9 Quadratic Reciprocity

9.1 Primes x^2+y^2, x^2+2y^2 and x^2+3y^2

Recall Fermat's two square theorem (Theorem 6.18), which says *if p is an odd prime, $p = x^2+y^2$ if and only if $p \equiv 1 \bmod 4$.*

Fermat generalized this to the following

Theorem 9.1. *Let p be an odd prime. Then $p = x^2+2y^2$ if and only if $p \equiv 1, 3 \bmod 8$.*

Theorem 9.2. *Let p be prime. Then $p = x^2+3y^2$ if and only if $p \equiv 1 \bmod 3$.*

How might we prove these two results?

Let's recall our proof of Fermat's two square theorem. One direction is easy: If $p \equiv 3 \bmod 4$, then $p \neq x^2+y^2$ by congruence conditions. For the other direction, suppose $p \equiv 1 \bmod 4$. Lagrange's Lemma 6.17 (which was proved with Wilson's theorem) said that $p|m^2+1$ for some m. Since $p|m^2+1 = (m+i)(m-i)$ but $p \nmid m \pm i$ in $\mathbb{Z}[i]$ ($\frac{m}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$), this means p is not prime in $\mathbb{Z}[i]$ (by the prime divisor property, which is equivalent to unique factorization). Then p has a nontrivial factorization $p = \alpha\beta$ in $\mathbb{Z}[i]$, so $p^2 = N(p) = N(\alpha)N(\beta) \implies N(\alpha) = N(\beta) = p$, i.e., $p = x^2+y^2$ where $x+yi = \alpha$.

Again, one direction of Theorems 9.1 and 9.2 are easy. If $p \equiv 5, 7 \bmod 8$, then $p \neq x^2+2y^2$ and if $p \equiv 2 \bmod 3$, then $p \neq x^2+3y^2$ (see Section 3.7). To prove the hard direction, one needs two things:

(i) unique factorization in $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3]$, which was covered in Chapter 7; and

(ii) appropriate analogues of Lagrange's Lemma 6.17.

In this chapter, we will prove a great generalization of Lagrange's lemma, which is known as the Law of Quadratic Reciprocity. This was first proven by Gauss, in many different ways, and might be viewed as the pinnacle of elementary number theory. Along the way, we will also cover another important result from elementary number theory—the Chinese Remainder Theorem.

9.2 Statement of Quadratic Reciprocity

Let p and q denote odd primes.

Definition 9.3. *We say a is a* **square**, *or* **quadratic residue**, *mod p if $x^2 \equiv a \bmod p$ for some $x \in \mathbb{Z}$. Otherwise, we say a is a* **nonsquare**, *or* **quadratic nonresidue**, *mod p.*

Example. *The squares mod 4 are $0, 1$; the nonsquares are $2, 3$ (up to congruence). (Okay, you might say 4 is not prime, but this example comes up often, and the definitions are the same for any mod n.)*

Example. *Lagrange's Lemma 6.17 says, if $p \equiv 1 \bmod 4$, then $p|m^2+1$ for some m, i.e., $m^2 \equiv -1 \bmod p$ for some m, i.e., -1 is a* square *mod p.*

We will soon see that these conditions are equivalent, i.e.,

$$p \text{ is a square mod } 4 \iff p \equiv 1 \bmod 4 \iff -1 \text{ is a square mod } p$$

(The first equivalence is because, up to congruence, only 0 and 1 are squares mod 4.)

I stated things in this form because it looks somewhat similar to quadratic reciprocity, which was originally conjectured by Euler in the following form:

If p and q are not both 3 mod 4*, then*

$$p \text{ is a square} \bmod q \iff q \text{ is a square} \bmod p. \tag{1}$$

If $p \equiv q \equiv 3 \bmod 4$, then

$$p \text{ is a square} \bmod q \iff q \text{ is } \textbf{not} \text{ a square} \bmod p. \tag{2}$$

It is convenient to introduce some new notation, which will allow us to combine these two cases into one.

Definition 9.4. *Let $a \in \mathbb{Z}$ such that $\gcd(a,p) = 1$ The* **Legendre symbol***, or* **quadratic residue symbol** *mod p is*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a square} \bmod p \\ -1 & else. \end{cases}$$

(One can extend this to all $\mathbb{Z}$ by setting $\left(\frac{a}{p}\right) = 0$ if $\gcd(a,p) = p$, but we will not use this.) Note we have defined the Legendre symbol as a map $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{\pm 1\}$, but since the value only depends on the congruence class mod p, we may view it as a map

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}.$$

Hence we can rewrite (1) as

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

and (2) as

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

This leads to the typical modern formulation of quadratic reciprocity.

Theorem 9.5. (Quadratic Reciprocity) *Let p, q be odd primes. Then*

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

This is equivalent to Euler's version because $\frac{p-1}{2}\frac{q-1}{2}$ is even unless $p \equiv q \equiv 3 \bmod 4$. (Note the statement in the text, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, is not valid when $p = q$.)

Example. *Note that*

$$\left(\frac{5}{p}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right).$$

The squares mod 5 *are* $0, 1, 4$*. Hence* 5 *is a square mod p if and only if $p = 5$ or $p \equiv 1, 4, \bmod 5$.*

Exercise 9.1. *Use quadratic reciprocity to determine for which primes p is* 7 *a square mod p.*

9.3 Euler's criterion

Again, let p be an odd prime. Denote by $\square_p \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ be the nonzero congruence classes which are squares mod p, e.g., $\square_5 = \{1, 4\}$. Hence for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we may say $\left(\frac{a}{p}\right) = 1$ if and only if $a \in \square_p$.

Exercise 9.2. *Show $\square_p$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Show the map $\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})$ given by $\sigma(x) = x^2$ is 2-to-1. Conclude the subgroup $\square_p$ has index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., $|\square_p| = \frac{p-1}{2}$.*

Note this exercise tells us that exactly half of the elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares and half are nonsquares. The squares and nonsquares are then the two cosets (remember cosets?) of $(\mathbb{Z}/p\mathbb{Z})^\times$ with respect to the subgroup $\square_p$.

Proposition 9.6. (Euler's criterion) *Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then*

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

Proof. Consider the map from $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ given by

$$\phi(a) \equiv a^{\frac{p-1}{2}} \bmod p$$

Note that $\phi(a) \equiv 1 \bmod p$ if $a \in \square_p$. This is because we can write $a \equiv x^2 \bmod p$ so

$$\phi(a) \equiv \phi(x^2) \equiv x^{p-1} \bmod p$$

by Fermat's little theorem. By the previous exercise, the squares mod p give $\frac{p-1}{2}$ solutions to the polynomial congruence $\phi(a) \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p$. By Lagrange's theorem on polynomial congruence solutions (Section 3.5), this is all of them.

Hence $\phi(a) \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p$ if and only if $a \in \square_p$, i.e., if and only if $\left(\frac{a}{p}\right) = 1$. If $\left(\frac{a}{p}\right) = 1$ we are done. If $\left(\frac{a}{p}\right) = -1$, then $a^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, but its square is $a^{p-1} \equiv 1 \bmod p$, hence it must be $\equiv -1 \bmod p$. Thus in either case, Euler's criterion holds. □

Proposition 9.7. *The map $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ is multiplicative, i.e., $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, i.e., it is a* group homomorphism. *Its kernel is $\square_p$.*

Recall the *kernel* of a multiplicative map $\chi : G \to \mathbb{C}^\times$ is defined to be the set of all a such that $\chi(a) = 1$.

Note: A group homomorphism $\chi : G \to \mathbb{C}^\times$ is called a *(group) character*. Hence the Legendre symbol is also called the *Legendre character* or *quadratic residue character.*

Proof. Multiplicatively follows from Euler's criterion:

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

Since congruence mod p distinguishes between 1 and -1, we can conclude $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

The statement that $\square_p$ is the kernel of $\left(\frac{\cdot}{p}\right)$ is immediate from the definitions of $\square_p$ and the Legendre symbol. □

Exercise 9.3. *Explicitly write down the values of* $\left(\frac{\cdot}{p}\right)$ *for* $p = 7, 11, 13$. *In each case, write down what the subgroup* $\square_p$ *of* $(\mathbb{Z}/p\mathbb{Z})^\times$ *is.*

Proposition 9.8. (First supplementary law)

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

Proof. By Euler's criterion, we have

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

□

Exercise 9.4. *Give a proof of the first supplementary law which does not require Euler's criterion as follows. We know if* $p \equiv 1 \bmod 4$, *then* $-1 \in \square_p$ *by Lagrange's lemma. So it suffices to show that* $-1 \notin \square_p$ *for* $p \equiv 3 \bmod 4$. *Show this using Exercise 9.2.*

The reason this is called the first supplementary law (to quadratic reciprocity) is the following. A common question that arises in number theory is to evaluate some Legendre symbol $\left(\frac{a}{p}\right)$ for some $a \in \mathbb{Z}$. Quadratic reciprocity tells us how to do it if a is odd and positive. To take care of $a < 0$, we need the first supplementary law, and to take care of a even, we need one more supplementary law for $\left(\frac{2}{p}\right)$. We will do this next, and then show how to put everything together to calculate any Legendre symbol.

9.4 The value of $\left(\frac{2}{p}\right)$

Again, p is an odd prime.

Proposition 9.9. (Second supplementary law)

$$\left(\frac{2}{p}\right) = 1 \iff 2 \in \square_p \iff p \equiv \pm 1 \bmod 8.$$

Proof. The text proves the cases $p \equiv 1, 5 \bmod 8$ with an crazy mess of congruences, leaving an equally complicated mess of congruences for the $p \equiv 3, 7 \bmod 8$ cases in the exercises. You can read that/do the exercise if you want, but I'll show you one and a half algebraic number theory proofs of theorem.

The first half of a proof *assumes unique factorization* (or rather the prime divisor property) in $\mathbb{Z}[\sqrt{2}]$ (which is true, and we should get to next semester).

Suppose $2 \equiv x^2 \bmod p$. Then $p | x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$, but p does not divide either term on the right. Hence p must not be prime in $\mathbb{Z}[\sqrt{2}]$ (prime divisor property), i.e., there is a nontrivial factorization $p = \alpha\beta$ in $\mathbb{Z}[\sqrt{2}]$. Thus $p^2 = N(p) = N(\alpha)N(\beta)$, which means $N(\alpha) = N(\beta) = p$. Writing $\alpha = a - b\sqrt{2}$, we see $p = a^2 - 2b^2$. The squares mod 8 are $0, 1, 4$, so we must have $p \equiv \pm 1 \bmod 8$.

If one tries to do the other direction in a similar way, it is more complicated and involves using (essentially) $\mathbb{Z}[\sqrt{\pm p}]$. See Cohn's *Advanced Number Theory.* I won't even sketch this, but I wanted

to point out the above argument for the ($\Rightarrow$) since it's an argument that we've used several times now.

There is a much more clever proof of the proposition using the 8-th roots of unity in Ono's *Introduction to Algebraic Number Theory*. It involves a couple things we haven't really covered yet, but I think you can probably follow the idea anyway, and it shows some of the power of roots of unity. It goes as follows. Let $\zeta = \zeta_8 = e^{2\pi i/8} = \sqrt{i}$ and $\eta = \zeta + \zeta^{-1}$. Then $\eta^2 = \zeta^2 + 2 + \zeta^{-2} = i + 2 - i = 2$, i.e., $\eta = \sqrt{2}$. Hence

$$2^{\frac{p-1}{2}} = \eta^{p-1} = \eta^p \eta^{-1} = (\zeta + \zeta^{-1})^p \eta^{-1}.$$

But

$$(\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \equiv \begin{cases} \zeta + \zeta^{-1} \equiv \eta \bmod p & p \equiv \pm 1 \bmod 8 \\ \zeta^3 + \zeta^{-3} \equiv -\eta \bmod p & p \equiv \pm 3 \bmod 8. \end{cases}$$

Here we have extended the mod notation to a more general ring of (algebraic) integers, namely $\mathbb{Z}[\zeta]$, which is not a problem (except possibly psychologically—again $\alpha \equiv \beta \bmod p$ means $p | \beta - \alpha$ in $\mathbb{Z}[\zeta]$). Therefore

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

which proves the proposition by Euler's criterion. □

In the ζ_8 proof, we used the fact that $(\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \bmod p$. Prove the equivalent statement for integers (your proof should apply to this case also):

Exercise 9.5. *Let $a, b \in \mathbb{N}$. Show for p prime*

$$(a + b)^p \equiv a^p + b^p \bmod p.$$

Show by example this is not true for p not prime.

9.5 The story so far

Before we prove quadratic reciprocity, let's see how we can compute any Legendre symbol using quadratic reciprocity and the first and second supplementary laws.

Example.

$$\left(\frac{12}{23}\right) = \left(\frac{2}{23}\right)^2 \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

I.e., 12 *is a square mod* 23*, which is not obvious without computing the squares mod* 23*. The first step was from multiplicativity, the second by quadratic reciprocity, the third by reduction mod* 3*, and the fourth by either the second supplementary law or just knowing what the squares are mod* 3*. An alternate way to do it is*

$$\left(\frac{12}{23}\right) = \left(\frac{-11}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{11}{23}\right) = (-1)(-1)\left(\frac{23}{11}\right) = \left(\frac{1}{11}\right) = 1.$$

Here the first step is by congruence mod 23*, the second by multiplicativity, the third by both the first supplementary law and quadratic reciprocity, the fourth by congruence mod* 11*, and the last is*

because 1 *is always a square mod* p*. In this case both ways are of about equal difficulty, but sometimes one way is considerably simpler, e.g., if we had* $\left(\frac{22}{23}\right)$ *it's easiest to write it as* $\left(\frac{-1}{23}\right)$ *and use the first supplementary law.*

Note that using this trick of writing $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$ we can always get away with not using the second supplementary law for computing a *specific* Legendre symbol. This is because we only need the second law if a is even, in which case $p - a$ is odd. One could also get away without using the first supplementary law, e.g., $\left(\frac{-3}{59}\right) = \left(\frac{56}{59}\right) = \left(\frac{115}{59}\right)$, but this makes things considerably more difficult.

I just wanted to point out that the supplementary laws are useful, but not necessary to compute *specific* Legendre symbols. However, we will *need* the supplementary laws when we want to prove general theorems—e.g., to determine which primes are of the form $x^2 + 2y^2$ or $x^2 + 3y^2$.

Example.

$$\left(\frac{30}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{3}{59}\right)\left(\frac{5}{59}\right) = (-1)(-1)\left(\frac{59}{3}\right)\left(\frac{59}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = -1 \cdot 1 = -1,$$

i.e., 30 *is not a square mod* 59*.*

Exercise 9.6. *Compute* $\left(\frac{24}{61}\right)$*,* $\left(\frac{30}{61}\right)$*, and* $\left(\frac{31}{61}\right)$*.*

9.6 The Chinese remainder theorem

The original form of the Chinese remainder theorem, which was found in Sun Tzu's (the Art of War guy) mathematical treatise dating to the 3rd century, is as follows:

Let $m, n \in \mathbb{N}$*. If* $\gcd(m, n) = 1$*, then each* $x = 0, 1, 2, \ldots, mn-1$ *has a distinct pair of remainders* $(x \bmod m, x \bmod n)$*.*

Example. *Do* $m = 3$*,* $n = 5$*.*

From the example, we observe that the the remainders $x \bmod m$ repeat with period m and $x \bmod n$ repeat with period n, so you will never get the same pair again until these periods match up, which happens at mn since $\gcd(m, n) = 1$. This is the proof of the Chinese remainder theorem.

You might wonder what the Chinese call the Chinese remainder theorem. Maybe just *the* remainder theorem? like the French just call French onion soup "onion soup," Canadians just call Canadian bacon "bacon," or Feynman just called the Feynman integral "*the* integral." I looked it up on Chinese Wikipedia, and apparently they also call it the Chinese remainder theorem. I guess they're pretty proud of it. In the past it had many different names—"Sun Tzu's Theorem" is the only one I can read, which was also they used to call the theorem in Japan.

9.7 The full Chinese remainder theorem

A slight modification of the above Chinese remainder theorem tells us

$$(x \bmod m, x \bmod n) = (y \bmod m, y \bmod n) \iff x \equiv y \bmod mn.$$

The above argument tells us that the pairs of remainders on the left are different when $x \not\equiv y \bmod mn$, but the converse is obvious

$$x \equiv y \bmod mn \iff x - y \equiv 0 \bmod mn \implies x - y \equiv 0 \bmod m \text{ and } x - y \equiv 0 \bmod n.$$

Hence we may rephrase the Chinese remainder theorem as statement that the map

$$\alpha : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

given by

$$\alpha(a) = (a \bmod m, a \bmod n)$$

is 1-1 and onto.[1] The full Chinese remainder theorem says that α is a *ring homomorphism*, i.e., $\alpha(0) = (0,0)$, $\alpha(1) = (1,1)$,

$$\alpha(a+b) = \alpha(a) + \alpha(b)$$

and

$$\alpha(ab) = \alpha(a)\alpha(b).$$

These facts are immediate from congruence arithmetic. Check it:

Exercise 9.7. *Let* $\gcd(m,n) = 1$ *and* $\alpha : (\mathbb{Z}/mn\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ *be given by* $\alpha(a,b) = (a \bmod m, b \bmod n)$. *Check that* $\alpha(0) = (0,0)$, $\alpha(1) = (1,1)$, $\alpha(a+b) = \alpha(a) + \alpha(b)$ *and* $\alpha(ab) = \alpha(a)\alpha(b)$. *This means* α *is a* ring homomorphism.

In summary, we have

Theorem 9.10. (Chinese remainder theorem) *Suppose* $\gcd(m,n) = 1$. *The map* $\alpha : (\mathbb{Z}/mn\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ *is a* ring isomorphism, *i.e., it is 1-1 and onto,* $\alpha(0) = (0,0)$, $\alpha(1) = (1,1)$, $\alpha(a+b) = \alpha(a) + \alpha(b)$ *and* $\alpha(ab) = \alpha(a)\alpha(b)$.

Corollary 9.11. *Suppose* $\gcd(m,n) = 1$. *Then*

$$(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

In particular $\phi(mn) = \phi(m)\phi(n)$, *where* ϕ *denotes Euler's* ϕ*-function.*

This says that the multiplicative group mod mn is isomorphic to the product of the multiplicative groups mod m and mod n. If you don't know what the product of two groups means, don't worry. What the corollary means should be clear from the proof. But for the record if G and H are two groups, their product $G \times H$ is the group of elements (g,h) where $g \in G, h \in H$ and the group multiplication is defined by $(g,h)(g',h') = (gg', hh')$. (*Isomorphic* means that two groups are really the same: precisely, that there is a bijective homomorphism from one to the other. A *homomorphism* is a function $f : G \to H$ which respects the group multiplication, i.e., $f(gg') = f(g)f(g')$.)

Proof. The corollary essentially makes the following claim:

$$x \in (\mathbb{Z}/mn\mathbb{Z})^\times \iff x \in (\mathbb{Z}/m\mathbb{Z})^\times \text{ and } x \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Again we have slightly abused notation here—what we mean precisely is an integer x is invertible mod mn if and only if it is both mod m and mod n. This is true because x is relatively prime to mn if and only if it is relatively prime to m and n.

To see this gives the statement of the corollary, observe that it means the following: if we restrict the map $\alpha : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ to $(\mathbb{Z}/mn\mathbb{Z})^\times$, we get a bijection of the group $(\mathbb{Z}/mn\mathbb{Z})^\times$ with the product group $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Since α is multiplicative, it is a *group isomorphism.* □

Exercise 9.8. *Exercises 9.7.1, 9.7.2.*

[1] We never defined what a mod m means if $a \in \mathbb{Z}/mn\mathbb{Z}$, but it should be obvious. If we want to be more precise, we can read this statement for $a \in \mathbb{Z}$, not $a \in \mathbb{Z}/mn\mathbb{Z}$, but since it clearly only depends on the value a mod mn, it indeed defines a function on $\mathbb{Z}/mn\mathbb{Z}$.

9.8 Proof of quadratic reciprocity

Proof. Let p, q be distinct odd primes. Set $P = \left\{1 \leq x \leq \frac{pq-1}{2} | \gcd(x, pq) = 1\right\}$, so $(\mathbb{Z}/pq\mathbb{Z})^\times = P \cup -P$, where $-P = \{-x | x \in P\}$. We consider $\prod_{x\in P} x \bmod p$ and $\bmod q$.

Note that P consists of $\frac{q-1}{2}$ full sequences $1, 2, \ldots, p-1 \bmod p$ and the half sequence $1, 2, \ldots, \frac{p-1}{2} \bmod p$ minus the multiples $q, 2q, \ldots, \frac{p-1}{2}q$ of q. Hence

$$\prod_{x\in P} x \equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!/q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \bmod p,$$

where the second equivalence comes from Wilson's theorem, along with the fact that $1/q^{\frac{p-1}{2}} \equiv \pm 1 \equiv q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod p$, using Euler's criterion. Similarly

$$\prod_{x\in P} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \bmod q.$$

In other words

$$\prod_{x\in P} \alpha(x) \equiv \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right), (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\right) \bmod (p, q) \tag{3}$$

On the other hand, since $(\mathbb{Z}/pq\mathbb{Z})^\times = P \cup -P$, the Chinese Remainder Theorem says that $\alpha(P) = \{\alpha(x) | x \in P\}$ contains exactly one of (a, b) and $(-a, -b)$ for each $1 \leq a \leq p-1$ and $1 \leq b \leq \frac{q-1}{2}$. Hence

$$\prod_{x\in P} \alpha(x) \equiv \pm \left((p-1)!^{\frac{q-1}{2}}, \left(\frac{q-1}{2}\right)!^{p-1}\right) \equiv \left((-1)^{\frac{q-1}{2}}, \left(\frac{q-1}{2}\right)!^{p-1}\right) \bmod (p, q).$$

Note that

$$-1 \equiv (q-1)! \equiv 1 \cdot 2 \cdots \frac{q-1}{2} \cdot (-1)(-2) \cdots (-\frac{q-1}{2}) \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q-1}{2}\right)!^2 \bmod q,$$

hence

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

Thus

$$\prod_{x\in P} \alpha(x) \equiv \pm \left((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \bmod (p, q). \tag{4}$$

Dividing (3) by (4), we get

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

This means

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

which is precisely the Quadratic Reciprocity Law. □

The following exercises are related to our proof of quadratic reciprocity.

Exercise 9.9. *Let p, q be distinct odd primes. Determine the elements $x \in (\mathbb{Z}/pq\mathbb{Z})^\times$ such that $x^2 \equiv 1 \bmod pq$.* (Hint: think about the Chinese Remainder Theorem). *Using this, prove that $\prod_{x\in(\mathbb{Z}/pq\mathbb{Z})^\times} x \equiv 1 \bmod pq$ in the same way we proved Wilson's Theorem.*

Exercise 9.10. *As in the proof, set*

$$P = \left\{ 1 \leq x \leq \frac{pq-1}{2} | \gcd(x, pq) = 1 \right\}.$$

Deduce from the previous exercise that $\left(\prod_{x\in P} x\right)^2 \equiv 1 \bmod pq$.

Note that if one knew $\prod_{x\in P} x \equiv \pm 1 \bmod pq$, *this would say $\prod_{x\in P} \alpha(x) \equiv \pm(1,1) \bmod (p,q)$, hence* (3) *would mean $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$, which is* not true. *(In the previous exercise, you determined which elements square to* 1, *and it's not just ± 1 anymore.) As we see from* (4), *the actual determination of $\prod_{x\in P} \alpha(x)$ (even up to ± 1) is more complicated. This is an example of how working* mod *pq is more complicated than working* mod *p.*

Now we can sketch the proofs of Theorems 9.1.

Proof. (of Theorem 9.1) First suppose p is an odd prime of the form $x^2 + 2y^2$. Then examining the squares mod 8 shows $p \equiv 1, 3 \bmod 8$. This is the easy direction of Theorem 9.1.

To prove the converse, we first claim that $p = x^2 + 2y^2$ if and only if p is not prime in $\mathbb{Z}[\sqrt{-2}]$, which we know has unique factorization from Chapter 7. If $p = x^2+2y^2$ then $(x+y\sqrt{-2})(x-y\sqrt{-2})$ is a non-trivial factorization of p in $\mathbb{Z}[\sqrt{-2}]$ so it is not prime. Conversely, if p factors non-trivially in $\mathbb{Z}[\sqrt{-2}]$, say $p = \alpha\beta$, then $p^2 = N(\alpha)N(\beta)$ implies $N(\alpha) = x^2 + 2y^2 = p$ where $\alpha = x + y\sqrt{-2}$. (Actually, we only need the "if" direction of this claim.)

Now suppose $p \equiv 1, 3 \bmod 8$. Then we claim $p|m^2 + 2$ for some m. This follow from the two supplementary laws of quadratic reciprocity: $p|m^2 + 2$ iff $m^2 \equiv -2 \bmod p$ iff $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$, which is true. Since $p|(m + \sqrt{-2})(m - \sqrt{-2})$, but $p \nmid m \pm \sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$, p is not prime by the prime divisor property. This proves the Theorem. □

Note that we did not actually need quadratic reciprocity—just the supplementary laws. We do however for Theorem 9.2, which is homework.

Exercise 9.11. *(Proof of Theorem 9.2) Let $p > 3$ be prime. (i) Show $p = x^2 + 3y^2$ implies $p \equiv 1 \bmod 3$. (ii) Show $p = X^2 - XY + Y^2$ with $X \equiv Y \bmod 2$ if and only if p is not prime in $\mathbb{Z}[\zeta_3]$. (iii) Find half-integers $a, b, c, d \in \frac{1}{2}\mathbb{Z}$ such that $X^2 - XY + Y^2 = x^2 + 3y^2$ where $x = aX + bY$, $y = cX + dY$. (iv) Deduce that $p = x^2 + 3y^2$ if and only if p is not prime in $\mathbb{Z}[\zeta_3]$. (v) Suppose $p \equiv 1 \bmod 3$. Using quadratic reciprocity, show $p|m^2 + 3$ for some m. Conclude p is of the form $x^2 + 3y^2$.*

9.9 Discussion

Worthwhile reading. I am thinking about trying to cover some higher reciprocity laws in the second semester, so let me know if you think it sounds interesting.