

# Quadratic Reciprocity

via Quadratic and Cyclotomic Fields

Tushar Muralidharan

Australian National University

November 2023

# Table of Contents

1 Introduction

2 A Proof

# Table of Contents

1 Introduction

2 A Proof

# What is Quadratic Reciprocity?

We say that  $a$  is a *quadratic residue modulo  $n$*  if  $a$  is congruent to a perfect square modulo  $n$ ; that is, if  $x^2 \equiv a \pmod{n}$  for some integer  $x$ .

## Definition

Let  $p$  be an odd prime. For any integer  $a$ , the *Legendre symbol*  $\left(\frac{a}{p}\right)$  is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

# What is Quadratic Reciprocity?

## Definition

Let  $p$  be an odd prime. For any integer  $a$ , the *Legendre symbol*  $\left(\frac{a}{p}\right)$  is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

## Theorem (Quadratic Reciprocity Law)

Let  $p$  and  $q$  be distinct odd primes. Then

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

# Why Should We Care?

*It is among the deepest and most beautiful results of elementary number theory and the beginning of a line of reciprocity theorems that culminate in the very general Artin reciprocity law, perhaps the most impressive theorem in all number theory.*

*Ireland and Rosen,  
A Classical Introduction to Modern Number Theory*

# Why Should We Care?

## Theorem (Quadratic Reciprocity Law)

*Let  $p$  and  $q$  be distinct odd primes. Then*

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

If we know whether  $p$  is a quadratic residue modulo  $q$ , then we can deduce whether  $q$  is a quadratic residue modulo  $p$ .

# Why Should We Care?

## Theorem (Quadratic Reciprocity Law)

Let  $p$  and  $q$  be distinct odd primes. Then

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

If we know whether  $p$  is a quadratic residue modulo  $q$ , then we can deduce whether  $q$  is a quadratic residue modulo  $p$ .

*If  $p$  and  $q$  are distinct odd primes, at least one of which is congruent to 1 modulo 4, then  $p$  is a quadratic residue modulo  $q$  if and only if  $q$  is a quadratic residue modulo  $p$ ; otherwise exactly one of  $p$  and  $q$  is a quadratic residue modulo the other.*

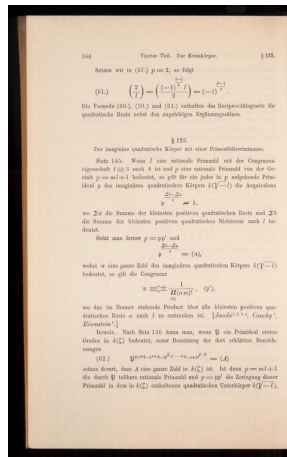
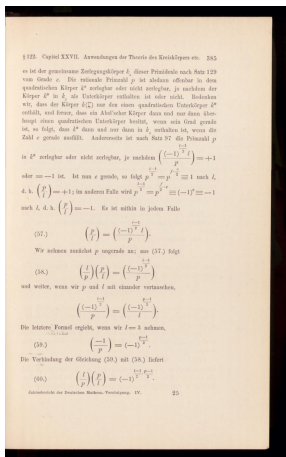
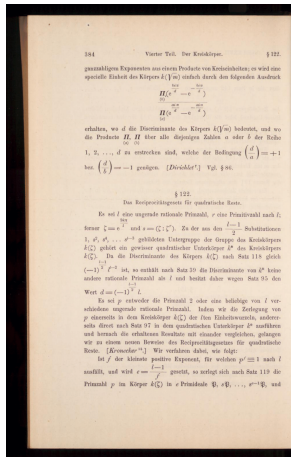


# Table of Contents

1 Introduction

2 A Proof

## We follow the proof of David Hilbert, given in his seminal work *Theory of Algebraic Number Fields* in 1896.



## Definition

Let  $\zeta_n$  be a primitive  $n$ -th root of unity. Then the  $n$ -th cyclotomic field is  $\mathbb{Q}(\zeta_n)$ .

Let  $p$  be an odd prime. This is where our proof starts. Later on, we'll choose an arbitrary distinct odd prime  $q$ .

## Definition

Let  $\zeta_n$  be a primitive  $n$ -th root of unity. Then the  $n$ -th cyclotomic field is  $\mathbb{Q}(\zeta_n)$ .

Let  $p$  be an odd prime. This is where our proof starts. Later on, we'll choose an arbitrary distinct odd prime  $q$ .

## Theorem

*There is an isomorphism*

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

*which sends the automorphism  $\sigma_a$  satisfying  $\sigma_a(\zeta_p) = \zeta_p^a$  to the residue  $a \bmod p$ .*

# Cyclotomic Fields

We have  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ . This is a cyclic group of even order, so there exists a unique subgroup  $H$  of  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  (the square elements) with order  $(p-1)/2$ . By the Fundamental Theorem of Galois Theory, this corresponds to a unique quadratic extension  $K$  of  $\mathbb{Q}$  contained in  $\mathbb{Q}(\zeta_p)$ .

# Cyclotomic Fields

We have  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ . This is a cyclic group of even order, so there exists a unique subgroup  $H$  of  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  (the square elements) with order  $(p-1)/2$ . By the Fundamental Theorem of Galois Theory, this corresponds to a unique quadratic extension  $K$  of  $\mathbb{Q}$  contained in  $\mathbb{Q}(\zeta_p)$ .

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

$$|$$

$$H$$

$$|$$

$$\{0\}$$

$$\mathbb{Q}$$

$$|$$

$$K$$

$$|$$

$$\mathbb{Q}(\zeta_p)$$

# Cyclotomic Fields

We have  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ . This is a cyclic group of even order, so there exists a unique subgroup  $H$  of  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  (the square elements) with order  $(p-1)/2$ . By the Fundamental Theorem of Galois Theory, this corresponds to a unique quadratic extension  $K$  of  $\mathbb{Q}$  contained in  $\mathbb{Q}(\zeta_p)$ .

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

$$|$$

$$H$$

$$|$$

$$\{0\}$$

$$\mathbb{Q}$$

$$|$$

$$K$$

$$|$$

$$\mathbb{Q}(\zeta_p)$$

We've shown that  $\mathbb{Q}(\zeta_p)$  **contains a unique quadratic subfield**. Write  $K = \mathbb{Q}(\sqrt{p^*})$  for some squarefree integer  $p^*$ .

We have the following result from Stevenhagen [1].

## Theorem

*A prime  $p$  ramifies in a number field  $K$  if and only if  $p$  divides the discriminant  $\Delta_K$ .*



# Cyclotomic Fields

We have the following result from Stevenhagen [1].

## Theorem

*A prime  $p$  ramifies in a number field  $K$  if and only if  $p$  divides the discriminant  $\Delta_K$ .*

We've seen that

$$\Delta_{\mathbb{Q}(\zeta_p)} = \Delta(\Phi_p) = (-1)^{(p-1)/2} N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\Phi'_p(\zeta_p)) = (-1)^{(p-1)/2} p^{p-2},$$

where  $\Phi_p(X) = \frac{X^p-1}{X-1} = \sum_{i=0}^{p-1} X^i$ . In particular,  $p$  is the only prime that divides the discriminant. The theorem tells us that  $p$  is the only prime that ramifies in  $\mathbb{Q}(\zeta_p)$ . Then  $p$  is the only possible prime that can ramify in  $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ . The theorem tells us that  $\Delta_{\mathbb{Q}(\sqrt{p^*})}$  **cannot have any prime divisors other than  $p$** . What is  $\Delta_{\mathbb{Q}(\sqrt{p^*})}$ ?

# Quadratic Fields

## Theorem

Let  $d \neq 1$  be a squarefree integer and  $K = \mathbb{Q}(\sqrt{d})$  the corresponding quadratic field. Then we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

# Quadratic Fields

## Theorem

Let  $d \neq 1$  be a squarefree integer and  $K = \mathbb{Q}(\sqrt{d})$  the corresponding quadratic field. Then we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

## Theorem

For a squarefree integer  $d \neq 1$ , the corresponding quadratic field  $K = \mathbb{Q}(\sqrt{d})$  has discriminant

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

## Theorem

*For a squarefree integer  $d \neq 1$ , the corresponding quadratic field  $K = \mathbb{Q}(\sqrt{d})$  has discriminant*

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Consider our quadratic subfield  $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ . Recall that  $\Delta_{\mathbb{Q}(\sqrt{p^*})}$  cannot have any prime divisors other than  $p$ , so we must have  $p^* \equiv 1 \pmod{4}$ .

# Quadratic Fields

## Theorem

*For a squarefree integer  $d \neq 1$ , the corresponding quadratic field  $K = \mathbb{Q}(\sqrt{d})$  has discriminant*

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Consider our quadratic subfield  $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ . Recall that  $\Delta_{\mathbb{Q}(\sqrt{p^*})}$  cannot have any prime divisors other than  $p$ , so we must have  $p^* \equiv 1 \pmod{4}$ . Since at least one prime divides  $p^*$ , we must have  $p \mid p^*$ .

# Quadratic Fields

## Theorem

*For a squarefree integer  $d \neq 1$ , the corresponding quadratic field  $K = \mathbb{Q}(\sqrt{d})$  has discriminant*

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Consider our quadratic subfield  $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ . Recall that  $\Delta_{\mathbb{Q}(\sqrt{p^*})}$  cannot have any prime divisors other than  $p$ , so we must have  $p^* \equiv 1 \pmod{4}$ . Since at least one prime divides  $p^*$ , we must have  $p \mid p^*$ . Then since  $p^*$  was assumed to be squarefree, we must have  $p^* = \pm p$ . Moreover,

$$p^* = \begin{cases} p & \text{if } p \equiv 1 \pmod{4} \\ -p & \text{if } p \equiv 3 \pmod{4} \end{cases} = (-1)^{(p-1)/2} p$$

so we have identified  $K$ .

# The Next Step

Let  $q$  be an odd prime distinct from  $p$ . This is the second arbitrary prime in the theorem. No primes other than  $p$  are ramified in  $\mathbb{Q}(\sqrt{p^*})$ , so  $q$  must be either split or inert.

We have the following result regarding quadratic fields from Stevenhagen [1].

## Theorem

*Let  $d \neq 1$  be squarefree and  $p$  an odd prime. Then  $p$  is split in  $\mathbb{Q}(\sqrt{d})$  for  $\left(\frac{d}{p}\right) = 1$ , inert for  $\left(\frac{d}{p}\right) = -1$ , and ramified for  $\left(\frac{d}{p}\right) = 0$ .*

Hence,  $q$  splits in  $K = \mathbb{Q}(\sqrt{p^*})$  if and only if  $\left(\frac{p^*}{q}\right) = 1$ .

# Some Useful Facts

Recall that  $H$  was defined to be the unique subgroup of square elements of  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong C_{p-1}$ . By the isomorphism

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times,$$

we may **identify  $H$  with the (nonzero) quadratic residues in  $(\mathbb{Z}/p\mathbb{Z})^\times$** .



# Some Useful Facts

Recall that  $H$  was defined to be the unique subgroup of square elements of  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong C_{p-1}$ . By the isomorphism

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times,$$

we may **identify  $H$  with the (nonzero) quadratic residues in  $(\mathbb{Z}/p\mathbb{Z})^\times$** . Also,

$$\begin{array}{c} \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ | \\ H \\ | \\ \{0\} \end{array}$$

$$\begin{array}{c} \mathbb{Q} \\ | \\ K \\ | \\ \mathbb{Q}(\zeta_p) \end{array}$$

By the Fundamental Theorem of Galois Theory,  $H \cong \text{Gal}(\mathbb{Q}(\zeta_p)/K)$ .

# Closing

Therefore, an automorphism  $\sigma_q \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  is in  $\text{Gal}(\mathbb{Q}(\zeta_p)/K)$  if and only if  $q$  is a quadratic residue modulo  $p$ , i.e.,  $\left(\frac{q}{p}\right) = 1$ .

# Closing

Therefore, an automorphism  $\sigma_q \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  is in  $\text{Gal}(\mathbb{Q}(\zeta_p)/K)$  if and only if  $q$  is a quadratic residue modulo  $p$ , i.e.,  $\left(\frac{q}{p}\right) = 1$ .

Now, the Galois group of the quadratic extension  $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$  has two elements: the identity map and the conjugation map  $\sqrt{p^*} \mapsto -\sqrt{p^*}$ . We identify  $\text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \{\pm 1\}$ .

Therefore, an automorphism  $\sigma_q \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$  is in  $\text{Gal}(\mathbb{Q}(\zeta_p)/K)$  if and only if  $q$  is a quadratic residue modulo  $p$ , i.e.,  $\left(\frac{q}{p}\right) = 1$ .

Now, the Galois group of the quadratic extension  $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$  has two elements: the identity map and the conjugation map  $\sqrt{p^*} \mapsto -\sqrt{p^*}$ . We identify  $\text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \{\pm 1\}$ .

Consider an automorphism  $\sigma_q$  in  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ . Let  $\sigma'_q$  be the restriction of  $\sigma_q$  on  $\mathbb{Q}(\sqrt{p^*})$ . Then  $\sigma'_q$  is the corresponding automorphism in  $\text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ . By Stevenhagen [1] (involving additional definitions), an element  $\sigma'_q$  in  $\text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$  is the identity if and only if  $q$  splits in  $\mathbb{Q}(\sqrt{p^*})$ , i.e.  $\left(\frac{p^*}{q}\right) = 1$ . However, the former condition is true if and only if  $\sigma_q$  fixes  $K = \mathbb{Q}(\sqrt{p^*})$ , i.e.  $\left(\frac{q}{p}\right) = 1$ .

The equivalence

$$\left(\frac{p^*}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1,$$

where

$$p^* = \begin{cases} p & \text{if } p \equiv 1 \pmod{4} \\ -p & \text{if } p \equiv 3 \pmod{4} \end{cases} = (-1)^{(p-1)/2} p$$

is what we need.

Since the Legendre symbol is multiplicative, we have

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

where we have used that  $-1$  is a square modulo  $p$  only if 4 divides  $p-1$ , so that  $\left(\frac{-1}{q}\right) = (-1)^{(p-1)/2}$ . This completes the proof of quadratic reciprocity. □

# Final Remarks

- The two Legendre symbols  $\left(\frac{p^*}{q}\right)$  and  $\left(\frac{q}{p}\right)$  secretly encoded information about the order of the Frobenius element  $\sigma_q$ .

# Final Remarks

- The two Legendre symbols  $\left(\frac{p^*}{q}\right)$  and  $\left(\frac{q}{p}\right)$  secretly encoded information about the order of the Frobenius element  $\sigma_q$ .
- The quadratic reciprocity law is sometimes accompanied by the supplementary result

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 5 \pmod{8}. \end{cases}$$





P. Stevenhagen (2019) *Number Rings*, Universiteit Leiden.