Torsion of elliptic curves over quartic fields

Filip Najman

University of Zagreb

joint work with Maarten Derickx (Zagreb)

Rational points 2025, Schney, July 31st 2025

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

Mordell-Weil theorem

By the Mordell-Weil theorem, for an elliptic curve E over a number field K, we have $E(K) \simeq E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$, where $E(K)_{\mathrm{tors}}$ is the torsion subgroup and r is the rank of $E(K)$.

This talk is about determining the possibilities for $E(K)_{\mathrm{tors}}$, where K varies through all degree d number fields.

This is really a question about degree d points on modular curves.

Modular curves

Let $m \mid n$ and ζ_m a fixed root of unity. The modular curve $Y_1(m,n)$ is the moduli space parametrizing triples (E,P,Q), where E is an elliptic curve, and P and Q are points of order m and n, respectively, generating a subgroup of $E[n]$ isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and such that $e_m(P, \frac{n}{m}Q) = \zeta_m$.

The modular curve $Y_0(n)$ is the moduli space parametrizing pairs (E,C), where E is an elliptic curve, and C is a cyclic subgroup of order n.

$X_1(m,n)$ and $X_0(n)$ are the compactifications of $Y_1(m,n)$ and $Y_0(n)$, obtained by adding finitely many cusps.

To find all the degree d points on X, one needs to study the rational points on the d-th symmetric power $X^{(d)} := \mathrm{Sym}^d X$.

We view elements of $X^{(d)}$ as effective degree d divisors.

Torsion groups over degree d number fields

We denote the set all the possible torsion groups $E(K)_{\mathrm{tors}}$ of all elliptic curves E over all number fields K of degree d by $\Phi(d)$.

We denote the set of primes dividing the order of any group in this set by $S(d)$.

The fact that $\Phi(d)$ is finite for all d is equivalent to the Uniform boundedness conjecture, proved by Merel.

Theorem (Merel, 1994)

There is a bound C_d such that $\#E(K)_{\mathrm{tors}} < C_d$ for all elliptic curves over all number fields K of degree d.

Torsion groups over degree d number fields

One can also consider the same problem on a restricted set of elliptic curves (such as base changes of elliptic curves over $\mathbb{Q}$, or E/K with $j(E) \in \mathbb{Q}$, or $\mathbb{Q}$-curves, etc.), or over a restricted set of number fields (e.g. only Galois/Abelian/cyclic, or totally real/imaginary number fields degree d, etc.).

There has been a lot of progress in questions of this type recently.

Proving the (non)existence of torsion groups

Definition

Let $X/\mathbb{Q}$ be a curve. A point $x \in X(K)$ is *sporadic* if there exist only finitely many points of degree $\leq [K : \mathbb{Q}]$ on X.

Example: a rational point on any genus ≥ 2 curve is sporadic.

There are 2 steps in determining $\Phi(d)$:

1) Find the torsion groups that appear infinitely often (up to $\overline{\mathbb{Q}}$-isomorphism, i.e for infinitely many different j-invariants). This set is denoted $\Phi_\infty(d)$.

   This is usually the easier step. For small d this problem amounts to determining all the $X_1(m, n)$ with gonality d.

2) The harder part is finding all the sporadic points and proving the non-existence of other sporadic points on all $Y_1(m, n)$.

Mazur's torsion theorem

Part 1) of the problem to determine $\Phi(1)$ was solved by Levi at the beginning of the 20th century, while the proof of 2) would wait for almost 70 years.

Theorem (Mazur's torsion theorem, 1976)

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

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \ldots, 10, 12, \text{ or}$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \ldots, 4.$$

Before Mazur proved the theorem, many other cases were eliminated by Levi in 1906-1908, Billing and Mahler in 1940, Nagell in 1952, Ogg in 1971, Mazur and Tate in 1973, Ligozat in 1975 and Kubert in 1976.

All of the curves corresponding to the groups above have genus 0, so there are ∞ many elliptic curves E such that $E(\mathbb{Q})_{tors} \simeq T$.

Torsion groups over quadratic fields

Mestre determined $\Phi_\infty(2)$ in 1981.

Kenku and Momose determined $\Phi(2)$ in 1986, assuming that $S(2) = \{2, 3, 5, 7, 11, 13\}$ (which they could not prove).

Kammieny determined in 1991 that $S(2)$ is as conjectured, proving

Theorem (Kenku & Momose, Kamienny)

The torsion of an elliptic curve over a quadratic field K is isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } n = 1, \ldots, 16 \text{ or } 18, \text{ or}$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ where } n = 1, \ldots, 6, \text{ or}$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \text{ where } n = 1, 2 \text{ or},$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Each group appears infinitely many times.

Torsion groups over cubic fields

Parent proved in 2003 that $S(3) = \{2, 3, 5, 7, 11, 13\}$.

Jeon, Kim & Schweizer proved in 2004:

$$\Phi_\infty(3) = \{\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \ldots, 16, 18, 20\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1, \ldots, 7\}.$$

In 2012. I found that the curve

$$y^2 + xy + y = x^3 - x^2 - 5x + 5,$$

which is the curve 162.c3 in the LMFDB database has torsion $\mathbb{Z}/21\mathbb{Z}$ over $\mathbb{Q}(\zeta_9)^+$.

Note that this gives a sporadic point on $Y_1(21)$ and shows that $\Phi(3) \supsetneq \Phi_\infty(3)$ (while $\Phi(1) = \Phi_\infty(1)$ and $\Phi(2) = \Phi_\infty(2)$).

Torsion groups over cubic fields

Finally, in 2021 the full classification was proved:

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

$\Phi(3) = \Phi_\infty(3) \cup \{\mathbb{Z}/21\mathbb{Z}\}$. *Moreover, the elliptic curve 162.c3 over* $\mathbb{Q}(\zeta_9)^+$ *is the only elliptic curve with* $\mathbb{Z}/21\mathbb{Z}$ *torsion over any cubic field.*

Torsion groups over quartic fields

Jeon, Kim and Park proved in 2006 that $\Phi_\infty(4)$ consists of the following groups:

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1 - 18, 20, 21, 22, 24\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, && n = 1 - 9\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, && n = 1 - 3\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, && n = 1, 2\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

Derickx, Kamienny, Stein and Stoll proved in 2021 that $S(4) = \{2, 3, 5, 7, 11, 13, 17\}$.

Torsion groups over quartic fields

Hence to determine $\Phi(4)$, we need to determine the quartic points on $Y_1(m,n)$ for all (m,n) such that $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ satisfies:

- G occurs only finitely many times as a quartic torsion group,
- for every proper subgroup $H \subsetneq G$, the group H occurs infinitely often as a quartic torsion group,
- $|G|$ is divisible only by primes ≤ 17.
- if G contains a subgroup isomorphic to $(\mathbb{Z}/k\mathbb{Z})^2$, then $\varphi(k)|4$,

There are 43 such groups. 14 of these have been ruled out in previous work of P. Bruin and N. in 2016.

The genus of $X_1(289)$ is 3269, the largest of the curves we need to deal with.

Torsion groups over quartic fields

Theorem (Derickx, N. 2025)

If K varies over all quartic number fields and E varies over all elliptic curves over K, the groups that appear as $E(K)_{\mathrm{tors}}$ are exactly the following

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1-18, 20, 21, 22, 24,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, && n = 1-9,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, && n = 1-3,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, && n = 1, 2,\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

In particular, we have $\Phi(4) = \Phi_\infty(4)$.

Sporadic points on $X_1(n)$

Why look at quartic torsion?

Obvious answer: 4 comes after 3.

Sporadic points on $Y_1(n)$ give another motivation. We saw that there are no sporadic points of degree 1 and 2, and that there exist sporadic cubic points on $Y_1(n)$. We have proved that there are no degree 4 sporadic points on $Y_1(n)$.

Kamienny to Mazur: *The existence of sporadic points always left me scratching my head. Do they fit into a framework, or is it just nature being unkind?*

Sporadic points on $X_1(n)$

van Hoeij did a search for sporadic points on $Y_1(n)$ in 2014, and from his results, one can work out the existence of sporadic points on $Y_1(n)$ of degree $5 \leq d \leq 13$.

Clark, Genao, Pollack and Saia proved in 2022. that $Y_1(n)$ has sporadic points for all $n \geq 721$ (of unspecified degree).

Conjecture (Derickx, N.)

There are sporadic points on modular curves $Y_1(n)$ of every degree except $1, 2$ and 4.

Sporadic points on $X_0(n)$

Conjecture (Derickx, N. 2025)

There are sporadic points on modular curves $Y_0(n)$ of every degree.

Theorem (Derickx, N. 2025)

There are sporadic points on modular curves $Y_0(n)$ of every degree $d \leq 2166$, and every degree d such that there exists an imaginary quadratic field with class number d.

It is widely believed that there exists an imaginary quadratic field with every class number d.

Mazur's method for $\Phi(1)$

The basic strategy of Mazur's proof that $X_1(p)$ has no non-cuspidal rational points for $p > 13$ was as follows:

1) Let $P \in E(\mathbb{Q})$ be a point of order p; $x = (E, P) \in Y_1(p)(\mathbb{Q})$.
2) Since the reduction modulo a good prime q is injective on the torsion, by the Hasse bound it follows that E cannot have good reduction modulo 3. Hence $x_{\mathbb{F}_3} = c_{\mathbb{F}_3}$ is a cusp.
3) Moreover WLOG, $c_{\mathbb{F}_3}$ maps to the cusp $\infty_{\mathbb{F}_3}$ of $X_0(p)$.
4) It is shown using *formal immersions* that there can be only a single point of $X_0(p)(\mathbb{Q})$ reducing to $\infty_{\mathbb{F}_3}$.
5) We know that $\infty_{\mathbb{Q}} \in X_0(p)(\mathbb{Q})$ reduces to $\infty_{\mathbb{F}_3}$, hence x cannot exist.

Method for $\Phi(2)$ and $\Phi(3)$

The same underlying ideas were used to determine $\Phi(2)$ after adapting the methods to work on $X_1(m,n)^{(d)}$.

Derickx, Etropolski, Van Hoeij, Morrow and Zureick-Brown combined this approach with general methods for curves in a computational tour de force to prove $\Phi(3)$.

Our methods of proving $\Phi(4)$

Using the same approach as for lower degrees is hopeless, at least for most curves $X_1(m, n)$ we need to deal with.

We deal with most cases using 3 methods: the *good reduction method*, the *Hecke sieve* and the *global method*.

Only the Hecke sieve requires computation, and not too much.

These methods eliminate all but 2 groups, which are then eliminated by ad hoc methods.

The computations for all these groups took about 6.5 CPU hours on a 10-year-old server at the University of Zagreb.

All this means that our methods are much more suitable to tackling the same question over higher degree number fields.

Good reduction

Proposition

Let p be an odd prime not dividing $n > 4$, and d an integer. Suppose $\mathrm{rk}\, J_1(n)(\mathbb{Q}) = 0$ *and suppose that* $\mathrm{gon}_{\mathbb{Q}} X_1(n) > d$. *Then every elliptic curve E over a degree d number field K with torsion $\mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ has good reduction at at least one prime of K above p.*

In the paper we have a more general version of this result which deals with $X_1(m, n)/\mathbb{Q}(\zeta_m)$.

Good reduction

Sketch of proof: Fix primes $\mathfrak{q}$ of $\mathbb{Q}(\zeta_n)$ and $\mathfrak{q}'$ of K above p.

Let $x \in Y_1(n)(K)$ be a point representing (E, P) for some point P. Denote the corresponding point $x^{(d)} \in X_1^{(d)}(n)(\mathbb{Q})$ and $\tilde{x}^{(d)} \in X_1^{(d)}(n)(\mathbb{F}_{\mathfrak{q}'})$ its reduction modulo $\mathfrak{q}'$.

If E had additive reduction modulo $\mathfrak{q}'$, then the point of order n would have to reduce to $\tilde{E}(\mathbb{F}_{\mathfrak{q}'})$, which is of order $a \cdot \#\mathbb{F}_{\mathfrak{q}'}$, where $a \leq 4$, which is not divisible by n, so impossible.

Good reduction

Assume E has multiplicative reduction at all primes of K above p. Then $\tilde{x}^{(d)}$ has to be a sum of reductions modulo $\mathfrak{q}$ of $\mathbb{Q}(\zeta_n)$-rational cusps, i.e., $\tilde{x}^{(d)} = \widetilde{C}$ for some effective cuspidal divisor $C \in X_1^{(d)}(n)(\mathbb{Q}(\zeta_n))$.

Let $c_0 \in X_1(n)(\mathbb{Q})$ be a fixed cusp.

We have

$$[x^{(d)} - C] = [x^{(d)} - dc_0] + [dc_0 - C].$$

Since $[x^{(d)} - dc_0] \in J_1(n)(\mathbb{Q}) = J_1(n)(\mathbb{Q})_{\mathrm{tors}}$ and since $dc_0 - C$ is a cuspidal divisor, by Manin-Drinfeld $[dc_0 - C]$ is torsion, so $[x^{(d)} - C] \in J_1(n)(\mathbb{Q}(\zeta_n))_{\mathrm{tors}}$.

Reduction mod $\mathfrak{q}$ is injective on $J_1(n)(\mathbb{Q}(\zeta_n))_{\mathrm{tors}}$, since p is unramified in $\mathbb{Q}(\zeta_n)$, so it follows that $[x^{(d)} - C] = [C - x^{(d)}] = 0$.

Good reduction

So there is a nonconstant function $f \in H^0(X_1(n)_{\mathbb{Q}(\zeta_n)}, \mathcal{O}(x^{(d)}))$.

Since the dimension of $H^0(X_1(n)_{\mathbb{Q}}, \mathcal{O}(x^{(d)}))$ is invariant under base change one has that $H^0(X_1(n)_{\mathbb{Q}}, \mathcal{O}(x^{(d)})) \geq 2$ as well and hence $\text{gon}_{\mathbb{Q}} X_1(n) \leq d$, which is a contradiction. □

This proposition is very useful when there are no elliptic curves with a point of order n over $\mathbb{F}_{p^k}$ for all $k \leq d$.

For example this happens when n is larger than $(\sqrt{p}+1)^{2d}$.

Then curves over number fields of degree d with a point of order n have to have bad reduction at all primes above p.

When n satisfies this it immediately proves the non-existence points of order n over degree d fields.

What goes wrong and how to save things

This allows us to eliminate 11 groups immediately.

However, the issue is that when n is not too large, there usually exist elliptic curves over $\mathbb{F}_{p^d}$ with a point of order n, hence there exist non-cuspidal divisors in $X_1(n)^{(d)}(\mathbb{F}_p)$.

We want to show that these are not reductions of rational divisors in $X_1(n)^{(d)}(\mathbb{Q})$.

Our strategy is to test whether these divisors behave in a way that is not compatible with being reductions of rational divisors.

We will act on them with Hecke operators. We call this the Hecke sieve.

Hecke operators

Let $q \nmid n$ be a prime. The diamond operator $\langle q \rangle$ acts on $X_1(n)$ as

$$\langle q \rangle (E, P) = (E, qP).$$

The Hecke operator T_q acts on $X_1(n)$ as:

$$T_q(E, P) = \sum_{G \subseteq E[q] \text{ of order } q} (E/G, P \bmod G).$$

Denote

$$A_q := T_q - q\langle q \rangle - 1.$$

Proposition

$$A_q(J_1(n)(\mathbb{Q})_{\mathrm{tors}}) = 0.$$

Hecke operators

Lemma

There exists a cusp $C_0 \in X_1(n)(\mathbb{Q})$ such that $A_q(C_0) = 0$.

Lemma

Suppose $\mathrm{rk}\, J_1(n)(\mathbb{Q}) = 0$. *Then for any $x^{(d)} \in X_1(n)^{(d)}(\mathbb{Q})$ we have $[A_q(x^{(d)})] = 0$.*

Proof:

Let $C_0 \in X_1(n)$ be a cusp such that $A_q(C_0) = 0$.

Let $y = [x^{(d)} - dC_0] \in J_1(n)(\mathbb{Q})$.

We have

$$0 = [A_q(y)] = [A_q(x^{(d)})] - [dA_q(C_0)] = [A_q(x^{(d)})].$$

The Hecke sieve

Proposition (Hecke Sieve)

Let p, q be different primes not dividing n. Assume $\operatorname{rk} J_1(n)(\mathbb{Q}) = 0$.

Then $x^{(d)} \in X_1(n)^{(d)}(\mathbb{Q})$ cannot reduce to $D \in X_1(n)^{(d)}(\mathbb{F}_p)$ such that $[A_q(D)] \neq 0$.

Note that the q is allowed to vary.

The Hecke sieve allows us to rule out all the remaining curves with rank 0 Jacobian, except 1 which needs some additional arguments.

The global method

To deal with the positive rank cases, we use the *global* or the *Derickx-Stoll* method.

The ideas originate from Maarten's PhD thesis, and were further developed recently by Maarten and Michael Stoll.

Proposition

Let $\operatorname{rk} J_1(n)(\mathbb{Q}) = \operatorname{rk} J_0(n)(\mathbb{Q})$ *and* $q \nmid n$ *be an odd prime, and let* $a \in (\mathbb{Z}/n\mathbb{Z})^\times/\langle -1\rangle$ *such that the order of* a *does not divide* d*. Then if* $\operatorname{gon}_{\mathbb{Q}} X_1(n) > 2(q+1)d$*, there is a cusp or a CM point in the support of every* $D \in X_1(n)^{(d)}(\mathbb{Q})$*.*

The global method

Proposition

Let $\operatorname{rk} J_1(n)(\mathbb{Q}) = \operatorname{rk} J_0(n)(\mathbb{Q})$ *and* $q \nmid n$ *be an odd prime and suppose there exists an* $a \in (\mathbb{Z}/n\mathbb{Z})^\times/\langle -1\rangle$ *such that the order of* a *does not divide* d*. Then if* $\operatorname{gon}_{\mathbb{Q}} X_1(n) > 2(q+1)d$*, there is a cusp or a CM point in the support of all* $D \in X_1(n)^{(d)}(\mathbb{Q})$*.*

Sketch of proof: Let $D \in Y_1(n)^{(d)}(\mathbb{Q})$ with no CM points in its support.

Note that $\langle a\rangle$ acts trivially on $J_0(n)(\mathbb{Q})$, so $(\langle a\rangle - 1)J_0(n)(\mathbb{Q}) = 0$, so

$$[(\langle a\rangle - 1)D] \in J_1(n)(\mathbb{Q})_{\mathrm{tors}},$$

so

$$[A_q(\langle a\rangle - 1)D] = 0.$$

The global method

Since the polar divisor of $A_q(\langle a \rangle - 1)D$ is of degree $\leq 2(q+1)d$, it follows that

$$A_q(\langle a \rangle - 1)D = 0.$$

By considering the moduli interpretation of A_q and $\langle a \rangle$, one sees that this is impossible unless there is at least one point in the support fixed by some power of $\langle a \rangle$ that is not the identity.

The fixed points of the diamond operators are cusps or CM points which completes the proof.

The global method

Example

Let $n = 289$. We have $\mathrm{gon}_{\mathbb{Q}} X_1(289) \geq 413$, and

$$\mathrm{rk}\, J_1(289)(\mathbb{Q}) = \mathrm{rk}\, J_0(289)(\mathbb{Q}) > 0.$$

We choose $3 = a \in (\mathbb{Z}/289\mathbb{Z})^\times / \langle -1 \rangle$ of order 136.

Clark, Genao, Pollack and Saia have shown that the smallest degree of a CM point on $X_1(289)$ is known to be 136.

Applying the proposition we get that $X_1(289)$ has no non-cuspidal non-CM points of degree ≤ 52.

In the paper, by using a more general version of the theorem we get that there are no non-cuspidal points of degree ≤ 59.

Higher degrees

$S(d)$ was determined for $5 \leq d \leq 7$ by Derickx, Kamienny, Stein and Stoll in 2021, and $S(8)$ was determined by Khawaja in 2024.

$\Phi_\infty(5)$ and $\Phi_\infty(6)$ were determined by Derickx and Sutherland in 2016.

Our methods are suitable for higher-degree number fields.

We apply our methods (without any computation) to degree 5, and eliminate more than half the groups necessary to determine $\Phi(5)$.

Thank you for your attention!