

Primes of the Form $x^2 + ny^2$

Negin Shadgar

University of Tehran

June 10, 2023

History of the Problem

Fermat's Theorem

For an odd prime p : $p = x^2 + y^2, x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Example

$$5 = 2^2 + 1^2$$

Related Theorems in Fermat's Work

For an odd prime p :

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8}$$

$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3, p \equiv 1 \pmod{3}$$

History of the Problem

Fermat's Theorem

For an odd prime p : $p = x^2 + y^2, x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Example

$$5 = 2^2 + 1^2$$

Related Theorems in Fermat's Work

For an odd prime p :

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8}$$

$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3, p \equiv 1 \pmod{3}$$

History of the Problem

Fermat's Theorem

For an odd prime p : $p = x^2 + y^2, x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Example

$$5 = 2^2 + 1^2$$

Related Theorems in Fermat's Work

For an odd prime p :

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8}$$

$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3, p \equiv 1 \pmod{3}$$

Main Question

Main Question

Given a positive integer n , which primes p can be expressed in the form $p = x^2 + ny^2$ where x and y are integers?

Main Question

Approach

- 1 Elementary approaches to the problem, using the works of Fermat, Euler, Lagrange, Legendre, and Gauss as a guide.
 - Quadratic Reciprocity and Decent Step
 - Theory of Quadratic Forms and Genus Theory
 - Cubic and Bi-quadratic Reciprocity

Main Question

Approach

- 1 Elementary approaches to the problem, using the works of Fermat, Euler, Lagrange, Legendre, and Gauss as a guide.
 - Quadratic Reciprocity and Decent Step
 - Theory of Quadratic Forms and Genus Theory
 - Cubic and Bi-quadratic Reciprocity

Main Question

Approach

- 1 Elementary approaches to the problem, using the works of Fermat, Euler, Lagrange, Legendre, and Gauss as a guide.
 - Quadratic Reciprocity and Decent Step
 - Theory of Quadratic Forms and Genus Theory
 - Cubic and Bi-quadratic Reciprocity

Main Question

Approach

- 1 Elementary approaches to the problem, using the works of Fermat, Euler, Lagrange, Legendre, and Gauss as a guide.
 - Quadratic Reciprocity and Decent Step
 - Theory of Quadratic Forms and Genus Theory
 - Cubic and Bi-quadratic Reciprocity

Main Question

Approach

- 1 Elementary approaches to the problem, using the works of Fermat, Euler, Lagrange, Legendre, and Gauss as a guide.
 - Quadratic Reciprocity and Decent Step
 - Theory of Quadratic Forms and Genus Theory
 - Cubic and Bi-quadratic Reciprocity

Main Question

Approach

2 Using Class Field Theory.

- Hilbert Class Field
- Ring Class Field

Main Question

Approach

② Using Class Field Theory.

- Hilbert Class Field
- Ring Class Field

Main Question

Approach

② Using Class Field Theory.

- Hilbert Class Field
- Ring Class Field

Main Question

Primary Goals

- 1 To answer our main question.
- 2 To bridge the gap between elementary number theory and class field theory.

Main Question

Primary Goals

- 1 To answer our main question.
- 2 To bridge the gap between elementary number theory and class field theory.

$$p = x^2 + y^2$$

Theorem

For an odd prime p : $p = x^2 + y^2$, $x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Proof.

$\Rightarrow$: Obvious.

$\Leftarrow$: Using the following two steps:

- Decent Step: if $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + y'^2$ for $x', y' \in \mathbb{Z}$.
- Reciprocity Step: if $p \equiv 1 \pmod{4}$ then $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$

$$p = x^2 + y^2$$

Theorem

For an odd prime p : $p = x^2 + y^2, x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Proof.

$\Rightarrow$: Obvious.

$\Leftarrow$: Using the following two steps:

- Decent Step: if $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + y'^2$ for $x', y' \in \mathbb{Z}$.
- Reciprocity Step: if $p \equiv 1 \pmod{4}$ then $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$

$$p = x^2 + y^2$$

Theorem

For an odd prime p : $p = x^2 + y^2$, $x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Proof.

$\Rightarrow$: Obvious.

$\Leftarrow$: Using the following two steps:

- Decent Step: if $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + y'^2$ for $x', y' \in \mathbb{Z}$.
- Reciprocity Step: if $p \equiv 1 \pmod{4}$ then $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$

$$p = x^2 + y^2$$

Theorem

For an odd prime p : $p = x^2 + y^2, x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Proof.

$\Rightarrow$: Obvious.

$\Leftarrow$: Using the following two steps:

- Decent Step: if $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + y'^2$ for $x', y' \in \mathbb{Z}$.
- Reciprocity Step: if $p \equiv 1 \pmod{4}$ then $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$

$$p = x^2 + y^2$$

Theorem

For an odd prime p : $p = x^2 + y^2$, $x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{4}$

Proof.

$\Rightarrow$: Obvious.

$\Leftarrow$: Using the following two steps:

- Decent Step: if $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + y'^2$ for $x', y' \in \mathbb{Z}$.
- Reciprocity Step: if $p \equiv 1 \pmod{4}$ then $p \mid x^2 + y^2$ where $\gcd(x, y) = 1$

$$p = x^2 + ny^2 \text{ for } n = 2, 3$$

Remark

The same two strategies (Decent and reciprocity steps) can be applied to prove the following statements:

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8}$$

$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3, p \equiv 1 \pmod{3}$$

- Our ideal is to generalize the aforementioned two steps i.e.

- 1 Decent Step
- 2 Reciprocity Step

$$p = x^2 + ny^2 \text{ for } n = 2, 3$$

Remark

The same two strategies (Decent and reciprocity steps) can be applied to prove the following statements:

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8}$$
$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3, p \equiv 1 \pmod{3}$$

- Our ideal is to generalize the aforementioned two steps i.e.
 - 1 Decent Step
 - 2 Reciprocity Step

$$p = x^2 + ny^2 \text{ for } n = 2, 3$$

Remark

The same two strategies (Decent and reciprocity steps) can be applied to prove the following statements:

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8}$$
$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3, p \equiv 1 \pmod{3}$$

- Our ideal is to generalize the aforementioned two steps i.e.
 - 1 Decent Step
 - 2 Reciprocity Step

Generalizing Decent Step

Idea

If $p \mid x^2 + ny^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + ny'^2$ for $x', y' \in \mathbb{Z}$.

This idea fails when $n = 5$.

If $n = 5$ then according to the decent step since $3 \mid 21 = 1^2 + 5(2^2)$ then 3 must be in the form of $x^2 + 5y^2$ for $x, y \in \mathbb{Z}$. But we know that this cannot happen.

- For now, we let go of the generalization of the decent step until introducing the theory of quadratic forms.

Generalizing Decent Step

Idea

If $p \mid x^2 + ny^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + ny'^2$ for $x', y' \in \mathbb{Z}$.

This idea fails when $n = 5$.

If $n = 5$ then according to the decent step since $3 \mid 21 = 1^2 + 5(2^2)$ then 3 must be in the form of $x^2 + 5y^2$ for $x, y \in \mathbb{Z}$. But we know that this cannot happen.

- For now, we let go of the generalization of the decent step until introducing the theory of quadratic forms.

Generalizing Decent Step

Idea

If $p \mid x^2 + ny^2$ where $\gcd(x, y) = 1$ then $p = x'^2 + ny'^2$ for $x', y' \in \mathbb{Z}$.

This idea fails when $n = 5$.

If $n = 5$ then according to the decent step since $3 \mid 21 = 1^2 + 5(2^2)$ then 3 must be in the form of $x^2 + 5y^2$ for $x, y \in \mathbb{Z}$. But we know that this cannot happen.

- For now, we let go of the generalization of the decent step until introducing the theory of quadratic forms.

Generalizing Reciprocity Step

Goal

Finding congruence conditions on prime p , guaranteeing $p \mid x^2 + ny^2$.

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n .
Then:

$$p \mid x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1$$

- Hence the reciprocity step can be restated as the following question:
Is there a congruence $p \equiv \alpha, \beta, \dots \pmod{4n}$ which implies $(-n/p) = 1$ when p is prime?

Generalizing Reciprocity Step

Goal

Finding congruence conditions on prime p , guaranteeing $p \mid x^2 + ny^2$.

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n .
Then:

$$p \mid x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1$$

- Hence the reciprocity step can be restated as the following question:
Is there a congruence $p \equiv \alpha, \beta, \dots \pmod{4n}$ which implies $(-n/p) = 1$ when p is prime?

Generalizing Reciprocity Step

Goal

Finding congruence conditions on prime p , guaranteeing $p \mid x^2 + ny^2$.

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n .
Then:

$$p \mid x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1$$

- Hence the reciprocity step can be restated as the following question:
Is there a congruence $p \equiv \alpha, \beta, \dots \pmod{4n}$ which implies $(-n/p) = 1$ when p is prime?

Definition Legendre Symbol

Let p be an odd prime number. The Legendre symbol is a function of a and p defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Euler's Conjectures

- Euler's obsession to find when $(-n/p) = 1$ leads to a really nice conjecture that is equivalent to quadratic reciprocity.

Some of Euler's Conjectures, Stated in Modern Notation.

- $(3/p) = 1 \iff p \equiv \pm 1 \pmod{12}$
- $(5/p) = 1 \iff p \equiv \pm 1, \pm 11(3^2) \pmod{20}$
- $(7/p) = 1 \iff p \equiv \pm 1, \pm 3(5^2), \pm 9 \pmod{28}$
- This promising look happens for n 's such that $-n$ is a prime number.

Euler's Conjectures

- Euler's obsession to find when $(-n/p) = 1$ leads to a really nice conjecture that is equivalent to quadratic reciprocity.

Some of Euler's Conjectures, Stated in Modern Notation.

- $(3/p) = 1 \iff p \equiv \pm 1 \pmod{12}$
- $(5/p) = 1 \iff p \equiv \pm 1, \pm 11(3^2) \pmod{20}$
- $(7/p) = 1 \iff p \equiv \pm 1, \pm 3(5^2), \pm 9 \pmod{28}$
- This promising look happens for n 's such that $-n$ is a prime number.

Euler's Conjectures

- Euler's obsession to find when $(-n/p) = 1$ leads to a really nice conjecture that is equivalent to quadratic reciprocity.

Some of Euler's Conjectures, Stated in Modern Notation.

- $(3/p) = 1 \iff p \equiv \pm 1 \pmod{12}$
- $(5/p) = 1 \iff p \equiv \pm 1, \pm 11(3^2) \pmod{20}$
- $(7/p) = 1 \iff p \equiv \pm 1, \pm 3(5^2), \pm 9 \pmod{28}$
- This promising look happens for n 's such that $-n$ is a prime number.

Euler's Conjectures

- Euler's obsession to find when $(-n/p) = 1$ leads to a really nice conjecture that is equivalent to quadratic reciprocity.

Some of Euler's Conjectures, Stated in Modern Notation.

- $(3/p) = 1 \iff p \equiv \pm 1 \pmod{12}$
 - $(5/p) = 1 \iff p \equiv \pm 1, \pm 11(3^2) \pmod{20}$
 - $(7/p) = 1 \iff p \equiv \pm 1, \pm 3(5^2), \pm 9 \pmod{28}$
- This promising look happens for n 's such that $-n$ is a prime number.

Euler's Conjectures

- Euler's obsession to find when $(-n/p) = 1$ leads to a really nice conjecture that is equivalent to quadratic reciprocity.

Some of Euler's Conjectures, Stated in Modern Notation.

- $(3/p) = 1 \iff p \equiv \pm 1 \pmod{12}$
- $(5/p) = 1 \iff p \equiv \pm 1, \pm 11(3^2) \pmod{20}$
- $(7/p) = 1 \iff p \equiv \pm 1, \pm 3(5^2), \pm 9 \pmod{28}$
- This promising look happens for n 's such that $-n$ is a prime number.

Quadratic Reciprocity

Conjecture

If p and q are distinct odd primes, then:

$$\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\beta^2 \pmod{4q} \text{ for some odd integer } \beta$$

- The remarkable fact is that this conjecture is equivalent to the usual statement of quadratic reciprocity.

Proposition

If p and q are distinct odd primes, then conjecture is equivalent to :

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Quadratic Reciprocity

Conjecture

If p and q are distinct odd primes, then:

$$\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\beta^2 \pmod{4q} \text{ for some odd integer } \beta$$

- The remarkable fact is that this conjecture is equivalent to the usual statement of quadratic reciprocity.

Proposition

If p and q are distinct odd primes, then conjecture is equivalent to :

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Quadratic Reciprocity

Conjecture

If p and q are distinct odd primes, then:

$$\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm \beta^2 \pmod{4q} \text{ for some odd integer } \beta$$

- The remarkable fact is that this conjecture is equivalent to the usual statement of quadratic reciprocity.

Proposition

If p and q are distinct odd primes, then conjecture is equivalent to :

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Generalizing Reciprocity Step

Lemma

If $D \equiv 0, 1 \pmod{4}$ is a nonzero integer, then there is a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z})^* \rightarrow \{\pm 1\}$ such that $\chi([p]) = (D/p)$ for odd primes p not dividing D . Furthermore

$$\chi([-1]) = \begin{cases} 1 & \text{when } D > 0 \\ -1 & \text{when } D < 0 \end{cases}$$

Generalizing Reciprocity Step

Corollary

Let n be a nonzero integer, and let $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \rightarrow \{\pm 1\}$ be the homomorphism from the previous Lemma when $D = -4n$. If p is an odd prime not dividing n , then the following are equivalent:

- i $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$.
- ii $(-n/p) = 1$
- iii $[p] \in \ker(\chi) \subset (\mathbb{Z}/4n\mathbb{Z})^*$

- This solves the Reciprocity Step, $\ker(\chi) = \{[\alpha], [\beta], [\gamma], \dots\}$ hence if $[p] \in \ker(\chi) \iff p \equiv \alpha, \beta, \gamma, \dots \pmod{4n}$, which is exactly the kind of condition we were looking for.

Generalizing Reciprocity Step

Corollary

Let n be a nonzero integer, and let $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \rightarrow \{\pm 1\}$ be the homomorphism from the previous Lemma when $D = -4n$. If p is an odd prime not dividing n , then the following are equivalent:

- i $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$.
- ii $(-n/p) = 1$
- iii $[p] \in \ker(\chi) \subset (\mathbb{Z}/4n\mathbb{Z})^*$

- This solves the Reciprocity Step, $\ker(\chi) = \{[\alpha], [\beta], [\gamma], \dots\}$ hence if $[p] \in \ker(\chi) \iff p \equiv \alpha, \beta, \gamma, \dots \pmod{4n}$, which is exactly the kind of condition we were looking for.

Generalizing Reciprocity Step

Corollary

Let n be a nonzero integer, and let $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \rightarrow \{\pm 1\}$ be the homomorphism from the previous Lemma when $D = -4n$. If p is an odd prime not dividing n , then the following are equivalent:

- i $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$.
- ii $(-n/p) = 1$
- iii $[p] \in \ker(\chi) \subset (\mathbb{Z}/4n\mathbb{Z})^*$

- This solves the Reciprocity Step, $\ker(\chi) = \{[\alpha], [\beta], [\gamma], \dots\}$ hence if $[p] \in \ker(\chi) \iff p \equiv \alpha, \beta, \gamma, \dots \pmod{4n}$, which is exactly the kind of condition we were looking for.

Generalizing Reciprocity Step

Corollary

Let n be a nonzero integer, and let $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \rightarrow \{\pm 1\}$ be the homomorphism from the previous Lemma when $D = -4n$. If p is an odd prime not dividing n , then the following are equivalent:

- i $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$.
- ii $(-n/p) = 1$
- iii $[p] \in \ker(\chi) \subset (\mathbb{Z}/4n\mathbb{Z})^*$

- This solves the Reciprocity Step, $\ker(\chi) = \{[\alpha], [\beta], [\gamma], \dots\}$ hence if $[p] \in \ker(\chi) \iff p \equiv \alpha, \beta, \gamma, \dots \pmod{4n}$, which is exactly the kind of condition we were looking for.

Generalizing Reciprocity Step

Corollary

Let n be a nonzero integer, and let $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \rightarrow \{\pm 1\}$ be the homomorphism from the previous Lemma when $D = -4n$. If p is an odd prime not dividing n , then the following are equivalent:

- i $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$.
- ii $(-n/p) = 1$
- iii $[p] \in \ker(\chi) \subset (\mathbb{Z}/4n\mathbb{Z})^*$

- This solves the Reciprocity Step, $\ker(\chi) = \{[\alpha], [\beta], [\gamma], \dots\}$ hence if $[p] \in \ker(\chi) \iff p \equiv \alpha, \beta, \gamma, \dots \pmod{4n}$, which is exactly the kind of condition we were looking for.

Quadratic Forms

Back to Generalizing the Decent Step

Definition

A **quadratic form** is a polynomial with terms all of the degree two.

$$f(x, y) = ax^2 + bxy + cy^2 \text{ with } a, b, c, x, y \in \mathbb{Z}.$$

Example

$$f(x, y) = x^2 + ny^2$$

Quadratic Forms

Back to Generalizing the Decent Step

Definition

A **quadratic form** is a polynomial with terms all of the degree two.

$$f(x, y) = ax^2 + bxy + cy^2 \text{ with } a, b, c, x, y \in \mathbb{Z}.$$

Example

$$f(x, y) = x^2 + ny^2$$

Definition

- i A form $ax^2 + bxy + cy^2$ is **primitive** if its coefficients a , b and c are relatively prime.
- ii An integer m is **represented** by a form $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y .
 - If the x and y are relatively prime, we say that m is **properly represented** by $f(x, y)$.
- Our main question can be restated as which primes are represented by the quadratic form $x^2 + ny^2$?

Definition

- i A form $ax^2 + bxy + cy^2$ is **primitive** if its coefficients a , b and c are relatively prime.
- ii An integer m is **represented** by a form $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y .
 - If the x and y are relatively prime, we say that m is **properly represented** by $f(x, y)$.
- Our main question can be restated as which primes are represented by the quadratic form $x^2 + ny^2$?

Definition

- i A form $ax^2 + bxy + cy^2$ is **primitive** if its coefficients a , b and c are relatively prime.
 - ii An integer m is **represented** by a form $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y .
 - If the x and y are relatively prime, we say that m is **properly represented** by $f(x, y)$.
- Our main question can be restated as which primes are represented by the quadratic form $x^2 + ny^2$?

Definition

- i A form $ax^2 + bxy + cy^2$ is **primitive** if its coefficients a , b and c are relatively prime.
- ii An integer m is **represented** by a form $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y .
 - If the x and y are relatively prime, we say that m is **properly represented** by $f(x, y)$.
- Our main question can be restated as which primes are represented by the quadratic form $x^2 + ny^2$?

Relation Between Quadratic Forms

Definition

Two forms $f(x, y)$ and $g(x, y)$ are **equivalent** if $\exists p, q, r, s \in \mathbb{Z}$ s.t.:
 $f(x, y) = g(px + qy, rx + sy)$, and $ps - qr = \pm 1$.

- i An equivalence is a **proper equivalence** if $ps - qr = 1$
- ii An equivalence is a **improper equivalence** if $ps - qr = -1$

Relation Between Quadratic Forms

Definition

Two forms $f(x, y)$ and $g(x, y)$ are **equivalent** if $\exists p, q, r, s \in \mathbb{Z}$ s.t.:
 $f(x, y) = g(px + qy, rx + sy)$, and $ps - qr = \pm 1$.

- i An equivalence is a **proper equivalence** if $ps - qr = 1$
- ii An equivalence is a **improper equivalence** if $ps - qr = -1$

Relation Between Quadratic Forms

Definition

Two forms $f(x, y)$ and $g(x, y)$ are **equivalent** if $\exists p, q, r, s \in \mathbb{Z}$ s.t.:
 $f(x, y) = g(px + qy, rx + sy)$, and $ps - qr = \pm 1$.

- i An equivalence is a **proper equivalence** if $ps - qr = 1$
- ii An equivalence is a **improper equivalence** if $ps - qr = -1$

Discriminant

Definition

Discriminant form $f(x, y) = ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Lemma

Suppose that the forms $f(x, y)$ and $g(x, y)$ have discriminant D and D' respectively, and $f(x, y) = g(px + qy, rx + sy)$, $p, q, r, s \in \mathbb{Z}$. Then:

$$D = (ps - qr)^2 D'$$

Corollary

Two forms have the same discriminant whenever $ps - qr = \pm 1$. Thus equivalent forms have the same discriminant

Discriminant

Definition

Discriminant form $f(x, y) = ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Lemma

Suppose that the forms $f(x, y)$ and $g(x, y)$ have discriminant D and D' respectively, and $f(x, y) = g(px + qy, rx + sy)$, $p, q, r, s \in \mathbb{Z}$. Then:

$$D = (ps - qr)^2 D'$$

Corollary

Two forms have the same discriminant whenever $ps - qr = \pm 1$. Thus equivalent forms have the same discriminant

Discriminant

Definition

Discriminant form $f(x, y) = ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Lemma

Suppose that the forms $f(x, y)$ and $g(x, y)$ have discriminant D and D' respectively, and $f(x, y) = g(px + qy, rx + sy)$, $p, q, r, s \in \mathbb{Z}$. Then:

$$D = (ps - qr)^2 D'$$

Corollary

Two forms have the same discriminant whenever $ps - qr = \pm 1$. Thus equivalent forms have the same discriminant

Relation Between Discriminant and Form

Definition

If $f(x, y) = ax^2 + bxy + cy^2$, then we have the identity

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

- If $D > 0$, then $f(x, y)$ represents both positive and negative integers, and we call the form **indefinite**.
- if $D < 0$, then the form represents only positive integers or only negative ones, depending on the sign of a , and $f(x, y)$ is accordingly called **positive definite** or **negative definite**.

Relation Between Discriminant and Form

Definition

If $f(x, y) = ax^2 + bxy + cy^2$, then we have the identity

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

- If $D > 0$, then $f(x, y)$ represents both positive and negative integers, and we call the form **indefinite**.
- if $D < 0$, then the form represents only positive integers or only negative ones, depending on the sign of a , and $f(x, y)$ is accordingly called **positive definite** or **negative definite**.

Relation Between Discriminant and Form

Definition

If $f(x, y) = ax^2 + bxy + cy^2$, then we have the identity

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

- If $D > 0$, then $f(x, y)$ represents both positive and negative integers, and we call the form **indefinite**.
- if $D < 0$, then the form represents only positive integers or only negative ones, depending on the sign of a , and $f(x, y)$ is accordingly called **positive definite** or **negative definite**.

Generalizing Decent Step

Proposition

Let n be an integer and p be an odd prime not dividing n . Then $(-n/p) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

- This prop. is relevant to generalize the Descent Step of Euler's strategy on representing prime divisors of $x^2 + ny^2$, $\gcd(x, y) = 1$.
- It gives us a first answer to this question, for such primes, satisfy $(-n/p) = 1$; hence are represented by forms of discriminant $-4n$.
- Our problem is there are too many quadratic forms of a given discriminant.

Generalizing Decent Step

Proposition

Let n be an integer and p be an odd prime not dividing n . Then $(-n/p) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

- This prop. is relevant to generalize the Descent Step of Euler's strategy on representing prime divisors of $x^2 + ny^2$, $\gcd(x, y) = 1$.
- It gives us a first answer to this question, for such primes, satisfy $(-n/p) = 1$; hence are represented by forms of discriminant $-4n$.
- Our problem is there are too many quadratic forms of a given discriminant.

Generalizing Decent Step

Proposition

Let n be an integer and p be an odd prime not dividing n . Then $(-n/p) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

- This prop. is relevant to generalize the Descent Step of Euler's strategy on representing prime divisors of $x^2 + ny^2$, $\gcd(x, y) = 1$.
- It gives us a first answer to this question, for such primes, satisfy $(-n/p) = 1$; hence are represented by forms of discriminant $-4n$.
- Our problem is there are too many quadratic forms of a given discriminant.

Generalizing Decent Step

Proposition

Let n be an integer and p be an odd prime not dividing n . Then $(-n/p) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

- This prop. is relevant to generalize the Descent Step of Euler's strategy on representing prime divisors of $x^2 + ny^2$, $\gcd(x, y) = 1$.
- It gives us a first answer to this question, for such primes, satisfy $(-n/p) = 1$; hence are represented by forms of discriminant $-4n$.
- Our problem is there are too many quadratic forms of a given discriminant.

Reduced Form

Definition

A primitive positive definite form $ax^2 + bxy + cy^2$ is said to be **reduced** if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$. (Note that a and c are positive since the form is positive definite.)

Example

$x^2 + ny^2$ is always a reduced form!

Theorem

Every primitive positive definite form is properly equivalent to a unique reduced form.

Reduced Form

Definition

A primitive positive definite form $ax^2 + bxy + cy^2$ is said to be **reduced** if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$. (Note that a and c are positive since the form is positive definite.)

Example

$x^2 + ny^2$ is always a reduced form!

Theorem

Every primitive positive definite form is properly equivalent to a unique reduced form.

Reduced Form

Definition

A primitive positive definite form $ax^2 + bxy + cy^2$ is said to be **reduced** if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$. (Note that a and c are positive since the form is positive definite.)

Example

$x^2 + ny^2$ is always a reduced form!

Theorem

Every primitive positive definite form is properly equivalent to a unique reduced form.

The Number of Reduced Forms

Proposition

There are only a finite number of reduced forms of discriminant D .

Theorem

Let $D < 0$ be fixed. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and $h(D)$ is equal to the number of reduced forms of discriminant D .

The Number of Reduced Forms

Proposition

There are only a finite number of reduced forms of discriminant D .

Theorem

Let $D < 0$ be fixed. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and $h(D)$ is equal to the number of reduced forms of discriminant D .

Summary of What We've Done

Proposition

Let n be a positive integer and p be an odd prime, not dividing n . Then $(-n/p) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.

- We showed quadratic reciprocity gives a general solution to the Reciprocity Step of Euler's strategy.
- We just solved the Descent Step, using the theory of quadratic forms.
- Put the two together and see what we get.
- Rather than treat the case of forms of discriminant $4n$, we will state a result that applies to all negative discriminants $D < 0$.

Summary of What We've Done

Proposition

Let n be a positive integer and p be an odd prime, not dividing n . Then $(-n/p) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.

- We showed quadratic reciprocity gives a general solution to the Reciprocity Step of Euler's strategy.
- We just solved the Descent Step, using the theory of quadratic forms.
- Put the two together and see what we get.
- Rather than treat the case of forms of discriminant $4n$, we will state a result that applies to all negative discriminants $D < 0$.

Summary of What We've Done

Proposition

Let n be a positive integer and p be an odd prime, not dividing n . Then $(-n/p) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.

- We showed quadratic reciprocity gives a general solution to the Reciprocity Step of Euler's strategy.
- We just solved the Descent Step, using the theory of quadratic forms.
- Put the two together and see what we get.
- Rather than treat the case of forms of discriminant $4n$, we will state a result that applies to all negative discriminants $D < 0$.

Summary of What We've Done

Proposition

Let n be a positive integer and p be an odd prime, not dividing n . Then $(-n/p) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.

- We showed quadratic reciprocity gives a general solution to the Reciprocity Step of Euler's strategy.
- We just solved the Descent Step, using the theory of quadratic forms.
- Put the two together and see what we get.
- Rather than treat the case of forms of discriminant $4n$, we will state a result that applies to all negative discriminants $D < 0$.

Summary of What We've Done

Proposition

Let n be a positive integer and p be an odd prime, not dividing n . Then $(-n/p) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.

- We showed quadratic reciprocity gives a general solution to the Reciprocity Step of Euler's strategy.
- We just solved the Descent Step, using the theory of quadratic forms.
- Put the two together and see what we get.
- Rather than treat the case of forms of discriminant $4n$, we will state a result that applies to all negative discriminants $D < 0$.

Put Together What We Have

Theorem

Let $D \equiv 0, 1 \pmod{4}$ be negative, and let $\chi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ be the homomorphism defined before. Then, for an odd prime p not dividing D , $[p] \in \ker(\chi)$ if and only if p is represented by one of the $h(D)$ reduced forms of discriminant D .

- This theorem provides a congruence for an odd prime p to be represented by a reduced form of discriminant D .

Put Together What We Have

Theorem

Let $D \equiv 0, 1 \pmod{4}$ be negative, and let $\chi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ be the homomorphism defined before. Then, for an odd prime p not dividing D , $[p] \in \ker(\chi)$ if and only if p is represented by one of the $h(D)$ reduced forms of discriminant D .

- This theorem provides a congruence for an odd prime p to be represented by a reduced form of discriminant D .

When $h(-4n) = 1 \dots$

Theorem

Let n be a positive integer. Then $h(-4n) = 1 \iff n = 1, 2, 3, 4$ or 7

- Review Euler's proof for Fermat's theorem.
- Why decent and reciprocity step works in these cases.

When $h(-4n) = 1 \dots$

Theorem

Let n be a positive integer. Then $h(-4n) = 1 \iff n = 1, 2, 3, 4$ or 7

- Review Euler's proof for Fermat's theorem.
- Why decent and reciprocity step works in these cases.

When $h(-4n) = 1 \dots$

Theorem

Let n be a positive integer. Then $h(-4n) = 1 \iff n = 1, 2, 3, 4$ or 7

- Review Euler's proof for Fermat's theorem.
- Why decent and reciprocity step works in these cases.

When $h(-4n) > 1 \dots$

Example

$$p \equiv 1, 3, 7, 9 \pmod{20} \Leftrightarrow (-5/p) = 1 \Leftrightarrow p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2.$$

- We need a method of separating reduced forms of the same discriminant, and this is where **genus theory** comes in.

Example

Let's work out some examples to see how this grouping works. When $D = -20$, one easily computes that:

$$\begin{aligned} x^2 + 5y^2 &\text{ represents } 1, 9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \\ 2x^2 + 2xy + 3y^2 &\text{ represents } 3, 7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \end{aligned}$$

When $h(-4n) > 1 \dots$

Example

$$p \equiv 1, 3, 7, 9 \pmod{20} \Leftrightarrow (-5/p) = 1 \Leftrightarrow p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2.$$

- We need a method of separating reduced forms of the same discriminant, and this is where **genus theory** comes in.

Example

Let's work out some examples to see how this grouping works. When $D = -20$, one easily computes that:

$$\begin{aligned} x^2 + 5y^2 &\text{ represents } 1, 9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \\ 2x^2 + 2xy + 3y^2 &\text{ represents } 3, 7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \end{aligned}$$

When $h(-4n) > 1 \dots$

Example

$$p \equiv 1, 3, 7, 9 \pmod{20} \Leftrightarrow (-5/p) = 1 \Leftrightarrow p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2.$$

- We need a method of separating reduced forms of the same discriminant, and this is where **genus theory** comes in.

Example

Let's work out some examples to see how this grouping works. When $D = -20$, one easily computes that:

$$\begin{aligned} x^2 + 5y^2 &\text{ represents } 1, 9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \\ 2x^2 + 2xy + 3y^2 &\text{ represents } 3, 7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \end{aligned}$$

Principal Form

Definition

Given a negative integer $D \equiv 0, 1 \pmod{4}$, the **principal form** is defined to be:

$$\begin{array}{ll} x^2 - \frac{D}{4}y^2, & D \equiv 0 \pmod{4} \\ x^2 + xy + \frac{1-D}{4}y^2 & D \equiv 1 \pmod{4}. \end{array}$$

- The principal form has discriminant D and is reduced.
- When $D = -4n$, we get $x^2 + ny^2$.

Principal Form

Definition

Given a negative integer $D \equiv 0, 1 \pmod{4}$, the **principal form** is defined to be:

$$\begin{aligned} x^2 - \frac{D}{4}y^2, & \quad D \equiv 0 \pmod{4} \\ x^2 + xy + \frac{1-D}{4}y^2 & \quad D \equiv 1 \pmod{4}. \end{aligned}$$

- The principal form has discriminant D and is reduced.
- When $D = -4n$, we get $x^2 + ny^2$.

Principal Form

Definition

Given a negative integer $D \equiv 0, 1 \pmod{4}$, the **principal form** is defined to be:

$$\begin{aligned} x^2 - \frac{D}{4}y^2, & \quad D \equiv 0 \pmod{4} \\ x^2 + xy + \frac{1-D}{4}y^2 & \quad D \equiv 1 \pmod{4}. \end{aligned}$$

- The principal form has discriminant D and is reduced.
- When $D = -4n$, we get $x^2 + ny^2$.

Values Represented by Quadratic Forms of a Same Disc

Lemma

Given a negative integer $D \equiv 0, 1 \pmod{4}$, let $\ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$ be as defined before, and let $f(x, y)$ be a form of discriminant D .

- i The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup $H \subset \ker(\chi)$.
- ii The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form a coset of H in $\ker(\chi)$.

Values Represented by Quadratic Forms of a Same Disc

Lemma

Given a negative integer $D \equiv 0, 1 \pmod{4}$, let $\ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$ be as defined before, and let $f(x, y)$ be a form of discriminant D .

- i The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup $H \subset \ker(\chi)$.
- ii The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form a coset of H in $\ker(\chi)$.

Values Represented by Quadratic Forms of a Same Disc

Lemma

Given a negative integer $D \equiv 0, 1 \pmod{4}$, let $\ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$ be as defined before, and let $f(x, y)$ be a form of discriminant D .

- i The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup $H \subset \ker(\chi)$.
- ii The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form a coset of H in $\ker(\chi)$.

Definition

If $f(x, y)$ and $g(x, y)$ are primitive positive definite forms of discriminant D , then a form $F(x, y)$ of the same type is their **composition** provided that:

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)),$$

where,

$$B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw, i = 1, 2$$

are integral bi-linear forms.

Composition

Direct Composition

- Two forms can be composed in many different ways, and the resulting forms need not be properly equivalent.
- If we want a well-defined operation on classes of forms, we must somehow **restrict** the notion of composition.

Proposition

Given the above composition data, Gauss proved that:

$$a_1 b_2 - a_2 b_1 = \pm f(1, 0), \quad a_1 c_2 - a_2 c_1 = \pm g(1, 0) *$$

Definition

The composition to be a **direct composition** provided that both signs are in $*$ are $+$.

Composition

Direct Composition

- Two forms can be composed in many different ways, and the resulting forms need not be properly equivalent.
- If we want a well-defined operation on classes of forms, we must somehow **restrict** the notion of composition.

Proposition

Given the above composition data, Gauss proved that:

$$a_1 b_2 - a_2 b_1 = \pm f(1, 0), \quad a_1 c_2 - a_2 c_1 = \pm g(1, 0) *$$

Definition

The composition to be a **direct composition** provided that both signs are in $*$ are $+$.

Composition

Direct Composition

- Two forms can be composed in many different ways, and the resulting forms need not be properly equivalent.
- If we want a well-defined operation on classes of forms, we must somehow **restrict** the notion of composition.

Proposition

Given the above composition data, Gauss proved that:

$$a_1 b_2 - a_2 b_1 = \pm f(1, 0), \quad a_1 c_2 - a_2 c_1 = \pm g(1, 0) *$$

Definition

The composition to be a **direct composition** provided that both signs are in $*$ are $+$.

Composition

Direct Composition

- Two forms can be composed in many different ways, and the resulting forms need not be properly equivalent.
- If we want a well-defined operation on classes of forms, we must somehow **restrict** the notion of composition.

Proposition

Given the above composition data, Gauss proved that:

$$a_1 b_2 - a_2 b_1 = \pm f(1, 0), \quad a_1 c_2 - a_2 c_1 = \pm g(1, 0) *$$

Definition

The composition to be a **direct composition** provided that both signs are in $*$ are $+$.

Lemma

Assume that $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ have discriminant D and satisfy $\gcd(a, a', (b + b')/2) = 1$ (since b and b' have the same parity, $(b + b')/2$ is an integer). Then there is a unique integer B modulo $2aa'$ such that:

$$B \equiv b \pmod{2a}$$

$$B \equiv b' \pmod{2a'}$$

$$B^2 \equiv D \pmod{4aa'}.$$

Definition

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant $D < 0$ which satisfy $\gcd(a, a', (b + b')/2) = 1$. Then the **Dirichlet composition** of $f(x, y)$ and $g(x, y)$ is the form

$$f(x, y)g(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

where B is the integer determined by the previous lemma.

Grouping Reduced Forms of Dics D

Definition

- i Let $C(D)$ be the set of classes of primitive positive definite forms of discriminant D . The group $C(D)$ is called the **class group**.
- ii The principal form of discriminant D introduced lies in what is called the **principal class**.
- iii The form $ax^2 - bxy + cy^2$ is called the **opposite** of $ax^2 + bxy + cy^2$.

Grouping Reduced Forms of Dics D

Definition

- i Let $C(D)$ be the set of classes of primitive positive definite forms of discriminant D . The group $C(D)$ is called the **class group**.
- ii The principal form of discriminant D introduced lies in what is called the **principal class**.
- iii The form $ax^2 - bxy + cy^2$ is called the **opposite** of $ax^2 + bxy + cy^2$.

Grouping Reduced Forms of Dics D

Definition

- i Let $C(D)$ be the set of classes of primitive positive definite forms of discriminant D . The group $C(D)$ is called the **class group**.
- ii The principal form of discriminant D introduced lies in what is called the **principal class**.
- iii The form $ax^2 - bxy + cy^2$ is called the **opposite** of $ax^2 + bxy + cy^2$.

Grouping Reduced Forms of Dics D

Theorem

Let $D \equiv 0, 1 \pmod{4}$ be negative. The Dirichlet composition induces a well-defined binary operation on $C(D)$, which makes $C(D)$ into a finite Abelian group whose order is the class number $h(D)$.

Furthermore, the identity element of $C(D)$ is the class containing the principal form.

$$\begin{array}{ll} x^2 - \frac{D}{4}y^2 & \text{if } D \equiv 0 \pmod{4} \\ x^2 + xy + \frac{1-D}{4}y^2 & \text{if } D \equiv 1 \pmod{4}, \end{array}$$

and the inverse of the class containing the for $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

Elements of Order ≤ 2

Lemma

A reduced form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant D has order ≤ 2 in the class group $C(D)$ if and only if $b = 0$, $a = b$ or $a = c$.

Proposition

Let $D \equiv 0, 1 \pmod{4}$ be negative, and let r be the number of odd primes dividing D . Define the number μ as follows: if $D \equiv 1 \pmod{4}$, then $\mu = r$, and if $D \equiv 0 \pmod{4}$, then $D = -4n$, where $n > 0$, and μ is determined by the following table:

n	μ
$n \equiv 3 \pmod{4}$	r
$n \equiv 1, 2 \pmod{4}$	$r + 1$
$n \equiv 4 \pmod{8}$	$r + 1$
$n \equiv 0 \pmod{8}$	$r + 2$

Then the class group $C(D)$ has exactly $2^{\mu-1}$ elements of order ≤ 2 .

Genus Theory to the Class Group $C(D)$

Next Step. To relate genus theory to the class group $C(D)$.

- All forms in a given class represent the same numbers.
- Sending the class to the coset of $H \subset \ker(\chi)$ it represents defines a map

$$\Phi : C(D) \longrightarrow \ker(\chi)/H$$

- i A given fiber $\Phi^{-1}(H'), H' \in \ker(\chi)/H$, consists of all classes in a given genus (this is what we called the genus of H')
- ii The image of Φ can be identified with the set of genera.

Genus Theory to the Class Group $C(D)$

Next Step. To relate genus theory to the class group $C(D)$.

- All forms in a given class represent the same numbers.
- Sending the class to the coset of $H \subset \ker(\chi)$ it represents defines a map

$$\Phi : C(D) \longrightarrow \ker(\chi)/H$$

- i A given fiber $\Phi^{-1}(H'), H' \in \ker(\chi)/H$, consists of all classes in a given genus (this is what we called the genus of H')
- ii The image of Φ can be identified with the set of genera.

Genus Theory to the Class Group $C(D)$

Next Step. To relate genus theory to the class group $C(D)$.

- All forms in a given class represent the same numbers.
- Sending the class to the coset of $H \subset \ker(\chi)$ it represents defines a map

$$\Phi : C(D) \longrightarrow \ker(\chi)/H$$

- i A given fiber $\Phi^{-1}(H'), H' \in \ker(\chi)/H$, consists of all classes in a given genus (this is what we called the genus of H')
- ii The image of Φ can be identified with the set of genera.

Genus Theory to the Class Group $C(D)$

Next Step. To relate genus theory to the class group $C(D)$.

- All forms in a given class represent the same numbers.
- Sending the class to the coset of $H \subset \ker(\chi)$ it represents defines a map

$$\Phi : C(D) \longrightarrow \ker(\chi)/H$$

- ① A given fiber $\Phi^{-1}(H'), H' \in \ker(\chi)/H$, consists of all classes in a given genus (this is what we called the genus of H')
- ② The image of Φ can be identified with the set of genera.

Genus Theory to the Class Group $C(D)$

Next Step. To relate genus theory to the class group $C(D)$.

- All forms in a given class represent the same numbers.
- Sending the class to the coset of $H \subset \ker(\chi)$ it represents defines a map

$$\Phi : C(D) \longrightarrow \ker(\chi)/H$$

- ① A given fiber $\Phi^{-1}(H'), H' \in \ker(\chi)/H$, consists of all classes in a given genus (this is what we called the genus of H')
- ② The image of Φ can be identified with the set of genera.

Proposition

Let $D \equiv 0, 1 \pmod{4}$ be negative. Then:

- 1 All genera of forms of disc D consist of the same number of classes.
- 2 The number of genera of forms of discriminant D is a power of two. More specifically, there are $2^{\mu-1}$ genera of forms of discriminant D , where μ is defined before.

Proposition

Let $D \equiv 0, 1 \pmod{4}$ be negative. Then:

- 1 All genera of forms of disc D consist of the same number of classes.
- 2 The number of genera of forms of discriminant D is a power of two. More specifically, there are $2^{\mu-1}$ genera of forms of discriminant D , where μ is defined before.

Proposition

Let $D \equiv 0, 1 \pmod{4}$ be negative. Then:

- 1 All genera of forms of disc D consist of the same number of classes.
- 2 The number of genera of forms of discriminant D is a power of two. More specifically, there are $2^{\mu-1}$ genera of forms of discriminant D , where μ is defined before.

When a Genus has a Single Class

Theorem

Let n be a positive integer. Then the following statements are equivalent:

- i Every genus of forms of discriminant $-4n$ consists of a single class.
- ii If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$ or $a = c$.
- iii The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$.
- iv The class number $h(-4n)$ equals $2^{\mu-1}$, where μ is defined before.

When a Genus has a Single Class

Theorem

Let n be a positive integer. Then the following statements are equivalent:

- i Every genus of forms of discriminant $-4n$ consists of a single class.
- ii If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$ or $a = c$.
- iii The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$.
- iv The class number $h(-4n)$ equals $2^{\mu-1}$, where μ is defined before.

When a Genus has a Single Class

Theorem

Let n be a positive integer. Then the following statements are equivalent:

- i Every genus of forms of discriminant $-4n$ consists of a single class.
- ii If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$ or $a = c$.
- iii The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$.
- iv The class number $h(-4n)$ equals $2^{\mu-1}$, where μ is defined before.

When a Genus has a Single Class

Theorem

Let n be a positive integer. Then the following statements are equivalent:

- i Every genus of forms of discriminant $-4n$ consists of a single class.
- ii If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$ or $a = c$.
- iii The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$.
- iv The class number $h(-4n)$ equals $2^{\mu-1}$, where μ is defined before.

When a Genus has a Single Class

Theorem

Let n be a positive integer. Then the following statements are equivalent:

- i Every genus of forms of discriminant $-4n$ consists of a single class.
- ii If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$ or $a = c$.
- iii The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}$.
- iv The class number $h(-4n)$ equals $2^{\mu-1}$, where μ is defined before.

Dics' Satisfying Genera with a Single Class

Some Interesting History

- Gauss lists 65 discriminants that satisfy the previous theorem, he was interested in these 65 n 's not for their relation to the question of when $p = x^2 + ny^2$, but rather because they had been discovered earlier by Euler in a different context.
- Gauss suggests that the 65 given by Euler are the only ones.
- In 1934 Chowla proved that the number of such n 's is finite.
- In 1973 it was known that Euler's list is complete except for possibly one more n .
- Whether or not this last n actually exists is still an open question.

Dics' Satisfying Genera with a Single Class

Some Interesting History

- Gauss lists 65 discriminants that satisfy the previous theorem, he was interested in these 65 n 's not for their relation to the question of when $p = x^2 + ny^2$, but rather because they had been discovered earlier by Euler in a different context.
- Gauss suggests that the 65 given by Euler are the only ones.
- In 1934 Chowla proved that the number of such n 's is finite.
- In 1973 it was known that Euler's list is complete except for possibly one more n .
- Whether or not this last n actually exists is still an open question.

Dics' Satisfying Genera with a Single Class

Some Interesting History

- Gauss lists 65 discriminants that satisfy the previous theorem, he was interested in these 65 n 's not for their relation to the question of when $p = x^2 + ny^2$, but rather because they had been discovered earlier by Euler in a different context.
- Gauss suggests that the 65 given by Euler are the only ones.
- In 1934 Chowla proved that the number of such n 's is finite.
- In 1973 it was known that Euler's list is complete except for possibly one more n .
- Whether or not this last n actually exists is still an open question.

Dics' Satisfying Genera with a Single Class

Some Interesting History

- Gauss lists 65 discriminants that satisfy the previous theorem, he was interested in these 65 n 's not for their relation to the question of when $p = x^2 + ny^2$, but rather because they had been discovered earlier by Euler in a different context.
- Gauss suggests that the 65 given by Euler are the only ones.
- In 1934 Chowla proved that the number of such n 's is finite.
- In 1973 it was known that Euler's list is complete except for possibly one more n .
- Whether or not this last n actually exists is still an open question.

Dics' Satisfying Genera with a Single Class

Some Interesting History

- Gauss lists 65 discriminants that satisfy the previous theorem, he was interested in these 65 n 's not for their relation to the question of when $p = x^2 + ny^2$, but rather because they had been discovered earlier by Euler in a different context.
- Gauss suggests that the 65 given by Euler are the only ones.
- In 1934 Chowla proved that the number of such n 's is finite.
- In 1973 it was known that Euler's list is complete except for possibly one more n .
- Whether or not this last n actually exists is still an open question.

Convenient number

Definition

Euler called a number n a **convenient number** if it satisfies the following criterion:

Let m be an odd number relatively prime to n , which is properly represented by $x^2 + ny^2$. If the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$, then m is a prime number.

- Euler was interested in convenient numbers because they helped him find large primes.

Proposition

A positive integer n is a convenient number if and only if for forms of discriminant $-4n$, every genus consists of a single class.

Convenient number

Definition

Euler called a number n a **convenient number** if it satisfies the following criterion:

Let m be an odd number relatively prime to n , which is properly represented by $x^2 + ny^2$. If the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$, then m is a prime number.

- Euler was interested in convenient numbers because they helped him find large primes.

Proposition

A positive integer n is a convenient number if and only if for forms of discriminant $-4n$, every genus consists of a single class.

Convenient number

Definition

Euler called a number n a **convenient number** if it satisfies the following criterion:

Let m be an odd number relatively prime to n , which is properly represented by $x^2 + ny^2$. If the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$, then m is a prime number.

- Euler was interested in convenient numbers because they helped him find large primes.

Proposition

A positive integer n is a convenient number if and only if for forms of discriminant $-4n$, every genus consists of a single class.

Genus Theory's Limitation

Note

Genus theory cannot solve our basic question for all n .

Example

$D = -108$ Genus theory is completely use less, since all three reduced forms $x^2 + 27y^2$ and $4x^2 \pm 2xy + 7y^2$ lie in the same genus.

Genus Theory's Limitation

Note

Genus theory cannot solve our basic question for all n .

Example

$D = -108$ Genus theory is completely use less, since all three reduced forms $x^2 + 27y^2$ and $4x^2 \pm 2xy + 7y^2$ lie in the same genus.

The Law of Cubic Reciprocity

Theorem

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod{3} \text{ and } 2 \text{ is a} \\ \text{cubic residue modulo } p \end{cases}$$

- The law of cubic reciprocity is intimately bound up with the ring $\mathbb{Z}[\omega]$.
- The main tool used to study the arithmetic of $\mathbb{Z}[\omega]$ is the norm function.

The Law of Cubic Reciprocity

Theorem

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod{3} \text{ and } 2 \text{ is a} \\ \text{cubic residue modulo } p \end{cases}$$

- The law of cubic reciprocity is intimately bound up with the ring $\mathbb{Z}[\omega]$.
- The main tool used to study the arithmetic of $\mathbb{Z}[\omega]$ is the norm function.

The Law of Cubic Reciprocity

Theorem

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod{3} \text{ and } 2 \text{ is a} \\ \text{cubic residue modulo } p \end{cases}$$

- The law of cubic reciprocity is intimately bound up with the ring $\mathbb{Z}[\omega]$.
- The main tool used to study the arithmetic of $\mathbb{Z}[\omega]$ is the norm function.

The Law of Bi-quadratic Reciprocity

Theorem

$$p = x^2 + 64y^2 \iff \begin{cases} p \equiv 1 \pmod{4} \text{ and } 2 \text{ is a} \\ \text{biquadratic residue modulo } p \end{cases}$$

- The law of bi-quadratic reciprocity is intimately bound up with the ring $\mathbb{Z}[i]$ (The Ring of Gaussian Integers).
- Also, our main tool is the Norm function.

The Law of Bi-quadratic Reciprocity

Theorem

$$p = x^2 + 64y^2 \iff \begin{cases} p \equiv 1 \pmod{4} \text{ and } 2 \text{ is a} \\ \text{biquadratic residue modulo } p \end{cases}$$

- The law of bi-quadratic reciprocity is intimately bound up with the ring $\mathbb{Z}[i]$ (The Ring of Gaussian Integers).
- Also, our main tool is the Norm function.

The Law of Bi-quadratic Reciprocity

Theorem

$$p = x^2 + 64y^2 \iff \begin{cases} p \equiv 1 \pmod{4} \text{ and } 2 \text{ is a} \\ \text{biquadratic residue modulo } p \end{cases}$$

- The law of bi-quadratic reciprocity is intimately bound up with the ring $\mathbb{Z}[i]$ (The Ring of Gaussian Integers).
- Also, our main tool is the Norm function.

Field Theory

Field Extension

Definition

- i If L is a field containing the sub-field K , then L is said to be an **extension field** (or simply an **extension**) of K , denoted L/K .
- ii The **degree** of a field extension L/K , denoted $[L : K]$, is the dimension of L as a vector space over K .

Example

$\mathbb{C}/\mathbb{R}$ is a field extension of degree 2.

Definition

- i If L is a field containing the sub-field K , then L is said to be an **extension field** (or simply an **extension**) of K , denoted L/K .
- ii The **degree** of a field extension L/K , denoted $[L : K]$, is the dimension of L as a vector space over K .

Example

$\mathbb{C}/\mathbb{R}$ is a field extension of degree 2.

Definition

- i If L is a field containing the sub-field K , then L is said to be an **extension field** (or simply an **extension**) of K , denoted L/K .
- ii The **degree** of a field extension L/K , denoted $[L : K]$, is the dimension of L as a vector space over K .

Example

$\mathbb{C}/\mathbb{R}$ is a field extension of degree 2.

Definition

An algebraic **number field** is an extension field L of the field of rational numbers $\mathbb{Q}$ such that the field extension $L/\mathbb{Q}$ has a finite degree.

Example

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a number field of degree 2.

Definition

An algebraic **number field** is an extension field L of the field of rational numbers $\mathbb{Q}$ such that the field extension $L/\mathbb{Q}$ has a finite degree.

Example

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a number field of degree 2.

Field Theory

Galois Extension

Definition

A **Galois extension** is an algebraic field extension L/K that is normal and separable.

Example

$\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is a Galois Extension. (ω is the 3rd root of unity.)

Definition

A **Galois extension** is an algebraic field extension L/K that is normal and separable.

Example

$\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is a Galois Extension. (ω is the 3rd root of unity.)

The Ring of Algebraic Integers

Definition

The ring of algebraic integers of a number field K is the ring of all algebraic integers contained in K .

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

- 1 $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- 2 $\mathcal{O}_{\mathbb{Q}\sqrt{-5}} = \mathbb{Z}\sqrt{-5}$

Proposition

We have unique factorization to prime ideals in $\mathcal{O}_K$.

The Ring of Algebraic Integers

Definition

The ring of algebraic integers of a number field K is the ring of all algebraic integers contained in K .

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

- 1 $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- 2 $\mathcal{O}_{\mathbb{Q}\sqrt{-5}} = \mathbb{Z}\sqrt{-5}$

Proposition

We have unique factorization to prime ideals in $\mathcal{O}_K$.

The Ring of Algebraic Integers

Definition

The ring of algebraic integers of a number field K is the ring of all algebraic integers contained in K .

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

- 1 $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- 2 $\mathcal{O}_{\mathbb{Q}\sqrt{-5}} = \mathbb{Z}\sqrt{-5}$

Proposition

We have unique factorization to prime ideals in $\mathcal{O}_K$.

The Ring of Algebraic Integers

Definition

The ring of algebraic integers of a number field K is the ring of all algebraic integers contained in K .

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

- 1 $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- 2 $\mathcal{O}_{\mathbb{Q}\sqrt{-5}} = \mathbb{Z}\sqrt{-5}$

Proposition

We have unique factorization to prime ideals in $\mathcal{O}_K$.

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

Primes in $\mathcal{O}_K$

Definition

Let p be a prime, and suppose that K is a number field and

$$p = \beta_1^{e_1} \beta_2^{e_2} \dots \beta_g^{e_g}$$

- i p **splits completely** in $\mathcal{O}_K$ if $e_i = 1$ for all $i \in \{1, 2, \dots, g\}$.
- ii p is **inert** in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.
- iii p **ramifies** in $\mathcal{O}_K$ if $\exists i \in \{1, 2, \dots, g\}$ such that $e_i > 1$.

Example

Let $K = \mathbb{Q}[i]$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Now:

- i $\langle 5 \rangle = \langle 1 + 2i \rangle \langle 2 + i \rangle$
- ii $\langle 3 \rangle$
- iii $\langle 2 \rangle = \langle 1 + i \rangle^2$

The Ring of Algebraic Integers for Quadratic Fields

Proposition

The ring of algebraic integers $\mathcal{O}_K$ of the quadratic field K . when $K = \mathbb{Q}(\sqrt{N})$ and N is squarefree, equals to :

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & N \not\equiv 1 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & N \equiv 1 \pmod{4} \end{cases}$$

Theorem

Given a number field K , there is a finite Galois extension L of K such that:

- i L is an unramified Abelian extension of K .
- ii Any unramified Abelian extension of K lies in L .

Definition

The field L of the Theorem is called the **Hilbert class field** of K .

Theorem

Given a number field K , there is a finite Galois extension L of K such that:

- i L is an unramified Abelian extension of K .
- ii Any unramified Abelian extension of K lies in L .

Definition

The field L of the Theorem is called the **Hilbert class field** of K .

Theorem

Given a number field K , there is a finite Galois extension L of K such that:

- i L is an unramified Abelian extension of K .
- ii Any unramified Abelian extension of K lies in L .

Definition

The field L of the Theorem is called the **Hilbert class field** of K .

Theorem

Given a number field K , there is a finite Galois extension L of K such that:

- i L is an unramified Abelian extension of K .
- ii Any unramified Abelian extension of K lies in L .

Definition

The field L of the Theorem is called the **Hilbert class field** of K .

Solution of $p = x^2 + ny^2$ for Infinitely Many n

Theorem

Let $n > 0$ be an integer satisfying the following condition:

$$n \text{ squarefree, } n \not\equiv 3 \pmod{4}.$$

Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$.

Artin Symbol

Lemma

Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in L . If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\sigma \in \text{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$.

Definition

The unique element σ of Lemma is called the **Artin symbol** and is denoted $\left(\frac{L/K}{\mathfrak{P}}\right)$ since it depends on the prime $\mathfrak{P}$ of L . Also, for any $\alpha \in \mathcal{O}_L$, we have

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}},$$

Artin Symbol

Lemma

Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in L . If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\sigma \in \text{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$.

Definition

The unique element σ of Lemma is called the **Artin symbol** and is denoted $\left(\frac{L/K}{\mathfrak{P}}\right)$ since it depends on the prime $\mathfrak{P}$ of L . Also, for any $\alpha \in \mathcal{O}_L$, we have

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}},$$

Relation $C(\mathcal{O}_K)$ and $\text{Gal}(L/K)$.

Definition

- $I_K :=$ Groups of fractional ideals of $\mathcal{O}_K$
- $P_K :=$ Groups of principal fractional ideals of $\mathcal{O}_K$

Theorem

If L is the Hilbert class field of a number field K , then the Artin map

$$\left(\frac{L/K}{\cdot} \right) : I_K \longrightarrow \text{Gal}(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K .
Thus the Artin map induces an isomorphism

$$C(\mathcal{O}_K) \xrightarrow{\sim} \text{Gal}(L/K).$$

Relation $C(\mathcal{O}_K)$ and $\text{Gal}(L/K)$.

Definition

- $I_K :=$ Groups of fractional ideals of $\mathcal{O}_K$
- $P_K :=$ Groups of principal fractional ideals of $\mathcal{O}_K$

Theorem

If L is the Hilbert class field of a number field K , then the Artin map

$$\left(\frac{L/K}{\cdot} \right) : I_K \longrightarrow \text{Gal}(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K .
Thus the Artin map induces an isomorphism

$$C(\mathcal{O}_K) \xrightarrow{\sim} \text{Gal}(L/K).$$

Relation $C(\mathcal{O}_K)$ and $\text{Gal}(L/K)$.

Definition

- $I_K :=$ Groups of fractional ideals of $\mathcal{O}_K$
- $P_K :=$ Groups of principal fractional ideals of $\mathcal{O}_K$

Theorem

If L is the Hilbert class field of a number field K , then the Artin map

$$\left(\frac{L/K}{\cdot} \right) : I_K \longrightarrow \text{Gal}(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K .
Thus the Artin map induces an isomorphism

$$C(\mathcal{O}_K) \xrightarrow{\sim} \text{Gal}(L/K).$$

Relation between $C(d_K)$ and $C(\mathcal{O}_K)$

Theorem

Let K be an imaginary quadratic field of discriminant $d_K < 0$. Then:

- i If $f(x, y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d_K , then

$$\left[a, \left(-b + \sqrt{d_K} \right) / 2 \right] = \left\{ ma + n \left(-b + \sqrt{d_K} \right) / 2 : m, n \in \mathbb{Z} \right\}$$

is an ideal of $\mathcal{O}_K$.

- ii The map sending $f(x, y)$ to $\left[a, \left(-b + \sqrt{d_K} \right) / 2 \right]$ induces an isomorphism between the form class group $C(d_K)$ and the ideal class group $C(\mathcal{O}_K)$. Hence the order of $C(\mathcal{O}_K)$ is the class number $h(d_K)$.

Relation between $C(d_K)$ and $C(\mathcal{O}_K)$

Theorem

Let K be an imaginary quadratic field of discriminant $d_K < 0$. Then:

- 1 If $f(x, y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d_K , then

$$\left[a, \left(-b + \sqrt{d_K} \right) / 2 \right] = \left\{ ma + n \left(-b + \sqrt{d_K} \right) / 2 : m, n \in \mathbb{Z} \right\}$$

is an ideal of $\mathcal{O}_K$.

- ii The map sending $f(x, y)$ to $\left[a, \left(-b + \sqrt{d_K} \right) / 2 \right]$ induces an isomorphism between the form class group $C(d_K)$ and the ideal class group $C(\mathcal{O}_K)$. Hence the order of $C(\mathcal{O}_K)$ is the class number $h(d_K)$.

Relation between $C(d_K)$ and $C(\mathcal{O}_K)$

Theorem

Let K be an imaginary quadratic field of discriminant $d_K < 0$. Then:

- 1 If $f(x, y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d_K , then

$$\left[a, \left(-b + \sqrt{d_K} \right) / 2 \right] = \left\{ ma + n \left(-b + \sqrt{d_K} \right) / 2 : m, n \in \mathbb{Z} \right\}$$

is an ideal of $\mathcal{O}_K$.

- ii The map sending $f(x, y)$ to $\left[a, \left(-b + \sqrt{d_K} \right) / 2 \right]$ induces an isomorphism between the form class group $C(d_K)$ and the ideal class group $C(\mathcal{O}_K)$. Hence the order of $C(\mathcal{O}_K)$ is the class number $h(d_K)$.

Example of Hilbert Class Fields

Base Field $K = \mathbb{Q}(\sqrt{-14})$

Proposition

The Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ is $L = K(\alpha)$, where $\alpha = \sqrt{2\sqrt{2} - 1}$.

Theorem

If $p \neq 7$ is an odd prime, then

$$p = x^2 + 14y^2 \iff \begin{cases} (-14/p) = 1 \text{ and } (x^2 + 1)^2 \equiv 8 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

Example of Hilbert Class Fields

Base Field $K = \mathbb{Q}(\sqrt{-14})$

Proposition

The Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ is $L = K(\alpha)$, where $\alpha = \sqrt{2\sqrt{2} - 1}$.

Theorem

If $p \neq 7$ is an odd prime, then

$$p = x^2 + 14y^2 \iff \begin{cases} (-14/p) = 1 \text{ and } (x^2 + 1)^2 \equiv 8 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

Solution of $p = x^2 + ny^2$ for All n

Theorem

Let $n > 0$ be an integer. Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$.

Finally, if $f_n(x)$ is any monic integer polynomial of degree $h(-4n)$ for which the above equivalence holds, then $f_n(x)$ is irreducible over $\mathbb{Z}$ and is the minimal polynomial of a primitive element of the ring class field L described above.

Example of Ring Class Fields

Base Field $K = \mathbb{Q}(\sqrt{-27})$

Proposition

The ring class field of the order $\mathbb{Z}[\sqrt{-27}] \subset K = \mathbb{Q}(\sqrt{-3})$ is $L = K(\sqrt[3]{2})$.

Theorem

If $p > 3$ is prime, then

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod{3} \text{ and } x^3 \equiv 2 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$

Example of Ring Class Fields

Base Field $K = \mathbb{Q}(\sqrt{-27})$

Proposition

The ring class field of the order $\mathbb{Z}[\sqrt{-27}] \subset K = \mathbb{Q}(\sqrt{-3})$ is $L = K(\sqrt[3]{2})$.

Theorem

If $p > 3$ is prime, then

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod{3} \text{ and } x^3 \equiv 2 \pmod{p} \\ \text{has an integer solution.} \end{cases}$$