Ranks of elliptic curves over number fields

Filip Najman

University of Zagreb

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

Dubrovnik, 23.6.2025.



This work was supported by the Croatian Science Foundation under the project number HRZZ IP-2022-10-5008.

History of the paper

Work on this project began while I was a PhD student of Andrej in 2010.

History of the paper

Work on this project began while I was a PhD student of Andrej in 2010.

I was very fortunate to have Andrej as my PhD advisor. He was always ready to help, answering numerous emails in any time of day (and night).

History of the paper

Work on this project began while I was a PhD student of Andrej in 2010.

I was very fortunate to have Andrej as my PhD advisor. He was always ready to help, answering numerous emails in any time of day (and night).

More importantly Andrej is a very nice person: very geneorus, kind, always joking, never judgemental.

History of the paper

Work on this project began while I was a PhD student of Andrej in 2010.

I was very fortunate to have Andrej as my PhD advisor. He was always ready to help, answering numerous emails in any time of day (and night).

More importantly Andrej is a very nice person: very geneorus, kind, always joking, never judgemental.

Andrej created the (today very numerous) number theory group in Zagreb from nothing. At the time it was very active, Andrej had many PhD students, multiple bilateral projects with Debrecen, Graz and Strasbourg, with guests visiting and giving seminars all the time.

History of the paper

Work on this project began while I was a PhD student of Andrej in 2010.

I was very fortunate to have Andrej as my PhD advisor. He was always ready to help, answering numerous emails in any time of day (and night).

More importantly Andrej is a very nice person: very geneorus, kind, always joking, never judgemental.

Andrej created the (today very numerous) number theory group in Zagreb from nothing. At the time it was very active, Andrej had many PhD students, multiple bilateral projects with Debrecen, Graz and Strasbourg, with guests visiting and giving seminars all the time.

After Andrej, certainly the most important person in the number theory group in Zagreb was Ivica; I had the privilege of attending his PhD course on the arithmetic of elliptic curves. At around the same time Borka started the number theory group in Split.

Some pictures



Graz, 2008.

Some pictures



Saint Etienne, 2009.

Some pictures



Vinko's PhD defense, 2011.

Some pictures



After Vinko's PhD defense, 2011.

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 $E(K)$.

For $E/\mathbb{Q}$, by Mazur's theorem, all the possible group structures of $E(\mathbb{Q})_{tors}$ are known, and it was proven by Merel that there is a bound on the size of the torsion of $E(K)$, depending only on $[K : \mathbb{Q}]$.

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 $E(K)$.

For $E/\mathbb{Q}$, by Mazur's theorem, all the possible group structures of $E(\mathbb{Q})_{tors}$ are known, and it was proven by Merel that there is a bound on the size of the torsion of $E(K)$, depending only on $[K : \mathbb{Q}]$.

It is not known which values the rank of a $E(\mathbb{Q})$ attains, and whether there is an upper bound for the rank.

Rank records

I, like many others, was inspired by Andrej's webpage about rank records of elliptic curves with prescribed torsion groups over $\mathbb{Q}$.

T	$B(T)>=$	Author(s)
0	29	Elkies - Klagsbrun (2024)
Z/2Z	20	Elkies - Klagsbrun (2020)
Z/3Z	15	Elkies - Klagsbrun (2020)
Z/4Z	13	Elkies - Klagsbrun (2020)
Z/5Z	9	Klagsbrun (2020)
Z/6Z	9	Klagsbrun (2020), Voznyy (2020)
Z/7Z	6	Klagsbrun (2020)
Z/8Z	6	Elkies (2006), Dujella - MacLeod - Peral (2013), Voznyy (2021)
Z/9Z	4	Fisher (2009), van Beek (2015), Dujella - Petricevic (2021), Dujella - Petricevic - Rathbun (2022)
Z/10Z	4	Dujella (2005,2008), Elkies (2006), Fisher (2016)
Z/12Z	4	Fisher (2008)
Z/2Z × Z/2Z	15	Elkies (2009)
Z/2Z × Z/4Z	9	Dujella - Peral (2012,2019), Klagsbrun (2020)
Z/2Z × Z/6Z	6	Elkies (2006), Dujella - Peral - Tadic (2015), Dujella - Peral (2020)
Z/2Z × Z/8Z	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell - Goins (2003), Rathbun (2003,2006,2013,2022), Dujella - Rathbun (2006), Flores - Jones - Rollick - Weigandt - Rathbun (2007), Fisher (2009), AttarBashi - Rathbun - Voznyy (2022), AttarBashi - Fisher - Rathbun - Voznyy (2022), AttarBashi - Fisher - Voznyy (2022)

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

It is a natural question to ask how the rank of an elliptic curve depends on the torsion.

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

It is a natural question to ask how the rank of an elliptic curve depends on the torsion.

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 - $\mathbb{Q}$

It is a natural question to ask how the rank of an elliptic curve depends on the torsion.

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 - $\mathbb{Q}$

It is a natural question to ask how the rank of an elliptic curve depends on the torsion.

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!

We will show that we the same is not true for number fields.

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

It is a natural question to ask how the rank of an elliptic curve depends on the torsion.

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!

We will show that we the same is not true for number fields.

In particular we will show that all elliptic curves over quadratic fields with points of order 13 or 18 have even rank. There are infinitely many such curves.

Complex multiplication

Let E be an elliptic curve with complex multiplication by an order O of an imaginary quadratic 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

Let E be an elliptic curve with complex multiplication by an order O of an imaginary quadratic 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 it 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 $\mathrm{Res}_{L/K} A$ is an abelian variety defined over the smaller field K, but with larger dimension, with the property that

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

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.

$\mathbb{Q}$-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 defined over K, 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 defined over K, where $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$.

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

$\mathbb{Q}$-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 defined over K, where $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$.

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

$\mathrm{Res}_{K/\mathbb{Q}} E$ is isomorphic over K to $E \times E^\sigma$ and it follows 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 defined over K, where $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$.

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

$\mathrm{Res}_{K/\mathbb{Q}} E$ is isomorphic over K to $E \times E^\sigma$ and it follows that E has false CM.

Hence such E will have even rank over K.

Elliptic curves with points of order 18

$Y_1(n)$ - the affine modular curve whose K-rational points classify the isomorphism classes of pairs (E, P), where E/K is an elliptic curve and $P \in E(K)$ is a point of order n.

Elliptic curves with points of order 18

$Y_1(n)$ - the affine modular curve whose K-rational points classify the isomorphism classes of pairs (E, P), where E/K is an elliptic curve and $P \in E(K)$ is a point of order n.

$X_1(n)$ - the compactification of $Y_1(n)$.

Elliptic curves with points of order 18

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

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.

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.

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^σ represents E^σ 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^σ represents E^σ 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^σ represents E^σ 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^σ represents E^σ 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

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

Elliptic curves with points of order 18

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

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

As we have seen, the only quadratic points on $X_1(18)$ are the ones such that $Q^\sigma = w_2(Q)$, so if $Q = (x, y)$ we have

$$(x^\sigma, y^\sigma) = (x, y)^\sigma = w_2(x, y) = (x, -y).$$

Elliptic curves with points of order 18

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

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

As we have seen, the only quadratic points on $X_1(18)$ are the ones such that $Q^\sigma = w_2(Q)$, so if $Q = (x, y)$ we have

$$(x^\sigma, y^\sigma) = (x, y)^\sigma = w_2(x, y) = (x, -y).$$

These are the points in the model above with rational x-s.

Elliptic curves with points of order 18

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

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

As we have seen, the only quadratic points on $X_1(18)$ are the ones such that $Q^\sigma = w_2(Q)$, so if $Q = (x, y)$ we have

$$(x^\sigma, y^\sigma) = (x, y)^\sigma = w_2(x, y) = (x, -y).$$

These are the points in the model above 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.

Similar results for other groups

Elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$ over quadratic fields are all defined over real quadratic fields, and all of them have even rank.

Similar results for other groups

Elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$ over quadratic fields are all defined over real quadratic fields, and all of them have even rank.

Elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields are all base changes of elliptic curves defined over $\mathbb{Q}$.

Similar results for other groups

Elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$ over quadratic fields are all defined over real quadratic fields, and all of them have even rank.

Elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields are all base changes of elliptic curves defined over $\mathbb{Q}$.

The common reason is that the modular curve $X_1(n)$ is hyperelliptic for (and only for!) $n = 13, 16$ and 18.

Similar results for other groups

Elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$ over quadratic fields are all defined over real quadratic fields, and all of them have even rank.

Elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields are all base changes of elliptic curves defined over $\mathbb{Q}$.

The common reason is that the modular curve $X_1(n)$ is hyperelliptic for (and only for!) $n = 13, 16$ and 18.

Elliptic curves with torsion $\mathbb{Z}/22\mathbb{Z}$ over quartic fields all have even rank.

Similar results for other groups

Elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$ over quadratic fields are all defined over real quadratic fields, and all of them have even rank.

Elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields are all base changes of elliptic curves defined over $\mathbb{Q}$.

The common reason is that the modular curve $X_1(n)$ is hyperelliptic for (and only for!) $n = 13, 16$ and 18.

Elliptic curves with torsion $\mathbb{Z}/22\mathbb{Z}$ over quartic fields all have even rank.

The modular curve $X_1(22)$ is a genus 6 bielliptic curve.

Final remarks

As far as I know, these are the only known instances where some property of the elliptic curve, not explained by the BSD conjecture, affects the rank of an elliptic curve.

Are there any more such examples?

Thank you for your attention!

Happy birthdays to Andrej,
Borka and Ivica!