MATH 361: NUMBER THEORY — EIGHTH LECTURE: QUADRATIC RECIPROCITY

Quadratic reciprocity is the first result of *modern* number theory. Motivated by specific problems, Euler and others worked on the quadratic reciprocity law in the 1700's, as described in texts such as David Cox's **Primes of the form** $x^2 + ny^2$ and Franz Lemmermeyer's **Reciprocity Laws**, but it was first proven by Gauss in 1796. From a naive viewpoint, there is no apparent reason for it to be true, but now we recognize it as the first of a family of reciprocity laws, themselves part of class field theory, itself part of the famous Langlands program.

Results up to now in the course, such as the Sun Ze Theorem, the cyclic structure of $(\mathbb{Z}/p\mathbb{Z})^\times$, or Hensel's Lemma may have been pleasing, but they have been essentially *unsurprising*. By contrast, the quadratic reciprocity *is* surprising.

Thanks to the results mentioned in the previous paragraph, we have essentially reduced the general congruence in one variable to the case of prime modulus

$$f(X) \equiv 0 \bmod p, \quad p \text{ prime}.$$

Here f is understood to be a polynomial with integer coefficients. If f has degree 1 then we have a fairly complete theory.

The next case is that f has degree 2, i.e., f is quadratic. Assuming that p is odd (i.e., excluding $p = 2$), the general quadratic congruence modulo p reduces as in high school algebra to

$$X^2 \equiv a \bmod p.$$

So the question is, for a fixed odd prime p, whether for a given value of a, the congruence has a solution. Clearly this depends only on a mod p, and so we may treat a as an equivalence class modulo p. But a related question is, for a fixed integer a, whether for a given odd prime $p \nmid a$, the congruence has a solution. It is not at all clear that this should be determined by a congruence condition on p, but we will see that in fact it depends only on p mod $4a$. This is one statement of quadratic reciprocity.

Contents

1. Initial definitions and results

Definition 1.1. *A nonzero square in $\mathbb{Z}/p\mathbb{Z}$ (i.e., a square in $(\mathbb{Z}/p\mathbb{Z})^\times$) is called a* **quadratic residue modulo** *p, or just a* **quadratic residue** *when p is clearly understood.*

Proposition 1.2. *Half of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are quadratic residues.*

Proof. One proof is to observe that there are at most $(p-1)/2$ squares because

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

Furthermore, these squares are all distinct because for any $a, b \in \mathbb{Z}/p\mathbb{Z}$,

$$a^2 = b^2 \implies (a-b)(a+b) = 0 \implies b = \pm a.$$

This completes the argument.

For a second proof, the map $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ given by $x \mapsto x^2$ is an abelian group homomorphism, and its kernel is $\{1, p-1\}$ because the polynomial equation $X^2 = 1$ can't have more than two roots over the field $\mathbb{Z}/p\mathbb{Z}$. The subgroup S of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ is the image of the map, isomorphic to the domain modulo the kernel, and therefore it comprises half of $(\mathbb{Z}/p\mathbb{Z})^\times$ as claimed. Further, let T denote the other coset of S in $(\mathbb{Z}/p\mathbb{Z})^\times$. Because $\{S, T\}$ is the quotient group $(\mathbb{Z}/p\mathbb{Z})^\times/S$, we see that

- the product of two quadratic residues is again a quadratic residue,
- the product of two quadratic nonresidues is a quadratic residue,
- and the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.

A third proof is to recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic,

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{g^0,\ g^1,\ g^2,\ \ldots,\ g^{p-2}\},$$

so that (omitting some details) the squares are precisely the even powers of the generator g. This third argument again gives the three bullets in the previous paragraph. □

It perhaps deserves note that in the multiplicative groups

$$\mathbb{R}_+^\times = \{\text{positive real numbers}\}$$

and

$$\mathbb{C}^\times = \{\text{nonzero complex numbers}\}$$

all elements are squares, while in the multiplicative group

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$$

only 1 is a square. The circumstance of half the elements being squares is not general. In any case, the obvious question now is

Which values $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ are the quadratic residues?

2. Some results proved by multiplying things together

From now on, p always denotes an odd prime.

The proof of Fermat's Little Theorem proceeds as follows. For any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, observe the equality of sets (with no reference to the order in which the elements appear)

$$\{1,\ 2,\ 3,\ \dots,\ p-1\} = \{a,\ 2a,\ 3a,\ \dots,\ (p-1)a\}.$$

This is because of the cancellation law in $(\mathbb{Z}/p\mathbb{Z})^\times$ (if $xa = ya$ then $x = y$) and the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is finite. From the set equality it follows that

$$1 \cdot 2 \cdot 3 \cdots (p-1) = a \cdot 2a \cdot 3a \cdots (p-1)a,$$

which is to say,

$$1 \cdot 2 \cdot 3 \cdots (p-1) = a^{p-1} 1 \cdot 2 \cdot 3 \cdots (p-1).$$

Cancel the nonzero element $1 \cdot 2 \cdot 3 \cdots (p-1)$ to get the desired result,

$$a^{p-1} = 1.$$

The proof of Wilson's Theorem is very similar. Again working in $(\mathbb{Z}/p\mathbb{Z})^\times$, the product

$$1 \cdot 2 \cdot 3 \cdots (p-1)$$

consists of pairwise products of elements and their (multiplicative) inverses except that each of 1 and $p-1$ is its own inverse. Thus the product is $p-1$, i.e., it is -1 because we are working modulo p.

The proof of Euler's Theorem is virtually identical to the proof of Fermat's Theorem. Let n be any positive integer, and let a be any element of $(\mathbb{Z}/n\mathbb{Z})^\times$. From the set-equality

$$\{b \in (\mathbb{Z}/n\mathbb{Z})^\times\} = \{ab : b \in (\mathbb{Z}/n\mathbb{Z})^\times\}$$

we have the equality of products (recalling that $\varphi(n)$ is by definition the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$)

$$\prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} b = \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} ab = a^{\varphi(n)} \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} b,$$

and we may cancel the product $\prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} b$ to get

$$a^{\varphi(n)} = 1.$$

In the next section we will continue to use the idea of the three proofs reviewed here.

3. The Legendre symbol, Euler's lemma, and Gauss's lemma

Let a be any integer, and let p be an odd prime. Define the *Legendre symbol* (a/p) as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a square modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a square modulo } p. \end{cases}$$

That is,

$$\left(\frac{a}{p}\right) = (\text{the number of solutions of } X^2 \equiv a \bmod p) \text{ minus one.}$$

Determining the number of solutions of the congruence $X^2 \equiv a \bmod p$ is equivalent to evaluating the Legendre symbol (a/p).

The definition of (a/p) instantly connotes that

$$\boxed{\textit{As a function of its numerator, } (a/p) \textit{ depends only on } a \textit{ mod } p.}$$

Also (see the end of the proof of Proposition 1.2), the cyclic structure of $(\mathbb{Z}/p\mathbb{Z})^\times$ does most of the work of showing that

$$\boxed{\textit{As a function of its numerator, } (a/p) \textit{ is multiplicative.}}$$

That is,

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

What is not at all obvious is that also, for *positive* a,

$$\boxed{\textit{As a function of its } \textbf{denominator}\textit{, } (a/p) \textit{ depends only on } p \textit{ mod } 4a.}$$

Later we will see that this is one statement of (most of) quadratic reciprocity.

Euler's Lemma provides a formula for the Legendre symbol.

Lemma 3.1 (Euler's Lemma)**.** *Let p be an odd prime, and let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then,*

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

Here we are working modulo p, i.e., we blur the distinction between the true integer $(a/p) = \pm 1$ and the element $a^{(p-1)/2} = \pm 1 + p\mathbb{Z}$ of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Proof. Consider the polynomial factorization (in $(\mathbb{Z}/p\mathbb{Z})[X]$)

$$X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1).$$

Because the left side has $p-1$ roots in $\mathbb{Z}/p\mathbb{Z}$, so does the right side, and because $\mathbb{Z}/p\mathbb{Z}$ is a field, each factor of the right side has at most $(p-1)/2$ roots, so each factor on the right side has exactly $(p-1)/2$ roots. The $(p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ satisfy the first factor in the right side because for any square $a = b^2$, by Fermat's Little Theorem,

$$a^{(p-1)/2} = (b^2)^{(p-1)/2} = b^{p-1} = 1.$$

Therefore the $(p-1)/2$ nonsquares satisfy the second factor in the right side. In sum, for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$,

$$\begin{aligned} a^{(p-1)/2} &= \begin{cases} 1 & \text{if } a \text{ is a residue,} \\ -1 & \text{if } a \text{ is a nonresidue} \end{cases} \\ &= \left(\frac{a}{p}\right). \end{aligned}$$

□

Euler's Lemma already suffices to compute the Legendre Symbol (a/p) in any specific case, especially because we have a fast raise-to-power algorithm. For example, for any odd prime p,

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

But Euler's Lemma doesn't provide *structural* insight to the behavior of the Legendre symbol. A first step in that direction is provided by Gauss's Lemma.

Lemma 3.2 (Gauss's Lemma)**.** *Let p be an odd prime, and let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Identify $(\mathbb{Z}/p\mathbb{Z})^\times$ with its set of representatives $\{1, 2, \ldots, p-1\}$. Consider the set*

$$T = \{a,\ 2a,\ \ldots,\ (\tfrac{p-1}{2})a\}.$$

Let ν be the number of elements of T that lie in $\{(p+1)/2,\ \ldots,\ p-1\}$. Then

$$\left(\frac{a}{p}\right) = (-1)^\nu.$$

Proof. No two elements of the set $\{1,\ \ldots,\ (p-1)/2\}$ are equal or additively opposite in $\mathbb{Z}/p\mathbb{Z}$. Consequently, the observation that for any $b, c \in \mathbb{Z}/p\mathbb{Z}$,

$$ba = \pm ca \implies b = \pm c,$$

shows that also no two elements of T are equal or additively opposite in $\mathbb{Z}/p\mathbb{Z}$. Let

$$x_1,\ \ldots,\ x_\mu$$

be the elements of T that lie in $\{1,\ \ldots,\ (p-1)/2\}$, and let

$$x'_1,\ \ldots,\ x'_\nu$$

be the elements of T that lie in $\{(p+1)/2,\ \ldots,\ p-1\}$. Then because no two elements of T are equal or additively opposite in $\mathbb{Z}/p\mathbb{Z}$, we have the set equality

$$\{x_1,\ \ldots,\ x_\mu,\ p-x'_1,\ \ldots, p-x'_\nu\} = \{1,\ 2,\ 3,\ \ldots,\ (p-1)/2\}.$$

Now, in the spirit of the proofs of Fermat's Little Theorem, Wilson's Theorem, and Euler's Theorem, multiply all the elements of T to compute that

$$\begin{aligned} a \cdot 2a \cdot 3a \cdots \tfrac{p-1}{2}a &= x_1 \cdots x_\mu \cdot x'_1 \cdots x'_\nu \\ &= (-1)^\nu x_1 \cdots x_\mu \cdot (p-x'_1) \cdots (p-x'_\nu) \\ &= (-1)^\nu 1 \cdot 2 \cdot 3 \cdots \tfrac{p-1}{2}. \end{aligned}$$

That is,

$$a^{(p-1)/2} \left(\tfrac{p-1}{2}\right)! = (-1)^\nu \left(\tfrac{p-1}{2}\right)!.$$

Because the factorial is invertible, it cancels,

$$a^{(p-1)/2} = (-1)^\nu,$$

and we are done by Euler's Lemma. □

As an example of using Gauss's Lemma, we compute the Legendre symbol

$$\left(\frac{-5}{p}\right), \quad p \text{ an odd prime.}$$

That is, the a in Gauss's Lemma is now -5, and we need to study the set

$$T = \{-5,\ 2 \cdot (-5),\ 3 \cdot (-5), \ldots,\ \tfrac{p-1}{2} \cdot (-5)\}.$$

The most negative of these is less negative than $-5p/2$, and so to count the relevant elements we need to intersect T with the first three "right halves" as $\mathbb{Z}/p\mathbb{Z}$ repeats ever leftward in $\mathbb{Z}$. That is, we need to count the number of T-elements that fall into the union of intervals

$$(-5p/2, -2p) \cup (-3p/2, -p) \cup (-p/2, 0).$$

Using the Division Theorem, write the arbitrary prime p as

$$p = 20q + r, \quad r \in \{1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19\}.$$

(*Wait, what th-?!... Why twenty?*) The T-elements that fall into $(-p/2, 0)$, into $(-3p/2, -p)$, or into $(-5p/2, -2p)$ take the form $-5k$ where

$$0 < 5k < p/2,$$
$$p < 5k < 3p/2,$$
$$2p < 5k < 5p/2.$$

Multiply through by 2 to clear the denominators, and these conditions are

$$0 < 10k < 20q + r,$$
$$40q + 2r < 10k < 60q + 3r,$$
$$80q + 4r < 10k < 100q + 5r.$$

In counting the number of multiples of 10 in an interval, we may freely shift the interval by any multiple of 10, and so the conditions simplify to

$$0 < 10k < 20q + r,$$
$$2r < 10k < 20q + 3r,$$
$$4r < 10k < 20q + 5r.$$

These conditions are

$$0 < 10k < r \quad \text{or} \quad r \leq 10k < 20q + r,$$
$$2r < 10k < 3r \quad \text{or} \quad 3r \leq 10k < 20q + 3r,$$
$$4r < 10k < 5r \quad \text{or} \quad 5r \leq 10k < 20q + 5r.$$

We need only to count the total number ν of appropriate k-values modulo 2. And each of the intervals $[r, 20q+r)$, $[3r, 20q+3r)$, $[5r, 20q+5r)$ contains two values $10k$. And so altogether it suffices to count the k-values such that

$$10k \in (0, r) \cup (2r, 3r) \cup (4r, 5r).$$

(*This* is why we took $p = 20q + r$: in the previous display q is gone and only r remains, so taking $p = 20q + r$ lets us simultaneously calculate $(-5/p)$ for all p rather than for one p at a time. For general (a/p) we take $p = 4|a|q + r$, as will be explained just below.) Now we can make a table of the possibilities as p mod 20 varies through all possibilities:

r	Conditions	ν	$(-5/p)$
1	$10k \in (0,1) \cup (2,3) \cup (4,5)$	0	1
3	$10k \in (0,3) \cup (6,9) \cup (12,15)$	0	1
7	$10k \in (0,7) \cup (14,21) \cup (28,35)$	2	1
9	$10k \in (0,9) \cup (18,27) \cup (36,45)$	2	1
11	$10k \in (0,11) \cup (22,33) \cup (44,55)$	3	-1
13	$10k \in (0,13) \cup (26,39) \cup (52,65)$	3	-1
17	$10k \in (0,17) \cup (34,51) \cup (68,85)$	5	-1
19	$10k \in (0,19) \cup (38,57) \cup (76,95)$	5	-1

That is, for any odd prime p,

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3, 7, 9 \bmod 20, \\ -1 & \text{if } p \equiv 11, 13, 17, 19 \bmod 20. \end{cases}$$

As an exercise, you should show using Gauss's Lemma that for any odd prime p,

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

and then show by an elementary argument that a convenient formula encapsulating this result is

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

As the examples $(-5/p)$ and $(2/p)$ illustrate, Gauss's Lemma is a *reduce to finite* result, showing in general that the Legendre symbol (a/p) for fixed a, as p varies through all the primes, depends only on the congruence class $p + 4a\mathbb{Z}$. We prove this next.

4. Proof that (a/p) depends only on p mod $4a$

Let p be an odd prime, and let $a \in \mathbb{Z}$ be coprime to p. Consider the integer multiples $ka \in \{a, 2a, \ldots, \frac{p-1}{2}a\}$ of a that lie in a right half modulo p, meaning that for some integer m,

$$(m - \tfrac{1}{2})p < ka < mp.$$

Because $1 \leq k \leq \frac{p-1}{2}$, the previous display is possible only for finitely many values of m. Because $\frac{p\pm1}{2}a = a\frac{p}{2} \pm \frac{a}{2}$, our last multiple of a and the next multiple of a straddle an integer multiple of $p/2$, and so the multiples $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ of a can't stop in the middle of a right half. Thus it suffices to show that for any fixed m out of finitely many possibilities, the parity of the number of *all* positive integers k such that ka lies in the mth right half modulo p depends only on $p + 4a\mathbb{Z}$; we don't need to worry about the condition $k \leq \frac{p-1}{2}$. Write $p = q4|a| + r$ with $0 \leq r < 4|a|$. The previous display, but now for one particular m, becomes

$$(m - \tfrac{1}{2})q4|a| + (m - \tfrac{1}{2})r < ka < mq4|a| + mr,$$

or, letting $k' = k - (m - \frac{1}{2})q4\,\mathrm{sgn}(a)$,

$$(m - \tfrac{1}{2})r < k'a < q2|a| + mr.$$

Because either $k'a < mr$ or $mr \leq k'a$, this is

$$(m - \tfrac{1}{2})r < k'a < mr \quad \text{or} \quad mr \leq k'a < q2|a| + mr.$$

But the interval $\big[mr, q2|a| + mr\big)$ contains $2q$ multiples of a, an even number of them, and so we need only to count the parity of the number of integers k' such that $(m - \frac{1}{2})r < k'a < mr$. This depends on r but is independent of q, as desired.

5. Two motivating examples

For our first example, consider the ring $R = \mathbb{Z}[i]$ of Gaussian integers. Which primes p in the ring $\mathbb{Z}$ of *rational* integers factor further in the larger ring R? One can verify that

$$\begin{aligned} 2 &= -i(1+i)^2, \\ 3 &\quad \text{doesn't factor}, \\ 5 &= (2+i)(2-i), \\ 7 &\quad \text{doesn't factor}, \\ 11 &\quad \text{doesn't factor}, \end{aligned}$$

$$\begin{aligned}
13 &= (3+2i)(3-2i),\\
17 &= (4+i)(4-i),\\
19 &\quad \text{doesn't factor},\\
23 &\quad \text{doesn't factor},\\
29 &= (5+2i)(5-2i),\\
31 &\quad \text{doesn't factor},\\
37 &= (6+i)(6-i).
\end{aligned}$$

Ignoring the prime 2, which is somehow behaving differently from the others, the pattern is:

The $1 \pmod 4$ *primes factor and the* $3 \pmod 4$ *primes do not.*

That is, by our calculation immediately after Euler's Lemma:

$$\boxed{\textit{The Legendre symbol } \left(\frac{-1}{p}\right) \textit{ indicates how } p \textit{ behaves in } \mathbb{Z}[\sqrt{-1}].}$$

For our second example, consider the ring $R = \mathbb{Z}[\sqrt{-5}]$, a nonunique factorization domain. In this ring it is the *ideals* that factor uniquely. In particular, each rational prime p determines an ideal pR in the ring. One can verify the factorizations, and later we will show the non-factorizations, in the assertions that

$$\begin{aligned}
2R &= (2, (1+\sqrt{-5}))^2,\\
3R &= (3, (1+\sqrt{-5})) \cdot (3, (1-\sqrt{-5})),\\
5R &= (\sqrt{-5})^2,\\
7R &= (7, (3+\sqrt{-5})) \cdot (7, (3-\sqrt{-5})),\\
11R &\quad \text{doesn't factor},\\
13R &\quad \text{doesn't factor},\\
17R &\quad \text{doesn't factor},\\
19R &\quad \text{doesn't factor},\\
23R &= (23, (15+\sqrt{-5})) \cdot (23, (15-\sqrt{-5})),\\
29R &= (29, (13+\sqrt{-5})) \cdot (29, (13-\sqrt{-5})),\\
31R &\quad \text{doesn't factor},\\
37R &\quad \text{doesn't factor}.
\end{aligned}$$

This time the primes 2 and 5 are different from the others, but otherwise, it turns out that the pattern is:

The $1, 3, 7, 9 \pmod{20}$ *primes factor, the* $11, 13, 17, 19 \pmod{20}$ *primes do not.*

That is, by our calculation immediately after Gauss's Lemma:

$$\boxed{\textit{The Legendre symbol } \left(\frac{-5}{p}\right) \textit{ indicates how } p \textit{ behaves in } \mathbb{Z}[\sqrt{-5}].}$$

Recall that the definition of (a/p) instantly connotes that for a fixed odd prime p,

$$\boxed{\textit{As a function of its numerator, } (a/p) \textit{ depends only on } a \bmod p.}$$

Also, the cyclic structure of $(\mathbb{Z}/p\mathbb{Z})^\times$ does most of the work of showing that

$$\boxed{\textit{As a function of its numerator, } (a/p) \textit{ is multiplicative.}}$$

That is, $(ab/p) = (a/p)(b/p)$. But what the previous two examples have shown is that for a fixed a,

$$\boxed{\textit{We are interested in } (a/p) \textit{ as a function of its } \textbf{denominator.}}$$

Thus:

> *We want a relation between the Legendre symbol as a function of its numerator (a function that we understand), and the Legendre symbol as a function of its denominator (a function that we care about).*

6. Statements of quadratic reciprocity

From now on, p and q denote distinct odd primes.

Euler conjectured the already-mentioned condition that for positive a,

$$\boxed{\textit{As a function of its } \textbf{denominator}\textit{, } (a/p) \textit{ depends only on } p \textit{ mod } 4a.}$$

More specifically, Euler conjectured that

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff p = \pm x^2 \bmod 4q \text{ for some } x.}$$

Here the right side gives $p = \pm x^2 \bmod 4$, showing that x must be odd and that the "$\pm$" must be "$+$" when $p = 1 \bmod 4$ and "$-$" when $p = 3 \bmod 4$. So Euler's conjecture is

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff \begin{cases} p = x^2 \bmod 4q \text{ for some } x \text{ if } p = 1 \bmod 4, \\ p = -x^2 \bmod 4q \text{ for some } x \text{ if } p = 3 \bmod 4. \end{cases}} \tag{1}$$

This is one statement of (most of) quadratic reciprocity. Another statement, due to Legendre, is that for all distinct odd primes p and q,

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

or, equivalently,

$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if at least one of } p \text{ and } q \text{ is 1 modulo 4,} \\ -1 & \text{if both } p \text{ and } q \text{ are 3 modulo 4.} \end{cases}}$$

This form of quadratic reciprocity is pleasingly symmetric in p and q.

Proposition 6.1. *Euler's conjecture* (1) *and Legendre's formulation* (2) *are equivalent.*

(Note: The proposition doesn't assert that either formulation of quadratic reciprocity is *true*, only that the truth of either implies the truth of the other.)

Proof. Introduce the quantity

$$p^* = (-1)^{(p-1)/2}p = \begin{cases} p & \text{if } p \equiv 1 \bmod 4, \\ -p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

That is,

$$p^* = \text{whichever of } \pm p \text{ equals 1 mod 4.}$$

With p^* introduced, Euler's conjecture (1) of quadratic reciprocity is

$$\left(\frac{q}{p}\right) = 1 \iff p^* \equiv x^2 \bmod 4q \text{ for some } x.$$

This equivalence is

$$\left(\frac{q}{p}\right) = 1 \iff \left\{ \begin{array}{l} p^* \equiv x^2 \bmod q \\ p^* \equiv x^2 \bmod 4 \end{array} \right\} \text{ for some } x.$$

The congruence modulo 4 requires x to be odd, and then both p^* and x^2 equal 1 mod 4, so the equivalence simplifies to

$$\left(\frac{q}{p}\right) = 1 \iff p^* \equiv x^2 \bmod q \text{ for some odd } x.$$

But if $p^* \equiv x^2 \bmod q$ some for some even x then also $p^* \equiv (x+q)^2 \bmod q$ and $x+q$ is odd, so in fact the equivalence is

$$\left(\frac{q}{p}\right) = 1 \iff p^* \equiv x^2 \bmod q \text{ for some } x.$$

Thus Euler's formulation of quadratic reciprocity rephrases as

$$\left(\frac{q}{p}\right) = 1 \iff \left(\frac{p^*}{q}\right) = 1.$$

This equivalence is an equality condition,

$$\left(\frac{p^*}{q}\right)\left(\frac{q}{p}\right) = 1,$$

which, recalling that $p^* = (-1)^{(p-1)/2}p$, is

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

or, by the established formula $(-1/q) = (-1)^{(q-1)/2}$, so that $(-1/q)^{(p-1)/2} = (-1)^{(p-1)/2\cdot(q-1)/2}$,

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

This is Legendre's formulation (2) of quadratic reciprocity. □

7. Lattice point counting proof of quadratic reciprocity

Proposition 7.1. *Gauss's Lemma implies Legendre's formulation* (2) *of quadratic reciprocity.*

Proof. Recall the set

$$T = \{q,\ 2q,\ \ldots,\ \left(\tfrac{p-1}{2}\right) q\} = \{qi : 1 \le i \le \tfrac{p-1}{2}\}.$$

Recall that the elements of $T \cap \{0,\ \ldots,\ (p-1)/2\}$ are denoted x_1 through x_μ, while the elements of $T \cap \{(p+1)/2,\ \ldots,\ p-1\}$ are denoted x'_1 through x'_ν, and that Gauss's Lemma asserts that

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

Write each element of T as

$$qi = \left\lfloor \frac{qi}{p} \right\rfloor p + r_i, \quad 0 < r_i < p.$$

If $1 \le r_i \le (p-1)/2$ then $r_i = x_j$ for some j, but if $(p+1)/2 \le r_i \le p-1$ then $r_i = x'_j$ for some j. To prove the proposition, we compute the parity of the sum

$$\sum_{i=1}^{(p-1)/2} qi$$

in two different ways. First,

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} qi = q \sum_{i=1}^{(p-1)/2} i &= q\left(\sum_{j=1}^{\mu} x_j + \sum_{j=1}^{\nu} (p - x'_j)\right) \\ &\equiv \left(\sum_{j=1}^{\mu} x_j + \nu + \sum_{j=1}^{\nu} x'_j\right) \mod 2.\end{aligned}$$

Second, the sum is also

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} qi &= \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor p + r_i \\ &= p \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{j=1}^{\mu} x_j + \sum_{j=1}^{\nu} x'_j \\ &\equiv \left(\sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{j=1}^{\mu} x_j + \sum_{j=1}^{\nu} x'_j\right) \mod 2.\end{aligned}$$

The previous two displays combine to give

$$\nu \equiv S(q,p) \bmod 2 \quad \text{where} \quad S(q,p) = \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qi}{p} \right\rfloor,$$

and thus

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

Exchanging the roles of p and q in the argument now gives

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

But $S(p,q) + S(q,p)$ is the number of lattice points in the box with lower left corner $(1,1)$ and upper right corner $(\frac{p-1}{2}, \frac{q-1}{2})$ (see figure 1). That is,

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

This is Legendre's formulation (2) of quadratic reciprocity. □

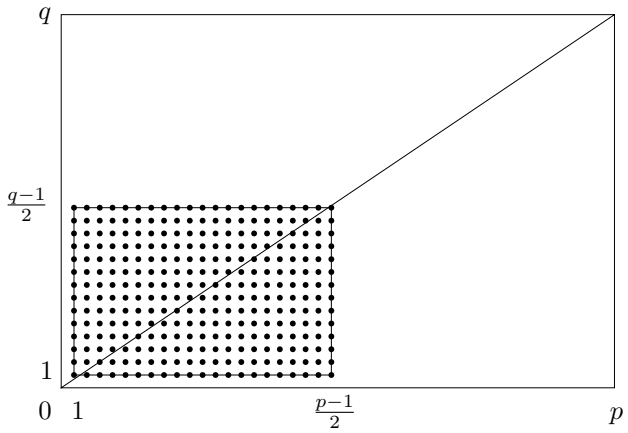

FIGURE 1. Lattice points

8. First version of the algorithm

Algorithmically, the useful form of the quadratic reciprocity law is that for all distinct odd primes p and q,

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

In practice we do not compute the power of -1 each time we use the formula but rather,

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

The utility of this is that for the left side we may assume that $p < q$, but then on the right side we may replace q by q mod p. And so evaluating the right side is a strictly smaller problem, and this process can be iterated until p and q get small quickly. There are also two auxiliary quadratic reciprocity results, which we have already proved: For all odd prime p,

$$\boxed{\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \quad \text{and} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}}$$

Again, we do not repeatedly work out the powers of -1, but rather

$$\boxed{\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \bmod 4 \\ -1 & \text{if } p = 3 \bmod 4 \end{cases}}$$

and

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

For an example,

$$\begin{aligned} \left(\frac{2017}{5003}\right) &= \left(\frac{5003}{2017}\right) = \left(\frac{969}{2017}\right) = \left(\frac{3 \cdot 17 \cdot 19}{2017}\right) \\ &= \left(\frac{3}{2017}\right)\left(\frac{17}{2017}\right)\left(\frac{19}{2017}\right) = \left(\frac{2017}{3}\right)\left(\frac{2017}{17}\right)\left(\frac{2017}{19}\right) \\ &= \left(\frac{1}{3}\right)\left(\frac{11}{17}\right)\left(\frac{3}{19}\right) = -\left(\frac{17}{11}\right)\left(\frac{19}{3}\right) = -\left(\frac{6}{11}\right)\left(\frac{1}{3}\right) \\ &= -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{11}{3}\right) = \left(\frac{2}{11}\right)\left(\frac{2}{3}\right) \\ &= (-1) \cdot (-1) = \boxed{1}. \end{aligned}$$

This calculation tells us that 2017 is a square modulo 5003 without finding the square roots. (In fact they are 606 and 4397.)

9. Speeding up the algorithm: the Jacobi symbol

For any integer a and any positive odd integer P the *Jacobi symbol* (a/P) is defined as follows:

$$\left(\frac{a}{P}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i} \quad \text{where } P = \prod_i p_i^{e_i}.$$

When P is an odd prime (understood to be positive), the Jacobi symbol is the Legendre symbol. However, for nonprime P, the condition $(a/P) = 1$ doesn't necessarily imply that a is a square modulo P, even though the condition $(a/P) = -1$ does imply that a is not a square modulo P.

The empty product case of the previous display says that $(a/1) = 1$ for all a.

In a moment we will prove that the quadratic reciprocity rules extend to the Jacobi symbol. That is, for all odd positive coprime P and Q,

$$\boxed{\left(\frac{P}{Q}\right) = (-1)^{(P-1)/2 \cdot (Q-1)/2} \left(\frac{Q}{P}\right)}$$

and for all odd positive P,

$$\boxed{\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2} \qquad \text{and} \qquad \left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}}$$

As above, we don't actually compute the powers of -1 but remember what they are in terms of P, Q mod 4 or P mod 4 or P mod 8. The Jacobi symbol rules further

speed Legendre symbol calculations because now we can use Jacobi symbols en route. For example,

$$\left(\frac{2017}{5003}\right) = \left(\frac{5003}{2017}\right) = \left(\frac{969}{2017}\right) = \left(\frac{2017}{969}\right) = \left(\frac{79}{969}\right)$$
$$= \left(\frac{969}{79}\right) = \left(\frac{21}{79}\right) = \left(\frac{79}{21}\right) = \left(\frac{16}{21}\right) = \boxed{1}.$$

This example demonstrates that Jacobi symbol calculations proceed as quickly as the Euclidean algorithm. Determining whether a quadratic congruence has solutions is as fast as solving a linear congruence.

The following result helps to prove that the quadratic reciprocity rules extend to the Jacobi symbol.

Lemma 9.1. *Let $p_1, \ldots, p_k$ be odd primes, not necessarily distinct, and consider their product $P = \prod_i p_i$. Then*

$$\frac{P-1}{2} \equiv \sum_i \frac{p_i - 1}{2} \bmod 2 \qquad \textit{and} \qquad \frac{P^2-1}{8} = \sum_i \frac{p_i^2 - 1}{8} \bmod 2.$$

Proof. For the first congruence, compute that

$$P = \prod_i (1 + (p_i - 1)) = 1 + \sum_i (p_i - 1) + \sum_{i<j} (p_i - 1)(p_j - 1) + \cdots$$
$$\equiv 1 + \sum_i (p_i - 1) \bmod 4,$$

and so

$$\frac{P-1}{2} \equiv \sum_i \frac{p_i - 1}{2} \bmod 2.$$

Similarly for the second congruence,

$$P^2 = \prod_i (1 + (p_i^2 - 1)) = 1 + \sum_i (p_i^2 - 1) + \sum_{i<j} (p_i^2 - 1)(p_j^2 - 1) + \cdots$$
$$\equiv 1 + \sum_i (p_i^2 - 1) \bmod 16,$$

and so

$$\frac{P^2-1}{8} \equiv \sum_i \frac{p_i^2 - 1}{8} \bmod 2.$$

In fact the last two congruences hold modulo 64 and 8 respectively, but that is more than we need. □

It follows from the lemma that for any positive odd $P = \prod_i p_i$ and any positive odd $Q = \prod_j q_j$ coprime to P,

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right) \cdot \prod_{i,j} \left(\frac{q_j}{p_i}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$$
$$= \prod_{i,j} (-1)^{(p_i-1)/2 \cdot (q_j-1)/2} = (-1)^{\sum_{i,j} (p_i-1)/2 \cdot (q_j-1)/2}$$
$$= (-1)^{\sum_i (p_i-1)/2 \cdot \sum_j (q_j-1)/2}$$
$$= (-1)^{(P-1)/2 \cdot (Q-1)/2},$$

and

$$\left(\frac{-1}{P}\right) = \prod_i \left(\frac{-1}{p_i}\right) = \prod_i (-1)^{(p_i-1)/2} = (-1)^{\sum_i (p_i-1)/2} = (-1)^{(P-1)/2},$$

and

$$\left(\frac{2}{P}\right) = \prod_i \left(\frac{2}{p_i}\right) = \prod_i (-1)^{(p_i^2-1)/8} = (-1)^{\sum_i (p_i^2-1)/8} = (-1)^{(P^2-1)/8}.$$

10. The Kronecker symbol

The Kronecker symbol further generalizes of the Legendre–Jacobi symbol. For denominator 2,

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a = 1, 7 \bmod 8, \\ -1 & \text{if } a = 3, 5 \bmod 8, \\ 0 & \text{if } a = 0 \bmod 2. \end{cases}$$

Thus $(a/2)$ depends on a mod 8, so that the property that (a/p) depends only on a mod p is lost for $p = 2$. Also, $(p/2) = (2/p)$ for odd primes p. For denominator -1,

$$\left(\frac{a}{-1}\right) = \operatorname{sgn}(a) = \begin{cases} 1 & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -1 & \text{if } a < 0. \end{cases}$$

The general Legendre–Jacobi–Kronecker symbol incorporates these two new conventions multiplicatively,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{\operatorname{sgn}(P)}\right) \prod_i \left(\frac{a}{p_i}\right) \quad \text{where } P = \operatorname{sgn}(P) \prod_i p_i.$$

Here the primes p_i can repeat. If P is negative, then (a/P) is not periodic in a, and if P is positive but even, then (a/P) need not be a function of a mod P. The Kronecker symbol quadratic reciprocity law is as follows.

Theorem 10.1. *Let P and Q be nonzero coprime integers,*

$$P = 2^{e_2} P' \quad \textit{where} \quad P' = \operatorname{sgn}(P) \prod_{p \text{ odd}} p^{e_p}$$

and

$$Q = 2^{f_2} Q' \quad \textit{where} \quad Q' = \operatorname{sgn}(Q) \prod_{p \text{ odd}} p^{f_p},$$

where $\min\{e_p, f_p\} = 0$ *for all p. Then*

$$\boxed{\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(P'-1)/2 \cdot (Q'-1)/2} (-1)^{(\operatorname{sgn}(P)-1)/2 \cdot (\operatorname{sgn}(Q)-1)/2}.}$$

The theorem does *not* decompose P as $\operatorname{sgn}(P)2^eP_o$, but rather P' has the same sign as P (and similarly for Q, of course). The factor $(-1)^{(\operatorname{sgn}(P)-1)/2\cdot(\operatorname{sgn}(Q)-1)/2}$ in the reciprocity law is 1 if at least one of P and Q is positive, -1 if both P and Q are negative.

Proof. Abbreviate $\operatorname{sgn}(P)$ to $\mathrm{s}P$ and similarly for $\mathrm{s}Q$. With $P = \mathrm{s}P2^{e_2}P_o$ and $Q = \mathrm{s}QQ_o$ (noting that 2 can't divide both P and Q), compute, noting that $(2/sQ) = 1$ and $(P_o/sQ) = 1$,

$$\left(\frac{P}{Q}\right) = \left(\frac{sP}{sQ}\right)\left(\frac{sP}{Q_o}\right)\left(\frac{2}{Q_o}\right)^e\left(\frac{P_o}{Q_o}\right)$$

and similarly, noting that $(Q_o/sP) = 1$ and $(sQ/2) = 1$,

$$\left(\frac{Q}{P}\right) = \left(\frac{sQ}{sP}\right)\left(\frac{sQ}{P_o}\right)\left(\frac{Q_o}{2}\right)^e\left(\frac{Q_o}{P_o}\right).$$

So their product is

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \left(\frac{sP}{sQ}\right)\left(\frac{sQ}{sP}\right)\left(\frac{sP}{Q_o}\right)\left(\frac{sQ}{P_o}\right)\left(\frac{2}{Q_o}\right)^e\left(\frac{Q_o}{2}\right)^e\left(\frac{P_o}{Q_o}\right)\left(\frac{Q_o}{P_o}\right),$$

and because $(sP/sQ)(sQ/sP) = 1$ and $(2/Q_o)(Q_o/2) = 1$ this reduces to

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \left(\frac{sP}{Q_o}\right)\left(\frac{sQ}{P_o}\right)\left(\frac{P_o}{Q_o}\right)\left(\frac{Q_o}{P_o}\right),$$

in which the possible power of 2 in P plays no role. By the results stated as consequences of Lemma 9.1, this is

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (sP)^{(Q_o-1)/2}(sQ)^{(P_o-1)/2}(-1)^{(P_o-1)/2\cdot(Q_o-1)/2}.$$

If $sP = sQ = 1$ then $P_o = P'$ and $Q_o = Q'$, and so this is the desired result,

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(P'-1)/2\cdot(Q'-1)/2}.$$

If $sP = 1$ and $sQ = -1$ then $P_o = P'$ and $Q_o = -Q'$, and so it is again the desired result,

$$\begin{aligned}\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) &= (-1)^{(P'-1)/2}(-1)^{(P'-1)/2\cdot(-Q'-1)/2}\\ &= (-1)^{(P'-1)/2\cdot(-Q'+1)/2}\\ &= (-1)^{(P'-1)/2\cdot(Q'-1)/2},\end{aligned}$$

and similarly if $sP = -1$ and $sQ = 1$. Finally, if $sP = sQ = -1$ then $P_o = -P'$ and $Q_o = -Q'$, and so it is

$$\begin{aligned}\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) &= (-1)^{(-P'-1)/2}(-1)^{(-Q'-1)/2}(-1)^{(-P'-1)/2\cdot(-Q'-1)/2}\\ &= -(-1)^{(-P'+1)/2}(-1)^{(-P'+1)/2\cdot(-Q'-1)/2}\\ &= -(-1)^{(-P'+1)/2\cdot(-Q'+1)/2}\\ &= -(-1)^{(P'-1)/2\cdot(Q'-1)/2},\end{aligned}$$

as desired in the last case. □

We end with three comments.

First, a full set of primes for $\mathbb{Z}$ should be extended to include one so-called *Archimedean prime*, and some authors (such as Conway–Sloane in *Sphere Packings, Lattices and Groups*) identify this prime with -1. Under the convention that -1 is prime, P and Q are not coprime if both are negative, and so the factor $(-1)^{(\mathrm{sgn}(P)-1)/2\cdot(\mathrm{sgn}(Q)-1)/2}$ is unnecessary. That is, it is arguably natural to tidy the reciprocity law by excluding the case that P and Q are both negative.

Second, another convention is to define $(a/-1) = 1$ for all nonzero a, making the Jacobi symbol depend only on the absolute value of its denominator. Under this convention the boxed reciprocity law in the theorem is unchanged, because $(\mathrm{sgn}\, P/\mathrm{sgn}\, Q)(\mathrm{sgn}\, Q/\mathrm{sgn}\, P) = 1$ for all nonzero P and Q either way.

Third, an equivalent version of the reciprocity law, sometimes more convenient to use, is that for P and Q as in the theorem,

$$\boxed{\left(\frac{P}{Q}\right)\left(\frac{Q}{|P|}\right) = (-1)^{(P'-1)/2\cdot(Q'-1)/2}.}$$

Indeed, if either of P, Q is positive then $(Q/|P|) = (Q/P)$, while if both are negative then $(Q/|P|) = -(Q/P)$. However, this last equality does use the definition $(a/-1) = \mathrm{sgn}(a)$ for nonzero a rather than $(a/-1) = 1$.