From last time:

DEFINITION: Let p be an odd prime. For $r \in \mathbb{Z}$ not a multiple of p we define the **Legendre symbol** of r with respect to p as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } [r] \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{if } [r] \text{ is a not square in } \mathbb{Z}_p. \end{cases}$$

PROPOSITION: Let p be an odd prime and a, b integers not divisible by p. Then

(1) $a \equiv b \pmod{p}$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

(3) $\left(\frac{a^2}{p}\right) = 1$. $\square$

THEOREM (QUADRATIC RECIPROCITY): Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \qquad \text{if either } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4},$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \qquad \text{if both } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}.$$

THEOREM (QUADRATIC RECIPROCITY PART 2): Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = 1 \qquad \text{if } p \equiv \pm 1 \pmod{8},$$

$$\left(\frac{2}{p}\right) = -1 \qquad \text{if } p \equiv \pm 3 \pmod{8}.$$

(1) Computing quadratic residues with QR & QR part 2:
   (a) Compute $\left(\frac{2}{7}\right)$, $\left(\frac{2}{11}\right)$, and $\left(\frac{2}{101}\right)$.
   (b) What does QR say about $\left(\frac{3}{7}\right)$? Simplify the new Legendre symbol and evaluate.
   (c) Apply the same strategy as the previous part to compute $\left(\frac{13}{107}\right)$.

(2) Computing quadratic residues QR, QR part 2, and the proposition:
   (a) Compute $\left(\frac{10}{13}\right)$ by starting with Proposition part (2), then continuing as in the previous problem.
   (b) Compute $\left(\frac{38}{127}\right)$.

(3) How many solutions does the equation $[4]x^2 - [13]x + [5] = 0$ have in $\mathbb{Z}_{103}$?

GAUSS' LEMMA: Let p be an odd prime and set $p' = \frac{p-1}{2}$. Note that every integer coprime to p is congruent modulo p to a unique integer in the set $S = \{\pm 1, \pm 2, \cdots, \pm p'\}$.

Let a be an integer coprime to p. Consider the sequence

$$a, 2a, 3a, \ldots, p'a$$

and replace each element in the sequence with element of S that is congruent with modulo p to get a list L of p'-many elements of S.

Then $\left(\dfrac{a}{p}\right) = (-1)^{\nu}$, where ν is the number of negative integers in L.

LEMMA: Let p and q be two coprime odd positive integers. Then

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

(4) (Partial) proof of QR part 2 using Gauss' Lemma: Let's just deal with $p \equiv 3 \pmod 8$. Write $p = 8\ell + 3$, so $p' = 4\ell + 1$. Compute L explicitly and deduce the result.

(5) Proof of Gauss' Lemma:
  (a) Show that none of the elements of L equal each other, nor are $\pm$ each other. Conclude that L is, in some order, $\pm 1, \pm 2, \ldots, \pm p'$, with each of $1, 2, \ldots, p'$ occurring once with a definite sign.
  (b) Compute the product of L modulo p two different ways and simplify.
  (c) Apply Euler's criterion, and conclude the proof.

(6) Proof of QR using Gauss' Lemma and other lemma: Take p, q distinct odd primes. For each $k \in \{1, 2, \ldots, p'\}$, write $kq = \lfloor kq/p \rfloor p + r_k$ with $1 \leq r_k \leq p - 1$. Write

$$\{[q], [2q], \ldots, [p'q]\} = \{[r_1], [r_2], \ldots, [r_{p'}]\} = \{[a_1], \ldots, [a_u]\} \cup \{[-b_1], \ldots, [-b_v]\}$$

with $0 < a_i < p'$ and $0 < b_i < p'$, as in the statement of Gauss' Lemma.
  (a) Explain why $\sum_{k=1}^{p'} k = \frac{p^2-1}{8}$.
  (b) Explain why $\sum_{k=1}^{p'} r_k = \sum_{i=1}^{t} a_i - \sum_{i=1}^{v} b_i + vp$.
  (c) Explain why $\sum_{i=1}^{t} a_i + \sum_{i=1}^{v} b_i = \frac{p^2-1}{8}$.
  (d) Explain why $\frac{p^2-1}{8} q = p \sum_{k=1}^{p'} \lfloor kq/p \rfloor + \sum_{i=1}^{t} a_i - \sum_{i=1}^{v} b_i + vp$.
  (e) Explain why $\frac{p^2-1}{8} (q-1) = p \sum_{k=1}^{p'} \lfloor kq/p \rfloor + vp - 2 \left(\sum_{i=1}^{v} b_i\right)$.
  (f) Explain why $v \equiv \sum_{k=1}^{p'} \lfloor kq/p \rfloor \pmod 2$, and apply Gauss' Lemma to deduce

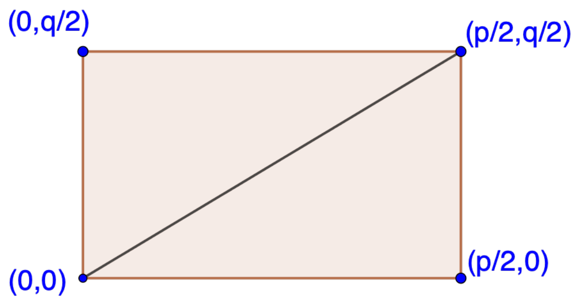
$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{p'} \lfloor kq/p \rfloor}.$$

  (g) Switch the roles of p and q, and plug the result into the other Lemma to show that

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

Deduce the theorem.

(7) Proof of other lemma: Consider the rectangle below.



(a) Show that the number of integer points inside the rectangle (excluding the edges) is $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

(b) Show that there are no integer points on the diagonal.

(c) Show that the number of integer points below the diagonal is $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$.

(d) Show that the number of integer points above the diagonal is $\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor$. Conclude the proof.