Билет 85.

Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]}$ для нечетного a. (тождеством с суммой по $\left[\frac{2ax}{p}\right]$ можно пользоваться без доказательства).

Опр. $ax^2 + bx + c \equiv 0 \pmod m$ – сравнение второго порядка

Опр. Пусть p – нечетное простое число. Тогда если $(a,p) = 1$ и $\exists\, x : x^2 \equiv a \pmod p$, то a – квадратичный вычет, иначе – невычет.

Опр. Символ Лежандра:

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

Т-ма $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]}$ для нечетного a.

▲ В процессе док-ва будем пользоваться тождеством $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$

Посчитаем $\left(\frac{2a}{p}\right)$:

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) \left(\frac{4(a+p)/2}{p}\right) = \left(\frac{(a+p)/2}{p}\right) =$$

$$= (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{x2(a+x)/2}{p}\right]} = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{(a+x)x}{p}\right]} = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p} + x\right]} =$$

$$= (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \sum_{x=1}^{\frac{p-1}{2}} x} = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}} \quad \left(\text{т.к. } x \text{ целое}\right)$$

$$\left(\frac{2a}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{2}{p}\right) = \left(\frac{a}{p}\right)\cdot(-1)^{\frac{p^2-1}{8}} \Rightarrow \left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]}$$

■