Intersecting Finite Sets of Positive Definite Integral Binary Quadratic Forms

Christopher Donnay, Havi Ellers, Kate O'Connor, Erin Wood

January 13, 2018

Acknowledgements

The Department of Mathematics and Statistics at Wake Forest

Acknowledgements

The Department of Mathematics and Statistics at Wake Forest
The NSF

Acknowledgements

The Department of Mathematics and Statistics at Wake Forest
The NSF
Professor Rouse

Acknowledgements

The Department of Mathematics and Statistics at Wake Forest
The NSF
Professor Rouse
Professor Thompson

Acknowledgements

The Department of Mathematics and Statistics at Wake Forest
The NSF
Professor Rouse
Professor Thompson
Organizers

Outline

Definition (Integral Binary Quadratic Form)

An **integral binary quadratic form** is a homogeneous polynomial $Q : \mathbb{Z}^2 \to \mathbb{Z}$ such that

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

Definition (Integral Binary Quadratic Form)

An **integral binary quadratic form** is a homogeneous polynomial $Q : \mathbb{Z}^2 \to \mathbb{Z}$ such that

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

Definition (Represented)

We say that an integer m is **represented** by a form $Q(x, y) = ax^2 + bxy + cy^2$ if there exist integers x and y such that $Q(x, y) = m$.

Definition (Intersection)

Let $S = \{Q_1, \ldots, Q_n\}$ be a set of quadratic forms. We say the **intersection** of S is the set of numbers that are represented by all of $Q_1, \ldots, Q_n$.

Definition (Intersection)

Let $S = \{Q_1, \ldots, Q_n\}$ be a set of quadratic forms. We say the **intersection** of S is the set of numbers that are represented by all of $Q_1, \ldots, Q_n$.

Definition (Trivial)

We say the intersection of $\{Q_1, \ldots, Q_n\}$ is **trivial** if the only number represented by all of $Q_1, \ldots, Q_n$ is 0.

Definition (Discriminant)

The **discriminant** of an integral binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is

$$\Delta = b^2 - 4ac.$$

Δ is a **fundamental discriminant** if and only if either:

- $\Delta \equiv 1 \pmod 4$ and is square-free, or,
- $\Delta = 4n$ for $n \in \mathbb{Z}$ such that $n \equiv 2, 3 \pmod 4$ and n is square-free.

Definition (Positive-Definite)

An integral binary quadratic form Q is said to be **positive-definite** if

(1) $Q(x, y) = 0 \Leftrightarrow x = 0$ and $y = 0$,

(2) For all (x, y) such that $x \neq 0$ and/or $y \neq 0$, $Q(x, y) > 0$.

Definition (Positive-Definite)

An integral binary quadratic form Q is said to be **positive-definite** if

(1) $Q(x, y) = 0 \Leftrightarrow x = 0$ and $y = 0$,

(2) For all (x, y) such that $x \neq 0$ and/or $y \neq 0$, $Q(x, y) > 0$.

Definition (Reduced)

A positive-definite integral binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is said to be **reduced** if

(1) $|b| \leq a \leq c$,

(2) $b \geq 0$ if $|b| = a$ or if $a = c$.

There is an equivalence relation between forms of the same discriminant.

1. Equivalent forms represent the same integers.
2. Proper equivalence and improper equivalence are defined using integral matrices of determinant 1 and -1 respectively.

There is an equivalence relation between forms of the same discriminant.

1. Equivalent forms represent the same integers.
2. Proper equivalence and improper equivalence are defined using integral matrices of determinant 1 and -1 respectively.

Definition (Proper Equivalence Class)

Two forms are in the same **proper equivalence class** if they are properly equivalent.

There is an equivalence relation between forms of the same discriminant.

1. Equivalent forms represent the same integers.
2. Proper equivalence and improper equivalence are defined using integral matrices of determinant 1 and -1 respectively.

Definition (Proper Equivalence Class)

Two forms are in the same **proper equivalence class** if they are properly equivalent.

Fact: These proper classes partition the set of quadratic forms of a fixed discriminant.

Definition (Class Number)

Let $\Delta < 0$ be fixed. Then the **class number** of Δ, denoted $h(\Delta)$, is the number of reduced forms of discriminant Δ.

Definition (Class Number)

Let $\Delta < 0$ be fixed. Then the **class number** of Δ, denoted $h(\Delta)$, is the number of reduced forms of discriminant Δ.

Definition (Class Group)

Let $\Delta \equiv 0, 1 \pmod 4$ be negative. Then the **class group** of Δ, denoted $C(\Delta)$, is the finite abelian group formed by the set of classes of primitive positive definite forms of discriminant Δ, whose order is the class number $h(\Delta)$. We choose the representative of a class to be the unique reduced form of the class.

Definition (Composition)

The group operation of the class group is called **composition**.

Definition (Composition)

The group operation of the class group is called **composition**.

The composition of two forms Q_1 and Q_2 is denoted as $Q_1 \circ Q_2$.

Definition (Composition)

The group operation of the class group is called **composition**.

The composition of two forms Q_1 and Q_2 is denoted as $Q_1 \circ Q_2$.

Fact: Let Q_1 and Q_2 be two forms of the same discriminant. If n_1 is represented by Q_1 and n_2 is represented by Q_2, then $n_1 n_2$ is represented by $Q_1 \circ Q_2$.

Definition (Principal Form)

The identity element of the class group is called the **principal form**, and is given by the following formula:

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

When do finite sets of positive definite integral binary quadratic forms have a trivial intersection? When do they have a non-trivial intersection?

Example

Let $\Delta = -20$. Then $h(\Delta) = 2$ and the two reduced forms of discriminant Δ are

$$\begin{aligned} Q_1(x,y) &= x^2 + 5y^2 \\ Q_2(x,y) &= 2x^2 + 2xy + 3y^2. \end{aligned}$$

Intersecting Forms of a Fixed Discriminant

Theorem (DEOTW)

Let $\Delta < 0$ be congruent to 0 or 1 mod 4 and let S_Δ be the set of all reduced, positive-definite binary quadratic forms of discriminant Δ. If $h(\Delta) = 2k$ for $k \in \mathbb{Z}$ and Δ is a fundamental discriminant then the intersection of all of the forms in S_Δ is trivial.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Example: Let $\Delta = -47$. Then $h(\Delta) = 5$.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Example: Let $\Delta = -47$. Then $h(\Delta) = 5$.

We know by an already proven lemma that a prime p is represented by some form of discriminant -47 if and only if $\left(\frac{p}{47}\right) = 1$.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Example: Let $\Delta = -47$. Then $h(\Delta) = 5$.

We know by an already proven lemma that a prime p is represented by some form of discriminant -47 if and only if $\left(\frac{p}{47}\right) = 1$.

Let n be an integer represented by all forms of discriminant -47 and let Q_i be the form of discriminant -47 that represents p.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Example: Let $\Delta = -47$. Then $h(\Delta) = 5$.

We know by an already proven lemma that a prime p is represented by some form of discriminant -47 if and only if $\left(\frac{p}{47}\right) = 1$.

Let n be an integer represented by all forms of discriminant -47 and let Q_i be the form of discriminant -47 that represents p.

Consider Q_j, another quadratic form of discriminant -47.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Example: Let $\Delta = -47$. Then $h(\Delta) = 5$.

We know by an already proven lemma that a prime p is represented by some form of discriminant -47 if and only if $\left(\frac{p}{47}\right) = 1$.

Let n be an integer represented by all forms of discriminant -47 and let Q_i be the form of discriminant -47 that represents p.

Consider Q_j, another quadratic form of discriminant -47.

Then there exists some form Q_k of discriminant -47 such that $Q_i \circ Q_k = Q_j$.

Intersecting Forms of a Fixed Discriminant

Next, we wanted to determine for which discriminants is the intersection of all forms of that discriminant is nonzero.

Theorem (DEOTW)

If n is represented by all forms F with $\Delta = -q$, where $q \equiv 3 \pmod 4$ is prime, then np, where p is an odd prime, is represented by all such F if $\left(\frac{p}{q}\right) = 1$.

Example: Let $\Delta = -47$. Then $h(\Delta) = 5$.

We know by an already proven lemma that a prime p is represented by some form of discriminant -47 if and only if $\left(\frac{p}{47}\right) = 1$.

Let n be an integer represented by all forms of discriminant -47 and let Q_i be the form of discriminant -47 that represents p.

Consider Q_j, another quadratic form of discriminant -47.

Then there exists some form Q_k of discriminant -47 such that $Q_i \circ Q_k = Q_j$.

Thus, by the composition law of quadratic forms, all forms of discriminant -47 represent np.

While this result is interesting, this theorem alone does not tell us that the intersection of all forms of discriminant -47 is nonzero.

While this result is interesting, this theorem alone does not tell us that the intersection of all forms of discriminant -47 is nonzero.

Theorem (DEOTW)

Let $\Delta < 0$ be congruent to 0 or $1 \pmod 4$ and $h(\Delta) = 2n+1$. Then the product of the x^2 and y^2 coefficients of all the non-principal, non-equivalent forms of discriminant Δ will be represented by all forms of discriminant Δ.

Example: Let $\Delta = -47$. Then we can show that all the forms of discriminant -47 represent the number $144 = 2 \cdot 6 \cdot 3 \cdot 4$.

Example: Let $\Delta = -47$. Then we can show that all the forms of discriminant -47 represent the number $144 = 2 \cdot 6 \cdot 3 \cdot 4$.

We know that the forms of discriminant -47 are

$$\begin{aligned} Q_1 &= x^2 + xy + 12y^2 \\ Q_2 &= 2x^2 + xy + 6y^2 \\ Q_3 &= 2x^2 - xy + 6y^2 \\ Q_4 &= 3x^2 + xy + 4y^2 \\ Q_5 &= 3x^2 - xy + 4y^2. \end{aligned}$$

Based on the Cayley Table obtained by composing these forms, $Q_2 = Q_2 \circ Q_3 \circ Q_4 \circ Q_4$.

Example: Let $\Delta = -47$. Then we can show that all the forms of discriminant -47 represent the number $144 = 2 \cdot 6 \cdot 3 \cdot 4$.

We know that the forms of discriminant -47 are

$$\begin{aligned} Q_1 &= x^2 + xy + 12y^2 \\ Q_2 &= 2x^2 + xy + 6y^2 \\ Q_3 &= 2x^2 - xy + 6y^2 \\ Q_4 &= 3x^2 + xy + 4y^2 \\ Q_5 &= 3x^2 - xy + 4y^2. \end{aligned}$$

Based on the Cayley Table obtained by composing these forms, $Q_2 = Q_2 \circ Q_3 \circ Q_4 \circ Q_4$.

Thus, by the composition law of quadratic forms, Q_2 represents $144 = 2 \cdot 6 \cdot 3 \cdot 4$.

Example: Let $\Delta = -47$. Then we can show that all the forms of discriminant -47 represent the number $144 = 2 \cdot 6 \cdot 3 \cdot 4$.

We know that the forms of discriminant -47 are

$$\begin{aligned} Q_1 &= x^2 + xy + 12y^2 \\ Q_2 &= 2x^2 + xy + 6y^2 \\ Q_3 &= 2x^2 - xy + 6y^2 \\ Q_4 &= 3x^2 + xy + 4y^2 \\ Q_5 &= 3x^2 - xy + 4y^2. \end{aligned}$$

Based on the Cayley Table obtained by composing these forms, $Q_2 = Q_2 \circ Q_3 \circ Q_4 \circ Q_4$.

Thus, by the composition law of quadratic forms, Q_2 represents $144 = 2 \cdot 6 \cdot 3 \cdot 4$.

A similar argument can be used to show that Q_1, Q_3, Q_4, and Q_5 also represent 144.

The proof for the general case uses a similar technique. Since the order of the group is odd, we are guaranteed the following group structure:

The proof for the general case uses a similar technique. Since the order of the group is odd, we are guaranteed the following group structure:

$$
\begin{aligned}
Q_1 &= x^2 + b_0xy + c_0y^2 \\
Q_2 &= a_1x^2 + b_1xy + c_1y^2 \\
Q_3 &= a_1x^2 - b_1xy + c_1y^2 \\
&\vdots \\
Q_{2n} &= a_nx^2 + b_nxy + c_ny^2 \\
Q_{2n+1} &= a_nx^2 - b_nxy + c_ny^2.
\end{aligned}
$$

The proof for the general case uses a similar technique. Since the order of the group is odd, we are guaranteed the following group structure:

$$
\begin{aligned}
Q_1 &= x^2 + b_0xy + c_0y^2 \\
Q_2 &= a_1x^2 + b_1xy + c_1y^2 \\
Q_3 &= a_1x^2 - b_1xy + c_1y^2 \\
&\vdots \\
Q_{2n} &= a_nx^2 + b_nxy + c_ny^2 \\
Q_{2n+1} &= a_nx^2 - b_nxy + c_ny^2.
\end{aligned}
$$

We can then use composition of forms to show that each form represents the product $\prod a_i c_i$.

Theorem (DEOTW)

Given two quadratic forms F_1 and F_2 of discriminants Δ_1 and Δ_2 such that $h(\Delta_1) = h(\Delta_2) = 1$, both forms represent a prime p not dividing the discriminants iff $\left(\frac{\Delta_1}{p}\right) = \left(\frac{\Delta_2}{p}\right) = 1$. Furthermore, if both forms represent p, they are guaranteed to represent the infinite class of integers $n^2 p$ for any $n \in \mathbb{Z}$.

Theorem (DEOTW)

Given two quadratic forms F_1 and F_2 of discriminants Δ_1 and Δ_2 such that $h(\Delta_1) = h(\Delta_2) = 1$, both forms represent a prime p not dividing the discriminants iff $\left(\frac{\Delta_1}{p}\right) = \left(\frac{\Delta_2}{p}\right) = 1$. Furthermore, if both forms represent p, they are guaranteed to represent the infinite class of integers $n^2 p$ for any $n \in \mathbb{Z}$.

By a previously known result, we know that if $\left(\frac{\Delta_1}{p}\right) = 1$, then p must be represented by some form of discriminant Δ_1. Since the class size is 1, F_1 represents p. Similarly, F_2 will represent p.

Theorem (DEOTW)

Given two quadratic forms F_1 and F_2 of discriminants Δ_1 and Δ_2 such that $h(\Delta_1) = h(\Delta_2) = 1$, both forms represent a prime p not dividing the discriminants iff $\left(\frac{\Delta_1}{p}\right) = \left(\frac{\Delta_2}{p}\right) = 1$. Furthermore, if both forms represent p, they are guaranteed to represent the infinite class of integers $n^2 p$ for any $n \in \mathbb{Z}$.

By a previously known result, we know that if $\left(\frac{\Delta_1}{p}\right) = 1$, then p must be represented by some form of discriminant Δ_1. Since the class size is 1, F_1 represents p. Similarly, F_2 will represent p.

We also know that if a form represents an integer m, then it will also represent $n^2 m$ for any $n \in \mathbb{Z}$. Therefore, both forms will represents $n^2 p$ for all $n \in \mathbb{Z}$.

Corollary (DEOTW)

If we take the intersection of all forms of class size 1*, we are guaranteed an infinite set.*

Corollary (DEOTW)

If we take the intersection of all forms of class size 1*, we are guaranteed an infinite set.*

Using quadratic residue laws, we can show that there exists some prime p such that p is represented by all forms of class size 1. Once we have found this prime p, we are guaranteed infinite elements in the intersection of the forms.

Theorem (DEOTW)

Let Δ_1, Δ_2 be discriminants of odd class size. Then all forms of discriminant Δ_1 and Δ_2 will have a non-trivial intersection.

Theorem (DEOTW)

Let Δ_1, Δ_2 be discriminants of odd class size. Then all forms of discriminant Δ_1 and Δ_2 will have a non-trivial intersection.

All forms of discriminant Δ_1 will represent some non-zero integer α. Then all such forms will represent α^2.

Theorem (DEOTW)

Let Δ_1, Δ_2 be discriminants of odd class size. Then all forms of discriminant Δ_1 and Δ_2 will have a non-trivial intersection.

All forms of discriminant Δ_1 will represent some non-zero integer α. Then all such forms will represent α^2.

Likewise, all forms of discriminant Δ_2 will represent an integer β, and therefore β^2. We then see that forms of both discriminants must represent $\alpha^2\beta^2$.

Example

Let $\Delta_1 = -23$ and $\Delta_2 = -47$. The reduced forms of discriminant Δ_1 are:

$$\begin{aligned} Q_1 &= x^2 + xy + 6y^2 \\ Q_2 &= 2x^2 + xy + 3y^2 \\ Q_3 &= 2x^2 - xy + 3y^2. \end{aligned}$$

Example

Let $\Delta_1 = -23$ and $\Delta_2 = -47$. The reduced forms of discriminant Δ_1 are:

$$\begin{aligned} Q_1 &= x^2 + xy + 6y^2 \\ Q_2 &= 2x^2 + xy + 3y^2 \\ Q_3 &= 2x^2 - xy + 3y^2. \end{aligned}$$

By our previous results, these forms each represent 6. Since Q_1 represents 6, we can compose Q_1 with each form to see that the composition of Q_1 with any form will represent 6^2.

Example

Let $\Delta_1 = -23$ and $\Delta_2 = -47$. The reduced forms of discriminant Δ_1 are:

$$\begin{aligned} Q_1 &= x^2 + xy + 6y^2 \\ Q_2 &= 2x^2 + xy + 3y^2 \\ Q_3 &= 2x^2 - xy + 3y^2. \end{aligned}$$

By our previous results, these forms each represent 6. Since Q_1 represents 6, we can compose Q_1 with each form to see that the composition of Q_1 with any form will represent 6^2.

Similarly, each form of discriminant $\Delta = -47$ will represent 144^2. Thus, all forms of discriminants $\Delta = -47$ and $\Delta = -23$ will represent $6^2 \cdot 144^2$.

$px^2 + bxy + qy^2$

What primes other than p and q are represented by the forms $px^2 + bxy + qy^2$?

$px^2 + bxy + qy^2$

What primes other than p and q are represented by the forms $px^2 + bxy + qy^2$?

An example:

(2,11)		$\Delta(Q)$	$C(\Delta)$
$Q_1(x,y)$	$2x^2 + 11y^2$	-88	$\mathbb{Z}/2\mathbb{Z}$
$Q_2(x,y)$	$2x^2 + xy + 11y^2$	-87	$\mathbb{Z}/6\mathbb{Z}$
$Q_3(x,y)$	$2x^2 - xy + 11y^2$	-87	$\mathbb{Z}/6\mathbb{Z}$
$Q_4(x,y)$	$2x^2 + 2xy + 11y^2$	-84	$(\mathbb{Z}/2\mathbb{Z})^2$

Modular Conditions

First we turn to *modular conditions*.

Modular Conditions

First we turn to *modular conditions*.

Due to Clark, Hicks, Parshall, and Thompson, we have a finite list of 2,779 regular forms for which we can determine complete modular conditions for the primes represented by the forms (at least for $p \nmid 2\Delta$).

Modular Conditions

First we turn to *modular conditions*.

Due to Clark, Hicks, Parshall, and Thompson, we have a finite list of 2,779 regular forms for which we can determine complete modular conditions for the primes represented by the forms (at least for $p \nmid 2\Delta$).

		Primes Represented
$Q_1(x,y)$	$2x^2 + 11y^2$	$\left(\frac{p}{11}\right) = -1$ and $p \equiv 3, 5 \pmod 8$

Modular Conditions

First we turn to *modular conditions*.

Due to Clark, Hicks, Parshall, and Thompson, we have a finite list of 2,779 regular forms for which we can determine complete modular conditions for the primes represented by the forms (at least for $p \nmid 2\Delta$).

		Primes Represented
$Q_1(x,y)$	$2x^2+11y^2$	$\left(\frac{p}{11}\right)=-1$ and $p\equiv 3,5 \pmod 8$
$Q_4(x,y)$	$2x^2+2xy+11y^2$	$\left(\frac{p}{3}\right)=-1$ and $\left(\frac{p}{7}\right)=1$

$2x^2 \pm xy + 11y^2$

What happens if we have a form for which we cannot determine complete modular conditions for the primes represented?

$2x^2 \pm xy + 11y^2$

What happens if we have a form for which we cannot determine complete modular conditions for the primes represented?

We turn to *splitting conditions*.

More Definitions

Fact: Let Q be a form of $\Delta = sn$ where s is all of the square factors of Δ. Then there is an associated quadratic number field $K = \mathbb{Q}(\sqrt{-n})$. K also has a discriminant,

$$d_K = \begin{cases} -n & \text{if } -n \equiv 1 \pmod 4 \\ -4n & \text{otherwise} \end{cases}.$$

More Definitions

Fact: Let Q be a form of $\Delta = sn$ where s is all of the square factors of Δ. Then there is an associated quadratic number field $K = \mathbb{Q}(\sqrt{-n})$. K also has a discriminant,

$$d_K = \begin{cases} -n & \text{if } -n \equiv 1 \pmod 4 \\ -4n & \text{otherwise} \end{cases}.$$

Definition (Ring of Integers)

Let K be a quadratic number field. The **ring of integers** $\mathcal{O}_K$ is the set of elements of K that are roots of monic polynomials with coefficients in $\mathbb{Z}$.

More Definitions

Definition (Prime Ideals in $\mathcal{O}_K$)

Let K be a quadratic number field, $\mathcal{O}_K$ be the ring of integers of K, and p be a prime ideal in $\mathbb{Q}$. Then p could behave in one of three ways in $\mathcal{O}_K$; either:

1. p is still prime and hence p is **inert**, i.e. $p\mathcal{O}_K = \mathfrak{p}$,
2. p factors into distinct primes and hence p **splits**, i.e. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$,
3. or p factors into non-distinct primes and hence p **ramifies**, i.e. $p\mathcal{O}_K = \mathfrak{p}^2$.

Why Splitting?

Let $\Delta < 0$ be a discriminant. For $p \nmid \Delta$, p is represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

Why Splitting?

Let $\Delta < 0$ be a discriminant. For $p \nmid \Delta$, p is represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

Similarly, for $p \nmid \Delta$, p splits in $\mathcal{O}_K$ if and only if $\left(\frac{d_k}{p}\right) = 1$.

Why Splitting?

Let $\Delta < 0$ be a discriminant. For $p \nmid \Delta$, p is represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

Similarly, for $p \nmid \Delta$, p splits in $\mathcal{O}_K$ if and only if $\left(\frac{d_k}{p}\right) = 1$.

Due to the relationship between Δ and d_K, p is represented by some form of discriminant Δ if and only if p splits in $\mathcal{O}_K$.

Why Splitting?

Let $\Delta < 0$ be a discriminant. For $p \nmid \Delta$, p is represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

Similarly, for $p \nmid \Delta$, p splits in $\mathcal{O}_K$ if and only if $\left(\frac{d_k}{p}\right) = 1$.

Due to the relationship between Δ and d_K, p is represented by some form of discriminant Δ if and only if p splits in $\mathcal{O}_K$.

$$Q_2(x, y) = 2x^2 + xy + 11y^2$$
$$Q_3(x, y) = 2x^2 - xy + 11y^2$$

Why Splitting?

Let $\Delta < 0$ be a discriminant. For $p \nmid \Delta$, p is represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

Similarly, for $p \nmid \Delta$, p splits in $\mathcal{O}_K$ if and only if $\left(\frac{d_k}{p}\right) = 1$.

Due to the relationship between Δ and d_K, p is represented by some form of discriminant Δ if and only if p splits in $\mathcal{O}_K$.

$$\begin{aligned} Q_2(x,y) &= 2x^2 + xy + 11y^2 \\ Q_3(x,y) &= 2x^2 - xy + 11y^2 \end{aligned}$$

We are forced to go to a larger field extension to gain more information about the primes represented by these forms. How much larger?

Why Splitting?

Let $\Delta < 0$ be a discriminant. For $p \nmid \Delta$, p is represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

Similarly, for $p \nmid \Delta$, p splits in $\mathcal{O}_K$ if and only if $\left(\frac{d_k}{p}\right) = 1$.

Due to the relationship between Δ and d_K, p is represented by some form of discriminant Δ if and only if p splits in $\mathcal{O}_K$.

$$\begin{aligned} Q_2(x, y) &= 2x^2 + xy + 11y^2 \\ Q_3(x, y) &= 2x^2 - xy + 11y^2 \end{aligned}$$

We are forced to go to a larger field extension to gain more information about the primes represented by these forms. How much larger?

The Hilbert class field!

Hilbert Class Field

Definition (Unramified Extension)

Let $F \subseteq E$ be a field extension. E is an **unramified extension** of F if all primes, both finite and infinite, are unramified in E.

Hilbert Class Field

Definition (Unramified Extension)

Let $F \subseteq E$ be a field extension. E is an **unramified extension** of F if all primes, both finite and infinite, are unramified in E.

Definition (Abelian Extension)

Let $F \subseteq E$ be a field extension. E is an **abelian extension** of F if $\mathrm{Gal}(E/F)$ is an abelian group.

Hilbert Class Field

Definition (Unramified Extension)

Let $F \subseteq E$ be a field extension. E is an **unramified extension** of F if all primes, both finite and infinite, are unramified in E.

Definition (Abelian Extension)

Let $F \subseteq E$ be a field extension. E is an **abelian extension** of F if $\mathrm{Gal}(E/F)$ is an abelian group.

Definition (Hilbert Class Field)

Let K be a quadratic number field. The **Hilbert class field** of K is the field L such that L is the maximal, unramified, abelian extension of K.

Theorem (DEOTW)

Let K be a quadratic number field, and L be the Hilbert class field of K. A prime p not dividing the discriminant of K is represented by some quadratic form Q of order m associated with K if and only if p splits into $\frac{[L:\mathbb{Q}]}{m}$ factors in L.

Theorem (DEOTW)

Let K be a quadratic number field, and L be the Hilbert class field of K. A prime p not dividing the discriminant of K is represented by some quadratic form Q of order m associated with K if and only if p splits into $\frac{[L:\mathbb{Q}]}{m}$ factors in L.

$$\begin{aligned} Q_2(x,y) &= 2x^2 + xy + 11y^2 \\ Q_3(x,y) &= 2x^2 - xy + 11y^2 \end{aligned}$$

Theorem (DEOTW)

Let K be a quadratic number field, and L be the Hilbert class field of K. A prime p not dividing the discriminant of K is represented by some quadratic form Q of order m associated with K if and only if p splits into $\frac{[L:\mathbb{Q}]}{m}$ factors in L.

$$\begin{aligned} Q_2(x,y) &= 2x^2 + xy + 11y^2 \\ Q_3(x,y) &= 2x^2 - xy + 11y^2 \end{aligned}$$

$$K = \mathbb{Q}(\sqrt{-87})$$

Theorem (DEOTW)

Let K be a quadratic number field, and L be the Hilbert class field of K. A prime p not dividing the discriminant of K is represented by some quadratic form Q of order m associated with K if and only if p splits into $\frac{[L:\mathbb{Q}]}{m}$ factors in L.

$$\begin{aligned} Q_2(x, y) &= 2x^2 + xy + 11y^2 \\ Q_3(x, y) &= 2x^2 - xy + 11y^2 \end{aligned}$$

$$K = \mathbb{Q}(\sqrt{-87})$$

$$[L : K] = 6 \Rightarrow [L : \mathbb{Q}] = 12$$

Theorem (DEOTW)

Let K be a quadratic number field, and L be the Hilbert class field of K. A prime p not dividing the discriminant of K is represented by some quadratic form Q of order m associated with K if and only if p splits into $\frac{[L:\mathbb{Q}]}{m}$ factors in L.

$$
\begin{aligned}
Q_2(x,y) &= 2x^2 + xy + 11y^2 \\
Q_3(x,y) &= 2x^2 - xy + 11y^2
\end{aligned}
$$

$$K = \mathbb{Q}(\sqrt{-87})$$

$$[L:K] = 6 \Rightarrow [L:\mathbb{Q}] = 12$$

$$|Q_2| = |Q_3| = 6$$

Theorem (DEOTW)

Let K be a quadratic number field, and L be the Hilbert class field of K. A prime p not dividing the discriminant of K is represented by some quadratic form Q of order m associated with K if and only if p splits into $\frac{[L:\mathbb{Q}]}{m}$ factors in L.

$$Q_2(x,y) = 2x^2 + xy + 11y^2$$
$$Q_3(x,y) = 2x^2 - xy + 11y^2$$

$$K = \mathbb{Q}(\sqrt{-87})$$

$$[L:K] = 6 \Rightarrow [L:\mathbb{Q}] = 12$$

$$|Q_2| = |Q_3| = 6$$

Q_2 and Q_3 are the only forms of order 6 in their class group, and hence a prime $p \nmid -87$ is represented by Q_2 and Q_3 if and only if p splits into 2 factors in L.

$px^2 + bxy + qy^2$

A motivating example:

		$\Delta(Q)$	$C(\Delta)$
$Q_1(x, y)$	$2x^2 + 11y^2$	-88	$\mathbb{Z}/2\mathbb{Z}$
$Q_2(x, y)$	$2x^2 + xy + 11y^2$	-87	$\mathbb{Z}/6\mathbb{Z}$
$Q_3(x, y)$	$2x^2 - xy + 11y^2$	-87	$\mathbb{Z}/6\mathbb{Z}$
$Q_4(x, y)$	$2x^2 + 2xy + 11y^2$	-84	$(\mathbb{Z}/2\mathbb{Z})^2$

Future Work

- Further classify what primes other than p and q are represented by all forms of the form $px^2 + bxy + qy^2$.

Future Work

- Further classify what primes other than p and q are represented by all forms of the form $px^2 + bxy + qy^2$.
- Classify what integers are in the intersection of forms of different discriminants of even class number.

Future Work

- Further classify what primes other than p and q are represented by all forms of the form $px^2 + bxy + qy^2$.
- Classify what integers are in the intersection of forms of different discriminants of even class number.
- Prove a conjecture about what is represented by all forms of a non-fundamental discriminant.