Quadratic reciprocity and higher reciprocity laws

Henry Twiss

University of Minnesota

May 2020

Outline

Outline

History

- Legendre (1785) proved the law of quadratic reciprocity in special cases.
- First complete proof due to Gauss (April 8, 1796).
- Gauss published six distinct proofs of the law before his death.
- By 1921 there were 56 know proofs.
- Eisenstein is credited with the proofs of the laws of cubic and biquadratic reciprocity.

History

- Legendre (1785) proved the law of quadratic reciprocity in special cases.
- First complete proof due to Gauss (April 8, 1796).
- Gauss published six distinct proofs of the law before his death.
- By 1921 there were 56 know proofs.
- Eisenstein is credited with the proofs of the laws of cubic and biquadratic reciprocity.

History

- Legendre (1785) proved the law of quadratic reciprocity in special cases.
- First complete proof due to Gauss (April 8, 1796).
- Gauss published six distinct proofs of the law before his death.
- By 1921 there were 56 know proofs.
- Eisenstein is credited with the proofs of the laws of cubic and biquadratic reciprocity.

History

- Legendre (1785) proved the law of quadratic reciprocity in special cases.
- First complete proof due to Gauss (April 8, 1796).
- Gauss published six distinct proofs of the law before his death.
- By 1921 there were 56 know proofs.
- Eisenstein is credited with the proofs of the laws of cubic and biquadratic reciprocity.

History

- Legendre (1785) proved the law of quadratic reciprocity in special cases.
- First complete proof due to Gauss (April 8, 1796).
- Gauss published six distinct proofs of the law before his death.
- By 1921 there were 56 know proofs.
- Eisenstein is credited with the proofs of the laws of cubic and biquadratic reciprocity.

Outline

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Congruences

Definition 2.1

If $a, b, m \in \mathbb{Z}$ with $m \neq 0$, we say that a is congruent to b modulo m if m divides $a - b$. This relation is written

$$a \equiv b \pmod{m}.$$

This is an equivalence relation on $\mathbb{Z}$. We say

$$\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$$

is the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of congruences classes modulo m. As a set, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. It is a ring under the operations

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}.$$

When $m = p$ a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

Let p be prime. It is an interesting question to ask when $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ has a square root in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to a solution to the equation

$$x^2 \equiv a \pmod{p}.$$

If this equation has a solution, we say a is a quadratic residue mod p; if not we say a is a quadratic nonresidue mod p. From now on we assume p is odd.

For example, 1^2, 2^2, 3^2, 4^2, 5^2, and 6^2 are congruent to 1, 4, 2, 2, 4, and 1, respectively mod 7. So 1, 2, and 4 are the quadratic residues mod 7 while 3, 5, and 6 are the nonresidues. This is a tedious process of finding quadratic residues!

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

It is natural to ask the following questions:

- If $x^2 \equiv a \pmod{p}$ has a solution, how many solutions are there?
- How many quadratic residues mod p are there?
- Is there a quick way to determine if a is a quadratic residue mod p?

The first question is easy to answer. If $a = 0$, $x = 0$ is the only solution, and if $a \neq 0$ then there are either zero or two solutions. The latter two questions are more difficult and will require the Legendre symbol.

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

It is natural to ask the following questions:

- If $x^2 \equiv a \pmod{p}$ has a solution, how many solutions are there?
- How many quadratic residues mod p are there?
- Is there a quick way to determine if a is a quadratic residue mod p?

The first question is easy to answer. If $a = 0$, $x = 0$ is the only solution, and if $a \neq 0$ then there are either zero or two solutions. The latter two questions are more difficult and will require the Legendre symbol.

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

It is natural to ask the following questions:

- If $x^2 \equiv a \pmod{p}$ has a solution, how many solutions are there?
- How many quadratic residues mod p are there?
- Is there a quick way to determine if a is a quadratic residue mod p?

The first question is easy to answer. If $a = 0$, $x = 0$ is the only solution, and if $a \neq 0$ then there are either zero or two solutions. The latter two questions are more difficult and will require the Legendre symbol.

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

It is natural to ask the following questions:

- If $x^2 \equiv a \pmod{p}$ has a solution, how many solutions are there?
- How many quadratic residues mod p are there?
- Is there a quick way to determine if a is a quadratic residue mod p?

The first question is easy to answer. If $a = 0$, $x = 0$ is the only solution, and if $a \neq 0$ then there are either zero or two solutions. The latter two questions are more difficult and will require the Legendre symbol.

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

It is natural to ask the following questions:

- If $x^2 \equiv a \pmod{p}$ has a solution, how many solutions are there?
- How many quadratic residues mod p are there?
- Is there a quick way to determine if a is a quadratic residue mod p?

The first question is easy to answer. If $a = 0$, $x = 0$ is the only solution, and if $a \neq 0$ then there are either zero or two solutions. The latter two questions are more difficult and will require the Legendre symbol.

Square Roots in $\mathbb{Z}/p\mathbb{Z}$

It is natural to ask the following questions:

- If $x^2 \equiv a \pmod{p}$ has a solution, how many solutions are there?
- How many quadratic residues mod p are there?
- Is there a quick way to determine if a is a quadratic residue mod p?

The first question is easy to answer. If $a = 0$, $x = 0$ is the only solution, and if $a \neq 0$ then there are either zero or two solutions. The latter two questions are more difficult and will require the Legendre symbol.

The Legendre Symbol

Definition 2.2

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol (a/p) is defined by

$$(a/p) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

It satisfies the following properties:

- $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.
- $(ab/p) = (a/p)(b/p)$.
- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

This induces a well-defined homomorphism

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p).$$

The Legendre Symbol

Definition 2.2

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol (a/p) is defined by

$$(a/p) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

It satisfies the following properties:

- $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.
- $(ab/p) = (a/p)(b/p)$.
- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

This induces a well-defined homomorphism

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p).$$

The Legendre Symbol

Definition 2.2

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol (a/p) is defined by

$$(a/p) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

It satisfies the following properties:

- $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.
- $(ab/p) = (a/p)(b/p)$.
- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

This induces a well-defined homomorphism

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p).$$

The Legendre Symbol

Definition 2.2

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol (a/p) is defined by

$$(a/p) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

It satisfies the following properties:

- $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.
- $(ab/p) = (a/p)(b/p)$.
- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

This induces a well-defined homomorphism

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p).$$

The Legendre Symbol

Definition 2.2

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol (a/p) is defined by

$$(a/p) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

It satisfies the following properties:

- $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.
- $(ab/p) = (a/p)(b/p)$.
- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

This induces a well-defined homomorphism

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p).$$

The Legendre Symbol

Definition 2.2

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol (a/p) is defined by

$$(a/p) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

It satisfies the following properties:

- $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.
- $(ab/p) = (a/p)(b/p)$.
- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

This induces a well-defined homomorphism

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p).$$

The Legendre Symbol

We can now answer the second question. Since

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p)$$

is a homomorphism, $\ker(-/p)$ (the set of quadratic residues) is an index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. So there are as many quadratic residues as nonresidues and they are $(p-1)/2$ in size.

We also have the supplementary laws:

$$(-1/p) = (-1)^{(p-1)/2} \quad \text{and} \quad (2/p) = (-1)^{(p^2-1)/8}.$$

They are both necessary to prove the law of quadratic reciprocity.

The Legendre Symbol

We can now answer the second question. Since

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p)$$

is a homomorphism, $\ker(-/p)$ (the set of quadratic residues) is an index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. So there are as many quadratic residues as nonresidues and they are $(p-1)/2$ in size.

We also have the supplementary laws:

$$(-1/p) = (-1)^{(p-1)/2} \quad \text{and} \quad (2/p) = (-1)^{(p^2-1)/8}.$$

They are both necessary to prove the law of quadratic reciprocity.

The Legendre Symbol

We can now answer the second question. Since

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p)$$

is a homomorphism, $\ker(-/p)$ (the set of quadratic residues) is an index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. So there are as many quadratic residues as nonresidues and they are $(p-1)/2$ in size.

We also have the supplementary laws:

$$(-1/p) = (-1)^{(p-1)/2} \quad \text{and} \quad (2/p) = (-1)^{(p^2-1)/8}.$$

They are both necessary to prove the law of quadratic reciprocity.

The Legendre Symbol

We can now answer the second question. Since

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p)$$

is a homomorphism, $\ker(-/p)$ (the set of quadratic residues) is an index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. So there are as many quadratic residues as nonresidues and they are $(p-1)/2$ in size.

We also have the supplementary laws:

$$(-1/p) = (-1)^{(p-1)/2} \quad \text{and} \quad (2/p) = (-1)^{(p^2-1)/8}.$$

They are both necessary to prove the law of quadratic reciprocity.

The Legendre Symbol

We can now answer the second question. Since

$$(-/p) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \qquad \bar{a} \mapsto (a/p)$$

is a homomorphism, $\ker(-/p)$ (the set of quadratic residues) is an index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. So there are as many quadratic residues as nonresidues and they are $(p-1)/2$ in size.

We also have the supplementary laws:

$$(-1/p) = (-1)^{(p-1)/2} \quad \text{and} \quad (2/p) = (-1)^{(p^2-1)/8}.$$

They are both necessary to prove the law of quadratic reciprocity.

Outline

The Law of Quadratic Reciprocity

The law of quadratic reciprocity relates (p/q) and (q/p).

Theorem 3.1

Let p and q be distinct odd primes. Then

$$(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}.$$

The law of quadratic reciprocity lets us compute (a/p) efficiently. In this respect, it answers our third question in the affirmative.

The Law of Quadratic Reciprocity

The law of quadratic reciprocity relates (p/q) and (q/p).

Theorem 3.1

Let p and q be distinct odd primes. Then

$$(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}.$$

The law of quadratic reciprocity lets us compute (a/p) efficiently. In this respect, it answers our third question in the affirmative.

The Law of Quadratic Reciprocity

The law of quadratic reciprocity relates (p/q) and (q/p).

Theorem 3.1

Let p and q be distinct odd primes. Then

$$(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}.$$

The law of quadratic reciprocity lets us compute (a/p) efficiently. In this respect, it answers our third question in the affirmative.

The Law of Quadratic Reciprocity

The law of quadratic reciprocity relates (p/q) and (q/p).

Theorem 3.1

Let p and q be distinct odd primes. Then

$$(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}.$$

The law of quadratic reciprocity lets us compute (a/p) efficiently. In this respect, it answers our third question in the affirmative.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

An Example

Let's see an example of quadratic reciprocity by computing $(79/101)$. In other words, let's see if $\overline{79}$ has a square root in $\mathbb{Z}/101\mathbb{Z}$.

$$\begin{aligned}
(79/101) &= (101/79) && \text{(law of quadratic reciprocity)} \\
&= (22/79) && (101 \equiv 22 \pmod{79}) \\
&= (2/79)(11/79) && \text{(multiplicativity)} \\
&= (11/79) && \text{(second supplementary law)} \\
&= -(79/11) && \text{(law of quadratic reciprocity)} \\
&= -(2/11) && (79 \equiv 2 \pmod{11}) \\
&= 1 && \text{(second supplementary law).}
\end{aligned}$$

We conclude 79 is a quadratic residue mod 101. Indeed, $33^2 \equiv 79 \pmod{101}$. This process is significantly more efficient to compute quadratic residues.

Outline

Setting for Cubic Reciprocity

We would like to understand solutions to the equation

$$x^3 \equiv a \pmod{p}.$$

It is best to work in $\mathbb{Z}[\omega]$ where ω is the primitive cube root of unity. In $\mathbb{Z}[\omega]$ we have a norm N defined by

$$N\alpha := a^2 - ab + b^2 \quad (\text{for } \alpha = a + b\omega \in \mathbb{Z}[\omega]).$$

If $\pi \in \mathbb{Z}[\omega]$ is a prime such that $N\pi \neq 3$ and $\pi \nmid \alpha$, then there is a unique integer $m = 0, 1, 2$ such that

$$\alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi}.$$

This additional setup only appears for higher reciprocity laws since $-1 \in \mathbb{Z}$.

Setting for Cubic Reciprocity

We would like to understand solutions to the equation

$$x^3 \equiv a \pmod{p}.$$

It is best to work in $\mathbb{Z}[\omega]$ where ω is the primitive cube root of unity. In $\mathbb{Z}[\omega]$ we have a norm N defined by

$$N\alpha := a^2 - ab + b^2 \quad (\text{for } \alpha = a + b\omega \in \mathbb{Z}[\omega]).$$

If $\pi \in \mathbb{Z}[\omega]$ is a prime such that $N\pi \neq 3$ and $\pi \nmid \alpha$, then there is a unique integer $m = 0, 1, 2$ such that

$$\alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi}.$$

This additional setup only appears for higher reciprocity laws since $-1 \in \mathbb{Z}$.

Setting for Cubic Reciprocity

We would like to understand solutions to the equation

$$x^3 \equiv a \pmod{p}.$$

It is best to work in $\mathbb{Z}[\omega]$ where ω is the primitive cube root of unity. In $\mathbb{Z}[\omega]$ we have a norm N defined by

$$N\alpha := a^2 - ab + b^2 \quad (\text{for } \alpha = a + b\omega \in \mathbb{Z}[\omega]).$$

If $\pi \in \mathbb{Z}[\omega]$ is a prime such that $N\pi \neq 3$ and $\pi \nmid \alpha$, then there is a unique integer $m = 0, 1, 2$ such that

$$\alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi}.$$

This additional setup only appears for higher reciprocity laws since $-1 \in \mathbb{Z}$.

Setting for Cubic Reciprocity

We would like to understand solutions to the equation

$$x^3 \equiv a \pmod{p}.$$

It is best to work in $\mathbb{Z}[\omega]$ where ω is the primitive cube root of unity. In $\mathbb{Z}[\omega]$ we have a norm N defined by

$$N\alpha := a^2 - ab + b^2 \quad (\text{for } \alpha = a + b\omega \in \mathbb{Z}[\omega]).$$

If $\pi \in \mathbb{Z}[\omega]$ is a prime such that $N\pi \neq 3$ and $\pi \nmid \alpha$, then there is a unique integer $m = 0, 1, 2$ such that

$$\alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi}.$$

This additional setup only appears for higher reciprocity laws since $-1 \in \mathbb{Z}$.

Setting for Cubic Reciprocity

We would like to understand solutions to the equation

$$x^3 \equiv a \pmod{p}.$$

It is best to work in $\mathbb{Z}[\omega]$ where ω is the primitive cube root of unity. In $\mathbb{Z}[\omega]$ we have a norm N defined by

$$N\alpha := a^2 - ab + b^2 \quad (\text{for } \alpha = a + b\omega \in \mathbb{Z}[\omega]).$$

If $\pi \in \mathbb{Z}[\omega]$ is a prime such that $N\pi \neq 3$ and $\pi \nmid \alpha$, then there is a unique integer $m = 0, 1, 2$ such that

$$\alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi}.$$

This additional setup only appears for higher reciprocity laws since $-1 \in \mathbb{Z}$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Cubic Residue Symbol

Definition 4.1

Let π and m be as before. Then the cubic residue symbol $(\alpha/\pi)_3$ is defined by

$$(\alpha/\pi)_3 := \begin{cases} \omega^m & \text{if } \pi \nmid \alpha, \\ 0 & \text{if } \pi \mid \alpha. \end{cases}$$

We say α is a cubic residue mod π if $(\alpha/\pi)_3 = 1$ and a cubic nonresidue otherwise. The cubic residue symbol satisfies properties analogous to the Legendre symbol:

- $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable.
- $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.
- $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3$.
- If $\alpha \equiv \beta \pmod{\pi}$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

The Law of Cubic Reciprocity

The units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$. We single out associates of primes to play the role of positive primes in $\mathbb{Z}$.

Definition 4.2

If π is a prime in $\mathbb{Z}[\omega]$, we say π is primary if $\pi \equiv 2 \pmod 3$.

Among the associates of π, exactly one is primary.

Theorem 4.1

Let λ and π be primary such that $N\lambda \neq 3$, $N\pi \neq 3$ and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_3 = (\pi/\lambda)_3.$$

The Law of Cubic Reciprocity

The units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$. We single out associates of primes to play the role of positive primes in $\mathbb{Z}$.

Definition 4.2

If π is a prime in $\mathbb{Z}[\omega]$, we say π is primary if $\pi \equiv 2 \pmod 3$.

Among the associates of π, exactly one is primary.

Theorem 4.1

Let λ and π be primary such that $N\lambda \neq 3$, $N\pi \neq 3$ and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_3 = (\pi/\lambda)_3.$$

The Law of Cubic Reciprocity

The units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$. We single out associates of primes to play the role of positive primes in $\mathbb{Z}$.

Definition 4.2

If π is a prime in $\mathbb{Z}[\omega]$, we say π is primary if $\pi \equiv 2 \pmod 3$.

Among the associates of π, exactly one is primary.

Theorem 4.1

Let λ and π be primary such that $N\lambda \neq 3$, $N\pi \neq 3$ and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_3 = (\pi/\lambda)_3.$$

The Law of Cubic Reciprocity

The units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$. We single out associates of primes to play the role of positive primes in $\mathbb{Z}$.

Definition 4.2

If π is a prime in $\mathbb{Z}[\omega]$, we say π is primary if $\pi \equiv 2 \pmod 3$.

Among the associates of π, exactly one is primary.

Theorem 4.1

Let λ and π be primary such that $N\lambda \neq 3$, $N\pi \neq 3$ and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_3 = (\pi/\lambda)_3.$$

The Law of Cubic Reciprocity

The units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$. We single out associates of primes to play the role of positive primes in $\mathbb{Z}$.

Definition 4.2

If π is a prime in $\mathbb{Z}[\omega]$, we say π is primary if $\pi \equiv 2 \pmod 3$.

Among the associates of π, exactly one is primary.

Theorem 4.1

Let λ and π be primary such that $N\lambda \neq 3$, $N\pi \neq 3$ and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_3 = (\pi/\lambda)_3.$$

Biquadratic Reciprocity

We work in $\mathbb{Z}[i]$; there is a norm $N\pi = \pi\bar{\pi}$. If π is prime such that $N\pi \neq 2$, there is a unique $m \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi}.$$

Let this define the biquadratic residue symbol $(\alpha/\pi)_4$. It satisfies analogous properties to the Legendre symbol. There is a notion of primary primes in $\mathbb{Z}[i]$.

Theorem 4.2

Let λ and π are primary with $N\lambda \neq 2$, $N\pi \neq 2$, and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_4(\pi/\lambda)_4 = (-1)^{((N\lambda-1)/4)((N\pi-1)/4)}.$$

Biquadratic Reciprocity

We work in $\mathbb{Z}[i]$; there is a norm $N\pi = \pi\bar{\pi}$. If π is prime such that $N\pi \neq 2$, there is a unique $m \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi}.$$

Let this define the biquadratic residue symbol $(\alpha/\pi)_4$. It satisfies analogous properties to the Legendre symbol. There is a notion of primary primes in $\mathbb{Z}[i]$.

Theorem 4.2

Let λ and π are primary with $N\lambda \neq 2$, $N\pi \neq 2$, and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_4(\pi/\lambda)_4 = (-1)^{((N\lambda-1)/4)((N\pi-1)/4)}.$$

Biquadratic Reciprocity

We work in $\mathbb{Z}[i]$; there is a norm $N\pi = \pi\bar{\pi}$. If π is prime such that $N\pi \neq 2$, there is a unique $m \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi}.$$

Let this define the biquadratic residue symbol $(\alpha/\pi)_4$. It satisfies analogous properties to the Legendre symbol. There is a notion of primary primes in $\mathbb{Z}[i]$.

Theorem 4.2

Let λ and π are primary with $N\lambda \neq 2$, $N\pi \neq 2$, and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_4(\pi/\lambda)_4 = (-1)^{((N\lambda-1)/4)((N\pi-1)/4)}.$$

Biquadratic Reciprocity

We work in $\mathbb{Z}[i]$; there is a norm $N\pi = \pi\bar{\pi}$. If π is prime such that $N\pi \neq 2$, there is a unique $m \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi}.$$

Let this define the biquadratic residue symbol $(\alpha/\pi)_4$. It satisfies analogous properties to the Legendre symbol. There is a notion of primary primes in $\mathbb{Z}[i]$.

Theorem 4.2

Let λ and π are primary with $N\lambda \neq 2$, $N\pi \neq 2$, and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_4(\pi/\lambda)_4 = (-1)^{((N\lambda-1)/4)((N\pi-1)/4)}.$$

Biquadratic Reciprocity

We work in $\mathbb{Z}[i]$; there is a norm $N\pi = \pi\bar{\pi}$. If π is prime such that $N\pi \neq 2$, there is a unique $m \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi}.$$

Let this define the biquadratic residue symbol $(\alpha/\pi)_4$. It satisfies analogous properties to the Legendre symbol. There is a notion of primary primes in $\mathbb{Z}[i]$.

Theorem 4.2

Let λ and π are primary with $N\lambda \neq 2$, $N\pi \neq 2$, and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_4(\pi/\lambda)_4 = (-1)^{((N\lambda-1)/4)((N\pi-1)/4)}.$$

Biquadratic Reciprocity

We work in $\mathbb{Z}[i]$; there is a norm $N\pi = \pi\bar{\pi}$. If π is prime such that $N\pi \neq 2$, there is a unique $m \in \{0, 1, 2, 3\}$ such that

$$\alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi}.$$

Let this define the biquadratic residue symbol $(\alpha/\pi)_4$. It satisfies analogous properties to the Legendre symbol. There is a notion of primary primes in $\mathbb{Z}[i]$.

Theorem 4.2

Let λ and π are primary with $N\lambda \neq 2$, $N\pi \neq 2$, and $N\lambda \neq N\pi$. Then

$$(\lambda/\pi)_4(\pi/\lambda)_4 = (-1)^{((N\lambda-1)/4)((N\pi-1)/4)}.$$

Outline

Unifying Proofs of Reciprocity Laws

With multiple proofs of quadratic, cubic, and biquadratic reciprocity, it is natural to ask if there is a "unifying idea" to prove all three. Gauss sums are this idea.

- Studied first by Gauss regarding quadratic reciprocity.
- Developed early in the 19th century in conjunction with Jacobi sums.
- They can be used to count solutions of polynomial equations over finite fields and thus zeta functions.

Unifying Proofs of Reciprocity Laws

With multiple proofs of quadratic, cubic, and biquadratic reciprocity, it is natural to ask if there is a "unifying idea" to prove all three. Gauss sums are this idea.

- Studied first by Gauss regarding quadratic reciprocity.
- Developed early in the 19th century in conjunction with Jacobi sums.
- They can be used to count solutions of polynomial equations over finite fields and thus zeta functions.

Unifying Proofs of Reciprocity Laws

With multiple proofs of quadratic, cubic, and biquadratic reciprocity, it is natural to ask if there is a "unifying idea" to prove all three. Gauss sums are this idea.

- Studied first by Gauss regarding quadratic reciprocity.
- Developed early in the 19th century in conjunction with Jacobi sums.
- They can be used to count solutions of polynomial equations over finite fields and thus zeta functions.

Unifying Proofs of Reciprocity Laws

With multiple proofs of quadratic, cubic, and biquadratic reciprocity, it is natural to ask if there is a "unifying idea" to prove all three. Gauss sums are this idea.

- Studied first by Gauss regarding quadratic reciprocity.
- Developed early in the 19th century in conjunction with Jacobi sums.
- They can be used to count solutions of polynomial equations over finite fields and thus zeta functions.

Unifying Proofs of Reciprocity Laws

With multiple proofs of quadratic, cubic, and biquadratic reciprocity, it is natural to ask if there is a "unifying idea" to prove all three. Gauss sums are this idea.

- Studied first by Gauss regarding quadratic reciprocity.
- Developed early in the 19th century in conjunction with Jacobi sums.
- They can be used to count solutions of polynomial equations over finite fields and thus zeta functions.

Characters and Gauss Sums

A character χ on $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*.$$

The Legendre symbol (t/p) is an example of a (quadratic) character on $(\mathbb{Z}/p\mathbb{Z})^*$. If ζ is a primitive p-th root of unity and $a \in \mathbb{Z}$, then

$$g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^t$$

is called a Gauss sum. When $\chi(t) = (t/p)$ we call the sum a quadratic Gauss sum. Manipulations of quadratic Gauss sums lead to an elegant proof of the law of quadratic reciprocity. Similarly one can use cubic and biquadratic Gauss sums to prove the laws of cubic and biquadratic reciprocity.

Characters and Gauss Sums

A character χ on $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*.$$

The Legendre symbol (t/p) is an example of a (quadratic) character on $(\mathbb{Z}/p\mathbb{Z})^*$. If ζ is a primitive p-th root of unity and $a \in \mathbb{Z}$, then

$$g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^t$$

is called a Gauss sum. When $\chi(t) = (t/p)$ we call the sum a quadratic Gauss sum. Manipulations of quadratic Gauss sums lead to an elegant proof of the law of quadratic reciprocity. Similarly one can use cubic and biquadratic Gauss sums to prove the laws of cubic and biquadratic reciprocity.

Characters and Gauss Sums

A character χ on $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*.$$

The Legendre symbol (t/p) is an example of a (quadratic) character on $(\mathbb{Z}/p\mathbb{Z})^*$. If ζ is a primitive p-th root of unity and $a \in \mathbb{Z}$, then

$$g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^{t}$$

is called a Gauss sum. When $\chi(t) = (t/p)$ we call the sum a quadratic Gauss sum. Manipulations of quadratic Gauss sums lead to an elegant proof of the law of quadratic reciprocity. Similarly one can use cubic and biquadratic Gauss sums to prove the laws of cubic and biquadratic reciprocity.

Characters and Gauss Sums

A character χ on $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*.$$

The Legendre symbol (t/p) is an example of a (quadratic) character on $(\mathbb{Z}/p\mathbb{Z})^*$. If ζ is a primitive p-th root of unity and $a \in \mathbb{Z}$, then

$$g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^t$$

is called a Gauss sum. When $\chi(t) = (t/p)$ we call the sum a quadratic Gauss sum. Manipulations of quadratic Gauss sums lead to an elegant proof of the law of quadratic reciprocity. Similarly one can use cubic and biquadratic Gauss sums to prove the laws of cubic and biquadratic reciprocity.

Characters and Gauss Sums

A character χ on $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*.$$

The Legendre symbol (t/p) is an example of a (quadratic) character on $(\mathbb{Z}/p\mathbb{Z})^*$. If ζ is a primitive p-th root of unity and $a \in \mathbb{Z}$, then

$$g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^t$$

is called a Gauss sum. When $\chi(t) = (t/p)$ we call the sum a quadratic Gauss sum. Manipulations of quadratic Gauss sums lead to an elegant proof of the law of quadratic reciprocity. Similarly one can use cubic and biquadratic Gauss sums to prove the laws of cubic and biquadratic reciprocity.

Characters and Gauss Sums

A character χ on $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*.$$

The Legendre symbol (t/p) is an example of a (quadratic) character on $(\mathbb{Z}/p\mathbb{Z})^*$. If ζ is a primitive p-th root of unity and $a \in \mathbb{Z}$, then

$$g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at} = \chi(a) \sum_{t=0}^{p-1} \chi(t)\zeta^t$$

is called a Gauss sum. When $\chi(t) = (t/p)$ we call the sum a quadratic Gauss sum. Manipulations of quadratic Gauss sums lead to an elegant proof of the law of quadratic reciprocity. Similarly one can use cubic and biquadratic Gauss sums to prove the laws of cubic and biquadratic reciprocity.

Outline

References

Thanks!

- K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory, Springer, 1982.
- J-P. Serre: A Course in Arithmetic, Springer, 1973.