23. 4/10

23.1. *The Legendre symbol* Let p be a positive odd prime.

Previously, we discussed how the structure of nonzero QRs and QNRs modulo p under multiplication is analogous to the structure of 1 and -1 under multiplication. To make this precise, define the *Legendre symbol* modulo p to be the function

$$\left(\frac{-}{p}\right) : (\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$$

for which

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a QR mod } p, \\ -1 & a \text{ is a QNR mod } p. \end{cases}$$

(Don't confuse this notation with a fraction!) The left-hand side is usually pronounced "a on p".

We showed on March 17 that the Legendre symbol is multiplicative:

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

for all $a, b \in (\mathbf{Z}/p\mathbf{Z})^\times$.

Therefore, to calculate $\left(\frac{a}{p}\right)$ for an arbitrary congruence class $a + p\mathbf{Z}$, it's enough to calculate $\left(\frac{\pm 1}{p}\right)$ and $\left(\frac{q}{p}\right)$ for prime q.

23.2. Certainly, $\left(\frac{1}{p}\right) = 1$. More interestingly, we can restate the equivalence

$$-1 \text{ is a QR modulo } p \iff p \equiv 1 \pmod 4$$

as the identity

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

because $\frac{p-1}{2}$ is even when $p \equiv 1 \pmod 4$, and odd when $p \equiv 3 \pmod 4$. In the same way, we can restate the equivalences

$$\begin{aligned} -2 \text{ is a QR modulo } p &\iff p \equiv 1, 3 \pmod 8, \\ -3 \text{ is a QR modulo } p &\iff p \equiv 1 \pmod 3 \end{aligned}$$

as the identities

$$\begin{aligned} \left(\frac{-2}{p}\right) &= (-1)^{\frac{(p-1)(p-3)}{8}}, \\ \left(\frac{-3}{p}\right) &= \left(\frac{p}{3}\right), \end{aligned}$$

respectively. Since $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, these are equivalent to

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$
$$\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

23.3. *Quadratic reciprocity* What happens if we do more calculations?

Example 23.1. We list the odd primes $p \neq 5$, and box those for which 5 is a quadratic residue modulo p:

$$3, 7, \boxed{11}, 13, 17, \boxed{19}, 23, \boxed{29}, \boxed{31}, 37, \boxed{41}, 43, 47, 53, \boxed{59}, \ldots$$

They are precisely the primes whose last digit is either 1 or 9. Thus they are precisely the odd primes congruent to 1 or 4 modulo 5.

In general, we are led to conjecture:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$
$$\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right),$$
$$\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{11}\right),$$
$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right),$$
$$\ldots$$

So we are led to conjecture that for $q \neq p$ a positive odd prime,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & q \equiv 1 \pmod 4, \\ (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) & q \equiv 3 \pmod 4 \end{cases}$$
$$= \begin{cases} \left(\frac{p}{q}\right) & p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right) & p, q \equiv 3 \pmod 4. \end{cases}$$

We can rewrite the last formula as:

Theorem 23.2 (Quadratic Reciprocity)**.** *For positive odd primes $p \neq q$, we have*

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

23.4. The law of quadratic reciprocity, combined with the multiplicativity of the Legendre symbol, is usually the fastest way to determine if an integer yields a quadratic residue modulo p. We may need the "supplementary" laws

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

to finish the job.

Example 23.3. Two ways to determine whether -43 is a QR modulo 163:

(1) First compute

$$\left(\frac{-43}{163}\right) = \left(\frac{-1}{163}\right)\left(\frac{43}{163}\right) = (-1)^{\frac{162}{2}}\left(\frac{43}{163}\right) = -\left(\frac{43}{163}\right).$$

Next observe that 43 is prime, and compute

$$\left(\frac{43}{163}\right) = (-1)^{\frac{162\cdot 42}{4}}\left(\frac{163}{43}\right) = -\left(\frac{163}{43}\right) = -\left(\frac{34}{43}\right) = -\left(\frac{2}{43}\right)\left(\frac{17}{43}\right).$$

Finally compute

$$\left(\frac{2}{43}\right) = (-1)^{\frac{43^2-1}{8}} = (-1)^{231} = -1,$$
$$\left(\frac{17}{43}\right) = (-1)^{21\cdot 8}\left(\frac{43}{17}\right) = \left(\frac{9}{17}\right) = 1.$$

Altogether, $\left(\frac{-43}{163}\right) = -(-(-1\cdot 1)) = -1$, so the answer is no.

(2) Alternatively, compute

$$\left(\frac{-43}{163}\right) = \left(\frac{120}{163}\right) = \left(\frac{2}{163}\right)^3\left(\frac{3}{163}\right)\left(\frac{5}{163}\right),$$

then compute

$$\left(\frac{2}{163}\right) = (-1)^{\frac{163^2-2}{8}} = (-1)^{3321} = -1,$$
$$\left(\frac{3}{163}\right) = (-1)^{81\cdot 1}\left(\frac{163}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$
$$\left(\frac{5}{163}\right) = (-1)^{81\cdot 2}\left(\frac{163}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

23.5. *Proof of the formula for* $\left(\frac{2}{p}\right)$ We already proved the formula for $\left(\frac{-1}{p}\right)$ in the course of proving the two-squares theorem. It was a special case of Euler's criterion:

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

In turn, we proved Euler's criterion by a "shuffling-the-deck"-type argument.

We will prove the formula for $\left(\frac{2}{p}\right)$ by a similar trick. We can rewrite the formula as

$$\begin{aligned}\left(\frac{2}{p}\right) &= \begin{cases} 1 & p \equiv 1, 7 \pmod{8}, \\ -1 & p \equiv 3, 5 \pmod{8} \end{cases} \\ &= \begin{cases} (-1)^{\frac{p-1}{4}} & p \equiv 1 \pmod{4}, \\ (-1)^{\frac{p+1}{4}} & p \equiv 3 \pmod{4}. \end{cases}\end{aligned}$$

The case where $p \equiv 3 \pmod{4}$ is left to Problem Set 5.

In what follows, we explain the case where $p \equiv 1$ (mod 4) through the example $p = 13$. Namely, observe that

$$\begin{aligned} 12! &= (1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11)(2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12) \\ &= (1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11)(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)(2^6) \\ &= (1 \cdot 3 \cdot 5)(7 \cdot 9 \cdot 11)(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)(2^6) \\ &\equiv (-12)(-10)(-8)(7 \cdot 9 \cdot 11)(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)(2^6) \pmod{13} \\ &\equiv (-1)^3(7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12)(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)(2^6) \pmod{13} \\ &\equiv (-1)^3(2^6)12! \pmod{13}. \end{aligned}$$

Since 12! is invertible modulo 13, we can cancel it from both sides, then multiply both sides by $(-1)^3$, to get

$$2^6 \equiv (-1)^3 \pmod{13}.$$

The left-hand side equals $\left(\frac{2}{13}\right)$ by Euler's criterion. The right-hand side equals $(-1)^{\frac{13-1}{4}}$.

24. 4/12

24.1. What are the odd primes $p \neq 7$ for which 7 is a quadratic residue modulo p? By quadratic reciprocity,

$$\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{7-1}{2}}\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right).$$

Above, $(-1)^{\frac{p-1}{2}}$ equals 1 when $p \equiv 3 \pmod 4$, and equals -1 otherwise; $\left(\frac{p}{7}\right)$ equals 1 when $p \equiv 1, 2, 4 \pmod 7$, and equals -1 otherwise. So

$$\left(\frac{7}{p}\right) = 1 \iff \begin{array}{rl} \text{either} & \begin{cases} p \equiv 1 \pmod 4, \\ p \equiv 1, 2, 4 \pmod 7 \end{cases} \\ \text{or} & \begin{cases} p \equiv 3 \pmod 4, \\ p \equiv 3, 5, 6 \pmod 7 \end{cases} \end{array}$$

The right-hand side can be reformulated in terms of congruences modulo 28.

24.2. *Quotient groups* We will use the "strong" Chinese Remainder Theorem and group theory to prove quadratic reciprocity. First we need a review:

If $(G, \star)$ is a group and $H \subseteq G$ a subgroup, then a *left coset* of H is a subset $S \subseteq G$ such that for some $x \in G$, we can write

$$S = \{x \star h \mid h \in H\}.$$

In this case, x is called a *representative* of the coset, and we write $S = x \star H$. Note that the representative determines the coset, but not vice versa. We write G/H for the set of left cosets of H.

All the groups we've studied have been *abelian*: This condition on G means $x \star y = y \star x$ for all $x, y \in G$. For such G, the set G/H forms a group in its own right, under the operation $\circ$ defined by

$$S \circ T = \{s \star t \mid s \in S,\ t \in T\}.$$

It's not obvious at first that $S \circ T$ is still a coset of H, but we can prove it: If $S = x \star H$ and $T = y \star H$, then

$$\begin{aligned} S \circ T &= \{x \star h \star y \star h' \mid h, h' \in H\} \\ &= \{x \star y \star h \star h' \mid h, h' \in H\} \\ &= x \star y \star H, \end{aligned}$$

by the abelian property and the closedness of H under multiplication. We say that $(G/H, \circ)$ is the *quotient* of G by H.

Example 24.1. For any $m \in \mathbf{Z}$, the set $H = m\mathbf{Z}$ forms a subgroup of $G = (\mathbf{Z}, +)$. Here, the quotient group $(G/H, \circ)$ is precisely $(\mathbf{Z}/m\mathbf{Z}, +)$.

24.3. Suppose G/H is finite. We say that $\{g_1, \ldots, g_k\} \subseteq G$ is a *full set of coset representatives* for H in G iff $g_1 H, \ldots, g_k H$ are all the elements of G/H, without repetition. Note that in this case, k only depends on H. The following observation will be key to our proof of quadratic reciprocity.

Lemma 24.2. *Suppose G/H is finite. If $\{g_1, \ldots, g_k\}$ and $\{g'_1, \ldots, g'_k\}$ are two full sets of coset representatives for H in G, then*

$$g_1 \star \cdots \star g_k \star H = g'_1 \star \cdots \star g'_k \star H$$

as cosets. Thus, $g_1 \star \cdots \star g_k$ and $g'_1 \star \cdots \star g'_k$ only differ by (composing under $\star$ with) an element of H.

24.4. Let p and q be distinct (positive) odd primes. Then

$$G = (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$$

forms a group under coordinate-wise multiplication, and

$$H = \{(1 + p\mathbf{Z}, 1 + q\mathbf{Z}), (-1 + p\mathbf{Z}, -1 + q\mathbf{Z})\}$$

forms a subgroup of G.

It will be convenient to introduce the notation $\pmod{p, q}$, so that I can write

$$(a, b) \pmod{p, q} \quad \text{to mean} \quad (a + p\mathbf{Z}, b + q\mathbf{Z})$$

going forward.

To give a full set of coset representatives for H in G, it suffices to give $|G/H|$ elements of G whose corresponding cosets are pairwise distinct: that is, elements $(a_i + p\mathbf{Z}, b_i + q\mathbf{Z})$ for $1 \leq i \leq |G/H|$ such that

$$(a_i, b_i) \not\equiv (a_j, b_j), (-a_j, -b_j) \pmod{(p, q)} \qquad \text{for all } i \neq j.$$

Note that $|G| = (p-1)(q-1)$ and $|H| = 2$, so

$$|G/H| = \frac{1}{2}(p-1)(q-1).$$

We'll generalize the following example:

Example 24.3. Take $p = 3$ and $q = 5$. Then

$$G = \{(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4)\},$$
$$H = \{(1,1), (2,4)\}.$$

We claim that $(1,1), (1,2), (2,1), (2,2)$ is a full set of coset representatives for H in G. Indeed,

$$(1,1) \star H = \{(1,1), (2,4)\} = H, \qquad (1,2) \star H = \{(1,2), (2,3)\},$$
$$(2,1) \star H = \{(2,1), (1,4)\}, \qquad (2,2) \star H = \{(2,2), (1,3)\}.$$

Every element of G occurs in exactly one of these four sets.

25. 4/14

25.1. We complete the proof of quadratic reciprocity. Like last time, we set $G = (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$ and

$$H = \{(1,1), (-1,-1) \pmod{p, q}\}.$$

We will exhibit two different full sets of coset representatives for H in G, then compare their products.

Lemma 25.1. *The set*

$$X = \left\{(a + p\mathbf{Z}, b + q\mathbf{Z}) \in G \mid 1 \leq b \leq \tfrac{q-1}{2}\right\}$$

is a full set of coset representatives for H in G.

Proof. We must show that if $(a + p\mathbf{Z}, b + q\mathbf{Z}), (a' + p\mathbf{Z}, b' + q\mathbf{Z}) \in X$ satisfy $(a, b) \equiv \pm(a', b') \pmod{p, q}$, then we must have $(a, b) \equiv (a', b')$. But since $1 \leq b, b' \leq \frac{q-1}{2}$, we must have $b \equiv b'$, which then forces $a \equiv a'$. Finally, X has the right size $\frac{1}{2}(p-1)(q-1)$. □

25.2. Let $G' = (\mathbf{Z}/pq\mathbf{Z})^\times$ as a group under multiplication. Recall that by the Chinese Remainder Theorem, the map

$$\begin{array}{rcl} G' & \xrightarrow{f} & G \\ a + pq\mathbf{Z} & \mapsto & (a + p\mathbf{Z}, a + q\mathbf{Z}) \end{array}$$

is an isomorphism of groups. Under this isomorphism, $H \subseteq G$ corresponds to

$$H' = \{(1 + pq\mathbf{Z}), (-1 + pq\mathbf{Z})\} \subseteq G'.$$

To give a full set of coset representatives for H' in G', it suffices to give elements $n_i + pq\mathbf{Z} \in G'$ for $1 \leq i \leq |G'/H'|$ such that $n_i \not\equiv \pm n_j \pmod{pq}$ for all $i \neq j$. Note that $|G'/H'| = |G/H|$.

Lemma 25.2. *The set*

$$Y' = \{n + pq\mathbf{Z} \in (\mathbf{Z}/pq\mathbf{Z})^\times \mid 1 \leq n \leq \tfrac{pq-1}{2}\}$$

is a full set of coset representatives for H' in G'.

Proof. We must show that if $n + pq\mathbf{Z}, n' + pq\mathbf{Z} \in Y'$ satisfy $n \equiv \pm n'$, then we must have $n \equiv n'$. This follows from the condition $1 \leq n, n' \leq \frac{pq-1}{2}$. To show that Y has the right size, we must show that $|Y'| = \frac{1}{2}|G'|$. This follows from observing that G' is the disjoint union of Y' and $-Y' = \{-y \mid y \in Y'\}$. □

Corollary 25.3. *The set*

$$Y = f(Y) = \left\{(n + p\mathbf{Z}, n + q\mathbf{Z}) \in G \mid 1 \leq n \leq \tfrac{pq-1}{2} \text{ and } \gcd(n, pq) = 1\right\}$$

is a full set of coset representatives for H in G.

25.3. Now we finish the proof of quadratic reciprocity. Let $x_1, \dots, x_{|G/H|}$, *resp.* $y_1, \dots, y_{|G/H|}$ be an ordering of the elements of X, *resp.* Y. By Lemma 24.2,

$$x_1 \star \cdots \star x_{|G/H|} \star H = y_1 \star \cdots \star y_{|G/H|} \star H$$

as cosets, where $\star$ is the group law of G, *i.e.*, coordinate-wise multiplication. What does this actually mean? We calculate both sides:

Lemma 25.4. *We have*

$$x_1 \star \cdots \star x_{|G/H|} \equiv ((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}) \pmod{p, q}.$$

Proof. Explicitly,

$$\begin{aligned} x_1 \star \cdots \star x_{|G/H|} &\equiv \prod_{\substack{1 \le a \le p-1 \\ 1 \le b \le (q-1)/2}} (a, b) \pmod{p, q} \\ &\equiv ((p-1)!^{\frac{q-1}{2}}, (\tfrac{q-1}{2})!^{p-1}) \pmod{p, q}. \end{aligned}$$

We can simplify both entries using Wilson's theorem. The first entry becomes $(-1)^{\frac{q-1}{2}} \pmod{p}$. As for the second entry,

$$-1 \equiv (q-1)! \equiv (-1)^{\frac{q-1}{2}} (\tfrac{q-1}{2})!^2 \pmod{q},$$

from which

$$\begin{aligned} (\tfrac{q-1}{2})!^{p-1} &\equiv ((\tfrac{q-1}{2})!^2)^{\frac{p-1}{2}} \pmod{q} \\ &\equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod{q} \end{aligned}$$

as claimed. □

Lemma 25.5. *We have*

$$y_1 \star \cdots \star y_{|G/H|} \equiv \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\right) \pmod{p, q}.$$

Proof. Explicitly, $y_1 \star \cdots \star y_{|G/H|} = (\Pi, \Pi)$, where

$$\Pi = \prod_{\substack{1 \le n \le (pq-1)/2 \\ \gcd(n, pq) = 1}} n.$$

So we must show that

$$\Pi \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}, \quad \Pi \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

By symmetry, it suffices to show the first equality.

As we run over integers n such that $1 \le n \le (pq-1)/2$, and reduce them modulo p, we get $\frac{q-1}{2}$ copies of the sequence $1, 2, \dots, p-1$, along with one copy of the sequence $1, 2, \ldots, \frac{p-1}{2}$. Restricting to n such that $\gcd(n, pq) = 1$ means excluding the values $n = q, 2q, \ldots, (\frac{p-1}{2})q$. This argument shows

$$\Pi \equiv \frac{(p-1)!^{\frac{q-1}{2}}(\frac{p-1}{2})!}{q \cdot (2q) \cdots (\frac{p-1}{2})q} \equiv q^{-\frac{p-1}{2}}(p-1)!^{\frac{q-1}{2}} \pmod{p}.$$

By Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$, and by Euler's criterion, $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$. □

Example 25.6. If $p = 5$ and $q = 7$, then

$$\{1 \le n \le \tfrac{pq-1}{2}\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \quad 16, 17\}.$$

Reducing modulo 5, this becomes

$$\{1 \le n \le \tfrac{pq-1}{2}\} = \{1, 2, 3, 4, 0, 1, 7, 3, 4, 0, 1, 2, 3, 14, 0, 1, 2\}.$$

Therefore, $\Pi \equiv \frac{4!^3 \cdot 2!}{7 \cdot 14} \pmod{5}$.

25.4. Since $H = \{(1, 1), (-1, -1) \pmod{p, q}\}$, the claim that

$$x_1 \star \cdots \star x_{|G/H|} \star H = y_1 \star \cdots \star y_{|G/H|} \star H$$

amounts to saying that either $x_1 \star \cdots \star x_{|G/H|}$ and $y_1 \star \cdots \star y_{|G/H|}$ are the same, or that they differ in both entries by a minus sign. So we have

$$(-1)^{q-1} \equiv \epsilon \cdot (-1)^{q-1} \left(\frac{q}{p}\right) \pmod{p},$$
$$(-1)^{p-1}(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \equiv \epsilon \cdot (-1)^{p-1} \left(\frac{p}{q}\right) \pmod{q}$$

for some sign $\epsilon \in \{\pm 1\}$.

Since $p, q > 2$, and each sides of each congruence is either 1 or -1, we can promote the congruences to equalities:

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

Multiplying these equalities together,

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