Elliptic curves with complex multiplication and abelian division fields

Asimina S. Hamakiotes

University of Connecticut

January 23, 2024

Goal

Let F be a number field and let E/F be an elliptic curve. Let $N \geq 2$.

Goal

Let F be a number field and let E/F be an elliptic curve. Let $N \geq 2$.

- When is the division field $F(E[N])$ abelian over F?

Goal

Let F be a number field and let E/F be an elliptic curve. Let $N \geq 2$.

- When is the division field $F(E[N])$ abelian over F?
- If $F(E[N])/F$ is not abelian, then what is the maximal abelian extension contained in $F(E[N])/F$?

Goal

Let F be a number field and let E/F be an elliptic curve. Let $N \geq 2$.

- When is the division field $F(E[N])$ abelian over F?
- If $F(E[N])/F$ is not abelian, then what is the maximal abelian extension contained in $F(E[N])/F$?

For this talk, we will focus on elliptic curves E with complex multiplication and fix F to be the minimal field of definition, i.e. $F = \mathbb{Q}(j(E))$.

What is an elliptic curve?

Definition

An *elliptic curve* E defined over a field K (char. $\neq 2, 3$) is an equation of the form

$$y^2 = x^3 + Ax + B, \quad A, B \in K,$$

where $4A^3 + 27B^2 \neq 0$ (for smoothness). More precisely, an elliptic curve defined over a field K is a smooth projective curve of genus 1, with at least one K-rational point.

What is an elliptic curve?

Definition

An *elliptic curve* E defined over a field K (char. $\neq 2, 3$) is an equation of the form

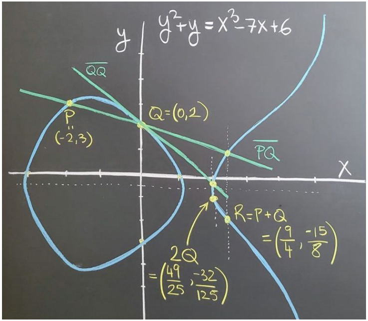
$$y^2 = x^3 + Ax + B, \quad A, B \in K,$$

where $4A^3 + 27B^2 \neq 0$ (for smoothness). More precisely, an elliptic curve defined over a field K is a smooth projective curve of genus 1, with at least one K-rational point.

There is a group law (abelian) on the L-rational points of E

$$E(L) = \{(x, y) \in E : x, y \in L\} \cup \mathcal{O},$$

with coordinates in any field $L \supset K$. We call $E(L)$ the *Mordell-Weil group* of E/L.



Mordell-Weil Theorem

Example

Let $E/\mathbb{Q} : y^2 = x^3 + 13x - 34$ (40.a4) be an elliptic curve. Then

$$E(\mathbb{Q}) = \{\mathcal{O}, (7, -20), (2, 0), (7, 20)\} = \langle (7, 20) \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Mordell-Weil Theorem

Example

Let $E/\mathbb{Q} : y^2 = x^3 + 13x - 34$ (40.a4) be an elliptic curve. Then

$$E(\mathbb{Q}) = \{\mathcal{O}, (7,-20), (2,0), (7,20)\} = \langle (7,20) \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Now consider the same curve E defined over $\mathbb{Q}(i)$. Then

$$E(\mathbb{Q}(i)) = \langle (1+2i, -2-6i), (-3, -10i) \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Mordell-Weil Theorem

Example

Let $E/\mathbb{Q} : y^2 = x^3 + 13x - 34$ (40.a4) be an elliptic curve. Then

$$E(\mathbb{Q}) = \{\mathcal{O}, (7, -20), (2, 0), (7, 20)\} = \langle (7, 20) \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Now consider the same curve E defined over $\mathbb{Q}(i)$. Then

$$E(\mathbb{Q}(i)) = \langle (1 + 2i, -2 - 6i), (-3, -10i) \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Theorem (Mordell-Weil, 1928)

Let F be a number field and let E/F be an elliptic curve. Then $E(F)$ is a finitely generated abelian group. In particular,

$$E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}},$$

where $E(F)_{tors}$ is a finite subgroup and $R_{E/F} \geq 0$.

Mordell-Weil groups

Example

(1) $E_1/\mathbb{Q} : y^2 = x^3 + 1$ (36.a4) only has six rational torsion points,

$$E_1(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

Mordell-Weil groups

Example

(1) $E_1/\mathbb{Q} : y^2 = x^3 + 1$ (36.a4) only has six rational torsion points,

$$E_1(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

(2) $E_2/\mathbb{Q} : y^2 = x^3 - 2$ (1728.o3) does not have any rational torsion points (other than $\mathcal{O}$). However, there is a point of infinite order,

$$E_2(\mathbb{Q}) = \langle (3, 5) \rangle \cong \mathbb{Z}.$$

Mordell-Weil groups

Example

(1) $E_1/\mathbb{Q} : y^2 = x^3 + 1$ (36.a4) only has six rational torsion points,

$$E_1(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

(2) $E_2/\mathbb{Q} : y^2 = x^3 - 2$ (1728.o3) does not have any rational torsion points (other than $\mathcal{O}$). However, there is a point of infinite order,

$$E_2(\mathbb{Q}) = \langle (3, 5) \rangle \cong \mathbb{Z}.$$

(3) $E_3/\mathbb{Q} : y^2 = x^3 - 1156x$ (18496.j3) has both torsion and infinite order points,

$$E_3(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2,$$

where the torsion subgroup is generated by $\langle (0, 0), (34, 0) \rangle$, and the free part is generated by $\langle (-2, 48), (-16, 120) \rangle$.

Torsion subgroups

Definition

Let F be a number field and let E/F be an elliptic curve. Let $N \in \mathbb{Z}^+$ and

$$E[N] = \{P \in E(\overline{F}) : [N]P = \mathcal{O}\},$$

be the *N-torsion subgroup* of $E(\overline{F})$.

Torsion subgroups

Definition

Let F be a number field and let E/F be an elliptic curve. Let $N \in \mathbb{Z}^+$ and

$$E[N] = \{P \in E(\overline{F}) : [N]P = \mathcal{O}\},$$

be the *N-torsion subgroup* of $E(\overline{F})$.

It is easy to show that over $\overline{F}$,

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

Torsion subgroups

Definition

Let F be a number field and let E/F be an elliptic curve. Let $N \in \mathbb{Z}^+$ and

$$E[N] = \{P \in E(\overline{F}) : [N]P = \mathcal{O}\},$$

be the *N-torsion subgroup* of $E(\overline{F})$.

It is easy to show that over $\overline{F}$,

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

In particular, there are some integers $a, b \geq 1$ such that

$$E(F)_{\text{tors}} \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/ab\mathbb{Z}.$$

Torsion subgroups

Definition

Let F be a number field and let E/F be an elliptic curve. Let $N \in \mathbb{Z}^+$ and

$$E[N] = \{P \in E(\overline{F}) : [N]P = \mathcal{O}\},$$

be the *N-torsion subgroup* of $E(\overline{F})$.

It is easy to show that over $\overline{F}$,

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

In particular, there are some integers $a, b \geq 1$ such that

$$E(F)_{\text{tors}} \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/ab\mathbb{Z}.$$

We will be interested in the N^{th}-division field of E over F,

$$F(E[N]) = F(\{x(P), y(P) : P \in E[N]\}).$$

Galois groups

Let $N \geq 2$ be an integer and let ζ_N be a primitive N^{th} root of unity.

Consider the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

Galois groups

Let $N \geq 2$ be an integer and let ζ_N be a primitive N^{th} root of unity.

Consider the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

We obtain $\mathbb{Q}(\zeta_N)$ when we adjoin the N-torsion points of $\overline{\mathbb{Q}}^{\times}$ to $\mathbb{Q}$,

$$\mathbb{Q}(\zeta_N) = \mathbb{Q}(\overline{\mathbb{Q}}^{\times}[N]).$$

Galois groups

Let $N \geq 2$ be an integer and let ζ_N be a primitive N^{th} root of unity.

Consider the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

We obtain $\mathbb{Q}(\zeta_N)$ when we adjoin the N-torsion points of $\overline{\mathbb{Q}}^\times$ to $\mathbb{Q}$,

$$\mathbb{Q}(\zeta_N) = \mathbb{Q}(\overline{\mathbb{Q}}^\times[N]).$$

We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is abelian. In fact,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

Galois groups

Let $N \geq 2$ be an integer and let ζ_N be a primitive N^{th} root of unity.

Consider the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

We obtain $\mathbb{Q}(\zeta_N)$ when we adjoin the N-torsion points of $\overline{\mathbb{Q}}^\times$ to $\mathbb{Q}$,

$$\mathbb{Q}(\zeta_N) = \mathbb{Q}(\overline{\mathbb{Q}}^\times[N]).$$

We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is abelian. In fact,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

Let E be an elliptic curve defined over $\mathbb{Q}$. Consider $\mathbb{Q}(E[N])/\mathbb{Q}$, where

$$\mathbb{Q}(E[N]) = \mathbb{Q}(\{x(P), y(P) : P \in E[N]\}).$$

Galois groups

Let $N \geq 2$ be an integer and let ζ_N be a primitive N^{th} root of unity.

Consider the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$.

We obtain $\mathbb{Q}(\zeta_N)$ when we adjoin the N-torsion points of $\overline{\mathbb{Q}}^\times$ to $\mathbb{Q}$,

$$\mathbb{Q}(\zeta_N) = \mathbb{Q}(\overline{\mathbb{Q}}^\times[N]).$$

We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is abelian. In fact,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

Let E be an elliptic curve defined over $\mathbb{Q}$. Consider $\mathbb{Q}(E[N])/\mathbb{Q}$, where

$$\mathbb{Q}(E[N]) = \mathbb{Q}(\{x(P), y(P) : P \in E[N]\}).$$

Question

What is $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$*?*

Galois groups

Let $E/\mathbb{Q}$ be an elliptic curve and $N \geq 2$.

Question

What is $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$*?*

Galois groups

Let $E/\mathbb{Q}$ be an elliptic curve and $N \geq 2$.

Question

What is $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$*?*

In general,

$$\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \subseteq \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$$

Galois groups

Let $E/\mathbb{Q}$ be an elliptic curve and $N \geq 2$.

Question

What is $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$*?*

In general,

$$\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \subseteq \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$$

In many cases,

$$\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Galois groups

Let $E/\mathbb{Q}$ be an elliptic curve and $N \geq 2$.

Question

What is $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$*?*

In general,

$$\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \subseteq \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$$

In many cases,

$$\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Question

Can $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$ *be abelian?*

What is known?

Let E be an elliptic curve defined over a number field F. Previously,

What is known?

Let E be an elliptic curve defined over a number field F. Previously,

- Halberstadt, Merel (2001), Merel and Stein (2001), and Rebolledo (2003), show that if p is prime, and $F(E[p]) = \mathbb{Q}(\zeta_p)$, then $p = 2, 3, 5$ or $p > 1000$.

What is known?

Let E be an elliptic curve defined over a number field F. Previously,

- Halberstadt, Merel (2001), Merel and Stein (2001), and Rebolledo (2003), show that if p is prime, and $F(E[p]) = \mathbb{Q}(\zeta_p)$, then $p = 2, 3, 5$ or $p > 1000$.
- When $F = \mathbb{Q}$, Paladino (2010) gives a classification as a two parameter family of all elliptic curves $E/\mathbb{Q}$ with $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$.

What is known?

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let $E/\mathbb{Q}$ *be an elliptic curve. Let* $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ *only for* $N = 2, 3, 4,$ *or* 5.
- *More generally, if* $\mathbb{Q}(E[N])/\mathbb{Q}$ *is abelian, then* $N = 2, 3, 4, 5, 6,$ *or* 8.

What is known?

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ *only for* $N = 2, 3, 4,$ *or* 5.
- *More generally, if* $\mathbb{Q}(E[N])/\mathbb{Q}$ *is abelian, then* $N = 2, 3, 4, 5, 6,$ *or* 8.

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ *only for* $N = 2$ *or* 3.
- *More generally, if* $\mathbb{Q}(E[N])/\mathbb{Q}$ *is abelian, then* $N = 2, 3,$ *or* 4.

What is known?

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ *only for* $N = 2, 3, 4,$ *or* 5.
- *More generally, if* $\mathbb{Q}(E[N])/\mathbb{Q}$ *is abelian, then* $N = 2, 3, 4, 5, 6,$ *or* 8.

Theorem (Lozano-Robledo, González-Jiménez, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. Let $N \geq 2$.

- $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ *only for* $N = 2$ *or* 3.
- *More generally, if* $\mathbb{Q}(E[N])/\mathbb{Q}$ *is abelian, then* $N = 2, 3,$ *or* 4.

Let E be an elliptic curve defined over a number field F and let $N \geq 2$. Can $F(E[N])/F$ be abelian?

Complex multiplication (CM)

Definition

Let E be an elliptic curve defined over a field F. We say that E has *complex multiplication* (CM) if $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

If E/F has CM, then $\mathrm{End}(E) \cong \mathcal{O}_{K,f}$, where $\mathcal{O}_{K,f}$ is the order in an imaginary quadratic field K with index $f \geq 1$ in $\mathcal{O}_K$, also called the conductor.

Complex multiplication (CM)

Definition

Let E be an elliptic curve defined over a field F. We say that E has *complex multiplication* (CM) if $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

If E/F has CM, then $\mathrm{End}(E) \cong \mathcal{O}_{K,f}$, where $\mathcal{O}_{K,f}$ is the order in an imaginary quadratic field K with index $f \geq 1$ in $\mathcal{O}_K$, also called the conductor.

Example

The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + x$ (64.a1) has the endomorphism

$$\phi(x, y) = (-x, iy),$$

where for $(x, y) \in E$, we have $(iy)^2 = (-x)^3 + (-x)$, so $(-x, iy) \in E$.

In this case, $\mathrm{End}(E) \cong \mathbb{Z}[i] = \mathcal{O}_{K,1}$, the maximal order of $K = \mathbb{Q}(i)$.

Notation

- K be an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers $\mathcal{O}_K$,
- $\mathcal{O}_{K,f}$ be the order of conductor $f \geq 1$ in K, with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j-invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

Notation

- K be an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers $\mathcal{O}_K$,
- $\mathcal{O}_{K,f}$ be the order of conductor $f \geq 1$ in K, with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j-invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

$E/\mathbb{Q}(j_{K,f})$ is an elliptic curve with CM by $\mathcal{O}_{K,f}$, and a minimal field of definition for E is $\mathbb{Q}(j_{K,f})$.

Notation

- K be an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers $\mathcal{O}_K$,
- $\mathcal{O}_{K,f}$ be the order of conductor $f \geq 1$ in K, with discriminant $\Delta_K f^2$,
- $j_{K,f}$ is the j-invariant associated to the order $\mathcal{O}_{K,f}$, i.e., $j(\mathbb{C}/\mathcal{O}_{K,f})$.

$E/\mathbb{Q}(j_{K,f})$ is an elliptic curve with CM by $\mathcal{O}_{K,f}$, and a minimal field of definition for E is $\mathbb{Q}(j_{K,f})$.

Example

Let $E/\mathbb{Q}(\sqrt{2})$ be the elliptic curve given by (32.1-a1),

$$y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right)x + 46\sqrt{2} - 69,$$

with CM by $\mathcal{O}_{K,4} = \mathbb{Z}[4i]$, where $K = \mathbb{Q}(i)$.
Here, $j_{K,4} = -29071392966\sqrt{2} + 41113158120$, so $\mathbb{Q}(j_{K,4}) = \mathbb{Q}(\sqrt{2})$.

When is $\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f})$ abelian?

Theorem 1 (H. and Lozano-Robledo, 2023)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$. Let $N \geq 2$ and let

$$G_{E,N} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$$

be the Galois group of the N-division field of E.

If $G_{E,N}$ is abelian, then N must equal $2, 3$, or 4. Furthermore, if $G_{E,N}$ is abelian, then it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some $0 \leq k \leq 3$.

When is $\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f})$ abelian?

Theorem 1 (H. and Lozano-Robledo, 2023)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$. Let $N \geq 2$ and let

$$G_{E,N} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$$

be the Galois group of the N-division field of E.

If $G_{E,N}$ is abelian, then N must equal $2, 3$, or 4. Furthermore, if $G_{E,N}$ is abelian, then it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some $0 \leq k \leq 3$.

Let $N = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$, where for $1 \leq i \leq r$, the p_i are primes and $e_i \geq 1$. We can study when $G_{E,N}$ is abelian, by studying when G_{E,p_i} is abelian.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*

- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and* f *is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*

- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and* f *is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} \neq 0, 1728$)

- $E_1/\mathbb{Q} : y^2 = x^3 + x^2 - 13x - 21$ (256.a1) has $j_{K,1} = 8000$,

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*

- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and f is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} \neq 0, 1728$)

- $E_1/\mathbb{Q} : y^2 = x^3 + x^2 - 13x - 21$ (256.a1) has $j_{K,1} = 8000$, where $K = \mathbb{Q}(\sqrt{-2})$, $\Delta_K = -8$, and $f = 1$, so $\Delta_K f^2 \equiv 0 \bmod 4$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*
- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and f is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} \neq 0, 1728$)

- $E_1/\mathbb{Q} : y^2 = x^3 + x^2 - 13x - 21$ (256.a1) has $j_{K,1} = 8000$, where $K = \mathbb{Q}(\sqrt{-2})$, $\Delta_K = -8$, and $f = 1$, so $\Delta_K f^2 \equiv 0 \bmod 4$. Therefore, $G_{E_1,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*

- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and f is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} \neq 0, 1728$)

- $E_1/\mathbb{Q} : y^2 = x^3 + x^2 - 13x - 21$ (256.a1) has $j_{K,1} = 8000$, where $K = \mathbb{Q}(\sqrt{-2})$, $\Delta_K = -8$, and $f = 1$, so $\Delta_K f^2 \equiv 0 \bmod 4$. Therefore, $G_{E_1,2} \cong \mathbb{Z}/2\mathbb{Z}$.
- $E_2/\mathbb{Q} : y^2 + xy = x^3 - x^2 - 107x + 552$ (49.a2) has $j_{K,1} = -3375$,

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*
- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and f is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} \neq 0, 1728$)

- $E_1/\mathbb{Q} : y^2 = x^3 + x^2 - 13x - 21$ (256.a1) has $j_{K,1} = 8000$, where $K = \mathbb{Q}(\sqrt{-2})$, $\Delta_K = -8$, and $f = 1$, so $\Delta_K f^2 \equiv 0 \bmod 4$. Therefore, $G_{E_1,2} \cong \mathbb{Z}/2\mathbb{Z}$.
- $E_2/\mathbb{Q} : y^2 + xy = x^3 - x^2 - 107x + 552$ (49.a2) has $j_{K,1} = -3375$, where $K = \mathbb{Q}(\sqrt{-7})$, $\Delta_K = -7 \equiv 1 \bmod 8$, and $f = 1$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 2$, then $G_{E,2}$ is abelian if and only if one of the following holds:

(a) $j_{K,f} \neq 0, 1728$ *and either*
- $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
- $\Delta_K \equiv 1 \bmod 8$ *and f is odd.*

In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} \neq 0, 1728$)

- $E_1/\mathbb{Q} : y^2 = x^3 + x^2 - 13x - 21$ (256.a1) has $j_{K,1} = 8000$, where $K = \mathbb{Q}(\sqrt{-2})$, $\Delta_K = -8$, and $f = 1$, so $\Delta_K f^2 \equiv 0 \bmod 4$. Therefore, $G_{E_1,2} \cong \mathbb{Z}/2\mathbb{Z}$.
- $E_2/\mathbb{Q} : y^2 + xy = x^3 - x^2 - 107x + 552$ (49.a2) has $j_{K,1} = -3375$, where $K = \mathbb{Q}(\sqrt{-7})$, $\Delta_K = -7 \equiv 1 \bmod 8$, and $f = 1$. Therefore, $G_{E_2,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Example ($j_{K,f} \neq 0, 1728$)

- Let $E_3/\mathbb{Q}(\sqrt{2})$ be given by (32.1-a1)

$$y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right)x + 46\sqrt{2} - 69.$$

Recall that E_3 has CM by $\mathcal{O}_{K,4} = \mathbb{Z}[4i]$ where $K = \mathbb{Q}(i)$ and

$$j_{K,4} = -29071392966\sqrt{2} + 41113158120.$$

We have $\Delta_K f^2 = -4 \cdot 16 = -64 \equiv 0 \bmod 4$, so $G_{E_3,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Example ($j_{K,f} \neq 0, 1728$)

- Let $E_3/\mathbb{Q}(\sqrt{2})$ be given by (32.1-a1)

$$y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right)x + 46\sqrt{2} - 69.$$

Recall that E_3 has CM by $\mathcal{O}_{K,4} = \mathbb{Z}[4i]$ where $K = \mathbb{Q}(i)$ and

$$j_{K,4} = -29071392966\sqrt{2} + 41113158120.$$

We have $\Delta_K f^2 = -4 \cdot 16 = -64 \equiv 0 \bmod 4$, so $G_{E_3,2} \cong \mathbb{Z}/2\mathbb{Z}$.

One can check that $E_3(\mathbb{Q}(\sqrt{2}))[2] \cong \mathbb{Z}/2\mathbb{Z}$ is generated by a point of order 2 defined over $\mathbb{Q}(\sqrt{2})$, namely

$$P = \left(2\sqrt{2} - \frac{3}{2},\ \frac{3}{4}\sqrt{2} - 2\right).$$

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) $j_{K,f} = 1728$, *so* $E/\mathbb{Q}$ *is given by* $y^2 = x^3 - dx$ *with* d *in* $\mathbb{Z}$. *Then*

- *If* d *is a square, then* $G_{E,2}$ *is trivial.*
- *If* d *is not a square, then* $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) *$j_{K,f} = 1728$, so $E/\mathbb{Q}$ is given by $y^2 = x^3 - dx$ with d in $\mathbb{Z}$. Then*
- *If d is a square, then $G_{E,2}$ is trivial.*
- *If d is not a square, then $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

(c) *$j_{K,f} = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ with d a cube in $\mathbb{Z}$. In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) $j_{K,f} = 1728$, *so* $E/\mathbb{Q}$ *is given by* $y^2 = x^3 - dx$ *with* d *in* $\mathbb{Z}$. *Then*

- *If* d *is a square, then* $G_{E,2}$ *is trivial.*
- *If* d *is not a square, then* $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

(c) $j_{K,f} = 0$ *and* $E/\mathbb{Q}$ *is given by* $y^2 = x^3 + d$ *with* d *a cube in* $\mathbb{Z}$. *In this case* $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} = 1728$ and $j_{K,f} = 0$)

- $E_4/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has $j_{K,1} = 1728$ and $d = 1$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) *$j_{K,f} = 1728$, so $E/\mathbb{Q}$ is given by $y^2 = x^3 - dx$ with d in $\mathbb{Z}$. Then*
- *If d is a square, then $G_{E,2}$ is trivial.*
- *If d is not a square, then $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

(c) *$j_{K,f} = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ with d a cube in $\mathbb{Z}$. In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example ($j_{K,f} = 1728$ and $j_{K,f} = 0$)

- $E_4/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has $j_{K,1} = 1728$ and $d = 1$. Therefore, $G_{E_4,2}$ is trivial.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) *$j_{K,f} = 1728$, so $E/\mathbb{Q}$ is given by $y^2 = x^3 - dx$ with d in $\mathbb{Z}$. Then*
- *If d is a square, then $G_{E,2}$ is trivial.*
- *If d is not a square, then $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

(c) *$j_{K,f} = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ with d a cube in $\mathbb{Z}$. In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example ($j_{K,f} = 1728$ and $j_{K,f} = 0$)

- $E_4/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has $j_{K,1} = 1728$ and $d = 1$. Therefore, $G_{E_4,2}$ is trivial.
- $E_5/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j_{K,1} = 1728$ and $d = 2$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) *$j_{K,f} = 1728$, so $E/\mathbb{Q}$ is given by $y^2 = x^3 - dx$ with d in $\mathbb{Z}$. Then*
- *If d is a square, then $G_{E,2}$ is trivial.*
- *If d is not a square, then $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

(c) *$j_{K,f} = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ with d a cube in $\mathbb{Z}$. In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example ($j_{K,f} = 1728$ and $j_{K,f} = 0$)

- $E_4/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has $j_{K,1} = 1728$ and $d = 1$. Therefore, $G_{E_4,2}$ is trivial.
- $E_5/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j_{K,1} = 1728$ and $d = 2$. Therefore, $G_{E_5,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) *$j_{K,f} = 1728$, so $E/\mathbb{Q}$ is given by $y^2 = x^3 - dx$ with d in $\mathbb{Z}$. Then*
- *If d is a square, then $G_{E,2}$ is trivial.*
- *If d is not a square, then $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

(c) *$j_{K,f} = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ with d a cube in $\mathbb{Z}$. In this case $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example ($j_{K,f} = 1728$ and $j_{K,f} = 0$)

- $E_4/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has $j_{K,1} = 1728$ and $d = 1$. Therefore, $G_{E_4,2}$ is trivial.
- $E_5/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j_{K,1} = 1728$ and $d = 2$. Therefore, $G_{E_5,2} \cong \mathbb{Z}/2\mathbb{Z}$.
- $E_6/\mathbb{Q} : y^2 = x^3 + 1$ (36.a4) has $j_{K,1} = 0$ and $d = 1$.

$G_{E,2} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[2])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

(b) $j_{K,f} = 1728$, *so* $E/\mathbb{Q}$ *is given by* $y^2 = x^3 - dx$ *with* d *in* $\mathbb{Z}$. *Then*

- *If* d *is a square, then* $G_{E,2}$ *is trivial.*
- *If* d *is not a square, then* $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

(c) $j_{K,f} = 0$ *and* $E/\mathbb{Q}$ *is given by* $y^2 = x^3 + d$ *with* d *a cube in* $\mathbb{Z}$. *In this case* $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example ($j_{K,f} = 1728$ and $j_{K,f} = 0$)

- $E_4/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has $j_{K,1} = 1728$ and $d = 1$. Therefore, $G_{E_4,2}$ is trivial.
- $E_5/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j_{K,1} = 1728$ and $d = 2$. Therefore, $G_{E_5,2} \cong \mathbb{Z}/2\mathbb{Z}$.
- $E_6/\mathbb{Q} : y^2 = x^3 + 1$ (36.a4) has $j_{K,1} = 0$ and $d = 1$. Therefore, $G_{E_6,2} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
  Here $4d = 8$ is a cube in $\mathbb{Z}$, but d and $-3d$ are not squares in $\mathbb{Z}$.

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
  Here $4d = 8$ is a cube in $\mathbb{Z}$, but d and $-3d$ are not squares in $\mathbb{Z}$.
  Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
  Here $4d = 8$ is a cube in $\mathbb{Z}$, but d and $-3d$ are not squares in $\mathbb{Z}$.
  Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 16$ (27.a4) has $j_{K,1} = 0$ and $d = 16$.

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
  Here $4d = 8$ is a cube in $\mathbb{Z}$, but d and $-3d$ are not squares in $\mathbb{Z}$.
  Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 16$ (27.a4) has $j_{K,1} = 0$ and $d = 16$.
  Here $4d = 4^3$ is a cube in $\mathbb{Z}$, and d is a square in $\mathbb{Z}$.

$G_{E,3} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[3])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 3$, then $G_{E,3}$ is abelian if and only if $j(E) = 0$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + d$ such that $4d$ is a cube in $\mathbb{Z}$.

- *If d and $-3d$ are not squares, then $G_{E,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*
- *If d or $-3d$ is a square, then $G_{E,3} \cong \mathbb{Z}/2\mathbb{Z}$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 + 2$ (1728.n4) has $j_{K,1} = 0$ and $d = 2$.
  Here $4d = 8$ is a cube in $\mathbb{Z}$, but d and $-3d$ are not squares in $\mathbb{Z}$.
  Therefore, $G_{E_1,3} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 16$ (27.a4) has $j_{K,1} = 0$ and $d = 16$.
  Here $4d = 4^3$ is a cube in $\mathbb{Z}$, and d is a square in $\mathbb{Z}$.
  Therefore, $G_{E_2,3} \cong \mathbb{Z}/2\mathbb{Z}$.

$G_{E,4} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[4])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 4$, then $G_{E,4}$ is abelian if and only if $j(E) = 1728$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + dx$ with

- *$d \in \{\pm 1, \pm 4\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$, or*
- *$d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

$G_{E,4} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[4])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 4$, then $G_{E,4}$ is abelian if and only if $j(E) = 1728$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + dx$ with

- *$d \in \{\pm 1, \pm 4\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$, or*
- *$d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 - 4x$ (64.a3) has $j(E_1) = 1728$ and $d = -4$.

$G_{E,4} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[4])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 4$, then $G_{E,4}$ is abelian if and only if $j(E) = 1728$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + dx$ with

- *$d \in \{\pm 1, \pm 4\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$, or*
- *$d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 - 4x$ (64.a3) has $j(E_1) = 1728$ and $d = -4$.

  Therefore, $G_{E_1,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

$G_{E,4} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[4])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 4$, then $G_{E,4}$ is abelian if and only if $j(E) = 1728$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + dx$ with

- *$d \in \{\pm 1, \pm 4\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$, or*
- *$d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 - 4x$ (64.a3) has $j(E_1) = 1728$ and $d = -4$. Therefore, $G_{E_1,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 9x$ (576.c4) has $j(E_2) = 1728$ and $d = 3^2$.

$G_{E,4} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[4])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 4$, then $G_{E,4}$ is abelian if and only if $j(E) = 1728$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + dx$ with

- *$d \in \{\pm 1, \pm 4\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$, or*
- *$d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 - 4x$ (64.a3) has $j(E_1) = 1728$ and $d = -4$. Therefore, $G_{E_1,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 9x$ (576.c4) has $j(E_2) = 1728$ and $d = 3^2$. 3 is a square-free integer that is not in $\{\pm 1, \pm 2\}$.

$G_{E,4} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[4])/\mathbb{Q}(j_{K,f}))$

Theorem 1 (H. and Lozano-Robledo, 2023)

If $N = 4$, then $G_{E,4}$ is abelian if and only if $j(E) = 1728$ and $E/\mathbb{Q}$ is given by $y^2 = x^3 + dx$ with

- *$d \in \{\pm 1, \pm 4\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$, or*
- *$d = \pm t^2$ for some square-free integer $t \notin \{\pm 1, \pm 2\}$, in which case $G_{E,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

Example

- $E_1/\mathbb{Q} : y^2 = x^3 - 4x$ (64.a3) has $j(E_1) = 1728$ and $d = -4$.
  Therefore, $G_{E_1,4} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E_2/\mathbb{Q} : y^2 = x^3 + 9x$ (576.c4) has $j(E_2) = 1728$ and $d = 3^2$.
  3 is a square-free integer that is not in $\{\pm 1, \pm 2\}$.
  Therefore, $G_{E_2,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Definition

Let $\rho_{E,N}$ be the *mod N Galois representation attached to E*:

$$\rho_{E,N} \colon \operatorname{Gal}(F(E[N])/F) \to \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

So we have $G_{E,N} = \operatorname{Gal}(F(E[N])/F) = \operatorname{im}(\rho_{E,N}) \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Definition

Let $\rho_{E,N}$ be the *mod N Galois representation attached to E*:

$$\rho_{E,N}\colon \operatorname{Gal}(F(E[N])/F) \to \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

So we have $G_{E,N} = \operatorname{Gal}(F(E[N])/F) = \operatorname{im}(\rho_{E,N}) \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

For an elliptic curve with CM, we know that $G_{E,N} \subseteq \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is actually contained in something smaller, which is almost abelian.

How do we study this?

Let E be an elliptic curve defined over a number field F and let $N \geq 2$.

Definition

Let $\rho_{E,N}$ be the *mod N Galois representation attached to E*:

$$\rho_{E,N}\colon \mathrm{Gal}(F(E[N])/F) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

So we have $G_{E,N} = \mathrm{Gal}(F(E[N])/F) = \mathrm{im}(\rho_{E,N}) \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

For an elliptic curve with CM, we know that $G_{E,N} \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is actually contained in something smaller, which is almost abelian.

$G_{E,N}$ is contained in the normalizer of Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$. We define the *Cartan subgroup* $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z},\ \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$. We define the *Cartan subgroup* $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z},\ \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

where δ and ϕ are defined as follows:

- If $\Delta_K f^2 \equiv 0 \bmod 4$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$. We define the *Cartan subgroup* $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z},\ \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

where δ and ϕ are defined as follows:

- If $\Delta_K f^2 \equiv 0 \bmod 4$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.
- If $\Delta_K f^2 \equiv 1 \bmod 4$, and N is even, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.

How do we study this?

Definition

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and let $N \geq 3$. We define the *Cartan subgroup* $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix} : a,b \in \mathbb{Z}/N\mathbb{Z},\ \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

where δ and ϕ are defined as follows:

- If $\Delta_K f^2 \equiv 0 \bmod 4$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.
- If $\Delta_K f^2 \equiv 1 \bmod 4$, and N is even, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.

The *normalizer of Cartan subroup* $\mathcal{N}_{\delta,\phi}(N)$ of $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ is

$$\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle.$$

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N}\colon \mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N}\colon \operatorname{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

1. *There is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ such that $\operatorname{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$, and*

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ *be an elliptic curve with CM by* $\mathcal{O}_{K,f}$*, let* $N \geq 3$*, and let* $\rho_{E,N}$ *be the Galois representation*

$$\rho_{E,N}\colon \operatorname{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

1. *There is a* $\mathbb{Z}/N\mathbb{Z}$*-basis of* $E[N]$ *such that* $\operatorname{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$*, and*
2. $\mathcal{C}_{\delta,\phi}(N) \cong (\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^{\times}$ *is a subgroup of index 2 in* $\mathcal{N}_{\delta,\phi}(N)$*, and*

How do we study this?

Theorem (Lozano-Robledo, 2021)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the Galois representation

$$\rho_{E,N} \colon \operatorname{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \operatorname{Aut}(E[N]) \cong \operatorname{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Then

1. *There is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ such that $\operatorname{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$, and*
2. *$\mathcal{C}_{\delta,\phi}(N) \cong (\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^\times$ is a subgroup of index 2 in $\mathcal{N}_{\delta,\phi}(N)$, and*
3. *The index of $\operatorname{im}(\rho_{E,N}) \subseteq \mathcal{N}_{\delta,\phi}(N)$ is a divisor of $2, 4$, or 6.*

Sketch of proof of Theorem 1

Theorem 1 (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$. Then $F(E[N])/F$ is abelian only for $N = 2$, 3, or 4.

Sketch of proof:

Sketch of proof of Theorem 1

Theorem 1 (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$. Then $F(E[N])/F$ is abelian only for $N = 2$, 3, or 4.

Sketch of proof:

(1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the subgroups of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ that can occur as images of ρ_{E,p^n}, up to conjugation.

Sketch of proof of Theorem 1

Theorem 1 (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$. Then $F(E[N])/F$ is abelian only for $N = 2$, 3, or 4.

Sketch of proof:

(1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the subgroups of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ that can occur as images of ρ_{E,p^n}, up to conjugation.

(2) We know what subgroups of $\mathcal{N}_{\delta,\phi}(N)$ are images of $\rho_{E,N}$ and we give conditions that will help characterize when a subgroup of $\mathcal{N}_{\delta,\phi}(N)$ is abelian (e.g. the Cartan subgroup is abelian).

Sketch of proof of Theorem 1

Theorem 1 (H. and Lozano-Robledo, 2023)

Let E/F be an elliptic curve with CM and $F = \mathbb{Q}(j(E))$. Then $F(E[N])/F$ is abelian only for $N = 2$, 3, or 4.

Sketch of proof:

(1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the subgroups of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ that can occur as images of ρ_{E,p^n}, up to conjugation.

(2) We know what subgroups of $\mathcal{N}_{\delta,\phi}(N)$ are images of $\rho_{E,N}$ and we give conditions that will help characterize when a subgroup of $\mathcal{N}_{\delta,\phi}(N)$ is abelian (e.g. the Cartan subgroup is abelian).

(3) We apply the results from (2) to all possible $G_{E,p} = \operatorname{im} \rho_{E,p}$ from (1) where $p \mid N$ and analyze under what circumstances $G_{E,N}$ is abelian.

$\square$

Conditions for determining if $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \; c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \text{ and } \; c_{\delta,\phi}(a,b) = \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix}.$$

Conditions for determining if $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \ c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \text{ and } \ c_{\delta,\phi}(a,b) = \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix}.$$

Lemma (H. and Lozano-Robledo, 2023)

Let $N \geq 2$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1, c_{\delta,\phi}(a,b) \in G$, for some $a, b \in \mathbb{Z}/N\mathbb{Z}$, such that the two matrices commute, then

$$b\phi \equiv 0 \bmod N \quad \textit{and} \quad 2b \equiv 0 \bmod N.$$

Moreover, if $\phi = 0$, and if $c_\varepsilon, c_{\delta,0}(a,b) \in G$ for some $\varepsilon \in \{\pm 1\}$, such that the two matrices commute, then the same conclusion holds.

Conditions for determining in $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \ c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \text{ and } \ c_{\delta,\phi}(a,b) = \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix}.$$

Conditions for determining in $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \ c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \text{ and } \ c_{\delta,\phi}(a,b) = \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix}.$$

Corollary (H. and Lozano-Robledo, 2023)

Let $N > 2$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a,b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

Conditions for determining in $G_{E,N}$ is abelian

Let $\varepsilon \in \{\pm 1\}$ and let

$$c_1 = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix},\ c_\varepsilon = \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix},\ \text{and}\ \ c_{\delta,\phi}(a,b) = \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix}.$$

Corollary (H. and Lozano-Robledo, 2023)

Let $N > 2$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a,b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

<u>**Proof:**</u> Assume that $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ is abelian. Then c_1 (or c_ε if $\phi = 0$) and $c_{\delta,\phi}(a,b)$ commute, so by the previous Lemma, we have that

$$b\phi \equiv 0 \bmod N \quad \text{and} \quad 2b \equiv 0 \bmod N.$$

If $N > 2$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $2b \equiv 0 \bmod N \implies 2 \equiv 0 \bmod N$. Therefore, G cannot be abelian.

$\square$

Example of proving that $G_{E,N}$ is not abelian

Corollary (H. and Lozano-Robledo, 2023)

Let $N > 2$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a, b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

Example of proving that $G_{E,N}$ is not abelian

Corollary (H. and Lozano-Robledo, 2023)

Let $N > 2$ and let $G \subseteq \mathcal{N}_{\delta,\phi}(N)$ be a subgroup. If $c_1 \in G$ (or $\phi = 0$ and $c_\varepsilon \in G$) and $c_{\delta,\phi}(a,b) \in G$ with $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, then G is non-abelian.

Example

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$. Let p be an odd prime dividing $f\Delta_K$, and $j_{K,f} \neq 0, 1728$. For $\varepsilon \in \{\pm 1\}$, consider the image

$$G_{E,p} = \left\langle \begin{pmatrix} -\varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \left\{ \begin{pmatrix} a & b \\ \delta b & a \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2},\ b \in \mathbb{Z}/p\mathbb{Z} \right\} \right\rangle.$$

Observe that $c_{\delta,0}(1,1) = \begin{pmatrix} 1 & 1 \\ \delta & 1 \end{pmatrix} \in G_{E,p}$ and $b = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Therefore, $G_{E,p}$ is not abelian, and hence, G_{E,p^n} is not abelian.

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ is mostly not abelian.

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ is mostly not abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ is mostly not abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

- $\mathbb{Q}(E[5])/\mathbb{Q}$ is not abelian, $G_{E,5} \cong (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$G_{E,5} = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}).$$

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.
We have seen that $F(E[N])/F$ is mostly not abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

- $\mathbb{Q}(E[5])/\mathbb{Q}$ is not abelian, $G_{E,5} \cong (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$G_{E,5} = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}).$$

- $\mathbb{Q}(E[4])/\mathbb{Q}$ is not abelian, $G_{E,4} \cong D_4$:

$$G_{E,4} = \left\langle \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}).$$

What if $F(E[N])/F$ is not abelian?

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$ and $F = \mathbb{Q}(j_{K,f})$.

We have seen that $F(E[N])/F$ is mostly not abelian.

Example

$E/\mathbb{Q} : y^2 = x^3 - 2x$ (256.b1) has $j(E) = 1728$. Observe that

- $\mathbb{Q}(E[5])/\mathbb{Q}$ is not abelian, $G_{E,5} \cong (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$G_{E,5} = \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}).$$

- $\mathbb{Q}(E[4])/\mathbb{Q}$ is not abelian, $G_{E,4} \cong D_4$:

$$G_{E,4} = \left\langle \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}).$$

Question

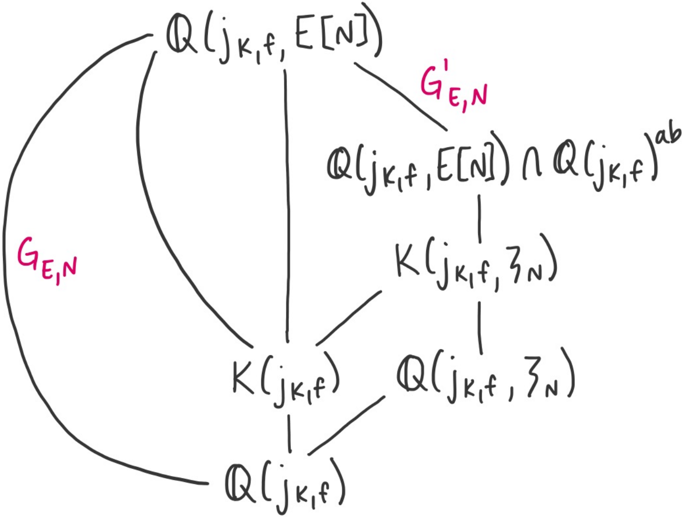
What is the maximal abelian extension contained in $F(E[N])/F$?

Field diagram

Let $N \geq 3$. Let $G_{E,N} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$.
Let $G'_{E,N}$ denote the commutator subgroup of $G_{E,N}$.

Field diagram

Let $N \geq 3$. Let $G_{E,N} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$.
Let $G'_{E,N}$ denote the commutator subgroup of $G_{E,N}$.



How to find the maximal abelian subextension

Sketch of proof:

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

(2) We know $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension and we can use that to find an upper bound, U, for the size of G'_{E,p^n}.

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

(2) We know $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension and we can use that to find an upper bound, U, for the size of G'_{E,p^n}.

- If E has CM by an order in K, then $K \subseteq \mathbb{Q}(E[p^n])$.

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

(2) We know $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension and we can use that to find an upper bound, U, for the size of G'_{E,p^n}.

- If E has CM by an order in K, then $K \subseteq \mathbb{Q}(E[p^n])$.
- By the existence of the Weil-pairing, $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[p^n])$.

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

(2) We know $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension and we can use that to find an upper bound, U, for the size of G'_{E,p^n}.

- If E has CM by an order in K, then $K \subseteq \mathbb{Q}(E[p^n])$.
- By the existence of the Weil-pairing, $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[p^n])$.
- If E is a quadratic twist by α, then $\mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(E[p^n])$.

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

(2) We know $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension and we can use that to find an upper bound, U, for the size of G'_{E,p^n}.

- If E has CM by an order in K, then $K \subseteq \mathbb{Q}(E[p^n])$.
- By the existence of the Weil-pairing, $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[p^n])$.
- If E is a quadratic twist by α, then $\mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(E[p^n])$.

(3) We can use the surjective reduction map $\pi : G'_{E,p^{n+1}} \to G'_{E,p^n}$ to get a lower bound, L, for the size of G'_{E,p^n}.

How to find the maximal abelian subextension

Sketch of proof:

(1) We have explicit matrix groups for G_{E,p^n}, so we can compute explicit commutator subgroups G'_{E,p^n}.

(2) We know $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is an abelian extension and we can use that to find an upper bound, U, for the size of G'_{E,p^n}.

- If E has CM by an order in K, then $K \subseteq \mathbb{Q}(E[p^n])$.
- By the existence of the Weil-pairing, $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[p^n])$.
- If E is a quadratic twist by α, then $\mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(E[p^n])$.

(3) We can use the surjective reduction map $\pi : G'_{E,p^{n+1}} \to G'_{E,p^n}$ to get a lower bound, L, for the size of G'_{E,p^n}.

(4) It turns out that $U = L$, so it must be that $K(\zeta_{p^n})$ or $K(\zeta_{p^n}, \sqrt{\alpha})$ is the maximal abelian subextension of $\mathbb{Q}(j_{K,f}, E[p^n])/\mathbb{Q}(j_{K,f})$.

$\square$

Results for $p = 3$

Theorem 2 (H., 2023)

Let $E/\mathbb{Q}$ be an elliptic curve with CM and $j(E) = 0$. Then for $n \geq 2$,

$[\mathcal{N}_{\delta,0}(3^n) : G_{E,3^n}]$	$\lvert G'_{E,3^n}\rvert$	$\mathbb{Q}(E[3^n]) \cap \mathbb{Q}^{ab}$
1	3^n	$\mathbb{Q}(\zeta_{3^n}, \sqrt{\alpha})$
2	3^n	$\mathbb{Q}(\zeta_{3^n})$
3	3^{n-1}	$\mathbb{Q}(\zeta_{3^n}, \sqrt{\alpha})$
6	3^{n-1}	$\mathbb{Q}(\zeta_{3^n})$

where α is a square-free integer, $\alpha \neq -3$, and $\lvert\mathcal{N}_{\delta,0}(3^n)\rvert = 3^{2n-1} \cdot 2^2$.
Note, $K = \mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\zeta_{3^n})$.

Results for $p = 3$

Theorem 2 (H., 2023)

Let $E/\mathbb{Q}$ be an elliptic curve with CM and $j(E) = 0$. Then for $n \geq 2$,

$[\mathcal{N}_{\delta,0}(3^n) : G_{E,3^n}]$	$\lvert G'_{E,3^n} \rvert$	$\mathbb{Q}(E[3^n]) \cap \mathbb{Q}^{ab}$
1	3^n	$\mathbb{Q}(\zeta_{3^n}, \sqrt{\alpha})$
2	3^n	$\mathbb{Q}(\zeta_{3^n})$
3	3^{n-1}	$\mathbb{Q}(\zeta_{3^n}, \sqrt{\alpha})$
6	3^{n-1}	$\mathbb{Q}(\zeta_{3^n})$

where α is a square-free integer, $\alpha \neq -3$, and $|\mathcal{N}_{\delta,0}(3^n)| = 3^{2n-1} \cdot 2^2$. Note, $K = \mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\zeta_{3^n})$.

The Galois groups of the maximal abelian extensions are,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{3^n})/\mathbb{Q}) \cong (\mathbb{Z}/3^n\mathbb{Z})^\times,$$
$$\mathrm{Gal}(\mathbb{Q}(\zeta_{3^n}, \sqrt{\alpha})/\mathbb{Q}) \cong (\mathbb{Z}/3^n\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z}.$$

Results for $p = 2$

Theorem 2 (H., 2023)

Let $E/\mathbb{Q}$ be an elliptic curve with CM and $j(E) = 1728$. Then for $n \geq 3$,

$[\mathcal{N}_{-1,0}(2^n) : G_{E,2^n}]$	$\lvert G'_{E,2^n} \rvert$	$\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab}$
1	2^{n-1}	$\mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha})$
2	2^{n-2}	$\mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha})$
4	2^{n-2}	$\mathbb{Q}(\zeta_{2^{n+1}})$

where α is a square-free integer, $\alpha \neq -1$, and $\lvert \mathcal{N}_{-1,0}(2^n) \rvert = 2^{2n}$.
Note, $K = \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_{2^{n+1}})$.

Results for $p = 2$

Theorem 2 (H., 2023)

Let $E/\mathbb{Q}$ be an elliptic curve with CM and $j(E) = 1728$. Then for $n \geq 3$,

$[\mathcal{N}_{-1,0}(2^n) : G_{E,2^n}]$	$\lvert G'_{E,2^n}\rvert$	$\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab}$
1	2^{n-1}	$\mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha})$
2	2^{n-2}	$\mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha})$
4	2^{n-2}	$\mathbb{Q}(\zeta_{2^{n+1}})$

where α is a square-free integer, $\alpha \neq -1$, and $\lvert\mathcal{N}_{-1,0}(2^n)\rvert = 2^{2n}$.
Note, $K = \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_{2^{n+1}})$.

The Galois groups of the maximal abelian extensions are,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+1}})/\mathbb{Q}) \cong (\mathbb{Z}/2^{n+1}\mathbb{Z})^{\times},$$
$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha})/\mathbb{Q}) \cong (\mathbb{Z}/2^{n+1}\mathbb{Z})^{\times} \times \mathbb{Z}/2\mathbb{Z}.$$

Results for $p = 2$

Theorem 2 (H., 2023)

Let $E/\mathbb{Q}$ be an elliptic curve with CM and $j(E) = 0$. Then for $n \geq 3$,

$[\mathcal{N}_{-1,1}(2^n) : G_{E,2^n}]$	$\lvert G'_{E,2^n} \rvert$	$\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab}$
1	$2^{n-1} \cdot 3$	$K(\zeta_{2^n})$
3	2^{n-1}	$K(\zeta_{2^n})$

where $K = \mathbb{Q}(\sqrt{-3})$, and $\lvert \mathcal{N}_{-1,1}(2^n) \rvert = 2^{2n-1} \cdot 3$.

Results for $p = 2$

Theorem 2 (H., 2023)

Let $E/\mathbb{Q}$ be an elliptic curve with CM and $j(E) = 0$. Then for $n \geq 3$,

$[\mathcal{N}_{-1,1}(2^n) : G_{E,2^n}]$	$\lvert G'_{E,2^n}\rvert$	$\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab}$
1	$2^{n-1} \cdot 3$	$K(\zeta_{2^n})$
3	2^{n-1}	$K(\zeta_{2^n})$

where $K = \mathbb{Q}(\sqrt{-3})$, and $\lvert\mathcal{N}_{-1,1}(2^n)\rvert = 2^{2n-1} \cdot 3$.

The Galois group of the maximal abelian extension is,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n}, \sqrt{-3})/\mathbb{Q}) \cong (\mathbb{Z}/2^n\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z}.$$

Results for $p > 3$ prime

Theorem (Daniels, Lozano-Robledo, 2021)

Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime. If $\rho_{E,p} \subseteq \mathcal{N}_{\delta,\phi}(p)$, then

$$K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab} \subseteq \mathbb{Q}(\zeta_p, \sqrt{d}),$$

for some $d \in \mathbb{Z}$. Thus, $\mathrm{Gal}(K_E(p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ or $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.

Results for $p > 3$ prime

Theorem (Daniels, Lozano-Robledo, 2021)

Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime. If $\rho_{E,p} \subseteq \mathcal{N}_{\delta,\phi}(p)$, then

$$K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab} \subseteq \mathbb{Q}(\zeta_p, \sqrt{d}),$$

for some $d \in \mathbb{Z}$. Thus, $\mathrm{Gal}(K_E(p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ or $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.

Conjecture (H., 2023)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$ for $f \geq 1$. Let $p > 3$ be a prime and let $n \in \mathbb{Z}^+$. Then

$$\mathbb{Q}(j_{K,f}, E[p^n]) \cap \mathbb{Q}(j_{K,f})^{ab} = \begin{cases} K(\zeta_{p^n}), \\ K(\zeta_{p^n}, \sqrt{\alpha}), \end{cases}$$

where $\alpha \in \mathbb{Q}(j_{K,f})$ is square-free such that $\alpha \neq 0, 1$ and $\sqrt{\alpha} \notin K$.

Questions?