Lecture 9.2

Last time:

- The laws of quadratic reciprocity are:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1 \text{ or } 7 \pmod 8 \\ -1, & p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if either is } \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if both are } \equiv 3 \pmod 4 \end{cases}$$

- Using these laws, together with

  * $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod{p}$

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

  * $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

allows us to quickly decide whether

$x^2 \equiv a \pmod{p}$ has solutions.

Let's prove Quadratic Reciprocity,

which can be written more compactly

as:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Exercise 1: Check that this formula is equivalent to the one stated above.

Recall that $\left(\frac{a}{p}\right) = (-1)^g$ where g is the number of $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ which fall into negative classes among

$$-\tfrac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \tfrac{p-1}{2}.$$

For a real number x, let $\lfloor x \rfloor$ be the "floor" of x, i.e. the largest integer

that of x, i.e. the largest integer $n \leq x$.

Lemma: For $p > 2$ prime and $a \in \mathbb{Z}$ odd and relatively prime to p,

$$\left(\frac{a}{p}\right) = (-1)^s \text{ where}$$

$$s = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ia}{p} \right\rfloor .$$

Pf: As before, let $ia \equiv r_i \pmod{p}$ for a unique $-\frac{p-1}{2} \leq r_i \leq \frac{p-1}{2}$ for each i.

To prove the formula for $\left(\frac{a}{p}\right)$, it's

enough to show r_i is positive if and only if $\left\lfloor \frac{2ia}{p} \right\rfloor$ is even, since then

$$s = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ia}{p} \right\rfloor \equiv g \pmod 2.$$

Write $ia = pk + r_i$ for $k \in \mathbb{Z}$.

Then $\left\lfloor \frac{2ia}{p} \right\rfloor = \left\lfloor 2k + \frac{2r_i}{p} \right\rfloor$

$$= \begin{cases} 2k, & \text{if } 0 \le r_i \le \frac{p-1}{2} \\ 2k-1, & \text{if } -\frac{p-1}{2} \le r_i < 0. \end{cases}$$

This proves the claim. □

In fact, it's enough to use the terms $\left\lfloor \frac{ia}{p} \right\rfloor$ in our sum:

Lemma For a, p as above, $\left(\frac{a}{p}\right) = (-1)^t$ where $t = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor$.

Pf: Since a, p are both odd, $b = \frac{a+p}{2} \in \mathbb{Z}$ and we can expand

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right) = \left(\frac{2b}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{b}{p}\right).$$

By the previous Lemma, $\left(\frac{b}{p}\right) = (-1)^{s_b}$

where $s_b = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ib}{p} \right\rfloor$

$$= \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{i(a+p)}{p} \right\rfloor$$

$$= \sum_{i=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{ia}{p} \right\rfloor + i \right)$$

$$= \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor + \sum_{i=1}^{\frac{p-1}{2}} i$$

$$= t + \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2}$$

$$= t + \frac{p^2-1}{8}.$$

Then $\left(\frac{a}{p}\right) = (-1)^t (-1)^{\frac{p^2-1}{8}} \left(\frac{2}{p}\right)$,

but the quadratic reciprocity law for $\left(\frac{2}{p}\right)$ is equivalent to

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

so the terms cancel and we get $\left(\frac{a}{p}\right) = (-1)^t$. □

Exercise 2: Verify that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Pf of Quadratic Reciprocity: Let

q be an odd prime distinct from p.

Set $s(p,q) = \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor$ and

$$s(q,p) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$$

so that by the Lemma,

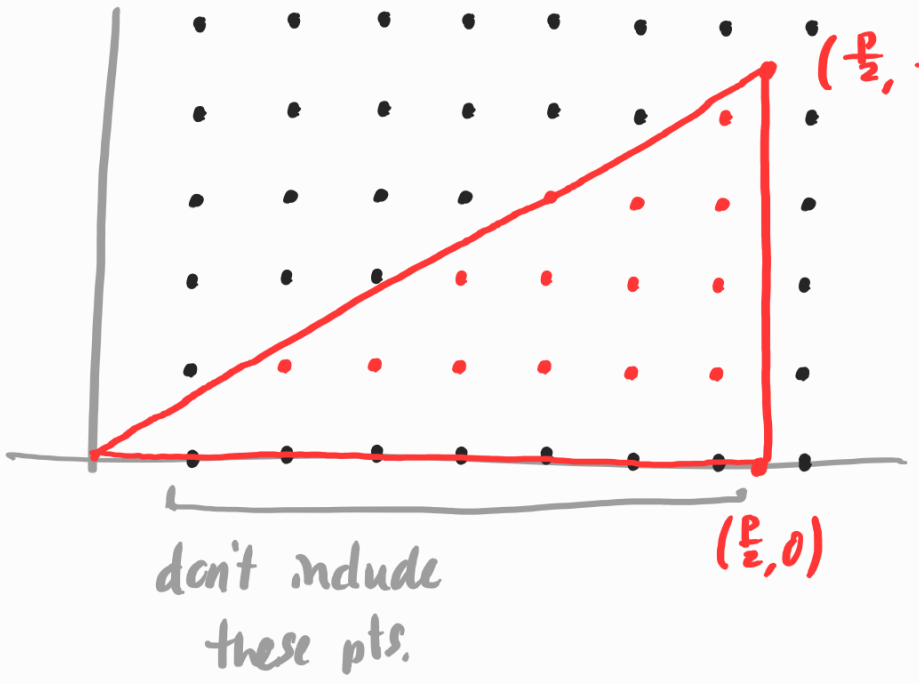
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s(p,q)}(-1)^{s(q,p)}.$$

To prove Quadratic Reciprocity, we will

show $s(p,q) + s(q,p) = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.

The amazing insight is to count

lattice points in the triangle



14 lattice points

A lattice point in $\mathbb{R}^2$ is a point (x,y) with $x, y \in \mathbb{Z}$.

Let's count them column-by-column, using the fact that the hypotenuse lies

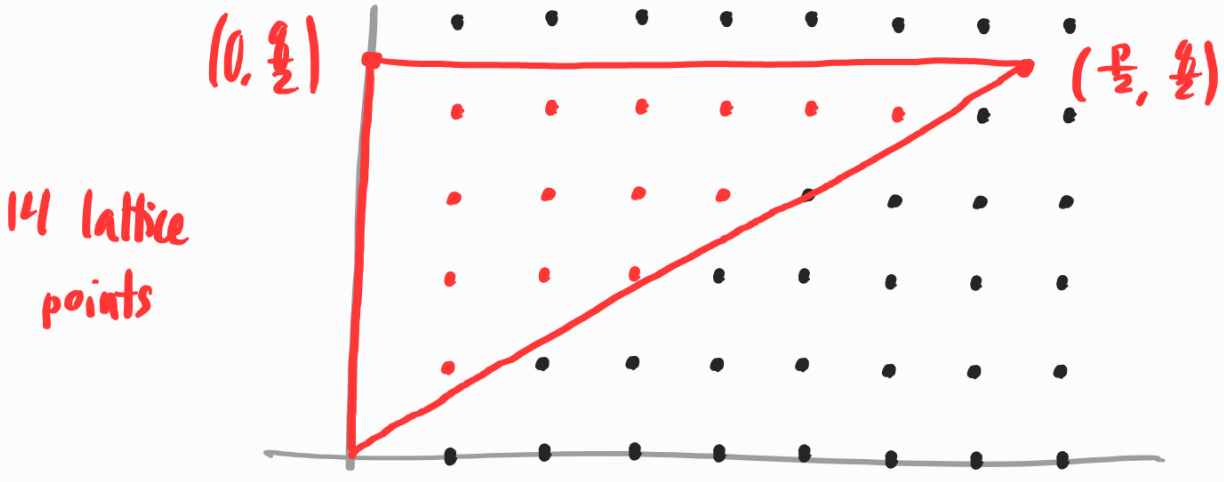
along $y = \frac{q}{p}x$:

- for $x = 1$, there are $\left\lfloor \frac{q}{p} \right\rfloor$ pts.
- for $x = 2$, there are $\left\lfloor \frac{2q}{p} \right\rfloor$ pts.
- in general, there are $\left\lfloor \frac{jq}{p} \right\rfloor$ lattice points in the triangle with $x = j$, for $1 \le j \le \frac{p-1}{2}$.

This means the total number of lattice points in the triangle is

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor = s(q,p).$$

Now let's reflect the triangle over its hypotenuse and count lattice points again:



By the same strategy, the total number of lattice points in this new triangle will be $s(p,q) = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$.

Since $\gcd(p,q) = 1$, no lattice points lie on the hypotenuse, so we just counted the total number of lattice points in the rectangle $(0, \frac{p}{2}) \times (0, \frac{q}{2})$ to be $s(p,q) + s(q,p)$.

On the other hand, the number of lattice points in this box is exactly $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$, so we're done. □

Exercise 3: Practice

Exercise 3: Practice counting lattice points inside rectangles $(0, \frac{a}{2}) \times (0, \frac{b}{2})$ and compare what happens when a and b are distinct primes, are coprime composites or share a common factor.

Make a conjecture based on your observations.

Next time: an application of quadratic reciprocity.