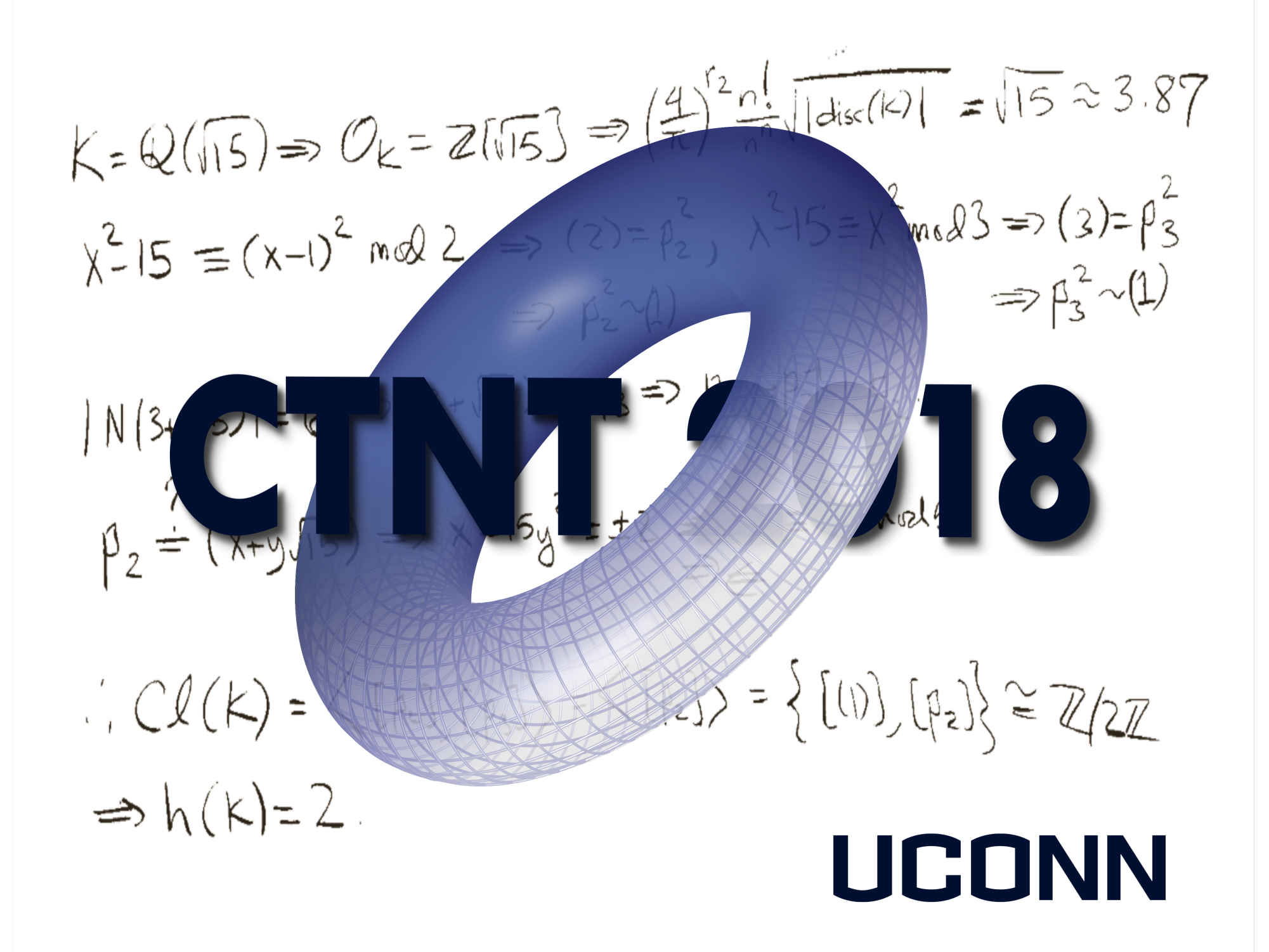

CTNT 2018
UCONN

Arithmetic Statistics
Lecture 3

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

May 28th

CTNT 2018
Connecticut Summer School
in Number Theory

PREVIOUSLY...

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

PREVIOUSLY...

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

Associative? Not when defined like this. See first slide in Lecture 4.

PREVIOUSLY...

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

Associative? Not when defined like this. See first slide in Lecture 4.

Gauss called this **proper equivalence**.

PREVIOUSLY...

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

Associative? Not when defined like this. See first slide in Lecture 4.

Gauss called this **proper equivalence**. If we change variables by a matrix in $\mathrm{GL}(2,\mathbb{Z})$ with determinant -1, Gauss called this **improper equivalence**. With $\det = \pm 1$ we say **wide equivalence**.

PREVIOUSLY...

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

Associative? Not when defined like this. See first slide in Lecture 4.

Gauss called this **proper equivalence**. If we change variables by a matrix in $\mathrm{GL}(2,\mathbb{Z})$ with determinant -1, Gauss called this **improper equivalence**. With $\det = \pm 1$ we say **wide equivalence**.

Proper equivalence leads to the *narrow* ideal class group of a ring of integers. **Wide equivalence** leads to the ideal class group.

PREVIOUSLY...

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 $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$.

PREVIOUSLY...

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 $N(\alpha) = 2$.
- 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 $g(x', y') = 2x'^2 + 2x'y' + 3y'^2$ represent the same numbers. Contradiction!!

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$?

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

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

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

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

$$ax^2 + bxy + cy^2 \longleftrightarrow cx'^2 - bx'y' + ay'^2.$$

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

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

$$ax^2 + bxy + cy^2 \longleftrightarrow cx'^2 - bx'y' + ay'^2.$$

$$(a, b+\sqrt{d}) \longleftrightarrow (c, -b+\sqrt{d}).$$

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

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

$$ax^2 + bxy + cy^2 \longleftrightarrow cx'^2 - bx'y' + ay'^2.$$

$$(a, b+\sqrt{d}) \longleftrightarrow (c, -b+\sqrt{d}).$$

$$\frac{-b+\sqrt{d}}{2} \cdot \left(a, \frac{b+\sqrt{d}}{2}\right) = \left(a \cdot \frac{-b+\sqrt{d}}{2}, \frac{b^2-d}{4}\right) = a\left(\frac{-b+\sqrt{d}}{2}, c\right).$$

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

$$\frac{-b+\sqrt{d}}{2} \cdot \left(a, \frac{b+\sqrt{d}}{2}\right) = \left(a \cdot \frac{-b+\sqrt{d}}{2}, \frac{b^2-d}{4}\right) = a\left(\frac{-b+\sqrt{d}}{2}, c\right).$$

Upshot:

Conversely, Gauss' reduction of binary quadratic forms gives a method to check the ideal class of any fractional ideal I.

For example, in $\mathbb{Q}(\sqrt{-5})$, we have $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Let $I = (3, 1+\sqrt{-5}) = (3, (2+\sqrt{-20})/2)$. Is it equivalent to $\mathcal{P}_2$? The norms of elements of I are of the form

$$3 \cdot (3x^2 + 2xy + 2y^2)$$

but the form $3x^2 + 2xy + 2y^2$ is not reduced.

$$\frac{-b+\sqrt{d}}{2} \cdot \left(a, \frac{b+\sqrt{d}}{2}\right) = \left(a \cdot \frac{-b+\sqrt{d}}{2}, \frac{b^2-d}{4}\right) = a\left(\frac{-b+\sqrt{d}}{2}, c\right).$$

Upshot:

$$\begin{aligned}\left(3, \frac{2+\sqrt{-20}}{2}\right) &= \frac{3}{\frac{-2+\sqrt{-20}}{2}}\left(2, \frac{-2+\sqrt{-20}}{2}\right) \\ &= \frac{3}{\frac{-2+\sqrt{-20}}{2}}(2, -1+\sqrt{-5}) = \frac{3}{\frac{-2+\sqrt{-20}}{2}}(2, 1+\sqrt{-5})\end{aligned}$$

Note: What does the second step to reduce forms do to ideals?

- 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 $b' = b - 2ka$.

Note: What does the second step to reduce forms do to ideals?

- 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 $b' = b - 2ka$.

It transforms binary forms as follows:

$$\begin{aligned} ax^2 + bxy + cy^2 &= a(x' - ky')^2 + b(x' - ky')y' + cy'^2 \\ &= ax'^2 + (-2ak + b)x'y' + (-ak^2 - bk + c)y'^2. \end{aligned}$$

So it transforms

$$\left(a, \frac{b + \sqrt{d}}{2}\right) \longleftrightarrow \left(a, \frac{b - 2ak + \sqrt{d}}{2}\right)$$

Note: What does the second step to reduce forms do to ideals?

- 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 $b' = b - 2ka$.

It transforms binary forms as follows:

$$\begin{aligned} ax^2 + bxy + cy^2 &= a(x' - ky')^2 + b(x' - ky')y' + cy'^2 \\ &= ax'^2 + (-2ak + b)x'y' + (-ak^2 - bk + c)y'^2. \end{aligned}$$

So it transforms

$$\left(a, \frac{b + \sqrt{d}}{2}\right) \longleftrightarrow \left(a, \frac{b - 2ak + \sqrt{d}}{2}\right)$$

and these ideals are identical.

Binary quadratic forms $\leftrightsquigarrow$ ideals in quadratic fields

Binary quadratic forms $\leftrightsquigarrow$ ideals in quadratic fields

leads to an isomorphism

$$\text{BQFs(d)} \,/\, \text{SL}(2,\mathbb{Z}) \cong \mathrm{Cl}^{+}(\mathcal{O}_{K_d}) \cong \mathrm{Cl}(\mathcal{O}_{K_d})$$

for $d < 0$, where the group law on the left-hand side is Gauss' composition of quadratic forms. (For $d > 0$, the narrow and wide class groups are not isomorphic in general.)

Binary quadratic forms $\leftrightsquigarrow$ ideals in quadratic fields

leads to an isomorphism

$$\mathrm{BQFs(d)} \,/\, \mathrm{SL}(2,\mathbb{Z}) \cong \mathrm{Cl}^{+}(\mathcal{O}_{K_d}) \cong \mathrm{Cl}(\mathcal{O}_{K_d})$$

for $d < 0$, where the group law on the left-hand side is Gauss' composition of quadratic forms. (For $d > 0$, the narrow and wide class groups are not isomorphic in general.)

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

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

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

Binary quadratic forms $\leftrightsquigarrow$ ideals in quadratic fields

leads to an isomorphism

$$\text{BQFs(d)} \,/\, \mathrm{SL}(2,\mathbb{Z}) \cong \mathrm{Cl}^+(\mathcal{O}_{K_d}) \cong \mathrm{Cl}(\mathcal{O}_{K_d})$$

for $d < 0$, where the group law on the left-hand side is Gauss' composition of quadratic forms. (For $d > 0$, the narrow and wide class groups are not isomorphic in general.)

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

The only values $d < 0$ with $\#\mathrm{Cl}(\mathcal{O}_{K_d}) = h(\mathcal{O}_{K_d}) = 1$, are

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

Binary quadratic forms $\leftrightsquigarrow$ ideals in quadratic fields

leads to an isomorphism

$$\text{BQFs(d)} \,/\, \text{SL}(2,\mathbb{Z}) \cong \text{Cl}^+(\mathcal{O}_{K_d}) \cong \text{Cl}(\mathcal{O}_{K_d})$$

for $d < 0$, where the group law on the left-hand side is Gauss' composition of quadratic forms. (For $d > 0$, the narrow and wide class groups are not isomorphic in general.)

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

The only values $d < 0$ with $\#\text{Cl}(\mathcal{O}_{K_d}) = h(\mathcal{O}_{K_d}) = 1$, are

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

Question

For what $d > 0$ do we have $h(\mathcal{O}_{K_d}) = 1$?

Binary quadratic forms $\leftrightsquigarrow$ ideals in quadratic fields

leads to an isomorphism

$$\text{BQFs(d)} \,/\, \text{SL}(2,\mathbb{Z}) \cong \text{Cl}^+(\mathcal{O}_{K_d}) \cong \text{Cl}(\mathcal{O}_{K_d})$$

for $d < 0$, where the group law on the left-hand side is Gauss' composition of quadratic forms. (For $d > 0$, the narrow and wide class groups are not isomorphic in general.)

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

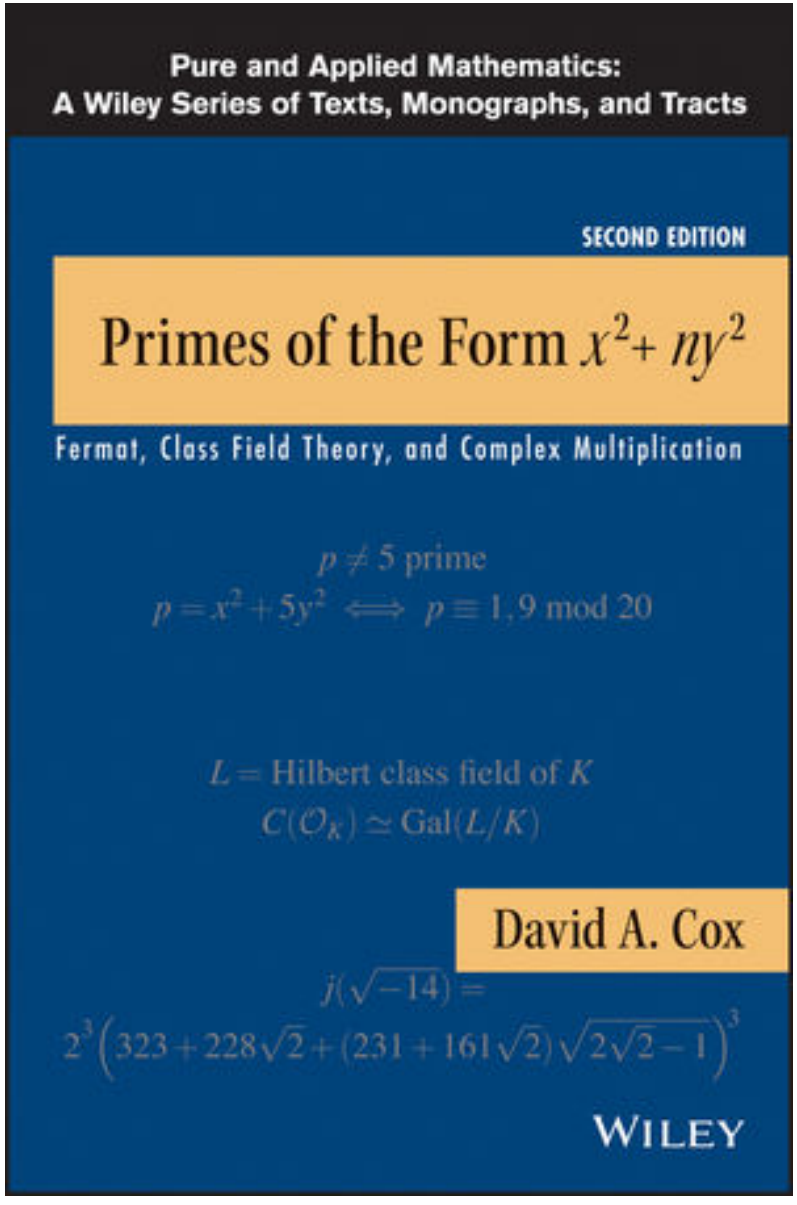
The only values $d < 0$ with $\#\text{Cl}(\mathcal{O}_{K_d}) = h(\mathcal{O}_{K_d}) = 1$, are

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

Question

For what $d > 0$ do we have $h(\mathcal{O}_{K_d}) = 1$?

Gauss' conjecture: there are infinitely many number fields with $h = 1$.



A full treatment of binary quadratic forms and ideal class groups (§1 through §3).

Ideal Class Groups

Ideal Class Groups

e.g., $\mathrm{Cl}(\mathbb{Q}(\sqrt{-5})) = \left\langle [\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}], [\mathcal{P}_2] \right\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Consider:

$$\mathcal{C} = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant } (d \equiv 0, 1 \bmod 4) \right\}.$$

Consider:

$$\mathcal{C} = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant } (d \equiv 0, 1 \bmod 4) \right\}.$$

Question

What finite abelian groups appear in $\mathcal{C}$?

Consider:

$$\mathcal{C} = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant } (d \equiv 0, 1 \bmod 4) \right\}.$$

Question

What finite abelian groups appear in $\mathcal{C}$?

Consider also:

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}.$$

Consider:

$$\mathcal{C} = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant } (d \equiv 0, 1 \bmod 4) \right\}.$$

Question

What finite abelian groups appear in $\mathcal{C}$?

Consider also:

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}.$$

Question

Is $\mathcal{C}(X)$ a "random" sequence of finite abelian groups?

Consider:

$$\mathcal{C} = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant } (d \equiv 0, 1 \bmod 4) \right\}.$$

Question

What finite abelian groups appear in $\mathcal{C}$?

Consider also:

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}.$$

Question

Is $\mathcal{C}(X)$ a "random" sequence of finite abelian groups?

Answer: NO. See genus theory.

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}.$$

Question

Is $\mathcal{C}(X)$ a "random" sequence of finite abelian groups?

Answer: NO. See genus theory.

The 2-part of the class group has a nice theory, called *genus theory* (see also Cox' "Primes of the form $x^2 + ny^2$".) In particular, if d is a fundamental discriminant, then

$$\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}$$

where r is the number of distinct prime divisors of d.

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}.$$

Question

Is $\mathcal{C}(X)$ a "random" sequence of finite abelian groups?

Answer: NO. See genus theory.

The 2-part of the class group has a nice theory, called *genus theory* (see also Cox' "Primes of the form $x^2 + ny^2$".) In particular, if d is a fundamental discriminant, then

$$\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2] \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}$$

where r is the number of distinct prime divisors of d.

Example

Let $d = -20$ (so that $r = 2$). Then, we have $\mathrm{Cl}(\mathbb{Q}(\sqrt{-20})) \cong \mathbb{Z}/2\mathbb{Z}$.

$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}$
is not random, but what about the odd part?

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}$$

is not random, but what about the odd part? Let

$$H_d = \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),\ H_{d,2} = \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$$

and $H_d^{\neq 2} = H_d / H_{d,2}$.

$$\mathcal{C}(X) = \left\{ \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}$$

is not random, but what about the odd part? Let

$$H_d = \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),\ H_{d,2} = \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$$

and $H_d^{\neq 2} = H_d / H_{d,2}$.

$$\mathcal{C}^{\neq 2}(X) = \left\{ H_d^{\neq 2} : d < 0 \text{ fundamental discriminant with } |d| \leq X \right\}.$$

Question

Is $\mathcal{C}^{\neq 2}(X)$ a "random" sequence of finite abelian groups?

Henri Cohen
1947–

Hendrik Lenstra
1949–

Conjecture (Cohen-Lenstra, 1984)

The sequence of groups $H_d^{\neq 2}$ ordered by $|d|$ behaves like a "random sequence of finite abelian groups of odd order".

Henri Cohen
1947–

Hendrik Lenstra
1949–

Conjecture (Cohen-Lenstra, 1984)

The sequence of groups $H_d^{\neq 2}$ ordered by $|d|$ behaves like a "random sequence of finite abelian groups of odd order".

What is a random finite abelian group?

Henri Cohen
1947–

Hendrik Lenstra
1949–

Conjecture (Cohen-Lenstra, 1984)

The sequence of groups $H_d^{\neq 2}$ ordered by $|d|$ behaves like a "random sequence of finite abelian groups of odd order".

What is a random finite abelian group? A group with random p-part...

Henri Cohen
1947–

Hendrik Lenstra
1949–

Conjecture (Cohen-Lenstra, 1984)

The sequence of groups $H_d^{\neq 2}$ ordered by $|d|$ behaves like a "random sequence of finite abelian groups of odd order".

What is a random finite abelian group? A group with random p-part...
What is a random finite abelian p-group?

Henri Cohen
1947–

Hendrik Lenstra
1949–

Conjecture (Cohen-Lenstra, 1984)

The sequence of groups $H_d^{\neq 2}$ ordered by $|d|$ behaves like a "random sequence of finite abelian groups of odd order".

What is a random finite abelian group? A group with random p-part...
What is a random finite abelian p-group?
What group is more likely: $\mathbb{Z}/p^3\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^3$, or $\mathbb{Z}/p\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^2$?

Conjecture (Cohen-Lenstra, 1984)

The sequence of groups $H_d^{\neq 2}$ ordered by $|d|$ behaves like a "random sequence of finite abelian groups of odd order".

Cohen-Lenstra: Let p be a prime. Assume that we have a "natural" unbiased stochastic process producing finite abelian p-groups. If we fix a finite abelian group G, then the probability that an output of the process is isomorphic to G is inversely proportional to the size of the automorphism group $\mathrm{Aut}(G)$.

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = \mathbb{Z}/p^3\mathbb{Z}$, so $k = 1$, $e_1 = 3$, $r_1 = 1$. Thus,

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\operatorname{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = \mathbb{Z}/p^3\mathbb{Z}$, so $k = 1$, $e_1 = 3$, $r_1 = 1$. Thus,

$$\#\operatorname{Aut}(\mathbb{Z}/p^3\mathbb{Z}) = (1 - p^{-1})(p^{3 \cdot 1 \cdot 1}) = (1 - 1/p)p^3 = (p-1)p^2.$$

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\operatorname{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = \mathbb{Z}/p^3\mathbb{Z}$, so $k = 1$, $e_1 = 3$, $r_1 = 1$. Thus,

$$\#\operatorname{Aut}(\mathbb{Z}/p^3\mathbb{Z}) = (1 - p^{-1})(p^{3 \cdot 1 \cdot 1}) = (1 - 1/p)p^3 = (p-1)p^2.$$

(Note: $\operatorname{Aut}(\mathbb{Z}/p^3\mathbb{Z}) \cong (\mathbb{Z}/p^3\mathbb{Z})^{\times}$.)

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = (\mathbb{Z}/p\mathbb{Z})^3$, so $k = 1$, $e_1 = 1$, $r_1 = 3$. Thus,

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = (\mathbb{Z}/p\mathbb{Z})^3$, so $k = 1$, $e_1 = 1$, $r_1 = 3$. Thus,

$$\begin{aligned} \#\,\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^3) &= (1 - p^{-1})(1 - p^{-2})(1 - p^{-3})p^{1 \cdot 3 \cdot 3} \\ &= (p - 1)(p^2 - 1)(p^3 - 1)p^3. \end{aligned}$$

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\operatorname{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = (\mathbb{Z}/p\mathbb{Z})^3$, so $k = 1$, $e_1 = 1$, $r_1 = 3$. Thus,

$$\begin{aligned} \#\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^3) &= (1 - p^{-1})(1 - p^{-2})(1 - p^{-3})p^{1 \cdot 3 \cdot 3} \\ &= (p - 1)(p^2 - 1)(p^3 - 1)p^3. \end{aligned}$$

(Note: $\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^3) \cong \mathrm{GL}(3, \mathbb{Z}/p\mathbb{Z})$.)

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\,\mathrm{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})$, so $k = 2$, $e_1 = 1$, $e_2 = 2$, $r_1 = 1$, $r_2 = 1$. Thus,

Theorem

Let $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$. Let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Then,

$$\#\operatorname{Aut}(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \cdot \left(\prod_{1 \leq i,j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

Example

Let $G = (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})$, so $k = 2$, $e_1 = 1$, $e_2 = 2$, $r_1 = 1$, $r_2 = 1$. Thus,

$$\begin{aligned} \#\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})) &= (1 - p^{-1})(1 - p^{-1}) p^{1 \cdot 1 \cdot 1} p^{1 \cdot 1 \cdot 1} p^{1 \cdot 1 \cdot 1} p^{2 \cdot 1 \cdot 1} \\ &= (p - 1)^2 p^3. \end{aligned}$$

Example

Let $p = 5$. Then:

$$\begin{aligned} \#\operatorname{Aut}(\mathbb{Z}/p^3\mathbb{Z}) &= (p-1)p^2 = 100 \\ \#\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^3) &= (p-1)(p^2-1)(p^3-1)p^3 = 1488000 \\ \#\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})) &= (p-1)^2p^3 = 2000. \end{aligned}$$

Cohen-Lenstra: Let p be a prime. Assume that we have a "natural" unbiased stochastic process producing finite abelian p-groups. If we fix a finite abelian group G, then the probability that an output of the process is isomorphic to G is inversely proportional to the size of the automorphism group $\mathrm{Aut}(G)$.

Cohen-Lenstra: Let p be a prime. Assume that we have a "natural" unbiased stochastic process producing finite abelian p-groups. If we fix a finite abelian group G, then the probability that an output of the process is isomorphic to G is inversely proportional to the size of the automorphism group $\mathrm{Aut}(G)$.

Formally: Let $\mathcal{G}_p$ be the set of all finite abelian p-groups. The Cohen-Lenstra weight ω is the measure on the set $\mathcal{G}_p$ such that

$$\omega(\{G\}) = 1/\#\,\mathrm{Aut}(G).$$

Cohen-Lenstra: Let p be a prime. Assume that we have a "natural" unbiased stochastic process producing finite abelian p-groups. If we fix a finite abelian group G, then the probability that an output of the process is isomorphic to G is inversely proportional to the size of the automorphism group $\mathrm{Aut}(G)$.

Formally: Let $\mathcal{G}_p$ be the set of all finite abelian p-groups. The Cohen-Lenstra weight ω is the measure on the set $\mathcal{G}_p$ such that

$$\omega(\{G\}) = 1/\#\,\mathrm{Aut}(G).$$

The (local) Cohen-Lenstra probability measure P is the probability measure on $\mathcal{G}_p$ that is obtained by scaling ω, i.e.:

$$P(M) = \omega(M)/\omega(\mathcal{G}_p) \quad \text{for} \quad M \subseteq \mathcal{G}_p.$$

Cohen-Lenstra: Let p be a prime. Assume that we have a "natural" unbiased stochastic process producing finite abelian p-groups. If we fix a finite abelian group G, then the probability that an output of the process is isomorphic to G is inversely proportional to the size of the automorphism group $\mathrm{Aut}(G)$.

Formally: Let $\mathcal{G}_p$ be the set of all finite abelian p-groups. The Cohen-Lenstra weight ω is the measure on the set $\mathcal{G}_p$ such that

$$\omega(\{G\}) = 1/\#\,\mathrm{Aut}(G).$$

The (local) Cohen-Lenstra probability measure P is the probability measure on $\mathcal{G}_p$ that is obtained by scaling ω, i.e.:

$$P(M) = \omega(M)/\omega(\mathcal{G}_p) \quad \text{for} \quad M \subseteq \mathcal{G}_p.$$

Theorem

$\omega(\mathcal{G}_p) = \prod_{i=1}^{\infty}(1 - p^{-i})^{-1}$.

Theorem

$\omega(\mathcal{G}_p) = \prod_{i=1}^{\infty}(1 - p^{-i})^{-1}$.

Example

Let $p = 5$.

Theorem

$\omega(\mathcal{G}_p) = \prod_{i=1}^{\infty}(1 - p^{-i})^{-1}$.

Example

Let $p = 5$. Then:

$$\omega(\mathcal{G}_5) = 1.315213\ldots$$

Theorem

$\omega(\mathcal{G}_p) = \prod_{i=1}^{\infty}(1-p^{-i})^{-1}$.

Example

Let $p = 5$. Then:

$$\omega(\mathcal{G}_5) = 1.315213\ldots$$

From before:

$$\begin{aligned} \#\,\mathrm{Aut}(\mathbb{Z}/p^3\mathbb{Z}) &= (p-1)p^2 = 100 \\ \#\,\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^3) &= (p-1)(p^2-1)(p^3-1)p^3 = 1488000 \\ \#\,\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})) &= (p-1)^2p^3 = 2000. \end{aligned}$$

Theorem

$\omega(\mathcal{G}_p) = \prod_{i=1}^{\infty}(1-p^{-i})^{-1}$.

Example

Let $p = 5$. Then:

$$\omega(\mathcal{G}_5) = 1.315213\ldots$$

From before:

$$\begin{aligned}
\#\,\mathrm{Aut}(\mathbb{Z}/p^3\mathbb{Z}) &= (p-1)p^2 = 100 \\
\#\,\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^3) &= (p-1)(p^2-1)(p^3-1)p^3 = 1488000 \\
\#\,\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})) &= (p-1)^2p^3 = 2000.
\end{aligned}$$

Therefore:

$$\begin{aligned}
P(\mathbb{Z}/p^3\mathbb{Z}) &= \frac{1/100}{1.315213\ldots} = 0.0076\ldots \text{ or } 0.76\% \\
P((\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})) &= \frac{1/2000}{1.315213\ldots} = 0.00038\ldots \text{ or } 0.038\%. \\
P((\mathbb{Z}/p\mathbb{Z})^3) &= \frac{1/1488000}{1.315213\ldots} = 0.0000005109\ldots \text{ or } 0.00005109\%.
\end{aligned}$$

WHY THIS MEASURE???

Question

Why would the Cohen-Lenstra measure be the correct measure?

Question

Why would the Cohen-Lenstra measure be the correct measure?

How do we expect random abelian p-groups to arise?

Question

Why would the Cohen-Lenstra measure be the correct measure?

How do we expect random abelian p-groups to arise? One way:

Question

Why would the Cohen-Lenstra measure be the correct measure?

How do we expect random abelian p-groups to arise? One way:

Pick random $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$, and let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

Question

Why would the Cohen-Lenstra measure be the correct measure?

How do we expect random abelian p-groups to arise? One way:

Pick random $k \geq 0$, $e_1 > \ldots > e_k > 0$, and $r_i > 0$ for $i = 1, \ldots, k$, and let

$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}.$$

This is **unnatural** because, for one thing, we would be assuming the structure theorem of finite abelian groups.

Instead, let us model random generators and relations.

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Choose r random relations $e_{1,i} g_1 + \cdots + e_{r,i} g_r = 0$, with $e_i \in \mathbb{Z}$.

In matrix form: $R = \begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,r} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ e_{r,1} & e_{r,2} & \cdots & e_{r,r} \end{pmatrix}$

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Choose r random relations $e_{1,i} g_1 + \cdots + e_{r,i} g_r = 0$, with $e_i \in \mathbb{Z}$.

In matrix form: $R = \begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,r} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ e_{r,1} & e_{r,2} & \cdots & e_{r,r} \end{pmatrix}$

Random group: $\mathbb{Z}^r / \mathrm{Col}(R)$.

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Choose r random relations $e_{1,i} g_1 + \cdots + e_{r,i} g_r = 0$, with $e_i \in \mathbb{Z}$.

In matrix form: $R = \begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,r} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ e_{r,1} & e_{r,2} & \cdots & e_{r,r} \end{pmatrix}$

Random group: $\mathbb{Z}^r / \mathrm{Col}(R)$. (But this is not a p-group.)

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Choose r random relations $e_{1,i} g_1 + \cdots + e_{r,i} g_r = 0$, with $e_i \in \mathbb{Z}$.

In matrix form: $R = \begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,r} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ e_{r,1} & e_{r,2} & \cdots & e_{r,r} \end{pmatrix}$

Random group: $\mathbb{Z}^r / \operatorname{Col}(R)$. (But this is not a p-group.)

Instead, random group: $\mathbb{Z}_p^r / \operatorname{Col}(R)$.

$$0 \longrightarrow \operatorname{Ker} R \longrightarrow \mathbb{Z}_p^r \longrightarrow \mathbb{Z}_p^r \longrightarrow \operatorname{Coker} R \cong \mathbb{Z}_p^r / \operatorname{Col}(R) \longrightarrow 0.$$

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Choose r random relations $e_{1,i} g_1 + \cdots + e_{r,i} g_r = 0$, with $e_i \in \mathbb{Z}$.

In matrix form: $R = \begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,r} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ e_{r,1} & e_{r,2} & \cdots & e_{r,r} \end{pmatrix}$

Random group: $\mathbb{Z}^r / \operatorname{Col}(R)$. (But this is not a p-group.)

Instead, random group: $\mathbb{Z}_p^r / \operatorname{Col}(R)$.

$$0 \longrightarrow \operatorname{Ker} R \longrightarrow \mathbb{Z}_p^r \longrightarrow \mathbb{Z}_p^r \longrightarrow \operatorname{Coker} R \cong \mathbb{Z}_p^r / \operatorname{Col}(R) \longrightarrow 0.$$

So we have a correspondence

finite abelian p-groups $\leftrightsquigarrow$ **matrices in $\mathbb{Z}_p^{r \times r}$ with full rank** .

Start with $r \geq 1$ generators $\mathbb{Z}^r = \langle g_1, \ldots, g_r \rangle$.

Choose r random relations $e_{1,i} g_1 + \cdots + e_{r,i} g_r = 0$, with $e_i \in \mathbb{Z}$.

In matrix form: $R = \begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,r} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ e_{r,1} & e_{r,2} & \cdots & e_{r,r} \end{pmatrix}$

Random group: $\mathbb{Z}^r / \operatorname{Col}(R)$. (But this is not a p-group.)

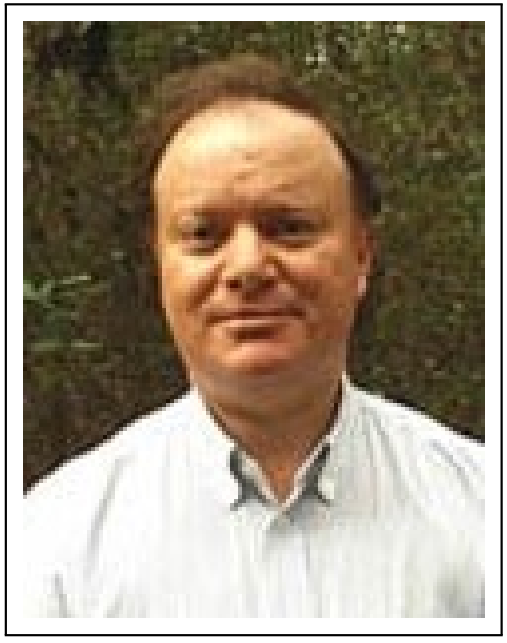
Instead, random group: $\mathbb{Z}_p^r / \operatorname{Col}(R)$.

$$0 \longrightarrow \operatorname{Ker} R \longrightarrow \mathbb{Z}_p^r \longrightarrow \mathbb{Z}_p^r \longrightarrow \operatorname{Coker} R \cong \mathbb{Z}_p^r / \operatorname{Col}(R) \longrightarrow 0.$$

So we have a correspondence

finite abelian p-groups $\leftrightsquigarrow$ **matrices in $\mathbb{Z}_p^{r \times r}$ with full rank** .

Moreover, $\mathbb{Z}_p$ is compact, it has a Haar measure (normalized to have total volume 1), and so $\mathbb{Z}_p^{r \times r}$ inherits a Haar measure from $\mathbb{Z}_p$.

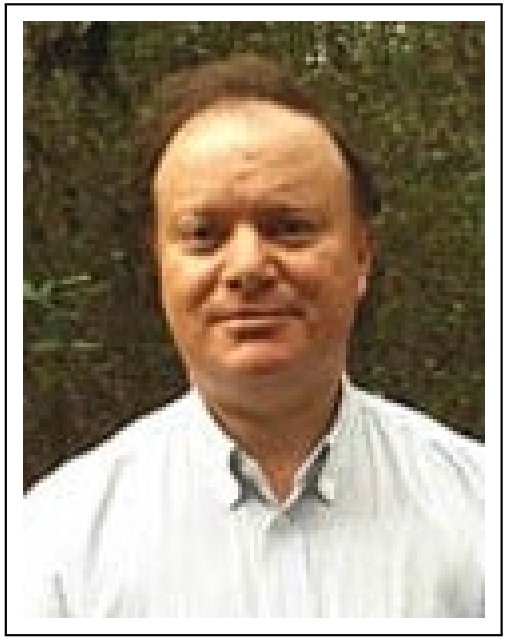


Eduardo Friedman

Lawrence Washington

Theorem (Friedman, Washington, 1987)

For a randomly chosen matrix $R \in \mathbb{Z}_p^{r \times r}$ w.r.t. the Haar measure,



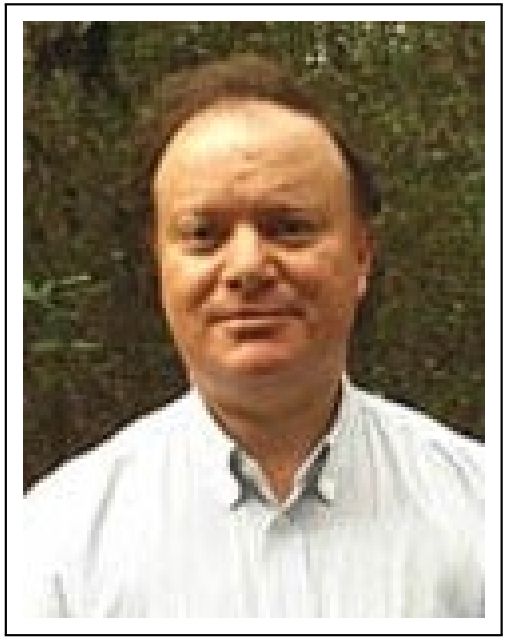
Eduardo Friedman

Lawrence Washington

Theorem (Friedman, Washington, 1987)

For a randomly chosen matrix $R \in \mathbb{Z}_p^{r \times r}$ w.r.t. the Haar measure,

1. $P(R \text{ has full rank}) = 1$ *for all* $r > 0$.



Eduardo Friedman

Lawrence Washington

Theorem (Friedman, Washington, 1987)

For a randomly chosen matrix $R \in \mathbb{Z}_p^{r\times r}$ w.r.t. the Haar measure,

1. $P(R \text{ has full rank }) = 1$ *for all* $r > 0$.
2. *For any finite abelian p-group G we have*

$$P(\mathrm{Coker}(R) \cong G) \longrightarrow P(G)$$

as $r \to \infty$, *where P is the* **Cohen-Lenstra probability measure**.

The idea of using $\#\,\mathrm{Aut}$ as a weight also appears in other contexts: lattices, quadratic forms, elliptic curves, etc.

The idea of using $\#\mathrm{Aut}$ as a weight also appears in other contexts: lattices, quadratic forms, elliptic curves, etc.

For quadratic fields, there is extensive data (with hundreds of millions of class groups) to support the Cohen-Lenstra heuristics. See Stephens and Williams [Stephens and Williams 88]; Jacobson, Lukes, and Williams [Jacobson et al. 95]; and Jacobson [Jacobson 98].

How about **real quadratic fields**? The Cohen-Lenstra heuristics for a real quadratic field $\mathbb{Q}(\sqrt{d})$ suggests the following:

Let $k \geq 1$ be an odd number. Then, the probability that the odd part of $h(\mathbb{Q}(\sqrt{d}))$, denoted by $h^*(\mathbb{Q}(\sqrt{d}))$, equals k is given by

$$P(h^*(\mathbb{Q}(\sqrt{d})) = k) = \frac{C \cdot \lambda(k)}{k}$$

where $C = 0.754458173\ldots$, and

$$\lambda(k)^{-1} = \prod_{p^\alpha || k} p^\alpha (1 - p^{-1})(1 - p^{-2}) \cdots (1 - p^{-\alpha}).$$

How about **real quadratic fields**? The Cohen-Lenstra heuristics for a real quadratic field $\mathbb{Q}(\sqrt{d})$ suggests the following:

Let $k \geq 1$ be an odd number. Then, the probability that the odd part of $h(\mathbb{Q}(\sqrt{d}))$, denoted by $h^*(\mathbb{Q}(\sqrt{d}))$, equals k is given by

$$P(h^*(\mathbb{Q}(\sqrt{d})) = k) = \frac{C \cdot \lambda(k)}{k}$$

where $C = 0.754458173\ldots$, and

$$\lambda(k)^{-1} = \prod_{p^\alpha || k} p^\alpha (1 - p^{-1})(1 - p^{-2}) \cdots (1 - p^{-\alpha}).$$

So, in particular, this implies

$$P(h^*(\mathbb{Q}(\sqrt{d})) = 1) = C = 0.754458173\ldots$$

How about **real quadratic fields**? The Cohen-Lenstra heuristics for a real quadratic field $\mathbb{Q}(\sqrt{d})$ suggests the following:

Let $k \geq 1$ be an odd number. Then, the probability that the odd part of $h(\mathbb{Q}(\sqrt{d}))$, denoted by $h^*(\mathbb{Q}(\sqrt{d}))$, equals k is given by

$$P(h^*(\mathbb{Q}(\sqrt{d})) = k) = \frac{C \cdot \lambda(k)}{k}$$

where $C = 0.754458173\ldots$, and

$$\lambda(k)^{-1} = \prod_{p^\alpha || k} p^\alpha (1 - p^{-1})(1 - p^{-2}) \cdots (1 - p^{-\alpha}).$$

So, in particular, this implies

$$P(h^*(\mathbb{Q}(\sqrt{d})) = 1) = C = 0.754458173\ldots$$

If we assume that the subfamily $\mathbb{Q}(\sqrt{p})$, over primes p, behaves similarly, then $h^* = h$, and

$$P(h(\mathbb{Q}(\sqrt{p})) = 1) = C = 0.754458173\ldots.$$

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*.