RECIPROCITY LAWS

JEREMY BOOHER

1. Introduction

The law of quadratic reciprocity gives a beautiful description of which primes are squares modulo p. Special cases of this law going back to Fermat, and Euler and Legendre conjectured it, but the first complete proof is due to Gauss, who in fact gave eight proofs. It states that if p and q are distinct odd primes, and at least one of them is congruent to 1 modulo 4, then p is a square modulo q if and only if q is a square modulo p. If both are 3 modulo 4, p is a square modulo q if and only if q is not a square modulo p. This is more clearly stated using the Legendre symbol.

Definition 1. Let p be a prime and a be an integer relatively prime to p. Then $\left(\frac{a}{p}\right)$ is defined to be 1 if $x^2 \equiv a \mod p$ has a solution, -1 otherwise.

By convention, if a is a multiple of p the Legendre symbol is defined to be zero. With this notation, the law can be compactly stated as follows.

Theorem 2 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

Two proofs relying on the same idea are given in Section 2: they are one of the proofs due to Gauss and a modern reformulation in terms of the language of algebraic number theory.

The search for generalizations of quadratic reciprocity was a major goal in the development of algebraic number theory. Versions for third and fourth powers were investigated by Gauss and Jacobi, and proven by Eisenstein. Some of these generalizations are discussed in Section 3. A generalization and unification of many such laws took place in the early twentieth century with the development of class field theory. Section 4 briefly outlines how class field theory connects with the law of quadratic reciprocity.

A great deal of information about the development of reciprocity laws and many unusual proofs are to be found in Lemmermeyer [3].

1.1. Preliminary Facts.

The law of quadratic reciprocity can be reformulated in terms of $p^* := (-1)^{\frac{p-1}{2}}p$, which has the property that $p^* \equiv 1 \mod 4$. This form matches the proofs we will give.

Theorem 3 (Quadratic Reciprocity')**.** *Let p and q be odd primes, and $p^* = (-1)^{\frac{p-1}{2}}p$. Then $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$.*

The equivalence relies on some standard properties of the Legendre symbol.

Proposition 4. *Let p be a prime and $a \in \mathbb{Z}$.*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ *(this is known as Euler's criterion).*
2. *The Legendre symbol is a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$.*
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Date: January 14, 2013.

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

The last two statements are known as the supplemental laws, since they deal with exceptional cases not covered by the statement of quadratic reciprocity. These easy statements, as well as the equivalence of the two statements of quadratic reciprocity, are proven in most elementary number theory books, for example Ireland and Rosen [2, Chapter 5].

2. Gauss's Proof and Algebraic Number Theory

After introducing the splitting of primes and the Frobenius element in basic algebraic number theory, a simple proof of the quadratic reciprocity law becomes possible. Although the full language of algebraic number theory did not develop until the end of the 19th century, this proof is essentially due to Gauss. After presenting the modern proof, we explain how Gauss would have proven it using Gauss sums to bypass non-existent language and techniques.

2.1. **Proof Using Galois Theory and Algebraic Number Theory.**

To prove the main case of quadratic reciprocity, Theorem 3, we will look at the splitting of primes in the unique quadratic subfield of a cyclotomic field. Let p and q be odd primes, and let p^* be $(-1)^{\frac{p-1}{2}}p$ as before. Consider the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity.

Proposition 5. *There is a unique quadratic subfield $K = \mathbb{Q}(\sqrt{p^*})$ of $\mathbb{Q}(\zeta_p)$.*

Proof. We know that $\mathbb{Q}(\zeta_p)$ is a Galois extension of $\mathbb{Q}$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$. As $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic, there is a unique index two subgroup, which consists of the quadratic residues modulo p. By the fundamental theorem of Galois theory there is a unique quadratic field K contained in $\mathbb{Q}(\zeta_p)$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$ is the subgroup of quadratic residues. Furthermore, the discriminant of $\mathbb{Q}(\zeta_p)$ is a power of p, so the only prime that ramifies in K is p. But the only quadratic field ramified only at p is $\mathbb{Q}(\sqrt{p^*})$.[1] □

Now we wish to understand how the rational prime q splits in the ring of integers of K. There are two ways to do this: directly using an understanding of quadratic fields, and indirectly using the Frobenius of q.

Proposition 6. *The following are equivalent:*

(1) *The prime q splits in $\mathcal{O}_K$.*
(2) *The polynomial $x^2 - x + \frac{1-p^*}{4}$ factors modulo q, i.e. $\left(\frac{p^*}{q}\right) = 1$.*
(3) *The element $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ fixes K.*

Proof. Standard algebraic number theory gives that (1) is equivalent to (2). Because $p^* \equiv 1 \mod 4$, the ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\frac{1+\sqrt{p^*}}{2}]$, so q splits if and only if the minimal polynomial of $x^2 - x - \frac{1-p^*}{4}$ factors modulo q. But this factors over $\mathbb{F}_q$ if and only if the roots lie in $\mathbb{F}_q$, in other words $\left(\frac{p^*}{q}\right) = 1$. Therefore the first two conditions are equivalent.

An argument using the Frobenius element shows that (1) and (3) are equivalent. Recall that the Frobenius element $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a lift of the Frobenius automorphism of the residue field. More precisely, let $\mathfrak{q}$ be a prime above q in $\mathbb{Z}[\zeta_p]$, the ring of integers of $\mathbb{Q}(\zeta_p)$, and let k' be the residue field $\mathbb{Z}[\zeta_p]/\mathfrak{q}$, a finite extension of $k = \mathbb{F}_q$. Then Frob_q is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ that reduces to the qth power map in $\mathrm{Gal}(k'/k)$. It is unique because the extension is Abelian and unramified at q. Likewise, we can define a Frobenius Frob'_q for K over $\mathbb{Q}$. Looking at the reduction on residue fields, it is clear that $\mathrm{Frob}_q|_K = \mathrm{Frob}'_q$. Now the order of a Frobenius is the degree of the residue field extension, so q splits completely in $\mathcal{O}_K$ if and only if Frob'_q is the identity. This happens if and only if Frob_q fixes K. □

[1] The field $\mathbb{Q}(\sqrt{-p^*})$ is also ramified at 2

The final step is to obtain a criterion for when Frob_q fixes K using Galois theory.

Proposition 7. *The Frobenius element* Frob_q *fixes* K *if and only if* $\left(\frac{q}{p}\right) = 1$.

Proof. Recall the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ identifies $a \in (\mathbb{Z}/p\mathbb{Z})^\times)$ with the automorphism σ_a over $\mathbb{Q}$ sending ζ_p to ζ_p^a. Now the residue extension k'/k is generated by adjoining pth roots of unity to k, so σ_q reduces to the Frobenius automorphism of the residue fields. Since in this case the Frobenius is unique, we see that $\mathrm{Frob}_q = \sigma_q$. Then Frob_q fixes K if and only if $q \in (\mathbb{Z}/p\mathbb{Z})^\times$ lies in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$, which by construction is the subgroup of quadratic residues modulo p. □

Combining Propositions 6 and 7 gives that $\left(\frac{p^*}{q}\right) = 1$ if and only if $\left(\frac{q}{p}\right) = 1$, so

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

This completes the proof of the law of quadratic reciprocity in the guise of Theorem 3.

2.2. **Proof Using Gauss Sums.** The main idea in the alternative formulation is that Gauss sums allow us to construct K and identify the splitting of q concretely. We first recall their definition and basic properties, then rephrase the above proof in Gauss's language.

Let n be a positive integer and χ be a group homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. Since all irreducible representations of $(\mathbb{Z}/n\mathbb{Z})^\times$ are one dimensional, χ is often simply called a character. It can be extended to a map $\mathbb{Z} \to \mathbb{C}$ by periodicity and setting it to be 0 on integers not relatively prime to n. Fix a primitive nth root of unity ζ_n.

Definition 8. The Gauss sum $g(\chi)$ is defined to be

$$g(\chi) = \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(x)\zeta_n^x.$$

Remark 9. The function $x \mapsto \zeta_n^x$ is an additive character of $\mathbb{Z}/n\mathbb{Z}$. In general, a Gauss sum is a combination of a multiplicative character with an additive character. A fruitful analogy is the group $\mathbb{R}^+$ and the Gamma function.

If p is an odd prime, let χ_p denote the quadratic character, so $\chi_p(a) = \left(\frac{a}{p}\right)$. We are mainly interested in $g(\chi_p)$, and would like to reduce it modulo q. This is a complex number so a priori this makes no sense. However, the Gauss sum can be interpreted as an algebraic integer or an element of a finite field as follows. Since χ_p takes on only the values ±1, $g(\chi_p)$ lies in $\mathbb{Z}[\zeta_p]$, the ring of integers of $\mathbb{Q}(\zeta_p)$. It is therefore possible to reduce this modulo q. Alternately, we can interpret the definition as an element in the finite extension of $\mathbb{F}_q$ obtained by adjoining pth roots unity.

We can use Gauss sums to recover the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ by calculating the size of $g(\chi_p)$. Then the algebraic number theory in the proof can be replaced by concrete calculations with the Gauss sum. The following proposition is analogous to Proposition 5.

Proposition 10. *For* p *a prime,* $g(\chi_p)^2 = p^*$. *Thus* $\mathbb{Q}(g(\chi_p))$ *is a quadratic subfield of* $\mathbb{Q}(\zeta_p)$.

Proof. To prove this, we will use a "twisted" Gauss sum

$$g_a(\chi_p) = \sum_{x \in \mathbb{F}_p} \chi_p(x)\zeta_p^{ax}.$$

Note that $g_0(\chi_p) = 0$ since half the elements of $\mathbb{F}_p$ are quadratic non-residues and half are quadratic residues. We will calculate

$$S = \sum_{a \in \mathbb{F}_p^\times} g_a(\chi_p)^2 = \sum_{a \in \mathbb{F}_p} g_a(\chi_p)^2$$

in two different ways. On one hand, as multiplying by $a \neq 0$ is a permutation of $\mathbb{F}_p^\times$ so

$$g_a(\chi_p) = \chi_p(a)^{-1} \sum_{ax \in \mathbb{F}_p} \chi_p(ax)\zeta_p^{ax} = \chi_p(a)^{-1} g(\chi_p).$$

Thus we can evaluate S as

$$S = \sum_{a \in \mathbb{F}_p} g_a(\chi_p)^2 = \sum_{a \in \mathbb{F}_p^\times} \chi_p(a)^{-2} g(\chi_p)^2 = g(\chi_p)^2 \sum_{a \in \mathbb{F}_p^\times} 1 = (p-1)g(\chi)^2.$$

On the other hand,

$$\begin{aligned} S &= \sum_{a \in \mathbb{F}_p} \sum_{x,y \in \mathbb{F}_p} \chi_p(x)\chi_p(y)\zeta_p^{a(x+y)} \\ &= \sum_{x,y \in \mathbb{F}_p} \chi_p(x)\chi_p(y) \sum_{a \in \mathbb{F}_p} \zeta_p^{a(x+y)}. \end{aligned}$$

When $x + y \neq 0$, the inner sum is a sum over all pth roots of unity, so equals 0. Otherwise it is the sum of p ones, and $\chi_p(x)\chi_p(-x) = (-1)^{\frac{p-1}{2}}$. Therefore we obtain

$$S = \sum_{x \in \mathbb{F}_p^\times} (-1)^{\frac{p-1}{2}} p = (p-1)p^*.$$

Equating the two expressions for S gives $g(\chi)^2 = p^*$. □

Remark 11. The problem of determining the sign of $g(\chi_p)$ is more delicate - see for example Ireland and Rosen [2, 6.4]. It is related to the functional equation for Dirichlet L-functions.

Let us try to use this alternative description of this quadratic subfield to determine when a prime q is split without using this language. We have the following, analogous to Proposition 6.

Proposition 12. *Let q be an odd prime not equal to p. Then $\left(\frac{p^*}{q}\right) = 1$ if and only if $g(\chi_p)^q \equiv g(\chi_p)$ mod q.*

Proof. Recall that Euler's criterion says that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. So using Proposition 10,

$$g(\chi_p)^{q-1} \equiv (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \mod q$$

Multiplying by $g(\chi_p)$, we see the equivalence. □

Of course, the condition that $g(\chi_p)^q = g(\chi_p) \mod q$ is exactly the condition, suitably interpreted, that Frob_q fixes the quadratic subfield $\mathbb{Q}(g(\chi_p))$.

Finally, we obtain an analogue of Proposition 7 by a direct calculation.

Proposition 13. *Let q be an odd prime not equal to p. Then $g(\chi_p)^q = \left(\frac{q}{p}\right) g(\chi_p) \mod q$.*

Proof. Recall that $(a+b)^q \equiv a^q + b^q \mod q$, so

$$\begin{aligned} g(\chi_p)^q &\equiv \left(\sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^a \right)^q \mod q \\ &\equiv \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)^q \zeta_p^{aq} \mod q \\ &\equiv \left(\frac{q}{p}\right)^{-1} \sum_{a \in \mathbb{F}_p^\times} \left(\frac{aq}{p}\right) \zeta_p^{aq} \mod q \end{aligned}$$

where the last step uses that $\left(\frac{a}{p}\right)$ is ±1, so raising it to an odd power does not change it. But the last sum is just $g(\chi_p)$ since multiplying by q is a permutation of $\mathbb{F}_p^\times$. Therefore

$$g(\chi_p)^q \equiv \left(\frac{q}{p}\right) g(\chi_p) \mod q. \qquad \square$$

Combining the last two propositions, we see that $\left(\frac{p^*}{q}\right) = 1$ if and only if $\left(\frac{q}{p}\right) = 1$, again yielding quadratic reciprocity.

3. Generalizations of Quadratic Reciprocity

There are two obvious directions to generalize quadratic reciprocity: ask the same questions about nth powers instead of squares, and ask the question about the residue fields of number fields other than $\mathbb{Q}$. To get nice answers, one needs the nth roots of unity to lie in the number field.

3.1. Cubic Reciprocity.

The simplest example of this is the law of cubic reciprocity, which addresses the question of third powers in $\mathbb{Q}(\zeta_3)$. The first step is to define a cubic residue symbol using the idea behind Euler's criterion.

Definition 14. For $\alpha \in \mathbb{Z}[\zeta_3]$ and π a prime of $\mathbb{Z}[\zeta_3]$, define the cubic residue character $\left(\frac{\alpha}{\pi}\right)_3$ to be the unique root of unity congruent to $\alpha^{(N\pi-1)/3}$ modulo π. If $\pi|3$, define $\left(\frac{\alpha}{\pi}\right) = 0$.

Just as we needed to use p^* instead of p to obtain a nice formulation of quadratic reciprocity, we need a way to distinguish one of the six associates of a prime in $\mathbb{Z}[\zeta_3]$.

Definition 15. If π is a prime in $\mathbb{Z}[\zeta_3]$, then π is primary if $\pi \equiv 2 \mod 3$.

The main law of cubic reciprocity is now easy to state.

Theorem 16 (Cubic Reciprocity)**.** *Let π_1 and π_2 be distinct primary primes (not above 3). Then*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

There are also supplemental laws for the prime above 3 and the units.

The first proof, first published by Eisenstein in 1844, uses the same techniques appearing in the previous proofs of quadratic reciprocity. The necessary result about Gauss sums is the following analogue of Proposition 10.

Proposition 17. *Let π be a primary prime and χ_π be the cubic residue character. Then $g(\chi_\pi)^3 = \pi^2\overline{\pi}$.*

The elementary proof of this uses Jacobi sums, which for characters χ_1 and χ_2 is $J(\chi_1, \chi_2) := \sum_{x\in\mathbb{F}_p} \chi_1(x)\chi_2(1-x)$. A complete proof is contained in Ireland and Rosen [2, Chapter 8 and 9].

The proof of cubic reciprocity proceeds in cases, depending on whether π_1 and π_2 are inert or split primes. For example, suppose $\pi_1 = q$ is inert and π_2 split, with norm p. Then the proposition combined with the definition of the cubic residue character tells us that

$$g(\chi_{\pi_2})^{q^2-1} \equiv \chi_q(p\pi_2) \mod q$$

Evaluating $g(\chi_{\pi_2})^{q^2}$ directly using the binomial theorem and then comparing gives one case of cubic reciprocity. The other cases are similar.

3.2. **Eisenstein Reciprocity.** The Eisenstein Reciprocity Law generalizes quadratic and cubic reciprocity to deal with pth powers in the cyclotomic field $\mathbb{Q}(\zeta_p)$.[2] Two of the difficulties are the failure of unique factorization, necessitating the use of ideals, and the more complicated splitting of the Gauss sums.

The power residue symbol is a generalization of the quadratic and cubic character. Let p be a prime, and $\mathfrak{q}$ a prime ideal in $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ above q. Suppose that $\mathfrak{q}$ is relatively prime to p.

Definition 18. Let $\alpha \in \mathbb{Z}[\zeta_p]$ and $\mathfrak{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ not containing p. The pth power residue symbol, $\left(\frac{\alpha}{\mathfrak{q}}\right)_p$ is defined, if $\alpha \notin \mathfrak{q}$, to be the unique pth root of unity such that $\alpha^{(N\mathfrak{q}-1)/p} \equiv \left(\frac{\alpha}{\mathfrak{q}}\right)_p$ mod $\mathfrak{q}$. If $\alpha \in \mathfrak{q}$, define the residue symbol to be 0.

Like the Legendre symbol and cubic residue character, the power residue symbol is obviously multiplicative and depends on α only modulo $\mathfrak{q}$.

As in the case for cubic reciprocity, we need to deal with the ambiguity introduced by units.

Definition 19. A nonzero element $\alpha \in \mathbb{Z}[\zeta_p]$ is called primary if it is not a unit, is prime to p, and is congruent to a rational integer modulo $(1-\zeta_p)^2$.

We can now state the pth power reciprocity law.

Theorem 20 (Eisenstein Reciprocity). *Let p be an odd prime, $a \in \mathbb{Z}$ prime to p, and $\alpha \in \mathbb{Z}[\zeta_p]$ a primary element. Suppose furthermore α and a are coprime. Then*

$$\left(\frac{\alpha}{a}\right)_p = \left(\frac{a}{\alpha}\right)_p .$$

The proof of this theorem is found in Ireland and Rosen [2, Chapter 14]. A major ingredient is the the Stickelberger Relation, which gives the non-obvious factorization for Gauss sums in $\mathbb{Q}(\zeta_p)$: it is a generalization of Proposition 10 and 17.

4. Class Field Theory and Reciprocity Laws

All of the above reciprocity laws can be proven using class field theory, in particular the existence of the Artin map identifying the Galois group of an Abelian extension of number fields with a quotient of the idele class group.[3] There are several ways to proceed (outlined in Exercises 1 and 2 of Cassels and Frölich [1]): we will use Hilbert symbols and the Hilbert reciprocity law.

Let n a positive integer, K be a number field containing the nth roots of unity, and v a place of K. Let $a, b \in K^\times$. One can define the norm residue symbol $(a,b)_v$ using the local Artin map ψ_v for the extension $K(\sqrt[n]{a})/K$ via the formula

$$(\sqrt[n]{a})^{\psi_v(b)} = (a,b)_v \sqrt[n]{a}.$$

This turns out to be a bilinear map $K^\times \times K^\times \to \mu_n$ that can be studied using class field theory. One important property is the product formula.

Theorem 21. *Let $a, b \in K^\times$. Then $\prod_v (a,b)_v = 1$, where the product ranges over all places of K.*

Given class field theory, this is not too difficult to prove.

In the case that $n = 2$, the norm residue symbol has a much more explicit description, and is known as the Hilbert symbol.

[2] Additional special cases were proven first, most notably biquadratic reciprocity which deals with fourth powers in $\mathbb{Z}[i]$.

[3] This is often called the Artin reciprocity law, not because it looks like other reciprocity laws but because special cases give many of the reciprocity laws.

Lemma 22. *The norm residue symbol $(a,b)_v$ is 1 if and only if the equation $z^2 - ax^2 - by^2 = 0$ has a non-trivial solution in $\mathcal{O}_{K_v}$.*

The proof of this lemma requires local class field theory. Note that the equation having a non-trivial solution is equivalent to saying that a is a norm from the extension $K(\sqrt{b})/K$.

In this special case, the product formula is known as the Hilbert reciprocity law. When $K = \mathbb{Q}$, it is equivalent to the law of quadratic reciprocity. We will show how to deduce quadratic reciprocity from it by performing local calculations for the Hilbert symbols.

Let p and q be distinct odd primes, and $p^* = (-1)^{\frac{p-1}{2}}p$ as before. We first consider the case when v is a finite place of $\mathbb{Q}$ that is not equal to p or q.

Proposition 23. *If $v \neq p, q, \infty$, then $(p^*, q)_v = 1$.*

Proof. We first treat the case when $v \neq 2$. We need to show that $z^2 - p^*x^2 - qy^2 = 0$ has a non-trivial solution in $\mathbb{Q}_v$. Chevalley's theorem says that the number of solutions in $\mathbb{F}_v$ is congruent to zero modulo v (Chapter 1 Theorem 3 of Serre [4]), so since $(0,0,0)$ is a solution there must be a non-zero one as well. Since $v \neq 2$, Hensel's lemma allows us to lift it to $\mathbb{Q}_v$.

When $v = 2$, Hensel's lemma requires a solution modulo 8 to lift to $\mathbb{Q}_2$. Since $p^* \equiv 1 \mod 4$, there are two cases: if $p^* \equiv 1 \mod 8$, take $z \equiv x \equiv 1 \mod 8$, $y \equiv 0 \mod 8$. if $p^* \equiv 5 \mod 8$, take $z \equiv x \equiv 1 \mod 8$ and $y \equiv 2 \mod 8$. Then apply Hensel's lemma. □

Now we deal with the case that $v = p$ or q. Since $(a,b)_v = (b,a)_v$, it suffices to consider $v = p$.

Proposition 24. *If $v = p$, then $(p^*, q)_p = \left(\frac{q}{p}\right)$.*

Proof. Suppose $z^2 - p^*x^2 - qy^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p$. This is homogenous, so we may assume the solution is in $\mathbb{Z}_p$ and that one of the variables is relatively prime to p. If $p|z$, then since $z^2 - p^*x^2 - qy^2 = 0$ we see that $p|y$ and hence $p^*x^2 = z^2 - qy^2 \equiv 0 \mod p^2$. Thus $p|x$, a contradiction. Likewise $p \nmid y$. Reducing modulo p, we see that $z^2 \equiv qy^2 \mod p$, so q is a square modulo p. Therefore if $(p^*, q)_p = 1$, then we have $\left(\frac{q}{p}\right) = 1$.

Conversely, suppose $\left(\frac{q}{p}\right) = 1$, so by Hensel's lemma there is an $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 = q$. Then $\alpha^2 - p^* \cdot 0^2 - q \cdot 1^2 = 0$, so $z^2 - p^*x^2 - qy^2 = 0$ has a non-trivial solution. □

Finally we deal with the infinite place.

Proposition 25. *If $v = \infty$, then $(p^*, q)_\infty = 1$.*

Proof. The only obstruction to $z^2 - p^*x^2 - qy^2 = 0$ having a non-trivial solution in $\mathbb{Q}_\infty = \mathbb{R}$ is the sign of p^* and q. As long as $p^*x^2 + qy^2$ takes on a positive value, a square root exist. But $p^*x^2 + qy^2$ can be made positive since q is always positive. □

We can now combine these calculations with the Hilbert reciprocity law to deduce quadratic reciprocity. Theorem 21, combined with Proposition 23-25 says that

$$1 = \prod_v (p^*, q)_v = (p^*, q)_p (p^*, q)_q (p^*, q)_\infty = \left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right).$$

It is worth noting that Hilbert reciprocity allows the supplemental laws to be recovered using the same techniques.

References

1. J.W.S. Cassels and A. Fröhlich, *Algebraic number theory: Proceedings of an instructional conference organized by the london mathematical society (a nato advanced study institute) with the support of the international mathematical union*, London Mathematical Society, 2010.

2. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, Springer, 1990.
3. F. Lemmermeyer, *Reciprocity laws: From euler to eisenstein*, Springer Monographs in Mathematics, Springer, 2000.
4. J.P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, Springer, 1973.