MATH 113: DISCRETE STRUCTURES
HOMEWORK DUE WEDNESDAY WEEK 13

Problem 1. Recall that given any integers a and n, there are integers k and ℓ such that

$$\gcd(a, n) = ka + \ell n.$$

Suppose that a and n are relatively prime.

(a) Prove that a has an inverse modulo n, *i.e.*, there exists an integer x such that $ax \equiv 1 \pmod{n}$.
(b) Show that the congruence $ay \equiv b \pmod{n}$ has a solution y for all b.

Problem 2. Find all solutions $x \in \{0, 1, \ldots, n-1\}$ to the congruence $3x^2 - x + 1 \equiv 0 \pmod{n}$ for $n = 8$ and for $n = 9$. You do not need to show your work (but double-check your results!).

Problem 3. There are integers n such that -1 has a square root in $\mathbb{Z}/n\mathbb{Z}$. To test this out, for each $n \in \{2, 3, \ldots, 13\}$, find all solutions $x \in \{0, 1, \ldots, n-1\}$ to the equation

$$x^2 \equiv -1 \pmod{n}.$$

You do not need to show your work. It may help to note that $-1 \equiv n - 1 \pmod{n}$. (There is a famous theorem regarding the existence of solutions in the case n is a prime congruent to 3 modulo 4.)