Torsion groups of elliptic curves over infinite Abelian extensions of $\mathbb{Q}$

BARCELONA, DECEMBER 5-7, 2019

Ivan Krijan

University of Zagreb, Department of Mathematics

ivan.krijan@math.hr

Abstract

We determine, for an elliptic curve $E/\mathbb{Q}$ and for all primes p, all the possible torsion groups $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$, where $\mathbb{Q}_{\infty,p}$ is the $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We do the same thing for the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{Q}$.

Introduction

For a prime number p, denote by $\mathbb{Q}_{\infty,p}$ the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and for a positive integer n, denote by $\mathbb{Q}_{n,p}$ the n^{th} layer of $\mathbb{Q}_{\infty,p}$, i.e. the unique subfield of $\mathbb{Q}_{\infty,p}$ such that $\mathrm{Gal}\left(\mathbb{Q}_{n,p}/\mathbb{Q}\right) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Recall that the $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is the unique Galois extension $\mathbb{Q}_{\infty,p}$ of $\mathbb{Q}$ such that

$$\mathrm{Gal}\left(\mathbb{Q}_{\infty,p}/\mathbb{Q}\right) \simeq \mathbb{Z}_p,$$

where $\mathbb{Z}_p$ is the additive group of the p-adic integers and is constructed as follows. Let

$$G = \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}\right) = \varprojlim_n \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}\right) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Here we know that $G = \Delta \times \Gamma$, where $\Gamma \simeq \mathbb{Z}_p$ and $\Delta \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ for $p \geq 3$ and $\Delta \simeq \mathbb{Z}/2\mathbb{Z}$ (generated by complex conjugation) for $p = 2$, so we define

$$\mathbb{Q}_{\infty,p} := \mathbb{Q}(\zeta_{p^\infty})^{\Delta}.$$

We also see that every layer is uniquely determined by

$$\mathbb{Q}_{n,p} = \mathbb{Q}(\zeta_{p^{n+1}})^{\Delta},$$

so for $p \geq 3$ it is the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$. More details and proofs of these facts about $\mathbb{Z}_p$-extensions and Iwasawa theory can be found in [8, Chapter 13].

Iwasawa theory for elliptic curves (see [5]) studies elliptic curves in $\mathbb{Z}_p$-extensions, in particular the growth of the rank and n-Selmer groups in the layers of the $\mathbb{Z}_p$-extensions.

We completely solve the problem of determining how the torsion of an elliptic curve defined over $\mathbb{Q}$ grows in the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. These results, interesting in their own right, might also find applications in other problems in Iwasawa theory for elliptic curves and in general. For example, to show that elliptic curves over $\mathbb{Q}_{\infty,p}$ are modular for all p, Thorne [7] needed to show that $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ for two particular elliptic curves.

Main results

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $p \geq 5$ be a prime number. Then*

$$E(\mathbb{Q}_{\infty,p})_{tors} = E(\mathbb{Q})_{tors}.$$

Theorem 2. *$E(\mathbb{Q}_{\infty,2})_{tors}$ is exactly one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && 1 \leq N \leq 10, \text{ or } N = 12, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && 1 \leq N \leq 4, \end{aligned}$$

and for each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathbb{Q}_{\infty,2})_{tors} \simeq G$.

Theorem 3. *$E(\mathbb{Q}_{\infty,3})_{tors}$ is exactly one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && 1 \leq N \leq 10, \text{ or } N = 12, 21 \text{ or } 27, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && 1 \leq N \leq 4. \end{aligned}$$

and for each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathbb{Q}_{\infty,3})_{tors} \simeq G$.

By Mazur's [6] theorem we see that

$$\begin{aligned} \{E(\mathbb{Q}_{\infty,2})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} &= \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\}, \\ \{E(\mathbb{Q}_{\infty,3})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} &= \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} \cup \{\mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}. \end{aligned}$$

However, given a specific $E/\mathbb{Q}$ it is not necessarily the case that $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$. Indeed there are many elliptic curves for which torsion grows from $\mathbb{Q}$ to $\mathbb{Q}_{\infty,p}$, and we investigate this question further. Specifically, for each prime p we find for which groups G there exists infinitely many j-invariants j such that there exists an elliptic curve $E/\mathbb{Q}$ with $j(E) = j$ and such that $E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}} \simeq G$.

Torsion growth

Theorem 4. *Let G be one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && 3 \leq N \leq 10, \text{ or } N = 12, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && 1 \leq N \leq 4, \end{aligned}$$

There exist infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariants such that $E(\mathbb{Q}_{\infty,2})_{tors} \simeq G$ and $E(\mathbb{Q})_{tors} \not\simeq G$.

Theorem 5. *There exist infinitely many $j \in \mathbb{Q}$ such that there exists elliptic curve $E/\mathbb{Q}$ with j-invariant j and*

$$E(\mathbb{Q})_{tors} \simeq \{0\} \qquad \text{and} \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Furthermore, there exist infinitely many $j \in \mathbb{Q}$ such that there exists elliptic curve $E/\mathbb{Q}$ with $j(E) = j$ and

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \qquad \text{and} \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Theorem 6. *There exist infinitely many $j \in \mathbb{Q}$ such that there exists elliptic curve $E/\mathbb{Q}$ with j-invariant j and*

$$E(\mathbb{Q})_{tors} \simeq \{0\} \qquad \text{and} \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}.$$

Theorem 7. *There exist infinitely many $j \in \mathbb{Q}$ such that there exists elliptic curve $E/\mathbb{Q}$ with $j(E) = j$ and*

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \qquad \text{and} \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/9\mathbb{Z}.$$

Examples of torsion growth

Next table lists elliptic curves of minimal conductor with torsion growth $\mathbb{Q} \to \mathbb{Q}_{\infty,2}$.

Cremona label	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,2})_{\text{tors}}$
704d1	$\{0\}$	$\mathbb{Z}/3\mathbb{Z}$
24a6	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$
704a1	$\{0\}$	$\mathbb{Z}/5\mathbb{Z}$
320c1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$
832f	$\{0\}$	$\mathbb{Z}/7\mathbb{Z}$
24a3	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$
1728j3	$\{0\}$	$\mathbb{Z}/9\mathbb{Z}$
768b1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/10\mathbb{Z}$
30a5	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$
14a5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
24a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
14a2	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
32a4	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

Next table lists elliptic curves of minimal conductor with torsion growth $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$.

Cremona label	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,3})_{\text{tors}}$
162b1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/21\mathbb{Z}$
27a4	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/27\mathbb{Z}$
324a2	$\{0\}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
324a1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
162b2	$\{0\}$	$\mathbb{Z}/7\mathbb{Z}$
27a3	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$

Compositum

Theorem 8. *Let $E/\mathbb{Q}$ be an elliptic curve, then*

$$E\left(\prod_{p \geq 5 \text{ prime}} \mathbb{Q}_{\infty,p}\right)_{tors} = E(\mathbb{Q})_{tors}.$$

Conjecture 1. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E\left(\prod_{p \text{ prime}} \mathbb{Q}_{\infty,p}\right)_{tors}$ is exactly one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z}, && 1 \leq n \leq 10 \text{ ili } n \in \{12, 21, 27\}, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, && 1 \leq n \leq 4. \end{aligned}$$

For each group G from the list above there exists an $E/\mathbb{Q}$ such that $E\left(\prod_{p \text{ prime}} \mathbb{Q}_{\infty,p}\right)_{tors} \simeq G$.

Proof of this Conjecture is author's current work.

Main tools

In this work we heavily rely on results of H. B. Daniels, A. Lozano-Robledo, F. Najman and A. V. Sutherland in [3] and E. Gonzalez-Jimenez and F. Najman in [4]. For all computations author uses `magma` [2].

References

[1] M. Chou, H. Daniels, I. Krijan and F. Najman, *Torsion of elliptic curves over Zp extensions of* $\mathbb{Q}$, submitted.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235265.

[3] H. B. Daniels, A. Lozano-Robledo, F. Najman, A. V. Sutherland, *Torsion points on rational elliptic curves over the compositum of all cubic fields,* Math. Comp. **87** (2018), 425–458.

[4] E. Gonzalez-Jimenez, F. Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. to appear.

[5] R. Greenberg, *Iwasawa theory for elliptic curves*, In: Viola C. (eds) Arithmetic Theory of Elliptic Curves. Lecture Notes in Mathematics, vol 1716. Springer, Berlin, Heidelberg, 1999.

[6] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), pp. 129–162.

[7] J. A. Thorne, *Elliptic curves over* $\mathbb{Q}_\infty$ *are modular*, J. Eur. Math. Soc. (JEMS), to appear.

[8] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1997.

Acknowledgements

The author 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 Programme (Grant KK.01.1.1.01.0004).