Constructing CM elliptic curves with minimal Galois image

Riccardo Pengo (based on joint work with Francesco Campagna)

arXiv:2201.04046 (To appear in the Proceedings of the 18th AGC^{2}T conference.)

Unité des mathématiques pures et appliquées, École normale supérieure de Lyon

riccardo.pengo@ens-lyon.fr, riccardopengo@gmail.com

https://sites.google.com/view/riccardopengo/

Atélier PARI/GP

Besançon, 12 January 2022

A disclaimer

From Karim's email, on the 13th of December, 2021:

> (1) A talk you could deliver in about 30 minutes related to an implementation project for PARI/GP. Mention whether it is a past implementation, work in progress or planned work. In the latter two cases, it will be helpful to identify bottlenecks and what help could be useful. "No talk" is an allowed answer. :-)

Computing the Galois image of a non-CM elliptic curve

Fix a number field F with algebraic closure $\overline{F}$, and an elliptic curve $E_{/F}$ such that $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$. Set $E_{\mathrm{tors}} := E(\overline{F})_{\mathrm{tors}}$ and $E[m] := E(\overline{F})[m]$ for any $m \in \mathbb{N}$. We have the Galois representation:

$$\rho_E \colon G_F := \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

putting together the ℓ-adic ones $\rho_{E,\ell^\infty} \colon G_F \to \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty]) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$, where $E[\ell^\infty] := \varinjlim_{n \in \mathbb{N}} E[\ell^n]$.

Serre (1971) The index $\mathscr{I}(E/F) := |\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \colon \rho_E(G_F)|$ is finite.

How can we make this theorem effective?

Lombardo (2015) $\mathscr{I}(E/F) < \exp(1.9 \cdot 10^{10}) \cdot (d_F \cdot \max\{1, h(E), \log(d_F)\})^{12395}$, where $d_F := [F \colon \mathbb{Q}]$ and $h(E)$ denotes the stable Faltings height of E, computed in PARI/GP by `ellheight(E)`.

Zywina (2015) The set $\{\mathscr{I}(E/\mathbb{Q}) \colon E_{/\mathbb{Q}}\} \subseteq \mathbb{N}$ is finite, if we assume Serre's uniformity conjecture.

Brau-Avila (2015) There is a *very slow*, deterministic algorithm which computes an integer $m \geq 2$ such that $\rho_E(G_F) = \pi_m^{-1}(\rho_{E,m}(G_F))$, where $\pi_m \colon \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \twoheadrightarrow \mathrm{Aut}_{\mathbb{Z}}(E[m])$ is the reduction map, and $\rho_{E,m} := \pi_m \circ \rho_E$. Moreover, there is another algorithm which computes $\rho_{E,m}(G_F)$, and thus can be used to compute $\mathscr{I}(E/F)$.

Galois images of CM elliptic curves

Fix a number field F, and an elliptic curve $E_{/F}$ such that $\mathrm{End}_F(E) \cong \mathscr{O} \subseteq K \subseteq F$, where $\mathscr{O}$ is an order inside an imaginary quadratic field K. Then $\rho_E(G_F) \subseteq \mathrm{Aut}_{\mathscr{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathscr{O}}^\times$, and $\mathscr{I}(E/F) := |\mathrm{Aut}_{\mathscr{O}}(E_{\mathrm{tors}}) \colon \widehat{\mathscr{O}}^\times|$ is finite.

Campagna & P. (2021) $\mathscr{I}(E/F) = [F \cap K^{\mathrm{ab}} \colon H_{\mathscr{O}}] \cdot (|\mathscr{O}^\times|/[F(E_{\mathrm{tors}}) \colon FK^{\mathrm{ab}}])$, where $H_{\mathscr{O}} = K(j(E))$ is the ring class field of $\mathscr{O}$. Moreover, for any finite $L \supseteq F$ such that $F(E_{\mathrm{tors}}) = LK^{\mathrm{ab}}$, one has:

$$\mathscr{I}(E/F) = \frac{|\mathscr{O}^\times| \cdot [L \cap K^{\mathrm{ab}} \colon K]}{|\mathrm{Pic}(\mathscr{O})| \cdot [L \colon F]}$$

and this allows us to compute $\mathscr{I}(E/F)$. Indeed, such an L always exists, and one can take $L = F(E[I])$ for any ideal $I \subseteq \mathscr{O}$ such that $|\mathbb{Z}/(I \cap \mathbb{Z})| > \max(2, |\mathscr{O}^\times|/2)$. This gives an algorithm to compute $\mathscr{I}(E/F)$.

Challenge: Implement this algorithm completely in PARI/GP.

Rouse, Sutherland & Zureick-Brown (2021): If $F = \mathbb{Q}$, there is an algorithm, more efficient than Brau-Avila's, which computes $\rho_{E,\ell^\infty}(G_F)$, for any prime $\ell \in \mathbb{N}$, using work of **Lozano-Robledo (2018)**. This algorithm works also without CM, is implemented in MAGMA, and was applied to the 238764310 elliptic curves appearing in the database by **Balakrishnan, Ho, Kaplan, Spicer, Stein & Weigandt (2016)**.

ENS DE LYON

How to face our first challenge

To implement the algorithm, we need the following steps:

- write a function `ellcmdisc(E)` which takes as input an elliptic curve E defined over a number field F and returns 1 if E does not have complex multiplication, and otherwise returns the discriminant $\Delta_{\mathcal{O}} \in \mathbb{Z}$ of the imaginary quadratic order $\mathcal{O}$ such that $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$;
- write a function `elldivfield(E,n)` which takes as input an elliptic curve E defined over a number field F, and an integer $n \in \mathbb{N}$ (or, more generally, an element $n \in \mathrm{End}_F(E)$), and outputs an irreducible polynomial $f(x) \in K[x]$ such that the number field $F[x]/(f)$ is the n-division field $F(E[n])$ of E;
- write a function `nfrelativize(f,g)` which, given two irreducible polynomials $f, g \in \mathbb{Q}[x]$ and some embedding $K := \mathbb{Q}[x]/(f) \hookrightarrow F := \mathbb{Q}[x]/(g)$, returns a polynomial $h(y) \in K[y]$ such that $F \cong K[y]/(h)$;
- write a function `subab(K,f,{flag = 0})` which, given a number field K and an irreducible polynomial $f \in K[x]$, returns another irreducible polynomial $g \in K[x]$ such that $K[x]/(g)$ is the maximal abelian sub-extension of $L := K[x]/(f)$. If `flag = 1`, return just the degree $[L \cap K^{ab} : K]$.

Then, we can easily compute $\mathscr{I}(E/F)$, using `quadclassunit` to compute $|\mathrm{Pic}(\mathcal{O})|$.

CM elliptic curves with minimal Galois image

Fix a number field F and an elliptic curve $E_{/F}$ such that $\mathrm{End}_F(E) \cong \mathscr{O} \subseteq K \subseteq F$.
Another good choice for a finite extension $L \supseteq F$ such that $F(E_{\mathrm{tors}}) = LK^{\mathrm{ab}}$, is given by $L = F(\sqrt[u]{\alpha})$, where $u = |\mathscr{O}^\times|$ and $\alpha \in F$ is such that E is the twist by $\sqrt[u]{\alpha}$ of an elliptic curve $E'_{/F}$ such that $F(E'_{\mathrm{tors}}) = FK^{\mathrm{ab}}$.

Campagna & P. (2020) For any $\mathscr{O}$ such that $\Delta_{\mathscr{O}} \not\in \{-4f^2 \mid f = p_1^{a_1} \cdots p_r^{a_r}, p_1 \equiv \cdots \equiv p_r \equiv 1(4)\}$, there are infinitely many non-isomorphic elliptic curves $E'_{/H_{\mathscr{O}}}$ such that $H_{\mathscr{O}}(E'_{\mathrm{tors}}) = K^{\mathrm{ab}}$.

The previous theorem gives an algorithm to construct such an E'. More precisely (if $\Delta_{\mathscr{O}} < -4$ and $K \neq \mathbb{Q}(i)$):

- take any elliptic curve $E_{/H_{\mathscr{O}}}$ such that $\mathrm{End}_{H_{\mathscr{O}}}(E) \cong \mathscr{O}$, *e.g.* `E = ellfromj(`$j(\mathscr{O})$`);`
- if $H_{\mathscr{O}}(E[3]) \subseteq K^{\mathrm{ab}}$, then $\mathscr{I}(E/H_{\mathscr{O}}) = 2$, and we can take $E' = E$;
- if $H_{\mathscr{O}}(E[3]) \not\subseteq K^{\mathrm{ab}}$, continue as follows:
  - take any (*e.g.* the smallest) prime $p \in \mathbb{N}$ which splits in K, is inert in $\mathbb{Q}(i)$, and such that $p \nmid \mathfrak{f}_{\mathscr{O}} \cdot \mathrm{N}_{H_{\mathscr{O}}/\mathbb{Q}}(\mathfrak{f}_E)$;
  - find $\alpha \in H_{\mathscr{O}}$ such that $H_{\mathscr{O}}(E[\mathfrak{p}]) = H_{\mathfrak{p},\mathscr{O}}(\sqrt{\alpha})$, where $p \cdot \mathscr{O} = \mathfrak{p}\overline{\mathfrak{p}}$ and $H_{p,\mathscr{O}}$ is the p-th ray class field of $\mathscr{O}$;
  - take $E' = E^{(\alpha)}$.

Challenge: Implement this algorithm completely in PARI/GP.
Theoretical challenge: Find $A, B \in \mathbb{Q}(u,v)$ such that $E' \colon y^2 = x^3 + A(j(\mathscr{O}), \Delta_{\mathscr{O}}) \cdot x + B(j(\mathscr{O}), \Delta_{\mathscr{O}})$ for each $\mathscr{O}$.

An explicit example

Consider $\mathscr{O} = \mathbb{Z}[\sqrt{-5}]$, so that $\Delta_{\mathscr{O}} = -20$ and $H_{\mathscr{O}} = \mathbb{Q}(\sqrt{-5}, i)$. Then, we can take:

$$E \colon y^2 = x^3 + 29736960(36023\sqrt{5} - 80550)x - 55826186240(16154216\sqrt{5} + 36121925)$$

so that $j(E) = 282880\sqrt{5} + 632000$ and $\mathscr{I}(E/H_{\mathscr{O}}) = 1$. We can take $p = 3$. Then, $3 \cdot \mathscr{O} = \mathfrak{p}\overline{p}$ with $\mathfrak{p} = (3, \sqrt{-5} + 1)$. Hence, we have the equality $H_{\mathfrak{p},\mathscr{O}} = H_{\mathscr{O}}$, which is reflected by the factorization:

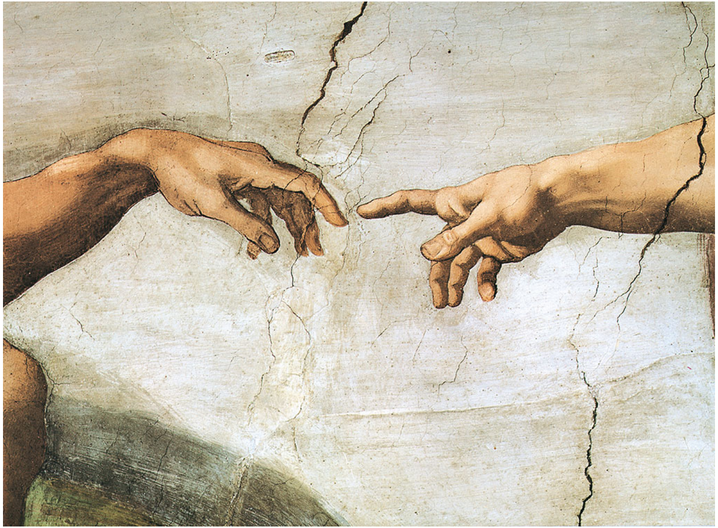
$$\begin{aligned} \phi_{E,3}(x) = 3 \cdot &(x + 594880 + 59840i - 26048\sqrt{-5} + 266816\sqrt{5}) \cdot \\ &(x + 594880 - 59840i + 26048\sqrt{-5} + 266816\sqrt{5}) \cdot \\ &(x^2 - (1189760 + 533632\sqrt{5})x - 2668089262080 - 1193205432320\sqrt{5}) \end{aligned}$$

of the 3-division polynomial of E. Thus, we have $H_{\mathscr{O}}(E[\mathfrak{p}]) = H_{\mathscr{O}}(\sqrt{\alpha})$, where:

$$\alpha := 13956546560 \cdot (1190435 + 2307955i - 1032149\sqrt{-5} + 532379\sqrt{5})$$

and $E' = E^{(\alpha)}$, which gives $E' \colon y^2 - \left(\frac{1-i+\sqrt{-5}+\sqrt{5}}{2}\right)xy - \left(\frac{1+i+\sqrt{-5}+\sqrt{5}}{2}\right)y = x^3 + x^2 + \left(2i - \sqrt{5}\right)x - 1 + 2i$.

Thank you very much for your attention!



A minimal and a maximal index...

Michelangelo Buonarroti,
La creazione di Adamo