

## MATH 361: NUMBER THEORY — EIGHTH LECTURE

### 1. QUADRATIC RECIPROCITY: INTRODUCTION

Quadratic reciprocity is the first result of *modern* number theory. Lagrange conjectured it in the late 1700's, 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  $(\mathbf{Z}/p\mathbf{Z})^\times$ , 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

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

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

$$X^2 \equiv a \pmod{p}.$$

So the question is whether for a given value of  $a$ , the congruence has a solution. Clearly this depends only on  $a \pmod{p}$ , and so we may treat  $a$  as an equivalence class modulo  $p$ .

**Definition 1.1.** *A nonzero square in  $\mathbf{Z}/p\mathbf{Z}$  (i.e., a square in  $(\mathbf{Z}/p\mathbf{Z})^\times$ ) 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  $(\mathbf{Z}/p\mathbf{Z})^\times$  are quadratic residues.*

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

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

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

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

This completes the argument.

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

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

so that (omitting some details) the squares are precisely the even powers of the generator  $g$ . This second argument shows incidentally 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.

□

The obvious question now is

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

(It perhaps deserves note that in the multiplicative groups

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

and

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

all elements are squares, while in the multiplicative group

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

only 1 is a square. The circumstance of half the elements being squares is not general.)

## 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  $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ , observe the equality of sets (with no reference to the sequence 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  $(\mathbf{Z}/p\mathbf{Z})^\times$  (if  $xa = ya$  then  $x = y$ ) and the fact that  $(\mathbf{Z}/p\mathbf{Z})^\times$  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  $(\mathbf{Z}/p\mathbf{Z})^\times$ , 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  $-1$  since 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  $(\mathbf{Z}/n\mathbf{Z})^\times$ . From the set-equality

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

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

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

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

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

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,

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

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

The definition of  $(a/p)$  instantly connotes that

*As a function of its numerator,  $(a/p)$  depends only on  $a \pmod{p}$ .*

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

*As a function of its numerator,  $(a/p)$  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*  $a$ ,

*As a function of its denominator,  $(a/p)$  depends only on  $\pm p \pmod{4a}$ .*

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  $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ . Then*

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

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

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

Since the left side has  $p - 1$  roots in  $\mathbf{Z}/p\mathbf{Z}$ , so does the right side, and so similarly to arguments that we have given in class, each factor of the right side has  $(p - 1)/2$

roots. The  $(p-1)/2$  squares in  $(\mathbf{Z}/p\mathbf{Z})^\times$  satisfy the first factor in the right side because for any square  $a^2$ , by Fermat's Little Theorem,

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

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

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

□

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

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

But Euler's Lemma does not 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  $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ . Consider the set*

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

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

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

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

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

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

$$x_1, \dots, x_\mu$$

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

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

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

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

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

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

That is,

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

Since the factorial is invertible, it cancels,

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

and we are done by Euler's Lemma.  $\square$

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

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

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 three "right halves" as  $\mathbf{Z}/p\mathbf{Z}$  repeats ever leftward in  $\mathbf{Z}$ . 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  $(-p/2, 0)$  take the form  $-5k$  where

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

or equivalently,  $0 < 5k < (20q + r)/2$ , or

$$0 < k < 2q + r/10.$$

Similarly, the  $T$ -elements that fall into  $(-3p/2, -p)$  take the form  $-5k$  where

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

or equivalently,  $20q + r < 5k < (60q + 3r)/2$ , or

$$4q + 2r/10 < k < 6q + 3r/10.$$

Finally, the  $T$ -elements that fall into  $(-5p/2, -2p)$  take the form  $-5k$  where

$$2p < 5k < 5p/2,$$

or equivalently,  $40q + 2r < 5k < (100q + 5r)/2$ , or

$$8q + 4r/10 < k < 10q + 5r/10.$$

We need only to count the total number  $\nu$  of appropriate  $k$ -values modulo 2, so we need to count the  $k$ -values such that

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

(*This is why we took  $p = 20q + r$ : only  $r$  affects the value of  $(-5/p)$ , so we are simultaneously calculating  $(-5/p)$  for all  $p$  rather than for one  $p$  at a time. For*

general  $(a/p)$  we take  $p = 4|a|q + r$ .) Now we can make a table of the possibilities as  $p \pmod{20}$  varies through all possibilities:

$r$	Conditions	$\nu$	$(-5/p)$
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  $p$ ,

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

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

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

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

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

#### 4. TWO MOTIVATING EXAMPLES

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

$$\begin{aligned} 2 &= -i(1+i)^2, \\ 3 &\text{ does not factor,} \\ 5 &= (2+i)(2-i), \\ 7 &\text{ does not factor,} \\ 11 &\text{ does not factor,} \\ 13 &= (3+2i)(3-2i), \\ 17 &= (4+i)(4-i), \\ 19 &\text{ does not factor,} \\ 23 &\text{ does not factor,} \\ 29 &= (5+2i)(5-2i), \\ 31 &\text{ does not factor,} \\ 37 &= (6+i)(6-i). \end{aligned}$$

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

*The 1 (mod 4) primes factor and the 3 (mod 4) primes do not.*

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

The Legendre symbol  $\left(\frac{-1}{p}\right)$  indicates how  $p$  behaves in  $\mathbf{Z}[i]$ .

For our second example, consider the ring  $R = \mathbf{Z}[\sqrt{-5}]$ , a nonunique factorization domain. We have heard that in this ring it is the *ideals* that factor uniquely. In particular, each rational prime  $p$  determines an ideal  $pR$  in the ring. Which such ideals factor in  $R$ ? One can verify that

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

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 (mod 20) primes factor, the 11, 13, 17, 19 (mod 20) primes do not.*

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

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

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

*As a function of its numerator,  $(a/p)$  depends only on  $a \pmod p$ .*

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

*As a function of its numerator,  $(a/p)$  is multiplicative.*

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

*We are interested in  $(a/p)$  as a function of its **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).*

## 5. STATEMENTS OF QUADRATIC RECIPROCITY

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

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

As a function of its **denominator**,  $(a/p)$  depends only on  $\pm p \pmod{4a}$ .

More specifically, Euler conjectured that

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

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

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

or, equivalently,

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

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

**Proposition 5.1.** *Euler's conjecture (1) and Legendre's formulation (2) are equivalent.*

(Note: The proposition does not 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

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

That is,

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

Then we have the following equivalences (using Euler's Criterion for the second one):

$$\begin{aligned} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) &= (-1)^{(p-1)/2 \cdot (q-1)/2} \\ &\iff \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p^*}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \\ &\iff (-1)^{(p-1)/2 \cdot (q-1)/2} \left(\frac{p^*}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \\ &\iff \left(\frac{p^*}{q}\right) \left(\frac{q}{p}\right) = 1 \\ &\iff \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right). \end{aligned}$$

So, Legendre's formulation (2) of quadratic reciprocity rephrases as an equivalence,

$$(3) \quad \left(\frac{q}{p}\right) = 1 \iff \left(\frac{p^*}{q}\right) = 1,$$

while Euler's formulation (1) of quadratic reciprocity is already an equivalence with the same condition on its left side,

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

To show the equivalence of (1) and (2), it suffices to show the equivalence of (3) and (4). And to show their equivalence it suffice to show the equivalence of the right side conditions,

$$(5) \quad \left(\frac{p^*}{q}\right) = 1 \iff p \equiv \pm x^2 \pmod{4q} \text{ for some } x.$$

But indeed,

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

and in fact, since  $x^2 \pmod{q} = (q - x)^2 \pmod{q}$ ,

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

Both  $p^*$  and  $x^2$  equal 1 mod 4 (because all odd squares equal 1 mod 4), so we have

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

And then, by the Sun-Ze Theorem,

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

Since  $p^*$  is one of  $\pm p$ , this establishes (5), completing the argument.  $\square$

## 6. PROOF OF QUADRATIC RECIPROCITY

**Proposition 6.1.** *Gauss's Lemma implies Legendre's formulation (2) of quadratic reciprocity.*

*Proof.* Recall the set

$$T = \{q, 2q, \dots, \left(\frac{p-1}{2}\right)q\} = \{qi : 1 \leq i \leq \frac{p-1}{2}\}.$$

Recall that the elements of  $T \cap \{0, \dots, (p-1)/2\}$  are denoted  $x_1$  through  $x_\mu$ , while the elements of  $T \cap \{(p+1)/2, \dots, p-1\}$  are denoted  $x'_1$  through  $x'_\nu$ , 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  $1 \leq r_i \leq (p-1)/2$  then  $r_i = x_j$  for some  $j$ , but if  $(p+1)/2 \leq r_i \leq p-1$  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,

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

Second, the sum is also

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

The previous two displays combine to give

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

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.  $\square$

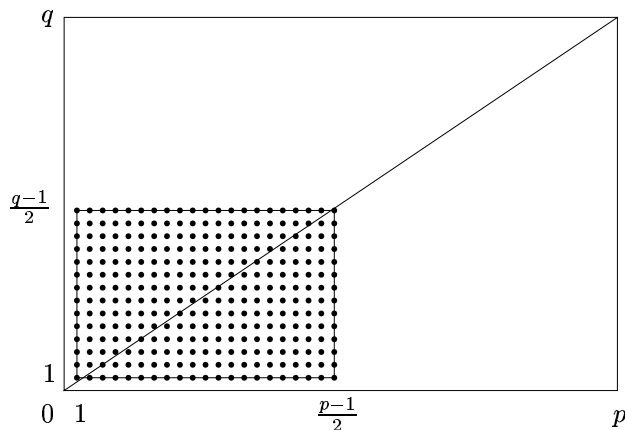


FIGURE 1. Lattice points

7. FIRST VERSION OF THE ALGORITHM

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

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

The utility of this formula is that for the left side we may assume that  $p < q$ , but then on the right side we may replace  $q$  by  $q \% p$ . 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: For all odd prime  $p$ ,

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

or, equivalently,  $(-1/p)$  is 1 if  $p$  is 1 modulo 4 but is  $-1$  if  $p$  is 3 modulo 4, and  $(2/p)$  is 1 if  $p$  is 1 or 7 modulo 8 but is  $-1$  if  $p$  is 3 or 5 modulo 8. We have already proved the auxiliary laws.

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.)

## 8. SPEEDING UP THE ALGORITHM: THE JACOBI SYMBOL

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

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

Thus when  $P$  is an odd prime, the Jacobi symbol is the Legendre symbol. However, for nonprime  $P$ , the condition  $(a/P) = 1$  does not 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  $P$ .

Note also 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  $P$  and  $Q$ ,

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

and for all odd positive  $P$ ,

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

The Jacobi symbol rules further speed Legendre symbol calculations since now we can use Jacobi symbols en route. For example,

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

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

$$\frac{P-1}{2} \equiv \sum_i \frac{p_i-1}{2} \pmod{2} \quad \text{and} \quad \frac{P^2-1}{8} \equiv \sum_i \frac{p_i^2-1}{8} \pmod{2}.$$

*Proof.* For the first congruence, compute that

$$\begin{aligned} P &= \prod_i (1 + (p_i - 1)) = 1 + \sum_i (p_i - 1) + \sum_{i \neq j} (p_i - 1)(p_j - 1) + \dots \\ &\equiv 1 + \sum_i (p_i - 1) \pmod{4}, \end{aligned}$$

and so

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

Similarly for the second congruence,

$$\begin{aligned} P^2 &= \prod_i (1 + (p_i^2 - 1)) = 1 + \sum_i (p_i^2 - 1) + \sum_{i \neq j} (p_i^2 - 1)(p_j^2 - 1) + \dots \\ &\equiv 1 + \sum_i (p_i^2 - 1) \pmod{16}, \end{aligned}$$

and so

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

□

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

$$\begin{aligned} \left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) &= \prod_{i,j} \left(\frac{p_i}{q_j}\right) \cdot \prod_{i,j} \left(\frac{q_j}{p_i}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right) \\ &= \prod_{i,j} (-1)^{(p_i-1)/2 \cdot (q_j-1)/2} = (-1)^{\sum_{i,j} (p_i-1)/2 \cdot (q_j-1)/2} \\ &= (-1)^{\sum_i (p_i-1)/2 \cdot \sum_j (q_j-1)/2} \\ &= (-1)^{(P-1)/2 \cdot (Q-1)/2}, \\ \left(\frac{-1}{P}\right) &= \prod_i \left(\frac{-1}{p_i}\right) = \prod_i (-1)^{(p_i-1)/2} = (-1)^{\sum_i (p_i-1)/2} \\ &= (-1)^{(P-1)/2}, \\ \left(\frac{2}{P}\right) &= \prod_i \left(\frac{2}{p_i}\right) = \prod_i (-1)^{(p_i^2-1)/8} = (-1)^{\sum_i (p_i^2-1)/8} \\ &= (-1)^{(P^2-1)/8}. \end{aligned}$$

A variant phrasing of the first two Jacobi symbol properties just shown is that for any odd  $P = \pm \prod_i p_i$  (positive or negative) and any positive odd  $Q = \prod_j q_j$  coprime to  $P$ ,

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

Finally, Kronecker incorporated even values into the denominator of Legendre-Jacobi symbols. Kronecker's extension of the Legendre symbol is

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

Thus  $(a/2)$  depends on  $a \pmod{8}$ . That is, for  $p = 2$  we have lost the property that  $(a/p)$  depends only on  $a \pmod{p}$ .

The Jacobi symbol extends correspondingly to arbitrary positive integer denominator,

$$\text{if } m = \prod_p p^{e_p} \text{ then } \left(\frac{a}{m}\right) = \prod_p \left(\frac{a}{p}\right)^{e_p}.$$

Again, if  $m$  is even then  $(a/m)$  as a function of its numerator no longer need depend only on  $a \bmod m$ .

The most general form of quadratic reciprocity that we need is as follows.

**Theorem 8.2.** *Let  $P$  be an arbitrary nonzero integer and let  $Q$  be a positive odd integer coprime to  $P$ ,*

$$P = 2^{e_2} P' \quad \text{where } P' = \pm \prod_{p \text{ odd}} p^{e_p}$$

and

$$Q = \prod_{p \text{ odd}} p^{f_p}, \quad f_p = 0 \text{ if } e_p > 0.$$

Then

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