Torsion subgroups of rational elliptic curves over some cyclotomic fields

Dubrovnik, Croatia

Borna Vukorepa

Faculty of Science
Department of Mathematics
University of Zagreb

26. 6. 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

Project co-financed by European Union through the

Motivation

- **Theorem 1 (M. Chou):** Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}^{ab})_{tors}$ is isomorphic to the one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, \ldots, 8, 9$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 3$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}, \quad m = 1, 2, 3, 4$$
$$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$
$$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Known useful results

- **Proposition 1:** Let $E/\mathbb{Q}$ be an elliptic curve, $n \in \mathbb{N}$ i K finite Galois extension of $\mathbb{Q}$. Let $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$ and $P \in E(K)$ point of order n. Then we have:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid M(\phi(n), [K : \mathbb{Q}]),$$

  where $M(\cdot, \cdot)$ is the greatest common divisor and ϕ is the Euler function.

Known useful results

- **Proof:** Let P be a point of order n with coordinates in K. Then we can take $Q \in E[n]$ such that $\{P, Q\}$ is a basis for $E[n]$. Consider the Galois representation modulo n with respect to E:

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z}).$$

Let $\sigma \in Gal(K/\mathbb{Q})$. Then we have $P^\sigma = \alpha P + \beta Q$ for some $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ because the action of σ on P preserves the order of a point.

Known useful results

- **Proof:** Let P be a point of order n with coordinates in K. Then we can take $Q \in E[n]$ such that $\{P, Q\}$ is a basis for $E[n]$. Consider the Galois representation modulo n with respect to E:

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z}).$$

  Let $\sigma \in Gal(K/\mathbb{Q})$. Then we have $P^\sigma = \alpha P + \beta Q$ for some $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ because the action of σ on P preserves the order of a point.

- From $P^\sigma - \alpha P = \beta Q$ follows $\beta Q \in E(K)$. If we had $\beta \neq 0$, the group $E(K)[n]$ would be bigger than $\mathbb{Z}/n\mathbb{Z}$. Thus, $\beta = 0$, so $P^\sigma \in \langle P \rangle$ for all $\sigma \in Gal(K/\mathbb{Q})$. Because of preserving the order, α has to be in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Known useful results

- Since by considering the restriction map we get $Gal(K/\mathbb{Q}) \cong Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Gal(\overline{\mathbb{Q}}/K)$, we have $P^\sigma \in \langle P \rangle$ for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\rho(\sigma) = \begin{pmatrix} \varphi(\sigma) & \tau(\sigma) \\ 0 & \psi(\sigma) \end{pmatrix},$$

where $\varphi, \psi, \tau : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z}$, and φ, ψ are homomorphisms with image in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Known useful results

- Since by considering the restriction map we get $Gal(K/\mathbb{Q}) \cong Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Gal(\overline{\mathbb{Q}}/K)$, we have $P^\sigma \in \langle P \rangle$ for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\rho(\sigma) = \begin{pmatrix} \varphi(\sigma) & \tau(\sigma) \\ 0 & \psi(\sigma) \end{pmatrix},$$

  where $\varphi, \psi, \tau : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z}$, and φ, ψ are homomorphisms with image in $(\mathbb{Z}/n\mathbb{Z})^\times$.
- We know that $P^\sigma = gP \Leftrightarrow \varphi(\sigma) = g$, for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, we have:

$$|Im(\varphi)| = |\{P^\sigma : \sigma \in Gal(K/\mathbb{Q})\}| = |Orb(P)|.$$

Known useful results

- It is clear that $\mathrm{Stab}(P) = Gal(K/\mathbb{Q}(P))$, so by orbit and stabilizer theorem we have:

$$|Im(\varphi)| = \frac{|Gal(K/\mathbb{Q})|}{|Gal(K/\mathbb{Q}(P))|} = [\mathbb{Q}(P) : \mathbb{Q}].$$

On the other hand, we have $Im(\varphi) \leq (\mathbb{Z}/n\mathbb{Z})^{\times}$, so we have:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(n).$$

$[\mathbb{Q}(P) : \mathbb{Q}] \mid [K : \mathbb{Q}]$ is obvious and the proof is complete.

Known useful results

- **Proposition 2:** Let $E/\mathbb{Q}$ be an elliptic curve and K a finite extension of $\mathbb{Q}$. If we have $E[m] \subseteq E(K)$, then we have $\zeta_m \subseteq K$.
- **Proof:** From the existence and properties of Weil pairing.

Known useful results

- **Theorem 2 (Najman):** Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quadratic extension. Then $E(K)_{tors}$ is isomorphic to the one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, \ldots, 9, 10, 12, 15, 16$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, 3, 4, 5, 6$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 2$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

$\mathbb{Z}/15\mathbb{Z}$ is the only group which appears in only finitely many cases, and only over the extensions $\mathbb{Q}(\sqrt{5})$ i $\mathbb{Q}(\sqrt{-15})$.

Known useful results

- **Theorem 3 (Najman):** Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a cubic extension. Then $E(K)_{tors}$ is isomorphic to the one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, \ldots, 10, 12, 13, 14, 18, 21$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, 3, 4, 7.$$

  $\mathbb{Z}/21\mathbb{Z}$ is the only group which appears in only finitely many cases, and only over the extension $\mathbb{Q}(\zeta_9)^+$.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of the following groups from Theorem 1:

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}, \quad m \geq 3.$$

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of the following groups from Theorem 1:

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}, \quad m \geq 3.$$

- **Proof:** Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. Then $E[n] \subseteq E(\mathbb{Q}(\zeta_{11}))$, so by the existence of the Weil pairing we have $\zeta_n \in \mathbb{Q}(\zeta_{11})$. That would mean $n \in \{1, 2, 11, 22\}$. The conclusion follows.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 13, 14, 15, 17, 18, 19, 21, 27, 37, 43, 67, 163.$$

Torzija nad $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 13, 14, 15, 17, 18, 19, 21, 27, 37, 43, 67, 163.$$

- **Proof:** Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/m\mathbb{Z}$ for some m from the statement. Then $E(\mathbb{Q}(\zeta_{11}))[m] \cong \mathbb{Z}/m\mathbb{Z}$ so we can use Proposition 1. If P is of order m, we have:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid M(\phi(m), 10).$$

It is easy to check that for all m in the statement we get:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid 2.$$

Therefore, that torsion appears already over quadratic extension, which is impossible by Theorem 2, except $m = 15$. But then we would have $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{-15})$. Since the only intermediate quadratic extension in this case is $\mathbb{Q}(\sqrt{-11})$, $m = 15$ is also impossible.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of these groups:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}.$$

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proof:** We will prove the statement for $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, the others go analogously. We just imitate the proof of the earlier proposition. Let $P \in E(\mathbb{Q}(\zeta_{11}))$ be of order 16 and let $\{P, Q\}$ be the basis for $E[16]$. Take $\sigma \in Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q})$. Because the order is preserved, we have $P^\sigma = aP + bQ$. From that it is easy to see that $b \in \{0, 8\}$. Multiplying by 2 we get $(2P)^\sigma = a(2P)$.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proof:** We will prove the statement for $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, the others go analogously. We just imitate the proof of the earlier proposition. Let $P \in E(\mathbb{Q}(\zeta_{11}))$ be of order 16 and let $\{P, Q\}$ be the basis for $E[16]$. Take $\sigma \in Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q})$. Because the order is preserved, we have $P^\sigma = aP + bQ$. From that it is easy to see that $b \in \{0, 8\}$. Multiplying by 2 we get $(2P)^\sigma = a(2P)$.
- $\{2P, 2Q\}$ is the basis for $E[8]$ and we can continue as in the proof of the proposition and conclude:

$$[\mathbb{Q}(2P) : \mathbb{Q}] \mid \phi(8) = 4.$$

Therefore, $\mathbb{Q}(2P)$ is either trivial or quadratic extension of $\mathbb{Q}$, because the degree also divides 10. We will prove that this implies that $\mathbb{Q}(P)$ is also trivial or quadratic extension of $\mathbb{Q}$.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proof:** Put $x(P) = x$ and let E be given by $y^2 = x^3 + bx + c$. Since $2P \neq O$, we have non-zero denominator in point duplication formula, so we get:

$$x^4 - 4x(2P)x^3 - 2bx^2 - (8c + 4bx(2P))x + b^2 - 4cx(2P) = 0.$$

This gives us $[\mathbb{Q}(x(P)) : \mathbb{Q}(x(2P))] \leq 4$, because $x(P)$ satisfies that equation. Combined with $[\mathbb{Q}(x(2P)) : \mathbb{Q}] \leq 2$, we get $[\mathbb{Q}(x(P)) : \mathbb{Q}] \leq 8$, but it is clear that factor 5 can't appear, so $\mathbb{Q}(x(P))$ is also trivial or quadratic extension of $\mathbb{Q}$. We also have:

$$y(P)^2 - x(P)^3 - bx(P) - c = 0,$$

so $[\mathbb{Q}(P) : \mathbb{Q}(x(P))] \leq 2$. Thus $[\mathbb{Q}(P) : \mathbb{Q}] \leq 4$, but since it also divides 10, we have that $\mathbb{Q}(P)$ is trivial or quadratic extension of $\mathbb{Q}$.

Torsion over $\mathbb{Q}(\zeta_{11})$

- P now generates torsion subgroup $\mathbb{Z}/16\mathbb{Z}$ which can still appear over quadratic extensions. $E(\mathbb{Q}(\zeta_{11}))$ has a point S of order 2 which is not in $\langle P \rangle$. Her y-coordinate is 0 and x-coordinate is a zero of third degree polynomial in $\mathbb{Q}[x]$, so $[\mathbb{Q}(S) : \mathbb{Q}] \leq 3$. But $3 \nmid 10$, so $[\mathbb{Q}(S) : \mathbb{Q}] \leq 2$. Now both P and S have coordinates in $\mathbb{Q}(\sqrt{-11})$, which is a contradiction with Theorem 2.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of these groups:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/16\mathbb{Z}.$$

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to any of these groups:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/16\mathbb{Z}.$$

- **Proof:** First we reduce the statement in both cases to the quadratic extension $\mathbb{Q}(\sqrt{-11})$ with the same methods as above. After that, we use standard methods of computing in Magma.

Torsion over $\mathbb{Q}(\zeta_{11})$

- $X_1(2,12)(\mathbb{Q}(\sqrt{-11}))$ has rank 0 and the same torsion as over $\mathbb{Q}$. Since $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ does not appear as a torsion over $\mathbb{Q}$, that group doesn't appear in this extension.
- For the second group, we consider the Jacobian $J_1(16)(\mathbb{Q}(\sqrt{-11}))$ of $X_1(16)(\mathbb{Q}(\sqrt{-11}))$. We compute that it has rank 0, two torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and points of odd order form the group $\mathbb{Z}/5\mathbb{Z}$.
- We also compute that $J_1(16)(\mathbb{Q})$ contains 20 points. After injecting $J_1(16)(\mathbb{Q}(\sqrt{-11}))$ into residue fields modulo prime ideal lying over p for several primes p (3), we are able to conclude that $\#J_1(16)(\mathbb{Q}(\sqrt{-11})) \mid 20$, so it also has 20 points.

Torsion over $\mathbb{Q}(\zeta_{11})$

- By computing cusps on $X_1(16)$, we can use the Sym^2 map to conclude (using the simple counting argument) that all elements of our Jacobian arise from cusps. Alternatively, we can compute Mumford representations of divisor classes on the Jacobian and explicitly see which divisors come from which points, and conclude that all arise from cusps.

Torsion over $\mathbb{Q}(\zeta_{11})$

- **Theorem:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is isomorphic to the one of the groups from Mazur theorem or to the one of the following groups:

$$\mathbb{Z}/11\mathbb{Z} \quad (121b2),$$
$$\mathbb{Z}/25\mathbb{Z} \quad (11a3),$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \quad (10230bg2).$$

Torsion over $\mathbb{Q}(\zeta_8)$

- $\mathbb{Q}(\zeta_8)$ is a Galois extension with the Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, so Theorem 4 applies.
- **Theorem 4 (M. Chou):** Let $E/\mathbb{Q}$ be a rational elliptic curve and K a quartic Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then $E(K)_{tors}$ is isomorphic to the one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, \ldots, 10, 12, 15, 16$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, \ldots, 6, 8$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 2$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}, \quad m = 1, 2$$
$$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Torsion over $\mathbb{Q}(\zeta_8)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is not isomorphic to any of these groups from Theorem 4:

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 2$$
$$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

- **Proof:** Existence of Weil pairing, like before. $\mathbb{Q}(\zeta_8)$ does not contain ζ_3.

Torsion over $\mathbb{Q}(\zeta_8)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is not isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.
- **Proof:** Proved by Bruin, Najman by looking at $X_1(4,8)(\mathbb{Q}(\zeta_8))$.

Torsion over $\mathbb{Q}(\zeta_8)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is not isomorphic to $\mathbb{Z}/15\mathbb{Z}$.
- **Proof:** Assume the contrary. Let P be a point on E which generates the torsion group $\mathbb{Z}/15\mathbb{Z}$. Every $\sigma \in Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ is of order 2, so $P^{\sigma^2} = P$.
- By identical reasoning as in Proposition 1, we get $P^\sigma = kP$, where $k^2 \equiv 1 \pmod{15}$. Solving this congruence gives $k \in \{1, -1, 4, -4\}$.
- Assume that P is not from some smaller field, but precisely from $\mathbb{Q}(\zeta_8)$. That means that all $\sigma \in Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ act differently on P, so all four options for k appear. Especially, we have $P^\sigma = -P$ for some σ.

Torsion over $\mathbb{Q}(\zeta_8)$

- Without loss of generality, say that σ fixes $\mathbb{Q}(i)$. Then, since $x(P^\sigma) = x(P)$ and $y(P^\sigma) = -y(P)$, we can conclude that $x(P) = u + vi$, $y(P) = k\sqrt{2} + l\sqrt{-2} = \sqrt{2}(k + li)$.
- If E is given by $y^2 = x^3 + bx + c$, from the above we conclude that the elliptic curve $E_1 : 2y^2 = x^3 + bx + c$ contains point $(x(P), \frac{y(P)}{\sqrt{2}})$, which is defined over $\mathbb{Q}(i)$.
- Now, by considering a morphism $\phi : E \to E_1$, $\phi(x, y) = (x, \frac{y}{\sqrt{2}})$, we conclude that E_1 has torsion subgroup $\mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(i)$, but that is impossible by Theorem 2.

Torsion over $\mathbb{Q}(\zeta_8)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.
- **Proof:** The rank of $X_1(2,12)(\mathbb{Q}(\zeta_8))$ is 0, the torsion is $\mathbb{Z}/8\mathbb{Z}$ and all points correspond to cusps.

Torsion over $\mathbb{Q}(\zeta_8)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is not isomorphic to $\mathbb{Z}/16\mathbb{Z}$.
- **Proof:** We use the identical procedure as for $\mathbb{Z}/15\mathbb{Z}$. The analogous congruence has four solutions again, so all the remaining arguments are the same and we arrive at the elliptic curve with torsion $\mathbb{Z}/16\mathbb{Z}$ over some intermediate quadratic field. Checking all of them in the same way as before, we conclude that this group does not appear as a torsion.

Torsion over $\mathbb{Q}(\zeta_8)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.
- **Proof:** The previous method does not give us reduction to quadratic fields as before, so we have to work with Jacobian over the whole $\mathbb{Q}(\zeta_8)$. Its rank is zero and it has 80 points, so by checking them all, we conclude that none of them come from a rational elliptic curve, so the proof is complete.

Torsion over $\mathbb{Q}(\zeta_8)$

- **Theorem:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_8))_{tors}$ is isomorphic to the one of the groups from Mazur theorem or to the one of the following groups:

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \quad (15.a5),$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \quad (2112.bd4).$$

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to any of the $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$ from Theorem 1 when $n > 2$.
- **Proof:** Again by the existence of Weil pairing.

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to any of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 19, 37, 43, 67, 163.$$

- **Proof:** This directly follows from a known result by Enrique Gonzalez-Jimenez and Najman (Growth of torsion groups of elliptic curves upon base change).

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to any of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 11, 15, 17, 25.$$

- **Proof:** We use Proposition 1 to reduce this to a quadratic subfield and then we apply Theorem 2.

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to $\mathbb{Z}/27\mathbb{Z}$.
- **Proof:** We use the analogous approach as in case for $\mathbb{Q}(\zeta_8)$ and $\mathbb{Z}/15\mathbb{Z}$ to reduce this to a cubic subfield and then applying Theorem 2. This can work because $k^6 \equiv 1 \pmod{27}$ has exactly six solutions.

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
- **Proof:** Assume the contrary. Let P be a torsion point of order 10 defined over $\mathbb{Q}(\zeta_7)$ and assume it is not defined over any subfield. We use the analogous approach as in case for $\mathbb{Q}(\zeta_8)$ and $\mathbb{Z}/15\mathbb{Z}$, but it is a bit harder now because if we have a basis $\{P, Q\}$ for $E[10]$, we get by similar reasoning as in Proposition 1 that for any $\sigma \in Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})$

$$P^\sigma = \alpha P + \beta Q,$$

  where $\beta \in \{0, 5\}$.
- If $\beta = 0$, it is easy to check that $\alpha^6 \equiv 1 \pmod{10}$ has only solutions ± 1.

Torsion over $\mathbb{Q}(\zeta_7)$

- If $\beta = 5$, we have to check six cases, depending on where σ sends $5Q$ and whether α is even or odd.
- As an example, take $5Q^\sigma = 5P$ and α even. Then we get

$$P^{\sigma^2} = \alpha(\alpha P + 5Q) + 5P = (\alpha^2 + 5)P,$$

because α is even. This means $P = P^{\sigma^6} = (\alpha^2 + 5)^3 P$. We check that $(\alpha^2 + 5)^3 \equiv 1 \pmod{10}$ has solutions ± 4.

- Going through all of the cases gives us that $\alpha \in \{1, 4, -4, -1\}$ when $\beta = 5$. Together with the case when $\beta = 0$, we have six possibilities and all six must appear since all σ act differently on P.

Torsion over $\mathbb{Q}(\zeta_7)$

- Similarly as in $\mathbb{Q}(\zeta_8)$ and $\mathbb{Z}/15\mathbb{Z}$, we can conclude that the point $(x(P), \frac{y(P)}{\sqrt{-7}})$ is defined over $\mathbb{Q}(\zeta_7)^+$, but we don't know over which field $5Q$ is defined, so we can't conclude as before.
- For now, we use Magma to compute that $X_1(2,10)(\mathbb{Q}(\zeta_7)) = X_1(2,10)(\mathbb{Q})$. This is enough to conclude that this subgroup can't appear.

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to any of the following groups:

$$\mathbb{Z}/16\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

- **Proof:** Proposition 1 reduces the case $\mathbb{Z}/16\mathbb{Z}$ to a quadratic subfield, after which a routine computation in Magma like before proves that this case is impossible.
- The case $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ succesfully gets resolved in Magma the same way as before.
- The case $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ is ruled out by Harris B. Daniels and Enrique Gonzalez-Jimenez in an article which considers torsion of rational elliptic curves over sextic fields.

Torsion over $\mathbb{Q}(\zeta_7)$

- **Proposition:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to $\mathbb{Z}/21\mathbb{Z}$.
- **Proof:** Assume the contrary. Then E has a 21-isogeny. Hence, we consider $X_0(21)(\mathbb{Q}(\zeta_7))$. Computation in Magma shows that $X_0(21)(\mathbb{Q}(\zeta_7)) = X_0(21)(\mathbb{Q})$. Points on $X_0(21)(\mathbb{Q})$ give rise to curves from $162B$ and $162C$ isogeny classes, none of which have that torsion group over this field.

Torsion over $\mathbb{Q}(\zeta_7)$

- **Theorem:** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is isomorphic to the one of the groups from Mazur theorem or to the one of the following groups:

$$\mathbb{Z}/13\mathbb{Z}, \quad (147.b2)$$
$$\mathbb{Z}/14\mathbb{Z}, \quad (49.a1)$$
$$\mathbb{Z}/18\mathbb{Z}, \quad (14.a4)$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}, \quad (49.a4)$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \quad (14.a5).$$