Хор. Билет 18. (в сквозной нумерации 60)

Порядки (показатели) элементов в системах вычетов. ~~Равенство~~ Если $\operatorname{ord} g = k$, $\operatorname{ord} h = \ell$, и $(k, \ell) = 1$, то $\operatorname{ord}(gh) = k\ell$.

- Порядки (показатели) элементов в системах вычетов.

Рассмотрим систему вычетов по модулю m.

Опр. Пусть $\gcd(g, m) = 1$. Тогда показатель $\operatorname{ord}(g) = k$, где k - минимальное натуральное число больше 0, такое, что $g^k \equiv 1$.

Замечание. Если ~~$\gcd(g, m) = 1$~~ $\gcd(g, m) \neq 1$, то $\operatorname{ord}(g) = \infty$.

- Если $\operatorname{ord} g = k$, $\operatorname{ord} h = \ell$, и $(k, \ell) = 1$, то $\operatorname{ord}(gh) = k\ell$.

$(gh)^{k\ell} = g^{k\ell} \cdot h^{k\ell} = (g^k)^\ell \cdot (h^\ell)^k \overset{m}{\equiv} 1^\ell \cdot 1^k = 1$

Значит, $\operatorname{ord}(gh) \mid (k\ell)$

В силу теоремы из прошлого билета:

$\operatorname{ord}(g^\ell) = \dfrac{\operatorname{ord}(g)}{(\ell, \operatorname{ord} g)} = \dfrac{k}{(\ell, k)} = k$; аналогично $\operatorname{ord}(h^k) = \ell$

~~$(gh)^{\operatorname{ord}(gh)\cdot\ell} \overset{m}{\equiv} g^{\operatorname{ord}(gh)\cdot\ell} \cdot 1 \overset{m}{\neq} 1$~~

Пусть $\operatorname{ord}(gh) = k_1 \cdot \ell_1$, где $k : k_1$, $\ell : \ell_1$.

$k_2 \cdot k_1 = k$; $\ell_2 \cdot \ell_1 = \ell$

$(gh)^{k_1\ell_1} \overset{m}{\equiv} 1$, тогда $\left((gh)^{k_1\ell_1}\right)^{k_2} \overset{m}{\equiv} 1$

Вместе с тем $(gh)^{k_1\ell_1 k_2} = (gh)^{k\ell_1} = (g^k)^{\ell_1} h^{k\ell_1} \overset{m}{\equiv} h^{k\ell_1}$

$h^{k\ell_1} \overset{m}{\equiv} 1 \overset{m}{\equiv} h^{\ell_1\ell_2}$ (Заметим, что $\operatorname{ord}(h^{\ell_1}) = \dfrac{\ell}{\ell_1} = \ell_2$)

$\Rightarrow k : \ell_2 \Rightarrow$ т.к. $(k, \ell) = 1$, то $\ell_2 = 1$, аналогично $k_2 = 1$

$\Rightarrow \operatorname{ord}(gh) = k\ell$