Torsion of $\mathbb{Q}$-curves over small odd prime degree number fields

Ivan Novak

Dubrovnik, June 26, 2025



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

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.
Examples:

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.
Examples:

- All elliptic curves defined over $\mathbb{Q}$.

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.
Examples:

- All elliptic curves defined over $\mathbb{Q}$.
- All elliptic curves with rational j-invariant.

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.
Examples:

- All elliptic curves defined over $\mathbb{Q}$.
- All elliptic curves with rational j-invariant.
- All elliptic curves isogenous to a $\mathbb{Q}$-curve.

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.
Examples:

- All elliptic curves defined over $\mathbb{Q}$.
- All elliptic curves with rational j-invariant.
- All elliptic curves isogenous to a $\mathbb{Q}$-curve.
- All CM elliptic curves.

What are $\mathbb{Q}$-curves?

A $\mathbb{Q}$-curve is an elliptic curve E defined over some number field K which is isogenous to all its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.
Examples:

- All elliptic curves defined over $\mathbb{Q}$.
- All elliptic curves with rational j-invariant.
- All elliptic curves isogenous to a $\mathbb{Q}$-curve.
- All CM elliptic curves.

Ribet proved that $\mathbb{Q}$-curves are exactly the elliptic curves over number fields which are modular, in the sense of being a quotient of some $J_1(N)$.

$\mathbb{Q}$-curves over odd degree number fields

Theorem (Cremona, Najman)

Let K be a number field and E/K a non-CM $\mathbb{Q}$-curve. If $\mathbb{Q}(j(E))$ has no quadratic subfields, then E is isogenous over K to an elliptic curve with rational j-invariant.

$\mathbb{Q}$-curves over odd degree number fields

Theorem (Cremona, Najman)

Let K be a number field and E/K a non-CM $\mathbb{Q}$-curve. If $\mathbb{Q}(j(E))$ has no quadratic subfields, then E is isogenous over K to an elliptic curve with rational j-invariant.

In particular, $\mathbb{Q}$-curves over odd degree number fields are isogenous to elliptic curves with rational j-invariant.

Torsion of rational elliptic curves

Theorem (Mazur)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:

$$\mathbb{Z}/N_1\mathbb{Z} \qquad \text{with } N_1 = 1, \ldots, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} \qquad \text{with } N_2 = 1, \ldots, 4.$$

Torsion of rational elliptic curves

Theorem (Mazur)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:

$$\mathbb{Z}/N_1\mathbb{Z} \qquad \text{with } N_1 = 1, \ldots, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} \qquad \text{with } N_2 = 1, \ldots, 4.$$

Theorem (Najman)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic extension. Then $E(K)_{tors}$ is either one of the 15 groups from Mazur's theorem, or one of $\mathbb{Z}/NZ$ with $N = 13, 14, 18, 21$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.

Torsion of rational elliptic curves, continued

Theorem (Lozano-Robledo)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quintic extension. Then $E(K)_{tors}$ is isomorphic to one of the 15 groups from Mazur's theorem, or one of $\mathbb{Z}/11\mathbb{Z}$ or $\mathbb{Z}/25\mathbb{Z}$.

Torsion of rational elliptic curves, continued

Theorem (Lozano-Robledo)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quintic extension. Then $E(K)_{tors}$ is isomorphic to one of the 15 groups from Mazur's theorem, or one of $\mathbb{Z}/11\mathbb{Z}$ or $\mathbb{Z}/25\mathbb{Z}$.

Theorem (González-Jiménez, Najman)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a septic extension. Then $E(K)_{tors}$ is isomorphic to one of the 15 groups from Mazur's theorem.

Torsion of $\mathbb{Q}$-curves over prime degree extensions other than $3, 5, 7$

Theorem (Le Fourn, Najman)

Possible torsion subgroups of $\mathbb{Q}$-curves over quadratic number fields are the 15 groups from Mazur's theorem and

$$\begin{aligned}
&\mathbb{Z}/N\mathbb{Z}, && \text{for } N = 13, 14, 15, 16, 18,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && \text{for } N = 5, 6,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} && \text{for } N = 1, 2,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. &&
\end{aligned}$$

Torsion of $\mathbb{Q}$-curves over prime degree extensions other than $3, 5, 7$

Theorem (Le Fourn, Najman)

Possible torsion subgroups of $\mathbb{Q}$-curves over quadratic number fields are the 15 groups from Mazur's theorem and

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \text{for } N = 13, 14, 15, 16, 18, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && \text{for } N = 5, 6, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} && \text{for } N = 1, 2, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Theorem (Cremona, Najman)

For prime $p > 7$, every $\mathbb{Q}$-curve over a degree p number field has torsion equal to one of the 15 groups from Mazur's theorem.

Torsion of elliptic curves with rational j-invariant

Theorem (Gužvić)

Let p be a prime number and E an elliptic curve with rational j-invariant defined over a number field K of degree p. Then $E(K)_{tors} = E'(K)_{tors}$ for some elliptic curve E' defined over $\mathbb{Q}$, unless $p = 2$ and $E(K)_{tors} = \mathbb{Z}/13\mathbb{Z}$.

Torsion of elliptic curves with rational j-invariant

Theorem (Gužvić)

Let p be a prime number and E an elliptic curve with rational j-invariant defined over a number field K of degree p. Then $E(K)_{tors} = E'(K)_{tors}$ for some elliptic curve E' defined over $\mathbb{Q}$, unless $p = 2$ and $E(K)_{tors} = \mathbb{Z}/13\mathbb{Z}$.

In particular, for odd prime degree number fields, nothing changes when going from rational elliptic curves to elliptic curves with rational j-invariant.

Main results

We prove that for $p = 3, 5$ or 7, the same holds for $\mathbb{Q}$-curves.

Main results

We prove that for $p = 3, 5$ or 7, the same holds for $\mathbb{Q}$-curves.

Theorem (N.)

Let $p = 3, 5$ or 7. Let E be a $\mathbb{Q}$-curve over a number field K of degree p. Then $E(K)_{tors} = E'(K)_{tors}$ for some elliptic curve E' with rational j-invariant.

The case $p = 3$

In the rest of the talk, we mostly focus on the case $p = 3$. So far, we have 20 groups for which we know they appear for elliptic curves with rational j-invariant.
We also have a result in the other direction.

The case $p = 3$

In the rest of the talk, we mostly focus on the case $p = 3$. So far, we have 20 groups for which we know they appear for elliptic curves with rational j-invariant.
We also have a result in the other direction.

Theorem (Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown)

Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)_{tors}$ is one of the 20 groups which appear for elliptic curves with rational j-invariant, or one of $\mathbb{Z}/N\mathbb{Z}$ with $N = 11, 15, 16, 20$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

The case $p = 3$

In the rest of the talk, we mostly focus on the case $p = 3$. So far, we have 20 groups for which we know they appear for elliptic curves with rational j-invariant.
We also have a result in the other direction.

Theorem (Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown)

Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)_{tors}$ is one of the 20 groups which appear for elliptic curves with rational j-invariant, or one of $\mathbb{Z}/N\mathbb{Z}$ with $N = 11, 15, 16, 20$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

It remains to prove that none of the mentioned six groups appear as torsion of a $\mathbb{Q}$-curve over a cubic field.

Images of Galois representations

To solve the problem, we use Galois representations of elliptic curves.

Images of Galois representations

To solve the problem, we use Galois representations of elliptic curves.
Let K be a number field and E/K an elliptic curve. For a positive integer N, the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[N]$, the group of points of order N.

Images of Galois representations

To solve the problem, we use Galois representations of elliptic curves.
Let K be a number field and E/K an elliptic curve. For a positive integer N, the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[N]$, the group of points of order N.
This defines a homomorphism $\rho_{E,N} : G_K \to \mathrm{Aut}(E[N])$ called the mod N Galois representation of E/K.

Images of Galois representations

To solve the problem, we use Galois representations of elliptic curves.
Let K be a number field and E/K an elliptic curve. For a positive integer N, the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[N]$, the group of points of order N.
This defines a homomorphism $\rho_{E,N} : G_K \to \mathrm{Aut}(E[N])$ called the mod N Galois representation of E/K.
Since $E[N]$ is isomorphic to $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$, after fixing a basis for $E[N]$, each $\sigma \in G_K$ acts as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Images of Galois representations, continued

The image of the Galois representation gives us information about torsion and isogenies of the elliptic curve.

Images of Galois representations, continued

The image of the Galois representation gives us information about torsion and isogenies of the elliptic curve.

The image is conjugate to a subgroup of uppertriangular matrices $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ if and only if E has an N-isogeny over K.

Images of Galois representations, continued

The image of the Galois representation gives us information about torsion and isogenies of the elliptic curve.

The image is conjugate to a subgroup of uppertriangular matrices $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ if and only if E has an N-isogeny over K.

The image is conjugate to a subgroup of matrices of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ if and only if E has a point of order N over K.

Images of Galois representations and isogenies

Now we discuss how the image changes upon applying an isogeny.

Images of Galois representations and isogenies

Now we discuss how the image changes upon applying an isogeny.

Lemma

Let E_1/K be an elliptic curve with an n-isogeny over K, and let P be the generator of the kernel of this isogeny. Let
$H = \{k \in (\mathbb{Z}/N\mathbb{Z})^\times \mid \sigma(P) = kP$ for some $\sigma \in G_F\}$.
Let $\phi : E_1 \to E_2$ be a cyclic isogeny defined over K. Let α be the order of $\phi(P)$ in E_2. Then $\rho_{E_2,n}(G_K)$ is conjugate to a subgroup of the group of all matrices of the form

$$\begin{bmatrix} h & \frac{n}{\alpha} \cdot * \\ \alpha \cdot * & * \end{bmatrix},$$

where $h \in H$.

Images of Galois representations and isogenies

Now we discuss how the image changes upon applying an isogeny.

Lemma

Let E_1/K be an elliptic curve with an n-isogeny over K, and let P be the generator of the kernel of this isogeny. Let
$H = \{k \in (\mathbb{Z}/N\mathbb{Z})^\times \mid \sigma(P) = kP$ for some $\sigma \in G_F\}$.
Let $\phi : E_1 \to E_2$ be a cyclic isogeny defined over K. Let α be the order of $\phi(P)$ in E_2. Then $\rho_{E_2,n}(G_K)$ is conjugate to a subgroup of the group of all matrices of the form

$$\begin{bmatrix} h & \frac{n}{\alpha} \cdot * \\ \alpha \cdot * & * \end{bmatrix},$$

where $h \in H$.

In particular, if E_1 has an n-isogeny, E_2 has an α-isogeny and an independent $\frac{n}{\alpha}$-isogeny for some α dividing n.

Images of Galois representations and twists

Now we discuss how the image changes upon quadratic twists.

Images of Galois representations and twists

Now we discuss how the image changes upon quadratic twists.

Lemma

Let E be an elliptic curve over a number field K. Let E' be a quadratic twist of E by $d \in K^\times$. Let $\psi : G_K \to \{-1, 1\}$ be the quadratic character defined by $\sigma(\sqrt{d}) = \psi(\sqrt{d})\sqrt{d}$. Denote by $\rho_{E,N}$ and $\rho_{E',N}$ the mod N Galois representations of E and E' respectively. Then, for an appropriate choice of bases of $E[N]$ and $E'[N]$, we have

$$\rho_{E,N}(\sigma) = \psi(\sigma)\rho_{E',N}(\sigma).$$

Proof strategy

Let E be a $\mathbb{Q}$-curve over a cubic field K with certain torsion structure. Let E' be a K-isogenous curve with rational j-invariant, and let E'' be a twist of E' which is defined over $\mathbb{Q}$.

Proof strategy

Let E be a $\mathbb{Q}$-curve over a cubic field K with certain torsion structure. Let E' be a K-isogenous curve with rational j-invariant, and let E'' be a twist of E' which is defined over $\mathbb{Q}$.

$$E \longrightarrow E' \longrightarrow E''.$$

Proof strategy

Let E be a $\mathbb{Q}$-curve over a cubic field K with certain torsion structure. Let E' be a K-isogenous curve with rational j-invariant, and let E'' be a twist of E' which is defined over $\mathbb{Q}$.

$$E \longrightarrow E' \longrightarrow E''.$$

We know a lot about Galois images of the rational elliptic curve E'', so we can use the previous two lemmas to obtain information about the Galois image of E and reach a contradiction.

Case $\mathbb{Z}/11\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

Case $\mathbb{Z}/11\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

If E has a point of order 11, then by the previous lemmas E'' has an 11-isogeny over a cubic field K. In fact, every element of $\rho_{E'',11}(G_K)$ has eigenvalue 1 or -1.

Case $\mathbb{Z}/11\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

If E has a point of order 11, then by the previous lemmas E'' has an 11-isogeny over a cubic field K. In fact, every element of $\rho_{E'',11}(G_K)$ has eigenvalue 1 or -1. It is known that rational elliptic curves with an 11-isogeny over a cubic field already have an 11-isogeny over $\mathbb{Q}$. There are two (up to $\overline{\mathbb{Q}}$-isomorphism) such elliptic curves E''. The orders of their Galois images mod 11 are not divisible by 3, so $\rho_{E'',11}(G_{\mathbb{Q}}) = \rho_{E'',11}(G_K)$. Each of the Galois images $\rho_{E'',11}(G_{\mathbb{Q}})$ contains a matrix with neither 1 nor -1 as eigenvalue, a contradiction.

Case $\mathbb{Z}/15\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

Case $\mathbb{Z}/15\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

Similarly to the previous case, we conclude that E'' has a rational 15-isogeny and there are again finitely many elliptic curves to check (four of them).

Case $\mathbb{Z}/15\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

Similarly to the previous case, we conclude that E'' has a rational 15-isogeny and there are again finitely many elliptic curves to check (four of them). However, $\rho_{E'',15}(G_{\mathbb{Q}})$ is divisible by 3, so $\rho_{E'',15}(G_K)$ can be any subgroup of index 3.

Case $\mathbb{Z}/15\mathbb{Z}$

$$E \longrightarrow E' \longrightarrow E''.$$

Similarly to the previous case, we conclude that E'' has a rational 15-isogeny and there are again finitely many elliptic curves to check (four of them). However, $\rho_{E'',15}(G_{\mathbb{Q}})$ is divisible by 3, so $\rho_{E'',15}(G_K)$ can be any subgroup of index 3. To conclude, we find a matrix in each of the index 3 subgroups of possible $\rho_{E'',15}(G_{\mathbb{Q}})$ which does not have 1 nor -1 as an eigenvalue mod 3 and mod 5.

Degrees 5 and 7

For $p = 5$ and 7, the list of possible torsion of elliptic curves over degree p number fields, so there is not a nice list of groups that one needs to check and there is a bit more casework to do.
However, the techniques used are similar to the cubic case.

A nice corollary

As mentioned earlier, Cremona and Najman have shown that for prime $p > 7$, every $\mathbb{Q}$-curve over a degree p number field has torsion equal to one of the 15 groups from Mazur's theorem.
Combining this with our results yields the following result.

A nice corollary

As mentioned earlier, Cremona and Najman have shown that for prime $p > 7$, every $\mathbb{Q}$-curve over a degree p number field has torsion equal to one of the 15 groups from Mazur's theorem.
Combining this with our results yields the following result.

Corollary

Let p be an odd prime number. If a group T appears as the torsion subgroup of some $\mathbb{Q}$-curve over a number field of degree p, then T also appears as the torsion subgroup of some elliptic curve over a number field of degree p with rational j-invariant.

The corollary is false for $p = 2$, because some groups (e.g. $\mathbb{Z}/18\mathbb{Z}$) appear as torsion of a quadratic $\mathbb{Q}$-curve, but do not appear as torsion of an elliptic curve with rational j-invariant.

Prime $p = 2$ fixed

However, the claim holds for all primes if we replace $\mathbb{Q}$-curves by elliptic curves isogenous to those with rational j-invariant.

Prime $p = 2$ fixed

However, the claim holds for all primes if we replace $\mathbb{Q}$-curves by elliptic curves isogenous to those with rational j-invariant.

Theorem (N.)

Let p be a prime number. If a group T is the torsion subgroup of some elliptic curve over a number field of degree p which is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve with rational j-invariant, then T is also the torsion subgroup of some elliptic curve over a number field of degree p with rational j-invariant.

Prime $p = 2$ fixed

However, the claim holds for all primes if we replace $\mathbb{Q}$-curves by elliptic curves isogenous to those with rational j-invariant.

Theorem (N.)

Let p be a prime number. If a group T is the torsion subgroup of some elliptic curve over a number field of degree p which is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve with rational j-invariant, then T is also the torsion subgroup of some elliptic curve over a number field of degree p with rational j-invariant.

Does this also hold for composite degrees?

Prime $p = 2$ fixed

However, the claim holds for all primes if we replace $\mathbb{Q}$-curves by elliptic curves isogenous to those with rational j-invariant.

Theorem (N.)

Let p be a prime number. If a group T is the torsion subgroup of some elliptic curve over a number field of degree p which is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve with rational j-invariant, then T is also the torsion subgroup of some elliptic curve over a number field of degree p with rational j-invariant.

Does this also hold for composite degrees?
I don't know.

Proof of the claim

Proof.

It remains to prove that groups $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ are not torsion subgroups of elliptic curves isogenous to those with rational j-invariant.

Proof of the claim

Proof.

It remains to prove that groups $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ are not torsion subgroups of elliptic curves isogenous to those with rational j-invariant. Case $\mathbb{Z}/14\mathbb{Z}$ follows from Vukorepa's result that there are no 14-isogenies of rational elliptic curves over quadratic extensions.

Proof of the claim

Proof.

It remains to prove that groups $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ are not torsion subgroups of elliptic curves isogenous to those with rational j-invariant.
Case $\mathbb{Z}/14\mathbb{Z}$ follows from Vukorepa's result that there are no 14-isogenies of rational elliptic curves over quadratic extensions.
Case $\mathbb{Z}/18\mathbb{Z}$ follows from the fact that every elliptic curve with a point of order 18 over a quadratic field is 2-isogenous to its conjugate. However, by Cremona and Najman's results on $\mathbb{Q}$-curves, if an elliptic curve E is isogenous to a rational elliptic curve, then the degree of isogeny from E to any of its conjugates is a square, a contradiction. □

Thank you.