Torsion subgroups of elliptic curves over number fields of small degree

Antonela Trbović

University of Zagreb

Representation Theory XVI
Dubrovnik, 24.6.2019.

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 za regionalni razvoj

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

E - elliptic curve
K - number field
$E(K)$ - the set of all K-rational points on E
Then

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$$

E - elliptic curve
K - number field
$E(K)$ - the set of all K-rational points on E
Then

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$$

Theorem (Mazur)

$E(\mathbb{Q})_{tors}$ can be one of the following 15 groups:

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 1, ..., 10, 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad n = 1, 2, 3, 4.$$

Possible torsion subgroups over quadratic fields

Theorem (Kamienny, Kenku, Momose)

$E(K)_{tors}$, where $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, can be one of the following 26 groups:

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 1, ..., 16, 18$$

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

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \quad n = 1, 2,$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Possible torsion subgroups over cubic fields

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

$E(K)_{tors}$, where K is a quadratic field, can be one of the following 26 groups:

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 1, ..., 16, 18, 20, 21$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad n = 1, ..., 7.$$

All these groups except $\mathbb{Z}/21\mathbb{Z}$ occur for infinitely many non isomorphic elliptic curves.

$Y_1(m,n)$ - modular curve whose every $K-$rational point corresponds to an isomorphism class of an elliptic curve together with an $m-$torsion point $P_m \in E(K)$ and an $n-$torsion point $P_n \in E(K)$ such that P_m and P_n generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$

$X_1(m,n)$ - compactification of $Y_1(m,n)$ (curve + cusps)

$X_1(n) = X_1(1,n)$

$Y_1(m,n)$ - modular curve whose every $K-$rational point corresponds to an isomorphism class of an elliptic curve together with an $m-$torsion point $P_m \in E(K)$ and an $n-$torsion point $P_n \in E(K)$ such that P_m and P_n generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$

$X_1(m,n)$ - compactification of $Y_1(m,n)$ (curve + cusps)

$X_1(n) = X_1(1,n)$

$$
\begin{aligned}
X_1(13): &\quad y^2 = f_{13}(x) = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1 \\
X_1(16): &\quad y^2 = f_{16}(x) = x(x^2+1)(x^2+2x-1) \\
X_1(18): &\quad y^2 = f_{18}(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1
\end{aligned}
$$

Definition

A point $P \in C(\bar{K})$ *is called quadratic if* $[K(P) : K] = 2$.

Definition

A point $P \in C(\bar{K})$ is called quadratic if $[K(P) : K] = 2$.

Given a model $y^2 = f(x)$ for C, there is an obvious way of producing quadratic points:

$$(x_0, \sqrt{f(x_0)}) \in C(\bar{K}), \quad x_0 \in K.$$

Points of this form will be called obvious quadratic points for the given model.

Lemma (Krumm)

Suppose that C/K has genus 2 and $C(K) \neq \emptyset$. Let J be the Jacobian variety of C.

1. *The set of non-obvious quadratic points for the model $y^2 = f(x)$ is finite if and only if $J(K)$ is finite.*

Lemma (Krumm)

Suppose that C/K has genus 2 and $C(K) \neq \emptyset$. Let J be the Jacobian variety of C.

1. *The set of non-obvious quadratic points for the model $y^2 = f(x)$ is finite if and only if $J(K)$ is finite.*
2. *Suppose that $J(K)$ is finite, and let q denote the number of non-obvious quadratic points for the given model. Then there is a relation*

$$q = 2j - 2 + w - c^2,$$

where $j = \#J(K)$, $c = \#C(K)$ and w is the number of points in $C(K)$ that are fixed by hyperelliptic involution.

Quadratic points on $X_1(18)$

Theorem (Krumm)

1. *The only non-obvious quadratic points for the model* $y^2 = f_{18}(x)$ *are the following four cusps:*

$$(\omega, \omega - 1), (\omega^2, \omega^2 - 1), (\omega, 1 - \omega), (\omega^2, 1 - \omega^2),$$

where $\omega = \dfrac{-1 + \sqrt{-3}}{2}$ *is a primitive cube root of unity. In particular, every non-cuspidal quadratic point on* $X_1(18)$ *is obvious.*

2. *If* $X_1(18)$ *has a quadratic point defined over the field* $K = \mathbb{Q}(\sqrt{d})$*, with* $d \neq -3$ *squarefree, then:*
   (a) $d > 0$. *Hence,* K *is a real quadratic field.*
   (b) $d \equiv 1 \pmod 8$. *Hence, the rational prime 2 splits in* K*.*
   (c) $d \not\equiv 2 \pmod 3$. *Hence, the prime 3 is not inert in* K*.*

Proof.

1. *We apply the Lemma to the curve* $C = X_1(18)$. *Using Magma we find that* $j = 21, w = 0, c = 6$, *and hence* $q = 4$. *Therefore,* $X_1(18)$ *has exactly four non-obvious quadratic points. Computing Mumford representation for the elements of* $J_1(18)(\mathbb{Q})$ *we obtain exactly two pairs* $(x^2 + x + 1, x - 1), (x^2 + x + 1, -x + 1)$. *These pairs clearly give rise to the four non-obvious quadratic points listed above. Note that these four points are cusps.*

2. Every quadratic point defined over K is obvious for the model $y^2 = f_{18}(x)$, so there is an $x_0 \in \mathbb{Q}$ such that $K = \mathbb{Q}(\sqrt{f_{18}(x_0)})$.
   (a) The polynomial function $x \mapsto f_{18}(x)$ only takes positive values for $x \in \mathbb{R}$, so $f_{18}(x_0) > 0$.
   (b) Letting $x_0 = n/d$ with n and d coprime integers, we have that $K = \mathbb{Q}(\sqrt{g(n,d)})$, where

$$g(n,d) = d^6 f_{18}(n/d) =$$

$$= n^6 + 2n^5 d + 5n^4 d^2 + 10n^3 d^4 + 10n^2 d^4 + 4nd^5 + d^6.$$

We claim that $g(n,d)$ is congruent to 1 (mod 8). If n and d are both odd, then

$$g(n,d) \equiv 1+2nd+5+10nd+10+4nd+1 = 17+16nd \equiv 1 \pmod 8.$$

We deal with other cases (and (c)) similarly. □

Theorem (Kenku, Momose)

Let K be a quadratic number field such that $Y_1(18)(K) \neq \emptyset$. Then 5 and 7 are unramified in K and either 2 splits or 3 does not split in K. Moreover, 3 is not inert in K.

Quadratic points on $X_1(13)$

Theorem (Momose)

Let K be a quadratic number field such that $Y_1(13)(K) \neq \emptyset$. Then the rational prime 2 splits in K and 3 is unramified in K.

Theorem (Krumm)

1. *All quadratic points on* $X_1(13)$ *are obvious for the model* $y^2 = f_{13}(x)$.
2. *If* $X_1(13)$ *has a quadratic point defined over the field* $K = \mathbb{Q}(\sqrt{d})$, *with squarefree, then:*
   (a) $d > 0$. *Hence,* K *is a real quadratic field.*
   (b) $d \equiv 1 \pmod 8$. *Hence, the rational prime 2 splits in* K.

Quadratic points on $X_1(16)$

It can be shown that all non-cuspidal quadratic points are obvious, but unlike with $X_1(13)$ and $X_1(18)$ we cannot use this description to prove results about the splitting of rational primes in quadratic extensions.
However, Krumm has noticed the following property of the ideal class groups:

Conjecture (Krumm)

Let $K \neq \mathbb{Q}(\sqrt{-15})$ be an imaginary quadratic field such that $X_1(16)$ has a quadratic point over K. Then the class number of K is divisible by 10.

Conjecture (Krumm)

Let $K \neq \mathbb{Q}(\sqrt{-15})$ be an imaginary quadratic field such that $X_1(16)$ has a quadratic point over K. Then the class number of K is divisible by 10.

Theorem (Krumm)

There are infinitely many imaginary quadratic fields K such that $X_1(16)$ has a quadratic point over K and the class number of K is divisible by 10.

Conjecture (Krumm)

Let $K \neq \mathbb{Q}(\sqrt{-15})$ be an imaginary quadratic field such that $X_1(16)$ has a quadratic point over K. Then the class number of K is divisible by 10.

Theorem (Krumm)

There are infinitely many imaginary quadratic fields K such that $X_1(16)$ has a quadratic point over K and the class number of K is divisible by 10.

Conjecture (T.)

There are infinitely many cubic number fields K such that $X_1(16)$ has a cubic point over K and the class number of K is divisible by 10.

Theorem (T.)

Let K be a cubic number field such that $Y_1(2,14)(K) \neq \emptyset$. If the rational primes 3,5,11,13 and 17 are primes of good reduction, then they remain prime in K.

Proof.

Since $(28,5) = 1$, *we have*

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \hookrightarrow E(\mathcal{O}_K/P),$$

where P is a prime lying over 5.

1. $5\mathcal{O}_K = P_1 \cdot P_2 \cdot P_3$

   $N_{K/\mathbb{Q}}(5\mathcal{O}_K) = N_{K/\mathbb{Q}}(5) = 5^3 = N_{K/\mathbb{Q}}(P_1 \cdot P_2 \cdot P_3) = N_{K/\mathbb{Q}}(P_1) \cdot N_{K/\mathbb{Q}}(P_2) \cdot N_{K/\mathbb{Q}}(P_3)$.

   Hence, $N_{K/\mathbb{Q}}(P_i) = 5, i = 1, 2, 3$, and $\mathcal{O}_K/P = \mathbb{F}_5$, so we have

   $$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \hookrightarrow E(\mathbb{F}_5).$$

   Hasse-Weil: $|\#E(\mathbb{F}_5) - (5+1)| \leq 2\sqrt{5}$, so

   $$\#E(\mathbb{F}_5) \leq 10.5 < 28.$$

2. $5\mathcal{O}_K = P_1^2 \cdot P_2$
   This cannot happen because the extension is Galois.

2. $5\mathcal{O}_K = P_1^2 \cdot P_2$
   This cannot happen because the extension is Galois.
3. $5\mathcal{O}_K = P_1^3$
   Similar as 1.

2. $5\mathcal{O}_K = P_1^2 \cdot P_2$
   This cannot happen because the extension is Galois.
3. $5\mathcal{O}_K = P_1^3$
   Similar as 1.
4. $5\mathcal{O}_K = P_1 \cdot P_2$
   This cannot happen because the extension is Galois.

2. $5\mathcal{O}_K = P_1^2 \cdot P_2$
   This cannot happen because the extension is Galois.
3. $5\mathcal{O}_K = P_1^3$
   Similar as 1.
4. $5\mathcal{O}_K = P_1 \cdot P_2$
   This cannot happen because the extension is Galois.
5. $5\mathcal{O}_K = P_1^2$
   Cannot happen because $N_{K/\mathbb{Q}}(5\mathcal{O}_K) = 5^3 = N_{K/\mathbb{Q}}(P_1)^2$.

2. $5\mathcal{O}_K = P_1^2 \cdot P_2$
   This cannot happen because the extension is Galois.
3. $5\mathcal{O}_K = P_1^3$
   Similar as 1.
4. $5\mathcal{O}_K = P_1 \cdot P_2$
   This cannot happen because the extension is Galois.
5. $5\mathcal{O}_K = P_1^2$
   Cannot happen because $N_{K/\mathbb{Q}}(5\mathcal{O}_K) = 5^3 = N_{K/\mathbb{Q}}(P_1)^2$.
6. $5\mathcal{O}_K = P_1$

Proposition (T.)

Let p be a prime satisfying $p \equiv 3 \pmod 8$, $p \equiv 2 \pmod 3$ and $\left(\frac{p}{5}\right) = -1$. Then, rank$(X_1(15)(\mathbb{Q}(\sqrt{p}))) = 0$.

Proposition (T.)

Let p be a prime satisfying $p \equiv 3 \pmod 8$ and $\left(\frac{p}{7}\right) = 1$. Then, rank$(X_1(14)(\mathbb{Q}(\sqrt{p}))) = 0$.

Denote $X = X_0(15)$. Then

$$rank(X(\mathbb{Q}(\sqrt{p}))) = rank(X(\mathbb{Q})) + rank(X^p(\mathbb{Q})).$$

Let X' be the curve that is $2-$isogenous to X, ϕ a $2-$isogeny from X to X', and ψ its dual isogeny. Then

$$rank(X(K)) \leq log_2(|S_\psi(X)| \cdot |S_\phi(X')|) - 2.$$

$$N^2 = -M^4 + 41pM^2e^2 - 400p^2e^4$$

Reducing modulo 3 and noticing that $p \equiv 2 \pmod 3$ we get

$$N^2 \equiv -M^4 + M^2e^2 - e^4 \equiv 2 \pmod 3,$$

which is not a quadratic residue modulo 3.