Finding Square Roots
Pre-class, Week 10

We saw earlier how to solve linear modular congruences. But how about quadratic congruences, such as

$$ax^2 + bx + x \equiv 0 \pmod{m}\,?$$

As in the case of linear congruence equations, the solution of this equation reduces to solving the congruence modulo prime divisors, i.e.

$$ax^2 + bx + c \equiv 0 \pmod{p}\,.$$

For small p, we can use trial and error for x to solve the equation. But for large p, we need some serious tools.

The first tool we will use is the quadratic formula. You might object: "How does that even apply in this case?" The proof is in the class activity, but let's for now accept that the formula is valid, when interpreted appropriately. Let us consider an example.

example: We will find the solutions of $3x^2 + x + 3 \equiv 0 \pmod{17}$. The quadratic formula says the roots are $\dfrac{-1 \pm \sqrt{1-36}}{6}$. We interpret division as multiplying by the inverse and note that $6^{-1} = 3 \pmod{17}$. To find the square root of a number $\sqrt{b} \pmod{p}$, we think of it as solving for $x^2 \equiv b \pmod{p}$. Note that $-35 \equiv 16 \pmod{17}$ and $4^2 \equiv 16 \pmod{17}$. Therefore, the roots are $3(-1 \pm \sqrt{16}) \equiv 3(-1 \pm 4) \pmod{17}$. This gives us $15, 9$ as two roots modulo 17.

Since we can always find $(2a)^{-1} \pmod{p}$ for a's such that $\gcd(a,p) = 1$, the only thing we need to worry about in solving the general quadratic equation is to be able to find square roots. And, for small p values, we can easily find the square root by trial error, or use primitive roots, or in some cases, we might have a lucky guess for a square root.

1. Solve the following equations, if possible, using the quadratic formula.

a. $7x^2 - 4x + 2 \equiv 0 \pmod{11}$

b. $7x^2 - 4x - 2 \equiv 0 \pmod{11}$

c. $3x^2 - 2x + 1 \equiv 0 \pmod{13}$

d. $2x^2 - 3x + 4 \equiv 0 \pmod{13}$

In the class activity, we will investigate more generally which numbers have square roots modulo p, but we will not have a constructive method for finding a square root. Check out `https://en.wikipedia.org/wiki/Cipolla%27s_algorithm` for one such algorithm.

Over →

As we saw in the previous class activity, a quadratic residue modulo p is an a for which $x^2 \equiv a \pmod{p}$ has a solution. There is a useful notational device, called the *Legendre symbol*, in the study of quadratic residues. The definition is as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Note that the notation is a little weird, and it looks as if it is fraction, but it has a completely different meaning.

2. Using the definition, determine the value of $\left(\frac{0}{p}\right), \left(\frac{1}{p}\right), \left(\frac{4}{p}\right)$ for any p.

3. Determine the value of $\left(\frac{-1}{p}\right)$ for a few different primes p. Can you see a pattern?