Abelian extensions arising from elliptic curves with complex multiplication

Asimina S. Hamakiotes

University of Connecticut

AMS Spring Eastern Sectional Meeting
April 5 - 6, 2025

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. $F = \mathbb{Q}(j(E))$.

Notation

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

Notation

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

- Let $\overline{F}$ be a fixed algebraic closure of F.

Notation

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

- Let $\overline{F}$ be a fixed algebraic closure of F.
- Let $N \geq 2$ be an integer and let

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

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

Notation

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

- Let $\overline{F}$ be a fixed algebraic closure of F.
- Let $N \geq 2$ be an integer and let

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

  be the **N-torsion subgroup of $E(\overline{F})$**.
- One can show that over $\overline{F}$, we have that $E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

Notation

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

- Let $\overline{F}$ be a fixed algebraic closure of F.
- Let $N \geq 2$ be an integer and let

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

  be the **N-torsion subgroup of $E(\overline{F})$**.
- One can show that over $\overline{F}$, we have that $E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.
- We will be interested in the **N^{th}-division field of E/F**,

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

  i.e., the field of definition of the coordinates of points 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 $N \geq 2$.

Definition

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

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

so we have $G_{E,N} := \operatorname{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \cong \operatorname{im}(\rho_{E,N})$.

Galois groups

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

Definition

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

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

so we have $G_{E,N} := \operatorname{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \cong \operatorname{im}(\rho_{E,N})$.

In general,

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

but in many cases,

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

Galois groups

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

Definition

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

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

so we have $G_{E,N} := \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \cong \mathrm{im}(\rho_{E,N})$.

In general,

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

but 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, i.e., can* $\mathrm{im}(\rho_{E,N})$ *be abelian?*

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?

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

- K be an imaginary quadratic field,

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

- K be an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers $\mathcal{O}_K$,

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

- K be an imaginary quadratic field,
- Δ_K is the discriminant of the ring of integers $\mathcal{O}_K$,
- $\mathcal{O}_{K,f}$ be an order in K of conductor $f \geq 1$, with discriminant $\Delta_K f^2$,

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

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

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

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

Abelian division fields

Let E/F be an elliptic curve with CM by $\mathcal{O}_{K,f}$, where

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

Theorem (H. and Lozano-Robledo, 2023)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, $f \geq 1$. 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. Further, if $G_{E,N}$ is abelian, then it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some $0 \leq k \leq 3$.

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

(1) *If $j_{K,f} \neq 0, 1728$, then $G_{E,N}$ is abelian if and only if:*

- $\underline{N = 2}$ *and either*
  - $\Delta_K f^2 \equiv 0 \bmod 4$, *or*
  - $\Delta_K \equiv 1 \bmod 8$ *and* $f \equiv 1 \bmod 2$.

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

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

(1) *If* $j_{K,f} \neq 0, 1728$*, then* $G_{E,N}$ *is abelian if and only if:*

- $\underline{N = 2}$ *and either*
  - $\Delta_K f^2 \equiv 0 \bmod 4$*, or*
  - $\Delta_K \equiv 1 \bmod 8$ *and* $f \equiv 1 \bmod 2$*.*

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

(2) *If* $j_{K,f} = 1728$*, then* $G_{E,N}$ *is abelian if and only if:*

- $\underline{N = 2}$*. In this case,* $G_{E,2} \cong \{0\}$ *or* $/2$ *according to whether* E *is given by* $y^2 = x^3 - dx$ *with* d *a square or a non-square in , respectively.*
- $\underline{N = 4}$ *and* $E/$ *is given by* $y^2 = x^3 + dx$ *with* $d \in \{\pm 1, \pm 4\}$ *or* $d = \pm t^2$ *for some square-free integer* $t \notin \{\pm 1, \pm 2\}$*, in which case* $G_{E,4} \cong (/2)^2$ *or* $(/2)^3$*, resp.*

Abelian division fields

Theorem (H. and Lozano-Robledo, 2023)

(1) *If* $j_{K,f} \neq 0, 1728$*, then* $G_{E,N}$ *is abelian if and only if:*

- $\underline{N = 2}$ *and either*
  - $\Delta_K f^2 \equiv 0 \bmod 4$*, or*
  - $\Delta_K \equiv 1 \bmod 8$ *and* $f \equiv 1 \bmod 2$*.*

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

(2) *If* $j_{K,f} = 1728$*, then* $G_{E,N}$ *is abelian if and only if:*

- $\underline{N = 2}$*. In this case,* $G_{E,2} \cong \{0\}$ *or* $/2$ *according to whether* E *is given by* $y^2 = x^3 - dx$ *with* d *a square or a non-square in , respectively.*
- $\underline{N = 4}$ *and* $E/$ *is given by* $y^2 = x^3 + dx$ *with* $d \in \{\pm 1, \pm 4\}$ *or* $d = \pm t^2$ *for some square-free integer* $t \notin \{\pm 1, \pm 2\}$*, in which case* $G_{E,4} \cong (/2)^2$ *or* $(/2)^3$*, resp.*

(3) *If* $j_{K,f} = 0$*, then* $G_{E,N}$ *is abelian if and only if:*

- $\underline{N = 2}$ *and* $E/$ *is given by* $y^2 = x^3 + d$ *with* d *a cube in . Then* $G_{E,2} \cong /2$*.*
- $\underline{N = 3}$ *and* $E/$ *is given by* $y^2 = x^3 + d$ *such that* $4d$ *is a cube in . If in addition* d *and* $3d$ *are not squares, then* $G_{E,3} \cong (/2)^2$*, and if* d *or* $3d$ *is a square, then* $G_{E,3} \cong /2$*.*

Example

Theorem (1a): If $N = 2$, then $G_{E,2}$ is abelian if and only if $j_{K,f} \neq 0, 1728$ and $\Delta_K f^2 \equiv 0 \bmod 4$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example

Theorem (1a): If $N = 2$, then $G_{E,2}$ is abelian if and only if $j_{K,f} \neq 0, 1728$ and $\Delta_K f^2 \equiv 0 \bmod 4$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right)x + 46\sqrt{2} - 69$$

Example

Theorem (1a): If $N = 2$, then $G_{E,2}$ is abelian if and only if $j_{K,f} \neq 0, 1728$ and $\Delta_K f^2 \equiv 0 \bmod 4$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right) x + 46\sqrt{2} - 69$$

Note that $j(E) = -29071392966\sqrt{2} + 41113158120$.

Example

Theorem (1a): If $N = 2$, then $G_{E,2}$ is abelian if and only if $j_{K,f} \neq 0, 1728$ and $\Delta_K f^2 \equiv 0 \bmod 4$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right) x + 46\sqrt{2} - 69$$

Note that $j(E) = -29071392966\sqrt{2} + 41113158120$.

This curve has CM by $\mathbb{Z}[\sqrt{-16}]$ which is the suborder of conductor $f = 4$ of $\mathcal{O}_K = \mathbb{Z}[i]$.

Example

Theorem (1a): If $N = 2$, then $G_{E,2}$ is abelian if and only if $j_{K,f} \neq 0, 1728$ and $\Delta_K f^2 \equiv 0 \bmod 4$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right) x + 46\sqrt{2} - 69$$

Note that $j(E) = -29071392966\sqrt{2} + 41113158120$.

This curve has CM by $\mathbb{Z}[\sqrt{-16}]$ which is the suborder of conductor $f = 4$ of $\mathcal{O}_K = \mathbb{Z}[i]$.

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

Example

Theorem (1a): If $N = 2$, then $G_{E,2}$ is abelian if and only if $j_{K,f} \neq 0, 1728$ and $\Delta_K f^2 \equiv 0 \bmod 4$. In this case, $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$.

Example (32.1-a1)

$$E/\mathbb{Q}(\sqrt{2}) : y^2 + \sqrt{2}xy = x^3 + x^2 + \left(15\sqrt{2} - 22\right) x + 46\sqrt{2} - 69$$

Note that $j(E) = -29071392966\sqrt{2} + 41113158120$.

This curve has CM by $\mathbb{Z}[\sqrt{-16}]$ which is the suborder of conductor $f = 4$ of $\mathcal{O}_K = \mathbb{Z}[i]$.

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

One can check that $E(\mathbb{Q}(\sqrt{2}))[2] \cong \mathbb{Z}/2\mathbb{Z}$ is generated by a non-trivial point of two torsion defined over $\mathbb{Q}(\sqrt{2})$, namely

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

Sketch of proof

Theorem (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 only abelian for $N = 2$, 3, or 4.

<u>**Sketch of proof:**</u>

Sketch of proof

Theorem (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 only abelian 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 groups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞}, up to conjugation.

Sketch of proof

Theorem (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 only abelian 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 groups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞}, up to conjugation.

(2) We understand 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

Theorem (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 only abelian 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 groups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞}, up to conjugation.

(2) We understand 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 above to all possible images $G_{E,N} = \operatorname{im} \rho_{E,N}$ from (1) and analyze under what circumstances we have that $G_{E,N}$ is abelian.

□

Abelian extensions contained in $F(E[N])/F$

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

Abelian extensions contained in $F(E[N])/F$

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

(1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.

Abelian extensions contained in $F(E[N])/F$

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

(1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.

(2) Let $N \geq 3$. Then, $K \subseteq F(E[N])$.

Abelian extensions contained in $F(E[N])/F$

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

(1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.

(2) Let $N \geq 3$. Then, $K \subseteq F(E[N])$.

(3) Let $N \geq 3$, $d \in F$ such that $\sqrt{d} \notin K$, and E^d be the twist of E by d. Then there is an explicitly computable integer $\alpha = \alpha(E^d)$, unique up to some power, such that $F(\sqrt{\alpha}) \subseteq F(E[N])$.

Abelian extensions contained in $F(E[N])/F$

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

(1) Let $N \geq 2$. By the existence of the Weil-pairing, $F(\zeta_N) \subseteq F(E[N])$.

(2) Let $N \geq 3$. Then, $K \subseteq F(E[N])$.

(3) Let $N \geq 3$, $d \in F$ such that $\sqrt{d} \notin K$, and E^d be the twist of E by d. Then there is an explicitly computable integer $\alpha = \alpha(E^d)$, unique up to some power, such that $F(\sqrt{\alpha}) \subseteq F(E[N])$.

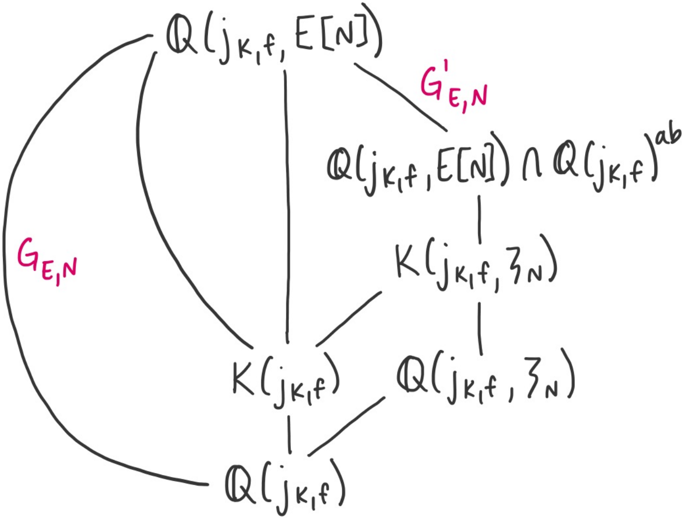
Therefore, we have that $K(j_{K,f}, \zeta_N, \sqrt{\alpha})$ is an abelian extension contained in $F(E[N])/F$, which is sometimes just $K(j_{K,f}, \zeta_N)$ if $\sqrt{\alpha} \in K(j_{K,f}, \zeta_N)$.

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 $G_{E,N}$.

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:

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

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

(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

$$K(j_{K,f}, \zeta_{p^n}) \quad \text{or} \quad K(j_{K,f}, \zeta_{p^n}, \sqrt{\alpha})$$

is the maximal abelian subextension of $\mathbb{Q}(j_{K,f}, E[p^n])/\mathbb{Q}(j_{K,f})$.

$\square$

Maximal abelian subextensions

Theorem (H., 2024)

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K, $f \geq 1$.

Maximal abelian subextensions

Theorem (H., 2024)

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K, $f \geq 1$.

(1) *If p is any prime such that $p \nmid \Delta_K f^2$, then*

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{p^n}).$$

Maximal abelian subextensions

Theorem (H., 2024)

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K, $f \geq 1$.

(1) *If p is any prime such that $p \nmid \Delta_K f^2$, then*

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{p^n}).$$

(2) *If $p > 2$ prime such that $p \mid \Delta_K f^2$, then*

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_{p^n}, \sqrt{\alpha}) & \text{if } E \text{ is a twist of a simplest model,} \\ \mathbb{Q}(\zeta_{p^n}) & \text{if } E \text{ is a simplest model.} \end{cases}$$

Maximal abelian subextensions

Theorem (H., 2024)

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of K, $f \geq 1$.

(1) *If p is any prime such that $p \nmid \Delta_K f^2$, then*

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{p^n}).$$

(2) *If $p > 2$ prime such that $p \mid \Delta_K f^2$, then*

$$\mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_{p^n}, \sqrt{\alpha}) & \textit{if } E \textit{ is a twist of a simplest model,} \\ \mathbb{Q}(\zeta_{p^n}) & \textit{if } E \textit{ is a simplest model.} \end{cases}$$

(3) *Let $p = 2$ such that $2 \mid \Delta_K f^2$.*

- *If $\Delta_K f^2 = -12$ or -28, then* $\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab} = K(\zeta_{2^{n+1}})$.
- *If $\Delta_K f^2 = -4, -8,$ or -16, then*

$$\mathbb{Q}(E[2^n]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_{2^{n+1}}, \sqrt{\alpha}) & \textit{if } E \textit{ is a twist of a simplest model,} \\ \mathbb{Q}(\zeta_{2^{n+1}}) & \textit{if } E \textit{ is a simplest model.} \end{cases}$$

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

E is a quadratic twist of $E'/\mathbb{Q} : y^2 = x^3 - 1715x + 33614$ (49.a2) by -14.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

E is a quadratic twist of $E'/\mathbb{Q} : y^2 = x^3 - 1715x + 33614$ (49.a2) by -14.

Thus, $\mathbb{Q}(E[7^n]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_{7^n}, \sqrt{-14})$.

Example

Example ($p = 7$ and $\Delta_K f^2 = -7$)

Let $E/\mathbb{Q} : y^2 = x^3 - 140x - 784$ (3136.n4), where $j(E) = -3375$.

Here $K = \mathbb{Q}(\sqrt{-7})$.

In this case, $G_{E,7^n} = \mathcal{N}_{\delta,0}(7^n)$, where $\delta = -7/4$.

E is a quadratic twist of $E'/\mathbb{Q} : y^2 = x^3 - 1715x + 33614$ (49.a2) by -14.

Thus, $\mathbb{Q}(E[7^n]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_{7^n}, \sqrt{-14})$.

The simplest CM curve E' has image

$$G_{E',7^n} = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \left\{ \begin{pmatrix} a & b \\ \delta b & a \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^{\times 2}, b \in \mathbb{Z}/7\mathbb{Z} \right\} \right\rangle,$$

which is an index 2 subgroup of $\mathcal{N}_{\delta,0}(7^n)$. Thus, $\mathbb{Q}(E[7^n]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_{7^n})$.

Questions?