HOW TO STUMBLE ONTO A PROOF OF QUADRATIC RECIPROCITY

(IF YOU HAPPEN TO BE COMFORTABLE WITH GAUSS SUMS)

LEO GOLDMAKHER

ABSTRACT. This is my favorite proof of Quadratic Reciprocity. It's short, conceptual, and easy to motivate, and is one of just two proofs of QR that I can reconstruct from memory on the fly. The proof is classical—a simplification (discovered by a number of mathematicians, including Cauchy, Eisenstein, and Jacobi) of Gauss' sixth proof—and is described in many places, e.g., in Ireland and Rosen's *A classical introduction to modern number theory*. My only (very slight!) innovation is to attempt to describe how one might invent this proof.

1. PROOF OF QUADRATIC RECIPROCITY

Our goal is to deduce Quadratic Reciprocity from basic facts about Gauss sums, most importantly, that

$$\Big| \underbrace{\sum_{a \in \mathbb{F}_p^\times} \chi(a) e\Big(\frac{a}{p}\Big)}_{\tau(\chi)} \Big| = \sqrt{p} \qquad \text{for all nontrivial } \chi \pmod p. \tag{1.1}$$

Here $\mathbb{F}_p^\times := \{1, 2, \dots, p-1\}$, $e(\alpha) := e^{2\pi i \alpha}$, and the quantity $\tau(\chi)$ inside the absolute values is the Gauss sum. I will assume familiarity with Gauss sums, but for completeness I review all relevant properties in section 2.

Quadratic Reciprocity is concerned with the Legendre symbol, so henceforth we work with the character $\chi(n) := \left(\frac{n}{p}\right)$. For this choice of character we can simplify (1.1) to

$$\tau(\chi)^2 = \chi(-1)p \tag{1.2}$$

(again, see section 2 for details). Since our goal is to get to QR, we need to involve $\left(\frac{p}{q}\right)$ somehow. The most expedient way to do this is to use Euler's identity for the Legendre symbol: raising both sides of (1.2) to the power $\frac{q-1}{2}$ yields

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

It's not immediately clear that we've made progress towards QR, but observe that $\chi(-1) = (-1)^{\frac{p-1}{2}}$. Thus our congruence can be rewritten

$$\tau(\chi)^{q-1} \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) \bmod q, \tag{1.3}$$

which suddenly looks extremely close to the statement of QR. This motivates us to state and prove

Proposition 1.1. *If $\chi \pmod p$ is the quadratic character and q is an odd prime different from p, then*

$$\tau(\chi)^{q-1} \equiv \chi(q) \bmod q.$$

Proof. It's not obvious how to simplify $\tau(\chi)^{q-1} \bmod q$, so we look for closely related quantities that are simpler to manipulate. Since $\tau(\chi)$ is a sum and q^{th} powers of sums reduce very nicely mod q (sometimes called the 'freshman's dream': $(x+y)^q \equiv x^q + y^q \bmod q$), we're led to consider

$$\tau(\chi)^q = \Big(\sum_{a \in \mathbb{F}_p^\times} \chi(a) e\Big(\frac{a}{p}\Big) \Big)^q \equiv \sum_{a \in \mathbb{F}_p^\times} \chi(a)^q e\Big(\frac{a}{p}\Big)^q \bmod q \equiv \sum_{a \in \mathbb{F}_p^\times} \chi(a) e\Big(\frac{aq}{p}\Big) \bmod q.$$

The sum on the right hand side smacks of $\tau(\chi)$, and we can make this connection explicit:

$$\sum_{a \in \mathbb{F}_p^\times} \chi(a) e\Big(\frac{aq}{p}\Big) = \chi(q)^2 \sum_{a \in \mathbb{F}_p^\times} \chi(a) e\Big(\frac{aq}{p}\Big) = \chi(q)\tau(\chi).$$

Putting everything together, we find $\tau(\chi)^q \equiv \chi(q)\tau(\chi) \bmod q$; dividing both sides by $\tau(\chi)$ proves the claim!

Alas, it's not quite so simple, because there's an important nuance we overlooked: (1.1) implies $\tau(\chi)^q$ isn't an integer, so what on earth does it mean to reduce $\tau(\chi)^q$ mod q? Our approach, which seemed so clear cut and correct at first glance, is broken. But let's try to salvage what we can. It's true that $\tau(\chi)^q$ isn't a rational integer, but it *is* an integer in the cyclotomic field $\mathbb{Q}(\zeta_p)$. What if we work in this setting instead of $\mathbb{Z}$? Our earlier computations all go through verbatim over $\mathbb{Z}[\zeta_p]$, and we conclude

$$\tau(\chi)^q \equiv \chi(q)\tau(\chi) \bmod q$$

(where both sides are elements of $\mathbb{Z}[\zeta_p]$). This work-around comes at a cost, however: $\mathbb{Z}[\zeta_p]/(q)$ might not be an integral domain, since it's possible that q factors in $\mathbb{Z}[\zeta_p]$, so we might not be able to divide both sides by $\tau(\chi)$. Still, we've arrived at something that seems tantalizingly close to what we want. What could we do other than divide? Multiply, of course! Multiplying both sides by $\tau(\chi)$ yields

$$\tau(\chi)^{q-1}\tau(\chi)^2 = \tau(\chi)^{q+1} \equiv \chi(q)\tau(\chi)^2 \bmod q.$$

Now observe that the quantities $\tau(\chi)^{q-1}$, $\tau(\chi)^2$, and $\chi(q)$ are all *rational* integers, so this congruence holds over $\mathbb{Z}$... which means division is back on the table. Dividing both sides by $\tau(\chi)^2$ yields the claim. □

Plugging the result of Proposition 1.1 into equation (1.3) yields Quadratic Reciprocity mod q; since $q \geq 3$, this implies Quadratic Reciprocity itself. We've stumbled our way to a proof of QR!

2. Properties of Gauss sums

In our arguments above we employed just a few basic properties of Gauss sums. All of these are classical (going back to Gauss), and all rely on two observations: $\alpha\mathbb{F}_p^\times = \mathbb{F}_p^\times$ for any $\alpha \in \mathbb{F}_p^\times$, and $\sum_{a\in\mathbb{F}_p^\times} \chi(a) = 0$ for any nontrivial χ (mod p).

Proposition 2.1. *$|\tau(\chi)| = \sqrt{p}$ for any nontrivial χ (mod p).*

Proof. We have

$$|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \sum_{a,b\in\mathbb{F}_p^\times} \chi(a)e\Big(\frac{a}{p}\Big)\overline{\chi(b)}e\Big(\frac{-b}{p}\Big) = \sum_{a,b\in\mathbb{F}_p^\times} \chi(a\bar{b})e\Big(\frac{a-b}{p}\Big),$$

where $\bar{b}$ denotes the multiplicative inverse of b (mod p). Setting $h := a\bar{b}$ yields

$$|\tau(\chi)|^2 = \sum_{h\in\mathbb{F}_p^\times} \chi(h) \sum_{b\in\mathbb{F}_p^\times} e\Big(\frac{b(h-1)}{p}\Big).$$

Since the inner sum is -1 for all $h \neq 1$ and is $p-1$ for $h = 1$, we deduce $|\tau(\chi)|^2 = p$ as claimed. □

Proposition 2.2. *For any integer ℓ we have* $\displaystyle\sum_{a\in\mathbb{F}_p^\times} \chi(a)e\Big(\frac{a\ell}{p}\Big) = \overline{\chi(\ell)}\tau(\chi)\,.$

Proof. If $\ell \equiv 0$ (mod p), the claim holds by orthogonality of characters. If $\ell \not\equiv 0$ (mod p), then

$$\chi(\ell)\sum_{a\in\mathbb{F}_p^\times} \chi(a)e\Big(\frac{a\ell}{p}\Big) = \sum_{a\in\mathbb{F}_p^\times} \chi(a\ell)e\Big(\frac{a\ell}{p}\Big) = \sum_{k\in\mathbb{F}_p^\times} \chi(k)e\Big(\frac{k}{p}\Big) = \tau(\chi).$$ □

Proposition 2.3. *If $\chi(n) = \left(\frac{n}{p}\right)$, then $\tau(\chi)^2 = \chi(-1)p$.*

Proof. Since $\overline{\chi} = \chi$, we have

$$\overline{\tau(\chi)} = \sum_{a\in\mathbb{F}_p^\times} \chi(a)e\Big(-\frac{a}{p}\Big) = \sum_{a\in\mathbb{F}_p^\times} \chi(-a)e\Big(\frac{a}{p}\Big) = \chi(-1)\tau(\chi).$$

Combining this with Proposition 2.1 yields the claim. □

3. Concluding remarks

Although I included a refresher on Gauss sums, I think this proof of Quadratic Reciprocity is only effective for someone who is already familiar with properties of $\tau(\chi)$. Of course, it's possible to use this proof to *motivate* the study of $\tau(\chi)$, but I think this approach would be a disservice to both Gauss sums and this proof of QR, making them seem ad hoc.

For me, there exist far more natural contexts for becoming acquainted with Gauss sums. Perhaps the most famous appearance of $\tau(\chi)$ is in the *root number*, a factor involved in the functional equation for Dirichlet L-functions. This is certainly a strong motivation for defining and studying the Gauss sum, but the functional equation is quite technical and daunting for someone exploring number theory for the first time, and I'm not at all convinced this is the best place to become acquainted with Gauss sums.

A simpler motivation comes from the discrete fourier transform. Given a character $\chi \pmod p$, it's natural to wonder what its fourier transform is. Some computation yields

$$\widehat{\chi} = \frac{\chi(-1)\tau(\chi)}{\sqrt{p}}\overline{\chi},$$

so the Gauss sum appears naturally. A different appearance of Gauss sums is in the so-called *twisted Poisson summation* formula

$$\sum_{n\in\mathbb{Z}} f\left(\frac{n}{N}\right)\chi(n) = \frac{\tau(\chi)}{p/N}\sum_{\ell\in\mathbb{Z}}\widehat{f}\left(\frac{\ell}{p/N}\right)\overline{\chi}(\ell),$$

which holds for any $f : \mathbb{R} \to \mathbb{R}$ satisfying $|f(t)| + |\widehat{f}(t)| \ll (1+|t|)^{-1-\delta}$ for some $\delta > 0$. Yet another appearance is in the study of character sums: Pólya and Vinogradov independently proved that

$$\sum_{n\le t}\chi(n) = \frac{\tau(\chi)}{2\pi i}\sum_{1\le|n|\le p}\frac{\overline{\chi}(n)}{n}\left(1 - e\Big(-\frac{nt}{p}\Big)\right) + O(\log p).$$

In short, I think the best introduction to Gauss sums is in the context of fourier analysis on $\mathbb{F}_p^\times$, not in the context of L-functions or quadratic reciprocity.

Dept of Mathematics and Statistics, Williams College, Williamstown, MA, USA 01267
Email address: Leo.Goldmakher@williams.edu