Directed Reading Spring 2026

Cameron Mars & Caiden Woolery

April 2026

Motivation: Representing Primes

The central question of 17th and 18th-century number theory: *For a fixed $n \in \mathbb{Z}$, which primes p can be written in the form $x^2 + ny^2$?*

Motivation: Representing Primes

The central question of 17th and 18th-century number theory: *For a fixed $n \in \mathbb{Z}$, which primes p can be written in the form $x^2 + ny^2$?*

Classic Results:

- **Fermat ($n = 1$):** $p = x^2 + y^2 \iff p = 2$ or $p \equiv 1 \pmod 4$.

Motivation: Representing Primes

The central question of 17th and 18th-century number theory: *For a fixed $n \in \mathbb{Z}$, which primes p can be written in the form $x^2 + ny^2$?*

Classic Results:

- **Fermat ($n = 1$):** $p = x^2 + y^2 \iff p = 2$ or $p \equiv 1 \pmod 4$.
- **Fermat ($n = 2$):** $p = x^2 + 2y^2 \iff p = 2$ or $p \equiv 1, 3 \pmod 8$.

Motivation: Representing Primes

The central question of 17th and 18th-century number theory: *For a fixed $n \in \mathbb{Z}$, which primes p can be written in the form $x^2 + ny^2$?*

Classic Results:

- **Fermat ($n = 1$):** $p = x^2 + y^2 \iff p = 2$ or $p \equiv 1 \pmod 4$.
- **Fermat ($n = 2$):** $p = x^2 + 2y^2 \iff p = 2$ or $p \equiv 1, 3 \pmod 8$.
- **Fermat ($n = 3$):** $p = x^2 + 3y^2 \iff p = 3$ or $p \equiv 1 \pmod 3$.

Motivation: Representing Primes

The central question of 17th and 18th-century number theory: *For a fixed $n \in \mathbb{Z}$, which primes p can be written in the form $x^2 + ny^2$?*

Classic Results:

- **Fermat ($n = 1$):** $p = x^2 + y^2 \iff p = 2$ or $p \equiv 1 \pmod 4$.
- **Fermat ($n = 2$):** $p = x^2 + 2y^2 \iff p = 2$ or $p \equiv 1, 3 \pmod 8$.
- **Fermat ($n = 3$):** $p = x^2 + 3y^2 \iff p = 3$ or $p \equiv 1 \pmod 3$.

The Wall: For $n = 5$, a prime p satisfies $p \equiv 1, 9 \pmod{20} \implies p$ is represented by *either* $x^2 + 5y^2$ OR $2x^2 + 2xy + 3y^2$.

Motivation: Representing Primes

The central question of 17th and 18th-century number theory: *For a fixed $n \in \mathbb{Z}$, which primes p can be written in the form $x^2 + ny^2$?*

Classic Results:

- **Fermat ($n = 1$):** $p = x^2 + y^2 \iff p = 2$ or $p \equiv 1 \pmod 4$.
- **Fermat ($n = 2$):** $p = x^2 + 2y^2 \iff p = 2$ or $p \equiv 1, 3 \pmod 8$.
- **Fermat ($n = 3$):** $p = x^2 + 3y^2 \iff p = 3$ or $p \equiv 1 \pmod 3$.

The Wall: For $n = 5$, a prime p satisfies $p \equiv 1, 9 \pmod{20} \implies p$ is represented by *either* $x^2 + 5y^2$ OR $2x^2 + 2xy + 3y^2$.

The Path Forward: To distinguish between these cases, we must move beyond specific examples and develop a general theory for:

$$f(x, y) = ax^2 + bxy + cy^2$$

What are Quadratic Forms?

A quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ where

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

What are Quadratic Forms?

A quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ where

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

A quadratic form is primitive if a, b, c are relatively prime, or $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.

What are Quadratic Forms?

A quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ where

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

A quadratic form is primitive if a, b, c are relatively prime, or $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.
An integer $m \in \mathbb{Z}$ is represented by a form $f(x, y)$ if $m = f(x, y)$ for some $x, y \in \mathbb{Z}$.

What are Quadratic Forms?

A quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ where

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

A quadratic form is primitive if a, b, c are relatively prime, or $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.
An integer $m \in \mathbb{Z}$ is represented by a form $f(x, y)$ if $m = f(x, y)$ for some $x, y \in \mathbb{Z}$.
If $\gcd(x, y) = 1$, we say m is properly represented by $f(x, y)$.

What are Quadratic Forms?

A quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ where

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

A quadratic form is primitive if a, b, c are relatively prime, or $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.
An integer $m \in \mathbb{Z}$ is represented by a form $f(x, y)$ if $m = f(x, y)$ for some $x, y \in \mathbb{Z}$.
If $\gcd(x, y) = 1$, we say m is properly represented by $f(x, y)$.
Example: $f(x, y) = x^2 + 2xy + 5y^2$

$$f(1, 1) = 1 + 2 + 5 = 8$$

8 is properly represented by $f(1, 1)$ since $\gcd(1, 1) = 1$

What are Quadratic Forms?

A quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ where

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

A quadratic form is primitive if a, b, c are relatively prime, or $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.
An integer $m \in \mathbb{Z}$ is represented by a form $f(x, y)$ if $m = f(x, y)$ for some $x, y \in \mathbb{Z}$.
If $\gcd(x, y) = 1$, we say m is properly represented by $f(x, y)$.
Example: $f(x, y) = x^2 + 2xy + 5y^2$

$$f(1, 1) = 1 + 2 + 5 = 8$$

8 is properly represented by $f(1, 1)$ since $\gcd(1, 1) = 1$

$$f(2, 2) = 4 + 8 + 20 = 32$$

32 is not properly represented by $f(2, 2)$

Equivalent Forms, Reduction

Two forms $f(x, y), g(x, y)$ are equivalent if there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1$$

Equivalent Forms, Reduction

Two forms $f(x, y), g(x, y)$ are equivalent if there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1$$

They are properly equivalent if $ps - qr = 1$, improperly equivalent otherwise.

Equivalent Forms, Reduction

Two forms $f(x, y), g(x, y)$ are equivalent if there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1$$

They are properly equivalent if $ps - qr = 1$, improperly equivalent otherwise.

We define the discriminant D of a form $f = ax^2 + bxy + cy^2$ to be

$$D = b^2 - 4ac$$

Equivalent Forms, Reduction

Two forms $f(x, y), g(x, y)$ are equivalent if there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1$$

They are properly equivalent if $ps - qr = 1$, improperly equivalent otherwise.

We define the discriminant D of a form $f = ax^2 + bxy + cy^2$ to be

$$D = b^2 - 4ac$$

A straightforward calculation shows that equivalent forms have the same discriminant.

Equivalent Forms, Reduction

Two forms $f(x, y), g(x, y)$ are equivalent if there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1$$

They are properly equivalent if $ps - qr = 1$, improperly equivalent otherwise.
We define the discriminant D of a form $f = ax^2 + bxy + cy^2$ to be

$$D = b^2 - 4ac$$

A straightforward calculation shows that equivalent forms have the same discriminant.
If $D < 0$, f is called positive definite or negative definite based on the sign of a.

Equivalent Forms, Reduction

Two forms $f(x, y), g(x, y)$ are equivalent if there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1$$

They are properly equivalent if $ps - qr = 1$, improperly equivalent otherwise.

We define the discriminant D of a form $f = ax^2 + bxy + cy^2$ to be

$$D = b^2 - 4ac$$

A straightforward calculation shows that equivalent forms have the same discriminant.

If $D < 0$, f is called positive definite or negative definite based on the sign of a.

A primitive, positive definite form $ax^2 + bxy + cy^2$ is said to be reduced if

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = a, \text{ or } a = c$$

Equivalent Forms Example

$f(x, y) = x^2 + y^2$ is equivalent to $g(x, y) = x^2 + 2xy + 2y^2$.

Equivalent Forms Example

$f(x, y) = x^2 + y^2$ is equivalent to $g(x, y) = x^2 + 2xy + 2y^2$.
We can do this by replacing x with $x + y$ and y with y.

Equivalent Forms Example

$f(x, y) = x^2 + y^2$ is equivalent to $g(x, y) = x^2 + 2xy + 2y^2$.
We can do this by replacing x with $x + y$ and y with y.
Consider that this is equivalent to saying that

$$f\left(M\begin{bmatrix}x\\y\end{bmatrix}\right) \equiv g\begin{bmatrix}x\\y\end{bmatrix} \iff f(x + y, y) = g(x, y)$$

Equivalent Forms Example

$f(x, y) = x^2 + y^2$ is equivalent to $g(x, y) = x^2 + 2xy + 2y^2$.
We can do this by replacing x with $x + y$ and y with y.
Consider that this is equivalent to saying that

$$f\left(M \begin{bmatrix} x \\ y \end{bmatrix}\right) \equiv g \begin{bmatrix} x \\ y \end{bmatrix} \iff f(x + y, y) = g(x, y)$$

where $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Equivalent Forms Example

$f(x, y) = x^2 + y^2$ is equivalent to $g(x, y) = x^2 + 2xy + 2y^2$.
We can do this by replacing x with $x + y$ and y with y.
Consider that this is equivalent to saying that

$$f\left(M \begin{bmatrix} x \\ y \end{bmatrix}\right) \equiv g \begin{bmatrix} x \\ y \end{bmatrix} \iff f(x + y, y) = g(x, y)$$

where $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
Since $\det M = ps - qr = 1 - 0 = 1$, these forms are properly equivalent, and M is orientation preserving.

Groups

A group $(G, \cdot)$ is a pair where G is a set and $\cdot$ is a function from $G \times G \to G$ where for $g, h \in G$, $(g, h) \mapsto g \cdot h$ such that

Groups

A group $(G, \cdot)$ is a pair where G is a set and $\cdot$ is a function from $G \times G \to G$ where for $g, h \in G$, $(g, h) \mapsto g \cdot h$ such that

1. There exists $e \in G$ such that for all $g \in G$,

$$ge = g = eg$$

Groups

A group $(G, \cdot)$ is a pair where G is a set and $\cdot$ is a function from $G \times G \to G$ where for $g, h \in G$, $(g, h) \mapsto g \cdot h$ such that

1. There exists $e \in G$ such that for all $g \in G$,

$$ge = g = eg$$

2. For all $g \in G$, there exists a $g^{-1} \in G$ such that

$$gg^{-1} = e = g^{-1}g$$

Groups

A group $(G, \cdot)$ is a pair where G is a set and $\cdot$ is a function from $G \times G \to G$ where for $g, h \in G$, $(g, h) \mapsto g \cdot h$ such that

1. There exists $e \in G$ such that for all $g \in G$,

$$ge = g = eg$$

2. For all $g \in G$, there exists a $g^{-1} \in G$ such that

$$gg^{-1} = e = g^{-1}g$$

3. For all $g, h, k \in G$,

$$(gh)k = g(hk)$$

Groups

A group $(G, \cdot)$ is a pair where G is a set and $\cdot$ is a function from $G \times G \to G$ where for $g, h \in G$, $(g, h) \mapsto g \cdot h$ such that

1. There exists $e \in G$ such that for all $g \in G$,

$$ge = g = eg$$

2. For all $g \in G$, there exists a $g^{-1} \in G$ such that

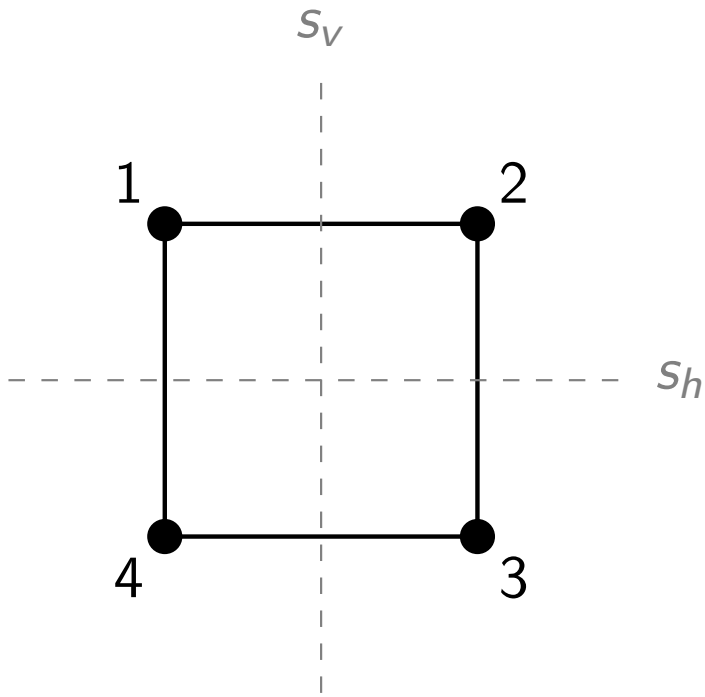
$$gg^{-1} = e = g^{-1}g$$

3. For all $g, h, k \in G$,

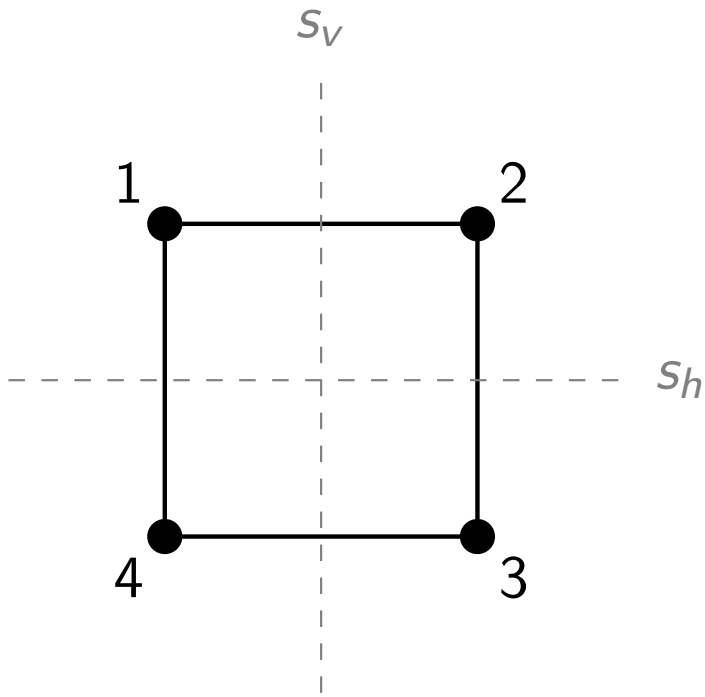
$$(gh)k = g(hk)$$

Importantly, a group induces a structure on some type of object such that combining things in the group preserves that structure.

Group Example: Symmetries of the Square (D_4)



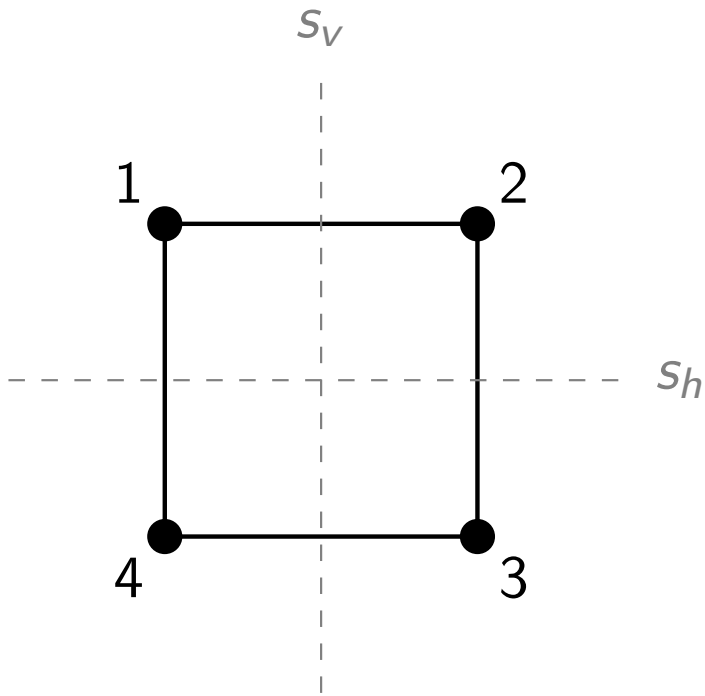
Group Example: Symmetries of the Square (D_4)



The group D_4 consists of 8 symmetries:

- 4 Rotations: $\{R_0, R_{90}, R_{180}, R_{270}\}$

Group Example: Symmetries of the Square (D_4)



The group D_4 consists of 8 symmetries:

- 4 Rotations: $\{R_0, R_{90}, R_{180}, R_{270}\}$
- 4 Reflections: Horizontal, Vertical, and 2 Diagonals.

Composition

Let

$$f(x,y) = ax^2 + bxy + cy^2, \qquad g(x,y) = a'x^2 + b'xy + c'y^2$$

Composition

Let

$$f(x,y) = ax^2 + bxy + cy^2, \qquad g(x,y) = a'x^2 + b'xy + c'y^2$$

be primitive positive definite binary quadratic forms of the same discriminant $D < 0$, and suppose

$$\gcd\left(a, a', \frac{b+b'}{2}\right) = 1.$$

Composition

Let

$$f(x,y) = ax^2 + bxy + cy^2, \qquad g(x,y) = a'x^2 + b'xy + c'y^2$$

be primitive positive definite binary quadratic forms of the same discriminant $D < 0$, and suppose

$$\gcd\left(a, a', \frac{b+b'}{2}\right) = 1.$$

Then the *Dirichlet composition* of f and g is the form

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

Composition

Let

$$f(x,y) = ax^2 + bxy + cy^2, \qquad g(x,y) = a'x^2 + b'xy + c'y^2$$

be primitive positive definite binary quadratic forms of the same discriminant $D < 0$, and suppose

$$\gcd\left(a, a', \frac{b+b'}{2}\right) = 1.$$

Then the *Dirichlet composition* of f and g is the form

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

where B is chosen so that

$$B \equiv b \pmod{2a}, \qquad B \equiv b' \pmod{2a'}, \qquad B^2 \equiv D \pmod{4aa'}.$$

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Step 1: Find B

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Step 1: Find B

The value $B = 1$ works since

$$1^2 = 1 \equiv -31 \pmod{16}$$

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Step 1: Find B

The value $B = 1$ works since

$$1^2 = 1 \equiv -31 \pmod{16}$$

Step 2: Construct the new form F

- $A = aa' = 2 \cdot 2 = 4$,

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Step 1: Find B

The value $B = 1$ works since

$$1^2 = 1 \equiv -31 \pmod{16}$$

Step 2: Construct the new form F

- $A = aa' = 2 \cdot 2 = 4$, $B = 1$,

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Step 1: Find B

The value $B = 1$ works since

$$1^2 = 1 \equiv -31 \pmod{16}$$

Step 2: Construct the new form F

- $A = aa' = 2 \cdot 2 = 4$, $B = 1$, $C = \frac{1^2 - (-31)}{4(4)} = \frac{32}{16} = 2$

Example: Composing Forms

Consider the discriminant $D = -31$. Let f and g be the same form:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Check the condition:

$$\gcd(a, a', \tfrac{b+b'}{2}) = \gcd(2, 2, 1) = 1$$

Step 1: Find B

The value $B = 1$ works since

$$1^2 = 1 \equiv -31 \pmod{16}$$

Step 2: Construct the new form F

- $A = aa' = 2 \cdot 2 = 4$, $B = 1$, $C = \frac{1^2 - (-31)}{4(4)} = \frac{32}{16} = 2$

The composed form is

$$(fg)(x, y) = F(x, y) = 4x^2 + xy + 2y^2$$

Class Group

This function of composition gives a *group structure*.

Class Group

This function of composition gives a *group structure*.
For closure, if f and g both have discriminant D, then their composition fg also has discriminant D.

Class Group

This function of composition gives a *group structure*.
For closure, if f and g both have discriminant D, then their composition fg also has discriminant D.
Example:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

Class Group

This function of composition gives a *group structure*.
For closure, if f and g both have discriminant D, then their composition fg also has discriminant D.
Example:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

From the previous slide,

$$(fg)(x, y) = 4x^2 + xy + 2y^2$$

Class Group

This function of composition gives a *group structure*.
For closure, if f and g both have discriminant D, then their composition fg also has discriminant D.
Example:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

From the previous slide,

$$(fg)(x, y) = 4x^2 + xy + 2y^2$$

This new form still has discriminant

$$1^2 - 4(4)(2) = 1 - 32 = -31$$

Class Group

This function of composition gives a *group structure*.
For closure, if f and g both have discriminant D, then their composition fg also has discriminant D.
Example:

$$f(x, y) = g(x, y) = 2x^2 + xy + 4y^2$$

From the previous slide,

$$(fg)(x, y) = 4x^2 + xy + 2y^2$$

This new form still has discriminant

$$1^2 - 4(4)(2) = 1 - 32 = -31$$

So composition stays in the same set of classes.

Class Group Cont.

For the identity,

Class Group Cont.

For the identity,
there is a special class that does nothing under composition.

Class Group Cont.

For the identity,
there is a special class that does nothing under composition.
For $D = -31$, the principal form is

$$e(x, y) = x^2 + xy + 8y^2$$

Class Group Cont.

For the identity,
there is a special class that does nothing under composition.
For $D = -31$, the principal form is

$$e(x, y) = x^2 + xy + 8y^2$$

Its discriminant is

$$1^2 - 4(1)(8) = 1 - 32 = -31$$

Class Group Cont.

For the identity,
there is a special class that does nothing under composition.
For $D = -31$, the principal form is

$$e(x, y) = x^2 + xy + 8y^2$$

Its discriminant is

$$1^2 - 4(1)(8) = 1 - 32 = -31$$

So e lies in the same collection of forms, and composing any form with the class of e gives back the same class.

Class Group Cont.

For the identity,
there is a special class that does nothing under composition.
For $D = -31$, the principal form is

$$e(x, y) = x^2 + xy + 8y^2$$

Its discriminant is

$$1^2 - 4(1)(8) = 1 - 32 = -31$$

So e lies in the same collection of forms, and composing any form with the class of e gives back the same class.
For example, the class of

$$f(x, y) = 2x^2 + xy + 4y^2$$

Class Group Cont.

For the identity,
there is a special class that does nothing under composition.
For $D = -31$, the principal form is

$$e(x, y) = x^2 + xy + 8y^2$$

Its discriminant is

$$1^2 - 4(1)(8) = 1 - 32 = -31$$

So e lies in the same collection of forms, and composing any form with the class of e gives back the same class.
For example, the class of

$$f(x, y) = 2x^2 + xy + 4y^2$$

satisfies

$$f \cdot e = f$$

Class Group Cont.

For inverses, we can work with a concrete example

Class Group Cont.

For inverses, we can work with a concrete example

For example, if

$$f(x, y) = 2x^2 + xy + 4y^2$$

Class Group Cont.

For inverses, we can work with a concrete example

For example, if

$$f(x, y) = 2x^2 + xy + 4y^2$$

then

$$f^{-1}(x, y) = 2x^2 - xy + 4y^2$$

Class Group Cont.

For inverses, we can work with a concrete example

For example, if

$$f(x, y) = 2x^2 + xy + 4y^2$$

then

$$f^{-1}(x, y) = 2x^2 - xy + 4y^2$$

Both have discriminant -31:

$$1^2 - 4(2)(4) = -31, \qquad (-1)^2 - 4(2)(4) = -31$$

Class Group Cont.

For inverses, we can work with a concrete example
For example, if

$$f(x, y) = 2x^2 + xy + 4y^2$$

then

$$f^{-1}(x, y) = 2x^2 - xy + 4y^2$$

Both have discriminant -31:

$$1^2 - 4(2)(4) = -31, \qquad (-1)^2 - 4(2)(4) = -31$$

Their classes compose to the principal class:

$$f \cdot f^{-1} = e$$

Class Group Cont.

For inverses, we can work with a concrete example
For example, if

$$f(x, y) = 2x^2 + xy + 4y^2$$

then

$$f^{-1}(x, y) = 2x^2 - xy + 4y^2$$

Both have discriminant -31:

$$1^2 - 4(2)(4) = -31, \qquad (-1)^2 - 4(2)(4) = -31$$

Their classes compose to the principal class:

$$f \cdot f^{-1} = e$$

This gives the intuitive motivation for the notion of a class group.

Closing Thoughts

We have introduced a way to represent possible primes, but had little underlying structure or understanding of how these equations behave.

Closing Thoughts

We have introduced a way to represent possible primes, but had little underlying structure or understanding of how these equations behave.

We can define machinery to make different representations equivalent, giving our first notion of deeper structure. Then, this was expanded on by showing relations on the equivalent classes that hold a group structure.

Closing Thoughts

We have introduced a way to represent possible primes, but had little underlying structure or understanding of how these equations behave.

We can define machinery to make different representations equivalent, giving our first notion of deeper structure. Then, this was expanded on by showing relations on the equivalent classes that hold a group structure.

By finding a method to relate quadratic forms to a well studied field, *group theory*, we are able to better understand and work with these quadratic forms and primes.