Torsion and exceptional units

Dino Lorenzini

University of Georgia

December 2024

Plan of the talk

Plan of the talk

Basic objects and basic questions.

Plan of the talk

Basic objects and basic questions.

Elliptic curves over number fields. Birch and Swinnerton-Dyer conjecture and Tamagawa numbers.

Plan of the talk

Basic objects and basic questions.

Elliptic curves over number fields. Birch and Swinnerton-Dyer conjecture and Tamagawa numbers.

Results and Conjectures

Plan of the talk

Basic objects and basic questions.

Elliptic curves over number fields. Birch and Swinnerton-Dyer conjecture and Tamagawa numbers.

Results and Conjectures

Exceptional units and Lenstra constant

Plan of the talk

Basic objects and basic questions.

Elliptic curves over number fields. Birch and Swinnerton-Dyer conjecture and Tamagawa numbers.

Results and Conjectures

Exceptional units and Lenstra constant

Abelian surfaces over $\mathbb{Q}$.

Curves and Fields

Let K be any field (in this talk, mostly $\mathbb{Q}$ or a number field).

Curves and Fields

Let K be any field (in this talk, mostly $\mathbb{Q}$ or a number field).

Let L/K be any finite field extension, of degree d.

Curves and Fields

Let K be any field (in this talk, mostly $\mathbb{Q}$ or a number field).

Let L/K be any finite field extension, of degree d.

Let X/K be a curve, of genus g.

Let $X(L) :=$ set of L-rational points.

Curves and Fields

Let K be any field (in this talk, mostly $\mathbb{Q}$ or a number field).

Let L/K be any finite field extension, of degree d.

Let X/K be a curve, of genus g.

Let $X(L) :=$ set of L-rational points.

If X is a plane projective curve defined by a homogeneous polynomial $F(x, y, z) \in K[x, y, z]$ of degree D, then

$$X(L) = \{(a : b : c) \in \mathbb{P}^2(L) \mid F(a, b, c) = 0\}$$

The genus of X/K is bounded by $(D-1)(D-2)/2$, with equality if X is smooth.

Curves and Fields

Let K be any field (in this talk, mostly $\mathbb{Q}$ or a number field).

Let L/K be any finite field extension, of degree d.

Let X/K be a curve, of genus g.

Let $X(L) :=$ set of L-rational points.

If X is a plane projective curve defined by a homogeneous polynomial $F(x, y, z) \in K[x, y, z]$ of degree D, then

$$X(L) = \{(a : b : c) \in \mathbb{P}^2(L) \mid F(a, b, c) = 0\}$$

The genus of X/K is bounded by $(D-1)(D-2)/2$, with equality if X is smooth.

A new point of X over L is an element in

$$X(L) \setminus (\cup_{K \subseteq F \subset L} X(F)).$$

Curves and Fields

Let K be any field (in this talk, mostly $\mathbb{Q}$ or a number field).

Let L/K be any finite field extension, of degree d.

Let X/K be a curve, of genus g.

Let $X(L) :=$ set of L-rational points.

If X is a plane projective curve defined by a homogeneous polynomial $F(x, y, z) \in K[x, y, z]$ of degree D, then

$$X(L) = \{(a : b : c) \in \mathbb{P}^2(L) \mid F(a, b, c) = 0\}$$

The genus of X/K is bounded by $(D-1)(D-2)/2$, with equality if X is smooth.

A new point of X over L is an element in

$$X(L) \setminus (\cup_{K \subseteq F \subset L} X(F)).$$

A new point is associated with a closed point P of X/K whose residue field $K(P)$ is isomorphic to L.

Elliptic curves

An elliptic curve E/K is a curve of genus 1 with a choice of a point $P_0 \in E(K)$. For the purpose of this talk, one may think of elliptic curves as smooth plane curves given by an equation of the form

$$y^2z = x^3 + axz^2 + bz^3$$

with $a, b \in K$ and $\Delta := -16(4a^3 + 27b^2) \neq 0$.

Elliptic curves

An elliptic curve E/K is a curve of genus 1 with a choice of a point $P_0 \in E(K)$. For the purpose of this talk, one may think of elliptic curves as smooth plane curves given by an equation of the form

$$y^2 z = x^3 + axz^2 + bz^3$$

with $a, b \in K$ and $\Delta := -16(4a^3 + 27b^2) \neq 0$. When such an equation is chosen, the chosen point P_0 is $(0 : 1 : 0)$.

Elliptic curves

An elliptic curve E/K is a curve of genus 1 with a choice of a point $P_0 \in E(K)$. For the purpose of this talk, one may think of elliptic curves as smooth plane curves given by an equation of the form

$$y^2z = x^3 + axz^2 + bz^3$$

with $a, b \in K$ and $\Delta := -16(4a^3 + 27b^2) \neq 0$. When such an equation is chosen, the chosen point P_0 is $(0 : 1 : 0)$.

Key fact: The set $E(K)$ can be endowed with the structure of an abelian group, with P_0 as neutral element.

Elliptic curves

An elliptic curve E/K is a curve of genus 1 with a choice of a point $P_0 \in E(K)$. For the purpose of this talk, one may think of elliptic curves as smooth plane curves given by an equation of the form

$$y^2 z = x^3 + axz^2 + bz^3$$

with $a, b \in K$ and $\Delta := -16(4a^3 + 27b^2) \neq 0$. When such an equation is chosen, the chosen point P_0 is $(0 : 1 : 0)$.

Key fact: The set $E(K)$ can be endowed with the structure of an abelian group, with P_0 as neutral element.

Mordell-Weil Theorem: When K is a number field, $E(K)$ is a finitely generated abelian group.

Elliptic curves

An elliptic curve E/K is a curve of genus 1 with a choice of a point $P_0 \in E(K)$. For the purpose of this talk, one may think of elliptic curves as smooth plane curves given by an equation of the form

$$y^2z = x^3 + axz^2 + bz^3$$

with $a, b \in K$ and $\Delta := -16(4a^3 + 27b^2) \neq 0$. When such an equation is chosen, the chosen point P_0 is $(0 : 1 : 0)$.

Key fact: The set $E(K)$ can be endowed with the structure of an abelian group, with P_0 as neutral element.

Mordell-Weil Theorem: When K is a number field, $E(K)$ is a finitely generated abelian group.

In other words, $E(K) \simeq T \times \mathbb{Z}^r$, where T is a finite abelian group called the torsion subgroup, and $r \geq 0$ is called the algebraic rank of E/K.

Basic Questions

- Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

Basic Questions

• Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

This problem is in general very hard. Here are some variants:

Basic Questions

• Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

This problem is in general very hard. Here are some variants:

(a) Given X_0/K of genus g and $d \geq 1$, determine whether there exists an extension L/K of degree d such that $X_0(L)$ contains a new point.

Basic Questions

• Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

This problem is in general very hard. Here are some variants:

(a) Given X_0/K of genus g and $d \geq 1$, determine whether there exists an extension L/K of degree d such that $X_0(L)$ contains a new point.

(b) Given L_0/K of degree d and $g \geq 1$, determine whether there exists a curve X/K of genus g such that $X(L_0)$ contains a new point.

Basic Questions

• Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

This problem is in general very hard. Here are some variants:

(a) Given X_0/K of genus g and $d \geq 1$, determine whether there exists an extension L/K of degree d such that $X_0(L)$ contains a new point. Or: infinitely many extensions L/K of degree d

(b) Given L_0/K of degree d and $g \geq 1$, determine whether there exists a curve X/K of genus g such that $X(L_0)$ contains a new point.

Basic Questions

• Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

This problem is in general very hard. Here are some variants:

(a) Given X_0/K of genus g and $d \geq 1$, determine whether there exists an extension L/K of degree d such that $X_0(L)$ contains a new point. Or: infinitely many extensions L/K of degree d

(b) Given L_0/K of degree d and $g \geq 1$, determine whether there exists a curve X/K of genus g such that $X(L_0)$ contains a new point. Or: infinitely many curves X/K of genus g

Basic Questions

• Given a curve X_0/K of genus g and an extension L_0/K of degree d, determine whether $X_0(L_0)$ contains a new point.

This problem is in general very hard. Here are some variants:

(a) Given X_0/K of genus g and $d \geq 1$, determine whether there exists an extension L/K of degree d such that $X_0(L)$ contains a new point. Or: infinitely many extensions L/K of degree d

(b) Given L_0/K of degree d and $g \geq 1$, determine whether there exists a curve X/K of genus g such that $X(L_0)$ contains a new point. Or: infinitely many curves X/K of genus g

Most of the talk will be Question (a) and special points on the modular curves $X_1(N)/\mathbb{Q}$ over number fields $L/\mathbb{Q}$.

The question (b)

The question (b)

Given: a finite extension L/K of degree d.
Find a curve X/K of small genus $g \geq 1$ such that X/K has a new point over L.

The question (b)

Given: a finite extension L/K of degree d.
Find a curve X/K of small genus $g \geq 1$ such that X/K has a new point over L.

Easy construction. Let $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x) \in K[x]$ denote the minimal polynomial of α over K. Then $(\alpha, 0)$ is a new point on the hyperelliptic curve X/K given by the equation $y^2 = f(x)$.

The question (b)

Given: a finite extension L/K of degree d.
Find a curve X/K of small genus $g \geq 1$ such that X/K has a new point over L.

Easy construction. Let $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x) \in K[x]$ denote the minimal polynomial of α over K. Then $(\alpha, 0)$ is a new point on the hyperelliptic curve X/K given by the equation $y^2 = f(x)$.

This curve has genus $(d-1)/2$ or $d/2 - 1$, and is a curve of genus 1 only when $d = 3, 4$.

The question (b)

Given: a finite extension L/K of degree d.
Find a curve X/K of small genus $g \geq 1$ such that X/K has a new point over L.

Easy construction. Let $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x) \in K[x]$ denote the minimal polynomial of α over K. Then $(\alpha, 0)$ is a new point on the hyperelliptic curve X/K given by the equation $y^2 = f(x)$.

This curve has genus $(d-1)/2$ or $d/2 - 1$, and is a curve of genus 1 only when $d = 3, 4$.

Open question. Let p be an odd prime. Let ζ_p denote a primitive p-th root of unity. Let $L := \mathbb{Q}(\zeta_p)$ denote the p-th cyclotomic field, with $[L : \mathbb{Q}] = p - 1$.

The question (b)

Given: a finite extension L/K of degree d.
Find a curve X/K of small genus $g \geq 1$ such that X/K has a new point over L.

Easy construction. Let $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x) \in K[x]$ denote the minimal polynomial of α over K. Then $(\alpha, 0)$ is a new point on the hyperelliptic curve X/K given by the equation $y^2 = f(x)$.

This curve has genus $(d-1)/2$ or $d/2 - 1$, and is a curve of genus 1 only when $d = 3, 4$.

Open question. Let p be an odd prime. Let ζ_p denote a primitive p-th root of unity. Let $L := \mathbb{Q}(\zeta_p)$ denote the p-th cyclotomic field, with $[L : \mathbb{Q}] = p - 1$.

Can you find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

The question (b)

Given: a finite extension L/K of degree d.
Find a curve X/K of small genus $g \geq 1$ such that X/K has a new point over L.

Easy construction. Let $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x) \in K[x]$ denote the minimal polynomial of α over K. Then $(\alpha, 0)$ is a new point on the hyperelliptic curve X/K given by the equation $y^2 = f(x)$.

This curve has genus $(d-1)/2$ or $d/2 - 1$, and is a curve of genus 1 only when $d = 3, 4$.

Open question. Let p be an odd prime. Let ζ_p denote a primitive p-th root of unity. Let $L := \mathbb{Q}(\zeta_p)$ denote the p-th cyclotomic field, with $[L : \mathbb{Q}] = p - 1$.

Can you find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

Same question for the totally real subfield $L := \mathbb{Q}(\zeta_p)^+$.

Some known theorems

Let K be a field of characteristic 0.

Some known theorems

Let K be a field of characteristic 0.

Theorem (Liu-L.) Let L/K be any finite extension of degree $d \leq 10$. Then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

(For $d \leq 9$, the result is due to Rohrlich in 1997.)

Some known theorems

Let K be a field of characteristic 0.

Theorem (Liu-L.) Let L/K be any finite extension of degree $d \leq 10$. Then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

(For $d \leq 9$, the result is due to Rohrlich in 1997.)

Theorem (Liu-L.) When $[L : K] = 12, 14, 15, 20, 21$ or 30 and L/K is abelian, then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

Some known theorems

Let K be a field of characteristic 0.

Theorem (Liu-L.) Let L/K be any finite extension of degree $d \leq 10$. Then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

(For $d \leq 9$, the result is due to Rohrlich in 1997.)

Theorem (Liu-L.) When $[L : K] = 12, 14, 15, 20, 21$ or 30 and L/K is abelian, then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

Theorem (Arvind Suresh) When L/K is Galois of degree $12, 14$ and 16, then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

Some known theorems

Let K be a field of characteristic 0.

Theorem (Liu-L.) Let L/K be any finite extension of degree $d \leq 10$. Then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

(For $d \leq 9$, the result is due to Rohrlich in 1997.)

Theorem (Liu-L.) When $[L : K] = 12, 14, 15, 20, 21$ or 30 and L/K is abelian, then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

Theorem (Arvind Suresh) When L/K is Galois of degree $12, 14$ and 16, then there exist infinitely many elliptic curves E/K such that $E(L)$ contains a new point.

In general, for L/K of degree d, Liu-L. find infinitely many hyperelliptic curves X/K of genus about $d/4$, such that $X(L)$ contains a new point, and Suresh produces curves where the genus is about $d/8$ when $K \subset F \subset L$ with $[L : F] = 2$.

Example of degree 17

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$.
Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.
The field $L/\mathbb{Q}$ is Galois with cyclic Galois group of order 17.

Example of degree 17

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$.
Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.
The field $L/\mathbb{Q}$ is Galois with cyclic Galois group of order 17.

Question (b) from earlier: Is it possible to find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

Example of degree 17

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$.
Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.
The field $L/\mathbb{Q}$ is Galois with cyclic Galois group of order 17.

Question (b) from earlier: Is it possible to find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

Answer: Yes, under the Birch and Swinnerton-Dyer conjecture.

Recall: The L-function and B-SD

For ease of exposition, assume that $K = \mathbb{Q}$ and consider an elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let E_p denote the reduction of E modulo p. When $p \nmid \Delta$, the reduction is an elliptic curve.

Recall: The L-function and B-SD

For ease of exposition, assume that $K = \mathbb{Q}$ and consider an elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let E_p denote the reduction of E modulo p. When $p \nmid \Delta$, the reduction is an elliptic curve.

Hasse's Theorem:
$p + 1 - 2\sqrt{p} \leq |E_p(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$.

Recall: The L-function and B-SD

For ease of exposition, assume that $K = \mathbb{Q}$ and consider an elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let E_p denote the reduction of E modulo p. When $p \nmid \Delta$, the reduction is an elliptic curve.

Hasse's Theorem:
$p + 1 - 2\sqrt{p} \leq |E_p(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$.

Packaging the $|E_p(\mathbb{F}_p)|$ together: the L-function $L(E/\mathbb{Q}, s)$.

Recall: The L-function and B-SD

For ease of exposition, assume that $K = \mathbb{Q}$ and consider an elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let E_p denote the reduction of E modulo p. When $p \nmid \Delta$, the reduction is an elliptic curve.

Hasse's Theorem:
$p + 1 - 2\sqrt{p} \leq |E_p(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$.

Packaging the $|E_p(\mathbb{F}_p)|$ together: the L-function $L(E/\mathbb{Q}, s)$.

Define $a_p := (p + 1) - |E_p(\mathbb{F}_p)|$, so that $|a_p| \leq 2\sqrt{p}$,

Recall: The L-function and B-SD

For ease of exposition, assume that $K = \mathbb{Q}$ and consider an elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let E_p denote the reduction of E modulo p. When $p \nmid \Delta$, the reduction is an elliptic curve.

Hasse's Theorem:
$p + 1 - 2\sqrt{p} \leq |E_p(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$.

Packaging the $|E_p(\mathbb{F}_p)|$ together: the L-function $L(E/\mathbb{Q}, s)$.

Define $a_p := (p+1) - |E_p(\mathbb{F}_p)|$, so that $|a_p| \leq 2\sqrt{p}$,

and

$$L^*(E/\mathbb{Q}, s) := \prod_{p \text{ prime},\ p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Recall: The L-function and B-SD

For ease of exposition, assume that $K = \mathbb{Q}$ and consider an elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let E_p denote the reduction of E modulo p. When $p \nmid \Delta$, the reduction is an elliptic curve.

Hasse's Theorem:
$p + 1 - 2\sqrt{p} \leq |E_p(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$.

Packaging the $|E_p(\mathbb{F}_p)|$ together: the L-function $L(E/\mathbb{Q}, s)$.

Define $a_p := (p+1) - |E_p(\mathbb{F}_p)|$, so that $|a_p| \leq 2\sqrt{p}$,

and

$$L^*(E/\mathbb{Q}, s) := \prod_{p \text{ prime},\ p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Then

$$L(E/\mathbb{Q}, s) = L^*(E/\mathbb{Q}, s) \cdot \prod_{p \mid \Delta} \text{explicit term}.$$

The Birch and Swinnerton-Dyer conjecture (I)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

The Birch and Swinnerton-Dyer conjecture (I)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

Conjecture (Part 1). The function $L(E/K, s)$ is holomorphic around $s = 1$ and thus we can consider its order of vanishing r_{an} at $s = 1$. In other words, there is a power series expansion

$$L(E/K, s) = \ell_0(s-1)^{r_{an}} + \ell_1(s-1)^{r_{an}+1} + \dots.$$

The integer r_{an} is called the analytic rank of E/K.

The Birch and Swinnerton-Dyer conjecture (I)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

Conjecture (Part 1). The function $L(E/K, s)$ is holomorphic around $s = 1$ and thus we can consider its order of vanishing r_{an} at $s = 1$. In other words, there is a power series expansion

$$L(E/K, s) = \ell_0(s-1)^{r_{an}} + \ell_1(s-1)^{r_{an}+1} + \dots.$$

The integer r_{an} is called the analytic rank of E/K.

It is conjectured that $r_{an} = r$.

The Birch and Swinnerton-Dyer conjecture (I)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

Conjecture (Part 1). The function $L(E/K, s)$ is holomorphic around $s = 1$ and thus we can consider its order of vanishing r_{an} at $s = 1$. In other words, there is a power series expansion

$$L(E/K, s) = \ell_0(s-1)^{r_{an}} + \ell_1(s-1)^{r_{an}+1} + \dots .$$

The integer r_{an} is called the analytic rank of E/K.

It is conjectured that $r_{an} = r$.

The integer r_{an} can often be computed directly. The integer r is much more difficult to compute directly, since there are no efficient methods for finding elements in $E(K)$.

Example of degree 17 revisited

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$. Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.

Example of degree 17 revisited

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$. Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.

Question (b) from earlier: Is it possible to find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

Example of degree 17 revisited

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$. Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.

Question (b) from earlier: Is it possible to find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

For each elliptic curve $E/\mathbb{Q}$ in Cremona's tables, compute the analytic ranks $r_{an}(\mathbb{Q})$ over $\mathbb{Q}$, and $r_{an}(L)$ over L.

Example of degree 17 revisited

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$. Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.

Question (b) from earlier: Is it possible to find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

For each elliptic curve $E/\mathbb{Q}$ in Cremona's tables, compute the analytic ranks $r_{an}(\mathbb{Q})$ over $\mathbb{Q}$, and $r_{an}(L)$ over L.

If for some $E/\mathbb{Q}$, we find that $r_{an}(\mathbb{Q}) < r_{an}(L)$, then conjecturally, $E(L)$ contains a new point of infinite order.

Example of degree 17 revisited

Consider the field $\mathbb{Q}(\zeta_{103})$, of degree $102 = 17 \cdot 6$. Let $L/\mathbb{Q}$ denote the unique subfield of $\mathbb{Q}(\zeta_{103})$ of degree 17.

Question (b) from earlier: Is it possible to find an elliptic curve $E/\mathbb{Q}$ with a new point over L?

For each elliptic curve $E/\mathbb{Q}$ in Cremona's tables, compute the analytic ranks $r_{an}(\mathbb{Q})$ over $\mathbb{Q}$, and $r_{an}(L)$ over L.

If for some $E/\mathbb{Q}$, we find that $r_{an}(\mathbb{Q}) < r_{an}(L)$, then conjecturally, $E(L)$ contains a new point of infinite order.

Conjectural such $E/\mathbb{Q}$: 173883a1 (thanks to Bill Allombert and gp-pari)

This is a semi-stable elliptic curve of rank 2 over $\mathbb{Q}$ with bad reduction at $p = 3, 149$, and 389. The equation is $y^2 + y = x^3 - x^2 - 310x + 1779$. Can one find an explicit new point over L? No similar examples found for prime degrees ≥ 19.

The Birch and Swinnerton-Dyer conjecture (II)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

The Birch and Swinnerton-Dyer conjecture (II)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

Conjecture (Part 2). The function $L(E/K, s)$ is holomorphic around $s = 1$ with a power series expansion

$$L(E/K, s) = \ell_0(s-1)^{r_{an}} + \ell_1(s-1)^{r_{an}+1} + \dots.$$

The conjecture predicts an explicit formula for the leading term ℓ_0.

The Birch and Swinnerton-Dyer conjecture (II)

Let K be a number field, and let E/K be an elliptic curve with L-function $L(E/K, s)$ and algebraic rank r. Then

Conjecture (Part 2). The function $L(E/K, s)$ is holomorphic around $s = 1$ with a power series expansion

$$L(E/K, s) = \ell_0 (s-1)^{r_{an}} + \ell_1 (s-1)^{r_{an}+1} + \dots .$$

The conjecture predicts an explicit formula for the leading term ℓ_0.

The following is sufficient for the rest of the talk:

$$\ell_0 = \frac{\prod_M c_M}{|E(K)_{tors}|^2} \cdot \text{ other terms}$$

For the rest of the talk, I will discuss the following question: Assume that $|E(K)_{tors}| > 1$. Are there often cancellations in the ratio $\frac{\prod_M c_M}{|E(K)_{tors}|^2}$?

The Tamagawa numbers c_M

For each maximal ideal M of $\mathcal{O}_K$, let $k_M := \mathcal{O}_K/M$. Let E/K be an elliptic curve.

The Tamagawa numbers c_M

For each maximal ideal M of $\mathcal{O}_K$, let $k_M := \mathcal{O}_K/M$. Let E/K be an elliptic curve.

There exists a finite abelian group $\Phi_{E,M}(k_M)$ and a group homomorphism

$$E(K) \longrightarrow \Phi_{E,M}(k_M)$$

The Tamagawa numbers c_M

For each maximal ideal M of $\mathcal{O}_K$, let $k_M := \mathcal{O}_K/M$. Let E/K be an elliptic curve.

There exists a finite abelian group $\Phi_{E,M}(k_M)$ and a group homomorphism

$$E(K) \longrightarrow \Phi_{E,M}(k_M)$$

The Tamagawa number at M is $c_M := |\Phi_{E,M}(k_M)|$.

The Tamagawa numbers c_M

For each maximal ideal M of $\mathcal{O}_K$, let $k_M := \mathcal{O}_K/M$. Let E/K be an elliptic curve.

There exists a finite abelian group $\Phi_{E,M}(k_M)$ and a group homomorphism

$$E(K) \longrightarrow \Phi_{E,M}(k_M)$$

The Tamagawa number at M is $c_M := |\Phi_{E,M}(k_M)|$.

When the elliptic curve has good reduction at M, then $c_M = 1$.

The Tamagawa numbers c_M

For each maximal ideal M of $\mathcal{O}_K$, let $k_M := \mathcal{O}_K/M$. Let E/K be an elliptic curve.

There exists a finite abelian group $\Phi_{E,M}(k_M)$ and a group homomorphism

$$E(K) \longrightarrow \Phi_{E,M}(k_M)$$

The Tamagawa number at M is $c_M := |\Phi_{E,M}(k_M)|$.

When the elliptic curve has good reduction at M, then $c_M = 1$.

Easily explained cancelation: Suppose that $E(K)$ contains a point P of prime order N and that for some maximal ideal M, the image of P under the map $E(K) \to \Phi_{E,M}(k_M)$ is not trivial. In that case, N divides c_M.

The Tamagawa numbers c_M

For each maximal ideal M of $\mathcal{O}_K$, let $k_M := \mathcal{O}_K/M$. Let E/K be an elliptic curve.

There exists a finite abelian group $\Phi_{E,M}(k_M)$ and a group homomorphism

$$E(K) \longrightarrow \Phi_{E,M}(k_M)$$

The Tamagawa number at M is $c_M := |\Phi_{E,M}(k_M)|$.

When the elliptic curve has good reduction at M, then $c_M = 1$.

Easily explained cancelation: Suppose that $E(K)$ contains a point P of prime order N and that for some maximal ideal M, the image of P under the map $E(K) \to \Phi_{E,M}(k_M)$ is not trivial. In that case, N divides c_M.

Néron class group: $\prod_M \Phi_{E,M}(k_M)/\mathrm{Im}(E(K))$ (C. Gonzalez-Aviles)

Elliptic curves over $\mathbb{Q}$

The product $c(E/K) := \prod_M c_M$ is called the global Tamagawa number.

Elliptic curves over $\mathbb{Q}$

The product $c(E/K) := \prod_M c_M$ is called the global Tamagawa number.

Initial Motivation. I learned from Amod Agashe that he had verified for all *optimal* elliptic curves in Cremona's table, that if $E/\mathbb{Q}$ has a $\mathbb{Q}$-point of order 5 or 7, then 5 or 7 divides $c(E/\mathbb{Q})$. He conjectured that this statement always holds.

Elliptic curves over $\mathbb{Q}$

The product $c(E/K) := \prod_M c_M$ is called the global Tamagawa number.

Initial Motivation. I learned from Amod Agashe that he had verified for all *optimal* elliptic curves in Cremona's table, that if $E/\mathbb{Q}$ has a $\mathbb{Q}$-point of order 5 or 7, then 5 or 7 divides $c(E/\mathbb{Q})$. He conjectured that this statement always holds.

This conjecture is true in full generality.

Elliptic curves over $\mathbb{Q}$

The product $c(E/K) := \prod_M c_M$ is called the global Tamagawa number.

Initial Motivation. I learned from Amod Agashe that he had verified for all *optimal* elliptic curves in Cremona's table, that if $E/\mathbb{Q}$ has a $\mathbb{Q}$-point of order 5 or 7, then 5 or 7 divides $c(E/\mathbb{Q})$. He conjectured that this statement always holds.

This conjecture is true in full generality.

Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.

Elliptic curves over $\mathbb{Q}$

The product $c(E/K) := \prod_M c_M$ is called the global Tamagawa number.

Initial Motivation. I learned from Amod Agashe that he had verified for all *optimal* elliptic curves in Cremona's table, that if $E/\mathbb{Q}$ has a $\mathbb{Q}$-point of order 5 or 7, then 5 or 7 divides $c(E/\mathbb{Q})$. He conjectured that this statement always holds.

This conjecture is true in full generality.

Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.

If $N = 5$, then N divides $c(E/\mathbb{Q})$, except when $E = X_1(11)$.

Elliptic curves over $\mathbb{Q}$

The product $c(E/K) := \prod_M c_M$ is called the global Tamagawa number.

Initial Motivation. I learned from Amod Agashe that he had verified for all *optimal* elliptic curves in Cremona's table, that if $E/\mathbb{Q}$ has a $\mathbb{Q}$-point of order 5 or 7, then 5 or 7 divides $c(E/\mathbb{Q})$. He conjectured that this statement always holds.

This conjecture is true in full generality.

Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.

If $N = 5$, then N divides $c(E/\mathbb{Q})$, except when $E = X_1(11)$.

How does this theorem generalize to higher degree number fields?

Elliptic curves over $\mathbb{Q}$ and small torsion

Can a similar statement be conjectured when $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational point of order $2, 3, 4$ or 6?

Elliptic curves over $\mathbb{Q}$ and small torsion

Can a similar statement be conjectured when $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational point of order $2, 3, 4$ or 6?

Yes, but one needs to consider the full leading term of the L-function of $E/\mathbb{Q}$. (Conjecture of Agashe and Stein)

Elliptic curves over $\mathbb{Q}$ and small torsion

Can a similar statement be conjectured when $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational point of order $2, 3, 4$ or 6?

Yes, but one needs to consider the full leading term of the L-function of $E/\mathbb{Q}$. (Conjecture of Agashe and Stein)

For instance:

Theorem (Mentzelos Melistas). Let $E/\mathbb{Q}$ be a semi-stable optimal elliptic curve of rank 0. Then $|E(\mathbb{Q})_{tors}|$ divides

$$c(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \text{number of components of } E(\mathbb{R}).$$

Elliptic curves over number fields

Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an elliptic curve with a K-rational point of prime order N.

Elliptic curves over number fields

Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an elliptic curve with a K-rational point of prime order N.

Hoped-for-theorem Assume that $N > 2d + 1$. Then N divides $\prod_M c_M$, except for finitely many exceptions over finitely many fields of degree d.

Elliptic curves over number fields

Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an elliptic curve with a K-rational point of prime order N.

Hoped-for-theorem Assume that $N > 2d + 1$. Then N divides $\prod_M c_M$, except for finitely many exceptions over finitely many fields of degree d.

Theorem (L.) Assume $d = 1$ and $N \geq 5$. Then N divides $\prod_M c_M$, except when $N = 5$ and $E/\mathbb{Q} = X_1(11)/\mathbb{Q}$.

Elliptic curves over number fields

Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an elliptic curve with a K-rational point of prime order N.

Hoped-for-theorem Assume that $N > 2d + 1$. Then N divides $\prod_M c_M$, except for finitely many exceptions over finitely many fields of degree d.

Theorem (L.) Assume $d = 1$ and $N \geq 5$. Then N divides $\prod_M c_M$, except when $N = 5$ and $E/\mathbb{Q} = X_1(11)/\mathbb{Q}$.

Theorem (L.) Assume $d = 2$ and $N \geq 7$. Then N divides $\prod_M c_M$, except for four explicit exceptions when $N = 7$ over $K = \mathbb{Q}(\zeta_3)$ and $K = \mathbb{Q}(\zeta_5)^+$.

Elliptic curves over number fields

Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an elliptic curve with a K-rational point of prime order N.

Hoped-for-theorem Assume that $N > 2d+1$. Then N divides $\prod_M c_M$, except for finitely many exceptions over finitely many fields of degree d.

Theorem (L.) Assume $d = 1$ and $N \geq 5$. Then N divides $\prod_M c_M$, except when $N = 5$ and $E/\mathbb{Q} = X_1(11)/\mathbb{Q}$.

Theorem (L.) Assume $d = 2$ and $N \geq 7$. Then N divides $\prod_M c_M$, except for four explicit exceptions when $N = 7$ over $K = \mathbb{Q}(\zeta_3)$ and $K = \mathbb{Q}(\zeta_5)^+$.

Theorem (L.) Assume $d = 3$ and $N \geq 11$. Then N divides $\prod_M c_M$, except for one exception when $N = 13$ over $K = \mathbb{Q}(\zeta_7)^+$.

Elliptic curves over number fields

Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an elliptic curve with a K-rational point of prime order N.

Hoped-for-theorem Assume that $N > 2d+1$. Then N divides $\prod_M c_M$, except for finitely many exceptions over finitely many fields of degree d.

Theorem (L.) Assume $d = 1$ and $N \geq 5$. Then N divides $\prod_M c_M$, except when $N = 5$ and $E/\mathbb{Q} = X_1(11)/\mathbb{Q}$.

Theorem (L.) Assume $d = 2$ and $N \geq 7$. Then N divides $\prod_M c_M$, except for four explicit exceptions when $N = 7$ over $K = \mathbb{Q}(\zeta_3)$ and $K = \mathbb{Q}(\zeta_5)^+$.

Theorem (L.) Assume $d = 3$ and $N \geq 11$. Then N divides $\prod_M c_M$, except for one exception when $N = 13$ over $K = \mathbb{Q}(\zeta_7)^+$.

The j-invariant of the exception is $j = -28672/3$. It has prime conductor $(3)\mathcal{O}_K$, with split multiplicative reduction of type I_1 at that prime.

Elliptic curves over quartic fields

Let $K/\mathbb{Q}$ be a number field of degree $d = 4$. Let E/K be an elliptic curve with a K-rational point of prime order $N \geq 11$.

Elliptic curves over quartic fields

Let $K/\mathbb{Q}$ be a number field of degree $d = 4$. Let E/K be an elliptic curve with a K-rational point of prime order $N \geq 11$.

Theorem (L.) Assume that $\mathcal{O}_K^*$ has rank 1 or 2. Then N divides $\prod_M c_M$, except for the following exceptions:

N	field K	$r(K)$	$\mathrm{disc}(K)$
$11(2), 13(j=0)$	$x^4 - x^3 - x^2 + x + 1$	1	117
$11(4)$	$x^4 - x^3 + 2x - 1$	2	-275
$11(2)$	$x^4 - x - 1$	2	-283

Elliptic curves over quartic fields

Let $K/\mathbb{Q}$ be a number field of degree $d = 4$. Let E/K be an elliptic curve with a K-rational point of prime order $N \geq 11$.

Theorem (L.) Assume that $\mathcal{O}_K^*$ has rank 1 or 2. Then N divides $\prod_M c_M$, except for the following exceptions:

N	field K	$r(K)$	$\mathrm{disc}(K)$
$11(2), 13(j=0)$	$x^4 - x^3 - x^2 + x + 1$	1	117
$11(4)$	$x^4 - x^3 + 2x - 1$	2	-275
$11(2)$	$x^4 - x - 1$	2	-283

Conjecture (L.) Assume that $\mathcal{O}_K^*$ has rank 3. Then N divides $\prod_M c_M$, except for the following exceptions:

N	field K	$r(K)$	$\mathrm{disc}(K)$
$11(2), 13, \mathbf{17}$	$x^4 - x^3 - 3x^2 + x + 1$	3	725

Elliptic curves over quartic fields

Let $K/\mathbb{Q}$ be a number field of degree $d = 4$. Let E/K be an elliptic curve with a K-rational point of prime order $N \geq 11$.

Theorem (L.) Assume that $\mathcal{O}_K^*$ has rank 1 or 2. Then N divides $\prod_M c_M$, except for the following exceptions:

N	field K	$r(K)$	$\mathrm{disc}(K)$
$11(2), 13(j=0)$	$x^4 - x^3 - x^2 + x + 1$	1	117
$11(4)$	$x^4 - x^3 + 2x - 1$	2	-275
$11(2)$	$x^4 - x - 1$	2	-283

Conjecture (L.) Assume that $\mathcal{O}_K^*$ has rank 3. Then N divides $\prod_M c_M$, except for the following exceptions:

N	field K	$r(K)$	$\mathrm{disc}(K)$
$11(2), 13, \mathbf{17}$	$x^4 - x^3 - 3x^2 + x + 1$	3	725

The curve with the point of order 17 was found by David Krumm around 2013 using his algorithm (with John Doyle) for listing elements of small heights in number fields.

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961)
There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961) There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Theorem (Beukers-Schlickewei, 1996) In any ring of integers $\mathcal{O}_K$, the number of exceptional units is bounded by $2^{8(1+\mathrm{rank}(\mathcal{O}_K^*))}$.

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961) There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Theorem (Beukers-Schlickewei, 1996) In any ring of integers $\mathcal{O}_K$, the number of exceptional units is bounded by $2^{8(1+\text{rank}(\mathcal{O}_K^*))}$.

Example In $\mathbb{Q}(\zeta_p)^+$, the number of exceptional units grows rather fast. For instance, when $p = 13, 17, 19$, and 23, there are respectively 1830, 11700, 28398, and 130812 exceptional units

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961) There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Theorem (Beukers-Schlickewei, 1996) In any ring of integers $\mathcal{O}_K$, the number of exceptional units is bounded by $2^{8(1+\mathrm{rank}(\mathcal{O}_K^*))}$.

Example In $\mathbb{Q}(\zeta_p)^+$, the number of exceptional units grows rather fast. For instance, when $p = 13, 17, 19$, and 23, there are respectively 1830, 11700, 28398, and 130812 exceptional units (Wildanger 2000, available in Magma).

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961) There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Theorem (Beukers-Schlickewei, 1996) In any ring of integers $\mathcal{O}_K$, the number of exceptional units is bounded by $2^{8(1+\text{rank}(\mathcal{O}_K^*))}$.

Example In $\mathbb{Q}(\zeta_p)^+$, the number of exceptional units grows rather fast. For instance, when $p = 13, 17, 19$, and 23, there are respectively 1830, 11700, 28398, and 130812 exceptional units (Wildanger 2000, available in Magma). The quadratic fields with exceptional units are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_5)^+$.

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961) There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Theorem (Beukers-Schlickewei, 1996) In any ring of integers $\mathcal{O}_K$, the number of exceptional units is bounded by $2^{8(1+\mathrm{rank}(\mathcal{O}_K^*))}$.

Example In $\mathbb{Q}(\zeta_p)^+$, the number of exceptional units grows rather fast. For instance, when $p = 13, 17, 19$, and 23, there are respectively 1830, 11700, 28398, and 130812 exceptional units (Wildanger 2000, available in Magma). The quadratic fields with exceptional units are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_5)^+$.

Theorem (L.) (weak version) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 7$ such that N does not divide $\prod_M c_M$.

Exceptional units

Let R be any ring. An exceptional unit in R is a unit r such that $1 - r$ is also a unit. (Terminology by Nagell in 1969)

Theorem (Siegel 1929, S. Lang 1960, S. Chowla 1961) There are only finitely many exceptional units in any ring of integers $\mathcal{O}_K$.

Theorem (Beukers-Schlickewei, 1996) In any ring of integers $\mathcal{O}_K$, the number of exceptional units is bounded by $2^{8(1+\mathrm{rank}(\mathcal{O}_K^*))}$.

Example In $\mathbb{Q}(\zeta_p)^+$, the number of exceptional units grows rather fast. For instance, when $p = 13, 17, 19$, and 23, there are respectively 1830, 11700, 28398, and 130812 exceptional units (Wildanger 2000, available in Magma). The quadratic fields with exceptional units are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_5)^+$.

Theorem (L.) (weak version) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 7$ such that N does not divide $\prod_M c_M$. Then $\mathcal{O}_K$ contains an exceptional unit.

The Lenstra constant

Let R be any ring. An exceptional sequence in R is a sequence $u_1 := 0, u_2 := 1, u_3, \ldots, u_m$, such that each difference $u_i - u_j$ $(i \neq j)$ is a unit in R.

The Lenstra constant

Let R be any ring. An exceptional sequence in R is a sequence $u_1 := 0, u_2 := 1,\ u_3, \ldots, u_m$, such that each difference $u_i - u_j$ $(i \neq j)$ is a unit in R.

It follows from the definition that $0, 1, r$ is an exceptional sequence if and only if r is an exceptional unit.

The Lenstra constant

Let R be any ring. An exceptional sequence in R is a sequence $u_1 := 0, u_2 := 1,\ u_3, \ldots, u_m$, such that each difference $u_i - u_j$ $(i \neq j)$ is a unit in R.

It follows from the definition that $0, 1, r$ is an exceptional sequence if and only if r is an exceptional unit.

If $0, 1, u_3, \ldots, u_m$ is an exceptional sequence in R, then for each maximal ideal M, the sequence reduces to distinct elements in R/M. In particular, $m \leq |R/M|$.

The Lenstra constant

Let R be any ring. An exceptional sequence in R is a sequence $u_1 := 0, u_2 := 1,\ u_3, \ldots, u_m$, such that each difference $u_i - u_j$ $(i \neq j)$ is a unit in R.

It follows from the definition that $0, 1, r$ is an exceptional sequence if and only if r is an exceptional unit.

If $0, 1, u_3, \ldots, u_m$ is an exceptional sequence in R, then for each maximal ideal M, the sequence reduces to distinct elements in R/M. In particular, $m \leq |R/M|$.

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$ (defined by H. Lenstra in 1977).

The Lenstra constant

Let R be any ring. An exceptional sequence in R is a sequence $u_1 := 0, u_2 := 1, u_3, \ldots, u_m$, such that each difference $u_i - u_j$ $(i \neq j)$ is a unit in R.

It follows from the definition that $0, 1, r$ is an exceptional sequence if and only if r is an exceptional unit.

If $0, 1, u_3, \ldots, u_m$ is an exceptional sequence in R, then for each maximal ideal M, the sequence reduces to distinct elements in R/M. In particular, $m \leq |R/M|$.

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$ (defined by H. Lenstra in 1977).

If K is a number field of degree d, then $M(K) \leq 2^d$.

If $K = \mathbb{Q}(\zeta_p)$, then $M(K) = d + 1$ (Lenstra).
If $K = \mathbb{Q}(\zeta_p)^+$, then $M(K) = 2d$ or $2d + 1$ (Leutbecher-Nicklash, 1987).

The Lenstra constant and torsion

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 11$ such that N does not divide $\prod_M c_M$. Then

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 11$ such that N does not divide $\prod_M c_M$. Then

- If $N = 11$, then $M(K) \geq 6$.

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 11$ such that N does not divide $\prod_M c_M$. Then

- If $N = 11$, then $M(K) \geq 6$.
- If $13 \leq N \leq 23$, then $M(K) \geq (N-1)/2$.

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 11$ such that N does not divide $\prod_M c_M$. Then

- If $N = 11$, then $M(K) \geq 6$.
- If $13 \leq N \leq 23$, then $M(K) \geq (N-1)/2$.

We expect that $M(K) \geq (N-1)/2$ for all primes N.

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 11$ such that N does not divide $\prod_M c_M$. Then

- If $N = 11$, then $M(K) \geq 6$.
- If $13 \leq N \leq 23$, then $M(K) \geq (N-1)/2$.

We expect that $M(K) \geq (N-1)/2$ for all primes N.

- If $23 \leq N \leq 101$, then $M(K) \geq 11$.

The Lenstra constant and torsion

The Lenstra constant $M(K)$ of K is the largest integer m such that there exists an exceptional sequence of length m in $\mathcal{O}_K$.

$M(K) \geq 3$ iff $\mathcal{O}_K^*$ contains an exceptional unit.

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order $N \geq 11$ such that N does not divide $\prod_M c_M$. Then

- If $N = 11$, then $M(K) \geq 6$.
- If $13 \leq N \leq 23$, then $M(K) \geq (N-1)/2$.

We expect that $M(K) \geq (N-1)/2$ for all primes N.

- If $23 \leq N \leq 101$, then $M(K) \geq 11$.

This theorem is due to Mestre (1981) when E/K has everywhere potentially good reduction (with the bound $M(K) \geq 5$ when $N = 11$).

Question on the Lenstra constant

Find a low bound $c = c(d)$ such that the following is true:

There only finitely many number fields $K/\mathbb{Q}$ of degree d such that $M(K) > c$.

Question on the Lenstra constant

Find a low bound $c = c(d)$ such that the following is true:

There only finitely many number fields $K/\mathbb{Q}$ of degree d such that $M(K) > c$.

For instance, can one take $c = d$ when d is prime?

Question on the Lenstra constant

Find a low bound $c = c(d)$ such that the following is true:

There only finitely many number fields $K/\mathbb{Q}$ of degree d such that $M(K) > c$.

For instance, can one take $c = d$ when d is prime?

Application. Recall

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order N such that N does not divide $\prod_M c_M$. Then

- If $11 \leq N \leq 23$, then $M(K) \geq (N-1)/2$.

Question on the Lenstra constant

Find a low bound $c = c(d)$ such that the following is true:

There only finitely many number fields $K/\mathbb{Q}$ of degree d such that $M(K) > c$.

For instance, can one take $c = d$ when d is prime?

Application. Recall

Theorem (L.) Let K be a number field. Suppose that E/K is an elliptic curve with a K-rational point of prime order N such that N does not divide $\prod_M c_M$. Then

- If $11 \leq N \leq 23$, then $M(K) \geq (N-1)/2$.

If there are only finitely many fields such that $M(K) > d$ then as soon as $(N-1)/2 > d$ (i.e., $N > 2d+1$), we get that there can exist only finitely many elliptic curves as in the theorem.

Algorithm

The modular curve $X_1(N)/\mathbb{Q}$ admits an equation $F_N(r, s) = 0$ called the raw form equation. We have $F_N(r, s) \in \mathbb{Z}[r, s]$.

Algorithm

The modular curve $X_1(N)/\mathbb{Q}$ admits an equation $F_N(r,s) = 0$ called the raw form equation. We have $F_N(r,s) \in \mathbb{Z}[r,s]$.

Theorem (L.). Let K be a number field. Let $11 \leq N \leq 23$ be prime. Suppose that E/K is an elliptic curve with a K-rational point P of prime order N such that N does not divide $\prod_M c_M$.

Algorithm

The modular curve $X_1(N)/\mathbb{Q}$ admits an equation $F_N(r,s) = 0$ called the raw form equation. We have $F_N(r,s) \in \mathbb{Z}[r,s]$.

Theorem (L.). Let K be a number field. Let $11 \leq N \leq 23$ be prime. Suppose that E/K is an elliptic curve with a K-rational point P of prime order N such that N does not divide $\prod_M c_M$. Let $(r_0, s_0) \in K^2$ denote the point on the curve $F_N(r,s) = 0$ corresponding to $(E/K, P)$.

Algorithm

The modular curve $X_1(N)/\mathbb{Q}$ admits an equation $F_N(r,s) = 0$ called the raw form equation. We have $F_N(r,s) \in \mathbb{Z}[r,s]$.

Theorem (L.). Let K be a number field. Let $11 \leq N \leq 23$ be prime. Suppose that E/K is an elliptic curve with a K-rational point P of prime order N such that N does not divide $\prod_M c_M$. Let $(r_0, s_0) \in K^2$ denote the point on the curve $F_N(r,s) = 0$ corresponding to $(E/K, P)$.

Then r_0 and s_0 are both exceptional units in $\mathcal{O}_K^*$.

Algorithm

The modular curve $X_1(N)/\mathbb{Q}$ admits an equation $F_N(r,s) = 0$ called the raw form equation. We have $F_N(r,s) \in \mathbb{Z}[r,s]$.

Theorem (L.). Let K be a number field. Let $11 \leq N \leq 23$ be prime. Suppose that E/K is an elliptic curve with a K-rational point P of prime order N such that N does not divide $\prod_M c_M$. Let $(r_0, s_0) \in K^2$ denote the point on the curve $F_N(r,s) = 0$ corresponding to $(E/K, P)$.

Then r_0 and s_0 are both exceptional units in $\mathcal{O}_K^*$.

Better: Then $0, 1, r_0, s_0, \frac{r_0-1}{s_0-1}$ is an exceptional sequence in $\mathcal{O}_K^*$.

Algorithm

The modular curve $X_1(N)/\mathbb{Q}$ admits an equation $F_N(r,s) = 0$ called the raw form equation. We have $F_N(r,s) \in \mathbb{Z}[r,s]$.

Theorem (L.). Let K be a number field. Let $11 \le N \le 23$ be prime. Suppose that E/K is an elliptic curve with a K-rational point P of prime order N such that N does not divide $\prod_M c_M$. Let $(r_0, s_0) \in K^2$ denote the point on the curve $F_N(r,s) = 0$ corresponding to $(E/K, P)$.

Then r_0 and s_0 are both exceptional units in $\mathcal{O}_K^*$.

Better: Then $0, 1, r_0, s_0, \frac{r_0 - 1}{s_0 - 1}$ is an exceptional sequence in $\mathcal{O}_K^*$.

Algorithm Given a field K, to find all E/K with a K-rational point of prime order N such that N does not divide $\prod_M c_M$, it suffices to find all solutions to $F_N(r,s) = 0$ with both r and s exceptional units in K.

The case of septic fields

Conjecture: Let $N \geq 17$ be prime. Then there exist only finitely many fields $K/\mathbb{Q}$ of degree $d = 7$ with an elliptic curve E/K having a K-rational torsion point of order N and such that N does not divide $\prod_M c_M$.

The case of septic fields

Conjecture: Let $N \geq 17$ be prime. Then there exist only finitely many fields $K/\mathbb{Q}$ of degree $d = 7$ with an elliptic curve E/K having a K-rational torsion point of order N and such that N does not divide $\prod_M c_M$.

The list of known such elliptic curves over septic fields:

N	field K (degree 7)	$ex(K)$	$M(K)$	discr(K)
$11(6), 13, \mathbf{25}$	$x^7 - x^6 - x^5 + x^4 - x^2 + x + 1$	366	≥ 12	-184607 (first)
$11(2), 13, \mathbf{19}$	$x^7 - x^6 + x^3 - x + 1$	336	≥ 10	-199559 (fifth)
$11(2), 13, \mathbf{17}$	$x^7 - 2x^6 + 4x^5 - 4x^4 + 3x^3 - x^2 - x + 1$	270	≥ 8	-250367(sixteenth)
$11(6), \mathbf{23}$	$x^7 - 3x^5 - x^4 + 3x^3 + 1$	960	≥ 11	612569 (second)
$11(6), \mathbf{23}$	$x^7 - x^6 - x^4 + 3x^2 - 1$	906	≥ 11	649177(fourth)
$11(2), \mathbf{17}$	$x^7 - x^6 - x^5 + 2x^3 + x^2 - 2x - 1$	882	≥ 10	661033
$11(2), \mathbf{23}$	$x^7 - 3x^6 + 5x^5 - 6x^4 + 3x^3 - x^2 - x + 1$	864	≥ 11	674057
$13(3), \mathbf{19}$	$x^7 - x^6 - x^5 + 3x^4 - 2x^3 + 2x - 1$	768	≥ 9	788857(sixteenth)
$11(6), \mathbf{17}$	$x^7 - x^6 - 4x^3 + 2x^2 + 2x - 1$	1908	≥ 13	-2932823 (seventh)
$\mathbf{17}^{**}$	$x^7 - x^6 - 2x^5 + 5x^4 - 6x^2 + x + 1$	1464	≥ 8	-3998639 (twentieth)

The case of septic fields

Conjecture: Let $N \geq 17$ be prime. Then there exist only finitely many fields $K/\mathbb{Q}$ of degree $d = 7$ with an elliptic curve E/K having a K-rational torsion point of order N and such that N does not divide $\prod_M c_M$.

The list of known such elliptic curves over septic fields:

N	field K (degree 7)	$ex(K)$	$M(K)$	$\mathrm{discr}(K)$
$11(6), 13, \mathbf{25}$	$x^7 - x^6 - x^5 + x^4 - x^2 + x + 1$	366	≥ 12	-184607 (first)
$11(2), 13, \mathbf{19}$	$x^7 - x^6 + x^3 - x + 1$	336	≥ 10	-199559 (fifth)
$11(2), 13, \mathbf{17}$	$x^7 - 2x^6 + 4x^5 - 4x^4 + 3x^3 - x^2 - x + 1$	270	≥ 8	-250367(sixteenth)
$11(6), \mathbf{23}$	$x^7 - 3x^5 - x^4 + 3x^3 + 1$	960	≥ 11	612569 (second)
$11(6), \mathbf{23}$	$x^7 - x^6 - x^4 + 3x^2 - 1$	906	≥ 11	649177(fourth)
$11(2), \mathbf{17}$	$x^7 - x^6 - x^5 + 2x^3 + x^2 - 2x - 1$	882	≥ 10	661033
$11(2), \mathbf{23}$	$x^7 - 3x^6 + 5x^5 - 6x^4 + 3x^3 - x^2 - x + 1$	864	≥ 11	674057
$13(3), \mathbf{19}$	$x^7 - x^6 - x^5 + 3x^4 - 2x^3 + 2x - 1$	768	≥ 9	788857(sixteenth)
$11(6), \mathbf{17}$	$x^7 - x^6 - 4x^3 + 2x^2 + 2x - 1$	1908	≥ 13	-2932823 (seventh)
$\mathbf{17}^{**}$	$x^7 - x^6 - 2x^5 + 5x^4 - 6x^2 + x + 1$	1464	≥ 8	-3998639 (twentieth)

Finitely many septic $K/\mathbb{Q}$ with $M(K) > 7$? $M(K) \leq 15$?

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N.

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Such an abelian surface is known to exist for $N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Such an abelian surface is known to exist for $N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Over $K = \mathbb{Q}(\zeta_7)^+$, an abelian surface A/K exists with $N = 31$ or 37.

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Such an abelian surface is known to exist for $N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Over $K = \mathbb{Q}(\zeta_7)^+$, an abelian surface A/K exists with $N = 31$ or 37.

Recall the situation for an elliptic curve $E/\mathbb{Q}$.
Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Such an abelian surface is known to exist for $N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Over $K = \mathbb{Q}(\zeta_7)^+$, an abelian surface A/K exists with $N = 31$ or 37.

Recall the situation for an elliptic curve $E/\mathbb{Q}$.
Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.
If $N = 5$, then N divides $c(E/\mathbb{Q})$, except when $E = X_1(11)$.

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Such an abelian surface is known to exist for $N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Over $K = \mathbb{Q}(\zeta_7)^+$, an abelian surface A/K exists with $N = 31$ or 37.

Recall the situation for an elliptic curve $E/\mathbb{Q}$.
Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.
If $N = 5$, then N divides $c(E/\mathbb{Q})$, except when $E = X_1(11)$.

Theorem (L.) *Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. If $N = 17$, or $N \geq 23$, then N divides $c(A/\mathbb{Q})$.*

Abelian surfaces over $\mathbb{Q}$

Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Such an abelian surface is known to exist for $N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Over $K = \mathbb{Q}(\zeta_7)^+$, an abelian surface A/K exists with $N = 31$ or 37.

Recall the situation for an elliptic curve $E/\mathbb{Q}$.
Theorem (L.) Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. If $N = 7, 8, 9, 10$, or 12, then N divides $c(E/\mathbb{Q})$.
If $N = 5$, then N divides $c(E/\mathbb{Q})$, except when $E = X_1(11)$.

Theorem (L.) *Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. If $N = 17$, or $N \geq 23$, then N divides $c(A/\mathbb{Q})$.*
If $N = 11, 13, 19$, there are cases where N does not divide $c(A/\mathbb{Q})$.

Known examples where N does not divide $c(A/\mathbb{Q})$

Known examples where N does not divide $c(A/\mathbb{Q})$

For $N = 11, 13$, and 19, there exist abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of prime order N where N does not divide $c(A/\mathbb{Q})$. In all known examples, $c(A/\mathbb{Q}) = 1$.

Known examples where N does not divide $c(A/\mathbb{Q})$

For $N = 11, 13,$ and 19, there exist abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of prime order N where N does not divide $c(A/\mathbb{Q})$. In all known examples, $c(A/\mathbb{Q}) = 1$.

$N = 19$: the only known example is $J_1(13)$.

Known examples where N does not divide $c(A/\mathbb{Q})$

For $N = 11, 13,$ and 19, there exist abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of prime order N where N does not divide $c(A/\mathbb{Q})$. In all known examples, $c(A/\mathbb{Q}) = 1$.

$N = 19$: the only known example is $J_1(13)$.

$N = 13$: only one known example.

Known examples where N does not divide $c(A/\mathbb{Q})$

For $N = 11, 13$, and 19, there exist abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of prime order N where N does not divide $c(A/\mathbb{Q})$. In all known examples, $c(A/\mathbb{Q}) = 1$.

$N = 19$: the only known example is $J_1(13)$.

$N = 13$: only one known example.

$N = 11$: *only four known examples*: one is conjecturally isogenous to $J_0(23)$, one is conjecturally a quotient of $J_1(67)$.

Known examples where N does not divide $c(A/\mathbb{Q})$

For $N = 11, 13$, and 19, there exist abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of prime order N where N does not divide $c(A/\mathbb{Q})$. In all known examples, $c(A/\mathbb{Q}) = 1$.

$N = 19$: the only known example is $J_1(13)$.

$N = 13$: only one known example.

$N = 11$: *only four known examples*: one is conjecturally isogenous to $J_0(23)$, one is conjecturally a quotient of $J_1(67)$.

Question. Are there only finitely many such abelian surfaces with $c(A/\mathbb{Q}) = 1$? (i.e., such that the Néron model of A has connected fibers)

THANKS!

Gracias!