Last time: Square roots

Our process for finding kth roots mod n depends on $\gcd(k,n)=1$. This basically never happens if $k=2$, so we need a new approach.

Question: For an odd prime p, what a satisfy $a \equiv b^2 \pmod{n}$?

i.e. what values a have square roots modulo p?

Let $a \in \mathbb{Z}$ with $p \nmid a$. Then if a is congruent to a square modulo p, we call it a quadratic residue (QR) modulo p. Otherwise, it's a (quadratic) nonresidue (NR) modulo p.

We showed

QR × QR = QR   QR × NR = NR   NR × NR = QR.

The Legendre symbol of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR,} \\ -1 & \text{if } a \text{ is a NR,} \\ 0 & \text{if } a \text{ is a multiple of } p. \end{cases}$$

So

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Theorem (Euler's Criterion)

If p is an odd prime then

$$a^{(p-1)/2} \equiv_p \left(\frac{a}{p}\right).$$

Corollary (Quadratic reciprocity, Part -1 and 2)

Let p be an odd prime. Then

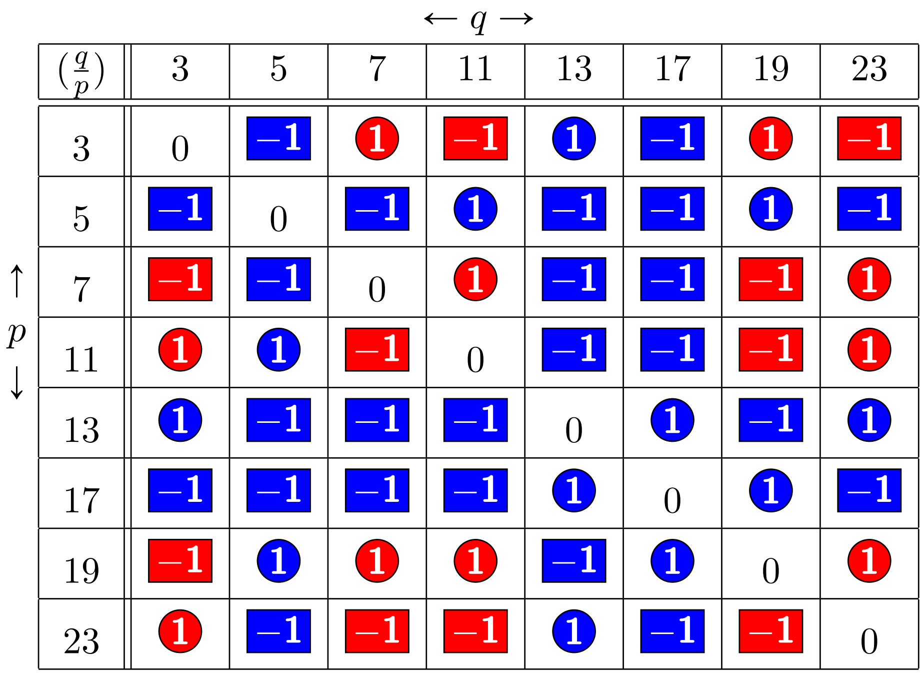
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1, \\ -1 & \text{if } p \equiv_4 -1. \end{cases} \quad \text{and} \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 \pm 1, \\ -1 & \text{if } p \equiv_8 \pm 3. \end{cases}$$

Strategy: use $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, and compute $\left(\frac{a}{p}\right)$ for small values, like primes.

← q →

↑ p ↓

$\left(\frac{q}{p}\right)$	3	5	7	11	13	17	19	23
3	0	$\boxed{-1}$	①	$\boxed{-1}$	①	$\boxed{-1}$	①	$\boxed{-1}$
5	$\boxed{-1}$	0	$\boxed{-1}$	①	$\boxed{-1}$	$\boxed{-1}$	①	$\boxed{-1}$
7	$\boxed{-1}$	$\boxed{-1}$	0	①	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①
11	①	①	$\boxed{-1}$	0	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①
13	①	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	0	①	$\boxed{-1}$	①
17	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①	0	①	$\boxed{-1}$
19	$\boxed{-1}$	①	①	①	$\boxed{-1}$	①	0	①
23	①	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①	$\boxed{-1}$	$\boxed{-1}$	0



← q →

↑ p ↓

$\left(\frac{q}{p}\right)$	3	5	7	11	13	17	19	23
3	0	$\boxed{-1}$	①	$\boxed{-1}$	①	$\boxed{-1}$	①	$\boxed{-1}$
5	$\boxed{-1}$	0	$\boxed{-1}$	①	$\boxed{-1}$	$\boxed{-1}$	①	$\boxed{-1}$
7	$\boxed{-1}$	$\boxed{-1}$	0	①	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①
11	①	①	$\boxed{-1}$	0	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①
13	①	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	0	①	$\boxed{-1}$	①
17	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①	0	①	$\boxed{-1}$
19	$\boxed{-1}$	①	①	①	$\boxed{-1}$	①	0	①
23	①	$\boxed{-1}$	$\boxed{-1}$	$\boxed{-1}$	①	$\boxed{-1}$	$\boxed{-1}$	0

blue: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ **red:** $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

Cols/rows that are all blue:

$$p, q = 5, 13, 17, 29, 37, 41, \dots \equiv_4 1$$

Theorem (Quadratic reciprocity, primes)

Let p and q be odd primes. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1, \\ -1 & \text{if } p \equiv_4 -1, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 \pm 1, \\ -1 & \text{if } p \equiv_8 \pm 3, \end{cases}$$

and

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv_4 1 \text{ or } q \equiv_4 1, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv_4 -1 \equiv_4 q. \end{cases}$$

(Presented without proof)

Example: Is 350 a perfect square modulo 13? We have

$$350 = 2 \cdot 5^2 \cdot 7,$$

so

$$\left(\frac{350}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)^2\left(\frac{7}{13}\right) = (-1)(\pm 1)^2\left(\frac{7}{13}\right) = \boxed{1} \quad \text{yes!}$$

Since $13 \equiv_4 1$, we have

$$\left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = (-1)(1).$$

Theorem (Quadratic reciprocity, primes)

Let p and q be odd primes. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1, \\ -1 & \text{if } p \equiv_4 -1, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 \pm 1, \\ -1 & \text{if } p \equiv_8 \pm 3, \end{cases}$$

and

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv_4 1 \text{ or } q \equiv_4 1, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv_4 -1 \equiv_4 q. \end{cases}$$

(Presented without proof)

Example: Is 350 a perfect square modulo 11? We still have $350 = 2 \cdot 5^2 \cdot 7$, so

$$\left(\frac{350}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{5}{11}\right)^2\left(\frac{7}{11}\right) = (-1)(\pm 1)^2\left(\frac{7}{11}\right) = \boxed{-1} \quad \text{no!}$$

Since $7 \equiv_4 -1$ and $11 \equiv_4 -1$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = (\pm 1)^2 = 1.$$

Theorem (Quadratic reciprocity, primes)

Let p and q be odd primes. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1, \\ -1 & \text{if } p \equiv_4 -1, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 \pm 1, \\ -1 & \text{if } p \equiv_8 \pm 3, \end{cases}$$

and

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv_4 1 \text{ or } q \equiv_4 1, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv_4 -1 \equiv_4 q. \end{cases}$$

(Presented without proof)

You try: Compute

$$\left(\frac{20}{31}\right), \quad \left(\frac{14}{137}\right), \quad \text{and} \quad \left(\frac{55}{179}\right).$$

(31, 137, and 179 are prime)

Thm. For a composite number $b = p_1 p_2 \cdots p_\ell$, we have

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_\ell}\right).$$

Theorem (Quadratic reciprocity, composites)

Let a and b be odd positive integers. Then

$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv_4 1, \\ -1 & \text{if } b \equiv_4 -1, \end{cases} \qquad \left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv_8 \pm 1, \\ -1 & \text{if } b \equiv_8 \pm 3, \end{cases}$$

and

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{a}{b}\right) & \text{if } b \equiv_4 1 \text{ or } a \equiv_4 1, \\ -\left(\frac{a}{b}\right) & \text{if } b \equiv_4 -1 \equiv_4 a. \end{cases}$$