Prime degree isogenies of elliptic curves over number fields

Nicolas Billerey

Université Clermont Auvergne
Laboratoire de mathématiques Blaise Pascal

8th atelier PARI/GP
Clermont-Ferrand, June 20, 2017

Notation

$\overline{\mathbf{Q}}$ algebraic closure of $\mathbf{Q}$;

$K \subset \overline{\mathbf{Q}}$ number field ;

$d = [K : \mathbf{Q}]$;

$\Delta_K = \mathrm{Disc}(K)$;

$\mathcal{O}_K$ integer ring of K ;

E/K elliptic curve ;

$\mathrm{End}_K(E)$ ring of K-endomorphisms of E.

Notation

$\overline{\mathbf{Q}}$ algebraic closure of $\mathbf{Q}$;

$K \subset \overline{\mathbf{Q}}$ number field ;

$d = [K : \mathbf{Q}]$;

$\Delta_K = \mathrm{Disc}(K)$;

$\mathcal{O}_K$ integer ring of K ;

E/K elliptic curve ;

$\mathrm{End}_K(E)$ ring of K-endomorphisms of E.

For every prime number p, write

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbf{Q}}/K) \longrightarrow \mathrm{Aut}(E[p])$$

the representation giving the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ on $E[p]$.

The set $\mathrm{Red}(E/K)$

The following are equivalent :

(i) The representation $\rho_{E,p}$ is reducible ;

(ii) There exist an elliptic curve E'/K and $\varphi \colon E \to E'$ a K-isogeny of degree p.

The set $\mathrm{Red}(E/K)$

The following are equivalent :

(i) The representation $\rho_{E,p}$ is reducible ;

(ii) There exist an elliptic curve E'/K and $\varphi \colon E \to E'$ a K-isogeny of degree p.

$$\mathrm{Red}(E/K) \overset{\text{def}}{=} \{p \text{ prime satisfying (i) and (ii)}\}.$$

Goal

We have

$$|\mathrm{Red}(E/K)| < +\infty \iff \mathrm{End}_K(E) = \mathbf{Z}.$$

Goal

We have

$$|\mathrm{Red}(E/K)| < +\infty \iff \mathrm{End}_K(E) = \mathbf{Z}.$$

Main goal : When $\mathrm{End}_K(E) = \mathbf{Z}$, explicitly compute the (finite) set $\mathrm{Red}(E/K)$ from a given Weierstrass equation of E.

Goal

We have

$$|\mathrm{Red}(E/K)| < +\infty \iff \mathrm{End}_K(E) = \mathbf{Z}.$$

Main goal : When $\mathrm{End}_K(E) = \mathbf{Z}$, explicitly compute the (finite) set $\mathrm{Red}(E/K)$ from a given Weierstrass equation of E.

Remarks.

Goal

We have
$$|\mathrm{Red}(E/K)| < +\infty \iff \mathrm{End}_K(E) = \mathbf{Z}.$$

Main goal : When $\mathrm{End}_K(E) = \mathbf{Z}$, explicitly compute the (finite) set $\mathrm{Red}(E/K)$ from a given Weierstrass equation of E.

Remarks.

1. Mazur ($K = \mathbf{Q}$) :

$$\mathrm{Red}(E/\mathbf{Q}) \subset \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

Goal

We have

$$|\mathrm{Red}(E/K)| < +\infty \Longleftrightarrow \mathrm{End}_K(E) = \mathbf{Z}.$$

Main goal : When $\mathrm{End}_K(E) = \mathbf{Z}$, explicitly compute the (finite) set $\mathrm{Red}(E/K)$ from a given Weierstrass equation of E.

Remarks.

1. Mazur ($K = \mathbf{Q}$) :

$$\mathrm{Red}(E/\mathbf{Q}) \subset \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

2. No known generalization of Mazur's result to degree $d > 1$.

Goal

We have

$$|\mathrm{Red}(E/K)| < +\infty \iff \mathrm{End}_K(E) = \mathbf{Z}.$$

Main goal : When $\mathrm{End}_K(E) = \mathbf{Z}$, explicitly compute the (finite) set $\mathrm{Red}(E/K)$ from a given Weierstrass equation of E.

Remarks.

1. Mazur ($K = \mathbf{Q}$) :

$$\mathrm{Red}(E/\mathbf{Q}) \subset \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

2. No known generalization of Mazur's result to degree $d > 1$.
3. Effective results (depending on E) of Gaudron-Rémond. Useful in practice ?

If E has good reduction at a prime ideal $\mathfrak{q}$, put :

If E has good reduction at a prime ideal $\mathfrak{q}$, put :

$\mathbf{F}_{\mathfrak{q}} = \mathcal{O}_K/\mathfrak{q}$ residual field ;

$\widetilde{E}/\mathbf{F}_{\mathfrak{q}}$ reduction of E modulo $\mathfrak{q}$;

$\mathrm{N}(\mathfrak{q}) = |\mathbf{F}_{\mathfrak{q}}|$ norm of $\mathfrak{q}$.

If E has good reduction at a prime ideal $\mathfrak{q}$, put :

$\mathbf{F}_{\mathfrak{q}} = \mathcal{O}_K/\mathfrak{q}$ residual field ;

$\widetilde{E}/\mathbf{F}_{\mathfrak{q}}$ reduction of E modulo $\mathfrak{q}$;

$\mathrm{N}(\mathfrak{q}) = |\mathbf{F}_{\mathfrak{q}}|$ norm of $\mathfrak{q}$.

Define

$$a_{\mathfrak{q}} = \mathrm{N}(\mathfrak{q}) + 1 - \left|\widetilde{E}(\mathbf{F}_{\mathfrak{q}})\right| \quad \text{and} \quad P_{\mathfrak{q}}(X) = X^2 - a_{\mathfrak{q}}X + \mathrm{N}(\mathfrak{q}).$$

Useful background on elliptic curves

If E has good reduction at a prime ideal $\mathfrak{q}$, put :

$\mathbf{F}_\mathfrak{q} = \mathcal{O}_K/\mathfrak{q}$ residual field ;

$\widetilde{E}/\mathbf{F}_\mathfrak{q}$ reduction of E modulo $\mathfrak{q}$;

$\mathrm{N}(\mathfrak{q}) = |\mathbf{F}_\mathfrak{q}|$ norm of $\mathfrak{q}$.

Define

$$a_\mathfrak{q} = \mathrm{N}(\mathfrak{q}) + 1 - \left|\widetilde{E}(\mathbf{F}_\mathfrak{q})\right| \quad \text{and} \quad P_\mathfrak{q}(X) = X^2 - a_\mathfrak{q} X + \mathrm{N}(\mathfrak{q}).$$

Hasse : $|a_\mathfrak{q}| \leq 2\sqrt{\mathrm{N}(\mathfrak{q})}$

If E has good reduction at a prime ideal $\mathfrak{q}$, put :

$\mathbf{F}_{\mathfrak{q}} = \mathcal{O}_K/\mathfrak{q}$ residual field ;

$\widetilde{E}/\mathbf{F}_{\mathfrak{q}}$ reduction of E modulo $\mathfrak{q}$;

$\mathrm{N}(\mathfrak{q}) = |\mathbf{F}_{\mathfrak{q}}|$ norm of $\mathfrak{q}$.

Define

$$a_{\mathfrak{q}} = \mathrm{N}(\mathfrak{q}) + 1 - \left|\widetilde{E}(\mathbf{F}_{\mathfrak{q}})\right| \quad \text{and} \quad P_{\mathfrak{q}}(X) = X^2 - a_{\mathfrak{q}}X + \mathrm{N}(\mathfrak{q}).$$

Hasse : $|a_{\mathfrak{q}}| \leq 2\sqrt{\mathrm{N}(\mathfrak{q})}$ or, equivalently,

$$P_{\mathfrak{q}}(X) = (X - \alpha_{\mathfrak{q}})(X - \beta_{\mathfrak{q}}) \quad \text{with} \quad |\alpha_{\mathfrak{q}}| = |\beta_{\mathfrak{q}}| = \sqrt{\mathrm{N}(\mathfrak{q})}.$$

General idea

Suppose that E is given by an integral Weierstrass equation of discriminant Δ_E.

General idea

Suppose that E is given by an integral Weierstrass equation of discriminant Δ_E.
For every prime number ℓ, one constructs an integer B_ℓ such that

$$p \in \mathrm{Red}(E/K) \Longrightarrow p \mid 6\Delta_K \cdot \mathrm{N}(\Delta_E) \cdot B_\ell.$$

General idea

Suppose that E is given by an integral Weierstrass equation of discriminant Δ_E.
For every prime number ℓ, one constructs an integer B_ℓ such that

$$p \in \mathrm{Red}(E/K) \Longrightarrow p \mid 6\Delta_K \cdot \mathrm{N}(\Delta_E) \cdot B_\ell.$$

Remarks.

1. We do not assume $\mathrm{End}_K(E) = \mathbf{Z}$,

Suppose that E is given by an integral Weierstrass equation of discriminant Δ_E.
For every prime number ℓ, one constructs an integer B_ℓ such that

$$p \in \mathrm{Red}(E/K) \Longrightarrow p \mid 6\Delta_K \cdot \mathrm{N}(\Delta_E) \cdot B_\ell.$$

Remarks.

1. We do not assume $\mathrm{End}_K(E) = \mathbf{Z}$, but if $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$ for all ℓ.

Suppose that E is given by an integral Weierstrass equation of discriminant Δ_E.
For every prime number ℓ, one constructs an integer B_ℓ such that

$$p \in \mathrm{Red}(E/K) \Longrightarrow p \mid 6\Delta_K \cdot \mathrm{N}(\Delta_E) \cdot B_\ell.$$

Remarks.

1. We do not assume $\mathrm{End}_K(E) = \mathbf{Z}$, but if $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$ for all ℓ.
2. By construction, $B_\ell = 0$ if ℓ is ‘bad’, i.e. E has bad reduction at some prime ideal above ℓ.

Suppose that E is given by an integral Weierstrass equation of discriminant Δ_E.
For every prime number ℓ, one constructs an integer B_ℓ such that

$$p \in \mathrm{Red}(E/K) \Longrightarrow p \mid 6\Delta_K \cdot \mathrm{N}(\Delta_E) \cdot B_\ell.$$

Remarks.

1. We do not assume $\mathrm{End}_K(E) = \mathbf{Z}$, but if $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$ for all ℓ.
2. By construction, $B_\ell = 0$ if ℓ is 'bad', i.e. E has bad reduction at some prime ideal above ℓ.
3. If $B_\ell \neq 0$ for some ('good') prime ℓ, then we get a bound on $\mathrm{Red}(E/K)$.

A monoïd law

The set $M = \{P \in \mathbf{Z}[X] \text{ monic such that } P(0) \neq 0\}$ equipped with the law $*$ defined for $P, Q \in M$ by

$$(P * Q)(X) = \mathrm{Res}_Z \left(P(Z), Z^{\deg(Q)} Q\left(\frac{X}{Z}\right)\right)$$

has a monoïd strucutre with identity element $\Psi_1(X) = X - 1$.

A monoïd law

The set $M = \{P \in \mathbf{Z}[X]$ monic such that $P(0) \neq 0\}$ equipped with the law $*$ defined for $P, Q \in M$ by

$$(P * Q)(X) = \mathrm{Res}_Z \left(P(Z), Z^{\deg(Q)} Q\left(\frac{X}{Z}\right)\right)$$

has a monoïd strucutre with identity element $\Psi_1(X) = X - 1$.

For any integer $r \geq 1$ and for any $P \in M$, there exists a unique polynomial $P^{(r)} \in M$ such that

$$(P * \Psi_r)(X) = P^{(r)}(X^r), \quad \text{where } \Psi_r(X) = X^r - 1.$$

The integers B_ℓ

For a good prime ℓ define

The integers B_ℓ

For a good prime ℓ define

$$P_\ell^* = \mathop{\ast}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12 v_{\mathfrak{q}}(\ell))} \in \mathbf{Z}[X] \quad \text{and} \quad B_\ell = \prod_{k=0}^{\lfloor \frac{d}{2} \rfloor} P_\ell^*(\ell^{12k}),$$

where $\mathfrak{q}$ runs through the prime ideals above ℓ and $v_{\mathfrak{q}}(\ell)$ denotes the valuation of $\ell \mathcal{O}_K$ at $\mathfrak{q}$.

The integers B_ℓ

For a good prime ℓ define

$$P_\ell^* = \mathop{\ast}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12 v_{\mathfrak{q}}(\ell))} \in \mathbf{Z}[X] \quad \text{and} \quad B_\ell = \prod_{k=0}^{\lfloor \frac{d}{2} \rfloor} P_\ell^*(\ell^{12k}),$$

where $\mathfrak{q}$ runs through the prime ideals above ℓ and $v_{\mathfrak{q}}(\ell)$ denotes the valuation of $\ell\mathcal{O}_K$ at $\mathfrak{q}$.

Remarks.

1. If $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$, for all ℓ.

The integers B_ℓ

For a good prime ℓ define

$$P_\ell^* = \mathop{\ast}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12 v_{\mathfrak{q}}(\ell))} \in \mathbf{Z}[X] \quad \text{and} \quad B_\ell = \prod_{k=0}^{\lfloor \frac{d}{2} \rfloor} P_\ell^*(\ell^{12k}),$$

where $\mathfrak{q}$ runs through the prime ideals above ℓ and $v_{\mathfrak{q}}(\ell)$ denotes the valuation of $\ell\mathcal{O}_K$ at $\mathfrak{q}$.

Remarks.

1. If $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$, for all ℓ.
2. If d is *odd*, then $B_\ell \neq 0$, for every good ℓ.

The integers B_ℓ

For a good prime ℓ define

$$P_\ell^* = \mathop{\ast}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12 v_{\mathfrak{q}}(\ell))} \in \mathbf{Z}[X] \quad \text{and} \quad B_\ell = \prod_{k=0}^{\lfloor \frac{d}{2} \rfloor} P_\ell^*(\ell^{12k}),$$

where $\mathfrak{q}$ runs through the prime ideals above ℓ and $v_{\mathfrak{q}}(\ell)$ denotes the valuation of $\ell\mathcal{O}_K$ at $\mathfrak{q}$.

Remarks.

1. If $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$, for all ℓ.
2. If d is *odd*, then $B_\ell \neq 0$, for every good ℓ.
3. There exist K and E/K with $\mathrm{End}_K(E) = \mathbf{Z}$ such that $B_\ell = 0$ for every ℓ,

The integers B_ℓ

For a good prime ℓ define

$$P_\ell^* = \mathop{\Large *}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12 v_{\mathfrak{q}}(\ell))} \in \mathbf{Z}[X] \quad \text{and} \quad B_\ell = \prod_{k=0}^{\lfloor \frac{d}{2} \rfloor} P_\ell^*(\ell^{12k}),$$

where $\mathfrak{q}$ runs through the prime ideals above ℓ and $v_{\mathfrak{q}}(\ell)$ denotes the valuation of $\ell\mathcal{O}_K$ at $\mathfrak{q}$.

Remarks.

1. If $\mathrm{End}_K(E) \neq \mathbf{Z}$, then $B_\ell = 0$, for all ℓ.
2. If d is *odd*, then $B_\ell \neq 0$, for every good ℓ.
3. There exist K and E/K with $\mathrm{End}_K(E) = \mathbf{Z}$ such that $B_\ell = 0$ for every ℓ, but it is ‘rare’ and in any case (assuming $\mathrm{End}_{\overline{\mathbf{Q}}}(E) = \mathbf{Z}$), another similar result applies.

The algorithm

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

The algorithm

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

1. $S_1 = \Omega\left(6\Delta_K \cdot \mathrm{N}(\Delta_E)\right)$.

The algorithm

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

1. $S_1 = \Omega\left(6\Delta_K \cdot \mathrm{N}(\Delta_E)\right)$.
2. `[initialisation]` Search for $\ell_0 <$ (bound1) such that we have $B_{\ell_0} \neq 0$. Set $B = B_{\ell_0}$.

The algorithm

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

1. $S_1 = \Omega\,(6\Delta_K \cdot \mathrm{N}(\Delta_E))$.
2. `[initialisation]` Search for $\ell_0 <$ (bound1) such that we have $B_{\ell_0} \neq 0$. Set $B = B_{\ell_0}$.
3. Search for $\ell_1, \ldots, \ell_m <$ (bound2) such that we have $B_{\ell_i} \neq 0$; for $i = 1, \ldots, m$ do

The algorithm

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

1. $S_1 = \Omega\,(6\Delta_K \cdot \mathrm{N}(\Delta_E))$.
2. `[initialisation]` Search for $\ell_0 <$ (bound1) such that we have $B_{\ell_0} \neq 0$. Set $B = B_{\ell_0}$.
3. Search for $\ell_1, \ldots, \ell_m <$ (bound2) such that we have $B_{\ell_i} \neq 0$; for $i = 1, \ldots, m$ do
   - $B = \gcd(B, B_{\ell_i})$, $\quad S_2 = \Omega(B)$ and $\quad S = S_1 \cup S_2$

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

1. $S_1 = \Omega\left(6\Delta_K \cdot \mathrm{N}(\Delta_E)\right)$.
2. `[initialisation]` Search for $\ell_0 <$ (bound1) such that we have $B_{\ell_0} \neq 0$. Set $B = B_{\ell_0}$.
3. Search for $\ell_1, \ldots, \ell_m <$ (bound2) such that we have $B_{\ell_i} \neq 0$; for $i = 1, \ldots, m$ do
   - $B = \gcd(B, B_{\ell_i})$, $\quad S_2 = \Omega(B) \quad$ and $\quad S = S_1 \cup S_2$
   - `[cleaning]`

$$
\begin{aligned}
S &\leftarrow S \setminus \{p \in S; \exists\ \mathfrak{q} \text{ good s.t. } P_{\mathfrak{q}} \text{ irreducible mod } p\} \\
S_1 &\leftarrow S \cap S_1
\end{aligned}
$$

The algorithm

For any integer $n \neq 0$, denote by $\Omega(n)$ its prime divisors.

1. $S_1 = \Omega\,(6\Delta_K \cdot \mathrm{N}(\Delta_E))$.
2. `[initialisation]` Search for $\ell_0 <$ (bound1) such that we have $B_{\ell_0} \neq 0$. Set $B = B_{\ell_0}$.
3. Search for $\ell_1, \ldots, \ell_m <$ (bound2) such that we have $B_{\ell_i} \neq 0$; for $i = 1, \ldots, m$ do
   - $B = \gcd(B, B_{\ell_i})$, $\quad S_2 = \Omega(B)$ and $\quad S = S_1 \cup S_2$
   - `[cleaning]`

$$\begin{aligned} S &\leftarrow S \setminus \{p \in S; \exists\ \mathfrak{q} \text{ good s.t. } P_{\mathfrak{q}} \text{ irreducible mod } p\} \\ S_1 &\leftarrow S \cap S_1 \end{aligned}$$

4. Determine $\mathrm{Red}(E/K) \subset S$.

TO DO

1. Certify step 4.

TO DO

1. Certify step 4.
2. Test/compare.

TO DO

1. Certify step 4.
2. Test/compare.
3. Compute equations of the isogenous curves/isogenies.

TO DO

1. Certify step 4.
2. Test/compare.
3. Compute equations of the isogenous curves/isogenies.
4. Compute the whole isogeny data (matrix, graph) ; see `ellisomat` command.