№29 p.1 | Квадратичные вычеты и невычеты. Символ Лежандра. Формула $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$

см билет №28

Def. Символ Лежандра $\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ - вычет} \\ -1, & a \text{ - невычет} \\ 0, & \text{если } (a,p) \neq 1 \end{cases}$

Th Критерий Эйлера

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (p)$$

Д-во:

$$a^{p-1} \equiv 1 (p) \Rightarrow a^{p-1} - 1 \equiv 0 (p) \Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (p)$$

(по Th Ферма)

Обе скобки не могут одновременно делиться на p, иначе их р-ть делилась бы на p.

При этом, если a - вычет, то

$$a \equiv x^2 (p) \Rightarrow a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (p).$$

Тогда если a - вычет, то $a^{\frac{p-1}{2}} = 1$.

a - невычет, то $a^{\frac{p-1}{2}} = -1$ ☒

Сл-е 1.

$$\left(\frac{1}{p}\right) = 1$$

Сл-е 2.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \Rightarrow \begin{cases} 1, & p = 4k+1 \\ -1, & p = 4k+3 \end{cases}$$

Сл-е 3. (мультипликативность)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Сл-е 4.

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$$