№30 р.1 Показатель. Показатель элта из Z_m делит $\ell(m)$. Первообразный корень (опр-е и ух-е при $m \leq 7$). Пример модуля, по к-му не существует первообр-го корня

Def. min, не нулевое число δ : $a^\delta \equiv 1 \pmod m$ наз-ся показателем a по модулю m.

Def. a - первообразный корень по mod. m, если $\delta = \ell(m)$

Утв. $\delta \mid \ell(m)$

Д-во.

Пусть δ не делит $\ell(m)$.

$\Rightarrow \ell(m) = k\cdot\delta + r \quad 0 < r < \delta$

$1 \equiv a^{\ell(m)} = a^{k\delta + r} \equiv a^r \quad r < \delta$?! ⊗

Примеры:

1) при $m = 8$ $\nexists$ первообр-го корня.

2) корни при $m \leq 7$

$m = 2 \quad g = 1$

$m = 3 \quad g = 2$

$m = 4 \quad g = 3$

$m = 5 \quad g = 2$

$m = 6 \quad g = 5$

$m = 7 \quad g = 3$