

BACKGROUND ON QUADRATIC RECIPROCITY (CTNT 2024)

KEITH CONRAD

1. INTRODUCTION

The question quadratic reciprocity addresses is this: when p is an odd prime and $a \in \mathbf{Z}$, is $a \bmod p$ a perfect square? That is, does $x^2 \equiv a \bmod p$ have a solution? This is a yes/no question. It is asking whether a square root of $a \bmod p$ exists, not how to find it.

Table 1 below lists the squares mod 3, 5, 7, and 11. For example, the squares mod 5 are 0, 1, and 4 and the nonsquares mod 5 are 2 and 3.

p	$a \bmod p$	0	1	2						Squares mod p			
3	$a^2 \bmod 3$	0	1	1						0, 1			
5	$a \bmod 5$	0	1	2	3	4							
	$a^2 \bmod 5$	0	1	4	4	1					0, 1, 4		
7	$a \bmod 7$	0	1	2	3	4	5	6					
	$a^2 \bmod 7$	0	1	4	2	2	4	1			0, 1, 2, 4		
11	$a \bmod 11$	0	1	2	3	4	5	6	7	8	9	10	
	$a^2 \bmod 11$	0	1	4	9	5	3	3	5	9	4	1	0, 1, 3, 4, 5, 9

TABLE 1. Squares mod p when $p = 3, 5, 7,$ and 11 .

2. COUNTING SQUARES MODULO A PRIME AND THE LEGENDRE SYMBOL

The nonzero square values mod p in the central part of Table 1 are symmetric around the middle, *e.g.*, 1, 4, 2, 2, 4, 1 mod 7. That reflects the algebraic rule $a^2 \equiv (-a)^2 \bmod p$, or equivalently $a^2 \equiv (p - a)^2 \bmod p$.

Lemma 2.1. *For an odd prime p , $a^2 \equiv b^2 \bmod p$ if and only if $a \equiv \pm b \bmod p$ and the number of nonzero squares modulo p is $(p - 1)/2$.*

Proof. Squaring on the group $(\mathbf{Z}/(p))^\times$ is a homomorphism of the group to itself with kernel ± 1 : $x^2 \equiv 1 \bmod p$ is the same as $x^2 - 1 = 0$ in the field $\mathbf{Z}/(p)$, which is the same as $(x + 1)(x - 1) = 0$ in $\mathbf{Z}/(p)$. The only solutions are 1 and -1 in $\mathbf{Z}/(p)$, which are distinct since $p > 2$. Since squaring on $(\mathbf{Z}/(p))^\times$ has kernel $\{\pm 1\}$, $a^2 = b^2$ in $(\mathbf{Z}/(p))^\times$ if and only if $a = bc$ where $c^2 = 1$ in $\mathbf{Z}/(p)$, and we showed $c = \pm 1$ in $\mathbf{Z}/(p)$, so $c \equiv \pm 1 \bmod p$.

Since $(\mathbf{Z}/(p))^\times$ has order $p - 1$ and squaring $(\mathbf{Z}/(p))^\times \rightarrow (\mathbf{Z}/(p))^\times$ has a kernel of order 2, its image has order $(p - 1)/2$. □

Example 2.2. The nonzero squares mod 11 are a^2 where $1 \leq a \leq (11 - 1)/2 = 5$, as we saw earlier in Table 1.

We can detect squares using a refinement of Fermat's little theorem. For all $a \not\equiv 0 \pmod p$, $a^{(p-1)/2} \pmod p$ is a square root of 1, since

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

Thus

$$(2.1) \quad a^{(p-1)/2} \equiv \pm 1 \pmod p.$$

Euler found that the value of $a^{(p-1)/2} \pmod p$ distinguishes squares from nonsquares, and his result in the next theorem is called *Euler's criterion*.

Theorem 2.3 (Euler). *Let p be an odd prime. For $a \not\equiv 0 \pmod p$,*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \pmod p & \text{if } a \equiv \square \pmod p, \\ -1 \pmod p & \text{if } a \not\equiv \square \pmod p. \end{cases}$$

Proof. Suppose $a \equiv b^2 \pmod p$ for some b . Then $b \not\equiv 0 \pmod p$, so

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod p$$

by Fermat's little theorem.

We now show the converse:

$$(2.2) \quad a^{(p-1)/2} \equiv 1 \pmod p \implies a \equiv \square \pmod p.$$

The congruence on the left says a is a root in $\mathbf{Z}/(p)$ of the polynomial $x^{(p-1)/2} - 1$. A polynomial with coefficients in a field has no more roots in the field than its degree, so there are *at most* $(p-1)/2$ roots of $x^{(p-1)/2} - 1$ in $\mathbf{Z}/(p)$. The nonzero squares in $\mathbf{Z}/(p)$ are roots, and Lemma 2.1 tells us there are $(p-1)/2$ nonzero squares in $\mathbf{Z}/(p)$, so the nonzero squares exhaust all the roots of $x^{(p-1)/2} - 1$ in $\mathbf{Z}/(p)$.

By (2.1) we know $a^{(p-1)/2} \equiv \pm 1 \pmod p$ for all $a \not\equiv 0 \pmod p$. Therefore by (2.2) we have $a^{(p-1)/2} \equiv -1 \pmod p$ for nonsquares $a \pmod p$. \square

Example 2.4. Table 2 below illustrates the distinction between squares and nonsquares in $(\mathbf{Z}/(11))^\times$ by raising everything to the power $\frac{11-1}{2} = 5$. The numbers a with 5th power 1 mod 11 are the nonzero squares mod 11 and the numbers with 5th power -1 mod 11 are the nonsquares mod 11. Compare with the bottom of Table 1.

a	1	2	3	4	5	6	7	8	9	10
$a^5 \pmod{11}$	1	-1	1	1	1	-1	-1	-1	1	-1

TABLE 2.

Example 2.5. Let's see if $30 \equiv \square \pmod{79}$ (the modulus is prime). Using a computer, $30^{(79-1)/2} = 30^{39} \equiv 78 \equiv -1 \pmod{79}$, so $30 \pmod{79}$ is not a square. That is not a calculation you would want to do directly by hand.

Euler's criterion (Theorem 2.3) lets us describe odd primes p where $-1 \pmod p$ is a square.

Corollary 2.6. *For odd primes p , $-1 \equiv \square \pmod p$ if and only if $p \equiv 1 \pmod 4$.*

Proof. By Euler's criterion, $-1 \equiv \square \pmod p \iff (-1)^{(p-1)/2} \equiv 1 \pmod p$. Since $(-1)^{(p-1)/2} = \pm 1$ and $-1 \not\equiv 1 \pmod p$, saying $(-1)^{(p-1)/2} \equiv 1 \pmod p$ is the same as $(-1)^{(p-1)/2} = 1 \pmod p$, which means $(p-1)/2$ is even. That is the same as $p = 1 + 4k$ for some $k \in \mathbf{Z}$. \square

A result like Corollary 2.6 for numbers besides -1 is not easy to obtain: $3 \equiv \square \pmod{p} \iff 3^{(p-1)/2} \equiv 1 \pmod{p}$, but there isn't a simple formula for $3^{(p-1)/2}$.

Squares and nonsquares in $(\mathbf{Z}/(p))^\times$ are called quadratic residues and quadratic non-residues. Gauss wrote $a R p$ when $a \pmod{p}$ is a quadratic residue and $a N p$ otherwise, e.g., $3 R 11$ and $6 N 11$. In 1798 Legendre introduced a notation that made the quadratic residue and quadratic non-residue relations into numerical functions.

Definition 2.7. For $a \in \mathbf{Z}$ and an odd prime p , the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as

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

The reason behind using these values, at least when $a \not\equiv 0 \pmod{p}$, is that they appear on the right side of Euler's criterion, so we can say

$$(2.3) \quad a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

We set $\left(\frac{a}{p}\right) = 0$ when $a \equiv 0 \pmod{p}$ so that this congruence is also valid in that case while keeping all the values of the Legendre symbol multiplicatively closed. It also makes the last part of Theorem 2.10 below true for all a .

Example 2.8. By Table 1, $\left(\frac{2}{3}\right) = -1$, $\left(\frac{2}{5}\right) = -1$, $\left(\frac{2}{7}\right) = 1$, and $\left(\frac{3}{11}\right) = 1$.

Example 2.9. The only nonzero squares mod 5 are 1 and 4. Since $-7 \equiv 3 \pmod{5}$, we have $\left(\frac{-7}{5}\right) = \left(\frac{3}{5}\right) = -1$. The Legendre symbol $\left(\frac{10}{5}\right)$ is 0.

The following theorem summarizes basic algebraic properties of the Legendre symbol.

Theorem 2.10. Let p be an odd prime. For all a and b in \mathbf{Z} ,

- (1) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$,
- (2) if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
- (3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
- (4) the number of solutions to $x^2 \equiv a \pmod{p}$ is $1 + \left(\frac{a}{p}\right)$.

Proof. The first property is just (2.3).

The second property reflects the fact that $\left(\frac{a}{p}\right)$ is determined by the behavior of $a \pmod{p}$.

For the third property, note $\left(\frac{ab}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ are 0, 1, or -1 , and these three values are distinct modulo p since $p > 2$. So we can check $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ in \mathbf{Z} by checking instead that $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$. Working modulo p , the two sides are congruent to powers:

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \pmod{p}, \\ \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &\equiv a^{(p-1)/2}b^{(p-1)/2} \pmod{p}. \end{aligned}$$

The right sides of both congruences are equal, so the left sides are congruent mod p and thus are equal in \mathbf{Z} since they are 0, 1, or -1 .

To show the fourth property, that $x^2 \equiv a \pmod{p}$ has $1 + \left(\frac{a}{p}\right)$ solutions mod p , take cases.

- If $a \pmod{p}$ is a nonsquare then $x^2 \equiv a \pmod{p}$ has 0 solutions and $1 + \left(\frac{a}{p}\right) = 1 - 1 = 0$.

- If $a \bmod p$ is a nonzero square then $x^2 \equiv a \bmod p$ has 2 solutions by Theorem 2.1 and $1 + \left(\frac{a}{p}\right) = 1 + 1 = 2$.
- If $a \equiv 0 \bmod p$ then $x^2 \equiv a \bmod p$ has 1 solution and $1 + \left(\frac{a}{p}\right) = 1 + \left(\frac{0}{p}\right) = 1 + 0 = 1$. \square

The third property of Theorem 2.10, called the multiplicativity of the Legendre symbol, says the following three facts about *nonzero* numbers modulo p when p is an odd prime:

- the product of two squares is a square (in terms of the Legendre symbol, $1 = 1 \cdot 1$),
- the product of a square and a nonsquare is a nonsquare ($-1 = (1)(-1) = (-1)(1)$),
- the product of two nonsquares is a square ($1 = (-1)(-1)$).

The first two facts are true in all fields, by simple algebra. But the last fact, that nonsquares in $\mathbf{Z}/(p)$ have a product that is a square, is somewhat special $\mathbf{Z}/(p)$: it is not true in most fields.

Example 2.11. In $\mathbf{Z}/(11)$, 2 and 7 are not squares. Their product is 3, which is a square ($3 = 5^2$ in $\mathbf{Z}/(11)$).

Example 2.12. When a modulus m is composite, it is usually *false* that a product of two nonsquares mod m is a square mod m . For instance, 2 and 7 are not squares mod 15, and their product 14 is also not a square mod 15.

The real numbers share with $\mathbf{Z}/(p)$ the property that the product of nonsquares is a square since two negative numbers have a product that is positive. This has a common explanation: when $K = \mathbf{Z}/(p)$ or \mathbf{R} , $[K^\times : (K^\times)^2] = 2$. Whenever K is a field in which $[K^\times : (K^\times)^2] = 2$, $K^\times / (K^\times)^2$ has order 2, which implies two nonsquares in K^\times are equal in $K^\times / (K^\times)^2$ and thus their product is in $(K^\times)^2$. In Example 2.12, the squares in $(\mathbf{Z}/(15))^\times$ have index 4, not 2. More generally, when $m > 1$ is odd, the squares in $(\mathbf{Z}/(m))^\times$ have index 2 if and only if m is a prime power.

Remark 2.13. When p is an arbitrary prime, even $p = 2$, at least one of 2, 3, or 6 is a square mod p . An interesting use of this is that it implies $x^4 - 10x^2 + 1 \bmod p$ is reducible for all p even though $x^4 - 10x^2 + 1$ is irreducible over \mathbf{Q} : see <https://kconrad.math.uconn.edu/blurbs/ringtheory/reducibleallp.pdf>.

For any nonzero integer a , factor it as

$$a = \varepsilon p_1 p_2 \cdots p_r,$$

where $\varepsilon = \pm 1$ and the p_i 's are prime numbers. Some p_i 's may be equal. By multiplicativity,

$$\left(\frac{a}{p}\right) = \left(\frac{\varepsilon}{p}\right) \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right).$$

Thus computing $\left(\frac{a}{p}\right)$ is reduced to the case where a is -1 or a prime number. Because of the peculiar nature of the prime 2 in the context of squares, it is useful to consider three cases rather than two: $a = -1$, $a = 2$, and $a = q$ is an odd prime. The evaluation of $\left(\frac{a}{p}\right)$ in these cases is given by the quadratic reciprocity law, which we turn to next.

3. THE QUADRATIC RECIPROCITY LAW

The following formulas for $\left(\frac{a}{p}\right)$ when a is an odd prime, -1 , or 2 are collectively called the quadratic reciprocity law.

Theorem 3.1 (Quadratic Reciprocity). *Let p and q be distinct odd primes. Then*

$$(3.1) \quad \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{if } p \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\frac{p}{q}\right), & \text{if } p \text{ and } q \equiv 3 \pmod{4} \end{cases}$$

and

$$(3.2) \quad \left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ -1, & \text{if } p \equiv 3 \pmod{4}, \end{cases} \quad \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1, & \text{if } p \equiv 3, 5 \pmod{8}, \end{cases}$$

Equation (3.1) is called the *main law* of quadratic reciprocity and the equations in (3.2) are called the *supplementary laws*. In words, the main law says

- if p or q is 1 mod 4 then $q \equiv \square \pmod{p}$ if and only if $p \equiv \square \pmod{q}$,
- if p and q are 3 mod 4 then $q \equiv \square \pmod{p}$ if and only if $p \not\equiv \square \pmod{q}$.

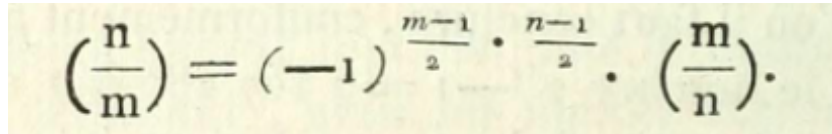
The supplementary laws say $-1 \equiv \square \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$ (which is Corollary 2.6) and $2 \equiv \square \pmod{p}$ if and only if $p \equiv \pm 1 \pmod{8}$.

The equations in (3.1) and (3.2) are expressible without using cases as

$$(3.3) \quad \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right), \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

This is because when p is an odd prime, or just an odd number, $(p-1)/2$ is even exactly when $p \equiv 1 \pmod{4}$, $p^2 \equiv 1 \pmod{16}$ when $p \equiv 1, 7 \pmod{8}$, and $p^2 \equiv 9 \pmod{16}$ when $p \equiv 3, 5 \pmod{8}$.

Figure 1 is how the main law appears in Legendre's *Essai sur la Théorie des Nombres* [6, p. 214], where m and n are distinct odd primes. At the top of this page Legendre introduced the term “loi de réciprocité”.



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

FIGURE 1. Quadratic reciprocity as written by Legendre in 1798.

Example 3.2. Let's use quadratic reciprocity to calculate $\left(\frac{30}{79}\right)$:

$$(3.4) \quad \left(\frac{30}{79}\right) = \left(\frac{2}{79}\right) \left(\frac{3}{79}\right) \left(\frac{5}{79}\right),$$

so computing $\left(\frac{30}{79}\right)$ is reduced to computing $\left(\frac{q}{79}\right)$ for $q = 2, 3$, and 5.

Since $79 \equiv 7 \pmod{8}$, the supplementary law tells us

$$\left(\frac{2}{79}\right) = 1.$$

Using the main law

$$\begin{aligned} \left(\frac{3}{79}\right) &= -\left(\frac{79}{3}\right) \quad \text{since } 3, 79 \equiv 3 \pmod{4} \\ &= -\left(\frac{1}{3}\right) \quad \text{since } 79 \equiv 1 \pmod{3} \\ &= -1 \end{aligned}$$

and

$$\begin{aligned} \left(\frac{5}{79}\right) &= \left(\frac{79}{5}\right) \quad \text{since } 5 \equiv 1 \pmod{4} \\ &= \left(\frac{4}{5}\right) \quad \text{since } 79 \equiv 4 \pmod{5} \\ &= 1. \end{aligned}$$

Thus $\left(\frac{30}{79}\right) = 1 \cdot (-1) \cdot 1 = -1$, so 30 is not a square modulo 79. We had seen this earlier in Example 2.5 by computing $30^{(79-1)/2} \pmod{79}$.

Example 3.3. Is 60 mod 103 a square? Note 103 is prime. We want to compute $\left(\frac{60}{103}\right)$. Since $60 = 4 \cdot 3 \cdot 5$,

$$\left(\frac{60}{103}\right) = \left(\frac{4}{103}\right) \left(\frac{3}{103}\right) \left(\frac{5}{103}\right) = \left(\frac{3}{103}\right) \left(\frac{5}{103}\right),$$

so we are reduced to computing $\left(\frac{3}{103}\right)$ and $\left(\frac{5}{103}\right)$. By the main law,

$$\begin{aligned} \left(\frac{3}{103}\right) &= -\left(\frac{103}{3}\right) \quad \text{since } 3, 103 \equiv 3 \pmod{4} \\ &= -\left(\frac{1}{3}\right) \quad \text{since } 103 \equiv 1 \pmod{3} \\ &= -1 \end{aligned}$$

and

$$\begin{aligned} \left(\frac{5}{103}\right) &= \left(\frac{103}{5}\right) \quad \text{since } 5 \equiv 1 \pmod{4} \\ &= \left(\frac{3}{5}\right) \quad \text{since } 103 \equiv 3 \pmod{5} \\ &= -1. \end{aligned}$$

Thus $\left(\frac{60}{103}\right) = (-1)(-1) = 1$, so 60 mod 103 is a square. This does *not* say what 60 mod 103 is a square of. By a brute force search, $60 \equiv 36^2 \pmod{103}$.

To carry out Legendre symbol calculations by hand, it is worth memorizing the nonzero squares modulo small primes so that you recognize them by sight: the only (nonzero) square mod 3 is 1, mod 5 there is only 1 and 4, and mod 7 there is only 1, 2, and 4. Since there are $(p-1)/2$ nonzero squares mod p , once you have found $(p-1)/2$ different squares you have found them all and you can stop. Also remember that for all odd a , $a^2 \equiv 1 \pmod{8}$.

Remark 3.4. Is $-1 \equiv \square \pmod{161}$? Since $161 \equiv 1 \pmod{4}$, by the supplementary law for $\left(\frac{-1}{p}\right)$ we have $\left(\frac{-1}{161}\right) = 1$, so $-1 \equiv \square \pmod{161}$. However, this reasoning is wrong because 161

is not prime: $161 = 7 \cdot 23$. In fact, $-1 \pmod{161}$ is *not* a square: if $-1 \equiv x^2 \pmod{161}$ then $-1 \equiv x^2 \pmod{7}$, but $-1 \pmod{7}$ is not a square: by the supplementary law $\left(\frac{-1}{7}\right) = -1$ since $7 \equiv 3 \pmod{4}$, or by Table 1 the nonzero squares mod 7 are 1, 2, and 4.

Another error to avoid is thinking $\left(\frac{a}{p}\right)^2 = 1$ since $\left(\frac{a}{p}\right) = \pm 1$: check first that $\left(\frac{a}{p}\right) \neq 0$.

Quadratic reciprocity was first conjectured by Euler in 1744. He proved the supplementary laws but not the main law. Legendre in 1785 proved some cases of the main law but his reasoning had gaps in other cases: see Appendix A. The first complete proof was given by Gauss in 1796 when he was 18. He called it the *aureum theorem* (“golden theorem”) and eventually found eight proofs. Quadratic reciprocity has more proofs than any other theorem in mathematics except perhaps the Pythagorean theorem. For a list of over 300 proofs, see https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html.

In the remaining three sections we will give three separate proofs of quadratic reciprocity. If one proof is too technical for you, try another. The second proof uses the least background. There is not any intuition that explains why the proofs should work. In each case quadratic reciprocity falls out as something like a little miracle.

4. PROOF BY GAUSS SUMS

One of the most commonly presented proofs of quadratic reciprocity (at least the main law) uses properties of the sum

$$G_p = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a = \sum_{a \not\equiv 0 \pmod{p}} \left(\frac{a}{p}\right) \zeta_p^a,$$

where ζ_p is a nontrivial p th root of unity. This sum is called a Gauss sum¹ and it first appeared in Gauss’ 6th proof of quadratic reciprocity. The value of G_p may depend on the choice of ζ_p . Often the standard nontrivial p th root of unity $e^{2\pi i/p}$ is used, but any choice will suffice here.

Example 4.1. Taking $p = 3$,

$$G_3 = \sum_{a=1}^2 \left(\frac{a}{3}\right) \zeta_3^a = \zeta_3 - \zeta_3^2 = \zeta_3 - \zeta_3^{-1}.$$

If $\zeta_3 = e^{2\pi i/3}$, then $G_3 = 2i \sin(2\pi/3) = 2i(\sqrt{3}/2) = i\sqrt{3}$. If $\zeta_3 = e^{-2\pi i/3}$, then $G_3 = -i\sqrt{3}$.

Example 4.2. Taking $p = 5$,

$$G_5 = \sum_{a=1}^4 \left(\frac{a}{5}\right) \zeta_5^a = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = (\zeta_5 + \zeta_5^{-1}) - (\zeta_5^2 + \zeta_5^{-2}).$$

If $\zeta_5 = e^{2\pi i/5}$, then $G_5 = 2 \cos(2\pi/5) - 2 \cos(4\pi/5) \approx 2.236067$, which looks like $\sqrt{5}$. If $\zeta_5 = e^{4\pi i/5}$, then $G_5 \approx -2.236067$ is apparently $-\sqrt{5}$.

Lemma 4.3. When p is an odd prime, $G_p^2 = (-1)^{(p-1)/2} p$.

¹The term “Gauss sum” has a much wider meaning as certain sums on finite rings, such as $\mathbf{Z}/(m)$ or finite fields: see <https://kconrad.math.uconn.edu/blurbs/gradnumthy/Gauss-Jacobi-sums.pdf>.

Proof. Write G_p^2 as a product of sums over two independent indices running over $(\mathbf{Z}/(p))^\times$:

$$G_p^2 = \sum_{a \neq 0} \left(\frac{a}{p}\right) \zeta_p^a \cdot \sum_{b \neq 0} \left(\frac{b}{p}\right) \zeta_p^b = \sum_{a, b \neq 0} \left(\frac{ab}{p}\right) \zeta_p^{a+b} = \sum_{a \neq 0} \sum_{b \neq 0} \left(\frac{ab}{p}\right) \zeta_p^{a+b}.$$

In the inner sum (for each nonzero a), make the change of variables $b \mapsto ab$, so

$$\begin{aligned} G_p^2 &= \sum_{a \neq 0} \sum_{b \neq 0} \left(\frac{a^2 b}{p}\right) \zeta_p^{a(1+b)} \\ &= \sum_{b \neq 0} \sum_{a \neq 0} \left(\frac{b}{p}\right) \zeta_p^{a(1+b)} \\ &= \sum_{b \neq 0} \left(\frac{b}{p}\right) \sum_{a \neq 0} (\zeta_p^{1+b})^a \\ &= \sum_{b \neq 0} \left(\frac{b}{p}\right) \left(\sum_a (\zeta_p^{1+b})^a - 1 \right) \end{aligned}$$

The number ζ_p^{1+b} is a nontrivial p th root of unity unless $b \equiv -1 \pmod{p}$, and when it is nontrivial the sum of its a th powers over all a is 0 (sum a finite geometric series), so separate the term in the outer sum where $b = -1$ from the other terms:

$$G_p^2 = \sum_{b \neq 0, -1} \left(\frac{b}{p}\right) (-1) + \left(\frac{-1}{p}\right) (p-1) = \sum_{b \neq 0} \left(\frac{b}{p}\right) + \left(\frac{-1}{p}\right) p.$$

The sum over nonzero b has as many Legendre symbol equal to 1 as to -1 since there are as many squares as nonsquares in $(\mathbf{Z}/(p))^\times$. Thus that sum is 0, so $G_p^2 = \left(\frac{-1}{p}\right) p$. \square

Theorem 4.4. *When p and q are distinct odd primes, $\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdots (q-1)/2} \left(\frac{p}{q}\right)$.*

Proof. The Gauss sum G_p lies in the ring $\mathbf{Z}[\zeta_p]$. Although q need not be prime in $\mathbf{Z}[\zeta_p]$, the quotient ring $\mathbf{Z}[\zeta_p]/(q)$ has prime characteristic q , so the q th power map on $\mathbf{Z}[\zeta_p]/(q)$ is additive. Since q is odd, $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$ no matter what value $\left(\frac{a}{p}\right)$ is, so

$$G_p^q \equiv \sum_{a \neq 0} \left(\frac{a}{p}\right)^q \zeta_p^{qa} \equiv \sum_{a \neq 0} \left(\frac{a}{p}\right) \zeta_p^{qa} \pmod{q\mathbf{Z}[\zeta_p]}.$$

Let $q' \pmod{p}$ be the inverse of $q \pmod{p}$, so $\left(\frac{q'}{p}\right) = \left(\frac{q}{p}\right)$. Make the change of variables $a \mapsto q'a$ in the sum on the right:

$$(4.1) \quad G_p^q \equiv \sum_{a \neq 0} \left(\frac{q'a}{p}\right) \zeta_p^a \equiv \left(\frac{q'}{p}\right) \sum_{a \neq 0} \left(\frac{a}{p}\right) \zeta_p^a = \left(\frac{q}{p}\right) G_p \pmod{q\mathbf{Z}[\zeta_p]}.$$

Since p is a unit in $\mathbf{Z}/(q)$, p is also a unit in $\mathbf{Z}[\zeta_p]/(q)$. Then the relation $G_p^2 = \pm p$ in Lemma 4.3 implies G_p is a unit in $\mathbf{Z}[\zeta_p]/(q)$, so we can divide through by G_p in (4.1):

$$(4.2) \quad G_p^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q\mathbf{Z}[\zeta_p]}.$$

Since $q-1$ is even, using Lemma 4.3 we get

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

Using this in (4.2),

$$(-1)^{(p-1)/2 \cdot (q-1)/2} p^{(q-1)/2} \equiv \left(\frac{q}{p}\right) \pmod{q\mathbf{Z}[\zeta_p]}.$$

Since $p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \pmod{q\mathbf{Z}}$,

$$(4.3) \quad (-1)^{(p-1)/2 \cdot (q-1)/2} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q\mathbf{Z}[\zeta_p]}.$$

The two sides of this congruences are ± 1 , so as long as $1 \not\equiv -1 \pmod{q\mathbf{Z}[\zeta_p]}$ the congruence in (4.3) implies equality of the two sides in \mathbf{Z} , which is the main law of quadratic reciprocity.

If $1 \equiv -1 \pmod{q\mathbf{Z}[\zeta_p]}$ then subtracting and dividing by q implies $2/q \in \mathbf{Z}[\zeta_p]$. Check that $\mathbf{Q} \cap \mathbf{Z}[\zeta_p] = \mathbf{Z}$ (this may a subtle point if you have not worked with algebraic integers), so $2/q \in \mathbf{Z}$, which is a contradiction. \square

Theorem 4.5. *When p is an odd prime, $\left(\frac{2}{p}\right) = 1$ when $p \equiv 1, 7 \pmod{8}$ and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3, 5 \pmod{8}$.*

Proof. We will use a modified Gauss sum

$$G = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 = \zeta_8 + \zeta_8^{-1} - (\zeta_8^3 + \zeta_8^{-3}).$$

The possible values of ζ_8 in \mathbf{C} are $e^{2\pi ia/8}$ where $a \in \{1, 3, 5, 7\}$. When $\zeta_8 = e^{2\pi i/7}$,

$$\zeta_8 + \zeta_8^{-1} = 2 \cos(2\pi/8) = 2 \cos(\pi/4) = 2/\sqrt{2} = \sqrt{2}$$

and

$$\zeta_8^3 + \zeta_8^{-3} = 2 \cos(6\pi/8) = 2 \cos(3\pi/4) = -2/\sqrt{2} = -\sqrt{2},$$

so $G = \sqrt{2} - (-\sqrt{2}) = 2\sqrt{2}$. In a similar way, G is $2\sqrt{2}$ or $-2\sqrt{2}$ when $\zeta_8 = e^{2\pi ia/8}$ and a is 3, 5, or 7. No matter which ζ_8 you pick, $G^2 = 8$.

The number G lies in the ring $\mathbf{Z}[\zeta_8]$. We will calculate with G in the quotient ring $\mathbf{Z}[\zeta_8]/(p)$, which has characteristic p even though p may not be prime in $\mathbf{Z}[\zeta_8]$. Since the p th power map is additive on rings with characteristic p and $(-1)^p = -1$,

$$G^p \equiv \zeta_8^p - \zeta_8^{3p} - \zeta_8^{5p} + \zeta_8^{7p} \pmod{p\mathbf{Z}[\zeta_p]}.$$

If $p \equiv \pm 1 \pmod{8}$, then the right side is G . If $p \equiv \pm 3 \pmod{8}$, then the right side is $-G$. Thus

$$(4.4) \quad G^p = \varepsilon_p G \pmod{p\mathbf{Z}[\zeta_8]}$$

where ε_p is 1 when $p \equiv \pm 1 \pmod{8}$ and ε_p is -1 when $p \equiv \pm 3 \pmod{8}$. Since 2 is a unit in $\mathbf{Z}/(p)$, 2 is also a unit in $\mathbf{Z}[\zeta_8]/(p)$. Then by $G^2 = 8$ we know G is a unit in $\mathbf{Z}[\zeta_8]/(p)$, so we can divide through (4.4) by G to get

$$(4.5) \quad G^{p-1} \equiv \varepsilon_p \pmod{p\mathbf{Z}[\zeta_8]}.$$

Since $p-1$ is even, $G^{p-1} = (G^2)^{(p-1)/2} = 8^{(p-1)/2} = (2^{(p-1)/2})^3$. We have $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{p\mathbf{Z}}$, so $8^{(p-1)/2} \equiv \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right) \pmod{p\mathbf{Z}}$. Using this in (4.5),

$$\left(\frac{2}{p}\right) \equiv \varepsilon_p \pmod{p\mathbf{Z}[\zeta_8]}.$$

As in the previous proof, since the two sides of this congruences are ± 1 , we get their equality in \mathbf{Z} as long as $1 \not\equiv -1 \pmod{p\mathbf{Z}[\zeta_8]}$, and that would be the supplementary law for $\left(\frac{2}{p}\right)$.

If $1 \equiv -1 \pmod{p\mathbf{Z}[\zeta_8]}$ then subtracting and dividing by p implies $2/p \in \mathbf{Z}[\zeta_8]$. Check that $\mathbf{Q} \cap \mathbf{Z}[\zeta_8] = \mathbf{Z}$, so $2/p \in \mathbf{Z}$, and that's a contradiction. \square

5. PROOF BY COUNTING SOLUTIONS TO CONGRUENCES MOD p

In this section we will prove the supplementary law for $\left(\frac{2}{p}\right)$ and the main law by a method due to V. A. Lebesgue² [5, pp. 132–134] in 1838. It is based on counting the number of points on the “mod p circle”

$$x^2 + y^2 \equiv a \pmod{p}.$$

Lemma 5.1. *For $a \in \mathbf{Z}/(p)$,*

$$|\{(x, y) : x, y \in \mathbf{Z}/(p), x^2 + y^2 = a\}| = \begin{cases} p - \left(\frac{-1}{p}\right), & \text{if } a \neq 0, \\ p + \left(\frac{-1}{p}\right)(p-1), & \text{if } a = 0. \end{cases}$$

In particular, the number of ways of writing a as a sum of two squares in $\mathbf{Z}/(p)$ is the same for all nonzero a .

Proof. Let N_a be the number of solutions. First we will compute N_0 and then we will look at N_a for $a \not\equiv 0 \pmod{p}$.

Since $N_0 = |\{(x, y) : x, y \in \mathbf{Z}/(p), x^2 = -y^2\}|$, if there is a solution with $y \not\equiv 0 \pmod{p}$ then dividing by y^2 shows $-1 \equiv \square \pmod{p}$. So contrapositively, if $-1 \not\equiv \square \pmod{p}$ then we must have $y \equiv 0 \pmod{p}$, so $x \equiv 0 \pmod{p}$, which means $N_0 = 1$. If $-1 \equiv \square \pmod{p}$, say $-1 \equiv t^2 \pmod{p}$, then $x^2 \equiv -y^2 \pmod{p}$ if and only if $x \equiv \pm ty \pmod{p}$, so for each nonzero y ($p-1$ choices for that) there are 2 choices of x and if $y = 0$ then $x = 0$. Thus $N_0 = 2(p-1) + 1 = 2p-1$, so

$$N_0 = \begin{cases} 1, & \text{if } -1 \not\equiv \square \pmod{p}, \\ 2p-1, & \text{if } -1 \equiv \square \pmod{p}, \end{cases}$$

which is described in a uniform way by the single formula $p + \left(\frac{-1}{p}\right)(p-1)$.

Now we compute N_a for $a \not\equiv 0 \pmod{p}$. We will show N_a is the same for all nonzero $a \pmod{p}$ and then compute this common value.

Write

$$N_a = \sum_{b+c=a} |\{x : x^2 \equiv b \pmod{p}\}| |\{y : y^2 \equiv c \pmod{p}\}|,$$

where the sum runs over all b and c in $\mathbf{Z}/(p)$ having sum a modulo p . By Theorem 2.10(4),

$$\begin{aligned} N_a &= \sum_{b+c=a} \left(1 + \left(\frac{b}{p}\right)\right) \left(1 + \left(\frac{c}{p}\right)\right) \\ &= \sum_{b+c=a} \left(1 + \left(\frac{b}{p}\right) + \left(\frac{c}{p}\right) + \left(\frac{bc}{p}\right)\right) \\ &= \sum_b \left(1 + \left(\frac{b}{p}\right) + \left(\frac{a-b}{p}\right) + \left(\frac{b(a-b)}{p}\right)\right) \\ &= p + \sum_b \left(\frac{b}{p}\right) + \sum_b \left(\frac{a-b}{p}\right) + \sum_b \left(\frac{b(a-b)}{p}\right). \end{aligned}$$

²This is not the Henri Lebesgue from measure theory.

There are as many squares as nonsquares among the nonzero values mod p , so the second and third sums above each contain as many 1's as -1 's, so both sums are 0. Thus

$$N_a = p + \sum_b \left(\frac{b(a-b)}{p} \right).$$

The formula looks like it depends on a . We will make the dependence disappear by a clever change of variables: in the sum over all $b \bmod p$, replace b with ab . (This is an invertible change of variables since $a \not\equiv 0 \pmod p$.) Then

$$N_a = p + \sum_b \left(\frac{ab(a-ab)}{p} \right) = p + \sum_b \left(\frac{a^2b(1-b)}{p} \right) = p + \sum_b \left(\frac{b(1-b)}{p} \right).$$

The last formula does not involve a , so all N_a for $a \not\equiv 0 \pmod p$ are the same. What is this common value?

Since $\sum_{a \bmod p} N_a = p^2$ (because every pair (x, y) in $(\mathbf{Z}/(p))^2$ is counted by one N_a), write N_a for $a \not\equiv 0 \pmod p$ as N_1 to get $N_0 + (p-1)N_1 = p^2$, so

$$N_1 = \frac{p^2 - N_0}{p-1} = \frac{p^2 - p - \left(\frac{-1}{p}\right)(p-1)}{p-1} = p - \left(\frac{-1}{p}\right). \quad \square$$

Theorem 5.2. For odd primes p ,

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

Proof. We will count the number of points on the “mod p unit circle”

$$x^2 + y^2 \equiv 1 \pmod p$$

in two ways. By Lemma 5.1, there are $p - \left(\frac{-1}{p}\right)$ points. We will now compute the number, as an integer modulo 8, in a different way.

The solutions to $x^2 + y^2 \equiv 1 \pmod p$ come in collections of size 8: given any solution (x, y) we have 8 solutions by changing signs independently:

$$(x, y), (-x, y), (x, -y), (-x, -y), (y, x), (-y, x), (y, -x), (-y, -x).$$

Actually, these 8 solutions mod p are different *provided* $x \not\equiv 0 \pmod p$, $y \not\equiv 0 \pmod p$, and $x \not\equiv \pm y \pmod p$. So the total number of solutions is congruent modulo 8 to the number of solutions with $x \equiv 0 \pmod p$ or $y \equiv 0 \pmod p$ or $x \equiv \pm y \pmod p$. The condition $x \equiv 0 \pmod p$ means $(x, y) = (0, \pm 1)$, $y \equiv 0 \pmod p$ means $(x, y) = (\pm 1, 0)$, and $x \equiv \pm y \pmod p$ means $(x, y) = (c, \pm c)$ where $2c^2 \equiv 1 \pmod p$. There are such c precisely when $2 \equiv \square \pmod p$, in which case c has 2 values. So the number of exceptions we have found is $2 + 2 + 4 = 8$ if $2 \equiv \square \pmod p$ and $2 + 2 + 0 = 4$ if $2 \not\equiv \square \pmod p$. Thus

$$p - \left(\frac{-1}{p}\right) \equiv \begin{cases} 0 \pmod 8, & \text{if } 2 \equiv \square \pmod p, \\ 4 \pmod 8, & \text{if } 2 \not\equiv \square \pmod p. \end{cases}$$

We can write this in a uniform way as

$$p - \left(\frac{-1}{p}\right) \equiv 2 \left(1 - \left(\frac{2}{p}\right) \right) \pmod 8.$$

Dividing this congruence by 2 (which reduces the modulus to 4) and rearranging terms,

$$\left(\frac{2}{p}\right) \equiv 1 - \frac{p - \left(\frac{-1}{p}\right)}{2} \pmod{4}.$$

Now take cases on $p \pmod{8}$. If $p \equiv 1 \pmod{8}$, $p - \left(\frac{-1}{p}\right) = p - 1 \equiv 0 \pmod{8}$, so $1 - \frac{p - \left(\frac{-1}{p}\right)}{2} \equiv 1 \pmod{4}$. If $p \equiv 3 \pmod{8}$, $p - \left(\frac{-1}{p}\right) = p + 1 \equiv 4 \pmod{8}$, so $1 - \frac{p - \left(\frac{-1}{p}\right)}{2} \equiv -1 \pmod{4}$. If $p \equiv 5 \pmod{8}$, $p - \left(\frac{-1}{p}\right) = p - 1 \equiv 4 \pmod{8}$, so $1 - \frac{p - \left(\frac{-1}{p}\right)}{2} \equiv -1 \pmod{4}$. Lastly, if $p \equiv 7 \pmod{8}$, $p - \left(\frac{-1}{p}\right) = p + 1 \equiv 0 \pmod{8}$, so $1 - \frac{p - \left(\frac{-1}{p}\right)}{2} \equiv 1 \pmod{4}$. We have computed $\left(\frac{2}{p}\right) \pmod{4}$ in all cases, which tells us $\left(\frac{2}{p}\right)$ as an integer since $1 \not\equiv -1 \pmod{4}$. \square

To prove the main law by this method we will count the number of points on the “mod p unit hypersphere”

$$(5.1) \quad x_1^2 + x_2^2 + \cdots + x_n^2 \equiv 1 \pmod{p}$$

in $(\mathbf{Z}/(p))^n$. (Actually, only odd n and $n = 2$ will be important for us; we used $n = 2$ already to compute $\left(\frac{2}{p}\right)$.) It will be convenient to work with equations in $\mathbf{Z}/(p)$ rather than congruences in \mathbf{Z} , principally because we will be introducing changes of variables that are simpler to describe within $\mathbf{Z}/(p)$. Thus we will view (5.1) as the equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 1$$

directly in $\mathbf{Z}/(p)$.

Definition 5.3. For an odd prime p and $n \geq 1$, let

$$N_{n,p} = |\{(x_1, \dots, x_n) \in (\mathbf{Z}/(p))^n : x_1^2 + \cdots + x_n^2 = 1\}|.$$

Since $x^2 = 1$ has two solutions in $\mathbf{Z}/(p)$, $N_{1,p} = 2$. By Lemma 5.1, $N_{2,p} = p - \left(\frac{-1}{p}\right)$. For $n \geq 3$, we will find a recursion connecting $N_{n,p}$ to $N_{n-2,p}$.

When trying to solve the equation

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + x_n^2 = 1$$

with $x_i \in \mathbf{Z}/(p)$, let x_1, \dots, x_{n-2} be chosen arbitrarily. There are p^{n-2} such choices that can be made. To solve for x_{n-1} and x_n amounts to writing $1 - x_1^2 - \cdots - x_{n-2}^2$ as a sum of two squares, and Lemma 5.1 tells us that the number of ways to write an element of $\mathbf{Z}/(p)$ as a sum of two squares depends only on whether or not the element is 0. Taking into account the formula in Lemma 5.1,

$$\begin{aligned} N_{n,p} &= \sum_{x_1, \dots, x_{n-2} \in \mathbf{Z}/(p)} |\{(x, y) \in (\mathbf{Z}/(p))^2 : x^2 + y^2 = 1 - x_1^2 - \cdots - x_{n-2}^2\}| \\ &= \sum_{x_1^2 + \cdots + x_{n-2}^2 \neq 1} \left(p - \left(\frac{-1}{p}\right)\right) + \sum_{x_1^2 + \cdots + x_{n-2}^2 = 1} \left(p + \left(\frac{-1}{p}\right)(p-1)\right). \end{aligned}$$

The term in both sums contains $p - \left(\frac{-1}{p}\right)$ and the term in the second sum contains an additional $\left(\frac{-1}{p}\right)p$. Thus for all $n \geq 3$,

$$\begin{aligned}
 N_{n,p} &= \sum_{x_1, \dots, x_{n-2}} \left(p - \left(\frac{-1}{p}\right) \right) + \sum_{x_1^2 + \dots + x_{n-2}^2 = 1} \left(\frac{-1}{p}\right) p \\
 &= p^{n-2} \left(p - \left(\frac{-1}{p}\right) \right) + \left(\frac{-1}{p}\right) p N_{n-2,p} \\
 (5.2) \quad &= p^{n-1} + \left(\frac{-1}{p}\right) (p N_{n-2,p} - p^{n-2}).
 \end{aligned}$$

Equation (5.2) is the key formula. It provides a recursion for the sequence $N_{n,p}$ linking any members that are two terms apart. We will focus on $N_{n,p}$ for odd n .

Since $N_{1,p} = 2$, by (5.2) we get

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

and

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

Doing this one more time,

$$\begin{aligned}
 N_{7,p} &= p^6 + \left(\frac{-1}{p}\right) (p N_{5,p} - p^5) \\
 &= p^6 + \left(\frac{-1}{p}\right) (p^5 + p^3 - p^5) \\
 &= p^6 + \left(\frac{-1}{p}\right) p^3.
 \end{aligned}$$

We collect all these formulas for $N_{n,p}$ in Table 3.

n	$N_{n,p}$
1	2
3	$p^2 + \left(\frac{-1}{p}\right)p$
5	$p^4 + p^2$
7	$p^6 + \left(\frac{-1}{p}\right)p^3$

TABLE 3.

Using the data in Table 3, it is not hard to conjecture the next result.

Theorem 5.4. For odd $n \geq 1$,

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

Proof. Use (5.2) and induction (the inductive step goes from n to $n+2$). \square

The reader is invited to use (5.2) to get a formula for $N_{n,p}$ when n is even following the same methods as we used when n is odd. The case of even $n > 2$ will turn out not to be necessary to prove the main law of quadratic reciprocity, so we omit it.

Remark 5.5. There is a geometric interpretation for part of Theorem 5.4. The number $N_{n,p}$ counts the solutions to a single equation in n -dimensional space over $\mathbf{Z}/(p)$ and the dominant term in its formula (for p fixed and n large) is p^{n-1} . A single equation in n variables is one constraint, so intuitively its solution space has “dimension” $n-1$. (Compare with Euclidean space, where the solution set of $x^2 + y^2 + z^2 = 1$ in \mathbf{R}^3 is a sphere, which is a surface and thus locally looks 2-dimensional: $2 = 3 - 1$.) The standard $(n-1)$ -dimensional space $(\mathbf{Z}/(p))^{n-1}$ has size p^{n-1} , and $\pm p^{(n-1)/2}$ in Theorem 5.4 is much smaller than p^{n-1} for large n , so to a *first approximation* the “ $(n-1)$ -dimensional unit hypersphere”

$$x_1^2 + \cdots + x_n^2 = 1$$

in $(\mathbf{Z}/(p))^n$ has about as many points as the standard $(n-1)$ -dimensional space $(\mathbf{Z}/(p))^{n-1}$.

Theorem 5.6. When p and q are distinct odd primes, $\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdots (q-1)/2} \left(\frac{p}{q}\right)$.

Proof. In Theorem 5.4, let $n = q$. That is, we look at

$$N_{q,p} = |\{(x_1, \dots, x_q) \in (\mathbf{Z}/(p))^q : x_1^2 + \cdots + x_q^2 = 1\}|.$$

By Theorem 5.4,

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

This is an exact formula for the number of solutions to $x_1^2 + \cdots + x_q^2 = 1$ in $\mathbf{Z}/(p)$. Reducing the formula for $N_{q,p}$ modulo q , p^{q-1} becomes 1 and $p^{\frac{q-1}{2}}$ becomes $\left(\frac{p}{q}\right)$:

$$(5.3) \quad N_{q,p} \equiv 1 + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

Now we will compute $N_{q,p} \pmod{q}$ by a wholly different method and compare to (5.3). The number $N_{q,p}$ counts solutions over $\mathbf{Z}/(p)$ to the polynomial equation $x_1^2 + \cdots + x_q^2 = 1$ in q variables. The polynomial $x_1^2 + \cdots + x_q^2$ is symmetric in its q variables. Therefore the solution set counted by $N_{q,p}$ is closed under *cyclic shifts*: if (x_1, x_2, \dots, x_q) is a solution, so are (x_2, x_3, \dots, x_1) , (x_3, x_4, \dots, x_2) , and so on. All solutions have q coordinates, and q is *prime*, so either a solution has no cyclic shifts besides itself (all x_i are equal) or it has q cyclic shifts. Therefore solutions where the coordinates are not all equal come in (disjoint) collections of size q . By counting $N_{q,p} \pmod{q}$, only the solutions with all coordinates equal matter in the counting, so

$$N_{q,p} \equiv |\{x \in \mathbf{Z}/(p) : qx^2 = 1\}| \pmod{q}.$$

How many solutions x are there to $qx^2 = 1$ in $\mathbf{Z}/(p)$? If q is a square in $\mathbf{Z}/(p)$ then there are two solutions. If q is a nonsquare then there are no solutions. In both cases, the number of solutions is $1 + \left(\frac{q}{p}\right)$. Comparing this to (5.3), we obtain

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

Subtracting 1 from both sides,

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

Both sides of this congruence are ± 1 , so being congruent modulo $q > 2$ implies they are equal in \mathbf{Z} , and that is the main law of quadratic reciprocity. \square

Remark 5.7. We used $N_{q,p}$ for prime q in the proof of the main law of quadratic reciprocity, but the proof of the formula for $N_{n,p}$ (odd n) in Theorem 5.4 used induction on n and therefore would not have worked if at that earlier point we only let n be prime.

6. PROOF BY ALGEBRAIC NUMBER THEORY

When K is a number field that is Galois over \mathbf{Q} and \mathfrak{p} is a prime ideal in \mathcal{O}_K that is unramified over the prime p below it, there is a unique $\sigma \in \text{Gal}(K/\mathbf{Q})$ such that

$$(6.1) \quad \sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}$$

for all $\alpha \in \mathcal{O}_K$. We call σ the *Frobenius element* associated to \mathfrak{p} and write it as $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})$. This construction is arguably the most important subtle concept in basic algebraic number theory, and studying its behavior on $\mathbf{Q}(\zeta_p)$ and the unique quadratic field inside it turns out to imply quadratic reciprocity.

There are three properties of Frobenius elements that we will use here: their orders, how they change when \mathfrak{p} is replaced by another prime over the same prime number, and their behavior under restriction to Galois subextensions over \mathbf{Q} .

- (1) The order of $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})$ in $\text{Gal}(K/\mathbf{Q})$ is the residue field degree $f(\mathfrak{p}|p)$. In particular, $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})$ is trivial if and only if p splits completely in K (all prime ideals lying over a prime in a Galois extension of \mathbf{Q} have the same residue field degree).
- (2) When \mathfrak{p}' is another prime ideal in \mathcal{O}_K lying over p , $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})$ and $\text{Frob}_{\mathfrak{p}'}(K/\mathbf{Q})$ are conjugate in $\text{Gal}(K/\mathbf{Q})$. In particular, when $\text{Gal}(K/\mathbf{Q})$ is abelian, so conjugacy classes have one element, the Frobenius elements $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})$ are all equal as \mathfrak{p} runs over the prime ideals lying over a common prime p . Therefore when $\text{Gal}(K/\mathbf{Q})$ is abelian it makes sense to speak of a Frobenius element in $\text{Gal}(K/\mathbf{Q})$ associated to each prime number p unramified in K : this is the common value of $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})$ for all \mathfrak{p} lying over p and we write it as $\text{Frob}_p(K/\mathbf{Q})$.
- (3) When $\mathbf{Q} \subset M \subset K$ and M/\mathbf{Q} is Galois, $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})|_M = \text{Frob}_{\mathfrak{p} \cap M}(M/\mathbf{Q})$ by considering (6.1) only when α runs over \mathcal{O}_M . Thus the Frobenius at \mathfrak{p} in $\text{Gal}(K/\mathbf{Q})$ restricts to the Frobenius at $\mathfrak{p} \cap M$ in $\text{Gal}(M/\mathbf{Q})$. When $\text{Gal}(K/\mathbf{Q})$ is abelian, so $\text{Gal}(M/\mathbf{Q})$ is also abelian, this restriction formula can be written as $\text{Frob}_{\mathfrak{p}}(K/\mathbf{Q})|_M = \text{Frob}_p(M/\mathbf{Q})$ when the prime number p is unramified in K .

Here are two important calculations of Frobenius elements in abelian Galois extensions of \mathbf{Q} .

Example 6.1. Let $K = \mathbf{Q}(\sqrt{d})$ where d is a squarefree integer, so $\text{Gal}(K/\mathbf{Q}) \cong \{\pm 1\}$ in one way: all groups of order 2 are uniquely isomorphic to each other. When $p \nmid 2d$, so p is unramified in K , what is $\text{Frob}_p(K/\mathbf{Q})$? It is trivial if and only if p splits completely in K , which is equivalent to saying $x^2 - d \pmod{p}$ splits completely in K (that relies on p being odd to avoid having to pay attention to $d \pmod{4}$). Thus $\text{Frob}_p(K/\mathbf{Q})$ is trivial in $\text{Gal}(K/\mathbf{Q})$ if and only if $\left(\frac{d}{p}\right) = 1$, so $\text{Frob}_p(K/\mathbf{Q})$ is nontrivial in $\text{Gal}(K/\mathbf{Q})$ if and only if $\left(\frac{d}{p}\right) = -1$. Hence the unique isomorphism $\text{Gal}(K/\mathbf{Q}) \rightarrow \{\pm 1\}$ lets us identify $\text{Frob}_p(K/\mathbf{Q})$ with $\left(\frac{d}{p}\right)$. In this way, Frobenius elements in the quadratic field $\mathbf{Q}(\sqrt{d})$ at unramified odd primes can be interpreted as the Legendre symbol $\left(\frac{d}{p}\right)$ where p varies.

Example 6.2. Let $K = \mathbf{Q}(\zeta_m)$, so $\text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/(m))^\times$ by looking at the exponent mod m by which an automorphism in the Galois group affects ζ_m (or equivalently, all the m th roots of unity). When $p \nmid m$, p is unramified in K (because $x^m - 1 \pmod{p}$ is separable) and $\text{Frob}_p(K/\mathbf{Q})$ is the unique $\sigma \in \text{Gal}(K/\mathbf{Q})$ such that (6.1) holds for all $\alpha \in \mathcal{O}_K$ (with \mathfrak{p} in (6.1) being any prime ideal lying over p in K). Let this Frobenius element σ correspond to $a \pmod{m}$ under the isomorphism $\text{Gal}(K/\mathbf{Q}) \rightarrow (\mathbf{Z}/(m))^\times$, meaning $\sigma(\zeta_m) = \zeta_m^a$. Setting $\alpha = \zeta_m$ in (6.1), we get

$$(6.2) \quad \zeta_m^a \equiv \zeta_m^p \pmod{\mathfrak{p}}.$$

In the finite field $\mathcal{O}_K/\mathfrak{p}$, of characteristic p , there are m different m th roots of unity since $p \nmid m$, so (6.2) implies $\zeta_m^a = \zeta_m^p$ in K . Thus $p \equiv a \pmod{m}$, so the isomorphism $\text{Gal}(K/\mathbf{Q}) \rightarrow (\mathbf{Z}/(m))^\times$ identifies $\text{Frob}_p(K/\mathbf{Q})$ with $p \pmod{m}$.

Theorem 6.3. When p and q are distinct odd primes, $\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \left(\frac{p}{q}\right)$ and $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 7 \pmod{8}$.

Proof. The extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is Galois with Galois group $G \cong (\mathbf{Z}/(p))^\times$, so G has order $p-1$ and the squares in G are a subgroup H with index 2. Let M be the subfield of $\mathbf{Q}(\zeta_p)$ fixed by H , so $[M : \mathbf{Q}] = [G : H] = 2$: M is a quadratic field.

$$\begin{array}{ccc} \mathbf{Q}(\zeta_p) & & \{1\} \\ \big| & & \big| \\ M & & H \\ \big| & & \big| \\ 2 & & 2 \\ \mathbf{Q} & & G \end{array}$$

We can determine M by ramification. The only prime ramifying in $\mathbf{Q}(\zeta_p)$ is p and some prime ramifies in M , so it must be p . Thus $M = \mathbf{Q}(\sqrt{\pm p})$ where the sign is chosen so that $\pm p \equiv 1 \pmod{4}$ (otherwise 2 would also ramify in M). When $p \equiv 1 \pmod{4}$ that sign has to be 1, and when $p \equiv 3 \pmod{4}$ it has to be -1 . Thus the sign is $\left(\frac{-1}{p}\right)$, so $M = \mathbf{Q}(\sqrt{p^*})$, where

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

When a prime $q \neq p$ splits in M will now be described two ways, and comparing the two descriptions will lead to quadratic reciprocity.

Since $p^* \equiv 1 \pmod{4}$ we have $\mathcal{O}_M = \mathbf{Z}[(1 + \sqrt{p^*})/2]$, so $[\mathcal{O}_M : \mathbf{Z}[\sqrt{p^*}]] = 2$. Thus when q is odd, it splits in M if and only if $x^2 - p^* \pmod{q}$ splits, meaning $\left(\frac{p^*}{q}\right) = 1$. Also q splits in M if and only if $\text{Frob}_q(M/\mathbf{Q})$ is trivial, and $\text{Frob}_q(M/\mathbf{Q}) = \text{Frob}_q(\mathbf{Q}(\zeta_p)/\mathbf{Q})|_M$, so q splits in M if and only if $\text{Frob}_q(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is in the kernel of the restriction map $G \rightarrow \text{Gal}(M/\mathbf{Q})$, which is H and those are the squares in G . The standard isomorphism $G \rightarrow (\mathbf{Z}/(p))^\times$ maps $\text{Frob}_q(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ to $q \pmod{p}$, so $\text{Frob}_q(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is a square in G if and only if $\left(\frac{q}{p}\right) = 1$. Thus $\left(\frac{p^*}{q}\right) = 1$ if and only if $\left(\frac{q}{p}\right) = 1$. Legendre symbols have two nonzero values, so $\left(\frac{p^*}{q}\right) = -1$ if and only if $\left(\frac{q}{p}\right) = -1$. Hence $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ in all cases. Since $p^* = \left(\frac{-1}{p}\right)p = (-1)^{(p-1)/2}p$,

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

The Frobenius element reasoning on odd primes also works at 2, so 2 splits in M if and only if $\left(\frac{2}{p}\right) = 1$ (each condition is equivalent to $\text{Frob}_2(M/\mathbf{Q})$ being trivial). Since $\mathcal{O}_M = \mathbf{Z}[(1 + \sqrt{p^*})/2]$ and $(1 + \sqrt{p^*})/2$ has minimal polynomial $x^2 - x + (1 - p^*)/4$ in $\mathbf{Z}[x]$, 2 splits in M if and only if $x^2 - x + (1 - p^*)/4 \pmod{2}$ splits. That happens if $p^* \equiv 1 \pmod{8}$ and not if $p^* \equiv 5 \pmod{8}$ (these are the only options for $p^* \pmod{8}$ since $p^* \equiv 1 \pmod{4}$). Check $p^* \equiv 1 \pmod{8}$ if $p \equiv \pm 1 \pmod{8}$ and not if $p \equiv \pm 3 \pmod{8}$, so 2 splits in M if and only if $p \equiv \pm 1 \pmod{8}$. Thus $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$. \square

APPENDIX A. LEGENDRE'S ATTEMPT TO PROVE QUADRATIC RECIPROCITY

In order to prove the main law of quadratic reciprocity

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

where p and q are distinct odd primes, Legendre considered 8 cases depending on $p \pmod{4}$, $q \pmod{4}$, and $\left(\frac{p}{q}\right)$. See Table 4.³ In each case, the main law predicts $\left(\frac{q}{p}\right)$ from the other information. Proving the main law amounts to verifying that the last column of the table is correct. Our treatment is based on [3, pp. 73–74], [7, pp.6–8], [8, pp. 326–330], and [9].

Case	$p \pmod{4}$	$q \pmod{4}$	$\left(\frac{p}{q}\right)$	$\left(\frac{q}{p}\right)$
1	1	1	1	1?
2	1	1	-1	-1?
3	1	3	1	1?
4	1	3	-1	-1?
5	3	1	1	1?
6	3	1	-1	-1?
7	3	3	1	-1?
8	3	3	-1	1?

TABLE 4.

We will show how Legendre proved some cases completely and other cases by assuming the existence of a prime satisfying conditions depending on p and q . An interesting aspect of Legendre's work is that it led to the conjecture that there are primes in arithmetic

³Legendre labeled these cases differently. Our ordering corresponds to his theorems 3, 4, 5, 2, 1, 6, 7, and 8, respectively.

progressions $a \pmod m$ when $(a, m) = 1$, which was proved about 50 years later by Dirichlet, for odd prime m in 1837 [1] and for general m in 1839 [2].

Legendre's attempt to prove quadratic reciprocity was based on the following important theorem that he had proved in 1785.

Theorem A.1 (Legendre). *If a , b , and c are nonzero integers that are pairwise relatively prime and squarefree, then the equation*

$$ax^2 + by^2 + cz^2 = 0$$

has an integral solution (x, y, z) besides $(0, 0, 0)$ if and only if the following two conditions hold:

- (1) a , b , and c are not all of the same sign,
- (2) $-ab \equiv \square \pmod{|c|}$, $-ac \equiv \square \pmod{|b|}$, and $-bc \equiv \square \pmod{|a|}$.

Proof. See [4, §3, Chap. 17]. □

What Legendre actually relied on was the following corollary to his theorem.

Corollary A.2. *If a , b , and c are nonzero integers that are pairwise relatively prime, squarefree, not all of the same sign, and are all $1 \pmod 4$, then either $-ab \not\equiv \square \pmod{|c|}$ or $-ac \not\equiv \square \pmod{|b|}$ or $-bc \not\equiv \square \pmod{|a|}$.*

Proof. Using $a, b, c \equiv 1 \pmod 4$ we will show $ax^2 + by^2 + cz^2 = 0$ has no integral solution (x, y, z) other than $(0, 0, 0)$, and then find out consequences of that from Theorem A.1.

If $ax^2 + by^2 + cz^2 = 0$ has an integral solution besides $(0, 0, 0)$, then divide through the equation by the highest power of 2 that goes into x , y , and z in order to assume that x or y or z is odd. Then when we reduce the equation $\pmod 4$ it becomes $x^2 + y^2 + z^2 \equiv 0 \pmod 4$, which is impossible unless x , y , and z are *all* even, and they are not.

Since a , b , and c fit the hypotheses of Theorem A.1 and they are not all of the same sign, the only way $ax^2 + by^2 + cz^2 = 0$ could have no integral solution besides $(0, 0, 0)$ is if $-ab \not\equiv \square \pmod c$ or $-ac \not\equiv \square \pmod b$ or $-bc \equiv \square \pmod a$. □

Among the 8 cases for quadratic reciprocity in Table 4, several are contrapositive pairs: 1 and 2, 3 and 6, and 4 and 5. So it suffices to focus on 1, 3, 4, 7, and 8. Legendre settled Cases 4 (thus also 5) and 7 unconditionally using Corollary A.2. To prove the remaining cases, he used Corollary A.2 and a choice of an auxiliary prime ℓ satisfying a condition $\pmod 4$ and two Legendre symbol conditions depending on p and q . The existence of that prime ℓ was not proved, which makes his proofs of Cases 1, 3, and 8 incomplete.

Cases 4 and 7: See Table 5. The choices of a , b , and c there satisfy $-ab \equiv \square \pmod{|c|}$ and $-ac \equiv \square \pmod{|b|}$ since $(\frac{-1}{q}) = -1$ and $|b| = 1$, so Corollary A.2 implies $-bc \not\equiv \square \pmod{|a|}$, which in Cases 4 and 7 translates into $q \not\equiv \square \pmod p$, so $(\frac{q}{p}) = -1$ in Cases 4 and 7.

Case	$p \pmod 4$	$q \pmod 4$	$(\frac{p}{q})$	a	b	c
4	1	3	-1	p	1	$-q$
7	3	3	1	$-p$	1	$-q$

TABLE 5.

To settle Cases 1, 3, and 8, Legendre used an auxiliary prime ℓ as described in Table 6. An asterisk in a column means there is no assumption about ℓ for that column and the

Legendre symbol in that column will be deduced from other columns. We place Case 8 first in the table because the role of an auxiliary prime there appears simpler than its role in Cases 1 and 3, as we will see below.

Case	$p \bmod 4$	$q \bmod 4$	$\left(\frac{p}{q}\right)$	$\ell \bmod 4$	$\left(\frac{\ell}{p}\right)$	$\left(\frac{p}{\ell}\right)$	$\left(\frac{\ell}{q}\right)$	a	b	c
8	3	3	-1	1	-1	*	-1	$-p$	ℓ	$-q$
1	1	1	1	3	*	-1	1	p	q	$-\ell$
3	1	3	1	1	-1	*	-1	p	$-q$	ℓ

TABLE 6.

Case 8: Assume there is a prime ℓ as in the first row of Table 6. From $\left(\frac{\ell}{p}\right) = -1$ we get $\left(\frac{p}{\ell}\right) = -1$ by Case 4 proved above. From $\left(\frac{\ell}{q}\right) = -1$ we get $\left(\frac{q}{\ell}\right) = -1$ by Case 4 above. Then $-ab = p\ell \equiv \square \pmod{q}$ and $-ac = -p\ell \equiv \square \pmod{\ell}$ (since $\ell \equiv 1 \pmod{4}$). By Corollary A.2 $-bc \not\equiv \square \pmod{|a|}$, which says $\left(\frac{q\ell}{p}\right) = -1$, and that implies $\left(\frac{q}{p}\right) = 1$.

Case 1: Assume there is a prime ℓ as in the second row of Table 6. From $\left(\frac{p}{\ell}\right) = -1$ we get $\left(\frac{\ell}{p}\right) = -1$ by Case 4 above, and from $\left(\frac{\ell}{q}\right) = 1$ we get $\left(\frac{q}{\ell}\right) = 1$ by Case 5, which is equivalent to Case 4. This implies $-ab = -p\ell \equiv \square \pmod{\ell}$ (since $\ell \equiv 3 \pmod{4}$) and $-ac = p\ell \equiv \square \pmod{q}$. By Corollary A.2 $-bc \not\equiv \square \pmod{|a|}$, which says $\left(\frac{q\ell}{p}\right) = -1$. Thus $\left(\frac{q}{p}\right) = 1$.

Case 3: Assume there is a prime ℓ as in the third row of Table 6. From $\left(\frac{\ell}{p}\right) = -1$ we get $\left(\frac{p}{\ell}\right) = -1$ by Case 2, which is equivalent to Case 1 above. From $\left(\frac{\ell}{q}\right) = -1$ we get $\left(\frac{q}{\ell}\right) = -1$ by Case 4 above. Then $-ab = p\ell \equiv \square \pmod{\ell}$ and $-ac = -p\ell \equiv \square \pmod{q}$ (since $q \equiv 3 \pmod{4}$). By Corollary A.2 $-bc \not\equiv \square \pmod{|a|}$, which says $\left(\frac{q\ell}{p}\right) = -1$, and that implies $\left(\frac{q}{p}\right) = 1$.

Let's analyze what we needed to know about auxiliary primes in Cases 1, 3, and 8.

In the proof of Case 8, the auxiliary prime ℓ satisfies conditions on $\ell \bmod 4$, $\left(\frac{\ell}{p}\right)$, and $\left(\frac{\ell}{q}\right)$, which are equivalent to conditions on $\ell \bmod 4pq$ by the Chinese remainder theorem. Wanting the existence of such ℓ is why Legendre assumed the existence of primes in suitable arithmetic progressions.

The auxiliary prime ℓ in Case 1 is determined by $\ell \bmod 4$, $\left(\frac{p}{\ell}\right)$, and $\left(\frac{\ell}{q}\right)$; that ℓ satisfies a value for $\left(\frac{p}{\ell}\right)$ looks more subtle than satisfying a value for $\left(\frac{\ell}{q}\right)$. We can bypass the assumption $\left(\frac{\ell}{q}\right) = -1$ in Case 1 by changing a , b , and c there: if $\ell \equiv 3 \pmod{4}$ and $\left(\frac{p}{\ell}\right) = -1$, set $(a, b, c) = (p, 1, -q\ell)$. Then $-ab = -p \equiv \square \pmod{|c|}$ since $-p \equiv \square \pmod{q}$ and $-p \equiv \square \pmod{\ell}$. We have $-ac \equiv \square \pmod{|b|}$ since $|b| = 1$. Therefore Corollary A.2 implies $-bc \not\equiv \square \pmod{|a|}$, so $\left(\frac{q\ell}{p}\right) = -1$. By Case 4 from $\left(\frac{p}{\ell}\right) = -1$ we get $\left(\frac{\ell}{p}\right) = -1$, so $\left(\frac{q\ell}{p}\right) = -1 \Rightarrow \left(\frac{q}{p}\right) = 1$, which is the goal in Case 1. So to settle Case 1 we only need a prime $\ell \equiv 3 \pmod{4}$ satisfying $\left(\frac{p}{\ell}\right) = -1$. The existence of such ℓ was demonstrated by Gauss in his first proof of quadratic reciprocity, and his argument is not as complicated as proving Dirichlet's theorem. So despite initial appearances, the existence of an auxiliary prime needed in Case 1 is actually simpler than the existence of the auxiliary prime in Case 8. Anyway, Legendre never proved the existence of any auxiliary primes that he needed.

In the proof of Case 3, the auxiliary prime ℓ satisfies conditions on $\ell \bmod 4$, $\left(\frac{\ell}{p}\right)$, and $\left(\frac{\ell}{q}\right)$ like in Case 8, but the proof of Case 3 also relies on Case 1 with primes p and ℓ , so settling Case 3 needs a second auxiliary prime r such that $r \equiv 3 \pmod{4}$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{r}{\ell}\right) = 1$.

Exercises.

1. Show $35 \equiv \square \pmod{73}$ in two ways: check $35^{(73-1)/2} \equiv 1 \pmod{73}$ and compute $\left(\frac{35}{73}\right)$ using quadratic reciprocity.
2. The number 1777 is prime. Use quadratic reciprocity to determine whether 71, 533, 929, 1083, and 1566 are squares modulo 1777. Make sure to factor the number into primes first. (Answer: all are squares except 533 and 1566.)
3. By the main law of quadratic reciprocity,

$$\left(\frac{229}{5999}\right) = \left(\frac{5999}{229}\right) = \left(\frac{45}{229}\right) = \left(\frac{5}{229}\right) = \left(\frac{229}{5}\right) = \left(\frac{4}{5}\right) = 1$$

since $229 \equiv 1 \pmod{4}$ and $5999 \equiv 45 \pmod{229}$. However, 229 actually is *not* a square mod 5999. Where was the mistake? And what is $229^{(5999-1)/2} \pmod{5999}$?

4. Use (5.2) to get a formula for $N_{n,p}$ when n is even.

REFERENCES

- [1] P. G. L. Dirichlet, “Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendliche viele Primzahlen enthält,” Abh. Kgl. Preuss. Akad. Wiss. Berlin (1837), 45–71. URL <https://www.biodiversitylibrary.org/item/93754#page/307/mode/1up>. English translation at <https://arxiv.org/abs/0808.1408>.
- [2] P. G. L. Dirichlet, “Recherches sur diverses applications de l’analyse infinitésimale à la théorie des nombres. Première partie,” J. Reine Angew. Math. **19** (1839), 324–369. URL <https://eudml.org/doc/147076>.
- [3] G. Frei, “The reciprocity law from Euler to Eisenstein,” pp. 67–90 in: *The Intersection of History and Mathematics* (C. Sasaki, M. Sugiura, J. W. Dauben eds.), Birkhauser, Basel, 1994.
- [4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.
- [5] V. A. Lebesgue, “Recherches sur les nombres (Part 2),” Journal de Mathématique Pures et Appliquées. **3** (1838), 113–144. URL <https://eudml.org/doc/235192>.
- [6] A. M. Legendre, *Essai sur la Théorie des Nombres*, Duprat, Paris, 1798. URL <https://archive.org/details/essaisurlathor00lege/page/n5 /mode/2up>
- [7] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer-Verlag, New York, 2000.
- [8] A. Weil, *Number Theory: An Approach through History from Hammurapi to Legendre*, Birkhauser, Boston, 1984.
- [9] S. Weintraub, “On Legendre’s Work on the Law of Quadratic Reciprocity,” Amer. Math. Monthly **118** (2011), 210–216.