№28 р.1 | Сравнения второй степени. Квадратичные вычеты и невычеты. Количество вычетов и невычетов по простому нечетному модулю p

Опр. $c_0 x^2 + c_1 x + c \equiv 0 \pmod m$ – ср-е второй степени

Опр. Пусть p – пр-е число > 2.

Если $(a,p)=1$ и $\exists x: x^2 \equiv a \pmod p$, то

a – квадратичный вычет

иначе a – невычет.

Утв. Если p – пр-е > 2, то $\exists$ ровно $\frac{p-1}{2}$ вычетов и $\frac{p-1}{2}$ невычетов.

Д-во:

Т.к. $x^2 \equiv (p-x)^2 \pmod p$, то достаточно показать, что $0^2, 1^2 \dots \left(\frac{p-1}{2}\right)^2$ – различны.

Пусть не так. и $x^2 \equiv y^2 \pmod p$. и $0 \le x, y \le \frac{p-1}{2}$

$(x^2 - y^2) \mid p \Rightarrow (x-y)(x+y) \mid p$

т.к. p – пр-е число $|x-y| < p$, то $(x+y) \mid p$

но $x+y \le p-1 \Rightarrow$?! ■