Power Reciprocity Law

Pitchayut Saengrungkongka

November 25, 2025

These notes were written in preparation to the 1-hour seminar talk given at MOP 2024.

Throughout these notes, let $\zeta_n = e^{2\pi i/n}$.

§1 Quadratic Reciprocity

Definition 1 (Legendre Symbol)**.**

For any integer a and prime p, define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & \text{there exists } x \text{ s.t. } x^2 \equiv a \pmod{p} \\ -1 & \text{there is no } x \text{ s.t. } x^2 \equiv a \pmod{p}. \end{cases}$$

Proposition 2.

For any integer a and odd prime p, we have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Theorem 3 (Quadratic Reciprocity)**.**

For any odd primes $p \neq q$, we have

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

This theorem implies, for example, that whether there exists a solution to $x^2 \equiv 5 \pmod{p}$ only depends on $p \bmod 20$.

There are many, many proofs of this theorem. I will show the proof that I think is the most conceptual. The idea of the proof is also generalized to various reciprocity laws and stems the development of algebraic number theory.

There two key components of the proof.

- In mod p, we have $(x+y)^p = x^p + y^p$. In particular, the difference has all coefficients divisible by p.
- For any odd prime q, $\sqrt{q}$ can be expressed as a sum of roots of unity.

Specifically, suppose that $\sqrt{q} = \zeta_1 + \zeta_2 + \cdots + \zeta_n$, where ζ_j are roots of unity. Then, in modulo p, we have

$$(\sqrt{q})^p = \zeta_1^p + \zeta_2^p + \cdots + \zeta_n^p,$$

and we want to figure out whether this is $\sqrt{q}$ (in which case, $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, so $\left(\frac{q}{p}\right) = 1$) or $-\sqrt{q}$ (in which case, $\left(\frac{q}{p}\right) = -1$). Exponentiating roots of unity is easy.

It's worth remarking that we are no longer work in $\mathbb{F}_p$, but we are working on the **algebraic closure** of $\mathbb{F}_p$ (denoted $\overline{\mathbb{F}}_p$), which means that we adjoin all roots of polynomials in $\mathbb{F}_p$. We won't go into details of how this is constructed, but the result is that we can add, subtract, multiply, and divide normally.

We now actually introduce how to express $\sqrt{q}$ is a sum of roots of unity.

Theorem 4 (Quadratic Gauss Sum)**.**

For any odd prime q, if $\zeta = e^{2\pi i/q}$, then we have

$$G(q) := \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta_q^a = \begin{cases} \pm\sqrt{q} & q \equiv 1 \pmod{4} \\ \pm i\sqrt{q} & q \equiv 3 \pmod{4} \end{cases}$$

Remark 5.

The signs turn out to be $+$ in both cases. This has an elementary proof, but it is much harder.

▶ *Proof.* We square the sum:

$$\begin{aligned} G(q)^2 &= \sum_{a=0}^{q-1}\sum_{b=0}^{q-1} \left(\frac{ab}{q}\right) \zeta_q^{a+b} \\ &= \sum_{t=0}^{q-1}\sum_{a=0}^{q-1} \left(\frac{a(t-a)}{q}\right) \zeta_q^{t} \\ &= \sum_{t=0}^{q-1} \zeta_q^t \sum_{a=1}^{q-1} \left(\frac{t/a-1}{q}\right) \\ &= \underbrace{(q-1)\left(\frac{-1}{q}\right)}_{t=0} + \sum_{t=1}^{q-1} \zeta_q^t \left(-\left(\frac{-1}{q}\right)\right) \\ &= q\left(\frac{-1}{q}\right) \end{aligned}$$

□

▶ *Proof of Quadratic Reciprocity.* We let $q^* = q(-1)^{\frac{q-1}{2}}$. Thus, $G(q) = \pm\sqrt{q^*}$. For convenience, assume $G(q) = \sqrt{q^*}$. Work over $\overline{F}_p$. We have

$$\begin{aligned} G(q)\left(\frac{q^*}{p}\right) = (G(q))^p &= \left(\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta_q^a\right)^p \\ &= \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta_q^{ap} \\ &= \sum_{a=1}^{q-1} \left(\frac{ap}{q}\right) \zeta_q^{a} = \left(\frac{p}{q}\right) G(q). \end{aligned}$$

Multiplying this by $\sqrt{q}^*$ gives $q^*\left(\frac{q^*}{p}\right) = q^*\left(\frac{p}{q}\right)$, and dividing by $q^* \neq 0$ gives $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$ in $\mathbb{F}_p$. Hence, we have $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$, and this establish quadratic reciprocity. □

§2 Cubic Reciprocity

The only fact we need to make the "raise to the power of p" argument work is that $\sqrt{q}$ can be expressed as a sum of roots of unity. To cast this in a more general settings, consider an irreducible polynomial f with root α, then **if α can be written as a sum of roots of unity, then there exists m such that how f splits in $\mathbb{F}_p$ only depends on p mod m.** For example, we can show that $x^3 - 3x + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p = 3$ or $p \equiv \pm 1 \pmod{9}$.

We are now interested in generalizing quadratic reciprocity to higher power. Specifically, characterize all prime p for which $x^3 \equiv a \pmod{p}$ has a solution for a fixed a. This would have been easy of $\sqrt[3]{a}$ can be expressed as roots of unity. However, with Galois theory, we can show that $\sqrt[3]{a}$ is not a sum of roots of unity, so we are sad.

To do this, we need to work in different number field. Consider $\mathbb{Z}[\zeta_3]$, where $\zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = e^{2\pi i/3}$. Each element $\alpha \in \mathbb{Z}[\zeta_3]$ has a **norm** $\mathrm{N}(\alpha) = |\alpha|^2$, which is multiplicative. Unique factorization holds in $\mathbb{Z}[\zeta_3]$. Moreover, we have

- primes $p \equiv 1 \pmod{3}$ will split into two conjugate primes (e.g., $7 = (3+\zeta_3)(3+\zeta_3^2) = (3+\zeta_3)(2-\zeta_3)$); each factor has norm p
- primes $\equiv 2 \pmod{3}$ do not factor (i.e., remain prime in $\mathbb{Z}[\zeta_3]$).

However, we need to be careful with **units**, elements u for which $u^{-1} \in \mathbb{Z}[\zeta_3]$. There are six of them: $\pm 1, \pm\zeta_3, \pm\zeta_3^2$.

Example 6.

Consider prime $3 + \zeta_3$ (factor of 7). Up to multiplication by unit, there are six choices: $3+\zeta_3$, $-3-\zeta_3$, $3\zeta_3 + \zeta_3^2 = -1 + 2\zeta_3$, $1 - 2\zeta_3$, $1 + 3\zeta_3^2 = -2 - 3\zeta_3$, and $2 + 3\zeta_3$.

We will pick the representative that is $\boldsymbol{\equiv 2 \pmod{3}}$. In particular, we will pick $2 + 3\zeta_3$ in this case.

Definition 7.

An element π is **primary** if and only if it is $\pi \equiv 2 \pmod{3}$.

Definition 8 (Cubic Residue Symbol)**.**

For any $\alpha \in \mathbb{Z}[\zeta_3]$ and primary π, define

$$\left(\frac{\alpha}{\pi}\right)_3 = \alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \bmod \pi \in \{1, \zeta_3, \zeta_3^2\}.$$

In particular, $\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff x^3 \equiv \alpha \pmod{\pi}$ has a solution. Moreover, $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3\left(\frac{\beta}{\pi}\right)_3$.

We now state the theorem.

Theorem 9 (Cubic Reciprocity).

For any primary primes $\pi_1, \pi_2 \in \mathbb{Z}[\zeta_3]$, we have

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

The proof of this theorem more techinical that quadratic reciprocity, but the spirit remains the same. We need to find something expressible as a sum of roots of unity. This time, we have the following key lemma.

Lemma 10.

Let $p \equiv 1 \pmod 3$ and suppose $p = \pi\overline{\pi}$ where π is primary. Let $\zeta_p = e^{2\pi i/p}$, then

$$\sqrt[3]{p\pi} = \sqrt[3]{\pi^2\overline{\pi}} = \sum_{a=1}^{p-1} \left(\frac{a}{\pi}\right)_3 \zeta_p^a.$$

The proof uses **Jacobi Sum** (the one that kills 2012 N8).

▶ *Proof Outline.* For two characters χ, ψ in $\mathbb{F}_p$, define Gauss sum and Jacobi sum

$$g(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta_p^t$$
$$J(\chi, \psi) = \sum_{t \in \mathbb{F}_p} \chi(t)\psi(1-t).$$

We can show that

$$|g(\chi)| = \sqrt{p} \text{ and } J(\chi, \psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}.$$

Now, let χ be the cubic residue character. We have $J(\chi, \chi) \in \mathbb{Z}[\zeta_3]$ and absolute value $\sqrt{p}$, so we can figure out the factorization. Using this with $J(\overline{\chi}, \overline{\chi})$ as well determins $g(\chi)$ and $g(\overline{\chi})$. □

§3 Introduction to Class Field Theory

The above proof idea can be easily adapted to fourth power, in which case whether $\sqrt[4]{a}$ exists in modulo p depends on how p factors in $\mathbb{Z}[i]$. The proof is pretty much the same as cubic.

We can even make this work to the n-th power reciprocity. In which case, we need to work with $\mathbb{Z}[\zeta_n]$ instead.

Notice that we are now getting into a lot of algebraic extensions of $\mathbb{Q}$ and $\mathbb{Z}$. **Algebraic Number Theory** is a subject that studies arbitrary extension of $\mathbb{Q}$ (i.e., adjoining arbitrary root of polynomials). The most annoying thing of this is that **not all such extension has unique factorization property**, and we have to work with a special kind of number, called **ideals** to make a finer distinction of primes.

One pinnacle result of algebraic number theory is class field theory, which is basically finding when such reciprocity laws work. In particular, for extension K, we want to characterize all extensions L for which the splitting behavior of things in L can be determined by a "simple" information from K. When $K = \mathbb{Q}$, the answer is only when L contains sums of roots of unity. However, things get much more complicated when K is arbitrary extension.

For any field extension L/K, we let $\mathrm{Gal}(L/K)$ be the group of field homomorphisms $L \to L$ that fixes K. For example,

- $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is the cyclic group of order 2 because there are two such automorphisms: the identity map and the one that sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$.
- If α is a root of cubic polynomial in $\mathbb{Q}[x]$, then $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is **usually** a group of the 6 permutations of $\{1, 2, 3\}$, determined by permutation of roots α, β, and γ of the cubic polynomial.

  (The only exception is when β has a nontrivial polynomial relation to α.)

Roughly speaking, Artin reciprocity states that

📝 **Theorem 11** (Artin Reciprocity, informal)**.**

If $\mathrm{Gal}(L/K)$ is abelian (any two elements are commutative), then how prime p splits in L is uniquely determined by the "modulo" information in K.

This generalizes basically all known reciprocity laws.

Here are some fun corollary from Artin Reciprocity that we will not prove.

📝 **Theorem 12.**

Let p be a prime. Then, p can be expressed in form $a^2 + 23b^2$ $(a, b \in \mathbb{Z})$ if and only if the polynomial $x^3 - x - 1$ factors into linear factors modulo p.