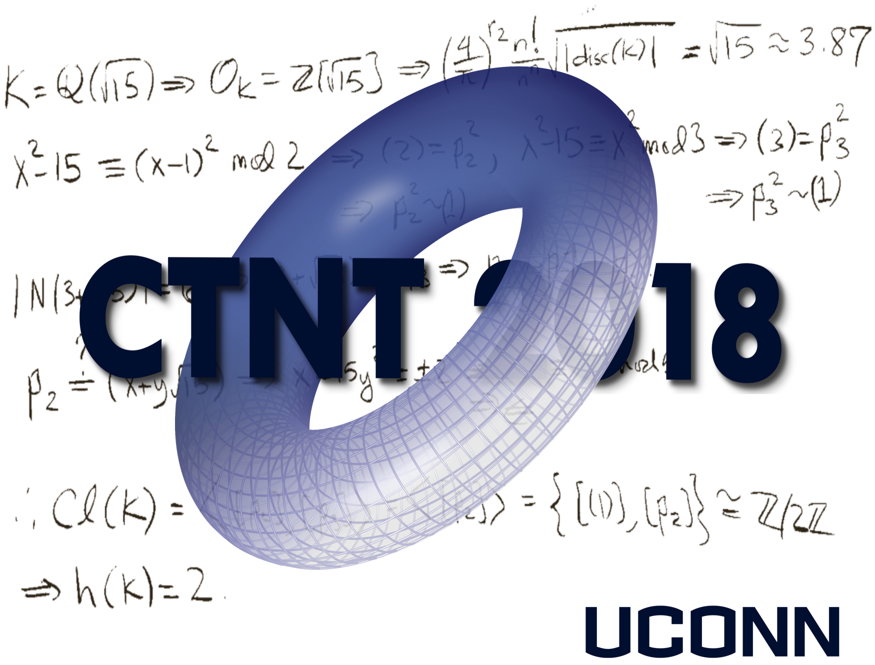

CTNT 2018
UCONN
$K = \mathbb{Q}(\sqrt{15}) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{15}]$
$x^2 - 15 \equiv (x-1)^2 \bmod 2$
$\Rightarrow \mathfrak{p}_3^2 \sim (1)$
$\Rightarrow h(K) = 2$

Arithmetic Statistics
Lecture 2

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

May 28$^{\text{th}}$

CTNT 2018
Connecticut Summer School
in Number Theory

A theme of *Arithmetic Statistics*: count a number-theoretic object relative to another.

A theme of *Arithmetic Statistics*: count a number-theoretic object relative to another. For example, every prime $p > 2$ is either $\equiv 1 \bmod 4$ or $3 \bmod 4$. Is there the same number of such primes up to X?

A theme of *Arithmetic Statistics*: count a number-theoretic object relative to another. For example, every prime $p > 2$ is either $\equiv 1 \bmod 4$ or $3 \bmod 4$. Is there the same number of such primes up to X?

Johann Peter
Gustav Lejeune
Dirichlet
1805 – 1859

Dirichlet's theorem on primes in arithmetic progressions:

Theorem (Dirichlet, de la Vallée-Poussin)

Let a and n be relatively prime natural numbers. Then, there are infinitely prime numbers $p \equiv a \bmod n$.

A theme of *Arithmetic Statistics*: count a number-theoretic object relative to another. For example, every prime $p > 2$ is either $\equiv 1 \bmod 4$ or $3 \bmod 4$. Is there the same number of such primes up to X?

Johann Peter
Gustav Lejeune
Dirichlet
1805 – 1859

Dirichlet's theorem on primes in arithmetic progressions:

Theorem (Dirichlet, de la Vallée-Poussin)

Let a and n be relatively prime natural numbers. Then, there are infinitely prime numbers $p \equiv a \bmod n$. Moreover,

$$\pi_{n,a}(X) \sim \frac{1}{\varphi(n)} \cdot \int_2^X \frac{1}{\log t} dt, \text{ where } \varphi(n) \text{ is the Euler phi function.}$$

Theorem (Dirichlet, de la Vallée-Poussin)

Let a and n be relatively prime natural numbers. Then, there are infinitely prime numbers $p \equiv a \bmod n$. Moreover,

$$\pi_{n,a}(X) \sim \frac{1}{\varphi(n)} \cdot \int_2^X \frac{1}{\log t} dt, \text{ where } \varphi(n) \text{ is the Euler phi function.}$$

Since $\varphi(4) = 2$, we have

$$\pi_{4,1}(X) \sim \frac{1}{2} \cdot \int_2^X \frac{1}{\log t} dt \sim \pi_{4,3}(X).$$

Theorem (Dirichlet, de la Vallée-Poussin)

Let a and n be relatively prime natural numbers. Then, there are infinitely prime numbers $p \equiv a \bmod n$. Moreover,

$$\pi_{n,a}(X) \sim \frac{1}{\varphi(n)} \cdot \int_2^X \frac{1}{\log t} dt, \text{ where } \varphi(n) \text{ is the Euler phi function.}$$

Since $\varphi(4) = 2$, we have

$$\pi_{4,1}(X) \sim \frac{1}{2} \cdot \int_2^X \frac{1}{\log t} dt \sim \pi_{4,3}(X).$$

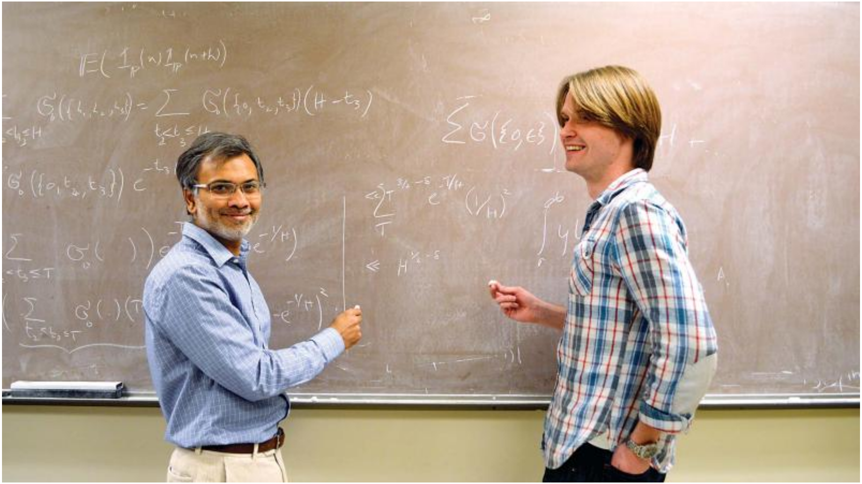
But...

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Chebyshev's bias (1853).

x	Number of primes $4n+3$ up to x	Number of primes $4n+1$ up to x
100	13	11
200	24	21
300	32	29
400	40	37
500	50	44
600	57	51
700	65	59
800	71	67
900	79	74
1000	87	80
2000	155	147
3000	218	211
4000	280	269
5000	339	329
6000	399	383
7000	457	442
8000	507	499
9000	562	554
10,000	619	609
20,000	1136	1125
50,000	2583	2549
100,000	4808	4783

(A table in "Prime number races", by Granville and Martin.)



See also “Unexpected biases in the distribution of consecutive primes”,
by Robert Lemke Oliver and Kannan Soundararajan.

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Chebyshev: is it always true that $\pi_{4,3}(X) \geq \pi_{4,1}(X)$? Equality at $X = 5, 17, 41, 461, \ldots$.

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Chebyshev: is it always true that $\pi_{4,3}(X) \geq \pi_{4,1}(X)$? Equality at $X = 5, 17, 41, 461, \ldots$. Inequality flips for the first time at $X = 26833$.

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Chebyshev: is it always true that $\pi_{4,3}(X) \geq \pi_{4,1}(X)$? Equality at $X = 5, 17, 41, 461, \ldots$. Inequality flips for the first time at $X = 26833$.

Theorem (Littlewood, 1914)

There are arbitrarily high values of X such that $\pi_{4,1}(X) > \pi_{4,3}(X)$.

Conjecture (Knapowski, Turán, 1962)

The inequality $\pi_{4,3}(X) \geq \pi_{4,1}(X)$ holds for 100% of all integers $X \geq 2$.

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Chebyshev: is it always true that $\pi_{4,3}(X) \geq \pi_{4,1}(X)$? Equality at $X = 5, 17, 41, 461, \ldots$. Inequality flips for the first time at $X = 26833$.

Theorem (Littlewood, 1914)

There are arbitrarily high values of X such that $\pi_{4,1}(X) > \pi_{4,3}(X)$.

Conjecture (Knapowski, Turán, 1962)

The inequality $\pi_{4,3}(X) \geq \pi_{4,1}(X)$ holds for 100% of all integers $X \geq 2$.

False: $\{x \leq X : \pi_{4,3}(x) \geq \pi_{4,1}(x)\}/X$ does not have a limit as $X \to \infty$.

Theorem (Rubinstein, Sarnak, 1994)

$$\frac{1}{\log X} \sum_{x \in S(X)} \frac{1}{x} \to 0.9959\ldots$$

as $X \to \infty$, where $S(X) = \{x \leq X : \pi_{4,3}(X) \geq \pi_{4,1}(X)\}$.

Why are primes $p \equiv 3 \bmod 4$ slightly more abundant than primes $p \equiv 1 \bmod 4$?

Why are primes $p \equiv 3 \bmod 4$ slightly more abundant than primes $p \equiv 1 \bmod 4$?

In short: 1 mod 4 is a square, while 3 mod 4 is not, in $\mathbb{Z}/4\mathbb{Z}$. (See Granville and Martin's *Prime Number Races*.)

Why are primes $p \equiv 3 \bmod 4$ slightly more abundant than primes $p \equiv 1 \bmod 4$?

In short: 1 mod 4 is a square, while 3 mod 4 is not, in $\mathbb{Z}/4\mathbb{Z}$.
(See Granville and Martin's *Prime Number Races*.)

Theorem (Fermat)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \bmod 4$.

That is, $p = x^2 + y^2$, for some $x, y \in \mathbb{Z}$, if and only if $p \equiv 1 \bmod 4$.

Quadratic Forms

Quadratic Forms

e.g., $f(x, y) = x^2 + y^2$.

A prime $p > 2$ is of the form $p \equiv 1 \mod 4$, if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.

A prime $p > 2$ is of the form $p \equiv 1 \mod 4$, if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.

Definition

A binary quadratic form is a function of the form

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

The function $f(x, y) = x^2 + y^2$ is an example of a binary quadratic form...

A prime $p > 2$ is of the form $p \equiv 1 \bmod 4$, if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.

Definition

A binary quadratic form is a function of the form

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

The function $f(x, y) = x^2 + y^2$ is an example of a binary quadratic form... What primes are represented by other binary quadratic forms? For instance, such as $g(a, b) = a^2 + 2ab + 2b^2$?

A prime $p > 2$ is of the form $p \equiv 1 \mod 4$, if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.

Definition

A binary quadratic form is a function of the form

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

The function $f(x, y) = x^2 + y^2$ is an example of a binary quadratic form... What primes are represented by other binary quadratic forms? For instance, such as $g(a, b) = a^2 + 2ab + 2b^2$?

Put $x = a + b$ and $y = b$. Then, $x^2 + y^2 = p$ if and only if $(a + b)^2 + b^2 = p$, if and only if $a^2 + 2ab + 2b^2 = p$.

A prime $p > 2$ is of the form $p \equiv 1 \bmod 4$, if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.

Definition

A binary quadratic form is a function of the form

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

The function $f(x, y) = x^2 + y^2$ is an example of a binary quadratic form... What primes are represented by other binary quadratic forms? For instance, such as $g(a, b) = a^2 + 2ab + 2b^2$?

Put $x = a + b$ and $y = b$. Then, $x^2 + y^2 = p$ if and only if $(a + b)^2 + b^2 = p$, if and only if $a^2 + 2ab + 2b^2 = p$.

From the point of view of **Arithmetic Statistics**, we would like to parametrize binary quadratic forms, according to the primes they represent.

$$x^2 + y^2 = p \Longleftrightarrow (a+b)^2 + b^2 = p \Longleftrightarrow a^2 + 2ab + 2b^2 = p.$$

We changed variables

$$\begin{cases} x = a + b \\ y = b \end{cases} \qquad \text{or} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

$$x^2+y^2=p \iff (a+b)^2+b^2=p \iff a^2+2ab+2b^2=p.$$

We changed variables

$$\begin{cases} x=a+b \\ y=b \end{cases} \qquad \text{or} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ could be replaced by any other matrix in $\mathrm{SL}(2,\mathbb{Z})$ and we would still have an invertible change of variables (such that itself and its inverse have integral coefficients).

$$x^2 + y^2 = p \Longleftrightarrow (a+b)^2 + b^2 = p \Longleftrightarrow a^2 + 2ab + 2b^2 = p.$$

We changed variables

$$\begin{cases} x = a + b \\ y = b \end{cases} \qquad \text{or} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ could be replaced by any other matrix in $\mathrm{SL}(2, \mathbb{Z})$ and we would still have an invertible change of variables (such that itself and its inverse have integral coefficients).

Thus, we can define an **action of** $\mathrm{SL}(2, \mathbb{Z})$ **on Binary Quadratic Forms (BQFs)** by

$$M \cdot f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f\left(M \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right)$$

for any $M \in \mathrm{SL}(2, \mathbb{Z})$.
Note: BQFs in each orbit represent the same numbers.

An alternative way to interpret a BQF:

$$f(x, y) = x^2 + y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

An alternative way to interpret a BQF:

$$f(x,y) = x^2 + y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

or, in general,

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

An alternative way to interpret a BQF:

$$f(x,y) = x^2 + y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

or, in general,

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

If $M \in \mathrm{SL}(2,\mathbb{Z})$, then

$$M \cdot f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \cdot M^t \cdot \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \cdot M \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

Example

The quadratic form $f(x, y) = x^2 + y^2$ corresponds to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. If we act on f by $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$, then we obtain the quadratic form that corresponds to

$$\begin{aligned} &\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}. \end{aligned}$$

The matrix $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ corresponds to the form $g(a, b) = a^2 + 2ab + 2b^2$.

We are interested in the orbit of a single BQF:

$$\mathrm{SL}(2,\mathbb{Z}) \cdot f = \{M \cdot f \in \text{BQFs} : M \in \mathrm{SL}(2,\mathbb{Z})\},$$

and the set of all orbits:

$$\text{BQFs} \,/\, \mathrm{SL}(2,\mathbb{Z}).$$

Question

We are interested in the orbit of a single BQF:

$$\mathrm{SL}(2,\mathbb{Z}) \cdot f = \{M \cdot f \in \text{BQFs} : M \in \mathrm{SL}(2,\mathbb{Z})\},$$

and the set of all orbits:

$$\text{BQFs} \,/\, \mathrm{SL}(2,\mathbb{Z}).$$

Question

When are two binary quadratic forms f and g in the same class?

For instance, are $11x^2 + 5xy + y^2$ and $x^2 + xy + 5y^2$ equivalent?

We are interested in the orbit of a single BQF:

$$\mathrm{SL}(2,\mathbb{Z}) \cdot f = \{M \cdot f \in \text{BQFs} : M \in \mathrm{SL}(2,\mathbb{Z})\},$$

and the set of all orbits:

$$\text{BQFs} \,/\, \mathrm{SL}(2,\mathbb{Z}).$$

Question

When are two binary quadratic forms f and g in the same class?

For instance, are $11x^2 + 5xy + y^2$ and $x^2 + xy + 5y^2$ equivalent?

Look for equivalence class invariants.

$$A \longleftrightarrow M^t \cdot A \cdot M$$

We are interested in the orbit of a single BQF:

$$\mathrm{SL}(2,\mathbb{Z}) \cdot f = \{M \cdot f \in \text{BQFs} : M \in \mathrm{SL}(2,\mathbb{Z})\},$$

and the set of all orbits:

$$\text{BQFs} \,/\, \mathrm{SL}(2,\mathbb{Z}).$$

Question

When are two binary quadratic forms f and g in the same class?

For instance, are $11x^2 + 5xy + y^2$ and $x^2 + xy + 5y^2$ equivalent?

Look for equivalence class invariants.

$$A \longleftrightarrow M^t \cdot A \cdot M$$

... since $\det(M) = 1$, the **determinant is invariant!**

$$\det(M^t \cdot A \cdot M) = \det(M^t) \cdot \det(A) \cdot \det(M) = 1 \cdot \det(A) \cdot 1 = \det(A).$$

Definition

Let $f(x,y) = ax^2 + bxy + cy^2$ *be a quadratic form, attached to the matrix* $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. *We define the discriminant of* f *by*

$$\mathrm{disc}(f) = -4 \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = b^2 - 4ac.$$

Definition

Let $f(x, y) = ax^2 + bxy + cy^2$ *be a quadratic form, attached to the matrix* $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$*. We define the discriminant of* f *by*

$$\mathrm{disc}(f) = -4 \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = b^2 - 4ac.$$

Example

$$\mathrm{disc}(x^2 + y^2) = -4 \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -4.$$

Definition

Let $f(x,y) = ax^2 + bxy + cy^2$ *be a quadratic form, attached to the matrix* $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. *We define the discriminant of* f *by*

$$\mathrm{disc}(f) = -4 \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = b^2 - 4ac.$$

Example

$\mathrm{disc}(x^2 + y^2) = -4 \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -4.$

Example

For $d \neq 0$, we have $\mathrm{disc}(x^2 - dy^2) = -4 \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix} = 4d.$

Definition

Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form, attached to the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. We define the discriminant of f by

$$\mathrm{disc}(f) = -4 \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = b^2 - 4ac.$$

Example

$\mathrm{disc}(x^2 + y^2) = -4 \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -4.$

Example

For $d \neq 0$, we have $\mathrm{disc}(x^2 - dy^2) = -4 \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix} = 4d.$

Example

We have $\mathrm{disc}(x^2 + xy + y^2) = 4(1/4 - 1) = -3.$

Definition

Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form, attached to the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. We define the discriminant of f by

$$\mathrm{disc}(f) = -4 \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = b^2 - 4ac.$$

We can similarly define $\mathrm{disc}([f])$ for each equivalence class $[f] \in \mathrm{BQFs} \,/\, \mathrm{SL}(2,\mathbb{Z})$, by

$$\mathrm{disc}([f]) = \mathrm{disc}(f)$$

where f is any representative of the class $[f]$.

Definition

Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form, attached to the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. We define the discriminant of f by

$$\operatorname{disc}(f) = -4 \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = b^2 - 4ac.$$

We can similarly define $\operatorname{disc}([f])$ for each equivalence class $[f] \in \mathrm{BQFs} \,/\, \mathrm{SL}(2,\mathbb{Z})$, by

$$\operatorname{disc}([f]) = \operatorname{disc}(f)$$

where f is any representative of the class $[f]$.

If $f, g \in [f]$, then $\operatorname{disc}(f) = \operatorname{disc}(g)$. **Is the converse true?**

Example

Are $11x^2 + 5xy + y^2$ and $x^2 + xy + 5y^2$ equivalent?

Example

Are $11x^2 + 5xy + y^2$ and $x^2 + xy + 5y^2$ equivalent?

$$\mathrm{disc}(11x^2+5xy+y^2) = 25-4\cdot 11 = -19 = 1-4\cdot 5 = \mathrm{disc}(x^2+xy+5y^2).$$

The discriminants coincide... how can we tell if they are actually equivalent?

Example

Are $11x^2 + 5xy + y^2$ and $x^2 + xy + 5y^2$ equivalent?

$\mathrm{disc}(11x^2+5xy+y^2) = 25-4\cdot 11 = -19 = 1-4\cdot 5 = \mathrm{disc}(x^2+xy+5y^2)$.

The discriminants coincide... how can we tell if they are actually equivalent?

Carl Friederich Gauss

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \leq a \leq c, \text{ and } b \geq 0 \text{ if } a = c.$$

For example, $x^2 + xy + 5y^2$ is reduced, but $11x^2 + 5xy + y^2$ is NOT.

For example, $x^2 + xy + 5y^2$ is reduced, but $11x^2 + 5xy + y^2$ is NOT.

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \leq a \leq c, \text{ and } b \geq 0 \text{ if } a = c.$$

Also Gauss: there is an algorithm to find the reduced reprentative. Steps in the algorithm:

For example, $x^2 + xy + 5y^2$ is reduced, but $11x^2 + 5xy + y^2$ is NOT.

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \leq a \leq c, \text{ and } b \geq 0 \text{ if } a = c.$$

Also Gauss: there is an algorithm to find the reduced reprentative. Steps in the algorithm:

1. If $c < a$, then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$.

For example, $x^2 + xy + 5y^2$ is reduced, but $11x^2 + 5xy + y^2$ is NOT.

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \leq a \leq c, \text{ and } b \geq 0 \text{ if } a = c.$$

Also Gauss: there is an algorithm to find the reduced reprentative. Steps in the algorithm:

1. If $c < a$, then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$.
2. If $b > a$ or $b \leq -a$, then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$, such that $b' \equiv b \bmod 2a$ and $-a < b' \leq a$, with $b' = b - 2ka$.

For example, $x^2 + xy + 5y^2$ is reduced, but $11x^2 + 5xy + y^2$ is NOT.

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \leq a \leq c, \text{ and } b \geq 0 \text{ if } a = c.$$

Also Gauss: there is an algorithm to find the reduced reprentative. Steps in the algorithm:

1. If $c < a$, then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$.
2. If $b > a$ or $b \leq -a$, then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$, such that $b' \equiv b \bmod 2a$ and $-a < b' \leq a$, with $b' = b - 2ka$.
3. If $c = a$ and $-a < b < 0$, then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$.

Example

Let $f(x, y) = 11x^2 + 5xy + y^2$.

- $a = 11 > 1 = c$. Change variables with $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 11 & 5/2 \\ 5/2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -5/2 \\ -5/2 & 11 \end{pmatrix},$$

which corresponds to $f_2(x, y) = x^2 - 5xy + 11y^2$.

Example

Let $f(x, y) = 11x^2 + 5xy + y^2$.

- $a = 11 > 1 = c$. Change variables with $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

  $$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 11 & 5/2 \\ 5/2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -5/2 \\ -5/2 & 11 \end{pmatrix},$$

  which corresponds to $f_2(x, y) = x^2 - 5xy + 11y^2$.
- $b = -5 \leq -1 = -a$. Let $b \equiv -5 \equiv 1 \bmod 2a$. So pick $-1 < b' = 1 \leq 1$, and $b' = -5 - 2 \cdot (-3)$, so $k = -3$.

Example

Let $f(x, y) = 11x^2 + 5xy + y^2$.

- $a = 11 > 1 = c$. Change variables with $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 11 & 5/2 \\ 5/2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -5/2 \\ -5/2 & 11 \end{pmatrix},$$

  which corresponds to $f_2(x, y) = x^2 - 5xy + 11y^2$.

- $b = -5 \leq -1 = -a$. Let $b \equiv -5 \equiv 1 \bmod 2a$. So pick $-1 < b' = 1 \leq 1$, and $b' = -5 - 2 \cdot (-3)$, so $k = -3$. So change variables with $M = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -5/2 \\ -5/2 & 11 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 5 \end{pmatrix},$$

  which corresponds to $f_3(x, y) = x^2 + xy + 5y^2$. (So equivalent!)

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \le a \le c, \text{ and } b \ge 0 \text{ if } a = c.$$

Example

The forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are both reduced and both of discriminant -20, so **they are not equivalent.**

Gauss: Every equivalence class of BQFs (with disc $= d < 0$) contains a unique reduced representative $f(x, y) = ax^2 + bxy + cy^2$ with the property

$$-a < b \leq a \leq c, \text{ and } b \geq 0 \text{ if } a = c.$$

Example

The forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are both reduced and both of discriminant -20, so **they are not equivalent.**

Question

Fix a (negative) discriminant d. Let BQFs(d) be the set of all binary quadratic forms of discriminant d. How many classes are there in

$$\mathrm{BQFs}(d)/\,\mathrm{SL}(2, \mathbb{Z}) \quad ?$$

Question

Fix a (negative) discriminant d. Let $\text{BQFs}(d)$ be the set of all binary quadratic forms of discriminant d. How many classes are there in

$$\text{BQFs}(d)/\,\text{SL}(2,\mathbb{Z}) \quad ?$$

Suppose $d < 0$ and $f(x, y) = ax^2 + bxy + cy^2$ is reduced, i.e., $-a < b \leq a \leq c$, and $b \geq 0$ if $a = c$.

Question

Fix a (negative) discriminant d. Let BQFs(d) be the set of all binary quadratic forms of discriminant d. How many classes are there in

$$\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z}) \quad ?$$

Suppose $d < 0$ and $f(x,y) = ax^2 + bxy + cy^2$ is reduced, i.e., $-a < b \leq a \leq c,$ and $b \geq 0$ if $a = c$. Then,

$$|d| = -d = 4 \cdot a \cdot c - b^2 \geq 4 \cdot a \cdot a - a^2 = 3a^2.$$

Question

Fix a (negative) discriminant d. Let BQFs(d) be the set of all binary quadratic forms of discriminant d. How many classes are there in

$$\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z}) \quad ?$$

Suppose $d < 0$ and $f(x, y) = ax^2 + bxy + cy^2$ is reduced, i.e., $-a < b \leq a \leq c,$ and $b \geq 0$ if $a = c$. Then,

$$|d| = -d = 4 \cdot a \cdot c - b^2 \geq 4 \cdot a \cdot a - a^2 = 3a^2.$$

Thus, $a \leq \sqrt{|d|/3}$.

Question

Fix a (negative) discriminant d. Let BQFs(d) be the set of all binary quadratic forms of discriminant d. How many classes are there in

$$\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z}) \quad ?$$

Suppose $d < 0$ and $f(x,y) = ax^2 + bxy + cy^2$ is reduced, i.e., $-a < b \le a \le c,$ and $b \ge 0$ if $a = c$. Then,

$$|d| = -d = 4 \cdot a \cdot c - b^2 \ge 4 \cdot a \cdot a - a^2 = 3a^2.$$

Thus, $a \le \sqrt{|d|/3}$. Hence:

- Finitely many options for a.
- $|b| \le a$, so finitely many options for b.
- $d = b^2 - 4ac$, so $c = (b^2 - d)/4a$ is determined by a and b.

This implies that there are **finitely many** classes in $\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z})$ when $d < 0$.

There are **finitely many** classes in $\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z})$ for $d < 0$.

There are **finitely many** classes in $\operatorname{BQFs}(d)/\operatorname{SL}(2,\mathbb{Z})$ for $d < 0$.

Definition

The number of classes in $\operatorname{BQFs}(d)/\operatorname{SL}(2,\mathbb{Z})$ *is denoted by* $h(d)$ *and called the class number of binary quadratic forms of discriminant* d*.*

There are **finitely many** classes in $\mathrm{BQFs}(d)/\mathrm{SL}(2,\mathbb{Z})$ for $d < 0$.

Definition

The number of classes in $\mathrm{BQFs}(d)/\mathrm{SL}(2,\mathbb{Z})$ *is denoted by* $h(d)$ *and called the class number of binary quadratic forms of discriminant* d*.*

Note: $d = b^2 - 4ac$, so $d \equiv 0$ or $1 \bmod 4$.

- If $d \equiv 0 \bmod 4$, then $x^2 - \frac{d}{4}y^2$ is reduced.
- If $d \equiv 1 \bmod 4$, then $x^2 + xy + \frac{1-d}{4}y^2$ is reduced.

These are called the *principal forms* of discriminant d.

There are **finitely many** classes in $\mathrm{BQFs}(d)/\mathrm{SL}(2,\mathbb{Z})$ for $d < 0$.

Definition

The number of classes in $\mathrm{BQFs}(d)/\mathrm{SL}(2,\mathbb{Z})$ *is denoted by* $h(d)$ *and called the class number of binary quadratic forms of discriminant* d*.*

Note: $d = b^2 - 4ac$, so $d \equiv 0$ or $1 \bmod 4$.

- If $d \equiv 0 \bmod 4$, then $x^2 - \frac{d}{4}y^2$ is reduced.
- If $d \equiv 1 \bmod 4$, then $x^2 + xy + \frac{1-d}{4}y^2$ is reduced.

These are called the *principal forms* of discriminant d. In particular, $h(d) \geq 1$ for every fundamental discriminant d ($\equiv 0$ or $1 \bmod 4$).

There are **finitely many** classes in $\mathrm{BQFs}(d)/\mathrm{SL}(2,\mathbb{Z})$ for $d < 0$.

Definition

The number of classes in $\mathrm{BQFs}(d)/\mathrm{SL}(2,\mathbb{Z})$ *is denoted by* $h(d)$ *and called the class number of binary quadratic forms of discriminant* d.

Note: $d = b^2 - 4ac$, so $d \equiv 0$ or $1 \bmod 4$.

- If $d \equiv 0 \bmod 4$, then $x^2 - \frac{d}{4}y^2$ is reduced.
- If $d \equiv 1 \bmod 4$, then $x^2 + xy + \frac{1-d}{4}y^2$ is reduced.

These are called the *principal forms* of discriminant d. In particular, $h(d) \geq 1$ for every fundamental discriminant d ($\equiv 0$ or $1 \bmod 4$).

Example

$h(-4) = 1$, so all BQFs of discriminant -4 are equivalent to $x^2 + y^2$.

There are **finitely many** classes in $\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z})$ for $d < 0$.

Definition

The number of classes in $\mathrm{BQFs}(d)/\,\mathrm{SL}(2,\mathbb{Z})$ *is denoted by* $h(d)$ *and called the class number of binary quadratic forms of discriminant* d*.*

Note: $d = b^2 - 4ac$, so $d \equiv 0$ or $1 \bmod 4$.

- If $d \equiv 0 \bmod 4$, then $x^2 - \frac{d}{4}y^2$ is reduced.
- If $d \equiv 1 \bmod 4$, then $x^2 + xy + \frac{1-d}{4}y^2$ is reduced.

These are called the *principal forms* of discriminant d. In particular, $h(d) \geq 1$ for every fundamental discriminant d ($\equiv 0$ or $1 \bmod 4$).

Example

$h(-4) = 1$, so all BQFs of discriminant -4 are equivalent to $x^2 + y^2$.

$h(-20) = 2$. All BQFs of disc. -20 are equivalent to $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$.

Exercise: Show that $h(-3) = h(-4) = 1$ and $h(-20) = 2$.

Back to representing primes by binary quadratic forms...

Proposition

Let $\gcd(a, b, c) = 1$*, let* p *be a prime, and put* $d = b^2 - 4ac$*.*

1. *If* $p = am^2 + bmn + cn^2$ *for integers* m, n*, then* $d \equiv \Box \bmod 4p$*.*
2. *If* d *is a square mod* $4p$*, then there exists a binary quadratic form of discriminant* d *that represents* p*.*

Back to representing primes by binary quadratic forms...

Proposition

Let $\gcd(a, b, c) = 1$*, let* p *be a prime, and put* $d = b^2 - 4ac$*.*

1. *If* $p = am^2 + bmn + cn^2$ *for integers* m, n*, then* $d \equiv \square \bmod 4p$*.*
2. *If* d *is a square* $\bmod 4p$*, then there exists a binary quadratic form of discriminant* d *that represents* p*.*

For (2), if $d \equiv b^2 \bmod 4p$, then $d = b^2 - 4pc$, and then the form $px^2 + bxy + cy^2$ represents p for $(x, y) = (1, 0)$.

Back to representing primes by binary quadratic forms...

Proposition

Let $\gcd(a,b,c)=1$, *let* p *be a prime, and put* $d=b^2-4ac$.

1. *If* $p=am^2+bmn+cn^2$ *for integers* m,n, *then* $d\equiv\square \bmod 4p$.
2. *If* d *is a square mod* $4p$, *then there exists a binary quadratic form of discriminant* d *that represents* p.

For (2), if $d\equiv b^2 \bmod 4p$, then $d=b^2-4pc$, and then the form $px^2+bxy+cy^2$ represents p for $(x,y)=(1,0)$.

Corollary

If $h(d)=1$, *then there is a BQF of discriminant* d *that represents* p *if and only if* d *is a square mod* $4p$.

Example

A BQF of discriminant -4 (such as x^2+y^2) represents $p>2$

Back to representing primes by binary quadratic forms...

Proposition

Let $\gcd(a, b, c) = 1$, *let* p *be a prime, and put* $d = b^2 - 4ac$.

1. *If* $p = am^2 + bmn + cn^2$ *for integers* m, n, *then* $d \equiv \square \bmod 4p$.
2. *If* d *is a square mod* $4p$, *then there exists a binary quadratic form of discriminant* d *that represents* p.

For (2), if $d \equiv b^2 \bmod 4p$, then $d = b^2 - 4pc$, and then the form $px^2 + bxy + cy^2$ represents p for $(x, y) = (1, 0)$.

Corollary

If $h(d) = 1$, *then there is a BQF of discriminant* d *that represents* p *if and only if* d *is a square mod* $4p$.

Example

A BQF of discriminant -4 (such as $x^2 + y^2$) represents $p > 2$ if and only if $\left(\frac{-4}{p}\right) = 1 = \left(\frac{-1}{p}\right)$

Back to representing primes by binary quadratic forms...

Proposition

Let $\gcd(a, b, c) = 1$*, let* p *be a prime, and put* $d = b^2 - 4ac$*.*

1. *If* $p = am^2 + bmn + cn^2$ *for integers* m, n*, then* $d \equiv \square \bmod 4p$*.*
2. *If* d *is a square mod* $4p$*, then there exists a binary quadratic form of discriminant* d *that represents* p*.*

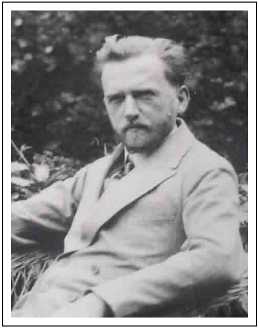
For (2), if $d \equiv b^2 \bmod 4p$, then $d = b^2 - 4pc$, and then the form $px^2 + bxy + cy^2$ represents p for $(x, y) = (1, 0)$.

Corollary

If $h(d) = 1$*, then there is a BQF of discriminant* d *that represents* p *if and only if* d *is a square mod* $4p$*.*

Example

A BQF of discriminant -4 (such as $x^2 + y^2$) represents $p > 2$ if and only if $\left(\frac{-4}{p}\right) = 1 = \left(\frac{-1}{p}\right)$ if and only if $p \equiv 1 \bmod 4$.



Kurt Heegner
1893 – 1965

Alan Baker
1939 – 2018

Harold Stark
1939–

Theorem (Heegner (1952), Baker (1966), Stark (1967))

The only values $d < 0$ with $h(d) = 1$, are

$$d = -3, -4, -7, -8, -11, -19, -43, -67, \text{ and } -163.$$

Corollary

If $h(d) = 1$, then there is a BQF of discriminant d that represents p if and only if d is a square mod $4p$.

Theorem (Baker (1966), Heegner (1952), Stark (1967))

The only values $d < 0$ with $h(d) = 1$, are

$$d = -3, -4, -7, -8, -11, -19, -43, -67, \text{ and } -163.$$

Corollary

If $h(d) = 1$, then there is a BQF of discriminant d that represents p if and only if d is a square mod $4p$.

Theorem (Baker (1966), Heegner (1952), Stark (1967))

The only values $d < 0$ with $h(d) = 1$, are

$$d = -3, -4, -7, -8, -11, -19, -43, -67, \text{ and } -163.$$

Example

Let p be a prime.

- $(d = -3)$ $x^2 + xy + y^2 = p$ if and only if $\left(\frac{-3}{p}\right) = 1$.

Corollary

If $h(d) = 1$, then there is a BQF of discriminant d that represents p if and only if d is a square mod $4p$.

Theorem (Baker (1966), Heegner (1952), Stark (1967))

The only values $d < 0$ with $h(d) = 1$, are

$$d = -3, -4, -7, -8, -11, -19, -43, -67, \text{ and } -163.$$

Example

Let p be a prime.

- $(d = -3)$ $x^2 + xy + y^2 = p$ if and only if $\left(\frac{-3}{p}\right) = 1$.
- $(d = -8)$ $x^2 + 2y^2 = p$ if and only if $\left(\frac{-2}{p}\right) = 1$.

Corollary

If $h(d) = 1$, then there is a BQF of discriminant d that represents p if and only if d is a square mod $4p$.

Theorem (Baker (1966), Heegner (1952), Stark (1967))

The only values $d < 0$ with $h(d) = 1$, are

$$d = -3, -4, -7, -8, -11, -19, -43, -67, \textit{ and } -163.$$

Example

Let p be a prime.

- ($d = -3$) $x^2 + xy + y^2 = p$ if and only if $\left(\frac{-3}{p}\right) = 1$.
- ($d = -8$) $x^2 + 2y^2 = p$ if and only if $\left(\frac{-2}{p}\right) = 1$.
- ($d = -20$)
  - $p = x^2 + 5y^2$ if and only if $p = 5$ or $p \equiv 1$ or 9 mod 20.
  - $p = 2x^2 + 2xy + 3y^2$ iff $p = 2$ or $p \equiv 3$ or 7 mod 20.

Before: primes represented by quadratic forms.

Question

What **numbers** are represented by BQFs?

Before: primes represented by quadratic forms.

Question

What **numbers** are represented by BQFs?

For instance, let $f(x, y) = x^2 + y^2$. Then,

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' + yy')^2 + (xy' - x'y)^2,$$

so if n, m are sums of squares, then $n \cdot m$ is also a sum of squares.

Before: primes represented by quadratic forms.

Question

What **numbers** are represented by BQFs?

For instance, let $f(x, y) = x^2 + y^2$. Then,

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' + yy')^2 + (xy' - x'y)^2,$$

so if n, m are sums of squares, then $n \cdot m$ is also a sum of squares. Similarly: $(x^2 + dy^2)(x'^2 + dy'^2) = (xx' + yy')^2 + d(xy' - x'y)^2$. So what if $f(x, y) = ax^2 + bxy + cy^2$?

Before: primes represented by quadratic forms.

Question

What **numbers** are represented by BQFs?

For instance, let $f(x, y) = x^2 + y^2$. Then,

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' + yy')^2 + (xy' - x'y)^2,$$

so if n, m are sums of squares, then $n \cdot m$ is also a sum of squares. Similarly: $(x^2 + dy^2)(x'^2 + dy'^2) = (xx' + yy')^2 + d(xy' - x'y)^2$. So what if $f(x, y) = ax^2 + bxy + cy^2$?

Gauss: If f and g are BQFs of discriminant d, then there exists $h \in \text{BQFs}(d)$ such that

$$f(x, y) \cdot g(x', y') = h(m, n),$$

where $m = m(x, y, x', y')$ and $n = n(x, y, x', y')$ are bilinear forms.

Gauss: If f and g are BQFs of discriminant d, then there exists $h \in \mathrm{BQFs}(d)$ such that

$$f(x,y) \cdot g(x',y') = h(m,n),$$

where $m = m(x,y,x',y')$ and $n = n(x,y,x',y')$ are bilinear forms.

Example (Gauss' "composition")

Let

$$f(x,y) = 4x^2 + 3xy + 5y^2, \text{ and } g(x',y') = 3x'^2 + x'y' + 6y'^2,$$

forms of discriminant -71.

Gauss: If f and g are BQFs of discriminant d, then there exists $h \in \text{BQFs}(d)$ such that

$$f(x,y) \cdot g(x',y') = h(m,n),$$

where $m = m(x,y,x',y')$ and $n = n(x,y,x',y')$ are bilinear forms.

Example (Gauss' "composition")

Let

$$f(x,y) = 4x^2 + 3xy + 5y^2, \text{ and } g(x',y') = 3x'^2 + x'y' + 6y'^2,$$

forms of discriminant -71. Then,

$$f(x,y)g(x',y') = 2m^2 + mn + 9n^2$$

which is also of discriminant -71, with

$$m = xx' - 3xy' - 2yx' - 3yy',$$

$$n = xx' + xy' + yx' - yy'.$$

Gauss' composition is extraordinarily complicated, and it takes Gauss pages to explain how it works in his *Disquisitiones Arithmeticae*.

characteristicus formae datae etiam toti classi et generi tribui potest; denique 1 semper esse numerum characteristicum formae classis et generis principalis, sive quamlibet formam e genere principali esse residuum determinantis sui.

VII. Si (g, h) est valor expr. $\sqrt{M(a, b, c)}\,(\text{mod.}\, m)$, atque $g' \equiv g$, $h' \equiv h$ (mod. m): erit etiam (g', h') valor eiusdem expressionis. Tales valores pro *aequivalentibus* haberi possunt; contra si (g, h), (g', h') sunt valores eiusdem expr. $\sqrt{M(a, b, c)}$, neque tamen simul $g' \equiv g$, $h' \equiv h\,(\text{mod.}\, m)$, *diversi* sunt censendi. Manifesto quoties (g, h) est valor talis expressionis, etiam $(-g, -h)$ erit, facileque demonstratur, hos valores semper esse diversos nisi $m = 2$. Aeque facile demonstratur, expressionem $\sqrt{M(a, b, c)}\,(\text{mod.}\, m)$ plures valores diversos quam duos tales (oppositos) habere non posse, quando m sit aut numerus primus impar aut numeri primi imparis potestas aut $= 4$; quando vero m sit $= 8$ aut altior potestas numeri 2, quatuor omnino dari. Hinc facile deducitur per VI, si determinans D formae (a, b, c) sit $= \pm 2^{\mu} A^{\alpha} B^{\beta} \ldots$, designantibus A, B etc. numeros primos impares diversos quorum multitudo $= n$, atque M numerus characteristicus illius formae: dari omnino vel 2^n vel 2^{n+1} vel 2^{n+2} valores diversos expr. $\sqrt{M(a, b, c)}\,(\text{mod.}\, D)$, prout μ vel < 2 vel $= 2$ vel > 2. Ita *e. g.* habentur sedecim valores expr. $\sqrt{7\,(12, 6, -17)}$ (mod. 240), puta $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Demonstrationem ampliorem quum ad sequentia non sit adeo necessaria, brevitatis gratia non apponimus.

VIII. Denique observamus, si duarum formarum aequivalentium (a, b, c), (a', b', c') determinans sit D, numerus characteristicus M, priorque transeat in posteriorem per substitutionem $\alpha, \beta, \gamma, \delta$: ex quovis valore expr. $\sqrt{M(a, b, c)}$ ut (g, h) sequi valorem expr. $\sqrt{M(a', b', c')}$, puta $(\alpha g + \gamma h,\ \beta g + \delta h)$. Demonstrationem quisque nullo negotio eruere poterit.

De compositione formarum.

234.

Postquam haec de formis in classes genera et ordines distribuendis praemisimus, proprietatesque generales quae ex his distinctionibus statim defluunt explicavimus, ad aliud argumentum gravissimum transimus a nemine hucusque attactum, de formarum *compositione*. In cuius disquisitionis limine, ne posthac demonstrationum seriem continuam interrumpere oporteat, statim intercalamus

LEMMA. *Habentur quatuor series numerorum integrorum*

$$a, a', a'' \ldots a^n; \quad b, b', b'' \ldots b^n; \quad c, c', c'' \ldots c^n; \quad d, d', d'' \ldots d^n$$

ex aeque multis (puta $n+1$*) terminis constantes, atque ita comparatae, ut*

$$cd'-dc',\ cd''-dc''\ \text{etc.},\quad c'd''-d'c''\ \text{etc. etc.}$$

respective sint

$$= k(ab'-ba'),\quad k(ab''-ba'')\ \text{etc.},\quad k(a'b''-b'a'')\ \text{etc. etc.}$$

sive generaliter

$$c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$$

denotante k *numerum integrum datum;* λ, μ *integros quoscunque inaequales inter* 0 *et* n *incl. quorum maior* μ *); *praeterea omnes* $a^\lambda b^\mu - b^\lambda a^\mu$ *divisorem communem non habent. Tunc inveniri possunt quatuor numeri integri* α, β, γ, δ *tales, ut sit*

$$\alpha a+\beta b = c,\quad \alpha a'+\beta b' = c',\quad \alpha a''+\beta b'' = c''\ \text{etc.}$$
$$\gamma a+\delta b = d,\quad \gamma a'+\delta b' = d',\quad \gamma a''+\delta b'' = d''\ \text{etc.}$$

sive generaliter

$$\alpha a^\nu+\beta b^\nu = c^\nu,\quad \gamma a^\nu+\delta b^\nu = a^\nu$$

quo facto erit

$$\alpha\delta-\beta\gamma = k$$

Quum per hyp. numeri $ab'-ba'$, $ab''-ba''$ etc. $a'b''-b'a''$ etc. (quorum multitudo erit $=\frac{1}{2}(n+1)n$) divisorem communem non habeant, inveniri poterunt totidem alii numeri integri, per quos illis resp. multiplicatis productorum summa fiat $=1$ (art. 40). Designentur hi multiplicatores per $(0,1)$, $(0,2)$ etc. $(1,2)$ etc., sive generaliter multiplicator ipsius $a^\lambda b^\mu - b^\lambda a^\mu$ per (λ,μ), ita ut sit

$$\Sigma(\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = 1$$

(Per literam Σ denotamus aggregatum omnium valorum expressionis, cui praefixa

*) Considerando a tamquam a^0, b tamquam b^0 etc. — Ceterum manifesto eadem aequatio valebit quoque quando $\lambda=\mu$ aut $\lambda>\mu$.

est, qui oriuntur tribuendo ipsis λ, μ omnes valores inaequales inter 0 et n, ita ut sit $\mu > \lambda$. Quo facto si statuitur

$$\Sigma(\lambda, \mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha, \quad \Sigma(\lambda, \mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \beta$$
$$\Sigma(\lambda, \mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma, \quad \Sigma(\lambda, \mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta$$

hi α, β, γ, δ proprietatibus praescriptis erunt praediti.

Dem. I. Denotante ν numerum quemcunque integrum inter 0 et n, erit

$$\begin{aligned} \alpha a^\nu + \beta b^\nu &= \Sigma(\lambda, \mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu) \\ &= \tfrac{1}{k}\Sigma(\lambda, \mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu) \\ &= \tfrac{1}{k} c^\nu \Sigma(\lambda, \mu)(c^\lambda d^\mu - d^\lambda c^\mu) \\ &= c^\nu \Sigma(\lambda, \mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu \end{aligned}$$

Et per calculum similem eruitur

$$\gamma a^\nu + \delta b^\nu = d^\nu. \quad Q.\ E.\ P.$$

II. Quoniam igitur

$$c^\lambda = \alpha a^\lambda + \beta b^\lambda, \quad c^\mu = \alpha a^\mu + \beta b^\mu$$

fit

$$c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$$

similique modo

$$\begin{aligned} a^\lambda c^\mu - c^\lambda a^\mu &= \beta(a^\lambda b^\mu - b^\lambda a^\mu) \\ d^\lambda b^\mu - b^\lambda d^\mu &= \gamma(a^\lambda b^\mu - b^\lambda a^\mu) \\ a^\lambda d^\mu - d^\lambda a^\mu &= \delta(a^\lambda b^\mu - b^\lambda a^\mu) \end{aligned}$$

ex quibus formulis valores ipsorum α, β, γ, δ multo facilius erui possunt, si modo λ, μ ita accipiuntur, ut $a^\lambda b^\mu - b^\lambda a^\mu$ non sit $= 0$, quod certo fieri poterit, quia omnes $a^\lambda b^\mu - b^\lambda a^\mu$ per hyp. divisorem communem non habent, adeoque *omnes* $= 0$ esse nequeunt. — Ex iisdem aequationibus deducitur, multiplicando primam per quartam, secundam per tertiam et subtrahendo,

$$(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2$$

unde necessario

$$\alpha\delta - \beta\gamma = k. \quad Q.\ E.\ S.$$

235.

Si forma $AXX+2BXY+CYY\dots F$

transit in productum e duabus formis

$$axx+2bxy+cyy\dots f,\quad \text{et}\quad a'x'x'+2b'x'y'+c'y'y'\dots f'$$

per substitutionem talem

$$\begin{aligned} X &= pxx'+p'xy'+p''yx'+p'''yy' \\ Y &= qxx'+q'xy'+q''yx'+q'''yy' \end{aligned}$$

(quod brevitatis causa in sequentibus semper ita exprimemus: Si F transit in ff' per substitutionem $p, p', p'', p'''; q, q', q'', q'''$*)), dicemus simpliciter, formam F *transformabilem* esse in ff'; si insuper haec transformatio ita est comparata, ut sex numeri

$$pq'-qp',\ pq''-qp'',\ pq'''-qp''',\ p'q''-q'p'',\ p'q'''-q'p''',\ p''q'''-q''p'''$$

divisorem communem non habeant: formam F e formis f, f' *compositam* vocabimus.

Inchoabimus hanc disquisitionem a suppositione generalissima, formam F in ff' transire per substitutionem $p, p', p'', p'''; q, q', q'', q'''$ et quae inde sequantur evolvemus. Manifesto huic suppositioni ex asse aequivalebunt sequentes novem aequationes (*i. e.* simulac hae aequationes locum habent, F per substitutionem dictam transibit in ff', et vice versa):

$$\begin{aligned}
App+2Bpq+Cqq &= aa' \quad\dots [1] \\
Ap'p'+2Bp'q'+Cq'q' &= ac' \quad\dots [2] \\
Ap''p''+2Bp''q''+Cq''q'' &= ca' \quad\dots [3] \\
Ap'''p'''+2Bp'''q'''+Cq'''q''' &= cc' \quad\dots [4] \\
App'+B(pq'+qp')+Cqq' &= ab' \quad\dots [5] \\
App''+B(pq''+qp'')+Cqq'' &= ba' \quad\dots [6] \\
Ap'p'''+B(p'q'''+q'p''')+Cq'q''' &= bc' \quad\dots [7] \\
Ap''p'''+B(p''q'''+q''p''')+Cq''q''' &= cb' \quad\dots [8] \\
A(pp'''+p'p'')+B(pq'''+qp'''+p'q''+q'p'')+C(qq'''+q'q'') &= 2bb' \quad\dots [9]
\end{aligned}$$

*) In hac igitur designatione ad ordinem tum coefficientium p, p' etc. tum formarum f, f' probe respicere oportet. Facile autem perspicietur, si ordo formarum f, f' convertatur ut prior fiat posterior coefficientes p', q' cum his p'', q'' commutandos esse, reliquos suo quemlibet loco manere.

Sint determinantes formarum F, f, f' resp. D, d, d'; divisores communes maximi numerorum $A, 2B, C$; $a, 2b, c$; $a', 2b', c'$ resp. M, m, m' (quos omnes positive acceptos supponimus). Porro determinentur sex numeri integri $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ ita ut sit

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m, \quad \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$$

Denique designentur numeri

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''', \quad p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

resp. per P, Q, R, S, T, U, sitque ipsorum divisor communis maximus positive acceptus $= k$. — Iam ponendo

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \quad \ldots\ldots [10]$$

fit ex aequ. 9

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \quad \ldots\ldots [11]$$

Ex his undecim aequationibus $1 \ldots 11$, sequentes novas evolvimus *):

$$\begin{aligned}
DPP &= d'aa \ldots\ldots [12]\\
DP(R-S) &= 2d'ab \ldots\ldots [13]\\
DPU &= d'ac - (\Delta\Delta - dd') \ldots\ldots [14]\\
D(R-S)^2 &= 4d'bb + 2(\Delta\Delta - dd') \ldots\ldots [15]\\
D(R-S)U &= 2d'bc \ldots\ldots [16]\\
DUU &= d'cc \ldots\ldots [17]\\
DQQ &= da'a' \ldots\ldots [18]\\
DQ(R+S) &= 2da'b' \ldots\ldots [19]\\
DQT &= da'c' - (\Delta\Delta - dd') \ldots\ldots [20]\\
D(R+S)^2 &= 4db'b' + 2(\Delta\Delta - dd') \ldots\ldots [21]\\
D(R+S)T &= 2db'c' \ldots\ldots [22]\\
DTT &= dc'c' \ldots\ldots [23]
\end{aligned}$$

Hinc rursus deducuntur hae duae:

*) Origo harum aequationum haec est: 12 ex 5.5 — 1.2; 13 ex 5.9 — 1.7 — 2.6; 14 ex 10.11 — 6.7; 15 ex 5.8 + 5.8 + 10.10 + 11.11 — 1.4 — 2.3 — 6.7 — 6.7; 16 ex 8.9 — 3.7 — 4.6; 17 ex 8.8 — 3.4. Deductio sex reliquarum eodem modo adornatur, si modo aequationes 2, 5, 7 cum aequationibus 3, 6, 8 resp. commutantur, et reliquae 1, 4, 9, 10, 11 eodem loco deinceps retinentur, puta 18 ex 6.6 — 1.3 etc.

Dirichlet was Gauss' student and, apparently, he traveled everywhere with a copy of his advisor's *Disquisitiones Arithmeticae*. He slept with it under his pillow, hoping that inspiration would come at night and it would help him understand some of the tougher passages in this book.

Dirichlet's hard work reading *Disquisitiones* paid off, and he went on to interpret Gauss' composition law of quadratic forms in terms of what we would today call **ideals**; and this, in turn, led to the birth of modern algebra by Dedekind.

(Quadratic) Number Fields

(Quadratic) Number Fields

e.g., $K = \mathbb{Q}(\sqrt{-5})$.

Richard Dedekind
1831 – 1916

Let d be a square-free integer and let $K_d = \mathbb{Q}(\sqrt{d})$.
Let $\mathcal{O}_{K_d}$ be the ring of integers of K_d. Then:

$$\mathcal{O}_{K_d} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Let d be a square-free integer and let $K_d = \mathbb{Q}(\sqrt{d})$.
Let $\mathcal{O}_{K_d}$ be the ring of integers of K_d. Then:

$$\mathcal{O}_{K_d} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Consider the set of all rings of integers $\mathcal{O}_{K_d}$:

$$\left\{\mathcal{O}_{K_d} : d \text{ square-free}\right\}.$$

Question

How many of these rings are Unique Factorization Domains?

Let d be a square-free integer and let $K_d = \mathbb{Q}(\sqrt{d})$.
Let $\mathcal{O}_{K_d}$ be the ring of integers of K_d. Then:

$$\mathcal{O}_{K_d} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Consider the set of all rings of integers $\mathcal{O}_{K_d}$:

$$\left\{ \mathcal{O}_{K_d} : d \text{ square-free} \right\}.$$

Question

How many of these rings are Unique Factorization Domains?

The ring $\mathcal{O}_{K_d}$ is a Dedekind domain, so UFD if and only if Principal Ideal Domain.

Let d be a square-free integer and let $K_d = \mathbb{Q}(\sqrt{d})$.
Let $\mathcal{O}_{K_d}$ be the ring of integers of K_d. Then:

$$\mathcal{O}_{K_d} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Consider the set of all rings of integers $\mathcal{O}_{K_d}$:

$$\left\{ \mathcal{O}_{K_d} : d \text{ square-free} \right\}.$$

Question

How many of these rings are Unique Factorization Domains?

The ring $\mathcal{O}_{K_d}$ is a Dedekind domain, so UFD if and only if Principal Ideal Domain.

Question

How many of these rings are Principal Ideal Domains?

Question

How many of these rings are Principal Ideal Domains?

We define the class group of $\mathcal{O}_{K_d}$ to measure the failure of being a PID.

$$\mathrm{Cl}(\mathcal{O}_{K_d}) = \frac{\text{Fractional ideals}}{\text{Principal Ideals}},$$

so that two fractional ideals are in the same class (write $I \sim J$ or $[I] = [J]$) if and only if there is a non-zero $\alpha \in K_d$ such that $I = \alpha \cdot J$.

Question

How many of these rings are Principal Ideal Domains?

We define the class group of $\mathcal{O}_{K_d}$ to measure the failure of being a PID.

$$\mathrm{Cl}(\mathcal{O}_{K_d}) = \frac{\text{Fractional ideals}}{\text{Principal Ideals}},$$

so that two fractional ideals are in the same class (write $I \sim J$ or $[I] = [J]$) if and only if there is a non-zero $\alpha \in K_d$ such that $I = \alpha \cdot J$.

Fact: Any ideal $I \subseteq \mathbb{Z}[\sqrt{d}]$ can be written

$$I = s \cdot (a, b + \sqrt{d}),$$

where $s, a, b \in \mathbb{Z}$, and a divides $b^2 - d$. Here

$$(a, b + \sqrt{d}) = \{ax + (b + \sqrt{d})y : x, y \in \mathbb{Z}\}.$$

Fact: Any ideal $I \subseteq \mathbb{Z}[\sqrt{d}]$ can be written

$$I = s \cdot (a, b + \sqrt{d}),$$

where $s, a, b \in \mathbb{Z}$, and a divides $b^2 - d$.

What is the **norm** of an element $ax + (b + \sqrt{d})y$, for some $x, y, \in \mathbb{Z}$?

Fact: Any ideal $I \subseteq \mathbb{Z}[\sqrt{d}]$ can be written

$$I = s \cdot (a, b + \sqrt{d}),$$

where $s, a, b \in \mathbb{Z}$, and a divides $b^2 - d$.

What is the **norm** of an element $ax + (b + \sqrt{d})y$, for some $x, y, \in \mathbb{Z}$?

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}}^{K_d}(ax + (b + \sqrt{d})y) &= (ax + (b + \sqrt{d})y) \cdot (ax + (b - \sqrt{d})y) \\
&= a^2x^2 + a(b - \sqrt{d})xy + a(b + \sqrt{d})xy + (b^2 - d)y^2 \\
&= a^2x^2 + 2abxy + 4acy^2 \\
&= a \cdot (ax^2 + 2bxy + 4cy^2),
\end{aligned}$$

where $b^2 - d = 4ac$.

Fact: Any ideal $I \subseteq \mathbb{Z}[\sqrt{d}]$ can be written

$$I = s \cdot (a, b + \sqrt{d}),$$

where $s, a, b \in \mathbb{Z}$, and a divides $b^2 - d$.

What is the **norm** of an element $ax + (b + \sqrt{d})y$, for some $x, y, \in \mathbb{Z}$?

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}}^{K_d}(ax + (b + \sqrt{d})y) &= (ax + (b + \sqrt{d})y) \cdot (ax + (b - \sqrt{d})y) \\
&= a^2x^2 + a(b - \sqrt{d})xy + a(b + \sqrt{d})xy + (b^2 - d)y^2 \\
&= a^2x^2 + 2abxy + 4acy^2 \\
&= a \cdot (ax^2 + 2bxy + 4cy^2),
\end{aligned}$$

where $b^2 - d = 4ac$. Then:

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}}^{K_d}\left(ax + \frac{(b + \sqrt{d})}{2}y\right) &= \left(ax + \frac{(b + \sqrt{d})}{2}y\right) \cdot \left(ax + \frac{(b - \sqrt{d})}{2}y\right) \\
&= a \cdot (ax^2 + bxy + cy^2).
\end{aligned}$$

$$\mathrm{N}_{\mathbb{Q}}^{K_d}\left(ax+\frac{(b+\sqrt{d})}{2}y\right)=\left(ax+\frac{(b+\sqrt{d})}{2}y\right)\cdot\left(ax+\frac{(b-\sqrt{d})}{2}y\right)$$
$$=a\cdot(ax^2+bxy+cy^2).$$

Example

Let $d=-20$. The values of $f(x,y)=x^2+5y^2$ are norms of elements in
$$(1,\sqrt{-20}/2)=(1,\sqrt{-5})=\mathcal{O}_{K_d}.$$

$$\mathrm{N}_{\mathbb{Q}}^{K_d}\left(ax+\frac{(b+\sqrt{d})}{2}y\right)=\left(ax+\frac{(b+\sqrt{d})}{2}y\right)\cdot\left(ax+\frac{(b-\sqrt{d})}{2}y\right)$$
$$=a\cdot(ax^2+bxy+cy^2).$$

Example

Let $d=-20$. The values of $f(x,y)=x^2+5y^2$ are norms of elements in

$$(1,\sqrt{-20}/2)=(1,\sqrt{-5})=\mathcal{O}_{K_d}.$$

Example

Let $d=-20$. The values of $g(x,y)=2x^2+2xy+3y^2$ are $(1/2)\cdot$norms of elements in

$$(2,(2+\sqrt{-20})/2)=(2,1+\sqrt{-5})=\mathcal{P}_2,$$

which is a prime ideal above 2.

Example

Let $d = -20$. The values of $g(x, y) = 2x^2 + 2xy + 3y^2$ are $(1/2)\cdot$norms of elements in

$$(2, (2 + \sqrt{-20})/2) = (2, 1 + \sqrt{-5}) = \mathcal{P}_2,$$

which is a prime ideal above 2.

Is the ideal $\mathcal{P}_2 = (2, 1 + \sqrt{-5})$ principal? Is $\mathcal{P}_2 \sim \mathcal{O}_{K_d}$?

Example

Let $d = -20$. The values of $g(x, y) = 2x^2 + 2xy + 3y^2$ are $(1/2)\cdot$norms of elements in

$$(2, (2 + \sqrt{-20})/2) = (2, 1 + \sqrt{-5}) = \mathcal{P}_2,$$

which is a prime ideal above 2.

Is the ideal $\mathcal{P}_2 = (2, 1 + \sqrt{-5})$ principal? Is $\mathcal{P}_2 \sim \mathcal{O}_{K_d}$? If so:

- There is $\alpha \in K_d$ such that $\mathcal{P}_2 = \alpha \cdot \mathcal{O}_{K_d}$.

Example

Let $d = -20$. The values of $g(x, y) = 2x^2 + 2xy + 3y^2$ are $(1/2)\cdot$norms of elements in

$$(2, (2 + \sqrt{-20})/2) = (2, 1 + \sqrt{-5}) = \mathcal{P}_2,$$

which is a prime ideal above 2.

Is the ideal $\mathcal{P}_2 = (2, 1 + \sqrt{-5})$ principal? Is $\mathcal{P}_2 \sim \mathcal{O}_{K_d}$? If so:

- There is $\alpha \in K_d$ such that $\mathcal{P}_2 = \alpha \cdot \mathcal{O}_{K_d}$.
- $N(\tau) = N(\alpha)N(\gamma)$ for every $\tau \in \mathcal{P}_2$ and some $\gamma \in \mathcal{O}_{K_d}$.

Example

Let $d = -20$. The values of $g(x,y) = 2x^2 + 2xy + 3y^2$ are $(1/2)$·norms of elements in

$$(2, (2+\sqrt{-20})/2) = (2, 1+\sqrt{-5}) = \mathcal{P}_2,$$

which is a prime ideal above 2.

Is the ideal $\mathcal{P}_2 = (2, 1+\sqrt{-5})$ principal? Is $\mathcal{P}_2 \sim \mathcal{O}_{K_d}$? If so:

- There is $\alpha \in K_d$ such that $\mathcal{P}_2 = \alpha \cdot \mathcal{O}_{K_d}$.
- $N(\tau) = N(\alpha)N(\gamma)$ for every $\tau \in \mathcal{P}_2$ and some $\gamma \in \mathcal{O}_{K_d}$.
- $2 = N(\mathcal{P}_2) = N(\alpha)N(\mathcal{O}_{K_d}) = N(\alpha)$, so $N(\alpha) = 2$.

Example

Let $d = -20$. The values of $g(x, y) = 2x^2 + 2xy + 3y^2$ are $(1/2)\cdot$norms of elements in

$$(2, (2 + \sqrt{-20})/2) = (2, 1 + \sqrt{-5}) = \mathcal{P}_2,$$

which is a prime ideal above 2.

Is the ideal $\mathcal{P}_2 = (2, 1 + \sqrt{-5})$ principal? Is $\mathcal{P}_2 \sim \mathcal{O}_{K_d}$? If so:

- There is $\alpha \in K_d$ such that $\mathcal{P}_2 = \alpha \cdot \mathcal{O}_{K_d}$.
- $N(\tau) = N(\alpha)N(\gamma)$ for every $\tau \in \mathcal{P}_2$ and some $\gamma \in \mathcal{O}_{K_d}$.
- $2 = N(\mathcal{P}_2) = N(\alpha)N(\mathcal{O}_{K_d}) = N(\alpha)$, so $N(\alpha) = 2$.
- Thus, norms from $\mathcal{P}_2$ equal norms from $\alpha\mathcal{O}_{K_d}$ implies

  $$2 \cdot g(x, y) = 2 \cdot f(x', y')$$

  so $f(x, y) = x^2 + 5y^2$ and $g(x, y) = 2x^2 + 2xy + 3y^2$ represent the same numbers.

Example

Let $d = -20$. The values of $g(x,y) = 2x^2 + 2xy + 3y^2$ are $(1/2)\cdot$norms of elements in

$$(2, (2+\sqrt{-20})/2) = (2, 1+\sqrt{-5}) = \mathcal{P}_2,$$

which is a prime ideal above 2.

Is the ideal $\mathcal{P}_2 = (2, 1+\sqrt{-5})$ principal? Is $\mathcal{P}_2 \sim \mathcal{O}_{K_d}$? If so:

- There is $\alpha \in K_d$ such that $\mathcal{P}_2 = \alpha \cdot \mathcal{O}_{K_d}$.
- $N(\tau) = N(\alpha)N(\gamma)$ for every $\tau \in \mathcal{P}_2$ and some $\gamma \in \mathcal{O}_{K_d}$.
- $2 = N(\mathcal{P}_2) = N(\alpha)N(\mathcal{O}_{K_d}) = N(\alpha)$, so $N(\alpha) = 2$.
- Thus, norms from $\mathcal{P}_2$ equal norms from $\alpha\mathcal{O}_{K_d}$ implies

  $$2 \cdot g(x,y) = 2 \cdot f(x',y')$$

  so $f(x,y) = x^2 + 5y^2$ and $g(x,y) = 2x^2 + 2xy + 3y^2$ represent the same numbers. Contradiction!!

THANK YOU

alvaro.lozano-robledo@uconn.edu

http://alozano.clas.uconn.edu

"*If by chance I have omitted anything*
more or less proper or necessary,
I beg forgiveness,
since there is no one who is without fault
and circumspect in all matters."

Leonardo Pisano (Fibonacci), *Liber Abaci*.