# Ranks of elliptic curves with prescribed torsion over number fields

Filip Najman

University of Zagreb

joint work with J. Bosman, P. Bruin, A. Dujella

Warwick, September 27, 2012.

# Introduction

**Theorem (Mordell-Weil)** For an elliptic curve $E$ over a number field $K$, $E(K)$ is a finitely generated abelian group.

# Introduction

**Theorem (Mordell-Weil)** For an elliptic curve $E$ over a number field $K$, $E(K)$ is a finitely generated abelian group.

$E(K) \simeq T \oplus \mathbb{Z}^r$, where $T$ is the torsion subgroup and $r$ is the rank of $E(K)$.

# Introduction

**Theorem (Mordell-Weil)** For an elliptic curve $E$ over a number field $K$, $E(K)$ is a finitely generated abelian group.

$E(K) \simeq T \oplus \mathbb{Z}^r$, where $T$ is the torsion subgroup and $r$ is the rank of $E(K)$.

We want to understand what $T$ and $r$ can be and especially how they depend on each other.

# Elliptic curves over $\mathbb{Q}$

**Theorem (Mazur)** The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 10 \text{ or } 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 4.$$

# Elliptic curves over $\mathbb{Q}$

**Theorem (Mazur)** The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \ldots, 10 \text{ or } 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \ldots, 4.$$

For every torsion group $T$ from Mazur's theorem, there are infinitely many elliptic curves $E$ such that $E(\mathbb{Q})_{tors} \simeq T$. The moduli space of elliptic curves with torsion $T$ is a genus 0 curve.

# Elliptic curves over $\mathbb{Q}$

**Theorem (Mazur)** The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \ldots, 10 \text{ or } 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \ldots, 4.$$

For every torsion group $T$ from Mazur's theorem, there are infinitely many elliptic curves $E$ such that $E(\mathbb{Q})_{tors} \simeq T$. The moduli space of elliptic curves with torsion $T$ is a genus 0 curve.

It is not known which values $\operatorname{rk} E(\mathbb{Q})$ can attain and whether it is bounded at all.

# Elliptic curves over $\mathbb{Q}$

**Theorem (Mazur)** The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 10 \text{ or } 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 4.$$

For every torsion group $T$ from Mazur's theorem, there are infinitely many elliptic curves $E$ such that $E(\mathbb{Q})_{tors} \simeq T$. The moduli space of elliptic curves with torsion $T$ is a genus 0 curve.

It is not known which values $\operatorname{rk} E(\mathbb{Q})$ can attain and whether it is bounded at all.

The largest known rank of $E(\mathbb{Q})$ is 28 (Elkies).

# The dependence of the rank on the torsion - $\mathbb{Q}$

What can we say about the rank of an elliptic curve over $\mathbb{Q}$, about which we know nothing except for its torsion group?

# The dependence of the rank on the torsion - $\mathbb{Q}$

What can we say about the rank of an elliptic curve over $\mathbb{Q}$, about which we know nothing except for its torsion group?

Nothing!

# The dependence of the rank on the torsion - $\mathbb{Q}$

What can we say about the rank of an elliptic curve over $\mathbb{Q}$, about which we know nothing except for its torsion group?

Nothing!

The rank of this curve might be odd,

What can we say about the rank of an elliptic curve over $\mathbb{Q}$, about which we know nothing except for its torsion group?

Nothing!

The rank of this curve might be odd, even,

# The dependence of the rank on the torsion - $\mathbb{Q}$

What can we say about the rank of an elliptic curve over $\mathbb{Q}$, about which we know nothing except for its torsion group?

Nothing!

The rank of this curve might be odd, even, it might be 0,

## The dependence of the rank on the torsion - $\mathbb{Q}$

What can we say about the rank of an elliptic curve over $\mathbb{Q}$, about which we know nothing except for its torsion group?

Nothing!

The rank of this curve might be odd, even, it might be 0, or 10 billion.

$$B(T) = \sup\{\mathrm{rank}\,(E(\mathbb{Q})) \,:\, E(\mathbb{Q})_{\mathrm{tors}} \cong T\}$$

| $T$ | $B(T) \geq$ | Author(s) |
|---|---|---|
| 0 | 28 | Elkies (06) |
| $\mathbb{Z}/2\mathbb{Z}$ | 19 | Elkies (09) |
| $\mathbb{Z}/3\mathbb{Z}$ | 13 | Eroshkin (07,08,09) |
| $\mathbb{Z}/4\mathbb{Z}$ | 12 | Elkies (06) |
| $\mathbb{Z}/5\mathbb{Z}$ | 8 | Dujella & Lecacheux (09), Eroshkin (09) |
| $\mathbb{Z}/6\mathbb{Z}$ | 8 | Eroshkin (08), Dujella & Eroshkin (08), Elkies (08), Dujella (08) |
| $\mathbb{Z}/7\mathbb{Z}$ | 5 | Dujella & Kulesz (01), Elkies (06), Eroshkin (09,11), Dujella & Lecacheux (09), Dujella & Eroshkin (09) |
| $\mathbb{Z}/8\mathbb{Z}$ | 6 | Elkies (06) |
| $\mathbb{Z}/9\mathbb{Z}$ | 4 | Fisher (09) |
| $\mathbb{Z}/10\mathbb{Z}$ | 4 | Dujella (05,08), Elkies (06) |
| $\mathbb{Z}/12\mathbb{Z}$ | 4 | Fisher (08) |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | 15 | Elkies (09) |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | 8 | Elkies (05), Eroshkin (08), Dujella & Eroshkin (08) |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | 6 | Elkies (06) |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | 3 | Connell (00), Dujella (00,01,06,08), Campbell & Goins (03), Rathbun (03,06), Flores, Jones, Rollick & Weigandt (07), Fisher (09) |

# Elliptic curves over number fields

We can study elliptic curves over number fields in essentially two ways: we can look at elliptic curves over a fixed number field, or we can look at all elliptic curves over all number fields of given degree $d$.

# Elliptic curves over number fields

We can study elliptic curves over number fields in essentially two ways: we can look at elliptic curves over a fixed number field, or we can look at all elliptic curves over all number fields of given degree $d$.

Over number fields, in both cases:

1. For some torsion groups $T$, there are finitely many elliptic curves with given torsion

# Elliptic curves over number fields

We can study elliptic curves over number fields in essentially two ways: we can look at elliptic curves over a fixed number field, or we can look at all elliptic curves over all number fields of given degree $d$.

Over number fields, in both cases:

1. For some torsion groups $T$, there are finitely many elliptic curves with given torsion
2. The torsion can tell us something about the rank

# Modular curves

$Y_1(m,n)$ - affine curve whose $K$-rational points classify isomorphism classes of elliptic curves $E$ with a pair $(P,R)$, where $P,R \in E(K)$ generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

# Modular curves

$Y_1(m,n)$ - affine curve whose $K$-rational points classify isomorphism classes of elliptic curves $E$ with a pair $(P,R)$, where $P,R \in E(K)$ generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

$X_1(m,n) = Y_1(m,n) \cup \{\text{cusps}\}$. We write $X_1(1,n) = X_1(n)$.

# Modular curves

$Y_1(m,n)$ - affine curve whose $K$-rational points classify isomorphism classes of elliptic curves $E$ with a pair $(P,R)$, where $P,R \in E(K)$ generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

$X_1(m,n) = Y_1(m,n) \cup \{\text{cusps}\}$. We write $X_1(1,n) = X_1(n)$.

For all but finitely many $(m,n)$ (take $n \geq 16$), $X_1(m,n)$ is a curve of genus $\geq 2$, so will, by Faltings' theorem, have only finitely many points over any number field $K$.

# Modular curves

$Y_1(m,n)$ - affine curve whose $K$-rational points classify isomorphism classes of elliptic curves $E$ with a pair $(P,R)$, where $P,R \in E(K)$ generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

$X_1(m,n) = Y_1(m,n) \cup \{\text{cusps}\}$. We write $X_1(1,n) = X_1(n)$.

For all but finitely many $(m,n)$ (take $n \geq 16$), $X_1(m,n)$ is a curve of genus $\geq 2$, so will, by Faltings' theorem, have only finitely many points over any number field $K$.

Hence, over a fixed number field over which some curve has $n$-torsion, for such $n$, there will be only finitely many such curves.

# The torsion determines the rank over fixed number fields

When we have finitely many curves with prescribed torsion, then it is not very surprising that we can say something about the rank, for example that it is bounded.

# The torsion determines the rank over fixed number fields

When we have finitely many curves with prescribed torsion, then it is not very surprising that we can say something about the rank, for example that it is bounded.

For example, there is exactly one elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(\sqrt{5})$ and this curve has rank 0.

# The torsion determines the rank over fixed number fields

When we have finitely many curves with prescribed torsion, then it is not very surprising that we can say something about the rank, for example that it is bounded.

For example, there is exactly one elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(\sqrt{5})$ and this curve has rank 0.

$$E(\mathbb{Q}(\sqrt{5}))_{tors} = \mathbb{Z}/15\mathbb{Z} \Longrightarrow \mathrm{rk}(E(\mathbb{Q}(\sqrt{5}))) = 0.$$

# The torsion determines the rank over fixed number fields

When we have finitely many curves with prescribed torsion, then it is not very surprising that we can say something about the rank, for example that it is bounded.

For example, there is exactly one elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(\sqrt{5})$ and this curve has rank 0.

$$E(\mathbb{Q}(\sqrt{5}))_{tors} = \mathbb{Z}/15\mathbb{Z} \Longrightarrow \mathrm{rk}(E(\mathbb{Q}(\sqrt{5}))) = 0.$$

Similarly, there is one ellitpic curve with torison $\mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(i, \sqrt{5})$ and one can show that

$$E(\mathbb{Q}(i, \sqrt{5}))_{tors} = \mathbb{Z}/15\mathbb{Z} \Longrightarrow \mathrm{rk}(E(\mathbb{Q}(i, \sqrt{5}))) = 1.$$

# Torsion of elliptic curves over fixed quadratic fields

**Theorem (N.)**

a) The torsion of an elliptic curve over $\mathbb{Q}(i)$ is isomorphic either to one of the groups from Mazur's theorem or to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.
b) The torsion of an elliptic curve over $\mathbb{Q}(\sqrt{-3})$ is isomorphic either to one of the groups from Mazur's theorem, or to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

**Theorem (Kenku & Momose, Kamienny)** Let $E$ be an elliptic curve over a quadratic field $K$. The torsion of $E(K)$ is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 16 \text{ or } 18,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 6,$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \text{ where } n = 1 \text{ or } 2,$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

# Torsion of elliptic curves over number fields of degree $d$

**Theorem (Kenku & Momose, Kamienny)** Let $E$ be an elliptic curve over a quadratic field $K$. The torsion of $E(K)$ is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 16 \text{ or } 18,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 6,$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \text{ where } n = 1 \text{ or } 2,$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

All of these groups appear as torsion groups for infinitely many nonisomorphic elliptic curves over quadratic fields.

# Sporadic points on $X_1$

The gonality of a curve $X$ is the lowest degree of a rational map from $X$ to $\mathbb{P}^1$. We call points on $X_1(m, n)$ which have degree smaller than the gonality of $X_1(m, n)$ *sporadic*.

# Sporadic points on $X_1$

The gonality of a curve $X$ is the lowest degree of a rational map from $X$ to $\mathbb{P}^1$. We call points on $X_1(m,n)$ which have degree smaller than the gonality of $X_1(m,n)$ *sporadic*.

Mazur, Kenku-Momose and Kamienny - no degree 1 or 2 sporadic points.

# Sporadic points on $X_1$

The gonality of a curve $X$ is the lowest degree of a rational map from $X$ to $\mathbb{P}^1$. We call points on $X_1(m, n)$ which have degree smaller than the gonality of $X_1(m, n)$ *sporadic*.

Mazur, Kenku-Momose and Kamienny - no degree 1 or 2 sporadic points.

Van Hoeij - there are degree 9 points on $X_1(29)$ and $X_1(31)$, which have gonality 11 and 12, respectively.

# Sporadic points on $X_1$

The gonality of a curve $X$ is the lowest degree of a rational map from $X$ to $\mathbb{P}^1$. We call points on $X_1(m, n)$ which have degree smaller than the gonality of $X_1(m, n)$ *sporadic*.

Mazur, Kenku-Momose and Kamienny - no degree 1 or 2 sporadic points.

Van Hoeij - there are degree 9 points on $X_1(29)$ and $X_1(31)$, which have gonality 11 and 12, respectively.

What is the minimal $d$ such that there is a degree $d$ sporadic point? From above it is $\leq 9$, and from Mazur, Kenku-Momose and Kamienny, it is $\geq 3$.

# Sporadic points on $X_1$

The gonality of a curve $X$ is the lowest degree of a rational map from $X$ to $\mathbb{P}^1$. We call points on $X_1(m,n)$ which have degree smaller than the gonality of $X_1(m,n)$ *sporadic*.

Mazur, Kenku-Momose and Kamienny - no degree 1 or 2 sporadic points.

Van Hoeij - there are degree 9 points on $X_1(29)$ and $X_1(31)$, which have gonality 11 and 12, respectively.

What is the minimal $d$ such that there is a degree $d$ sporadic point? From above it is $\leq 9$, and from Mazur, Kenku-Momose and Kamienny, it is $\geq 3$.

It is exactly 3!

**Theorem (Jeon, Kim & Schweizer)**

When we run through all elliptic curves over all cubic fields the groups that appear infinitely often are exactly

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 16, \ 18, \text{ or } 20$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 7,$$

# Sporadic points on $X_1$

**Theorem (Jeon, Kim & Schweizer)**
When we run through all elliptic curves over all cubic fields the groups that appear infinitely often are exactly

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \ldots, 16, \ 18, \text{ or } 20$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \ldots, 7,$$

All the corresponding modular curves are of gonality $\leq 3$.

# Sporadic points on $X_1$

**Theorem (Jeon, Kim & Schweizer)**
When we run through all elliptic curves over all cubic fields the groups that appear infinitely often are exactly

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 16, \ 18, \text{ or } 20$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 7,$$

All the corresponding modular curves are of gonality $\leq 3$.

$\exists!$ pair $(E, K)$, where $E/\mathbb{Q}$ is an elliptic curve, $K$ a cubic field and $E(K)_{tors} \simeq \mathbb{Z}/21\mathbb{Z}$, so $X_1(21)$ has a sporadic point. $X_1(21)$ has gonality 4.

# Sporadic points on $X_1$

**Theorem (Jeon, Kim & Schweizer)**
When we run through all elliptic curves over all cubic fields the groups that appear infinitely often are exactly

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \ldots, 16, \ 18, \text{ or } 20$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \ldots, 7,$$

All the corresponding modular curves are of gonality $\leq 3$.

$\exists!$ pair $(E, K)$, where $E/\mathbb{Q}$ is an elliptic curve, $K$ a cubic field and $E(K)_{tors} \simeq \mathbb{Z}/21\mathbb{Z}$, so $X_1(21)$ has a sporadic point. $X_1(21)$ has gonality 4.

The unique curve with 21-torsion is 162B1 over the field defined by $x^3 - 3x^2 + 3$ (which is $\mathbb{Q}(\zeta_9)^+$.)

# Sporadic points on $X_1$

**Theorem (Jeon, Kim & Schweizer)**
When we run through all elliptic curves over all cubic fields the groups that appear infinitely often are exactly

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \dots, 16, \ 18, \text{ or } 20$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \dots, 7,$$

All the corresponding modular curves are of gonality $\leq 3$.

$\exists!$ pair $(E, K)$, where $E/\mathbb{Q}$ is an elliptic curve, $K$ a cubic field and $E(K)_{tors} \simeq \mathbb{Z}/21\mathbb{Z}$, so $X_1(21)$ has a sporadic point. $X_1(21)$ has gonality 4.

The unique curve with 21-torsion is 162B1 over the field defined by $x^3 - 3x^2 + 3$ (which is $\mathbb{Q}(\zeta_9)^+$.)

There might be other elliptic curves (not defined over $\mathbb{Q}$) with 21-torsion over cubic fields, but there can be only finitely many.

# The result

**Theorem (Bosman, Bruin, Dujella, N.)**

1. Any elliptic curve over any quadratic field with a point of order 13 or 18 has even rank.

# The result

**Theorem (Bosman, Bruin, Dujella, N.)**

1. Any elliptic curve over any quadratic field with a point of order 13 or 18 has even rank.
2. Any elliptic curve over any quartic field with a point of order 22 has even rank.

# Complex multiplication

We want a systematic way to say something about the rank of elliptic curves with given torsion over all number fields of fixed degree $d$.

# Complex multiplication

We want a systematic way to say something about the rank of elliptic curves with given torsion over all number fields of fixed degree $d$.

Let $E$ be an elliptic curve with complex multiplication by an order $O$ of an imaginary quadratic number field $K$. If $L$ is a number field containing $K$, then $E(L)$ is not just a $\mathbb{Z}$-module, but also an $O$-module.

# Complex multiplication

We want a systematic way to say something about the rank of elliptic curves with given torsion over all number fields of fixed degree $d$.

Let $E$ be an elliptic curve with complex multiplication by an order $O$ of an imaginary quadratic number field $K$. If $L$ is a number field containing $K$, then $E(L)$ is not just a $\mathbb{Z}$-module, but also an $O$-module.

As a result, if $E(L)$ is a $O$-module of rank $n$, it is a $\mathbb{Z}$-module of rank $2n$, so the rank of $E(L)$ is necessarily even.

# Restriction of scalars

Let $A$ be an abelian variety defined over $L$, where $L/K$ is a finite Galois extension of number fields.

# Restriction of scalars

Let $A$ be an abelian variety defined over $L$, where $L/K$ is a finite Galois extension of number fields.

Weil's restriction of scalars $\operatorname{Res}_{L/K} A$ is an abelian variety defined over the smaller field $K$, but with larger dimension, with the property that

$$\operatorname{Res}_{L/K} A(K) \simeq A(L).$$

# An example

Let $E : y^2 = x^3 + i$. If we want to find $E(\mathbb{Q}(i))$, we are looking for the solutions of $(c + di)^2 = (a + bi)^3 + i$, or in other words

$$c^2 + 2cdi - d^2 = a^3 + 3a^2bi - 3ab^2 - b^3i + i,$$

# An example

Let $E : y^2 = x^3 + i$. If we want to find $E(\mathbb{Q}(i))$, we are looking for the solutions of $(c + di)^2 = (a + bi)^3 + i$, or in other words

$$c^2 + 2cdi - d^2 = a^3 + 3a^2bi - 3ab^2 - b^3i + i,$$

So we get

$$a^3 - 3ab^2 - c^2 + d^2 = 0, \tag{1}$$

$$2cd + 3a^2b + b^3 - 1 = 0. \tag{2}$$

$\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}} E$ is the abelian variety defined by equations (1) and (2).

# False complex multiplication

In a similar way as with elliptic curves with CM, if $\mathrm{End}(\mathrm{Res}_{L/K} E)$ contians an order of a quadratic field, this implies that

$$\mathrm{Res}_{L/K} E(K) \simeq E(L)$$

is a $\mathbb{Z}$-module of even rank.

# False complex multiplication

In a similar way as with elliptic curves with CM, if $\mathrm{End}(\mathrm{Res}_{L/K} E)$ contians an order of a quadratic field, this implies that

$$\mathrm{Res}_{L/K} E(K) \simeq E(L)$$

is a $\mathbb{Z}$-module of even rank.

We call this *false complex multiplication*.

# $\mathbb{Q}$-curves

An elliptic curve $E$ which is isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates is called a $\mathbb{Q}$-curve.

An elliptic curve $E$ which is isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates is called a $\mathbb{Q}$-curve.

Let $E$ be a $\mathbb{Q}$-curve defined over a quadratic field $K$, such that $\phi : E \to E^{\sigma}$ is an isogeny of degree $n$, where $\langle \sigma \rangle = \mathrm{Gal}(K/\mathbb{Q})$.

# $\mathbb{Q}$-curves

An elliptic curve $E$ which is isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates is called a $\mathbb{Q}$-curve.

Let $E$ be a $\mathbb{Q}$-curve defined over a quadratic field $K$, such that $\phi : E \to E^\sigma$ is an isogeny of degree $n$, where $\langle \sigma \rangle = \mathrm{Gal}(K/\mathbb{Q})$.

$\mathrm{Res}_{K/\mathbb{Q}} E$ is isomorphic over $K$ to $E \times E^\sigma$ and if $n$ is not a square then it will follow that $E$ has false CM.

# $\mathbb{Q}$-curves

An elliptic curve $E$ which is isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates is called a $\mathbb{Q}$-curve.

Let $E$ be a $\mathbb{Q}$-curve defined over a quadratic field $K$, such that $\phi : E \to E^\sigma$ is an isogeny of degree $n$, where $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$.

$\mathrm{Res}_{K/\mathbb{Q}} E$ is isomorphic over $K$ to $E \times E^\sigma$ and if $n$ is not a square then it will follow that $E$ has false CM.

Note that $\sigma \circ \phi : E(K) \to E(K)$ is a homomorphism of groups which is not multiplication-by-$m$, since $|\operatorname{Ker} \sigma \circ \phi|$ is non-square.

# Elliptic curves with points of order 18

The modular curve $X_1(18)$ is hyperelliptic of genus 2 with hyperelliptic involution $w_2$.

The modular curve $X_1(18)$ is hyperelliptic of genus 2 with hyperelliptic involution $w_2$.

Fix a cusp $C \in X_1(18)(\mathbb{Q})$. We look at the map

$$f : \operatorname{Sym}^2 X_1(18) \to J_1(18),$$

$$\{P, Q\} \to [P + Q - C - w_2(C)],$$

which is an isomorphism away from the fibre above 0 which consists of the pairs of points $\{P, w_2(P)\}$ which are fixed by the hyperelliptic involution $w_2$.

# Elliptic curves with points of order 18

The modular curve $X_1(18)$ is hyperelliptic of genus 2 with hyperelliptic involution $w_2$.

Fix a cusp $C \in X_1(18)(\mathbb{Q})$. We look at the map

$$f : \mathrm{Sym}^2 X_1(18) \to J_1(18),$$

$$\{P, Q\} \to [P + Q - C - w_2(C)],$$

which is an isomorphism away from the fibre above 0 which consists of the pairs of points $\{P, w_2(P)\}$ which are fixed by the hyperelliptic involution $w_2$.

As $J_1(18)(\mathbb{Q}) \simeq \mathbb{Z}/21\mathbb{Z}$, we can check that the inverse image of any point except 0 is a pair of cusps. Let $K$ be a quadratic field, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$.

# Elliptic curves with points of order 18

The modular curve $X_1(18)$ is hyperelliptic of genus 2 with hyperelliptic involution $w_2$.

Fix a cusp $C \in X_1(18)(\mathbb{Q})$. We look at the map

$$f : \operatorname{Sym}^2 X_1(18) \to J_1(18),$$

$$\{P, Q\} \to [P + Q - C - w_2(C)],$$

which is an isomorphism away from the fibre above 0 which consists of the pairs of points $\{P, w_2(P)\}$ which are fixed by the hyperelliptic involution $w_2$.

As $J_1(18)(\mathbb{Q}) \simeq \mathbb{Z}/21\mathbb{Z}$, we can check that the inverse image of any point except 0 is a pair of cusps. Let $K$ be a quadratic field, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$.

Now take a non-cusp point $Q$ in $X_1(18)(K)$. Then $f(\{Q, Q^\sigma\}) \in J_1(18)(\mathbb{Q})$, thus it has to be 0, so $Q^\sigma = w_2(Q)$.

# Elliptic curves with points of order 18

If in the moduli interpretation of $Q \in X_1(18)$ represents $E$, then $Q^\sigma$ represents $E^\sigma$ and $w_2(Q)$ represents a curve that is 2-isogenous to $E$.

# Elliptic curves with points of order 18

If in the moduli interpretation of $Q \in X_1(18)$ represents $E$, then $Q^\sigma$ represents $E^\sigma$ and $w_2(Q)$ represents a curve that is 2-isogenous to $E$.

Hence, all elliptic curves with a point of order 18 are isogenous to their Galois conjugate by an isogeny of degree 2.

# Elliptic curves with points of order 18

If in the moduli interpretation of $Q \in X_1(18)$ represents $E$, then $Q^\sigma$ represents $E^\sigma$ and $w_2(Q)$ represents a curve that is 2-isogenous to $E$.

Hence, all elliptic curves with a point of order 18 are isogenous to their Galois conjugate by an isogeny of degree 2.

It follows that all elliptic curves with a point of order 18 over quadratic fields have false CM. It can be shown that

$$\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}} E) \simeq \mathbb{Z}[\sqrt{-2}]$$

for all such curves $E$.

# Elliptic curves with points of order 18

If in the moduli interpretation of $Q \in X_1(18)$ represents $E$, then $Q^\sigma$ represents $E^\sigma$ and $w_2(Q)$ represents a curve that is 2-isogenous to $E$.

Hence, all elliptic curves with a point of order 18 are isogenous to their Galois conjugate by an isogeny of degree 2.

It follows that all elliptic curves with a point of order 18 over quadratic fields have false CM. It can be shown that

$$\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}} E) \simeq \mathbb{Z}[\sqrt{-2}]$$

for all such curves $E$.

So, all elliptic curves with torsion $\mathbb{Z}/18\mathbb{Z}$ over quadratic fields have even rank.

# Elliptic curves with points of order 18

The modular curve $X_1(18)$ has a model

$$X_1(18) : y^2 = f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 \quad (3)$$

The modular curve $X_1(18)$ has a model

$$X_1(18) : y^2 = f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 \quad (3)$$

As we have seen, the only quadratic points on $X_1(18)$ are the ones fixed by the hyperelliptic involution. These are the points in the model (3) with rational $x$-s.

# Elliptic curves with points of order 18

The modular curve $X_1(18)$ has a model

$$X_1(18) : y^2 = f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 \quad (3)$$

As we have seen, the only quadratic points on $X_1(18)$ are the ones fixed by the hyperelliptic involution. These are the points in the model (3) with rational $x$-s.

But for every $x \in \mathbb{R}$, $f(x)$ is positive. As all the quadratic points are of the form $(x, \sqrt{f(x)})$, $x \in \mathbb{Q}$, this implies that all of them are defined over real quadratic fields.

# Elliptic curves with points of order 13

The modular curve $X_1(13)$ is hyperelliptic of genus 2 with hyperelliptic involution $\langle 5 \rangle$.

# Elliptic curves with points of order 13

The modular curve $X_1(13)$ is hyperelliptic of genus 2 with hyperelliptic involution $\langle 5 \rangle$.

It can be shown that for every point $P \in Y_1(13)(K)$, $\langle 5 \rangle P = P^\sigma$.

# Elliptic curves with points of order 13

The modular curve $X_1(13)$ is hyperelliptic of genus 2 with hyperelliptic involution $\langle 5 \rangle$.

It can be shown that for every point $P \in Y_1(13)(K)$, $\langle 5 \rangle P = P^\sigma$.

This implies that an elliptic curve $E$ with a point of order 13 over a quadratic field $K$ is *isomorphic* to its Galois conjugate $E^\sigma$, and

$$\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}} E) \simeq \mathbb{Z}[\sqrt{-1}].$$

# Elliptic curves with points of order 13

The modular curve $X_1(13)$ is hyperelliptic of genus 2 with hyperelliptic involution $\langle 5 \rangle$.

It can be shown that for every point $P \in Y_1(13)(K)$, $\langle 5 \rangle P = P^\sigma$.

This implies that an elliptic curve $E$ with a point of order 13 over a quadratic field $K$ is *isomorphic* to its Galois conjugate $E^\sigma$, and

$$\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}} E) \simeq \mathbb{Z}[\sqrt{-1}].$$

It follows that all elliptic curves over quadratic fields with a point of order 13 have even rank.

# Elliptic curves with points of order 13

In exactly the same way as for elliptic curves with $\mathbb{Z}/18\mathbb{Z}$ torsion, it can be shown that elliptic curves with 13-torsion cannot exist over imaginary quadratic fields.

# Elliptic curves with a point of order 22 over quartic fields

The modular curve $X_1(22)$ is a genus 6 curve, which is *bielliptic*, meaning that it has a degree 2 map to an elliptic curve (11A3 in this case).

# Elliptic curves with a point of order 22 over quartic fields

The modular curve $X_1(22)$ is a genus 6 curve, which is *bielliptic*, meaning that it has a degree 2 map to an elliptic curve (11A3 in this case).

It can be shown that all quartic points on $Y_1(22)$ correspond to quadratic points on $Y_1(22)/\iota$.

# Elliptic curves with a point of order 22 over quartic fields

The modular curve $X_1(22)$ is a genus 6 curve, which is *bielliptic*, meaning that it has a degree 2 map to an elliptic curve (11A3 in this case).

It can be shown that all quartic points on $Y_1(22)$ correspond to quadratic points on $Y_1(22)/\iota$.

The moduli interpretation of $Y_1(22)/\iota$ implies that every elliptic curve with a point of order 22 over a quartic field $L$ is a $K$-curve (meaning that it is isogenous to all of its $\mathrm{Gal}(\overline{K}/K)$-conjugates), where $K$ is a quadratic subfield of $L$.

# Elliptic curves with a point of order 22 over quartic fields

The modular curve $X_1(22)$ is a genus 6 curve, which is *bielliptic*, meaning that it has a degree 2 map to an elliptic curve (11A3 in this case).

It can be shown that all quartic points on $Y_1(22)$ correspond to quadratic points on $Y_1(22)/\iota$.

The moduli interpretation of $Y_1(22)/\iota$ implies that every elliptic curve with a point of order 22 over a quartic field $L$ is a $K$-curve (meaning that it is isogenous to all of its $\mathrm{Gal}(\overline{K}/K)$-conjugates), where $K$ is a quadratic subfield of $L$.

Furthermore, $\mathrm{End}(\mathrm{Res}_{L/K} E) \simeq \mathbb{Z}[\sqrt{-2}]$ , so it follows that every elliptic curve with a point of order 22 over a quartic field has even rank.

Thank you for your attention!