Torsion groups of elliptic curves over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$

Ivan Krijan, ikrijan@math.hr
joint with M. Chou, H. B. Daniels and F. Najman

Department of Mathematics, University of Zagreb, Croatia

Representation Theory XVI,
Number Theory Section,
Dubrovnik, Croatia,
27. 06. 2019.

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/

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

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

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 za regionalni razvoj

Project co-financed by European Union through the European Regional Development Fund

$\mathbb{Z}_p$-extension

Let p be a prime number. $\mathbb{Z}_p$-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.

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

For a prime number $p \geq 3$, we know that $\mathbb{Z}_p^\times = \Delta \times \mathbb{Z}_p$, where $\Delta \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. We define

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

Every layer is uniquely determined by

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

$\mathbb{Z}_p$-extension

For $p = 2$ we have $\mathbb{Q}_{n,2} = \mathbb{Q}\left(\cos\left(\frac{\pi}{2^{n+1}}\right)\right)$ and $\mathbb{Q}_\infty = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_{n,2}$.

So, for a prime number p:

- $\mathbb{Q}_{\infty,p}$ is $\mathbb{Z}_p$-extension of $\mathbb{Q}$,
- $\mathbb{Q}_{n,p}$ is the n^{th} layer of $\mathbb{Q}_{\infty,p}$, i.e. we have

$$\mathbb{Q} = \mathbb{Q}_{0,p} \subset \mathbb{Q}_{1,p} \subset \mathbb{Q}_{2,p} \subset \cdots \subset \mathbb{Q}_{\infty,p}.$$

We determine, for an elliptic curve $E/\mathbb{Q}$ and for all 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 $\mathbb{Q}$.

Motivation

We know that (Mordel-Weil)

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r.$$

Iwasawa theory for elliptic curves 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.
In this work 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 needed to show that $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ for two particular elliptic curves.

Auxiliary results

Lemma (H. B. Daniels, A. Lozano-Robledo, F. Najman, A. V. Sutherland)

Let E be an elliptic curve over a number field K, let F be a Galois extension of $\mathbb{Q}$, let p be a prime, and let k be the largest integer for which $E[p^k] \subseteq E(F)$. If $E(F)_{tors}$ contains a subgroup isomorphic to $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$ with $j \geq k$, then E admits a K-rational p^{j-k}-isogeny.

Theorem (B. Mazur)

Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then

$$n \leq 19 \text{ or } n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

Auxiliary results

Corollary

Let p be an odd prime number, $E/\mathbb{Q}$ elliptic curve and $P \in E(\mathbb{Q}_{\infty,p})_{tors}$ a point of order q^n for some prime q and positive integer n, then

$$q^n \in \{2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 25, 27, 32, 37, 43, 67, 163\}.$$

Lemma

Let p and q be prime numbers such that $q - 1 \nmid p$ and $p \nmid q - 1$. Let $K/\mathbb{Q}$ be a cyclic extension of degree p, and $P \in E$ a point of degree q. If $P \in E(K)$, then $P \in E(\mathbb{Q})$.

Auxiliary results

Theorem (E. Gonzalez-Jimenez and F. Najman)

Let p be the smallest prime divisor of a positive integer d and let $K/\mathbb{Q}$ be a number field of degree d.

- *If $p \geq 11$, then $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*
- *If $p = 7$, then $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$, for all primes $q \neq 7$.*
- *If $p = 5$, then $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$, for all primes $q \neq 5, 7, 11$.*
- *If $p = 3$, then $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$, for all primes $q \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

Theorem

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

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

Proof.

For primes $p \geq 11$, we know that $E(\mathbb{Q}_{n,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, for each positive integer n. It follows that $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$. It remains to prove this fact for the cases $p = 7$ and $p = 5$.

Case $p = 7$. We only need to prove that $E(\mathbb{Q}_{\infty,7})[7^\infty] = E(\mathbb{Q})[7^\infty]$.

We conclude that there is no 49-torsion in $E(\mathbb{Q}_{\infty,7})$, so it remains to prove that $E(\mathbb{Q}_{\infty,7})[7] = E(\mathbb{Q})[7]$.

Let $P \in E(\mathbb{Q}_{\infty,7})$ be a point of order 7. Point P is then defined over some field of degree at most $7^2 - 1$. Therefore, $P \in E(\mathbb{Q}_{1,7})$. Now it now follows that $P \in E(\mathbb{Q})$ and we are done. □

Proof.

Case $p = 5$ reduces to showing that $E(\mathbb{Q}_{\infty,5})[11] = \{O\}$ and $E(\mathbb{Q}_{\infty,5})[25] = \{O\}$.

Let $P \in E(\mathbb{Q}_{\infty,5})$ be a point of order 11, then $P \in E(\mathbb{Q}_{1,5})$. The modular curve $X_1(11)$ is the elliptic curve $y^2 + y = x^3 - x^2$. We can easily compute (using Magma) that $X_1(11)$ has rank 0 and torsion $\mathbb{Z}/5\mathbb{Z}$ over $\mathbb{Q}_{1,5}$, and all the torsion points are cusps, so there are no elliptic curves with 11-torsion over $\mathbb{Q}_{1,5}$.

For $E(\mathbb{Q}_{\infty,5})[25]$ we compute that

$$G_{\mathbb{Q}}(25) = \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z},\ b \in \{7, -1, -7, 1\} \right\}.$$

Finally, we calculate that

$600 = [\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_{\mathbb{Q}}(25)] \mid [\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : im(\overline{\rho}_{5,E})]$, a contradiction with a Theorem of R. Greenberg which states that the index $[\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : im(\overline{\rho}_{5,E})]$ isn't divisible by 25. □

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. $E(\mathbb{Q}_{\infty,3})_{tors}$ is exactly one of the following groups:

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

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

If $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ is isomorphic to one of the following groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \leq N \leq 6, \text{ or } N = 8, 10 \text{ or } 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad N = 2 \text{ or } 4, \end{aligned}$$

then $E(\mathbb{Q}_{\infty,3})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$.

- Growth (from $\mathbb{Q}$ to $\mathbb{Q}_{\infty,3}$)

$$\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z} \qquad \text{and} \qquad \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}$$

  appears for finitely many different j-invariants, because $X_0(21)$ and $X_0(27)$ have finitely many rational points.
- For all the other cases there exist infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariants such that $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq G$ and $E(\mathbb{Q})_{\text{tors}} \not\simeq G$.
- For example, elliptic curve (Cremona label 324a1) $y^2 = x^3 - 21x + 37$ has torsion $\mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Q}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}_{\infty,3}$.

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

Cremona lebel	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,3})_{\text{tors}}$
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	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. $E(\mathbb{Q}_{\infty,2})_{tors}$ is exactly one of the following groups:

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

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

- Let G be one of the following groups:

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

  There exist infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariants such that $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq G$ and $E(\mathbb{Q})_{\text{tors}} \not\simeq G$.
- Again, for example elliptic curve $y^2 = x^3 - 876x + 13232$ (Cremona label 1728j3) has torsion $\{0\}$ over $\mathbb{Q}$ and torsion $\mathbb{Z}/9\mathbb{Z}$ over $\mathbb{Q}_{\infty,2}$, more precisely already over $\mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$.

This 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	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

Sketch of the proof of $\mathbb{Q}_{\infty,3}$ case

- Result by E. Gonzalez-Jimenez and F. Najman (which tells us possibilities for $[\mathbb{Q}(P):\mathbb{Q}]$, where P is a point of order p on E) tells us that $E(\mathbb{Q}_{\infty,3})[q^\infty] = \{0\} = E(\mathbb{Q})[q^\infty]$, for all prime numbers q different from 2, 3, 5, 7, 13 and 19.
- We prove that $E(\mathbb{Q}_{\infty,3})$ does not contain a point of order 19 nor a point of order 13.
- Next step is proving that $E(\mathbb{Q}_{\infty,3})[5^\infty] = E(\mathbb{Q})[5^\infty]$.
- We show that if $E(\mathbb{Q}_{\infty,3})$ contains a point of order 7, then $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ is $\mathbb{Z}/7\mathbb{Z}$ or $\mathbb{Z}/21\mathbb{Z}$.
- if $E(\mathbb{Q})[2^\infty] \subsetneq E(\mathbb{Q}_{\infty,3})[2^\infty]$, then

$$E(\mathbb{Q}_{\infty,3})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

- $E(\mathbb{Q}_{\infty,3})$ does not contain a point of order 18.
- Finally, if $E(\mathbb{Q}_{\infty,3})[3^\infty] \simeq \mathbb{Z}/3\mathbb{Z}$, then $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ is one of the following groups

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/21\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Sketch of the proof of $\mathbb{Q}_{\infty,2}$ case

- Again, by E. Gonzalez-Jimenez and F. Najman we conclude that $E(\mathbb{Q}_{\infty,2})[q^\infty] = \{0\} = E(\mathbb{Q})[q^\infty]$ for all prime numbers q different from 2, 3, 5, 7, 13 and 17.
- We prove that $E(\mathbb{Q}_{\infty,2})$ does not contain a point of order 17 nor a point of order 13.
- If $E(\mathbb{Q}_{\infty,2})$ contains point of order 7, then $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$ is $\mathbb{Z}/7\mathbb{Z}$.
- If $E(\mathbb{Q}_{\infty,2})$ contains point of order 5, then $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$ is $\mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/10\mathbb{Z}$.
- If $E(\mathbb{Q}_{\infty,2})$ contains point of order 9, then $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$ is $\mathbb{Z}/9\mathbb{Z}$.
- If $E(\mathbb{Q}_{\infty,2})$ contains point of order 12, then $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$ is $\mathbb{Z}/12\mathbb{Z}$.
- Finally we use result of Y. Fujita which states that $E(\mathbb{Q}_{\infty,2})[2^\infty] \leq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Thank you for your attention!