From Picard groups of hyperelliptic curves to class groups of quadratic fields

Jean Gillibert

International Conference on Class Groups of Number Fields and Related Topics, HRI, Allahabad
October 11, 2018

Elliptic curves over $\mathbb{Q}$

An **elliptic curve** E over a $\mathbb{Q}$ is a non-singular (or smooth) projective curve defined by an equation of the form

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{Q}$$

This is called a **Weierstrass equation**.

Elliptic curves over $\mathbb{Q}$

An **elliptic curve** E over a $\mathbb{Q}$ is a non-singular (or smooth) projective curve defined by an equation of the form

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{Q}$$

This is called a **Weierstrass equation**.

One defines the **discriminant** of E as being the quantity

$$\Delta := -16 \cdot (4a^3 + 27b^2)$$

Elliptic curves over $\mathbb{Q}$

An **elliptic curve** E over a $\mathbb{Q}$ is a non-singular (or smooth) projective curve defined by an equation of the form

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{Q}$$

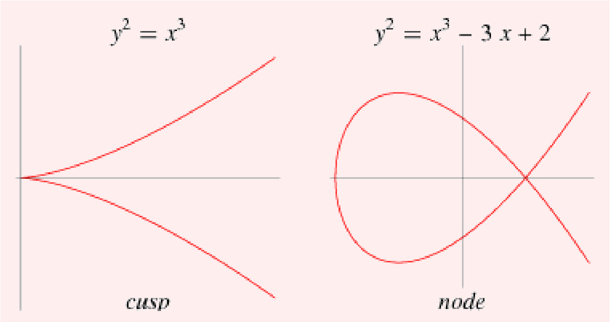
This is called a **Weierstrass equation**.

One defines the **discriminant** of E as being the quantity

$$\Delta := -16 \cdot (4a^3 + 27b^2)$$

Classical fact:

$$E \text{ is non-singular} \iff x^3 + ax + b \;\text{ has no double root} \\ \iff \Delta \neq 0$$


$y^2 = x^3$
$y^2 = x^3 - 3x + 2$
cusp
node

Why are elliptic curves important?

Short answer: they have a group law, which turns them into an algebraic group

Why are elliptic curves important?

Short answer: they have a group law, which turns them into an algebraic group

Detailed answer: there are exactly three types of algebraic groups of dimension one

- $\mathbb{A}^1$ with addition: $\mathbb{G}_a$
- $\mathbb{A}^1 \setminus \{0\}$ with multiplication: $\mathbb{G}_m$
- Elliptic curves

Remark: this classification is over an algebraically closed field. Over an arbitrary field, one has also quadratic twists of $\mathbb{G}_m$

Why are elliptic curves arithmetically important?

Mordell-Weil Theorem (Mordell, 1922): $E(\mathbb{Q})$ is a finitely generated abelian group:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

The integer r is called the rank of $E(\mathbb{Q})$, denoted by $\text{rk}_{\mathbb{Z}} E(\mathbb{Q})$

Why are elliptic curves arithmetically important?

Mordell-Weil Theorem (Mordell, 1922): $E(\mathbb{Q})$ is a finitely generated abelian group:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

The integer r is called the rank of $E(\mathbb{Q})$, denoted by $\text{rk}_{\mathbb{Z}} E(\mathbb{Q})$

Recent heuristics by Bhargava, Kane, Lenstra, Park, Poonen, Rains, Voight, and Wood:

When E runs through all elliptic curves over $\mathbb{Q}$, $\text{rk}_{\mathbb{Z}} E(\mathbb{Q})$ should be bounded by 21, except for finitely many "exceptional" cases!

Why are elliptic curves arithmetically important?

Mordell-Weil Theorem (Mordell, 1922): $E(\mathbb{Q})$ is a finitely generated abelian group:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

The integer r is called the rank of $E(\mathbb{Q})$, denoted by $\text{rk}_{\mathbb{Z}} E(\mathbb{Q})$

Recent heuristics by Bhargava, Kane, Lenstra, Park, Poonen, Rains, Voight, and Wood:

When E runs through all elliptic curves over $\mathbb{Q}$, $\text{rk}_{\mathbb{Z}} E(\mathbb{Q})$ should be bounded by 21, except for finitely many "exceptional" cases!

In particular, $\text{rk}_{\mathbb{Z}} E(\mathbb{Q})$ should be bounded...

Reduction of elliptic curves

By change of variables, we may find a Weierstrass equation for E whose coefficients are integers:

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{Z}$$

Given a prime number p, we say that E has **good reduction** at p if one can find an integral Weierstrass equation such that

$$\Delta \not\equiv 0 \pmod{p}$$

In other terms, the reduction modulo p of the equation is an elliptic curve over $\mathbb{F}_p$.

Reduction of elliptic curves

By change of variables, we may find a Weierstrass equation for E whose coefficients are integers:

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{Z}$$

Given a prime number p, we say that E has **good reduction** at p if one can find an integral Weierstrass equation such that

$$\Delta \not\equiv 0 \pmod{p}$$

In other terms, the reduction modulo p of the equation is an elliptic curve over $\mathbb{F}_p$.

Remark: if $p = 2$ or 3 one has to use a more general Weierstrass equation. This explains the -16 in the definition of Δ.

Basic facts on reduction

Bad primes are the divisors of Δ, so there are finitely many.

Fact: An elliptic curve over $\mathbb{Q}$ always has at least one bad place!

So, whenever one considers the arithmetic of elliptic curves over $\mathbb{Q}$, one has to handle bad places at some point.

Basic facts on reduction

Bad primes are the divisors of Δ, so there are finitely many.

Fact: An elliptic curve over $\mathbb{Q}$ always has at least one bad place!

So, whenever one considers the arithmetic of elliptic curves over $\mathbb{Q}$, one has to handle bad places at some point.

Related fact: there does not exist everywhere unramified extensions of $\mathbb{Q}$.

Basic facts on reduction

Bad primes are the divisors of Δ, so there are finitely many.

Fact: An elliptic curve over $\mathbb{Q}$ always has at least one bad place!

So, whenever one considers the arithmetic of elliptic curves over $\mathbb{Q}$, one has to handle bad places at some point.

Related fact: there does not exist everywhere unramified extensions of $\mathbb{Q}$.

Remark: if one replaces $\mathbb{Q}$ by an arbitrary number field, then the situation changes for both objects.

Good reduction points

Given $P \in E(\mathbb{Q})$, say that P has **everywhere good reduction** if, for all primes p, the reduction of P mod p is not a singular point on the reduction of E mod p.

Denote by $E^0(\mathbb{Q})$ the set of points with everywhere good reduction.

Good reduction points

Given $P \in E(\mathbb{Q})$, say that P has **everywhere good reduction** if, for all primes p, the reduction of P mod p is not a singular point on the reduction of E mod p.

Denote by $E^0(\mathbb{Q})$ the set of points with everywhere good reduction.

Theorem: $E^0(\mathbb{Q})$ is a subgroup of finite index in $E(\mathbb{Q})$, hence

$$\mathrm{rk}_{\mathbb{Z}} E^0(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}).$$

In practive, given a point $P \in E(\mathbb{Q})$, there exists some multiple of P which belongs to $E^0(\mathbb{Q})$.

From elliptic curves to class groups

Mazur-Tate's class group pairing: let K be a number field. Then we have a bilinear map of abelian groups

$$\begin{aligned} E^0(\mathbb{Q}) \times E(K) &\longrightarrow \mathrm{Cl}(K) \\ (P, Q) &\longmapsto \langle P, Q \rangle^{\mathrm{cl}} \end{aligned}$$

Barry Mazur and John Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983

Definition of the class group pairing

A point $P \in E(\mathbb{Q})$ gives rise to a degree zero line bundle L_P on E. If P belongs to E^0, then L_P entends (uniquely) into a line bundle $\mathcal{L}_P$ on the minimal regular model $\mathcal{X} \to \mathrm{Spec}(\mathbb{Z})$ of E.

Definition of the class group pairing

A point $P \in E(\mathbb{Q})$ gives rise to a degree zero line bundle L_P on E. If P belongs to E^0, then L_P entends (uniquely) into a line bundle $\mathcal{L}_P$ on the minimal regular model $\mathcal{X} \to \mathrm{Spec}(\mathbb{Z})$ of E.

On the other hand, a point $Q \in E(K)$ gives rise to an integral section $Q : \mathrm{Spec}(\mathcal{O}_K) \to \mathcal{X}$, and we let

$$\langle P, Q \rangle^{\mathrm{cl}} := Q^* \mathcal{L}_P$$

which belongs to $\mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K)) = \mathrm{Cl}(K)$.

Relation with work of Buell

Mazur and Tate make the following remark: using the language of quadratic forms, a map $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ has been constructed by Buell in 1977.

Relation with work of Buell

Mazur and Tate make the following remark: using the language of quadratic forms, a map $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ has been constructed by Buell in 1977.

This map should be $\langle -, Q\rangle^{\mathrm{cl}}$ for some specific point $Q \in E(K)$.

Relation with work of Buell

Mazur and Tate make the following remark: using the language of quadratic forms, a map $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ has been constructed by Buell in 1977.

This map should be $\langle -, Q\rangle^{\mathrm{cl}}$ for some specific point $Q \in E(K)$.

This was proved later by Call in his PhD thesis (1986).

More recently, a new proof of this result appeared in

Duncan Buell and Gregory Call, *Class pairings and isogenies on elliptic curves*, J. Number Theory **167** (2016).

Which classes can be built from one given curve?

Given $Q \in E(K)$, the class group pairing induces a group morphism

$$\langle -, Q \rangle^{\mathrm{cl}} : E^0(\mathbb{Q}) \longrightarrow \mathrm{Cl}(K)$$

Question: given a field K, is it possible to find a curve E and a point $Q \in E(K)$ such that $\langle -, Q \rangle^{\mathrm{cl}}$ is surjective?

Which classes can be built from one given curve?

Given $Q \in E(K)$, the class group pairing induces a group morphism

$$\langle -, Q \rangle^{\mathrm{cl}} : E^0(\mathbb{Q}) \longrightarrow \mathrm{Cl}(K)$$

Question: given a field K, is it possible to find a curve E and a point $Q \in E(K)$ such that $\langle -, Q \rangle^{\mathrm{cl}}$ is surjective?

Remark: if $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ is surjective, then

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) &\geq \dim_2 \mathrm{Cl}(K)[2] - \dim_2 E^0(\mathbb{Q})_{\mathrm{tors}} \\ &\geq \dim_2 \mathrm{Cl}(K)[2] - 2. \end{aligned}$$

Which classes can be built from one given curve?

Given $Q \in E(K)$, the class group pairing induces a group morphism

$$\langle -, Q \rangle^{\mathrm{cl}} : E^0(\mathbb{Q}) \longrightarrow \mathrm{Cl}(K)$$

Question: given a field K, is it possible to find a curve E and a point $Q \in E(K)$ such that $\langle -, Q \rangle^{\mathrm{cl}}$ is surjective?

Remark: if $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ is surjective, then

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) &\geq \dim_2 \mathrm{Cl}(K)[2] - \dim_2 E^0(\mathbb{Q})_{\mathrm{tors}} \\ &\geq \dim_2 \mathrm{Cl}(K)[2] - 2. \end{aligned}$$

There exist quadratic fields K for which $\dim_2 \mathrm{Cl}(K)[2]$ is arbitrarily large. So the surjectivity implies the existence of elliptic curves over $\mathbb{Q}$ whose rank is arbitrarily large.

Which classes can be built from one given curve?

Given $Q \in E(K)$, the class group pairing induces a group morphism

$$\langle -, Q \rangle^{\mathrm{cl}} : E^0(\mathbb{Q}) \longrightarrow \mathrm{Cl}(K)$$

Question: given a field K, is it possible to find a curve E and a point $Q \in E(K)$ such that $\langle -, Q \rangle^{\mathrm{cl}}$ is surjective?

Remark: if $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ is surjective, then

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) &\geq \dim_2 \mathrm{Cl}(K)[2] - \dim_2 E^0(\mathbb{Q})_{\mathrm{tors}} \\ &\geq \dim_2 \mathrm{Cl}(K)[2] - 2. \end{aligned}$$

There exist quadratic fields K for which $\dim_2 \mathrm{Cl}(K)[2]$ is arbitrarily large. So the surjectivity implies the existence of elliptic curves over $\mathbb{Q}$ whose rank is arbitrarily large. Not likely!

Question: is the pairing non-degenerate?

Question: More precisely, given $P \in E^0(\mathbb{Q})$, does there exist some field K and some $Q \in E(K)$ such that

$$\langle P, Q \rangle^{\mathrm{cl}} \neq 0 \text{ ?}$$

This question was asked (in a more general setting) by Agboola and Pappas in 2000.

Question: is the pairing non-degenerate?

Question: More precisely, given $P \in E^0(\mathbb{Q})$, does there exist some field K and some $Q \in E(K)$ such that

$$\langle P, Q \rangle^{\mathrm{cl}} \neq 0 \ ?$$

This question was asked (in a more general setting) by Agboola and Pappas in 2000.

Theorem (G.–Levin, 2012): Yes if P is a torsion point.
More precisely, one can find infinitely many Q defined over imaginary quadratic fields K such that the map $\langle -, Q \rangle^{\mathrm{cl}}$ is injective on $E^0(\mathbb{Q})_{\mathrm{tors}}$

In fact, our result holds for “imaginary” hyperelliptic curves over $\mathbb{Q}$, *i.e.* curves defined by equations of the form

$$y^2 = f(x)$$

where $f \in \mathbb{Q}[x]$ is a monic square-free polynomial of odd degree.

Ingredients of our proof: Kummer theory and Hilbert’s irreducibility theorem.

For points of infinite order, we need another strategy!

ICCGNFRT 2017

Debopam Chakraborty gave a talk in which he explicitely constructs ideal classes of order 2 over biquadratic fields from points on elliptic curves (joint work with Anupam Saikia).

Then he mentions a paper by Ragnar Soleng according to which one can build from points of infinite order ideal classes whose order is arbitrarily large!

I immediately looked for a copy of Soleng's paper.

Ragnar Soleng, *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*, J. Number Theory **46** (1994).

Soleng's result

Without refering to previous constructions, Soleng defines a family of maps $E^0(\mathbb{Q}) \to \mathrm{Cl}(K)$ using the language of quadratic forms.

His construction is the same than Buell's one, so according to Call his maps are $\langle -, Q\rangle^{\mathrm{cl}}$ for some Q.

Theorem (Soleng, 1994): Let E be an elliptic curve over $\mathbb{Q}$, and let $P \in E^0(\mathbb{Q})$ be a point of infinite order. Then there exists a sequence $(Q_n)_{n\in\mathbb{N}}$ of points defined over quadratic imaginary fields such that the order of $\langle P, Q_n\rangle^{\mathrm{cl}}$ is unbounded when $n \to \infty$.

The proof is less than one page long!

Soleng's setting

Consider an integral Weierstrass equation of E

$$y^2 = f(x) \qquad f \in \mathbb{Z}[x], \text{ monic of degree 3.}$$

Any rational point $P \in E(\mathbb{Q}) \setminus \{0\}$ can be written as

$$P = \left(\frac{A}{e^2}, \frac{B}{e^3} \right)$$

with A, B, e in $\mathbb{Z}$ such that

$$\gcd(A, e) = \gcd(B, e) = 1.$$

Remark: If P belongs to $E^0(\mathbb{Q})$, then $\gcd(A, 2B, e) = 1$.

Soleng's definition of the map

Fix $n \in \mathbb{Z}$, and let $Q_n := (n, \sqrt{f(n)})$. If $f(n)$ is not a square, then Q_n is a quadratic point on E.

Soleng's construction

$$P = \left(\frac{A}{e^2}, \frac{B}{e^3}\right) \rightsquigarrow F_n := \left[(ne^2 - A), 2kB, \frac{k^2B^2 - f(n)}{ne^2 - A}\right]$$

where k is some integer such that $ke^3 \equiv 1 \pmod{ne^2 - A}$.

This binary quadratic form F_n has discriminant $4f(n)$.

The condition $\gcd(A, 2B, e) = 1$ implies that F_n is primitive, hence defines a class $\mathrm{cl}(F_n)$ in $\mathrm{Cl}(\mathbb{Z}[\sqrt{f(n)}])$.

Soleng's proof

$\langle P, Q_n\rangle^{\mathrm{cl}}$ is the image of $\mathrm{cl}(F_n)$ by the natural map

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{f(n)}]) \longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{f(n)}))$$

Assume $f(n)$ is squarefree, and < -3. Then the kernel of this map has order ≤ 3.

Soleng's proof

$\langle P, Q_n \rangle^{\mathrm{cl}}$ is the image of $\mathrm{cl}(F_n)$ by the natural map

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{f(n)}]) \longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{f(n)}))$$

Assume $f(n)$ is squarefree, and < -3. Then the kernel of this map has order ≤ 3.

Theorem (Hooley, 1967): there exist infinitely many values of n such that $f(n)$ is square-free.

So it suffices to prove the result for the map

$$E^0(\mathbb{Q}) \to \mathrm{Cl}(\mathbb{Z}[\sqrt{f(n)}]);\, P \mapsto \mathrm{cl}(F_n)$$

Soleng's proof, continued

Lemma: When $n \to -\infty$, the form F_n is not equivalent to the identity form $[1, 0, -f(n)]$.

Soleng's proof, continued

Lemma: When $n \to -\infty$, the form F_n is not equivalent to the identity form $[1, 0, -f(n)]$.

The proof is based on the following idea: if two binary quadratic forms over $\mathbb{Z}$ have small coefficients in X^2 compared to their (negative) discriminant, then they are not equivalent.

Soleng's proof, continued

Lemma: When $n \to -\infty$, the form F_n is not equivalent to the identity form $[1, 0, -f(n)]$.

The proof is based on the following idea: if two binary quadratic forms over $\mathbb{Z}$ have small coefficients in X^2 compared to their (negative) discriminant, then they are not equivalent.

$$F_n := \left[(ne^2 - A), 2kB, \frac{k^2B^2 - f(n)}{ne^2 - A}\right]$$

When $n \to -\infty$, $ne^2 - A$ (linear in n) is small compared to the discriminant $4f(n)$ (cubic in n). $\square$

The hyperelliptic case

It is tempting to generalize Soleng's proof when replacing f by a monic, square-free polynomial of odd degree.

This means that we are considering the imaginary hyperelliptic curve C defined by

$$y^2 = f(x)$$

The genus of C is $g(C) := (\deg(f) - 1)/2$.

Hooley's result cannot be extended to arbitrary degrees, so we make the following assumption:

Hypothesis: f is the product of polynomials of degree ≤ 3.

Line bundles on hyperelliptic curves

We replace the elliptic curve E by the Jacobian variety J of C, which is an abelian variety over $\mathbb{Q}$.

Points on J are degree zero divisor classes, or line bundles, on C.

We have a subgroup $J^0(\mathbb{Q}) \subset J(\mathbb{Q})$ consisting of points with everywhere good reduction, and a class group pairing

$$J^0(\mathbb{Q}) \times C(K) \longrightarrow \mathrm{Cl}(K)$$

Question: is there an explicit description of $J(\mathbb{Q})$?

Mumford's representation

Every element in $J(\mathbb{Q}) = \mathrm{Pic}^0(C)$ can be uniquely represented by a quadratic form $[u, 2v, w]$ over $\mathbb{Q}[x]$, with discriminant $4f$, where:

(1) u is monic;

(2) $\deg v < \deg u \leq g(C)$.

In this correspondence, the quadratic form $F = [u, 2v, w]$ corresponds to the divisor

$$D_F := \mathrm{div}(u) \cap \mathrm{div}(y - v) = \sum_{i=1}^{r} P_i - r \cdot \infty$$

where $P_i = (x_i, y_i)$, the x_i are the roots of u, and $v(x_i) = y_i$.

Mumford's representation

Every element in $J(\mathbb{Q}) = \mathrm{Pic}^0(C)$ can be uniquely represented by a quadratic form $[u, 2v, w]$ over $\mathbb{Q}[x]$, with discriminant $4f$, where:

(1) u is monic;

(2) $\deg v < \deg u \leq g(C)$.

In this correspondence, the quadratic form $F = [u, 2v, w]$ corresponds to the divisor

$$D_F := \mathrm{div}(u) \cap \mathrm{div}(y - v) = \sum_{i=1}^{r} P_i - r \cdot \infty$$

where $P_i = (x_i, y_i)$, the x_i are the roots of u, and $v(x_i) = y_i$.

People doing cryptography with hyperelliptic curves over finite fields use this all the time, refeering to Cantor's paper!

Elliptic curve case

A point $P \in E(\mathbb{Q})$ is represented by a quadratic form over $\mathbb{Q}[x]$.

Which one?

Elliptic curve case

A point $P \in E(\mathbb{Q})$ is represented by a quadratic form over $\mathbb{Q}[x]$.

Which one?

$$P = \left(\frac{A}{e^2}, \frac{B}{e^3}\right) \rightsquigarrow F := \left[x - \frac{A}{e^2}, 2\frac{B}{e^3}, \frac{\left(\frac{B}{e^3}\right)^2 - f(x)}{x - \frac{A}{e^2}}\right]$$

Elliptic curve case

A point $P \in E(\mathbb{Q})$ is represented by a quadratic form over $\mathbb{Q}[x]$.

Which one?

$$P = \left(\frac{A}{e^2}, \frac{B}{e^3}\right) \rightsquigarrow F := \left[x - \frac{A}{e^2}, 2\frac{B}{e^3}, \frac{\left(\frac{B}{e^3}\right)^2 - f(x)}{x - \frac{A}{e^2}}\right]$$

Compare this to Soleng's construction:

$$P \rightsquigarrow F_n := \left[(ne^2 - A), 2kB, \frac{k^2B^2 - f(n)}{ne^2 - A}\right]$$

where k is the inverse of e^3 modulo $(ne^2 - A)$.

Conclusion

By chasing denominators, q.f. over $\mathbb{Q}[x] \rightsquigarrow$ q.f. over $\mathbb{Z}[x]$.

A natural generalization of Soleng's construction is to consider the specialization map

$$\begin{aligned} \{\text{q.f. over } \mathbb{Z}[x] \text{ with disc. } 4f\} &\longrightarrow \{\text{q.f. over } \mathbb{Z} \text{ with disc. } 4f(n)\} \\ [u, 2v, w] &\longmapsto [u(n), 2v(n), w(n)] \end{aligned}$$

This map is just $L_P \mapsto Q_n^* L_P$ (specialisation on line bundles along the section Q_n).

One recovers Mazur-Tate's definition of the class group pairing.

At the same time, one obtains a new proof of the fact that Soleng's and Buell's constructions coincide with the class group pairing.

Classical analogy

algebraic geometry	number theory
curve $C/\mathbb{Q}$	number field $K/\mathbb{Q}$
with $\phi : C \to \mathbb{P}^1$ of degree 2	with $[K : \mathbb{Q}] = 2$
Jacobian $J(C) := \mathrm{Pic}^0(C)$	Class group $\mathrm{Cl}(K)$

Classical analogy

algebraic geometry	number theory
curve $C/\mathbb{Q}$	number field $K/\mathbb{Q}$
with $\phi : C \to \mathbb{P}^1$ of degree 2	with $[K : \mathbb{Q}] = 2$
Jacobian $J(C) := \mathrm{Pic}^0(C)$	Class group $\mathrm{Cl}(K)$
quadratic form over $\mathbb{P}^1$	quadratic form over $\mathbb{Z}$

Classical analogy

algebraic geometry	number theory
curve $C/\mathbb{Q}$	number field $K/\mathbb{Q}$
with $\phi : C \to \mathbb{P}^1$ of degree 2	with $[K : \mathbb{Q}] = 2$
Jacobian $J(C) := \mathrm{Pic}^0(C)$	Class group $\mathrm{Cl}(K)$
quadratic form over $\mathbb{P}^1$	quadratic form over $\mathbb{Z}$

Melanie Wood, 2011: generalisation to arbitrary double covers of schemes! This involves *sheaves* of quadratic forms.

Further directions

Further directions

- Replace $\mathbb{Q}$ by an arbitrary number field K;

Further directions

- Replace $\mathbb{Q}$ by an arbitrary number field K;
- Replace the hyperelliptic curve C by a **trigonal** curve

$$C \to \mathbb{P}^1 \qquad \text{of degree } 3$$

The work of Bhargava on *higher composition laws* allows to represent divisor classes on C by binary **cubic** forms.

Thank you for your attention!