Projects: Elliptic Curves

Sara Arias-de-Reyna

July 2018

1 First Project: Computing images of mod ℓ Galois representations attached to elliptic curves

In this project we consider elliptic curves E defined over the field of rational numbers, which we assume defined by an affine Weierstrass equation of the general shape

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

for some coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$.

Given a prime number ℓ, the action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group of ℓ-torsion points of E induces a Galois representation

$$\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Let $K = \mathbb{Q}(E[\ell])$ be the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the points of ℓ-torsion of E; in other words, K is the fixed field of $\overline{\mathbb{Q}}$ by $\ker \overline{\rho}_{E,\ell}$. The extension $K/\mathbb{Q}$ is finite and Galois, satisfying that $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{Gal}(K/\mathbb{Q})$. In this project, we want to compute this Galois group in some examples.

Our main tool will be to consider the Frobenius elements at primes different from ℓ. Given a prime $p \neq \ell$, which is unramified in the extension $K/\mathbb{Q}$, choose a prime $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K which lies above p, and set $D_{\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma\mathfrak{p} = \mathfrak{p}\}$. This is the *decomposition group at* p. Denoting by k_p the residue field $\mathcal{O}_K/\mathfrak{p}$, the reduction map

$$D_{\mathfrak{p}} \to \mathrm{Gal}(k_p/\mathbb{F}_p)$$

is an isomorphism. Let $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ be the element in $D_{\mathfrak{p}}$ projecting onto the map $x \mapsto x^p$ (the Frobenius element in $\mathrm{Gal}(k_p/\mathbb{F}_p)$). This element depends on the choice of $\mathfrak{p}|p$, but if we choose a different prime of $\mathcal{O}_K$ above p, we obtain an element conjugate to $\mathrm{Frob}_{\mathfrak{p}}$. Thus, abusing notation, we will denote it by Frob_p. The next proposition (cf. [Ser72, §4]) tells us what is the characteristic polynomial of the image of Frob_p by $\overline{\rho}_{E,\ell}$ (which is well-defined, since it is invariant by conjugation).

We will see in the morning lectures that those primes p such that the elliptic curve has good reduction mod p are unramified in the extension $K/\mathbb{Q}$ (this follows from the so-called Néron-Ogg-Shafarevich criterion).

Proposition 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve, ℓ a prime number, $\overline{\rho}_{E,\ell}$ the Galois representation attached to the ℓ-torsion points of E, and $p \neq \ell$ a prime number such that E has good reduction at p. Then*

$$\begin{cases} \operatorname{trace}(\overline{\rho}_{E,\ell}(\operatorname{Frob}_p)) = 1 + p - \operatorname{card}(\widetilde{E}_p(\mathbb{F}_p)) \mod \ell \\ \det(\overline{\rho}_{E,\ell}(\operatorname{Frob}_p)) = p \mod \ell \end{cases}$$

where $\widetilde{E}_p$ denotes the reduction of E at p.

The above proposition provides us with the characteristic polynomials of many elements in $\operatorname{Im}\overline{\rho}_{E,\ell}$. In fact, Chebotarev's Density Theorem tells us that, if we computed $\overline{\rho}_{E,\ell}(\operatorname{Frob}_p)$ for *all* primes p of good reduction for E (with possibly finitely many exceptions), we would obtain elements belonging to each conjugacy class of $\operatorname{Im}\overline{\rho}_{E,\ell}$.

Theorem 1.2 (Chebotarev)**.** *Let L/K be a finite Galois extension of number fields, let $X \subset \operatorname{Gal}(L/K)$ be a subset that is fixed by conjugation. Then the set S of primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\operatorname{Frob}_\mathfrak{p} \in X$ has a density, equal to*

$$\operatorname{card} X / \operatorname{card}(\operatorname{Gal}(L/K)).$$

For more details regarding density of sets of primes in number fields, as well as references for a proof, see [Ser98, Chapter 1].

Remark 1.3. *In particular, it follows from Theorem 1.2 that $\det \overline{\rho}_{E,\ell} : \operatorname{Gal}(K/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ coincides with the mod ℓ cyclotomic character, which is surjective.*

Our aim is to determine $\operatorname{Gal}(K/\mathbb{Q})$ by computing the image of enough Frobenius elements. We know that $\operatorname{Gal}(K/\mathbb{Q}) \simeq \operatorname{Im}\overline{\rho}_{E,\ell}$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, such that the restriction of the determinant to this subgroup is surjective. A result of Serre (cf. [Ser72, Proposition 19]) shows that, when $\ell \geq 5$, the information provided by the characteristic polynomial of the image of Frob_p *for all* p is enough to determine if $\operatorname{Gal}(K/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$ or not.

Proposition 1.4. *Let $\ell \geq 5$ be a prime, $H \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be a subgroup such that:*

1. *There exists $s_1 \in H$ with $\operatorname{trace}(s_1)^2 - 4\det(s_1)$ a nonzero square in $\mathbb{F}_\ell$ and $\operatorname{trace}(s_1) \neq 0$.*
2. *There exists $s_2 \in H$ with $\operatorname{trace}(s_2)^2 - 4\det(s_2)$ a non-square in $\mathbb{F}_\ell$ and $\operatorname{trace}(s_2) \neq 0$.*
3. *There exists $s_3 \in H$ with $u = \operatorname{trace}(s_3)^2/\det(s_3)$ satisfying: $u \neq 0, 1, 2, 4$ and $u^2 - 3u + 1 \neq 0$.*

Then H contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. If $\det|_H$ is surjective, then $H = \mathrm{GL}_2(\mathbb{F}_\ell)$.

In particular, if $\ell \geq 5$, it suffices to show that, for any pair $(a, b) \in \mathbb{F}_\ell \times \mathbb{F}_\ell^\times$, there exists $s \in H$ such that $\operatorname{charpoly}(s) = T^2 + aT + b$.

Note that, while Proposition 1.4 allows you to prove that $\operatorname{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, it does not allow you to prove anything if the image is smaller. Using explicit versions of Chebotarev's Density Theorem, one can determine a bound, depending on E, such that, if some polynomial $T^2 + aT + b$ does not

appear as the characteristic polynomial of Frob_p for some prime p strictly smaller than this bound, then it will not appear as the characteristic polynomial of the Frobenius element for any p. As a consequence, a finite computation will provide a proof that the image is *not* surjective. For more details, see [Sut16].

If $\ell = 2$ or 3, the situation is more complicated, since only the characteristic polynomials of Frobenius elements are not enough to determine if $\mathrm{Im}\overline{\rho}_{E,\ell}$ is the whole group $\mathrm{GL}_2(\mathbb{F}_\ell)$. Luckily, in these cases the equations that define the ℓ-torsion points of E are still simple enough to be manipulated.

For $\ell = 2$, we have that $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, and it has only three proper subgroups up to conjugation, namely

$$H_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, H_2 \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}, H_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

The coordinates of the points of order exactly 2 of $E(\overline{\mathbb{Q}})$ are the roots of the polynomial

$$P(x) = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Using the group of points of 2-torsion which are defined over $\mathbb{Q}$ and the discriminant of E, we can determine $\mathrm{Im}\overline{\rho}_{E,\ell}$ completely, as shown in the next proposition (cf. [RV01, Proposition 2.1]).

Proposition 1.5. *Let $E(\mathbb{Q})[2]$ the group of 2-torsion points defined over $\mathbb{Q}$, and let Δ_E be the discriminant of E. Then it holds:*

$$\mathrm{Im}\overline{\rho}_{E,\ell} = \begin{cases} H_1 \text{ if } E(\mathbb{Q})[2] \neq \{O\} \text{ and } \Delta_E \in \mathbb{Q}^2 \\ H_2 \text{ if } E(\mathbb{Q})[2] \neq \{O\} \text{ and } \Delta_E \notin \mathbb{Q}^2 \\ H_3 \text{ if } E(\mathbb{Q})[2] = \{O\} \text{ and } \Delta_E \in \mathbb{Q}^2 \\ \mathrm{GL}_2(\mathbb{F}_\ell) \text{ if } E(\mathbb{Q})[2] = \{O\} \text{ and } \Delta_E \notin \mathbb{Q}^2 \end{cases}$$

For $\ell = 3$, recall that the 3-division polynomial

$$\psi_3(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$$

satisfies that its roots are precisely the x-coordinates of the 3-torsion points of E (cf. [Sil92, Exercise 3.7, Chapter III]). We can complete this information with the discriminant of E to obtain a surjectivity criterion (cf. [RV01, Theorem 2.3]).

Proposition 1.6. *Let $E/\mathbb{Q}$ be an elliptic curve. The following conditions are equivalent:*

- *ψ_3 does not have any rational roots and $\Delta_E \notin \mathbb{Q}^3$;*
- $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_3)$.

Exercise 1.1. *For the following elliptic curves, check whether the image of $\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, for the primes $\ell = 2, 3, 5, 7, 11$:*

1. $E_1 : y^2 + y = x^3 - x^2$
2. $E_2 : y^2 + xy + y = x^3 - x$
3. $E_3 : y^2 + y = x^3 - x$

Exercise 1.2. *Consider the elliptic curve E defined over $\mathbb{Q}$ by the Weierstrass equation $E : y^2 + xy = x^3 - x^2 - 107x + 552$. Can you find a single prime ℓ such that $\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$?*

The previous exercise shows an example of an elliptic curve $E/\mathbb{Q}$ with *complex multiplication*, that is to say, such that the ring of endomorphisms $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is strictly bigger than $\mathbb{Z}$. There are only 13 j-invariants in $\mathbb{Q}$ corresponding to elliptic curves with complex multiplication.

Assume $E/\mathbb{Q}$ has complex multiplication; then $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is an order in an imaginary quadratic field (cf. [Sil92, Cor. 9.4, Chap. III]), say K. Then any $\phi \in \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is in fact defined over K (cf. [Sil94, Theorem 2.2.b, Chap. II]). Thus, if we take any $\phi \in \mathrm{End}_{\overline{\mathbb{Q}}}(E)$, and consider its restriction to $E[\ell]$, we obtain a morphism of $\mathbb{F}_\ell$-vector spaces that commutes with the image of any $\sigma \in G_K$ by the representation $\overline{\rho}_{E,\ell}$. In particular, we conclude that $\overline{\rho}_{E,\ell}(G_K)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose commutator is strictly greater than $\mathbb{Z}$. It can be shown that such a subgroup is abelian (cf. [Sil94, Ex 2.6, Chap. II]). Therefore, $\mathrm{Im}\overline{\rho}_{E,\ell}$ is either an abelian group or has an abelian group of index 2; in both cases, it is strictly smaller than $\mathrm{GL}_2(\mathbb{F}_\ell)$ if $\ell > 2$.

For the computational part of this project, we will rely on the data collected in the **database of L-functions, modular forms and related objetcts (LMFDB)**, which can be found at

`http://www.lmfdb.org/`

Here you can find lists of elliptic curves, together with many data related to them, including the images of $\overline{\rho}_{E,\ell}$ in many cases. You can check whether your computations in Exercise 1.1 were correct.

The elliptic curves are usually ordered according to their *conductor*. This is an integer number which contains information about the *reduction* of the elliptic curve at different primes, via the action of the inertia group at all rational primes on the ℓ-adic Tate module. We will tackle it in the morning lectures; for the moment, it suffices to know that the conductor of an elliptic curve $E/\mathbb{Q}$ is a number, whose prime factors are those primes where E has bad reduction.

Each curve is uniquely determined by a label. The label consists of two parts: a number, which equals the conductor or the elliptic curve, a letter, which identifies the isogeny class, and a number, which distinguishes the curves inside each isogeny class. For example, the labels of the elliptic curves in the exercise above are (11.a3), (14.a5) and (37.a1).

Remark 1.7. *To compute the characteristic polynomial of $\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$, you needed to compute the number of points of the reduction $\widetilde{E}_p$ for many primes p. In fact, this information is also contained in*

the LMFDB. For each elliptic curve, there appears a modular form in the database. For example, for the curve E_3 above the modular form is

$$f(q) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} \\ - 5q^{11} - 6q^{12} - 2q^{13} + 2q^{14} + 6q^{15} - 4q^{16} - 12q^{18} + O(q^{20})$$

For each prime $p \neq \ell$ of good reduction of E (that is, not dividing the conductor of E), the coefficient a_p of q^p coincides with $p + 1 - \mathrm{card}(\widetilde{E}_p(\mathbb{F}_p))$. The existence of a modular form which encodes information about the number of points of the reduction of E modulo p is precisely the statement of the Shimura-Taniyama conjecture. You can check this fact in the examples you computed.

Serre conjectured that the largest prime ℓ such that there exists some elliptic curve $E/\mathbb{Q}$, without complex multiplication, with $\mathrm{Im}\overline{\rho}_{E,\ell} \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ is $\ell = 37$. D. Zywina refines this conjecture as follows (cf. [Zyw15a, Conjecture 1.12]):

Conjecture 1.8. *If E is an elliptic curve over $\mathbb{Q}$, without complex multiplication, and $\ell \geq 17$ is a prime such that the pair $(\ell, j_E) \notin \{(17, -17\cdot 373^3/2^{17}), (17, -17^2\cdot 101^3/2), (37, -7\cdot 11^3), (37, -7\cdot 137^3\cdot 2083^3)\}$. Then $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$.*

Zywina has verified this conjecture for all elliptic curves $E/\mathbb{Q}$ with conductor at most 360000 (cf. [Zyw15b]).

2 Second Project: Elliptic curves with isomorphic ℓ-torsion modules

In this project, we fix an elliptic curve $E/\mathbb{Q}$, and a prime ℓ such that $\overline{\rho}_{E,\ell}$ is surjective onto $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let $K = \mathbb{Q}(E[\ell])$. Then we know that $K/\mathbb{Q}$ is a finite Galois extension with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$. We ask the following question:

Question 1: Is there some other elliptic curve $E'/\mathbb{Q}$ such that the field $K' = \mathbb{Q}(E'[\ell])$ coincides with K?

Actually, we can also consider a more restrictive question, namely:

Question 2: Is there some other elliptic curve $E'/\mathbb{Q}$ such that the representations $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic?

It is clear that if $E'/\mathbb{Q}$ is an elliptic curve such that $\overline{\rho}_{E',\ell}$ is isomorphic to $\overline{\rho}_{E,\ell}$ (meaning that the $G_\mathbb{Q}$-modules $E[\ell]$ and $E'[\ell]$ are isomorphic), then $K = K'$. However, it is not immediate to determine whether the other implication holds (can you say something about it?)

Note that, if we have an isogeny $\varphi : E \to E'$ defined over $\mathbb{Q}$, then φ induces an isomorphism of $G_\mathbb{Q}$-modules between $E[\ell]$ and $E'[\ell]$. Thus, isogenous elliptic curves provide us with a trivial answer to Question 2. In the rest of the project, we will look for *non-isogenous* elliptic curves providing a positive answer to the questions.

To address the second question, we need to recall some facts from the representation theory of groups. First of all, we state the following classical result (cf. [CR62, (30.16)]).

Theorem 2.1 (Brauer-Nesbitt)**.** *Let ℓ be a prime and V a finite dimensional $\mathbb{F}_\ell$-vector space. Let $\overline{\rho}, \overline{\rho}' : G \to \mathrm{GL}_n(V)$ be two irreducible representations. Then $\overline{\rho}$ and $\overline{\rho}'$ are isomorphic if and only if for all $g \in G$, the characteristic polynomials of $\rho(g)$ and $\rho'(g)$ coincide.*

Combining this result with Chebotarev's Density Theorem, we obtain the following result:

Proposition 2.2. *Let $E/\mathbb{Q}$, $E'/\mathbb{Q}$ be two elliptic curves. Assume that, for all primes p of good reduction for E and E', we have the equality*

$$\mathrm{charpoly}(\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)) = \mathrm{charpoly}(\overline{\rho}_{E',\ell}(\mathrm{Frob}_p)). \tag{2.2}$$

Then $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic.

Note that, since $\det \overline{\rho}_{E,\ell}(\mathrm{Frob_p}) = p = \det \overline{\rho}_{E',\ell}(\mathrm{Frob}_p)$, condition (2.2) is equivalent to $a_p \equiv a'_p \mod \ell$, where $a_p = p + 1 - \mathrm{card}(\widetilde{E}_p(\mathbb{F}_\ell))$ and $a'_p = p + 1 - \mathrm{card}(\widetilde{E'}_p(\mathbb{F}_\ell))$.

However, in finite time we can only check finitely many of the congruences above. Luckily for us, if the first few congruences hold, then one can prove that all congruences will hold as well. This result makes use of the theory of modular forms and the proof of the Shimura-Taniyama conjecture. The bound C up to which one needs to check the congruences depends on the conductors N and N' of E and E' respectively. This invariant carries information about the reduction of the elliptic curve at each prime p. For example, the exponent of p in N is 1 if and only if the reduction of E at p is multiplicative.

The next proposition is taken from [KO92, Proposition 4]:

Proposition 2.3. *Let E, E' be two elliptic curves defined over $\mathbb{Q}$, with conductors N and N' respectively. Let S be the set of prime numbers where E has split multiplicative reduction and E' has non-split multiplicative reduction. Define the quantities:*

$$M = \mathrm{lcm}(N, N') \prod_{p \in S} p$$

$$\mu(M) = M \prod_{\substack{p|M \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$$

Then the following conditions are equivalent:

1. *$\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic.*
2. *For all $p < \mu(M)/6$ not dividing NN', we have $a_p \equiv a'_p \pmod{\ell}$, and for all $p < \mu(M)/6$ with $p|NN'$ but $p^2 \nmid NN'$, we have $a_p a'_p \equiv p + 1 \pmod{\ell}$.*

Before starting to compare representations coming from different elliptic curves, some further considerations about the conductor are in order. The conductor N of an elliptic curve $E/\mathbb{Q}$ is a number defined in terms of the ramification of the *ℓ-adic* representations $\rho_{E,\ell} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$. If

$E'/\mathbb{Q}$ is another elliptic curve, a necessary condition for $\rho_{E,\ell}$ and $\rho_{E',\ell}$ to be isomorphic is that, for all primes $p \neq \ell$, the exponent of p in N coincides with the exponent of p in N'.

Since $\overline{\rho}_{E,\ell}$ is the mod ℓ reduction of $\rho_{E,\ell}$, it turns out that $\overline{\rho}_{E,\ell}$ can only be ramified at p if $\rho_{E,\ell}$ is ramified at p. However, in the process of reducing mod ℓ, some ramification can be lost. Thus, in order for $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic is no longer necessary that the conductors of E and E' coincide (away from the prime ℓ). But, the loss of ramification is a relatively rare phenomenon, so we can expect that the conductors of E and E' should not be too different.

Exercise 2.1. *Compare the mod ℓ representations attached to the following pair of elliptic curves (this example is taken from [KO92]):*

$$\ell = 7, \begin{cases} (26.a2) & E : y^2 + xy + y = x^3 - 5x - 8 \\ (182.a1) & E' : y^2 + xy + `y = x^3 - 4609x + 120244 \end{cases}$$

Exercise 2.2. *Can you find an example of a prime ℓ and a couple of non-isogenous elliptic curves $E, E'/\mathbb{Q}$, with the same conductor, such that $\overline{\rho}_{E,\ell} \simeq \overline{\rho}_{E',\ell}$?*

Exercise 2.3. *Does it always happen that, whenever $\overline{\rho}_{E,\ell} \simeq \overline{\rho}_{E',\ell}$, then E and E' have either the same conductor, or the same conductor outside of ℓ? Check the following example (this example is taken from [FK17]).*

$$\ell = 7, \begin{cases} (52.a1) & E : y^2 = x^3 - 4x - 3 \\ (988.c1) & E' : y^2 = x^3 - 362249x + 165197113 \end{cases}$$

What do you observe? Can you make a conjecture about a necessary condition on the conductors of E and E' in order for $\overline{\rho}_{E,\ell} \simeq \overline{\rho}_{E',\ell}$ to be isomorphic?

Exercise 2.4. *Compare the mod ℓ representations attached to the following pair of elliptic curves (this example is taken from [KO92]):*

$$\ell = 3, \begin{cases} (11.a3) & E : y^2 + y = x^3 - x^2; \\ (121.c2) & E' : y^2 + xy = x^3 + x^2 - 2x - 7; \end{cases}$$

3 Third Project: $\mathrm{GL}_2(\mathbb{F}_\ell)$-extensions of $\mathbb{Q}$ coming from the mod ℓ-torsion of elliptic curves

Fix a prime ℓ, and consider a fixed Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$. In the second project, we considered the question of determining if there can be two "essentially different" elliptic curves such that $K = \mathbb{Q}(E[\ell]) = \mathbb{Q}(E'[\ell])$. In this project, we address the question of the existence of *at least* one elliptic curve with $K \simeq \mathbb{Q}(E[\ell])$, once we have fixed K.

Exercise 3.1. *Knowing that $\det \overline{\rho}_{E,\ell} = \chi_\ell$, can you give a necessary condition for a number field K to satisfy $K = \mathbb{Q}(E[\ell])$?*

Given a Galois extension $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$, its discriminant Δ_K gives us information about the primes that ramify in $K/\mathbb{Q}$. We give here a precise formulation (cf. Theorem 3.12.11 of [Koc00])

Theorem 3.1 (Dedekind's Discriminant Theorem)**.** *Let $K/\mathbb{Q}$ be a finite extension, Δ_K its discriminant and p a prime number. Suppose that*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_g^{e_g}$$

is the decomposition of the ideal $p\mathcal{O}_K$ into prime ideals of $\mathcal{O}_K$, and let f_i be the inertia degree $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$.

Then the exponent of p in Δ_K satisfies

$$v_p(\Delta_K) \geq (e_1 - 1)f_1 + \cdots + (e_g - 1)f_g,$$

with equality if and only if $p \nmid e_i$ for all $i = 1, \ldots g$.

In our case, $K/\mathbb{Q}$ is a Galois extension, hence denoting by e the ramification index at p, f the inertia degree at p, and g the number of primes of $\mathcal{O}_K$ above p, we have $v_p(\Delta_K) \geq (e-1)fg$, with equality if and only if p is tamely ramified in $K/\mathbb{Q}$.

Can you find a necessary condition for a number field K to be equal to $\mathbb{Q}(E[\ell])$, in terms of the discriminant Δ_K and the conductor of E?

In the database of L-functions, modular forms, and related objects (LMFDB), we can find lists of polynomials whose decomposition fields have prescribed Galois groups.

Exercise 3.2. *For $\ell = 2$, go through the list of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ (label 6T2), and try to find elliptic curves $E/\mathbb{Q}$ satisfying that $K = \mathbb{Q}(E[\ell])$. Can you find some number field $K/\mathbb{Q}$ which (conjecturally) does not correspond to any elliptic curve?*

Exercise 3.3. *Prove that, for any Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, there exists an elliptic curve $E/\mathbb{Q}$ such that $\mathbb{Q}(E[2]) \simeq K$ (Hint: Look at the equations that give the coordinates of the 2-torsion points of an elliptic curve).*

For $\ell \geq 3$, the situation is more complicated because the degree $[K : \mathbb{Q}]$ is too big to make explicit computations! In the LMFDB you can find polynomials $P(X) \in \mathbb{Q}[X]$ of degree 8 whose splitting field K is $\mathrm{GL}_2(\mathbb{F}_3)$. However, you only have information about the number field $F := \mathbb{Q}[X]/(F(X))$. If we have a tower of fields $\mathbb{Q} \subset F \subset K$, we have the following relationship between the discriminants Δ_K, Δ_F and $\delta_{K/F}$ (which is an ideal of $\mathcal{O}_F$):

$$\Delta_K = \mathrm{Norm}_{F/\mathbb{Q}}(\delta_{K/F})\Delta_F^{[K:F]}$$

Exercise 3.4. *Fix $\ell = 3$. The LMFDB includes a list of polynomials $P(X)$ of degree 8 whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$ (label 8T23). Go through the list of elliptic curves $E/\mathbb{Q}$, ordered by conductor, and take those with $\mathrm{Im}\rho_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_3)$. For each such curve, there exists a degree-8*

polynomial $P(x) \in \mathbb{Q}[X]$ whose splitting field coincides with $\mathbb{Q}(E[\ell])$ (prove it!). Try to match up the polynomials $P(x)$ and the elliptic curves $E/\mathbb{Q}$. Is there some polynomial which (conjecturally) does not correspond to any elliptic curve?

In fact, it can be proven that, if $\ell = 3, 5$, given a Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, there exist (infinitely many) elliptic curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[\ell]) = K$, cf. [Rub97, Theorem 3]. The situation changes drastically when we consider primes $\ell \geq 7$: There exist Galois extensions $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$ which do not come from elliptic curves defined over $\mathbb{Q}$, that is, there is no elliptic curve $E/\mathbb{Q}$ such that $\mathbb{Q}(E[\ell]) = K$. You can find a proof in [Cal06, §3]. The different behaviour for small values of ℓ and large values of ℓ is due to the fact that the modular curves $X(\ell)$, $\ell = 2, 3, 5$, have genus 0, whereas $X(\ell)$ has genus $g \geq 1$ for all primes $\ell \geq 7$.

References

[Cal06] Frank Calegari. Mod p representations on elliptic curves. *Pacific J. Math.*, 225(1):1–11, 2006.

[CR62] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[FK17] N. Freitas and A. Kraus. On the symplectic type of isomorphims of the p-torsion of elliptic curves. *arXiv:1607.01218*, pages 1–75, 2017.

[KO92] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[Koc00] Helmut Koch. *Number theory*, volume 24 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2000. Algebraic numbers and functions, Translated from the 1997 German original by David Kramer.

[Rub97] Karl Rubin. Modularity of mod 5 representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 463–474. Springer, New York, 1997.

[RV01] Amadeu Reverter and Núria Vila. Images of mod p Galois representations associated to elliptic curves. *Canad. Math. Bull.*, 44(3):313–322, 2001.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sil92] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016.

[Zyw15a] David J. Zywina. On the possible images of the mod ℓ representations assoicated to elliptic curves over $\mathbb{Q}$. *arXiv:1508.07660*, 2015.

[Zyw15b] David J. Zywina. On the surjectivity of mod ell representations associated to elliptic curves. *arXiv:1508.07661*, 2015.