91. Показатели. Первообразные корни. Существование по модулю p.

Лемма: Если порядки чисел $x_1, \ldots, x_k$ взаимно-просты, то порядок $x_1 \cdot \ldots \cdot x_k$ равен произведению порядков.

▲ Докажем для двух чиел, для большего числа - по индукции. Пусть $\mathrm{ord}_n\, a = \delta_a, \mathrm{ord}_n\, b = \delta_b, (\delta_a, \delta_b) = 1$. Тогда $(ab)^{\delta_a\delta_b} = (a^{\delta_a})^{\delta_b}(b^{\delta_b})^{\delta_a} = 1 (\mathrm{mod}\, n)$. Докажем, что $k < \delta_a\delta_b$ не являются порядками. Пусть $(ab)^k = 1 \,(\mathrm{mod}\, n)$. Возведем обе части в степень δ_a: $(a^{\delta_a})^k b^{k\delta_a} = b^{k\delta_a} = 1 \Rightarrow k\delta_a \vdots \delta_b,\ (\delta_a, \delta_b) = 1 \Rightarrow\ k \vdots \delta_b$. Аналогично показываем, что $k \vdots \delta_a \Rightarrow \mathrm{ord}_n(ab) = \delta_a\delta_b$ ■

Утверждение: Если p нечетное простое число то по модулю p существует первообразный корень.

▲ Пусть $\delta_1, \ldots, \delta_{p-1}$ - показатели (порядки) чисел $1, \ldots, p-1$ соответственно. Рассмотрим $\tau := [\delta_1, \ldots, \delta_{p-1}] = q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k}$ - каноническое разложение.

$\forall i \in \{1, \ldots, k\}\ \exists \delta \in \{\delta_1, \ldots, \delta_n\}\ \exists a :\ \delta = aq_i^{\alpha_i},\ (a, q_i) = 1$ (верно, так как если полная степень делителя НОКа не входит ни в какое из чисел, то ее не должно быть в НОКе)

Зафиксируем i и найдем соответствующую ему δ. Выберем x такой что δ - его показатель. $1 = x^{\delta} = x^{aq_i^{\alpha_i}} = (x^a)^{q_i^{\alpha_i}} \,(\mathrm{mod}\ p) \Rightarrow q_i^{\alpha_i}$ - порядок x^a (меньше не может быть так как иначе δ не был бы порядком x)

Рассмотрим $g = \prod_{i=1}^{k} x_i^{a_i}$ (по всем i). По лемме порядок g равен $q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k} = \tau \Rightarrow \tau \leq p-1$ (так как это порядок).

Рассмотрим сравнение $x^{\tau} \equiv 1 (\mathrm{mod}\, p)$. Все числа $1. \ldots, p-1$ являются его корнями (так как τ - НОК их порядков) $\Rightarrow \tau \geq p-1$ (так как многочлен не может иметь больше корней чем его степень) $\Rightarrow \tau = p-1 \Rightarrow g$ - первообразный корень. ■

92. Показатели. Первообразные корни. Существование по модулю p^{α}, $\alpha \geq 2$: формулировка и доказательство леммы. Существование по модулю $2p^{\alpha}$.

Лемма: $\exists t :\ (g+pt)^{p-1} = 1 + pu,\ (p, u) = 1$

▲

$$(g+pt)^{p-1} = g^{p-1} + g^{p-2}(p-1)pt + p^2a = \underbrace{1+pv}_{g^{p-1}} + p(g^{p-2}(p-1)t + pa) = 1 + p(v + \underbrace{g^{p-2}(p-1)}_{\text{взаимно просто с } p}\ t + pa)$$

Так как t можно выбирать любым, легко можем подобрать его так, чтобы $v + g^{p-2}(p-1)t$ было взаимно просто с p. Тогда $u = v + g^{p-2}(p-1)t + pa$ - искомое ■

Утверждение 1: По модулю $p^{\alpha}, \alpha > 2$ (p - нечетное простое) существует первообразный корень.

Утверждение: По модулю $2p^{\alpha}$ (p - нечетное простое) существует первообразный корень.

▲

$$\varphi(2p^{\alpha}) = \varphi(2)\varphi(p^{\alpha}) = \varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Для подсчета $\varphi(p^{\alpha})$ воспользовались тем, что чисел кратных p, которые меньше p^{α} всего $p^{\alpha-1}$.

Пусть $g+pt$ - первообразный корень по модулю p^{α}. Если $g+pt$ - нечетное, то это и есть первообразный корень по модулю $2p^{\alpha}$ (если $a = (g+pt)^{\varphi(2p^{\alpha})}$ нечетное, то $a-1$ - четное, а значит $a - 1 \vdots p^{\alpha} \Leftrightarrow a - 1 \vdots 2p^{\alpha}$)

Если $g + pt$ - чётное, то берем $g + pt + p^{\alpha}$ ■

93. Показатели. Первообразные корни. Существование по модулю p^α, $\alpha \geq 2$: формулировка леммы (б/д) и вывод существования из неё. Существование по модулю $2p^\alpha$.

Лемма: $\exists t:\ (g+pt)^{p-1} = 1 + pu,\ (p,u) = 1$

Утверждение 1: По модулю $p^\alpha, \alpha > 2$ (p - нечетное простое) существует первообразный корень.

▲ Покажем, что найденный в лемме $g+pt$ - первообразный корень по модулю p^α. Пусть δ - показатель $g+pt$ по модулю p^α.

$$(g+pt)^\delta \equiv 1 \pmod{p^\alpha} \Rightarrow (g+pt)^\delta \equiv 1 \pmod{p}$$

g - первообразный корень по модулю $p \Rightarrow \delta \vdots (p-1)$. С друой строны δ делит $\varphi(p^\alpha) = p^{\alpha-1}(p-1) \Rightarrow \delta = p^k(p-1), k \leq a-1$.

$$(g+pt)^{p-1} = 1 + pu, (p,u) = 1 \text{ (по лемме)}$$

$$(g+pt)^{p(p-1)} = (1+pu)^p = 1 + p^2u + p^3v = 1 + p^2(u+pv) = 1 + p^2u_1, (u_1,p) = 1$$

$(u_1,p) = 1 \Rightarrow u_1$ не содержит делителя $p^{\alpha-2}$ (при $\alpha \neq 2$) $\Rightarrow (1+gt)^{p(p-1)} \not\equiv 1 \pmod{p^\alpha}$

Будем повторять такой процесс для получившегося равенства пока не получим

$$(g+pt)^{p^{\alpha-1}(p-1)} = 1 + p^\alpha u_{\alpha-1} \equiv 1 \pmod{p^\alpha}$$

Следовательно, так как все меньшие δ вида $p^k(p-1)$ не подходят, порядком $g+pt$ является $p^{\alpha-1}(p-1) = \varphi(p^\alpha) \Rightarrow g+pt$ - первообразный корень ■

Замечание: существование по модулю $2p^\alpha$ см. билет 93.

94. Показатели. Первообразные корни. Несуществование по модулю 2^n, $n > 3$.

Замечание: Покажем, что по модулям 2 и 4 первообразные корни существуют.

$m = 2$: $\varphi(2) = 1, 1^1 \equiv 1 \pmod{2} \Rightarrow 1$ - первообразный корень

$m = 4$: $\varphi(4) = 2, 3^2 = 9 \equiv 1 \pmod{4}$, $3^1 \not\equiv 1 \pmod{4} \Rightarrow 3$ - первообразный корень

Утверждение: По модулю $2^\alpha, \alpha \geq 3$ не существует первообразных корней.

▲ $\varphi(2^\alpha) = 2^{\alpha-1}$ (все нечетные числа)

Пусть $a = 1+2t$ - нечетное. Покажем, что $a^{(2^{\alpha-2})} \equiv 1 \pmod{2^\alpha}$

$$(1+2t)^2 = 1 + 4t + 4t^2 = 1 + 4\underbrace{t(t+1)}_{\text{четное}} = 1 + 8t_1$$

$$(1+2t)^4 = (1+8t_1)^2 = 1 + 16t_1 + 64t_1^2 = 1 + 16t_2$$

$$\dots$$

$$(1+2t)^{(2^k)} = 1 + 2^{k+2}t_k$$

$$\dots$$

$$(1+2t)^{(2^{\alpha-2})} = 1 + 2^\alpha t_{\alpha-2} \equiv 1 \pmod{2^\alpha}$$

Следовательное любое нечетное число (то есть любое число, взаимно простое с 2^α) не является первообразным корнем $\Rightarrow$ первообразных корней по этому модулю нет ■

95. Показатели. Первообразные корни. Несуществование по модулям, отличным от $2^n, p^\alpha, 2p^\alpha$.

▲ Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$. $\varphi(n) = \prod_{i=1}^m \varphi(p_i^{k_i}) = \prod_{i=1}^m p_i^{k_i-1}(p_i - 1)$. Предположим противное: пусть существует g - первообразный корень по модулю n. Из теоремы Эйлера верно

$$\begin{cases} g^{(p_1-1)p_1^{k_1-1}} \equiv 1 \,(\mathrm{mod}\ p_1^{k_1}) \\ \ldots \\ g^{(p_m-1)p_m^{k_m-1}} \equiv 1 \,(\mathrm{mod}\ p_m^{k_m}) \end{cases}$$

Очевидно, что $\forall i\ z = \varphi(n)/2 = \frac{\prod_{i=1}^m p_i^{k_i-1}(p_i-1)}{2} \vdots (p_i - 1)p_i^{k_i-1}$ (двойку можно забрать из любого множителя относящегося к простому делителю, отличному от i-ого). Тогда верно

$$\begin{cases} g^z \equiv 1 \,(\mathrm{mod}\ p_1^{k_1}) \\ \ldots \\ g^z \equiv 1 \,(\mathrm{mod}\ p_m^{k_m}) \end{cases}$$

Пусть $g^z = 1 + p_1^{k_1}a = 1 + p_2^{k_2}b \Rightarrow p_1^{k_1}a = p_2^{k_2}b$. В силу взаимной простоты $p_1, p_2 \Rightarrow a \vdots p_2^{k_2} \Rightarrow g^z = 1 + p_1^{k_1}p_2^{k_2}a_1$. По индукции будем присоединять все больше множителей и в итоге получим

$$g^z = 1 + p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}t = 1 + nt \equiv 1 \,(\mathrm{mod}\ n),\ z = \varphi(n)/2 < \varphi(n) \Rightarrow$$

$$\Rightarrow g \text{ не является первообразным корнем по модулю } n \ \blacksquare$$