Quadratic Residue

February 8, 2026

Denote $\mathbb{F}_p = \{0, \dots, p-1\}$.

P1 (O0) Show that

$$x^2 + ax \equiv 0 \pmod{p}$$

has at most 2 solutions for $x \in \mathbb{F}_p$ for a prime p and integer a.

P2 (O1) Show that

$$x^2 + a \equiv 0 \pmod{p}$$

has at most 2 solutions for $x \in \mathbb{F}_p$ for a prime p and integer a.

P3 (O2) Show that

$$x^2 + ax + b = 0 \pmod{p}$$

has at most 2 solutions for $x \in \mathbb{F}_p$ for a prime p and integers a, b.

P4 (O2) Find all integer solutions to

$$x^2 = 2y^{10} + 11.$$

P5 (O2) Let p be a prime. Show that if there exists x such that

$$x^2 \equiv a \pmod{p}$$

and there does not exist y such that

$$y^2 \equiv b \pmod{p},$$

then there does not exist z such that

$$z^2 \equiv ab \pmod{p}.$$