CRT and basics of modular arithmetic

February 8, 2026

P1 (O1) Let p be a prime and $a, b \in \mathbb{Z}$. Show that there exists

$$x \in \{0, 1, \ldots, p-1\}$$

such that

$$ax + b \equiv 0 \pmod{p}.$$

P2 (O1) Let p, q be distinct primes and $a, b \in \mathbb{Z}$. Suppose there exist integers x_1, x_2 such that

$$ax_1 + b \equiv 0 \pmod{p} \quad \text{and} \quad ax_2 + b \equiv 0 \pmod{q}.$$

Show that there exists an integer x such that

$$ax + b \equiv 0 \pmod{pq}.$$

P3 (O3) Let $x, y \in \mathbb{N}$ and let p, q be primes. Show that the equation

$$(x+y)^2 = (pq+1)x + y$$

has at most four solutions in natural numbers.

P4 (O2) Let p be a prime and let $a \in \mathbb{N}$ with $p \nmid a$. Bob and Amy start with $n = a$ and alternately replace n by nb, where $p \nmid b$, starting with Bob. Amy wins if she can on her turn replace current number n, with m, such that

$$m \equiv 1 \pmod{p}.$$

For which values of a does Amy have a winning strategy?

P5 (O2) Let $P(x)$ be a polynomial with integer coefficients and let q be a prime. Show that for all integers a,

$$P(a+q) \equiv P(a) \pmod{q}.$$