Quadratic Reciprocity

Nicolas Diaz-Wahl

Abstract

I use Fermat's sum of squares theorem and Gauss' proof to motivate quadratic reciprocity and basic ideas in algebraic number theory. In particular, splitting of primes in the Gaussian integers is a key tool. Quadratic reciprocity is proved by studying the splitting behavior of primes in cyclotomic fields and their unique quadratic subfields. The Artin symbol is related to the Legendre symbol, motivating higher reciprocity laws and class field theory.

1 Motivating problem

A natural question in number theory is to identify the integers that are the sum of two squares, i.e. solve the Diophantine equation

$$x^2 + y^2 = n.$$

The ancient identity

$$(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$$

reduces this question to the problem of deciding which *primes* are the sum of two squares. The following pattern was identified by Fermat.

Theorem 1. *A prime $p \in \mathbb{Z}$ is the sum of two squares if and only if $p = 2$ or $p \equiv 1 \bmod 4$.*

Example 1.

$$2 = 1^2 + 1^2,\ 5 = 1^2 + 2^2,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,\ 29 = 2^2 + 5^2,\ 73 = 3^2 + 8^2, \text{ etc.}$$

The direction $p = x^2 + y^2 \implies p = 2$ or $p \equiv 1 \bmod 4$ is trivial. But how on Earth do you use the congruence condition to produce integers x, y such that $p = x^2 + y^2$?

I'm sure there are nice ways of motivating this argument, but let me just flash it in front of your eyes to see what key ideas go into the proof.

Proof. (1) Use number fields/rings! If $p = x^2 + y^2$, note that p factors as $(x + iy)(x - iy)$ in $\mathbb{Z}[i]$. We now have the hint that we should consider prime factorizations in $\mathbb{Z}[i]$.

(a) We first identify the units of $\mathbb{Z}[i]$. They are the $x + iy$ such that $x^2 + y^2 = 1$ (why?) so we find that $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Cool.

(b) The quantity $x^2 + y^2$ associated to $x + iy$ seems important; let's call it the *norm* $N(x + iy)$. It's easy to see that $N(\alpha\beta) = N(\alpha)N(\beta)$. We can reinterpret (a) as the statement $\alpha \in \mathbb{Z}[i]^\times \iff N(\alpha) = 1$. Exercise: this is true for arbitrary number rings. Prove it!

(c) If p is a prime in $\mathbb{Z}$, consider its factorization in $\mathbb{Z}[i]$ (why is a UFD btw, in fact its Euclidean with norm being the norm): $p = \pi_1^{e_1} \cdots \pi_r^{e_r}$. Then

$$p^2 = N(p) = \prod_{i=1}^{r} N(\pi_i)^{e_i},$$

so $r \leq 2$ (b/c norm of an irreducible can't be 1, ow it's a unit) and $e_i \leq 2$. This leaves two possibilities: p is irreducible in $\mathbb{Z}[i]$ or $p = \pi\bar{\pi}$ (with $N(\pi) = p$). In fact, it's easy to show that $N(\pi)$ is prime in $\mathbb{Z}$ iff π is irreducible in $\mathbb{Z}[i]$ (Ex: generalize this as much as possible).

Hence we deduce the following lemma:

Lemma 1. *$p = x^2 + y^2$ iff p is reducible in $\mathbb{Z}[i]$.*

(2) Relate the (ir)reducibility of p to squares mod p! I don't really know how to motivate this well, so let's just dive in.

If $p = x^2 + y^2$, then if z is the inverse of y mod p, we have $0 \equiv pz^2 \equiv (xz)^2 + 1 \bmod p$, i.e. $(xz)^2 \equiv -1 \bmod p$, so -1 is a square mod p. OK and? Well, the converse holds too! If $-1 \equiv u^2 \bmod p$, then $p | u^2 + 1$. To show that p is the sum of two squares, it is enough to show that p is reducible. Suppose for contradiction that p is irreducible, *hence prime* because $\mathbb{Z}[i]$ is a UFD (note how crucial of an assumption this is). Then since $p | u^2 + 1 = (u + i)(u - i)$, we have $p | u \pm i$, but it obviously doesn't. So p is reducible, and p is the sum of two squares.

(3) Relate -1 being a square mod p to $p \equiv 1 \bmod 4$. We tackle this in the next section. In summary, the structure of the proof goes as follows:

$$p = x^2 + y^2 \iff p \text{ is reducible in } \mathbb{Z}[i] \iff -1 \text{ is a square mod } p \iff p \equiv 1 \bmod 4. \qquad \square$$

Okay, lit. So somehow the properties of squares mod p is important here, so let's study this in more detail.

Exercise 1. Relate the the conditions that $p = x^2 + 2y^2$ or $p = x^2 + xy + y^2$ to -2 and -3 being squares mod p. What happens to $p = x^2 + 3y^2$? What goes wrong with $p = x^2 + 5y^2$?

Exercise 2. Let n be a nonzero integer and p be an odd prime not dividing n. Then

$$p | x^2 + ny^2, \ \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1.$$

2 Quadratic Residues

Definition 2. We say a is a *quadratic residue* mod p if $p \nmid a$ and there is some $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod p$.

The *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p | a \\ 1 & a \text{ is a QR mod } p \\ -1 & a \text{ is not a QR mod } p. \end{cases}$$

At once, we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

For a fixed (odd) prime p, it would be nice to have an easy way to characterize the quadratic residues mod p. Do we all know FLT? $a^{p-1} \equiv 1 \bmod p$.

Proposition 3 (Euler)**.** *Let p be an odd prime:*

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

Proof. In general, $a^{p-1} \equiv 1 \bmod p$. Consider the polynomial

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

If $a \equiv x^2 \bmod p$, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$, so the squares mod p divide $t^{\frac{p-1}{2}} - 1$. Thus the nonsquares divide the other factor (since all nonzero a divide $t^{p-1} - 1$). Sick. □

Note that in the proof of Theorem **??**, we were not characterizing when a specific number is a square mod p, but the *converse*; *for which primes p* is -1 is a quadratic residue? The answer we want is that $p = 2$ or $p \equiv 1 \bmod 4$, the former case being clear.

Corollary 4. *Let p be an odd prime:*

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4.$$

Proof. By the proposition,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p \iff (-1)^{\frac{p-1}{2}} = 1 \text{ (since } p > 2) \iff p \equiv 1 \bmod 4.$$ □

This concludes the proof of Theorem **??**. To solve the problem of characterizing $p = x^2 + 2y^2$, we need to find a condition for when $\left(\frac{-2}{p}\right) = 1$. Since $-2 = 2(-1)$, it is enough to characterize primes for which 2 is a square. In fact, to characterize primes for which n is a square mod p, it's enough to do so for -1, 2, and odd primes p. This leads to the utterly cracked theorem known as quadratic reciprocity:

Theorem 5 (Gauss' law of quadratic reciprocity)**.** *Let p and q be odd primes:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{4}} = \begin{cases} +1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv -1 \bmod 4 \end{cases}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases},$$

and

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

The last condition can be interpreted as p is a square mod q iff q is a square mod p (if either is 1 mod 4), and p is a square mod q iff q is *not* a square mod p if both are 3 mod 4.

Example 2. We identify the primes for which 14 is a quadratic residue.

3 All of algebraic number theory

We now need some algebraic number theory. This is not the most elementary proof, but the elementary proofs are not enlightening.

3.1 Structure of integer rings

Theorem 6 (Integer rings are Dedekind domains)**.** *Let $K/\mathbb{Q}$ be a number field, and $\mathcal{O}_K$ be the ring of integers in K. Then $\mathcal{O}_K$ is a Noetherian integrally closed domain of dimension 1 (Dedekind domain), and is free as a $\mathbb{Z}$-module of rank $|K : \mathbb{Q}|$. In particular, every ideal I in $\mathcal{O}_K$ factors (uniquely) as a product of prime ideals: $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.*

Proof sketch. Integrally closed is *apriori* true; dimension 1 follows because $\dim \mathbb{Z} = 1$ and an integral extension of rings preserves dimension (going-up theorem). Since $\mathcal{O}_K$ is a torsion-free $\mathbb{Z}$-module, it is free (structure of modules over a PID). For the claim that it has rank $|K : \mathbb{Q}|$, see Neukirch pg. 12-13 (or any ANT book); this implies Noetherian. The statement about prime factorization follows from the primary decomposition theorem for Noetherian rings and the fact that the localization of a Dedekind domain is a DVR, where primary ideals are powers of prime ideals, and these behave well under localization. □

Given a factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

he e_i are the *ramification indices*. Moreover, $k(\mathfrak{P}_i) = \mathcal{O}_L/\mathfrak{P}_i$ over $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ is a finite extension of finite fields; the degree f_i is called the *residue field degree*. It is obvious that e_i and f_i are multiplicative over towers: i.e. if $M/L/K$ is a tower of field extensions, and we have a chain of primes $\mathfrak{p} \subsetneq \mathfrak{P} \subsetneq x$, then $e(x/\mathfrak{p}) = e(x/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$ and $f(x/\mathfrak{p}) = f(x/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$.

Theorem 7 (Basic structure of Dedekind and Galois extensions)**.** *Let L/K be an extension of number fields with integer rings $\mathcal{O}_K$, $\mathcal{O}_L$. Fix a prime $\mathfrak{p}$ of K.*

(a) *We have the fundamental identity*

$$\sum_{i=1}^{g} e_i f_i = |L : K|.$$

(b) *If the extension L/K is Galois, then $e_1 = \cdots = e_g$, $f_1 = \cdots = f_g$, and $\mathrm{Gal}(L/K)$ acts transtively on $\operatorname{Spec} \mathcal{O}_L/\mathfrak{p}$. Thus the fundamental identity reduces to*

$$efg = |L : K|.$$

(c) *Define the decomposition group $D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\mathfrak{P} = \mathfrak{P}\}$. Then $D(\mathfrak{P}/\mathfrak{p})$ acts on $k(\mathfrak{P})/k(\mathfrak{p})$ via $\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}$. The map $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) : \sigma \mapsto \bar{\sigma}$ is surjective; the kernel is the inertia group $I(L/K)$.*

(d) *We have $\#D(\mathfrak{P}/\mathfrak{p}) = ef$, hence $\#I(\mathfrak{P}/\mathfrak{p}) = e$.*

The latter two statements can be condensed into the "fundamental short exact sequence"

$$1 \to I(\mathfrak{P}/\mathfrak{p}) \to D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \to 1.$$

Remark 8. Over p-adic fields. there is a unique prime in each field, so the sequence simplifies to

$$1 \to I(L/K) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K) \to 1.$$

Proof. (a) Since $\mathfrak{p}$ (resp. $\mathfrak{P}_i$) contain p, $k(\mathfrak{p})$ and $k(\mathfrak{P}_i)$ are $\mathbb{F}_p$-vector spaces; finite degree follows from the fact that $\mathcal{O}_K$ (resp. $\mathcal{O}_L$) are of finite rank over $\mathbb{Z}$, so their dimension is in fact at most $|K:\mathbb{Q}|$ (resp. $|L:\mathbb{Q}|$) over $\mathbb{F}_p$. The fundamental identity follows from the Chinese remainder theorem and Nakayama's lemma, and is a good exercise for both. Here goes: we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \bigoplus_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i}.$$

We have a filtration $\mathcal{O}_L/\mathfrak{P}_i^{e_i} \supsetneq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supsetneq \cdots \supsetneq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supsetneq 0$ whose associated gradeds are isomorphic to $k(\mathfrak{P}_i)$, so $\dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{P}_i^{e_i} = e_i f_i$. Lifting a $k(\mathfrak{p})$-basis of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ to generators for $\mathcal{O}_L$ over $\mathcal{O}_K$ (use Nakayama) implies that $\dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = |L:K|$.

(b) The equality of the e_i and f_i follows from the transitivity of the Galois action. If $\mathfrak{P}' \neq \sigma\mathfrak{P}$ for any σ, by CRT there is a $x \in \mathcal{O}_L$ such that

$$x \equiv 0 \bmod \mathfrak{P}' \quad \text{and} \quad x \equiv 1 \bmod \sigma\mathfrak{P}\ \forall \sigma \in \mathrm{Gal}(L/K).$$

Hence $N_{L/K}(x) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma x$ is in $\mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$, but $x \notin \sigma\mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L/K)$ implies $\sigma x \notin \mathfrak{P}$, so $\prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma x \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, a contradiction.

(c) Since $k(\mathfrak{P})/k(\mathfrak{p})$ is an extension of finite fields, it is Galois (this is actually true for general residue field). As such, pick a primitive element $k(\mathfrak{P}) = k(\mathfrak{p})(\bar{\theta})$ and a lift θ in $\mathcal{O}_L$. Then the minimal polynomial of $\bar{\theta}$ divides the reduction of the minimal polynomial of θ, so the conjugates of the roots of $\bar{\theta}$ are roots of $\bar{f}(X)$, so there is a zero θ' of $f(X)$ such that $\theta' \equiv \sigma\theta \bmod \mathfrak{P}$,

(d) This is just orbit-stabilizer applied to the transitive action of $\mathrm{Gal}(L/K)$ on $\operatorname{Spec}\mathcal{O}_L/\mathfrak{p}$. Note that $D(\mathfrak{P}/\mathfrak{p}) = \mathrm{Gal}(L/K)^{\mathfrak{P}}$ whose index in $\mathrm{Gal}(L/K)$ is the size of the orbit, i.e. g. The rest follows easily. □

Theorem 9 (Dedekind-Kummer Theorem)**.** *Let L/K be an extension of number fields, and suppose $\mathcal{O}_L = \mathcal{O}_K[\theta]$ for some $\theta \in L$. Let $f(x) \in \mathcal{O}_K[x]$ be the minimum polynomial of θ over K. For a prime $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$, if*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_g(x)^{e_g} \bmod p,$$

then the ideals $\mathfrak{P}_i := f_i(\theta)\mathcal{O}_L + \mathfrak{p}\mathcal{O}_L$ are prime, and

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Moreover, the residue class degrees $f(\mathfrak{P}_i|\mathfrak{p})$ are $\deg \bar{f}_i(x)$ for each i.

Proof. What are the primes of

$$\mathcal{O}[\theta]/\mathfrak{p} = \mathcal{O}[X]/(\bar{f}(X) + \mathfrak{p}) \simeq k(\mathfrak{p})[X]/\left(\prod \bar{f}_i(X)^{e_i}\right) \simeq \bigoplus_{i=1}^{g} k(\mathfrak{p})[X]/(\bar{f}_i(X)^{e_i})$$

? □

Corollary 10. *Keep notation as above. A prime $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ is unramified if and only if $\mathfrak{p}$ does not divide the discriminant of $f(x)$. If L/K is Galois, $\mathfrak{p}$ is totally split if and only if $f(x)$ has a root modulo $\mathfrak{p}$. A prime $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ is inert if and only if $f(x)$ is irreducible modulo $\mathfrak{p}$.*

3.2 Splitting and the Artin Symbol

Suppose L/K is a finite extension of number fields, unramified at $\mathfrak{p}$. Pick a prime $\mathfrak{P}|\mathfrak{p}$. Then the inertia group $I(\mathfrak{P}/\mathfrak{p})$ is trivial. Hence $D(\mathfrak{P}/\mathfrak{p}) \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. The latter is cyclic, being a finite extension of finite fields, and is generated by the Frobenius element $x \mapsto x^q$. Hence the unique lift of Frobenius to $D(\mathfrak{P}/\mathfrak{p})$ exists, and we call it the *Artin symbol*

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K).$$

Note that it is well-defined up to conjugacy, we suppress the dependence on $\mathfrak{P}$. If L/K is abelian, there is truly no dependence on $\mathfrak{P}$, and this will be the case for our situation.

Definition 11. We say $\mathfrak{p}$ *splits completely* in L if all $\mathfrak{P}_i|\mathfrak{p}$ have $f_i = e_i = 1$, so $g = |L : K|$.

We say $\mathfrak{p}$ is *inert* if $g = 1$ and $\mathfrak{p}$ is unramified, so $f = |L : K|$.

Proposition 12. *Keep the situation of L/K a Galois extension with group G, fix $\mathfrak{p} \in \operatorname{Spec} K$, and let $\mathfrak{P}$ be any prime lying over $\mathfrak{p}$.*

1. $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$ *iff $\mathfrak{p}$ splits completely.*
2. *The Artin symbol generates* $\mathrm{Gal}(L/K)$ *if and only if $\mathfrak{p}$ is inert in L. In particular, non-cyclic extensions have no inert primes.*

Proof. Let e and f denote the common ramification indices of the primes lying over $\mathfrak{p}$. Then $\mathfrak{p}$ splits completely by definition when $e = f = 1$. In particular, $\mathfrak{p}$ is unramified, hence $D_\mathfrak{p} \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ which is trivial since $f = 1$. Since the Artin symbol generates $D_\mathfrak{p}$, it is trivial.

Recall $\mathfrak{p}$ is inert if and only if $e = g = 1$, hence $f = \#D_\mathfrak{p}$. Moreover, $g = 1$ means only one prime lies over $\mathfrak{p}$, hence $D_\mathfrak{p} = G$ which is isomorphic to $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ since $\mathfrak{p}$ is unramified. Since the Galois group of an extension of finite groups is cyclic, the Artin symbol generates $D_\mathfrak{p} = G$. In particular, G is cyclic. Thus, non-cyclic extensions have no inert primes as claimed. □

A cute corollary to this is that Φ_n is reducible modulo every prime whenever $(\mathbb{Z}/n\mathbb{Z})^\times$ is non-cyclic (i.e. $n \neq 2, 4$, p or $2p$ for an odd prime p). Indeed, $\Phi_n(x)$ is irreducible modulo p if and only if p is inert in $\mathbb{Q}(\zeta_n)$, whose Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.

3.3 Criterion for ramification

Theorem 13. *Let $K/\mathbb{Q}$ be a number field, and $\omega_1, \ldots, \omega_n$ be an integral basis of $\mathcal{O}_K/\mathbb{Z}$. The discriminant is given by*

$$d_{K/\mathbb{Q}} = \mathrm{disc}(\omega_1, \ldots, \omega_n) = \det(\sigma_i\omega_i)^2 = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)).$$

The ramified primes are precisely those dividing the discriminant.

If $1, \alpha, \ldots, \alpha^{d-1}$ is a power basis and $f(X)$ is the minimal polynomial of α, its discriminant is given by $(f'(\alpha))$.

3.4 Cyclotomic Fields

Now we can start attacking our goal of proving quadratic reciprocity. The main insight required is that the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ is a *ray class field*, i.e. it is ramified precisely at primes dividing n with the

Proposition 14. *Let p be a prime and put $\zeta = \zeta_{p^r}$. The extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ of degree $\varphi(p^r)$ has*

(a) *Galois group* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/p^r\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)p^{r-1}\mathbb{Z})$;

(b) *integer ring* $\mathbb{Z}[\zeta_{p^r}]$;

(c) *is ramified only at p, and the ideal $\mathfrak{p} = (1-\zeta)$ is the unique prime lying over p.*

Proof sketch. (a) Y'all should know this. $|\mathbb{Q}(\zeta) : \mathbb{Q}| = \varphi(p^r)$, and the automorphisms induced by $\zeta \mapsto \zeta^a$ for $(a, p^r) = 1$ are $\varphi(p^r)$-many; since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is normal, we're done.

(b) The set $1, \zeta, \ldots, \zeta^{d-1}$ is a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$, and has p-power discriminant $\pm p^s$; this will imply (c) once we know that it's $\mathbb{Z}$-span is the integral basis. This implies $p^s\mathcal{O} \subset \mathbb{Z}[\zeta] \subset \mathcal{O}$. From the identity

$$p = \prod_{i \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (1-\zeta^i),$$

it follows that $\mathfrak{p} = (1-\zeta)$ is prime and $\mathcal{O}/\mathfrak{p}\mathcal{O} \simeq \mathbb{F}_p$, so $\mathcal{O} \subset \mathbb{Z} + (1-\zeta)\mathcal{O}$, and $\mathcal{O} = (1) = (1-\zeta, \zeta) = \mathbb{Z}[\zeta] + \mathfrak{p}$. Multipying by $1-\zeta$ and substituting, we get that

$$\lambda\mathcal{O} = \lambda^2\mathcal{O} + \lambda\mathbb{Z}[\zeta] \implies \lambda^2\mathcal{O} + \mathbb{Z}[\zeta] = \mathcal{O}.$$

Taking higher powers of λ, we see that $\mathcal{O} = \mathbb{Z}[\zeta]$. □

Lemma 2. *The ring of integers in $\mathbb{Q}(\sqrt{d})$ is*

$$\mathcal{O} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[(1+\sqrt{d})/2] & d \equiv 1 \end{cases}$$

and has discriminant $4d$ and d respectively.

Proof. Exercise. □

4 The proof

We consider the following setup. Fix an odd prime p, and consider the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Fix a prime $\ell \neq p$.

Lemma 3. *The field $\mathbb{Q}(\zeta_p)$ contains a unique quadratic subfield, namely $\mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2}p$.*

Proof. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic of even order, there is a unique subgroup of index 2 corresponding to a unique quadratic subextension of degree 2 (by Galois theory). Quadratic extensions are of the form $\mathbb{Q}(\sqrt{d})$. By Lemma **??**, such an extension is ramified at $4d$ if $d \equiv 2, 3 \bmod 4$, and d if $d \equiv 1 \bmod p$. By the ramification being multiplicative in towers, we need $d = \pm p$; so the discriminant of $\mathbb{Q}(\zeta_p)$ is p if $p \equiv 1 \bmod 4$, and $4p$ if $p \equiv 3 \bmod 4$, but the discriminant of $\mathbb{Q}(\sqrt{-p})$ is p if $p \equiv 3 \bmod 4$, so $p^* = (-1)^{(p-1)/2}p$ gives the right ramification. This explains the sign in quadratic reciprocity! □

Lemma 4. *Denote the Artin symbol* $\left(\frac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{\ell}\right)$ *by* $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. *Then*

$$\sigma_\ell(\sqrt{p^*}) = \left(\frac{\ell}{p}\right)\sqrt{p^*}$$

Proof. The Artin symbol generates $\mathrm{Gal}(L/K)$ if and only if $\mathfrak{p}$ is inert in L. In particular, non-cyclic extensions have no inert primes. □

Lemma 5. *Let* ℓ *and* p *be distinct odd primes, and denote the Artin symbol* $\left(\frac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{\ell}\right)$ *by* σ_ℓ. *Then* $\sigma_\ell(\sqrt{p^*}) = \left(\frac{\ell}{p}\right)\sqrt{p^*}$.

Proof. Note that $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = p - 1$ is even, and fix an isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ which is cyclic of order $p-1$. By the Galois correspondence, the quadratic field $\mathbb{Q}(\sqrt{p^*})$ corresponds to the unique subgroup of index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, namely the subgroup of quadratic residues. Thus if $\sigma_\ell \leftrightarrow \ell$ is a square modulo p, we have $\sigma_\ell(\sqrt{p^*}) = \sqrt{p^*}$, else if ℓ is not a square, $\sigma_\ell(\sqrt{p^*}) = -\sqrt{p^*}$, thus σ_ℓ acts as the Legendre symbol on $\sqrt{p^*}$ as asserted. □

Lemma 6. *We have* σ_ℓ *acts trivially on* $\sqrt{p^*}$ *if and only if* p^* *is a square modulo* ℓ.

Proof. Immediate consequence of Proposition **??**. Spelling it out, we have σ_ℓ fixes $\sqrt{p^*}$ if and only if $\sigma_\ell|_{\mathbb{Q}(\sqrt{p^*})} = 1$, thus $D_\ell = 1$, meaning $f_\ell = 1$, so ℓ splits completely in $\mathbb{Q}(\sqrt{p^*})$. This means $x^2 - p^* \equiv 0 \bmod \ell$ has a root by Dedekind-Kummer, i.e. p^* is a quadratic residue modulo ℓ. □

Proof of Quadratic Reciprocity. We have ℓ is a square modulo p if and only if σ_ℓ acts trivially on $\mathbb{Q}(\sqrt{p^*})$, if and only if p^* is square modulo ℓ. □

This strategy is not limited to the case of odd primes p and ℓ. The so-called supplementary laws can be proved by a similar manner.

Proposition 15. *Let* p *be an odd prime.*

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

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

Proof. (a) Let $K = \mathbb{Q}(i)$ and $p \neq 2$ be prime, hence p is unramified in K, and σ_p denote the Artin symbol $\left(\frac{K/\mathbb{Q}}{p}\right)$. Then $\sigma_p(i) = 1 \iff p$ splits in $K \iff x^2 + 1$ splits modulo p, i.e. $\left(\frac{-1}{p}\right) = 1$. Hence

$$\sigma_p(i) = \left(\frac{-1}{p}\right) i.$$

If $p \equiv 1 \bmod 4$, we have

$$\sigma_p(i) = i^p = i^{1+4k} = i,$$

while if $p \equiv 3 \bmod 4$, we have

$$\sigma_p(i) = i^p = i^{3+4k} = i^3 = -i,$$

so $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 4$. More succinctly,

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

which is consistent with Euler's criterion.

(b) Let ζ be an 8th root of unity, and set $K = \mathbb{Q}(\zeta)$. Fix a prime $p \neq 2$ so that p is unramified in K. Then $(\zeta + \zeta^{-1})^2 = \zeta^2 + (\zeta^{-2}) + 2\zeta\zeta^{-1} = 2$, so $\zeta + \zeta^{-1} = \sqrt{2}$. Fix a prime $p \neq 2$, and let σ_p denote the Artin symbol $\left(\frac{K/\mathbb{Q}}{p}\right)$. Then $\sigma_p(\sqrt{2}) = 1 \iff p$ splits in $\mathbb{Q}(\sqrt{2}) \iff x^2 - 2$ has a root modulo p, i.e. $\left(\frac{2}{p}\right) = 1$. Hence

$$\sigma_p(\sqrt{2}) = \left(\frac{2}{p}\right)\sqrt{2}.$$

If $p \equiv \pm 1 \bmod 8$, then

$$\sigma_p(\sqrt{2}) = \sigma_p(\zeta + \zeta^{-1}) = \zeta^p + \zeta^{-p} = \zeta^{1+8k} + \zeta^{-1+8k} = \zeta + \zeta^{-1} = \sqrt{2},$$

while if $p \equiv \pm 3 \bmod 8$, we have

$$\sigma_p(\sqrt{2}) = \sigma_p(\zeta + \zeta^{-1}) = \zeta^p + \zeta^{-p} = \zeta^{3+8k} + \zeta^{-3+8k} = \zeta^3 + \zeta^{-3} = -\sqrt{2},$$

so σ_p fixes $\sqrt{2}$ if and only if $p \equiv \pm 1 \bmod 8$, i.e. $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 8$. More succinctly,

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

□

The "mod 8" condition for the latter supplementary law always struck me as somewhat strange. In retrospect, we see that the 4 and 8 appearing in both laws come from the fact that $\sqrt{-1}$ and $\sqrt{2}$ lie in the 4th and 8th cyclotomic fields respectively. The central nature of cyclotomic fields foreshadows class field theory. Indeed, class field theory characterizes the primes that split in abelian extensions of a number field K in terms its class group. The Kronecker-Weber theorem states that every abelian extension of $\mathbb{Q}$ is cyclotomic, thus cyclotomic fields control the arithmetic of abelian extensions of $\mathbb{Q}$ (in a functorial and reciprocal manner).