Isogenies over quadratic fields of elliptic curves with rational j-invariant

Borna Vukorepa

Faculty of science
Department of mathematics
University of Zagreb

5. 5. 2022.

Funding

Funding

This work was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Program (Grant KK.01.1.1.01.0004).

Za više informacija posjetite:
http://bela.phy.hr/quantixlie/hr/
https://strukturnifondovi.hr/

For more information:
http://bela.phy.hr/quantixlie/hr/
https://strukturnifondovi.hr/

Sadržaj ove prezentacije isključiva je odgovornost Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije.

The content of this presentation is exclusive responsibility of the Faculty of Science University of Zagreb and does not represent opinion of the European Union

EUROPSKA UNIJA
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

Operativni program KONKURENTNOST I KOHEZIJA

Projekt sufinancira Europska unija iz Europskog fonda

Project co-financed by European Union through the

Known results about isogenies

Theorem 1.1 (Mazur, Kenku et. al.)

Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over $\mathbb{Q}$. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication (CM), then $n \leq 18$ uz $n \neq 14$ or $n \in \{21, 25, 37\}$.

Known results about isogenies

Theorem 1.1 (Mazur, Kenku et. al.)

Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over $\mathbb{Q}$. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication (CM), then $n \leq 18$ uz $n \neq 14$ or $n \in \{21, 25, 37\}$.

- Ordered pairs $(E/K, C)$, where C is a cyclic subgroup defined over number field K of order n, are parametrized by noncuspidal K-rational points on the modular curve $X_0(n)$.

Known results about isogenies

Theorem 1.1 (Mazur, Kenku et. al.)

Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over $\mathbb{Q}$. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication (CM), then $n \leq 18$ uz $n \neq 14$ or $n \in \{21, 25, 37\}$.

- Ordered pairs $(E/K, C)$, where C is a cyclic subgroup defined over number field K of order n, are parametrized by noncuspidal K-rational points on the modular curve $X_0(n)$.
- It is natural to ask ourselves the same question for number fields K other than $\mathbb{Q}$, but all the K-rational points on all $X_0(n)$ have only been determined for $K = \mathbb{Q}$.

Known results about isogenies

Theorem 1.2 (Momose)

Let K be a quadratic extension of $\mathbb{Q}$ which is not imaginary with class number equal to 1. Then $X_0(p)(K)$ contains noncuspidal points for only finitely many primes p.

Theorem 1.2 (Momose)

Let K be a quadratic extension of $\mathbb{Q}$ which is not imaginary with class number equal to 1. Then $X_0(p)(K)$ contains noncuspidal points for only finitely many primes p.

- Using the properties of hyperelliptic and Atkin-Lehner involutions, Najman and Bruin determined all the quadratic points on all hyperelliptic $X_0(n)$ for which $J_0(n)(\mathbb{Q})$ is of rank 0.

Known results about isogenies

Theorem 1.2 (Momose)

Let K be a quadratic extension of $\mathbb{Q}$ which is not imaginary with class number equal to 1. Then $X_0(p)(K)$ contains noncuspidal points for only finitely many primes p.

- Using the properties of hyperelliptic and Atkin-Lehner involutions, Najman and Bruin determined all the quadratic points on all hyperelliptic $X_0(n)$ for which $J_0(n)(\mathbb{Q})$ is of rank 0.
- Özman and Siksek determined all the quadratic points on all non-hyperelliptic $X_0(n)$ of genus up to 5 for which $J_0(n)(\mathbb{Q})$ is of rank 0 by using the Mordell-Weil sieve.

- Box described all the quadratic points on all $X_0(n)$ of genus up to 5 for which $J_0(n)(\mathbb{Q})$ has positive rank using a variant of Chabauty's method developed by Siksek.

Known results about isogenies

- Box described all the quadratic points on all $X_0(n)$ of genus up to 5 for which $J_0(n)(\mathbb{Q})$ has positive rank using a variant of Chabauty's method developed by Siksek.
- Najman and V. described all the quadratic points on bielliptic curves $X_0(n)$ by adapting and improving the methods of Box and Siksek.

Known results about isogenies

- Box described all the quadratic points on all $X_0(n)$ of genus up to 5 for which $J_0(n)(\mathbb{Q})$ has positive rank using a variant of Chabauty's method developed by Siksek.
- Najman and V. described all the quadratic points on bielliptic curves $X_0(n)$ by adapting and improving the methods of Box and Siksek.
- A lot of information is known about the possible mod p images of Galois for $E/\mathbb{Q}$. Also, a form of j-invariant is associated to each possible image: we know which forms of j-invariants give specific mod p images of Galois.

Known results about isogenies

- Box described all the quadratic points on all $X_0(n)$ of genus up to 5 for which $J_0(n)(\mathbb{Q})$ has positive rank using a variant of Chabauty's method developed by Siksek.
- Najman and V. described all the quadratic points on bielliptic curves $X_0(n)$ by adapting and improving the methods of Box and Siksek.
- A lot of information is known about the possible mod p images of Galois for $E/\mathbb{Q}$. Also, a form of j-invariant is associated to each possible image: we know which forms of j-invariants give specific mod p images of Galois.
- Most of those results come from Zywina, but some cases were completed by Balakrishnan and others.

Known results about isogenies

- Najman determined all the possible prime isogeny degrees of non-CM elliptic curves with a rational j-invariant defined over number fields of degree at most 7. They are the same primes as for the rational field.

Known results about isogenies

- Najman determined all the possible prime isogeny degrees of non-CM elliptic curves with a rational j-invariant defined over number fields of degree at most 7. They are the same primes as for the rational field.
- The next natural step is to answer the same question for isogenies of composite degree. The main result is the following:

Known results about isogenies

- Najman determined all the possible prime isogeny degrees of non-CM elliptic curves with a rational j-invariant defined over number fields of degree at most 7. They are the same primes as for the rational field.
- The next natural step is to answer the same question for isogenies of composite degree. The main result is the following:

Theorem 1.3 (V.)

Let K be a quadratic number field and E/K a non-CM elliptic curve with a rational j-invariant. Assume E has a cyclic n-isogeny defined over K. Then $n \leq 18$ with $n \neq 14$ or $n \in \{20, 21, 24, 25, 32, 36, 37\}$.

Proof outline

- Notice that it is enough to consider non-CM elliptic curves defined over $\mathbb{Q}$ because we can descend from E/K to $E'/\mathbb{Q}$ using a quadratic twist and isomorphism defined over K and the quadratic twist preserves the presence of an isogeny.

Proof outline

- The proof is conducted in several steps. We prove:

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.
- If $p^2 \mid n$, then $p \in \{2, 3, 5\}$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.
- If $p^2 \mid n$, then $p \in \{2, 3, 5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2,7),(3,7),(7,13)\}$.
- If $p^2 \mid n$, then $p \in \{2,3,5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
- If $2^k \mid n$, then $k \leq 5$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.
- If $p^2 \mid n$, then $p \in \{2, 3, 5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
- If $2^k \mid n$, then $k \leq 5$.
- If $n = 2^a 3^b$, then $n \in \{2, 4, 8, 16, 32, 3, 6, 12, 24, 9, 18, 36\}$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.
- If $p^2 \mid n$, then $p \in \{2, 3, 5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
- If $2^k \mid n$, then $k \leq 5$.
- If $n = 2^a 3^b$, then $n \in \{2, 4, 8, 16, 32, 3, 6, 12, 24, 9, 18, 36\}$.
- If $n = 2^a 5^b$, then $n \in \{2, 4, 8, 16, 32, 5, 10, 20, 25\}$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.
- If $p^2 \mid n$, then $p \in \{2, 3, 5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
- If $2^k \mid n$, then $k \leq 5$.
- If $n = 2^a 3^b$, then $n \in \{2, 4, 8, 16, 32, 3, 6, 12, 24, 9, 18, 36\}$.
- If $n = 2^a 5^b$, then $n \in \{2, 4, 8, 16, 32, 5, 10, 20, 25\}$.
- If $n = 3^a 5^b$, then $n \in \{3, 9, 5, 15, 25\}$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.
- If $p^2 \mid n$, then $p \in \{2, 3, 5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
- If $2^k \mid n$, then $k \leq 5$.
- If $n = 2^a 3^b$, then $n \in \{2, 4, 8, 16, 32, 3, 6, 12, 24, 9, 18, 36\}$.
- If $n = 2^a 5^b$, then $n \in \{2, 4, 8, 16, 32, 5, 10, 20, 25\}$.
- If $n = 3^a 5^b$, then $n \in \{3, 9, 5, 15, 25\}$.
- $n \notin \{14, 30, 63\}$.

Proof outline

- The proof is conducted in several steps. We prove:
- If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2,7),(3,7),(7,13)\}$.
- If $p^2 \mid n$, then $p \in \{2,3,5\}$.
- If $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
- If $2^k \mid n$, then $k \leq 5$.
- If $n = 2^a 3^b$, then $n \in \{2,4,8,16,32,3,6,12,24,9,18,36\}$.
- If $n = 2^a 5^b$, then $n \in \{2,4,8,16,32,5,10,20,25\}$.
- If $n = 3^a 5^b$, then $n \in \{3,9,5,15,25\}$.
- $n \notin \{14,30,63\}$.
- $n \neq 91$.

Proof outline

- For a finite cyclic subgroup C of E, let $\mathbb{Q}(C)$ be the smallest field such that $G_{\mathbb{Q}(C)}$ acts on C. Notice that this is also the field of definition of an isogeny with kernel C.

Proof outline

- For a finite cyclic subgroup C of E, let $\mathbb{Q}(C)$ be the smallest field such that $G_{\mathbb{Q}(C)}$ acts on C. Notice that this is also the field of definition of an isogeny with kernel C.
- For $E/\mathbb{Q}$ and a positive integer n, denote with $\rho_{E,n} : G_{\mathbb{Q}} \mapsto \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the mod n Galois representation of E.

Proof outline

- For a finite cyclic subgroup C of E, let $\mathbb{Q}(C)$ be the smallest field such that $G_{\mathbb{Q}(C)}$ acts on C. Notice that this is also the field of definition of an isogeny with kernel C.
- For $E/\mathbb{Q}$ and a positive integer n, denote with $\rho_{E,n} : G_{\mathbb{Q}} \mapsto \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the mod n Galois representation of E.

Definition 2.1

We say that the p-adic Galois representation $\rho_{E,p^\infty} : G_{\mathbb{Q}} \mapsto \mathrm{GL}_2(\mathbb{Z}_p)$ of E is defined modulo p^k if the image $\rho_{E,p^\infty}(G_{\mathbb{Q}})$ contains the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}_p) \mapsto \mathrm{GL}_2(\mathbb{Z}_p/p^k\mathbb{Z}_p)$.

Proof outline

- Here are some well-known lemmas which will be useful to us:

Lemma 2.2 (Najman)

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime such that $\rho_{E,p}$ is surjective, and C a subgroup of E[p] of order p. Then $[\mathbb{Q}(C) : \mathbb{Q}] = p + 1$.

Lemma 2.3 (Najman)

Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E[p]$. Let $C = \langle P \rangle$. Then $[\mathbb{Q}(P) : \mathbb{Q}(C)]$ *divides* $p - 1$.

Proof outline

Lemma 2.4 (Najman)

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime such that the image of $\rho_{E,p}$ is contained in the normalizer of the non-split Cartan subgroup and let $\langle P \rangle = C \subseteq E[p]$ a cyclic subgroup of order p. Then:

- *If $p \equiv 1 \pmod 3$, then $[\mathbb{Q}(C) : \mathbb{Q}] \geq p + 1$.*
- *If $p \equiv 2 \pmod 3$, then $[\mathbb{Q}(C) : \mathbb{Q}] \geq (p + 1)/3$.*

Lemma 2.5 (Cremona, Najman)

Let E be an elliptic curve defined over a number field K such that its p-adic representation is defined modulo p^{n-1} for some $n \geq 1$. Then for any cyclic subgroup C of $E(\overline{K})$ of order p^n, we have $[K(C) : K(pC)] = p$.

Different prime divisors of isogeny degree

Proposition 3.1 (V.)

Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over a quadratic field K. If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.

- Let's, for example, eliminate the pairs $(2, 11)$ and $(5, 13)$. Very similar conclusions are used in other cases. Assume $2 \mid n$ and $11 \mid n$.

Different prime divisors of isogeny degree

Proposition 3.1 (V.)

Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over a quadratic field K. If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.

- Let's, for example, eliminate the pairs $(2, 11)$ and $(5, 13)$. Very similar conclusions are used in other cases. Assume $2 \mid n$ and $11 \mid n$.
- It is known from Zywina's result on the possible mod 11 images of Galois that the image of $\rho_{E,11}$ is surjective, conjugate to a subgroup of $B(11)$ or to a subgroup of $N_{ns}(11)$.

Different prime divisors of isogeny degree

Proposition 3.1 (V.)

Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over a quadratic field K. If $p < q$ are two prime divisors of n, then $q \leq 5$ or $(p, q) \in \{(2, 7), (3, 7), (7, 13)\}$.

- Let's, for example, eliminate the pairs $(2, 11)$ and $(5, 13)$. Very similar conclusions are used in other cases. Assume $2 \mid n$ and $11 \mid n$.
- It is known from Zywina's result on the possible mod 11 images of Galois that the image of $\rho_{E,11}$ is surjective, conjugate to a subgroup of $B(11)$ or to a subgroup of $N_{ns}(11)$.
- Clearly, E has an 11-isogeny defined over quadratic field. Let C be the kernel of that 11-isogeny.

Different prime divisors of isogeny degree

- In the surjective case, we can use Lemma 2.2 to get $[\mathbb{Q}(C) : \mathbb{Q}] = 12$.

Different prime divisors of isogeny degree

- In the surjective case, we can use Lemma 2.2 to get $[\mathbb{Q}(C) : \mathbb{Q}] = 12$.
- If the image of $\rho_{E,11}$ is conjugate to a subgroup of $N_{ns}(11)$, then it is known by the work of Najman and Gonzalez-Jimenez that $[\mathbb{Q}(P) : \mathbb{Q}] = 120$ for any P of order 11.

Different prime divisors of isogeny degree

- In the surjective case, we can use Lemma 2.2 to get $[\mathbb{Q}(C) : \mathbb{Q}] = 12$.
- If the image of $\rho_{E,11}$ is conjugate to a subgroup of $N_{ns}(11)$, then it is known by the work of Najman and Gonzalez-Jimenez that $[\mathbb{Q}(P) : \mathbb{Q}] = 120$ for any P of order 11.
- By putting $C = \langle P \rangle$, we can use Lemma 2.3 to get $[\mathbb{Q}(P) : \mathbb{Q}(C)] \mid 10$, so: $[\mathbb{Q}(C) : \mathbb{Q}] = \frac{[\mathbb{Q}(P):\mathbb{Q}]}{[\mathbb{Q}(P):\mathbb{Q}(C)]} \geq 12$.

Different prime divisors of isogeny degree

- In the surjective case, we can use Lemma 2.2 to get $[\mathbb{Q}(C) : \mathbb{Q}] = 12$.
- If the image of $\rho_{E,11}$ is conjugate to a subgroup of $N_{ns}(11)$, then it is known by the work of Najman and Gonzalez-Jimenez that $[\mathbb{Q}(P) : \mathbb{Q}] = 120$ for any P of order 11.
- By putting $C = \langle P \rangle$, we can use Lemma 2.3 to get $[\mathbb{Q}(P) : \mathbb{Q}(C)] \mid 10$, so: $[\mathbb{Q}(C) : \mathbb{Q}] = \frac{[\mathbb{Q}(P):\mathbb{Q}]}{[\mathbb{Q}(P):\mathbb{Q}(C)]} \geq 12$.
- Otherwise, there is an 11-isogeny is defined over $\mathbb{Q}$, in which case it is known that $j(E) \in \{-11 \cdot 131^3, -11^2\}$. Since the 11-isogeny is defined over a quadratic extension, this case must occur.

Different prime divisors of isogeny degree

- It is well-known that either E has a 2-isogeny over $\mathbb{Q}$ or every 2-isogeny of E is defined over the field of degree 3.

Different prime divisors of isogeny degree

- It is well-known that either E has a 2-isogeny over $\mathbb{Q}$ or every 2-isogeny of E is defined over the field of degree 3.
- If E had a 2-isogeny over $\mathbb{Q}$, it would have a 22-isogeny over $\mathbb{Q}$, which is impossible.

Different prime divisors of isogeny degree

- It is well-known that either E has a 2-isogeny over $\mathbb{Q}$ or every 2-isogeny of E is defined over the field of degree 3.
- If E had a 2-isogeny over $\mathbb{Q}$, it would have a 22-isogeny over $\mathbb{Q}$, which is impossible.
- If every 2-isogeny is defined over the field of degree 3, then E can't have a cyclic n-isogeny defined over quadratic field. Hence, we have eliminated the pair $(2, 11)$.

Different prime divisors of isogeny degree

- Now let's eliminate the pair $(5, 13)$. Assume $5 \mid n$ and $13 \mid n$. Clearly, E has a 65-isogeny defined over a quadratic extension of $\mathbb{Q}$. That means E is represented by a quadratic point on $X_0(65)$. Box has described all quadratic points on $X_0(65)$.

Different prime divisors of isogeny degree

- Now let's eliminate the pair $(5, 13)$. Assume $5 \mid n$ and $13 \mid n$. Clearly, E has a 65-isogeny defined over a quadratic extension of $\mathbb{Q}$. That means E is represented by a quadratic point on $X_0(65)$. Box has described all quadratic points on $X_0(65)$.
- There are infinitely many of them and all come from $X_0(65)^+(\mathbb{Q})$ via quotient map $\rho : X_0(65) \mapsto X_0(65)^+$. Notice that $X_0(65)(\mathbb{Q})$ contains no non-cuspidal points, so we can assume that E is represented by some quadratic, but not rational point Q on $X_0(65)$.

Different prime divisors of isogeny degree

- Now let's eliminate the pair $(5, 13)$. Assume $5 \mid n$ and $13 \mid n$. Clearly, E has a 65-isogeny defined over a quadratic extension of $\mathbb{Q}$. That means E is represented by a quadratic point on $X_0(65)$. Box has described all quadratic points on $X_0(65)$.
- There are infinitely many of them and all come from $X_0(65)^+(\mathbb{Q})$ via quotient map $\rho : X_0(65) \mapsto X_0(65)^+$. Notice that $X_0(65)(\mathbb{Q})$ contains no non-cuspidal points, so we can assume that E is represented by some quadratic, but not rational point Q on $X_0(65)$.
- If $Q \in X_0(65)$ represents the pair (E, C), then the point $w_{65}(Q)$ is the same as Q^σ (Galois conjugate) and represents the pair (E^σ, C'), where E and E^σ are 65-isogenous.

Different prime divisors of isogeny degree

- Now let's eliminate the pair $(5, 13)$. Assume $5 \mid n$ and $13 \mid n$. Clearly, E has a 65-isogeny defined over a quadratic extension of $\mathbb{Q}$. That means E is represented by a quadratic point on $X_0(65)$. Box has described all quadratic points on $X_0(65)$.
- There are infinitely many of them and all come from $X_0(65)^+(\mathbb{Q})$ via quotient map $\rho : X_0(65) \mapsto X_0(65)^+$. Notice that $X_0(65)(\mathbb{Q})$ contains no non-cuspidal points, so we can assume that E is represented by some quadratic, but not rational point Q on $X_0(65)$.
- If $Q \in X_0(65)$ represents the pair (E, C), then the point $w_{65}(Q)$ is the same as Q^σ (Galois conjugate) and represents the pair (E^σ, C'), where E and E^σ are 65-isogenous.
- Since E is defined over $\mathbb{Q}$, we have $E \cong E^\sigma$ and E is 65-isogenous to itself, hence it has CM, contradiction.

Non-squarefree isogeny degree

Proposition 4.1 (V.)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Assume that $p^2 \mid n$ for some prime p. Then $p \in \{2, 3, 5\}$.

Non-squarefree isogeny degree

Proposition 4.1 (V.)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Assume that $p^2 \mid n$ for some prime p. Then $p \in \{2, 3, 5\}$.

- To prove this, we will use the following result:

Theorem 4.2 (Lombardo, Tronto)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \geq 7$ a prime. If E has a p-isogeny over $\mathbb{Q}$, then the image of ρ_{E,p^∞} contains a Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Non-squarefree isogeny degree

- Proof: Clearly, E has a cyclic p^2-isogeny and a cyclic p-isogeny defined over K.

Non-squarefree isogeny degree

- Proof: Clearly, E has a cyclic p^2-isogeny and a cyclic p-isogeny defined over K.
- Assume $p > 7$. Then we can use the lemmas 2.2, 2.3 and 2.4 similarly as with $p = 11$ earlier to show that the p-isogeny is actually defined over $\mathbb{Q}$.

Non-squarefree isogeny degree

- Proof: Clearly, E has a cyclic p^2-isogeny and a cyclic p-isogeny defined over K.
- Assume $p > 7$. Then we can use the lemmas 2.2, 2.3 and 2.4 similarly as with $p = 11$ earlier to show that the p-isogeny is actually defined over $\mathbb{Q}$.
- Now we can use Theorem 4.2 to conclude that the image of ρ_{E,p^∞} contains a Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Non-squarefree isogeny degree

- Proof: Clearly, E has a cyclic p^2-isogeny and a cyclic p-isogeny defined over K.
- Assume $p > 7$. Then we can use the lemmas 2.2, 2.3 and 2.4 similarly as with $p = 11$ earlier to show that the p-isogeny is actually defined over $\mathbb{Q}$.
- Now we can use Theorem 4.2 to conclude that the image of ρ_{E,p^∞} contains a Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.
- Every Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ is conjugate to this specific Sylow pro-p subgroup:

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \mid a \equiv d \equiv 1 \pmod p, c \equiv 0 \pmod p \right\}.$$

Non-squarefree isogeny degree

- Hence, we can choose compatible bases for all $E[p^k]$ such that the image of ρ_{E,p^∞} contains S.

- Hence, we can choose compatible bases for all $E[p^k]$ such that the image of ρ_{E,p^∞} contains S.
- This means that p-adic representation ρ_{E,p^∞} is defined modulo p (see definition 2.1).

Non-squarefree isogeny degree

- Hence, we can choose compatible bases for all $E[p^k]$ such that the image of ρ_{E,p^∞} contains S.
- This means that p-adic representation ρ_{E,p^∞} is defined modulo p (see definition 2.1).
- Now we can use Lemma 2.5 to conclude that for any cyclic subgroup C of $E(\overline{\mathbb{Q}})$ of order p^2, we have $[\mathbb{Q}(C) : \mathbb{Q}(pC)] = p$, so any cyclic p^2-isogeny has to be defined over a field of degree at least $p > 7$.

Non-squarefree isogeny degree

- Now assume $p = 7$. If E has a rational 7-isogeny, we can repeat the identical conclusions since we can again use the theorem 4.2.

Non-squarefree isogeny degree

- Now assume $p = 7$. If E has a rational 7-isogeny, we can repeat the identical conclusions since we can again use the theorem 4.2.
- Otherwise, we must have a 7-isogeny defined over a quadratic field. We can again use the results of Zywina as before with $p = 11$ combined with the lemmas 2.2, 2.3, 2.4 to deduce that the image of $\rho_{E,7}$ is conjugate to a subgroup of $N_s(7)$.

Non-squarefree isogeny degree

- Now assume $p = 7$. If E has a rational 7-isogeny, we can repeat the identical conclusions since we can again use the theorem 4.2.
- Otherwise, we must have a 7-isogeny defined over a quadratic field. We can again use the results of Zywina as before with $p = 11$ combined with the lemmas 2.2, 2.3, 2.4 to deduce that the image of $\rho_{E,7}$ is conjugate to a subgroup of $N_s(7)$.
- By Zywina, there are three such possible images, two of which only appear when $j(E) = 2268945/128$.

Non-squarefree isogeny degree

- If we have $j(E) = 2268945/128$, we can use the classical modular polynomial $\Phi_N(X, Y)$.

Non-squarefree isogeny degree

- If we have $j(E) = 2268945/128$, we can use the classical modular polynomial $\Phi_N(X, Y)$.
- It is known by the result of Igusa that for a field F of characteristic not dividing N, a non-CM elliptic curve E/F has a cyclic N-isogeny if and only if $\Phi_N(X, j(E))$ has a zero in F.

Non-squarefree isogeny degree

- If we have $j(E) = 2268945/128$, we can use the classical modular polynomial $\Phi_N(X, Y)$.
- It is known by the result of Igusa that for a field F of characteristic not dividing N, a non-CM elliptic curve E/F has a cyclic N-isogeny if and only if $\Phi_N(X, j(E))$ has a zero in F.
- We can factor $\Phi_{49}(X, 2268945/128)$ into three irreducible factors of degrees 14, 14, 21 respectively. Therefore, a cyclic 49-isogeny is defined over a number field of degree (at least) 14.

Non-squarefree isogeny degree

- The third possible image of $\rho_{E,7}$ is the whole $N_s(7)$. We use Magma to check all subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ and select only those which reduce modulo 7 to $N_s(7)$, all up to conjugation. Those are the possible images of $\rho_{E,49}$.

- The third possible image of $\rho_{E,7}$ is the whole $N_s(7)$. We use `Magma` to check all subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ and select only those which reduce modulo 7 to $N_s(7)$, all up to conjugation. Those are the possible images of $\rho_{E,49}$.
- There are 8 such subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ up to conjugation. The following result will be helpful:

Non-squarefree isogeny degree

- The third possible image of $\rho_{E,7}$ is the whole $N_s(7)$. We use `Magma` to check all subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ and select only those which reduce modulo 7 to $N_s(7)$, all up to conjugation. Those are the possible images of $\rho_{E,49}$.
- There are 8 such subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ up to conjugation. The following result will be helpful:

Theorem 4.3 (Lombardo, Tronto)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \geq 5$ a prime. The image of ρ_{E,p^∞} contains all scalars congruent to 1 modulo p.

Non-squarefree isogeny degree

- Out of the 8 mentioned subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$, 4 of them contain only one scalar (out of 7) congruent to 1 modulo 7, a contradiction with Theorem 4.3.

Non-squarefree isogeny degree

- Out of the 8 mentioned subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$, 4 of them contain only one scalar (out of 7) congruent to 1 modulo 7, a contradiction with Theorem 4.3.
- Two of them act on the cyclic subgroups of $E[49]$ of order 49 such that the corresponding orbit lengths are 14 and 42 in both cases, so a cyclic 49-isogeny is defined over the field of degree (at least) 14 in those cases.

Non-squarefree isogeny degree

- Out of the 8 mentioned subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$, 4 of them contain only one scalar (out of 7) congruent to 1 modulo 7, a contradiction with Theorem 4.3.
- Two of them act on the cyclic subgroups of $E[49]$ of order 49 such that the corresponding orbit lengths are 14 and 42 in both cases, so a cyclic 49-isogeny is defined over the field of degree (at least) 14 in those cases.
- The two remaining subgroups are conjugate to a subgroup of $N_s(49)$. If there exists a non-CM elliptic curve over $\mathbb{Q}$ satisfying that, it will be represented by a point on $X_s(49)(\mathbb{Q})$.

Non-squarefree isogeny degree

- Recall that there is a $\mathbb{Q}$-isomorphism $X_s(N) \cong X_0^+(N^2)$.

Non-squarefree isogeny degree

- Recall that there is a $\mathbb{Q}$-isomorphism $X_s(N) \cong X_0^+(N^2)$.
- By studying the modular interpretation of that isomorphism, it is easy to see that CM points and cusps on $X_s(p^r)$ correspond to CM points and cusps on $X_0^+(p^{2r})$ for a prime p.

Non-squarefree isogeny degree

- Recall that there is a $\mathbb{Q}$-isomorphism $X_s(N) \cong X_0^+(N^2)$.
- By studying the modular interpretation of that isomorphism, it is easy to see that CM points and cusps on $X_s(p^r)$ correspond to CM points and cusps on $X_0^+(p^{2r})$ for a prime p.
- Momose and Shimura have studied the rational points on $X_0^+(p^r)$. By their result, we know that $X_0^+(7^r)(\mathbb{Q})$ consists only of cusps and CM-points for $r \geq 3$. Since we were considering $X_s(7^2) \cong X_0^+(7^4)$, we are done.

14-isogeny

- Now we prove the following proposition:

Proposition 5.1

Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Then $n \neq 14$.

14-isogeny

- Now we prove the following proposition:

Proposition 5.1

Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Then $n \neq 14$.

- Notice that E can have a rational 14-isogeny, but then E must have CM.

14-isogeny

- Now we prove the following proposition:

Proposition 5.1

Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Then $n \neq 14$.

- Notice that E can have a rational 14-isogeny, but then E must have CM.
- If E didn't have a rational 2-isogeny, then any 2-isogeny would be defined over a number field of degree 3, making it impossible for E to have a 14-isogeny defined over quadratic number field.

14-isogeny

- Now we prove the following proposition:

Proposition 5.1

Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Then $n \neq 14$.

- Notice that E can have a rational 14-isogeny, but then E must have CM.
- If E didn't have a rational 2-isogeny, then any 2-isogeny would be defined over a number field of degree 3, making it impossible for E to have a 14-isogeny defined over quadratic number field.
- Hence, E has a rational 2-isogeny.

14-isogeny

- This means that E must have a 7-isogeny defined over a quadratic number field, but not over $\mathbb{Q}$.

14-isogeny

- This means that E must have a 7-isogeny defined over a quadratic number field, but not over $\mathbb{Q}$.
- By recalling Zywina's result as before, we see that the image of $\rho_{E,7}$ has to be conjugate to a subgroup of $N_s(7)$.

14-isogeny

- This means that E must have a 7-isogeny defined over a quadratic number field, but not over $\mathbb{Q}$.
- By recalling Zywina's result as before, we see that the image of $\rho_{E,7}$ has to be conjugate to a subgroup of $N_s(7)$.
- Zywina also gives us the form for j-invariant of curves with that mod 7 representation. We match that form with the form of the j-invariants allowing a rational 2-isogeny:

14-isogeny

- This means that E must have a 7-isogeny defined over a quadratic number field, but not over $\mathbb{Q}$.
- By recalling Zywina's result as before, we see that the image of $\rho_{E,7}$ has to be conjugate to a subgroup of $N_s(7)$.
- Zywina also gives us the form for j-invariant of curves with that mod 7 representation. We match that form with the form of the j-invariants allowing a rational 2-isogeny:

$$\frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7} = \frac{(s+16)^3}{s}.$$

14-isogeny

- We get a genus 3 projective curve on which we want to find all the rational points.

14-isogeny

- We get a genus 3 projective curve on which we want to find all the rational points.
- Using `Magma`, we map it to a curve which has a degree 2 quotient that is an elliptic curve with only 6 rational points.

14-isogeny

- We get a genus 3 projective curve on which we want to find all the rational points.
- Using `Magma`, we map it to a curve which has a degree 2 quotient that is an elliptic curve with only 6 rational points.
- By taking the preimages, we find all the rational points on the starting curve, none of which give us a desired non-CM curve E.

14-isogeny

- We get a genus 3 projective curve on which we want to find all the rational points.
- Using `Magma`, we map it to a curve which has a degree 2 quotient that is an elliptic curve with only 6 rational points.
- By taking the preimages, we find all the rational points on the starting curve, none of which give us a desired non-CM curve E.
- Those points are: $(2 : -256 : 1)$, $(-1 : -16 : 1)$, $(0 : -16 : 1)$, $(0 : 1 : 0)$, $(1 : 0 : 0)$.

14-isogeny

- We get a genus 3 projective curve on which we want to find all the rational points.
- Using `Magma`, we map it to a curve which has a degree 2 quotient that is an elliptic curve with only 6 rational points.
- By taking the preimages, we find all the rational points on the starting curve, none of which give us a desired non-CM curve E.
- Those points are: $(2 : -256 : 1)$, $(-1 : -16 : 1)$, $(0 : -16 : 1)$, $(0 : 1 : 0)$, $(1 : 0 : 0)$.
- The last two don't give us a j-invariant and other give us j-invariants 0 or 54000. That completes the proof.

91-isogeny

- Our goal is to show that there are no elliptic curves $E/\mathbb{Q}$ with a cyclic 91-isogeny defined over a quadratic extension of $\mathbb{Q}$. We could try using the similar approach as with 14-isogeny.

91-isogeny

- Our goal is to show that there are no elliptic curves $E/\mathbb{Q}$ with a cyclic 91-isogeny defined over a quadratic extension of $\mathbb{Q}$. We could try using the similar approach as with 14-isogeny.
- Since E has 91-isogeny, it must have 13-isogeny and 7-isogeny over a quadratic extension.

91-isogeny

- Our goal is to show that there are no elliptic curves $E/\mathbb{Q}$ with a cyclic 91-isogeny defined over a quadratic extension of $\mathbb{Q}$. We could try using the similar approach as with 14-isogeny.
- Since E has 91-isogeny, it must have 13-isogeny and 7-isogeny over a quadratic extension.
- Using lemmas 2.2, 2.3 and 2.4 like before, we can show that there is a rational 13-isogeny and that the image of $\rho_{E,7}$ is $N_s(7)$.

91-isogeny

- Our goal is to show that there are no elliptic curves $E/\mathbb{Q}$ with a cyclic 91-isogeny defined over a quadratic extension of $\mathbb{Q}$. We could try using the similar approach as with 14-isogeny.
- Since E has 91-isogeny, it must have 13-isogeny and 7-isogeny over a quadratic extension.
- Using lemmas 2.2, 2.3 and 2.4 like before, we can show that there is a rational 13-isogeny and that the image of $\rho_{E,7}$ is $N_s(7)$.
- We can match the j-invariants allowing those two properties, but we will get a curve of a very large genus.

91-isogeny

- We will determine all quadratic points on $X_0(91)$ up to those points that appear as pullbacks of rational points on $X_0(91)^+$ (non-exceptional points).

91-isogeny

- We will determine all quadratic points on $X_0(91)$ up to those points that appear as pullbacks of rational points on $X_0(91)^+$ (non-exceptional points).
- We will see that all the exceptional points are either cusps or CM points.

91-isogeny

- We will determine all quadratic points on $X_0(91)$ up to those points that appear as pullbacks of rational points on $X_0(91)^+$ (non-exceptional points).
- We will see that all the exceptional points are either cusps or CM points.
- On the other hand, we can use the identical modular interpretation argument as with $n = 65$ to show that if a non-exceptional point on $X_0(91)$ represents an $E/\mathbb{Q}$, then E is 91-isogenous to itself, so it has CM.

91-isogeny

- We will use the relative symmetric Chabauty developed by Siksek and used by Box.

91-isogeny

- We will use the relative symmetric Chabauty developed by Siksek and used by Box.
- For some smooth, projective non-hyperelliptic curve $X/\mathbb{Q}$, the method provides a criterion for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$.

91-isogeny

- We will use the relative symmetric Chabauty developed by Siksek and used by Box.
- For some smooth, projective non-hyperelliptic curve $X/\mathbb{Q}$, the method provides a criterion for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$.
- Also, the method provides a criterion for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$, up to points appearing as pullbacks of points on $C(\mathbb{Q})$, where C is a degree 2 quotient of X.

91-isogeny

- We will use the relative symmetric Chabauty developed by Siksek and used by Box.
- For some smooth, projective non-hyperelliptic curve $X/\mathbb{Q}$, the method provides a criterion for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$.
- Also, the method provides a criterion for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$, up to points appearing as pullbacks of points on $C(\mathbb{Q})$, where C is a degree 2 quotient of X.
- In our case, we have $X = X_0(91)$ and $C = X_0(91)^+$. We also need $rk(J(X)) = rk(J(C))$, which is true in our case as both ranks are 2.

91-isogeny

- We are able to replicate the same method used by Box.

91-isogeny

- We are able to replicate the same method used by Box.
- We get that there are no other quadratic points on $X_0(91)$ apart from the known ones and the pullbacks of rational points on $X_0(91)^+$.

91-isogeny

- We are able to replicate the same method used by Box.
- We get that there are no other quadratic points on $X_0(91)$ apart from the known ones and the pullbacks of rational points on $X_0(91)^+$.
- All the exceptional (non-pullback) points on $X_0(91)$ are the four cusps and a pair of conjugate CM points defined over $\mathbb{Q}(\sqrt{13})$ and fixed by w_{91}.

91-isogeny

- We are able to replicate the same method used by Box.
- We get that there are no other quadratic points on $X_0(91)$ apart from the known ones and the pullbacks of rational points on $X_0(91)^+$.
- All the exceptional (non-pullback) points on $X_0(91)$ are the four cusps and a pair of conjugate CM points defined over $\mathbb{Q}(\sqrt{13})$ and fixed by w_{91}.
- As described earlier, the non-exceptional points can only give us CM curves $E/\mathbb{Q}$, so the proof is complete.