Хф. Билет 19. (в сквозной нумерации 61) Date

Пусть $\varphi(m) = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ – каноническое разложение числа $\varphi(m)$ 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

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

Доказательство:

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

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

Т.к. $\varphi(m) \vdots \operatorname{ord}(g)$, то $\operatorname{ord}(g) = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$, где

$$0 \le \beta_1 \le \alpha_1; \ldots; 0 \le \beta_s \le \alpha_s$$

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

Т.к. $\frac{\varphi(m)}{p_i} \not\vdots\, g$, то $\beta_i = \alpha_i$

(иначе верно, что $\alpha_1 \ge \beta_1; \ldots; \alpha_{i-1} \ge \beta_{i-1}; \alpha_i - 1 \ge \beta_i;$ $\alpha_{i+1} \ge \beta_{i+1}; \ldots; \alpha_s \ge \beta_s$, и тогда $\frac{\varphi(m)}{p_i} \vdots \operatorname{ord}(g)$)

Эти рассуждения верны для всех i, поэтому $\operatorname{ord}(g) = \varphi(m)$. Ч.Т.Д.