equiv 1 \pmod{11} \quad \Rightarrow \quad 5 \text{ не подходит.}$$

- $g = 6$:

$$6^2 = 36 \equiv 3 \not\equiv 1 \pmod{11}, \quad 6^5 \equiv 10 \not\equiv 1 \pmod{11}$$

$$\Rightarrow \quad 6 \text{ — первообразный корень.}$$

- $g = 7$:

$$7^2 = 49 \equiv 5 \not\equiv 1 \pmod{11}, \quad 7^5 \equiv 10 \not\equiv 1 \pmod{11}$$

$$\Rightarrow \quad 7 \text{ — первообразный корень.}$$

- $g = 8$:

$$8^2 = 64 \equiv 9 \not\equiv 1 \pmod{11}, \quad 8^5 = 32768 \equiv 10 \not\equiv 1 \pmod{11}$$

$$\Rightarrow \quad 8 \text{ — первообразный корень.}$$

- $g = 9$:

$$9^5 \equiv 1 \pmod{11} \quad \Rightarrow \quad 9 \text{ не подходит.}$$

- $g = 10$:

$$10^2 = 100 \equiv 1 \pmod{11} \quad \Rightarrow \quad 10 \text{ не подходит.}$$

Таким образом, первообразными корнями по модулю 11, лежащими на интервале от 0 до 11, являются:

$$\{2, 6, 7, 8\}.$$

№2 Пусть $m = 2p + 1$, тогда:

$$\varphi(m) = 2p$$

Значит, чтобы -2 был первообразным корнем, нужно, чтобы:

$$\forall q \mid 2p : (-2)^{\frac{2p}{q}} \not\equiv 1 \pmod{2p+1}$$

У числа $2p$ ровно 2 простых делителя 2 и p, рассмотрим каждый:

1) $q = 2$:

   Тогда, нужно, чтобы выполнялось:

$$(-2)^p \not\equiv 1 \pmod{2p+1}$$

   Пусть обратное:

$$(-2)^p \equiv 1 \pmod{2p+1} \quad (*)$$

   По малой теореме Ферма мы знаем, что:

$$(-2)^{2p} \equiv 1 \pmod{2p+1}$$

   Значит, чтобы выполнялось $(*)$, нужно:

$$p = 2p \implies p = 0$$

   Но такого не может быть, так как $p \equiv -1 \pmod 4$, противоречие. Следовательно $(*)$ не выполняется

2) $q = p$: Тогда, нужно, чтобы выполнялось:

$$(-2)^2 \equiv 4 \not\equiv 1 \pmod{2p+1}$$

То есть:

$$4 \neq 1 + (2p+1)k, \quad k \in \mathbb{Z}$$

$$3 \neq 2pk + k$$

Рассмотрим обратное:

$$3 = 2pk + k \implies k \mid 3$$

Рассмотрим все четыре случая:

$$\begin{cases} k = 0 : 3 = 0 \quad \varnothing \\ k = 1 : 3 = 2p + 1 \implies 2p = 2 \implies p = 1 \, \varnothing \quad (\text{т.к. } p \equiv -1 \pmod 4) \\ k = 2 : 1 = 4p \quad \varnothing \\ k = 3 : 3 = 6p + 3 \implies p = 0 \quad \varnothing \end{cases}$$

Следовательно :

$$(-2)^2 \equiv 4 \not\equiv 1 \pmod{2p+1}$$

Следовательно:

$$\forall q \mid 2p : (-2)^{\frac{2p}{q}} \not\equiv 1 \pmod{2p+1}$$

А значит -2 - первообразный корень

№3 Модуль 79 — простое число. Количество первообразных корней по модулю 79 равно $\varphi(\varphi(79)) = \varphi(78)$, где φ — функция Эйлера. Разложим 78 на простые множители:

$$78 = 2 \times 3 \times 13$$

Тогда:

$$\varphi(78) = \varphi(2) \times \varphi(3) \times \varphi(13) = 1 \times 2 \times 12 = 24$$

Таким образом, существует 24 первообразных корня по модулю 79

Пусть g — один из первообразных корней по модулю 79. Тогда все первообразные корни имеют вид:

$$g^k, \quad \text{где } 1 \leqslant k \leqslant 77 \text{ и } (k, 78) = 1$$

Произведение всех первообразных корней равно:

$$P = \prod_{\substack{1 \leqslant k \leqslant 77 \\ (k,78)=1}} g^k$$

Обозначим сумму показателей через:

$$S = \sum_{\substack{1 \leqslant k \leqslant 77 \\ (k,78)=1}} k$$

Сумма чисел, взаимно простых с m и меньших m, равна:

$$S = \frac{m \cdot \varphi(m)}{2}$$

Для $m = 78$:

$$S = \frac{78 \cdot \varphi(78)}{2} = \frac{78 \cdot 24}{2} = 78 \cdot 12 = 936$$

Заметим, что $936 = 78 \times 12$, поэтому:

$$S \equiv 0 \pmod{78}$$

Подставляя S в выражение для P, получаем:

$$P = g^S = g^{78\times 12} = \left(g^{78}\right)^{12}.$$

Поскольку показатель g равен 78, выполняется:

$$g^{78} \equiv 1 \pmod{79}$$

Следовательно:

$$P \equiv 1^{12} \equiv 1 \pmod{79}$$

№4 Пусть g — первообразный корень по модулю m, и $k \in \mathbb{N}$. Требуется доказать, что:

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

показатель элемента g^k по модулю m — это наименьшее натуральное число d, такое что:

$$(g^k)^d \equiv 1 \pmod{m}.$$

Это эквивалентно:

$$g^{kd} \equiv 1 \pmod{m}.$$

Так как g — первообразный корень, его показатель равен $\varphi(m)$. Следовательно:

$$g^{\varphi(m)} \equiv 1 \pmod{m},$$

и для любого $t \in \mathbb{N}$:

$$g^t \equiv 1 \pmod{m} \iff \varphi(m) \mid t$$

Из условия $g^{kd} \equiv 1 \pmod{m}$ следует, что:

$$\varphi(m) \mid kd.$$

Минимальное d, удовлетворяющее $\varphi(m) \mid kd$, определяется как:

$$d = \frac{\varphi(m)}{(k, \varphi(m))}.$$

Это следует из того, что:

$$\text{НОК}(k, \varphi(m)) = \frac{k \cdot \varphi(m)}{(k, \varphi(m))},$$

и тогда:

$$d = \frac{\text{НОК}(k, \varphi(m))}{k} = \frac{\varphi(m)}{(k, \varphi(m))}.$$

Предположим, существует $d' < d$, такое что $\varphi(m) \mid kd'$. Тогда:

$$kd' = \varphi(m) \cdot \frac{k}{\gcd(k, \varphi(m))} \cdot \frac{d'}{d}.$$

Но $\frac{d'}{d} < 1$, что противоречит целочисленности. Следовательно, d действительно минимально.

Поэтому:

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

№5 Количество элементов в приведённой системе вычетов по модулю p:

$$\varphi(p) = p - 1 = 2^k$$

Любой элемент g этой системы имеет показатель d, делящий 2^k, то есть $d = 2^m$, где $0 \leqslant m \leqslant k$. Первообразный корень — это элемент показателя 2^k.

- **Если g — первообразный корень**, то его показатель 2^k. Если бы g был квадратичным вычетом, то существовал бы элемент x, такой что $g \equiv x^2 \mod p$. Тогда показатель x был бы 2^{k+1} ($g^{2^k} \equiv x^2$), что невозможно, так как максимальный показатель 2^k. Следовательно, g — квадратичный невычет.

- **Если g — квадратичный невычет**. Предположим, что показатель g равен 2^m, где $m < k$. Тогда $g^{2^{m-1}} \equiv -1 \mod p$. Возведём обе части в квадрат:

  $$g^{2^m} \equiv 1 \mod p.$$

  Это означает, что $g^{2^m} \equiv 1 \mod p$, что противоречит тому, что показатель g равен 2^m. Следовательно, $m = k$, и g — первообразный корень.

Первообразный корень имеет максимальный показатель 2^k, что исключает возможность быть квадратом. Квадратичный невычет, не будучи квадратом, обязан иметь максимальный показатель. Таким образом, эквивалентность доказана.