Faltings method, Galois extensions of exponent four and abelian surfaces over $\mathbb{Q}$

Ane Anema

Rijksuniversiteit Groningen

22 January 2016

Motivation

- Consider the following curves over $\mathbb{Q}$

$$\begin{aligned} C &: y^2 = \left(x^3 + 60x + 20\right)(60x + 20)(60x - 60) \\ E_1 &: y^2 = x^3 - 39x - 70 \\ E_2 &: y^2 = x^3 - 52500x - 5537500. \end{aligned}$$

- Are $\operatorname{Jac}(C)$ and $E_1 \times E_2$ isogeneous over $\mathbb{Q}$?
- Possible methods to answer this question:
  1. $\mathbb{C}$ uniformization, see Van Wamelen (1999);
  2. $\mathbb{Q}_p$ uniformization, see Kadziela (2007);
  3. Faltings method.

Outline

History

- Introduced by Faltings (1983) to prove Shafarevich Conjecture.
- Made effective by Serre for certain elliptic curves.
- Extended to more general 2-adic 2-dimensional representations by Livné (1987) and by Chênevert (2008).
- Generalized to ℓ-adic d-dimensional representations by Grenié (2007).

Isogeny Theorem

Theorem (Faltings)

If A_1, A_2 are abelian varieties of dimension d over a number field K, then:

- *the action of G_K on $T_\ell A_i \otimes \mathbb{Q}_\ell$ is semi-simple for $i = 1, 2$,*
- *there is an isomorphism*

$$\mathrm{Hom}_K(A_1, A_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[G_K]}(T_\ell A_1, T_\ell A_2).$$

The method - a version in between Chênevert and Grenié

Theorem

- *G a profinite group,*
- *$\rho_i : G \to \mathrm{GL}_d(\mathbb{Z}_\ell)$ a continuous representation for $i = 1, 2$,*
- *$e \in \mathbb{Z}$ such that $d \leq \ell^e$,*
- *$\Sigma \subset G$ such that the characteristic polynomials of $\rho_1(h)$ and $\rho_2(h)$ are equal for all $h \in \Sigma$, and*
- *$N \subset G$ an open normal subgroup with $\bar{\rho}_i(N)$ a ℓ-subgroup.*

If

$$\overline{\Sigma} = \left\{ g h^n g^{-1} : g \in G, h \in \Sigma, n \in \mathbb{Z} \right\}$$

maps surjectively to G/N^{ℓ^e}, then $\mathrm{tr}\,(\rho_1) = \mathrm{tr}\,(\rho_2)$.

Note: N^m is defined as the closure of $\langle n^m : n \in N \rangle$ in G.

Corollary

If the ρ_i are also semi-simple, then they are isomorphic.

Example

- E_1, E_2 elliptic curves over a number field K.
- S the set of primes of bad reduction of E_i and primes above 2.
- Galois representations

$$\begin{tikzcd} G_K \arrow[r, "\rho_i"] \arrow[d] & \mathrm{Aut}\,(T_2 E_i) \cong \mathrm{GL}_2(\mathbb{Z}_2) \\ \mathrm{Gal}\,(K_S/K). \arrow[ur, dashed, "\rho_i'"'] & \end{tikzcd}$$

- Apply method to ρ_1', ρ_2':
  - $d = 2$, $\ell = 2$ and $e = 1$.
  - $G = \mathrm{Gal}\,(K_S/K)$ and $N = \mathrm{Gal}\,(K_S/K(E_1[2], E_2[2]))$.
  - $G/N^2 \cong \mathrm{Gal}\,(L/K)$ with L the maximal exponent 2 extension of $K(E_1[2], E_2[2])$ in K_S.
  - Čebotarev density theorem.

Deviation group

- Consider the $\mathbb{Z}_\ell$-linear extension of $\rho = (\rho_1, \rho_2)$

$$\tilde{\rho} : \mathbb{Z}_\ell[G] \longrightarrow \mathrm{M}_d(\mathbb{Z}_\ell) \oplus \mathrm{M}_d(\mathbb{Z}_\ell).$$

- Denote $M = \operatorname{im} \tilde{\rho}$.
- The *deviation map* δ is

$$\delta : \ \mathbb{Z}_\ell[G] \xrightarrow{\tilde{\rho}} M \longrightarrow M/\ell M$$

and the *deviation group* is $\delta(G) \subset (M/\ell M)^*$.

Proposition

Let $\Sigma \subset G$ be such that for every conjugacy class C of $\delta(G)$ there exists a $g \in \Sigma$ with $\delta(g) \in C$. Then

$$\operatorname{tr}(\rho_1) \neq \operatorname{tr}(\rho_2) \quad \Longrightarrow \quad \operatorname{tr}(\rho_1)|_\Sigma \neq \operatorname{tr}(\rho_2)|_\Sigma.$$

Proof.

- Suppose $\mathrm{tr}(\rho_1) \neq \mathrm{tr}(\rho_2)$. Then

$$m = \max\{n \in \mathbb{Z} : \mathrm{tr}(\rho_1) \equiv \mathrm{tr}(\rho_2) \mod \ell^n\} < \infty.$$

- Choose $g \in G$ such that $\mathrm{tr}(\rho_1(g)) \not\equiv \mathrm{tr}(\rho_2(g)) \mod \ell^{m+1}$.
- Take $h \in \Sigma$ such that $\delta(h) = \delta\left(aga^{-1}\right)$ for some $a \in G$.
- Consider the R-module homomorphism $\psi : M \to R/\ell^{m+1}$

$$(A, B) \longmapsto \mathrm{tr}(A) - \mathrm{tr}(B) \mod \ell^{m+1}.$$

- Since $\ell M \subset \ker \psi$, we get $\bar{\psi} : M/\ell M \to R/\ell^{m+1}$.
- Now

$$\psi \circ \rho(h) = \bar{\psi} \circ \delta(h) = \bar{\psi} \circ \delta\left(aga^{-1}\right) = \psi \circ \rho\left(aga^{-1}\right) = \psi \circ \rho(g).$$

- So $\mathrm{tr}(\rho_1(h)) \neq \mathrm{tr}(\rho_2(h))$.

$\square$

- Since $\delta(G) \subset (M/\ell M)^*$ and

$$\begin{tikzcd} M \arrow[r] \arrow[d] & M/\ell M \arrow[d, dashed] \\ \mathrm{M}_d(\mathbb{Z}_\ell) \oplus \mathrm{M}_d(\mathbb{Z}_\ell) \arrow[r] & \mathrm{M}_d(\mathbb{F}_\ell) \oplus \mathrm{M}_d(\mathbb{F}_\ell) \end{tikzcd}$$

commutes, we obtain $\delta(G) \to \bar{\rho}(G)$.

Example (In general $\delta(G) \to \bar{\rho}(G)$ not injective)

There exist non-isogeneous elliptic curves E_1, E_2 over $\mathbb{Q}$ with all 2-torsion rational. In this case $\bar{\rho}(G_{\mathbb{Q}})$ is trivial, but $\delta(G_{\mathbb{Q}})$ is not!

Proposition

The order of $\delta(G)$ is less than ℓ^{2d^2}.

Residue kernel

- Suppose that $N = \ker \bar{\rho}$, then

$$1 \longrightarrow \delta(N) \longrightarrow \delta(G) \longrightarrow \bar{\rho}(G) \longrightarrow 1$$

with $\bar{\rho}(G)$ in principal well-known and $\delta(N)$ a ℓ-group.

Proposition

Let $e \in \mathbb{Z}$ such that $d \leq \ell^e$ and N such that $\bar{\rho}(N)$ a ℓ-group. If $n \in N$ and the characteristic polynomials of $\rho_1(n)$ and $\rho_2(n)$ are equal, then $\delta(n)$ has order dividing ℓ^e.

Proof.

- Denote the characteristic polynomial of $\rho_i(n)$ by $\chi_i \in \mathbb{Z}_\ell[x]$.
- Cayley-Hamilton Theorem: $\chi_i(\rho_i(n)) = 0$.
- Jordan Normal Form of $\bar{\rho}_i(n)$: $\chi_i \equiv (x-1)^d \mod \ell$.
- Since $\chi_1 = \chi_2$ and $\chi_i = (x-1)^d - \ell F$ for some $F \in \mathbb{Z}_\ell[x]$,

$$(\rho(n) - 1)^d = \ell F(\rho(n)) \in \ell M.$$

- Hence $\delta(n)^{\ell^e} = 1$.

$\square$

Recall

Theorem

- *G a profinite group,*
- *$\rho_i : G \to \mathrm{GL}_d(\mathbb{Z}_\ell)$ a continuous representation for $i = 1, 2$,*
- *$e \in \mathbb{Z}$ such that $d \leq \ell^e$,*
- *$\Sigma \subset G$ such that the characteristic polynomials of $\rho_1(h)$ and $\rho_2(h)$ are equal for all $h \in \Sigma$, and*
- *$N \subset G$ an open normal subgroup with $\bar{\rho}_i(N)$ a ℓ-subgroup.*

If

$$\overline{\Sigma} = \left\{ g h^n g^{-1} : g \in G, h \in \Sigma, n \in \mathbb{Z} \right\}$$

maps surjectively to G/N^{ℓ^e}, then $\mathrm{tr}\,(\rho_1) = \mathrm{tr}\,(\rho_2)$.

Proof of the theorem

Recall that $\overline{\Sigma} = \left\{ g h^k g^{-1} : g \in G, h \in \Sigma, k \in \mathbb{Z} \right\}$.

- Given $h \in \overline{\Sigma}$, the characteristic polynomials of $\rho_i(h)$ are equal.

Claim: $N^{\ell^e} \subset \ker \delta$.

- Consider

$$\begin{tikzcd} N \arrow[r, two heads, "\delta"] \arrow[d, two heads] & \delta(N) \arrow[d, two heads] \\ N/N^{\ell^e} \arrow[r, dashed, two heads] & \delta(N)/\delta(N)^{\ell^e}. \end{tikzcd}$$

- Let $\bar{n} \in \delta(N)/\delta(N)^{\ell^e}$ and $n \in N$ a lift of $\bar{n}$.
- $nN^{\ell^e} = hN^{\ell^e}$ with $h \in \overline{\Sigma}$, because $\overline{\Sigma}/N^{\ell^e} = G/N^{\ell^e}$.
- $h \in N$ since $N^{\ell^e} \subset N$.
- $\delta(h) \in \delta(N)[\ell^e]$.

Proposition

Let H be a finite ℓ-group. If for all $g \in H$ there exists a $h \in H[\ell^e]$ such that $gH^{\ell^e} = hH^{\ell^e}$, then H has exponent dividing ℓ^e.

So

$$\begin{tikzcd} G \arrow[r, two heads, "\delta"] \arrow[d, two heads] & \delta(G) \\ G/N^{\ell^e} \arrow[ur, dashed, two heads, "\tilde{\delta}"'] & \end{tikzcd}$$

Suppose that $\mathrm{tr}\,(\rho_1) \neq \mathrm{tr}\,(\rho_2)$.

- Let $C \subset \delta(G)$ be a conjugacy class.
- Choose a $g \in G$ such that $\delta(g) \in C$.
- There exists a $h \in \overline{\Sigma}$ such that $gN^{\ell^e} = hN^{\ell^e}$. So $\delta(h) \in C$.
- Hence $\mathrm{tr}\,(\rho_1)|_{\overline{\Sigma}} \neq \mathrm{tr}\,(\rho_1)|_{\overline{\Sigma}}$.
- Contradiction.

Remarks

- $\mathbb{Z}_\ell$ can be replaced by $\mathcal{O}_{K_\ell}$ with $[K_\ell : \mathbb{Q}_\ell] < \infty$.
- Is G/N^{ℓ^e} finite? If the pro-ℓ quotient of N is finitely generated, then: yes. (Restricted Burnside Problem)
- Grenié uses *powerful pro-p groups* to bound the length of the lower p-central series of $\delta(N)$:

$$P_1(\delta(N)) \geq P_2(\delta(N)) \geq P_3(\delta(N)) \geq \dots$$

with $P_1(G) = G$ and $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$.

Outline

Preliminaries

- Let K be a number field and S a finite set of places.
- A Galois extension L/K has exponent 4 if $\mathrm{Gal}(L/K)$ is of exponent 4.
- If $L_1, L_2/K$ are exponent 4 Galois extensions, then so is $L_1 \cdot L_2/K$.
- The maximal exponent 4 extension $K_{S,4}$ of K unramified outside S is the compositum of all finite exponent 4 Galois extensions of K unramified outside S.

Results

Let $K = \mathbb{Q}$ and $S = \{2, 3, \infty\}$.

- $[\mathbb{Q}_{S,4} : \mathbb{Q}] = 2^{15}$.
- $\mathbb{Q}_{S,4}$ is the splitting field of $f_1 f_2 f_3$ with

$$
\begin{aligned}
f_1 &= x^8 + 4x^6 + 4x^4 - 2, \\
f_2 &= x^{16} - 4x^{14} + 4x^{12} + 4x^{10} - 4x^6 - 20x^4 + 4x^2 + 25, \\
f_3 &= x^{16} - 20x^{12} + 84x^8 + 96x^6 - 128x^4 - 96x^2 - 8.
\end{aligned}
$$

- For all of the 272 conjugacy classes C of

$$G_{S,4} = \mathrm{Gal}\left(\mathbb{Q}_{S,4}/\mathbb{Q}\right)$$

  computed the smallest prime p such that $\mathrm{Fr}_p \in C$.
  - The 5 largest such p are

$$862417, 926977, 1484737, 1501009, 2977153.$$

Maximal 2-extensions

- Let $\hat{K}_S$ be the maximal 2-extension of K unramified outside S.
- Galois cohomology provides a (partial) pro-2 presentation of

$$\hat{G}_S = \mathrm{Gal}\left(\hat{K}_S/K\right).$$

- Use Koch (2002) and Wingberg (1991):
  - $K = \mathbb{Q}$ and $S = \{2, 3, \infty\}$

    $$\hat{G}_S = \left\langle s_3, t_3, t_\infty : t_3^2\left[t_3^{-1}, s_3^{-1}\right], t_\infty^2 \right\rangle.$$

  - $K = \mathbb{Q}$ and $S = \{2, \infty\}$

    $$\hat{G}_S = \left\langle s_3, t_\infty : t_\infty^2 \right\rangle.$$

  - $K = \mathbb{Q}\left(\sqrt[3]{10}\right)$ and $S = \{\mathfrak{p}_2, \mathfrak{p}_{3a}, \mathfrak{p}_{3b}, \infty_{\mathbb{R}}\}$

    $$\hat{G}_S = \left\langle s_{\mathfrak{p}_{3a}}, t_{\mathfrak{p}_{3a}}, s_{\mathfrak{p}_{3b}}, t_{\mathfrak{p}_{3b}}, t_\infty : t_{\mathfrak{p}_{3a}}^2\left[t_{\mathfrak{p}_{3a}}^{-1}, s_{\mathfrak{p}_{3a}}^{-1}\right], t_{\mathfrak{p}_{3b}}^2\left[t_{\mathfrak{p}_{3b}}^{-1}, s_{\mathfrak{p}_{3b}}^{-1}\right], t_\infty^2 \right\rangle.$$

- $\left[\mathbb{Q}_{\{2,\infty\}} : \mathbb{Q}\right] = \infty.$

Exponent four quotients

K	S	$\lvert G_{S,4}\rvert$	2-class	conjugacy classes
$\mathbb{Q}$	$2, \infty$	2^6	4	13
$\mathbb{Q}$	$2, 3, \infty$	2^{15}	5	272
$\mathbb{Q}(\sqrt[3]{10})$	$\mathfrak{p}_2, \infty$	2^{37}	7	1 832 960
$\mathbb{Q}(\sqrt[3]{10})$	$\mathfrak{p}_2, \mathfrak{p}_{3a}, \mathfrak{p}_{3b}, \infty$	2^{234}	7	
$\mathbb{Q}$	$2, 3, 5, \infty$	$\leq 2^{73}$	≤ 5	

- Compute $G_{S,4}$ from $\hat{G}_S$ with the p-quotient algorithm in Magma.
- A naive way to obtain $\mathbb{Q}_{S,4}$ is as a tower of exponent 2 extensions.
- For $K = \mathbb{Q}$ and $S = \{2, 3, \infty\}$:

$$\mathbb{Q} \xrightarrow{8} \mathbb{Q}(\zeta_{24}) \xrightarrow{128} L \xrightarrow{32} \mathbb{Q}_{S,4}.$$

n	$\lvert B(n,4)\rvert$	2-class
1	2^2	2
2	2^{12}	5
3	2^{69}	7
4	2^{422}	10
5	2^{2728}	13

Transitive groups

Suppose that $\mathbb{Q}_{S,4}$ is the splitting field of a monic, irreducible $f \in [x]$ of degree d.

- The action of $G_{S,4}$ on the roots $\{\alpha_1, \ldots, \alpha_d\}$ of f is a transitive group.
- The isomorphism class of a transitive group has a label $d\mathrm{T}n$ with $n \in \mathbb{Z}_{>0}$.
- $\mathbb{Q}_{S,4} = \mathbb{Q}(\alpha_1)^{\mathrm{nc}}$.
- $\mathbb{Q}(\alpha_1)$ corresponds to a subgroup $H \subset G_{S,4}$ of index d with trivial $\mathrm{Core}\,(G_{S,4}, H)$.

Case $S = \{2, \infty\}$:

- $[G_{S,4} : H] = 8$ and transitive group with label 8T30.
- Tables of number fields by Jones and Roberts (2014):

$$x^8 + 4x^6 + 4x^4 - 2.$$

- The polynomial of degree 64 in Grenié (2007) defines the same field.

Case $S = \{2, 3, \infty\}$:

- $[G_{S,4} : H] = 128$.
- Using the normal lattice of $G_{S,4}$ and careful elimination:

$$\mathbb{Q}_{S,4} = \mathbb{Q}_{\{2,\infty\},4} \cdot {L_1}^{\mathrm{nc}} \cdot {L_2}^{\mathrm{nc}}$$

  - $[L_i, \mathbb{Q}] = 16$.
  - $\mathrm{Gal}\left({L_1}^{\mathrm{nc}}/\mathbb{Q}\right)$ has label 16T915 or 16T926.
  - $\mathrm{Gal}\left({L_2}^{\mathrm{nc}}/\mathbb{Q}\right)$ has label 16T1468.

Frobenius elements

Use Dokchitser and Dokchitser (2013) to compute for every conjugacy class $C \subset G_{S,4}$ a prime $p \geq 5$ such that $\mathrm{Fr}_p \in C$:

- Recall that $\mathbb{Q}_{S,4}$ is the splitting field of $f = f_1 f_2 f_3$ and consider $G_{S,4} \subset S_{\deg f}$.
- Choose $h = x^3 - 3x$.
- Define for every conjugacy class C of $G_{S,4}$

$$\Gamma_C = \prod_{\sigma \in C} \left(x - \sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i) \right) \in \mathbb{Z}[x].$$

- In this case the Γ_C are coprime. So

$$\sigma \in C \iff \Gamma_C \left(\sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i) \right) = 0.$$

- Factor f over $\mathbb{Q}_p$.
- Irreducible factors correspond to cycles of Fr_p.
- Compute roots of f in $K_p/\mathbb{Q}_p$ unramified of degree 4.
- Use Hensel Lemma to compute $\mathrm{Fr}_p(\alpha_i)$.
- Evaluate in the Γ_C's.

Outline

Theorem

Let A_1 and A_2 be abelian varieties of dimension two over $\mathbb{Q}$. If

- *A_1 and A_2 have good reduction at every prime $p \neq 2, 3$,*
- *the degree of $\mathbb{Q}(A_1[2], A_2[2])/\mathbb{Q}$ is a power of two, and*
- *for every prime p in 'a known finite list' the characteristic polynomials of Frobenius for A_1 and A_2 are equal,*

then A_1 and A_2 are isogeneous over $\mathbb{Q}$.

Theorem

The number of isogeny classes of two-dimensional abelian varieties A over $\mathbb{Q}$ with good reduction at every prime $p \neq 2, 3$ and the degree of $\mathbb{Q}(A[2])/\mathbb{Q}$ a power of two is at most $2.2 \cdot 10^{1783}$.

- There are no number fields of degree 3, 5, 7 and 9–15 unramified outside 2, see Jones (2010).

Theorem (Grenié)

Let A_1 and A_2 be abelian varieties of dimension two over $\mathbb{Q}$. If

- *A_1 and A_2 have good reduction at every prime $p \neq 2$, and*
- *for every prime p in $\{5, 7, 11, 17, 23, 31\}$ the characteristic polynomials of Frobenius for A_1 and A_2 are equal,*

then A_1 and A_2 are isogeneous over $\mathbb{Q}$.

Theorem

The number of isogeny classes of two-dimensional abelian varieties A over $\mathbb{Q}$ with good reduction at every prime $p \neq 2$ is at most $9.3 \cdot 10^{20}$.

Outline

Conclusions and outlook

Conclusions:

- Faltings method in general not practical.

Outlook:

- $\mathrm{Gal}\left(\hat{\mathbb{Q}}_S/\mathbb{Q}\right)$ for $S = \{2, p, \infty\}$ with $p \equiv \pm 3 \mod 8$ known.
- Global function field.
- If A_1, A_2 are abelian surfaces over $\mathbb{Q}$, then compute the maximal exponent 4 subfield of $\mathbb{Q}(A_1[2^\infty], A_2[2^\infty])$.
- Compute all genus 2 curves $C/\mathbb{Q}$ with a rational point and good reduction outside $S = \{2, 3, \infty\}$ and $\mathbb{Q}(\mathrm{Jac}\,(C)[2])$ a 2-extension.