

## QUADRATIC RECIPROCITY II: THE PROOFS

PETE L. CLARK

We shall prove the Quadratic Reciprocity Law and its “second supplement.”

### 1. PRELIMINARIES ON CONGRUENCES IN CYCLOTOMIC RINGS

For a positive integer  $n$ , let  $\zeta_n = e^{\frac{2\pi i}{n}}$  be a primitive  $n$ th root of unity, and let

$$R_n = \mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + \dots + a_{n-1}\zeta_n^{n-1} \mid a_i \in \mathbb{Z}\}.$$

Recall that an **algebraic integer** is a complex number  $\alpha$  which satisfies a monic polynomial relation with  $\mathbb{Z}$ -coefficients: there exist  $n$  and  $a_0, \dots, a_{n-1}$  such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0.$$

We need the following purely algebraic fact:

**Proposition 1.** *The algebraic integers form a subring of the complex numbers.*

This amounts to showing that if  $\alpha$  and  $\beta$  are algebraic integers, then  $\alpha + \beta$  and  $\alpha \cdot \beta$  are algebraic integers (which is plausible but not so trivial to prove). We have relegated the proof to [Integral Elements and Extensions].

Let  $p$  be a prime number; for  $x, y \in R_n$ , we will write  $x \equiv y \pmod{p}$  to mean that there exists a  $z \in R_n$  such that  $x - y = pz$ . Otherwise put, this is congruence modulo the principal ideal  $pR_n$  of  $R_n$ .

Since  $\mathbb{Z} \subset R_n$ , if  $x$  and  $y$  are ordinary integers, the notation  $x \equiv y \pmod{p}$  is ambiguous: interpreting it as a usual congruence in the integers, it means that there exists an integer  $n$  such that  $x - y = pn$ ; and interpreting it as a congruence in  $R_n$ , it means that  $x - y = pz$  for some  $z \in R_n$ . The key technical point is that these two notions of congruence are in fact the same:

**Lemma 2.** *If  $x, y \in \mathbb{Z}$  and  $z \in R_n$  are such that  $x - y = pz$ , then  $z \in \mathbb{Z}$ .*

Proof: Just dividing by  $p$ , we find that the complex number  $z = \frac{x-y}{p}$  is visibly an element of  $\mathbb{Q}$ . Now we need the fact, proved in Handout 2, that the only algebraic integers which are rational numbers are the usual integers. (This is the reason why we needed to assert that every element of  $R_n$  was an algebraic integer.)

To prove the second supplement we will take  $n = 8$ . To prove the QR law we will take  $n = p$  an odd prime. These choices will be constant throughout each of the proofs so we will abbreviate  $\zeta = \zeta_8$  (resp.  $\zeta_p$ ) and  $R = R_8$  (resp.  $R_p$ ).

### 2. PROOF OF THE SECOND SUPPLEMENT

Put  $\zeta = \zeta_8$ , a primitive eighth root of unity and  $R = R_8 = \mathbb{Z}[\zeta_8]$ . We have:

$$0 = \zeta^8 - 1 = (\zeta^4 + 1)(\zeta^4 - 1).$$

Since  $\zeta^4 \neq 1$  (primitivity), we must have  $\zeta^4 + 1 = 0$ . Multiplying by  $\zeta^{-2}$  we get

$$\zeta^2 + \zeta^{-2} = 0.$$

So

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

Putting  $\tau = \zeta + \zeta^{-1}$ , we have  $\tau^2 = 2$ . Now we calculate

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \binom{2}{p} \pmod{pR}.$$

The “ $\equiv$ ” is by Euler’s relation. Multiplying through by  $\tau$ , we get:

$$(1) \quad \tau^p \equiv \binom{2}{p} \tau \pmod{p}.$$

**Lemma 3.** (“Schoolboy binomial theorem”)

Let  $R$  be any commutative ring,  $p$  a prime number and  $x, y \in R$ . We have

$$(x + y)^p \equiv x^p + y^p \pmod{pR}.$$

Proof: The binomial formula asserts that

$$(x + y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \dots + \binom{p}{p-1}x^1y^{p-1} + y^p,$$

where  $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ . Now suppose  $0 < i < p$ . Since  $p$  is prime,  $p!$  is divisible by  $p$  and  $i!$  and  $(p-i)!$ , being a product of positive integers all less than  $p$ , are not. So each of the binomial coefficients is divisible by  $p$  except the first and the last.

Therefore

$$\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{pR}.$$

Case 1:  $p \equiv 1 \pmod{8}$ . Then  $\zeta^p = \zeta$ , and hence  $\zeta^{-p} = \zeta^{-1}$ , so

$$\tau^p \equiv \zeta^p + \zeta^{-p} \equiv \zeta + \zeta^{-1} = \tau \pmod{pR}$$

so (1) becomes

$$\tau \equiv \binom{2}{p} \tau \pmod{pR}.$$

It is tempting to cancel the  $\tau$ ’s, but we must be careful:  $pR$  need not be a prime ideal of the ring  $R$ .<sup>1</sup> But, sneakily, instead of dividing we *multiply* by  $\tau$ , getting

$$2 \equiv \tau^2 \equiv 2 \binom{2}{p} \pmod{pR},$$

which by Lemma 2 means that

$$2 \equiv 2 \binom{2}{p} \pmod{p}$$

in the usual sense. Since 2 is a unit in  $\mathbb{Z}/p\mathbb{Z}$ , dividing both sides by 2 is permissible. We do so, getting the desired conclusion in this case:

$$\binom{2}{p} \equiv 1 \pmod{p}.$$

Case 2:  $p \equiv -1 \pmod{8}$  is very similar: this time  $\zeta^p = \zeta^{-1}$ , but still  $\tau^p \equiv$

<sup>1</sup>In fact, it can be shown *not* to be prime in the case  $p \equiv 1 \pmod{8}$ .

$\zeta^p + \zeta^{-p} \equiv \zeta^{-1} + \zeta = \tau \pmod{pR}$ . The remainder of the argument is the same, in particular the conclusion:  $\left(\frac{2}{p}\right) \equiv 1 \pmod{p}$ .

Case 3:  $p \equiv 3 \pmod{8}$ . Now we have

$$\tau^p \equiv \zeta^p + \zeta^{-p} \equiv \zeta^3 + \zeta^{-3} \equiv \zeta^4\zeta^{-1} + \zeta^{-4}\zeta \equiv -(\zeta + \zeta^{-1}) \equiv -\tau \pmod{pR}.$$

Thus we get this time

$$-\tau \equiv \left(\frac{2}{p}\right) \tau \pmod{pR},$$

and again we multiply by  $\tau$  to get a congruence modulo  $p$  and conclude

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

Case 4:  $p \equiv 5 \pmod{8}$ : Exercise (Case 4 is to Case 3 as Case 2 is to Case 1.)

### 3. PROOF OF THE QUADRATIC RECIPROCITY LAW MODULO...

The above proof is due in spirit to Euler. It is very ingenious, but how do we adapt it to prove the Quadratic Reciprocity Law: e.g., what should play the role of  $\tau$ ?

Let us now take  $p$  to be an odd prime,  $\zeta = e^{\frac{2\pi i}{p}}$  to be a primitive  $p$ th root of unity, and  $R = \mathbb{Z}[\zeta]$ . A good start would be to find an explicit element  $\tau$  of  $R$  with  $\tau^2 = p$ .

This would mean in particular that  $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta)$ , which is far from obvious. Indeed, it need not even be quite true. Take  $p = 3$ : since  $\zeta_3 = e^{\frac{2\pi i}{3}} = \left(\frac{1-\sqrt{-3}}{2}\right)$ , the cyclotomic field  $\mathbb{Q}(\zeta_3)$  is the same as the imaginary quadratic field  $\mathbb{Q}(\sqrt{-3})$ . There is an element  $\tau \in \mathbb{Z}[\zeta_3]$  with  $\tau^2 = -3$  but not one with  $\tau^2 = 3$ .

But take heart: finding a square root of  $p$  in  $\mathbb{Q}(\zeta_p)$  isn't exactly what we wanted anyway. Recall that a strange factor of  $\pm 1$  according to whether  $p \equiv \pm 1 \pmod{4}$  is the hallmark of quadratic reciprocity. So actually we are on the right track.

Now, like a *deus ex machina* comes the **Gauss sum**:<sup>2</sup>

$$\tau := \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t.$$

In other words, we sum up all the  $p$ th roots of unity, but we insert  $\pm 1$  signs in front of them according to a very particular recipe. This looks a bit like a random walk in the complex plane with  $p$  steps of unit length. A probabilist would guess that the magnitude of the complex number  $\tau$  is roughly  $\sqrt{p}$ .<sup>3</sup> Well, it is our lucky day:

**Theorem 4.** (*Gauss*)

$$\tau^2 = (-1)^{\frac{p-1}{2}} p.$$

That is,  $|\tau| = \sqrt{p}$  on the nose! The extra factor of  $(-1)^{\frac{p-1}{2}}$  is more than welcome, since it appears in the quadratic reciprocity law. In fact, we define  $p^* = (-1)^{\frac{p-1}{2}} p$ , and then it is entirely straightforward to check the following

<sup>2</sup>We make the convention that from now until the end of the handout, all sums extend over  $0 \leq i \leq p-1$ .

<sup>3</sup>Much more on this, the **philosophy of almost square root error**, can be found in the analytic number theory part of these notes.

**Lemma 5.** *The quadratic reciprocity law is equivalent to the fact that for distinct odd primes  $p$  and  $q$ , we have*

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

Proof: Exercise.

Remarkably, we can now push through a proof as in the last section:

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

and suddenly our way is clear: multiply by  $\tau$  to get

$$(2) \quad \tau^q \equiv \left(\frac{p^*}{q}\right) \tau \pmod{q}.$$

On the other hand, we have

$$\tau^q \equiv \left(\sum_t \left(\frac{t}{p}\right) \zeta^t\right)^q \equiv \sum_t \left(\frac{t}{p}\right) \zeta^{qt} \pmod{q}.$$

Now, since  $q$  is prime to  $p$  and hence to the order of  $\zeta$ , the elements  $\zeta^{qt}$  still run through all distinct  $p$ th roots of unity as  $t$  runs from 0 to  $p-1$ . In other words, we can make the change of variable  $t \mapsto q^{-1}t$  and then the sum becomes

$$\sum_t \left(\frac{q^{-1}t}{p}\right) \zeta^t = \left(\frac{q^{-1}}{p}\right) \sum_t \left(\frac{t}{p}\right) \zeta^t = \left(\frac{q}{p}\right) \tau.$$

So we win: substituting this into (2) we get

$$\left(\frac{q}{p}\right) \tau \equiv \left(\frac{p^*}{q}\right) \tau \pmod{q},$$

and multiplying through by  $\tau$  we get an ordinary congruence

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod{q};$$

since  $p^*$  is prime to  $q$ , we may cancel to get

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q},$$

and finally that

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

#### 4. ... THE COMPUTATION OF THE GAUSS SUM

Of course, it remains to prove Theorem 4. We wish to show that if

$$\tau = \sum_t \left(\frac{t}{p}\right) \zeta^t,$$

then

$$\tau^2 = p^* = (-1)^{\frac{p-1}{2}} p.$$

We do this by introducing a slightly more general sum: for any integer  $a$ , we define

$$\tau_a := \sum_t \left(\frac{t}{p}\right) \zeta^{at}.$$

If  $a \equiv 0 \pmod{p}$ , then

$$\tau_a = \sum_t \left(\frac{t}{p}\right) \zeta^{ap} = \sum_t \left(\frac{t}{p}\right).$$

Notice that  $\tau_a$  came up in the proof of the quadratic reciprocity law and we quickly rewrote it in terms of  $\tau$ . That argument still works here, to give:

$$\tau_a = \left(\frac{a}{p}\right) \tau.$$

Now we will evaluate the sum  $\sum_a \tau_a \tau_{-a}$  in two different ways. First, if  $a \neq 0$ , then

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

On the other hand

$$\tau_0 = \sum_t \left(\frac{t}{p}\right) \zeta^{0t} = \sum_t \left(\frac{t}{p}\right) = 0,$$

since each nonzero quadratic residue mod  $p$  contributes  $+1$ , each quadratic non-residue contributes  $-1$ , and we have an equal number of each. It follows that

$$\sum_a \tau_a \tau_{-a} = (-1)^{\frac{p-1}{2}} (p-1) \tau^2.$$

We also have

$$\tau_a \tau_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)}.$$

**Lemma 6.**

- a) If  $a \equiv 0 \pmod{p}$ , then  $\sum_t \zeta^{at} = p$ ;
- b) Otherwise  $\sum_t \zeta^{at} = 0$ .

The proof is easy. So interchanging the summations we get

$$\sum_a \tau_a \tau_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \sum_a \zeta^{a(x-y)}.$$

The inner sum is 0 for all  $x \neq y$ , and the outer sum is 0 when  $x = y = 0$ . For each of the remaining  $p-1$  values of  $x = y$ , we get a contribution to the sum of  $p$ , so

$$\sum_a \tau_a \tau_{-a} = (p-1)p.$$

Equating our two expressions for  $\sum_a \tau_a \tau_{-a}$  gives

$$(p-1)p = (-1)^{\frac{p-1}{2}} (p-1) \tau^2,$$

which gives the desired result:

$$\tau^2 = (-1)^{\frac{p-1}{2}} p = p^*.$$

## 5. COMMENTS

Working through this proof feels a little bit like being an accountant who has been assigned to carefully document a miracle. Nevertheless, every single proof I have seen feels this way, sometimes to an even greater extent. At least in this proof the miracle can be “bottled”: there are many fruitful generalizations of Gauss sums, which can be used to prove an amazing variety of results in mathematics, from number theory to partial differential equations (really!).

The proof just given is a modern formulation of Gauss’ sixth and last proof, in which his polynomial identities have been replaced by more explicit reference to algebraic integers. In particular I took the proof from the wonderful text of Ireland and Rosen, with only very minor expository modifications. In addition to being no harder than any other proof of QR that I have ever seen, it has other merits: first, it shows that the cyclotomic field  $\mathbb{Q}(\zeta_p)$  contains the quadratic field  $\mathbb{Q}(\sqrt{p^*})$  – in fact, Galois theory shows that this is the *unique* quadratic field contained in  $\mathbb{Q}$  – a fact which comes up again and again in algebraic number theory. Second, the proof can be adapted with relative ease to prove certain generalizations of the quadratic reciprocity law to cubic and biquadratic residues (for this see Ireland and Rosen again). These higher reciprocity laws were much sought by Gauss but found only by his student Eisenstein (not the filmmaker).

Finally, we mention that the Gauss sum can be made to look more like the “Gaussians” one studies in continuous mathematics: you are asked in the homework to show that

$$\tau = \sum_t e^{\frac{2\pi it^2}{p}}.$$