QUADRATIC RECIPROCITY

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) $\left(\frac{a^2}{p}\right) = 1$. □

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 $\left(\frac{13}{107}\right)$.

(a) $\left(\frac{2}{7}\right) = 1$, $\left(\frac{2}{11}\right) = -1$, and $\left(\frac{2}{101}\right) = -1$.
(b) $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
(c) $\left(\frac{13}{107}\right) = \left(\frac{107}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$.

(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 $\left(\frac{38}{127}\right)$.

(a) $\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = -1 \cdot \left(\frac{13}{5}\right) = -1 \cdot \left(\frac{3}{5}\right) = -1 \cdot \left(\frac{5}{3}\right) = -1 \cdot \left(\frac{2}{3}\right) = -1 \cdot -1 = 1.$
(b) $\left(\frac{38}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{19}{127}\right) = 1 \cdot -1 \cdot \left(\frac{127}{19}\right) = 1 \cdot -1 \cdot \left(\frac{127}{19}\right) = 1 \cdot -1 \cdot \left(\frac{13}{19}\right) = 1 \cdot -1 \cdot \left(\frac{19}{13}\right) = 1 \cdot -1 \cdot \left(\frac{5}{13}\right) = 1 \cdot -1 \cdot \left(\frac{13}{5}\right) = 1 \cdot -1 \cdot \left(\frac{3}{5}\right) = 1 \cdot -1 \cdot -1 = 1.$

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

We compute $[b^2 - 4ac] = [169 - 2 \cdot 4 \cdot 5] = [129] = [26]$. We compute $\left(\frac{26}{103}\right) = \left(\frac{2}{103}\right)\left(\frac{13}{103}\right) = 1 \cdot \left(\frac{103}{13}\right) = 1 \cdot \left(\frac{12}{13}\right) = 1 \cdot \left(\frac{4}{13}\right) \cdot \left(\frac{3}{13}\right) = 1 \cdot 1 \cdot \left(\frac{13}{3}\right) = 1 \cdot 1 \cdot \left(\frac{1}{3}\right) = 1$. So, $[26] \in \mathbb{Z}_{103}$ is a nonzero square, and there are two solutions.

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.

We apply Gauss' Lemma with $a = 2$: we look at the sequence

$$2, 4, 6, \ldots 4\ell, 4\ell + 2, \ldots, 8\ell + 2$$

and compute the list L

$$L = \{2, 4, 6, \ldots 4\ell, -(4\ell + 1), \ldots, -1\}.$$

Thus, the number of positive elements is 2ℓ and the number of negative elements is $p' - 2\ell = 2\ell + 1$, so by Gauss' Lemma,

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

(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, $\pm 1, \pm 2, \dots, \pm p'$, with each of $1, 2, \dots, p'$ 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.

(a) None are equal, since $ia \equiv ja \pmod p$ implies $i \equiv j \pmod p$, and none are negative of each other, since $ia \equiv -ja \pmod p$ implies $i + j \equiv 0 \pmod p$, which can't happen for $0 \le i < j \le p'$.
(b) The product of L modulo p is

$$a \cdot 2a \cdot 3a \cdots p'a \equiv (\pm 1) \cdot (\pm 2) \cdot (\pm 3) \cdots (\pm p') \pmod p,$$

so, if v is the number of negatives, we have

$$a^{p'}(p')! \equiv (-1)^v (p')! \pmod p.$$

Since $(p')!$ is a unit mod p, we must have

$$a^{p'} \equiv (-1)^v \pmod p.$$

(c) By Euler's criterion,

$$\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^v \pmod p.$$

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

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

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.

(a) This sum equals $\frac{p'(p'+1)}{2} = \frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}$.
(b) Every r_k is either some a_i or $p - b_i$, and each a_i and b_i occurs exactly once.

(c) As in the proof of Gauss' Lemma, each number between 1 and p' occurs exactly once as an a_i or as a b_i. Then use part (a).

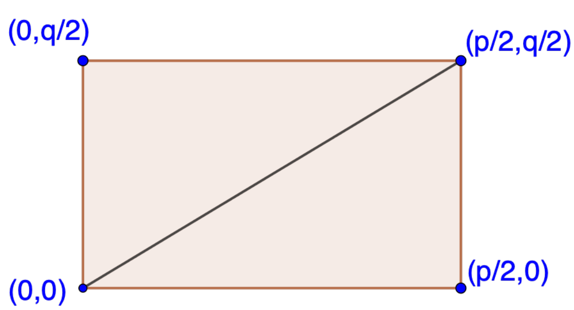
(d)
$$\frac{p^2-1}{8}(q-1) = \sum_{k=1}^{p'} kq = p\sum_{k=1}^{p'}\lfloor kq/p\rfloor + \sum_{k=1}^{p'} r_k$$
$$= p\sum_{k=1}^{p'}\lfloor kq/p\rfloor + \sum_{i=1}^{t} a_i - \sum_{i=1}^{v} b_i + vp.$$

(e) Take (d) minus (c).

(f) Taking (e) modulo 2, since $q-1$ is even and p is odd, we get this congruence. By Gauss' Lemma, $\left(\frac{q}{p}\right) \equiv (-1)^v$, and swapping in for v, we get the statement.

(g) Switching roles,
$$\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'}\lfloor \ell p/q\rfloor},$$
where $q' = \frac{q-1}{2}$. Plugging into the other Lemma yields
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$
Since $\frac{p-1}{2}$ is even if and only if $p \equiv 1 \pmod 4$ and likewise with q, the exponent above is odd if and only if $p \equiv q \equiv 3 \pmod 4$. The statement of QR follows.

(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.

(a) The integer points inside are exactly the pairs (k,ℓ) with $1 \le k \le \frac{p-1}{2}$ and $1 \le \ell \le \frac{q-1}{2}$.

(b) A point (a, b) on the diagonal would have $qa = pb$, which would imply a is a multiple of p (since p, q coprime), which is impossible.

(c) The possible x values are $1 \leq k \leq \frac{p-1}{2}$ and for any given k, the possible y values are bounded below by 1 and above by kq/p; since these are integers, they range from 1 to $\lfloor \frac{kq}{p} \rfloor$. This yields the sum in the statement.

(d) The first part follows from (c) by switching roles. Since every point in the square is either above or below the diagonal, the equality follows from (a), (c), and (d).