Tutorial : Quadratic Reciprocity

Reciprocity Theorems: why do they happen? why are they important? Every time I see a proof of quadratic reciprocity it's usually at the end of a textbook just to show off all the "concepts" we have learned. For me, the argument's tell me it's true but if we are trying to solve the equiation:

$$x^2 \equiv p \pmod{q}$$

it doesn't explain why $p \leftrightarrow q$ should be possible, why these numbers should be on equal footing. And if we look at other "reciprocity theorems" can their proofs be told in "elementary" language i.e. with numbers!

These days I find the Legendre symbol misleading. Let's try another way:

$$\Big[x^2 \equiv p \pmod{q}\Big] \leftrightarrow \Big[x^2 \equiv q \pmod{p}\Big]$$

except this is not true when but $p = 4k + 3$ and $q = 4k + 3$ then we have the opposite

$$\Big[x^2 \equiv p \pmod{q}\Big] \leftrightarrow \Big[x^2 \not\equiv q \pmod{p}\Big]$$

How is this applied in the real world? I think that's an open question. All I can say is that the concept of the integers $\mathbb{Z}$ becomes are scaffolding for understanding a chaotic world, that really has no intrinsic concept of number.[1]

Can you come up with a better concept than $\mathbf{0}$ or better than $\mathbb{Z}$? No.

Usually the justification is that Quadratic Reciprocity is connect to other branches of mathematics. Let's try:

$$\big[\text{fermat's little theorem(s)}\big] \to \big[\text{QR}\big] \to \big[\text{three squares}\big] \to \big[\text{Banach-Tarski paradox}\big]$$

[1] Why is there no **dynamical systems** proof of Quadratic Reciprocity? We will not discuss cryptrography in any way, but maywe we could discuss **coding** or **information theory**. Just, number theory is to as "applied" as one would like. Philosophically it's about abstracting away from the real world something extremely pure.

A Wikipedia has a separate page for proofs of Quadratic Reciprocity. Let's try the willy-nilly Eisenstein proof, which I despise.

Theorem **98** of Hardy's "Introduction to the Theory of Numbers" states:

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

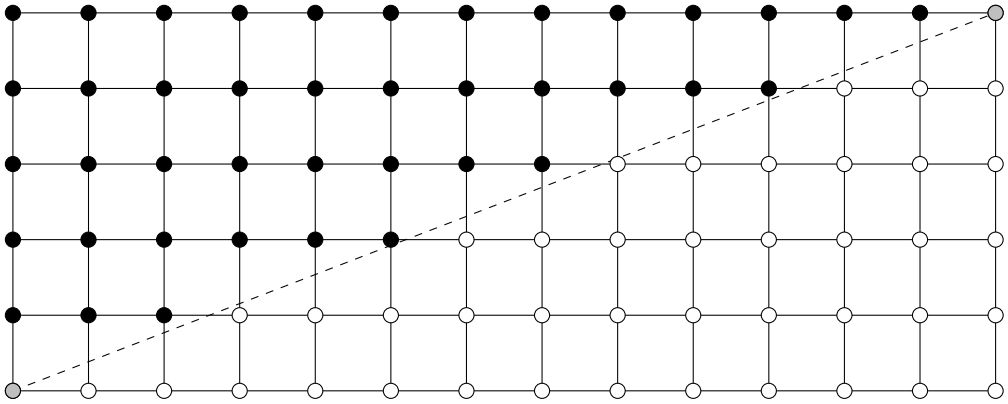
for any two odd primes p and q. And **99**=**98** splitting into the two cases:

$$x^2 \equiv q \pmod{p} \quad \leftrightarrow \quad x^2 \not\equiv p \pmod{q} \quad \text{if } p = 4k+3, q = 4k+3$$

$$x^2 \equiv q \pmod{p} \quad \leftrightarrow \quad x^2 \equiv p \pmod{q} \quad \text{otherwise}$$

And there is theorem **100** which is a lemma about lattice point counting:

$$\sum_{s=1}^{\frac{p-1}{2}} \left[\frac{s\,q}{p}\right] + \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{s\,p}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$



Finally there is Lemma **92** "Gauss Lemma"

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

where $\mu = \left(m \times \{1, 2, \ldots, \frac{p-1}{2}\}\right) \cap \{1, 2, \ldots, \frac{p-1}{2}\}$. We multiplyl the numbers between 0 and $\frac{p-1}{2}$ take the mod p operation and see if it returns to that range.

The chapter of the book is called **Fermat's Theorem and It's Consequences** so if that's not a hint I don't what is.

We might also use Lemma **83**

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

Hardy placed his discussion of Quadratric Reciprocity after: two chapters on primes, a chapter on the "Geometry of Numbers" (e.g. $0 < \frac{1}{3} < \frac{1}{2} < \frac{2}{3} < 1$), a chapter on Irrational numbers (which uses integrals $\int$, he proves e is irrational.) and a Chapter on congruences. These days I take it to mean that QR should't really matter much to you, unless you've explored $\mathbb{R}$ first, and then we'll need those pure, crystalline properties of $\mathbb{Z}$.

B QR contains Fermat's two-squares theorem: $\left[p = a^2 + b^2\right] \leftrightarrow \left[p = 4k + 1\right]$.

I see that Quadratic Reciprcity rested on a develop of the notion geometry of numbers and actions of the permutation group. We may have taken advantage of modern ideas like "scissors congruence" in the proof of the Eisenstein lemma.[2]

Quadratric reciprocity contains all of these two-squares kind of statement.

$$\begin{aligned} p = x^2 + 2\,y^2 &= p \equiv 1, 3 \ (8) \\ p = x^2 + 3\,y^2 &= p \equiv 1 \quad (3) \end{aligned}$$

It takes a "descent" step to turn these $\mathbb{Z}/p\mathbb{Z}$ statements into statements over $\mathbb{Z}$. We can conclude

splitting of primes = reciprocity = Fermat descent

Number theorists condense all of this into **Abelian Class Field Theory**. Quadratic residues and sums of squares type questions seem to be related.

What are some of these newer reciprocity statements like? These things used hard to find in the literature, have these lovely textbooks, stated in (relatively) basic language.

C Zolotarev's proof of Quadratic Reciprocity should come as no surprise, since if you really wanted to, could write the entire thing in terms of factorials and cogruences.[3] We could eximaine the group isomorhism:

$$(\mathbb{Z}/p\mathbb{Z})^\times \oplus (\mathbb{Z}/q\mathbb{Z})^\times \simeq (\mathbb{Z}/pq\mathbb{Z})^\times$$

This is known as the Chinese remainder theorem. Tautologically $p \times q \simeq pq$ but we are asked to find the isomorphism:

$$\left[a \in (\mathbb{Z}/p\mathbb{Z})^\times\right] \mapsto \left[(a, 1) \in (\mathbb{Z}/p\mathbb{Z})^\times \oplus (\mathbb{Z}/q\mathbb{Z})^\times\right]$$

Both groups are cyclic (they have size $p - 1$ and $q - 1$) and these numbers are **not** relatively prime. They have a common factor of 2. And this lifts to groups[4]

$$\{1, -1\} \oplus \{1, -1\} = (\mathbb{Z}/2\mathbb{Z})^+ \oplus (\mathbb{Z}/2\mathbb{Z})^+ \subseteq (\mathbb{Z}/p\mathbb{Z})^\times \oplus (\mathbb{Z}/q\mathbb{Z})^\times$$

We don't know about the behavior of $\sqrt{-1}$ in these settings. Then we are going to count "carefully" where this careful counting hopefully has a name already...

---

[2] Hardy placed his discussion of Quadratric Reciprocity after:

- two chapters on primes,
- a chapter on the "Geometry of Numbers" (e.g. $0 < \frac{1}{3} < \frac{1}{2} < \frac{2}{3} < 1$),
- a chapter on Irrational numbers (which uses integrals $\int$, he proves e is irrational.)
- and a Chapter on congruences.

These days I take it to mean that QR should't really matter much to you, unless you've explored $\mathbb{R}$ first, and then we'll need those pure, crystalline properties of $\mathbb{Z}$.

[3] This would be the proof of **Rousseau**.

[4] and perhaps group-like objects

References

(1) Masanori Morishita **Knots and Primes** (Universitext) Springer, 2012.

(2) Anton Deitmar **Automorphic Forms** (Universitext) Springer, 2013.

(3) Nancy Childress **Class Field Theory** (Universitext) Springer, 2009.

(4) Jared Weinstein **Reciprocity Laws and Galois Representations: Recent Breakthroughs** Bull. Amer. Math. Soc. 53 (2016), 1-39 https://doi.org/10.1090/bull/1515