

Пусть $e(m) = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$ — каноническое разложение числа $e(m)$ на простые сомножители, $(g, m) = 1$. В этом случае g — первообразный корень в \mathbb{Z}_m тогда и только тогда, когда g не является решением ни одного из сравнений

$$g^{\frac{e(m)}{p_k}} \equiv 1 \pmod{m} \quad \text{при } k = 1, \dots, s.$$

Доказательство:

\Rightarrow По определению, первообразный корень не может удовлетворять ни одному из таких сравнений.

\Leftarrow Заметим, что если для некоторого i $\frac{e(m)}{p_i} \vdots \text{ord}(g)$, то g удовлетворяет сравнению $g^{\frac{e(m)}{p_i}} \equiv 1 \pmod{m}$ для этого i . Поэтому $\text{ord}(g)$ не является делителем ни одного числа вида $\frac{e(m)}{p_i}$.

\nexists III.к. $e(m) \vdots \text{ord}(g)$, то $\text{ord}(g) = p_1^{\beta_1} \cdot \dots \cdot p_s^{\beta_s}$, где $0 \leq \beta_1 \leq \alpha_1$; \dots ; $0 \leq \beta_s \leq \alpha_s$

$$\frac{e(m)}{p_i} = p_1^{\alpha_1} \cdot \dots \cdot p_{i-1}^{\alpha_{i-1}} \cdot p_i^{\alpha_i - 1} \cdot p_{i+1}^{\alpha_{i+1}} \cdot \dots \cdot p_s^{\alpha_s}$$

III.к. $\frac{e(m)}{p_i} \not\vdots \text{ord}(g)$, то $\beta_i = \alpha_i$

(иначе верно, что $\alpha_1 \geq \beta_1$; \dots ; $\alpha_{i-1} \geq \beta_{i-1}$; $\alpha_i - 1 \geq \beta_i$;
 $\alpha_{i+1} \geq \beta_{i+1}$; \dots ; $\alpha_s \geq \beta_s$,
 и тогда $\frac{e(m)}{p_i} \vdots \text{ord}(g)$)

Эти рассуждения верны для всех i , поэтому $\text{ord}(g) = e(m)$. \square III.Д.