№ 54

Р. 1

Ср-я второй степени. кв вычеты и невычеты.

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

См билеты 28, 29.

$S = \{1, 2, \dots \frac{p-1}{2}\}$ - полная система вычетов

$a \cdot 1 = \varepsilon_1 r_1$ $\quad \varepsilon_s = \pm 1$

$a \cdot 2 = \varepsilon_2 \cdot r_2$ $\quad r_s \in S$

$\vdots$ $\quad$ все различны

$a \cdot \frac{p-1}{2} = \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}$

Лемма (Гаусса)

$\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_s$

Д-во,

Перемножим все ср-ия.

$a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2} \equiv \prod_{s \in S} \varepsilon_s \left(r_1 r_2 \cdots r_{\frac{p-1}{2}}\right)$

↑

каждый остаток ровно один раз, итого $\Leftarrow$

$\Leftarrow$ $a \cdot k = \varepsilon_k \cdot r \Rightarrow a^2 k^2 \equiv r^2$

$a \cdot l = \varepsilon_l \cdot r \Rightarrow a^2 l^2 \equiv r^2$ $\Rightarrow a^2 x^2 \equiv r^2$ имеет 4 корня

- противоречие с ТК Лагранжа

$\Rightarrow a^{\frac{p-1}{2}} \equiv \prod_{s \in S} \varepsilon_s \Rightarrow \left(\frac{a}{p}\right) \equiv \prod_{s \in S} \varepsilon_s$ ☒

Сл-е $\left(\frac{a}{p}\right) = (-1)^{\sum_{s \in S} \left[\frac{2as}{p}\right]}$

Д-во

$\left[\frac{2as}{p}\right] = \left[2\left[\frac{as}{p}\right] + 2\left\{\frac{as}{p}\right\}\right] = 2\left[\frac{as}{p}\right] + \left[2\left\{\frac{as}{p}\right\}\right]$

но $\left[2\left\{\frac{as}{p}\right\}\right] = \begin{cases} 0, & as < p/2 \iff as \le \frac{p-1}{2} \iff \varepsilon_s = 1 \\ 1, & as > p/2 \iff as \ge \frac{p+1}{2} \iff \varepsilon_s = -1 \end{cases}$

$\iff \varepsilon_s = 1 \Rightarrow \left[\frac{2as}{p}\right]$ - чет

$\varepsilon_s = -1 \Rightarrow \left[\frac{2as}{p}\right]$ - нечет

$\Rightarrow \varepsilon_s = (-1)^{\left[\frac{2as}{p}\right]}$

$\Rightarrow$ подставим в левую $\Rightarrow \left(\frac{a}{p}\right) = \prod_{s \in S} (-1)^{\left[\frac{2as}{p}\right]} = (-1)^{\sum_{s \in S}\left[\frac{2as}{p}\right]}$

∎