GALOIS REPRESENTATIONS AND STATISTICS

COURSE: SAMUELE ANNI AND RENÉ SCHOOF
NOTES: ROSS PATERSON

Lecture 1 (Schoof)

1. Elliptic Curves

Let E/F be an elliptic curve over a number field. We take the notation:

- $E(\overline{F})$ is the group of points over the algebraic closure;
- for a prime $\ell \in \mathbb{Z}_{\geq 1}$ write $E[\ell]$ for the ℓ-torsion points in $E(\overline{F})$, which is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ as an abelian group;
- $F_\ell := F(E[\ell])$;
- Note that $\mathrm{Gal}(\overline{F}/F)$ acts on $E[\ell]$, and so we obtain a map

$$\mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

We denote by $G_\ell \cong \mathrm{Gal}(F_\ell/F)$ the image of Galois under this map.

Example 1. $E : y^2 + y = x^3 + x$ over $F = \mathbb{Q}$. We begin by looking at division polynomials $f_\ell(x) \in \mathbb{Z}[x]$ using the recursive `elldivpol` algorithm in PARI. By definition, $f_\ell(x) = 0$ if and only if x is the x-coordinate of a nonzero ℓ-division point. For ℓ an odd prime we have $\deg(f_\ell) = \frac{\ell^2-1}{2}$. Now for some explicit examples.

- For $\ell = 2$: `elldivpol` gives us $f_2(x) = 4x^3 - 4x + 1$, and then using `Galoisgroup` we see that this polynomial has Galois group isomorphic to $S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$. Thus $G_2 = \mathrm{GL}_2(\mathbb{F}_2)$.
- For $\ell = 3$: `elldivpol` gives us that $f_3(x) = 3x^4 - 6x^2 + 3x - 1$, and then using `Galoisgroup` we get that this polynomial has Galois group S_4. For 3-torsion points the x coordinates correspond to the lines in $E[3]$, so points in $\mathbb{P}_1(\mathbb{F}_3)$. Thus $\mathrm{Gal}(f)$ can be viewed as a subgroup of $\mathrm{PGL}_2(\mathbb{F}_3)$, and since it is $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$ we see that it is acting as the full $\mathrm{PGL}_2(\mathbb{F}_3)$ on this space. In particular, using Exercise 2 below, $G_3 = \mathrm{GL}_2(\mathbb{F}_3)$.

Exercise 2. Show that if $H \leq \mathrm{GL}_2(\mathbb{F}_3)$ surjects onto $\mathrm{PGL}_2(\mathbb{F}_3)$ (under the natural projection $\mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{PGL}_2(\mathbb{F}_3)$) then $H = \mathrm{GL}_2(\mathbb{F}_3)$

Example 3. $E' : y^2 = x^3 + x^2 - 2x - 1$, let ζ_7 be a fixed primitive 7th root of unity.

- For $\ell = 2$: The zeroes of the cubic are Galois conjugates of $\zeta_7 + \zeta_7^{-1}$. Thus the points in $E[2]$ generate the totally real subfield of $\mathbb{Q}(\zeta_7)$, which is a cyclic cubic extension of $\mathbb{Q}$, and so $G_2 \cong C_3 \subseteq \mathrm{GL}_2(\mathbb{F}_2)$.

- For $\ell = 3$: the 3-division polynomial is $(x-2)(3x^3+10x^2+8x+4)$. The cubic is an S_3-cubic whose splitting field has quadratic subfield $\mathbb{Q}(\sqrt{-3})$. The linear factor corresponds to the points $(2, \pm\sqrt{7})$. Note that this is sufficient to show that the order of the Galois image is at least $6 \times 2 = 12$. Moreover, if $P = (2, \sqrt{7})$ then $\langle P \rangle \leq E[3]$ is a Galois stable subgroup. Thus the image of Galois is contained in the group of matrices of the form

$$\begin{pmatrix} \psi & * \\ 0 & \omega \end{pmatrix}.$$

Where ψ is the sign character on $\mathrm{Gal}(\mathbb{Q}(\sqrt{7})/\mathbb{Q})$, and ω is some character of $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ (since the determinant is a character). There are at most 12 possible matrices of this form, and so this whole group must be the image of Galois.

It will be important to look at the ring of endomorphisms of E over F. In fact $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$ or $\mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field.

Case: Defined CM. Assuming that $\mathrm{End}_F(E) \cong \mathcal{O}$ for $\mathcal{O}$ an order in an imaginary quadratic field. Then

$$\mathcal{O} = \mathrm{End}(E) \to \mathrm{End}_{\mathrm{ab}}(E[\ell]).$$

The kernel of this map is $\ell\mathrm{End}(E)$. Indeed: if $f|_{E[\ell]} = 0$ then $\ker([\ell]) \subseteq \ker(f)$, meaning that

$$f = g \circ [\ell] = [\ell] \circ g \in \ell\mathrm{End}(E).$$

Thus we have an injection

$$\mathcal{O}_\ell\mathcal{O} \to \{2 \times 2\text{-matrices over } \mathbb{F}_\ell\} =: M_{2\times 2}(\mathbb{F}_\ell).$$

The condition that every element of $\mathcal{O}$ is defined over F gives us that the image of $\mathcal{O}/\ell\mathcal{O}$ in $M_{2\times 2}(\mathbb{F}_\ell)$ must commute with the image of G_ℓ. That is to say, G_ℓ must be contained in the centraliser of $(\mathcal{O}/\ell\mathcal{O})^\times \subseteq M_{2\times 2}(\mathbb{F}_\ell)$.

Exercise 4. Show that $(\mathcal{O}/\ell\mathcal{O})^\times$ is its own centralizer, and so $G_\ell \subseteq (\mathcal{O}/\ell\mathcal{O})^\times$.

Based on the splitting type of ℓ in $\mathcal{O}$ we see:

- if ℓ is split then $\mathcal{O}_\ell/\mathcal{O}_\ell^\times = \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ (split Cartan)
- if ℓ is inert then $\mathcal{O}_\ell/\mathcal{O}_\ell^\times = \mathbb{F}_{\ell^2}^\times$ (nonsplit Cartan)
- if ℓ is split then $\mathcal{O}_\ell/\mathcal{O}_\ell^\times = \mathbb{F}_\ell[\varepsilon]$

Case: Undefined CM. Assuming that $\mathrm{End}_F(E) \subsetneq \mathrm{End}(E) \cong \mathcal{O}$ for $\mathcal{O}$ an order in an imaginary quadratic field. Then we have a surjection

$$\mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(\mathcal{O}) = \{\mathrm{Id}, c\}$$

Thus the endomorphisms are defined over a degree 2 extension F'/F. Moreover $G_\ell \subset$normaliser of $\mathcal{O}/\ell\mathcal{O}^\times$. The size of the Galois image can be

$$\begin{cases} 2(\ell-1)^2 & \text{if normaliser of split cartan} \\ 2(\ell^2-1) & \text{if normaliser of non split cartan} \\ (\ell-1)^2\ell & \text{if Borel} = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \end{cases}$$

Non-CM. In the case of non-CM elliptic curves, we have the following theorem of Serre.

Theorem 5 (Serre 1972)**.** *Let E/F be an elliptic curve over a number field without CM (i.e.* $\mathrm{End}(E) \cong \mathbb{Z}$*). Then there is a constant C, depending on E, such that for all $\ell > C$ the image of*

$$\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

is surjective

Conjecture 6 (Serre)**.** *The constant above can be chosen uniformly in E.*

Weil Pairing. An important concept related to the Galois image is the Weil pairing.

Definition 7. There is a non-degenerate alternating bilinear pairing called the Weil pairing

$$e_\ell : E[\ell] \times E[\ell] \to \mu_\ell,$$

which is defined over F (meaning it is $\mathrm{Gal}(\overline{F}/F)$-equivariant).

Since the pairing is non-degenerate, note that if P, Q is a basis of $E[\ell]$ then $e_\ell(P, Q) = \zeta_\ell$ for a primitive ℓth root of unity ζ_ℓ. In particular since the left hand side is invariant under $\mathrm{Gal}(\overline{F}/F_\ell)$ we must have $F(\zeta_\ell) \subseteq F_\ell$.

Exercise 8. Use the Galois equivariance of the Weil pairing to check that the diagram below commutes:

$$\begin{array}{ccc} G_\ell = \mathrm{Gal}(F_\ell/F) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell) \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \det} \\ \mathrm{Gal}(F(\zeta_\ell)/F) & \longrightarrow & \mathbb{F}_\ell^\times. \end{array}$$

In particular, if $F(\zeta_\ell)/F$ has degree $\ell - 1$ then this means that the determinant map must be surjective and so our Galois image must not be too small! Moreover, this assumption on the degree always holds for all but finitely many ℓ since F is a number field.

Proposition 9. *If $H \leq \mathrm{GL}_2(\mathbb{F}_\ell)$ is a proper subgroup, and $\det(H) = \mathbb{F}_\ell^\times$, then one of the following is true*

- *$H \subseteq$normaliser of Cartan (split or nonsplit)*
- *$H \subseteq$Borel*
- *The image of H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is an exceptional subgroup A_4, S_4, A_5 in $\mathrm{PGL}_2(\mathbb{F}_\ell)$*

Proof. If $\ell \mid \#H$ then H contains an element σ of order ℓ. In particular, there is an element $\sigma \in H$ such that $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If there is a $\tau \in H$ which fixes another point in $\mathbb{F}_\ell \times \mathbb{F}_\ell$ then we can show that it can be moved around to get that $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is in H. It is an exercise to show that these two matrices generate $\mathrm{SL}_2(\mathbb{F}_\ell)$. Thus $H \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$, and since the determinant map is assumed to be surjective then $H = \mathrm{GL}_2(\mathbb{F}_\ell)$. If τ does not exist then we leave it as an exercise to show.

If $\ell \nmid \#H$ then all $\sigma \in H$ are diagonalisable, and writing $\overline{\sigma}$ =image of $\sigma \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ we see that every $\overline{\sigma}$ in the image of H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ must have two fixed

points in $\mathbb{P}^1(\mathbb{F}_\ell)$. It is then an exercise to copy the proof over $\mathbb{C}$ that shows we are in one of the cases above. □

1.1. **Finding Elements.** Finding elements in $G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ might be hard, but finding characteristic polynomials (of Frobenius elements $\mathrm{Frob}_\mathfrak{p}$) is not so hard. It is standard theory that F_ℓ/F is unramified outside of the set of bad primes of E and ℓ, so we consider these unramified $\mathfrak{p}$. We denote

$$\mathrm{Gal}(F_\ell/F) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$
$$\mathrm{Frob}_\mathfrak{p} \mapsto A_\mathfrak{p}.$$

Then the characteristic polynomial of $A_\mathfrak{p}$ is $X^2 - a_p X + p \in \mathbb{F}_\ell[X]$ where $p + 1 - a_p = \#E(k_\mathfrak{p})$.

Example 10. $E : y^2 + y = x^3 - x$, $F = \mathbb{Q}$, $p = 3$. Then $\#E(\mathbb{F}_3) = 7$ so $a_3 = 3$ and the characteristic polynomial is $x^2 - 3x + 3$.

For $\ell = 2$: $G_2 \subseteq \mathrm{GL}_2(\mathbb{F}_2)$ has $\mathrm{Frob}_3 \mapsto A_3$ with characteristic polynomial $x^2 + x + 1$ so has order 3.

For $p = 5$, $\ell = 2$: Characteristic polynomial is $X^2 + 1$ and so the Frobenius at 5 is order 2.

If $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$ then all possible characteristic polynomials are those of some $A \in G_\ell$. The converse is true if $\ell \neq 3$.

Theorem 11 (Serre's Criterion)**.** *($\ell \geq 5$). Let E/F be an elliptic curve over a number field and $H = G_\ell$ be the image of Galois in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Assume that all of the following hold:*

- *$\exists \sigma \in H$ with characteristic polynomial $X^2 - tX + p$ for which the discriminant is a nonzero square and $t \neq 0$;*
- *$\exists \sigma \in H$ with characteristic polynomial $X^2 - tX + p$ for which the discriminant is a nonsquare and $t \neq 0$;*
- *$\exists \sigma \in H$ with characteristic polynomial $X^2 - tX + p$ for which $t^2/\det(\sigma) \neq 0, 1, 2, 4, \frac{3 \pm \sqrt{5}}{2}$.*

Then $H = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Lecture 2 (Schoof)

An alternative formulation of Serre's open image theorem from last time is the following.

Theorem 12 (Serre)**.** *Let E/F be an elliptic curve over a number field. If $G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ is a proper subgroup for infinitely many ℓ then E must have CM.*

Some observations:

- We can extend F to a larger number field without loss of generality. In particular:
  - we may get rid of all of the places of additive reduction and assume that we have semistable reduction (here meaning all reduction types of E are good or split multiplicative); and
  - we may assume that F is complex and Galois over $\mathbb{Q}$.
- We may assume that our infinitely many primes are of good reduction, are unramified in F, and satisfy $\det(G_\ell) = \mathbb{F}_\ell^\times$ (equivalently: that we have $\mathbb{Q}(\zeta_\ell) \cap F = \mathbb{Q}$).

Yesterday we saw that there are infinitely many primes ℓ such that G_ℓ is contained in one of a Borel (meaning upper triangular matrices), normalizer of Cartan or exceptional.

Consider

$$\begin{array}{c} F_\ell \\ \Big| G_\ell \\ F \end{array}$$

Let $I_\mathfrak{l} \subseteq G_\ell$ be the inertia subgroup for $\mathfrak{l} \mid \ell$ (so of good reduction). Then $\#(E \mod \mathfrak{l})[\ell] = \begin{cases} \ell & \text{ordinary} \\ 1 & \text{supersingular.} \end{cases}$

(1) If ordinary then we have the exact sequence

$$0 \longrightarrow \ker \longrightarrow E[\ell] \xrightarrow{\text{red}} (E \mod \mathfrak{l})[\ell] \longrightarrow 0$$

where $\#\ker = \ell$. Inertia acts trivially on the rightmost group, so must act as

$$\begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$$

where ω is the cyclotomic character. Thus the image is in the Borel subgroup.

Exercise 13. $y^2 = x^3 + x^2 - 2x - 1$ has 3-division polynomial

$$(x-2)(3x^3 + 10x^2 + 8x + 4) = (x-2)(3x - (1 + 3 + 3^2 + \dots))(\text{quadratic})$$

Note the nontrivial 3-torsion points in $\mathbb{Q}_3$ are then $(2, \pm\sqrt{7})$, and moreover if we extend the field by a quadratic extension we obtain $\left(\frac{1+3+3^2+\dots}{3}, \frac{\pm\sqrt{-3}}{3^2}(1 + 3 + \dots)\right)$. It is not hard to see from this that the Galois image is

$$\begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix}$$

(2) If supersingular then take the formal group associated to E over $F_\mathfrak{l}$: let

$$H(z, w) = z + w + (\deg \geq 2),$$

and let $\mathfrak{m}$ be the maximal ideal of the integers of $\overline{\mathbb{Q}_\ell}$. Then $\mathfrak{m}$ is a group using H for composition, and moreover

$$\mathfrak{m} = \left\{ P \in E(\overline{\mathbb{Q}_\ell}) \ : \ P \text{ reduces to } \infty \bmod \mathfrak{l} \right\}.$$

The ℓ-torsion of $\mathfrak{m}$ is precisely

$$\left\{ z \in \mathfrak{m} \ : \ \underbrace{H(z, H(z, H(z, \dots)))}_{\ell} = 0 \right\}$$

$$= \ell z + (\text{higher degree}).$$

Formal groups in characteristic ℓ:

$$[\ell]z = H'(z^{\ell^h})$$

where h is the height of the formal group, and $H' = a_1 z + a_2 x^2 + \dots$ and $a_1 \neq 0 \mod \mathfrak{l}$. We are supersingular if and only if $h = 2$.

Now $z \in E[\ell]$ if and only if $\underbrace{\ell z + \ldots}_{\text{div by } \ell} + Z^{\ell^2} = 0$, which is equivalent to $z = 0$ or Z is a zero of an Eisenstein polynomial. Thus

$$\#I_{\mathfrak{l}} = \ell^2 - 1$$

and is cyclic. Note that

$$\begin{array}{ccccc} I_{\mathfrak{l}} & \subset & G_\ell & \subset & \mathrm{GL}_2(\mathbb{F}_\ell) \\ \downarrow & & & \swarrow & \\ \overline{I}_{\mathfrak{l}} & \subset & \mathrm{PGL}_2(\mathbb{F}_\ell) & & \end{array}$$

In particular since $\#I_{\mathfrak{l}} = \ell^2 - 1$, we must have $\#\overline{I}_{\mathfrak{l}} \geq \ell + 1$ and so the image of G_ℓ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is of size at least $\ell + 1$. Thus $G_\ell \subset$exceptional group for only finitely many ℓ.

Proposition 14. *There is an extension F'/F with $[F' : F] \leq 2$ such that for infinitely many ℓ the image of $G_{F'}$ is in Borel or Cartan.*

Proof. Suppose that for infinitely many primes ℓ, we have $G_\ell \subset$normaliser of Cartan but not Cartan. Recall that Cartan is the matrices $\left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$, and the normaliser of Cartan is generated by the Cartan subgroup together with the matrices of the form $\left\{\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}\right\}$. In particular, for each such ℓ we get a quadratic extension $F_\ell/F'/F$ depending on ℓ.
Claim: This extension is everywhere unramified and so (via finiteness of the class group and class field theory) we can choose F' to work for infinitely many ℓ.

Proof of claim. What primes can ramify? Well precisely

(1) $\mathfrak{p} \mid \ell$ of good reduction (by our assumptions on ℓ the good reduction is for free); or
(2) $\mathfrak{p} \nmid \ell$ of bad reduction.

In case 1., if $\mathfrak{p} \mid \ell$ of good reduction then have

$$\begin{array}{c} F_\ell \\ | C \\ F' \\ | \\ F \end{array}$$

and the total group is contained in $N =$normaliser of Cartan, we want $I_{\mathfrak{p}} \subset C$. We saw $I_{\mathfrak{p}} = \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$ if E is ordinary and $\#I_{\mathfrak{p}} = \ell^2 - 1$ if E is supersingular. It is then pure group theory to conclude that $I_{\mathfrak{p}} \subseteq C$.

In case 2. let $\mathfrak{p} \mid p \neq \ell$ be a bad prime. Our assumptions ensure that $\mathfrak{p}$ is split multiplicative and so we appeal to the Tate curve.

$$\overline{\mathbb{Q}_p}/q^{\mathbb{Z}} \cong E(\overline{\mathbb{Q}_p}).$$

So moreover we have a short exact sequence

$$0 \longrightarrow \mu_\ell(\overline{\mathbb{Q}_p}) \longrightarrow E[\ell] \longrightarrow q^{\mathbb{Z}}/q^{\ell\mathbb{Z}} \longrightarrow 0.$$

Thus $I_{\mathfrak{p}} = \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$. □

□

Corollary 15. *Have E/F' and infinitely many primes ℓ for which G_ℓ is contained in either Borel or Cartan (split/nonsplit).*

Remark 16. So in other words we're rid of the exceptional and normaliser of Cartan cases!

Proposition 17. *If G_ℓ is contained in non-split Cartan for infinitely many ℓ then there are also infinitely many ℓ for which G_ℓ is contained in split Cartan (which is contained in Borel).*

Remark 18. This is the hardest part of the proof, we skip it for time.

As a result we now have:

Corollary 19. *For infinitely many primes ℓ we have G_ℓ is contained in Borel.*

Claim: This implies that E has CM.

Proof of claim. We have infinitely many ℓ with G_ℓ contained in Borel, which is the group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Thus for each such ℓ we have an ℓ-isogeny

$$E \xrightarrow{\varphi_\ell} E_{(\ell)}.$$

However the size of the isogeny class of E over F is finite, so there exists ℓ' with $E_{(\ell)} = E_{(\ell')}$ over F.

$$\begin{array}{ccc} E & \xrightarrow{\varphi_\ell} & E_{(\ell)} \\ & \nwarrow^{\widehat{\varphi}_{\ell'}} & \downarrow \cong \\ & & E_{(\ell')}. \end{array}$$

However $\deg(\widehat{\varphi}_{\ell'}\varphi_\ell) = \ell\ell'$ which is not square, but $\deg([n]) = n^2$ and so $\widehat{\varphi}_{\ell'}\varphi_\ell$ is an endomorphism of E which is not in $\mathbb{Z}$. □

Why was the size of the F-isogeny class of an elliptic curve over F finite? Well one way is to use Faltings (1983), but Serre did not have access to this yet!

Serre: Fix E with good reduction outside of S, then use the result of Shaferevich (1962) that

$$\{E'/F \ : \ E' \text{ is } F\text{-isogenous to } E\} \subseteq \{E'/F \ : \ \text{good reduction outside of } S\}$$

This set is actually finite:

Proof. write $y^2 = x^3 + Ax + B$ for $A, B \in \mathcal{O}_S$ with good reduction. Then the discriminant $4A^3 + 27B^2 \in \mathcal{O}_S^\times/\mathcal{O}_S^{\times 12}$ which is a finite group. Moreover for each allowable discriminant ε we obtain an elliptic curve $4A^3 + 27B^2 = \varepsilon$! What a miracle! Shafarevich then uses a result of Thue (a precursor to Siegel–Mahler) that there are only finitely many solutions. □

Lecture 3 (Anni)

For the rest of the course we will aim for the following

(1) Almost all elliptic curves over $\mathbb{Q}$ are Serre curves. (Work of Jones and Zywina)
(2) Inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ over $\mathbb{Q}$. (work of Wiese, Dieulefait, Maeda)

Let us begin.

2. Almost All Elliptic Curves are Serre Curves

Let $E/\mathbb{Q}$ be an elliptic curve, $G_\mathbb{Q}$ the absolute Galois group, $n \in \mathbb{Z}_{>1}$. Consider the mod n Galois representation

$$\rho_{E,n} : G_\mathbb{Q} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where the final isomorphism requires a choice of basis. Choosing bases compatibly, these assemble into a Galois image

$$\rho_E : G_\mathbb{Q} \to \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Definition 20. n is *exceptional* if $\rho_{E,n}$ is not surjective.

Question 21. *How big is $\rho_E(G_\mathbb{Q})$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$?*

(1) If E has CM then every integer (except perhaps 2) is exceptional, so the index of the image of ρ_E in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is infinite.
(2) If E does not have CM then, as we saw in René's lectures, Serre showed that $i_E := [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{im}(\rho_E)] < \infty$. Equivalently, there exists $n_E \in \mathbb{Z}_{\geq 1}$ such that
$$\rho_E(G_\mathbb{Q}) = \pi^{-1}\rho_{E,n_E}(G_\mathbb{Q})$$
where $\pi : \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n_E\mathbb{Z})$ is the natural reduction map. This implies that for any fixed E there are only finitely many exceptional primes p, since any such p must divide n_E.

Proposition 22 (Mazur, suggested by Serre)**.** *If $E/\mathbb{Q}$ is semistable, meaning every prime is good or multiplicative, and does not have CM, then $\rho_{E,p}$ is surjective for every prime $p \geq 11$.*

In particular if E is semistable then

$$\{2, 3, 5, 7\} \supseteq \{\text{exceptional primes of } E\}.$$

Theorem 23 (Zywina, 2011)**.** *If $E/\mathbb{Q}$ does not have CM, and $N = \prod_{p|N_E} p$ is the radical of the conductor N_E. Then there exists C constant such that*

$$i_E \leq C(68N(1 + \log\log(N))^{1/2})^{24\omega(N)}.$$

Under GRH we can find C' such that

$$i_E \leq (C' \log(N) \log\log(2N)^3)^{24\omega(N)}.$$

Question 24. *Can $i_E = 1$?*

Answer 25. No (Serre).

Definition 26. Call $E/\mathbb{Q}$ a *Serre curve* if $i_E = 2$, i.e. $\rho_E(G_\mathbb{Q}) \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ has index 2.

Lemma 27. *Let $E/\mathbb{Q}$ be such that:*

(1) E has no exceptional primes; and
(2) E is not exceptional at 4 and 9; and
(3) $[\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : \rho_{E,8}(G_{\mathbb{Q}})] \neq 2$; and
(4) $\exists p$ prime such that $p > 3$, $p \mid M_{\Delta_{\mathrm{sf}(E)}}$, where this (thus far undefined) integer being divided is the Serre number.

Then E is a Serre curve.

Actually when he showed that $i_E \neq 1$, Serre showed something stronger. He showed that $\rho_E(G_{\mathbb{Q}}) \subseteq H_E \subseteq \mathrm{GL}_2(\widehat{Z})$ where H_E has index 2, is quite explicit, and is known as the Serre subgroup. Now we should define the Serre number and group.

Definition 28. Let $E : y^2 = x^3 + Ax + B = \prod_{i=1}^{3}(x - e_i)$, so that e_i are the x-coordinates of the nontrivial 2-torsion points. The discriminant is $\Delta(E) = ((e_1 - e_2)(e_1 - e_3)(e_2 - e_3))^2$, let Δ_{sqf} be the squarefree part of Δ_E. Note that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2])$.

The mod 2 representation is as below,

$$\begin{array}{ccccc} G_{\mathbb{Q}} & \xrightarrow{\rho_{E,2}} & \mathrm{GL}_2(\mathbb{F}_2) & \xrightarrow{\sim} & \mathrm{GL}_2(\mathbb{F}_2) \cong S_3 \\ & \searrow & & \nearrow & \\ & & \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) & & \end{array}$$

where S_3 is acting on the roots e_1, e_2, e_3 in the natural way. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ we have that $\sigma(\sqrt{\Delta_E}) = \varepsilon(\sigma)\sqrt{\delta_E}$ where ε is the sign character on S_3.

- If $\sqrt{\Delta_E} \in \mathbb{Q}$ then $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \subseteq A_3 \cong C_3$. Define $M_1 = 2$ and $H_2 = \pi^{-1}(A_3)$
- if $\sqrt{\Delta_E} \notin \mathbb{Q}$ then $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_D)$ for some $D \in \mathbb{Z}_{\geq 2}$ by Kronecker–Weber. Thus, via the Weil pairing as in Schoof's lectures,

  $$\mathbb{Q}(\sqrt{\Delta_E}) \subset \mathbb{Q}(\zeta_D) \subset \mathbb{Q}(E[D]).$$

  Thus $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[D]) \neq \mathbb{Q}$, and we say E has *entanglement*.

Lemma 29. *Let W be a squarefree integer and* $D_W := \begin{cases} |W| & \text{if } W \cong 1 \mod 4 \\ 4\,|W| & \text{else.} \end{cases}$.

Then $\mathbb{Q}(\sqrt{W}) \subset \mathbb{Q}(\zeta_D)$ if and only if $D_W \mid D$. For such D and $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[D])/\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/D\mathbb{Z})$, we have

$$\sigma(\sqrt{W}) = \left(\frac{W}{\det(\sigma)}\right)\sqrt{W}.$$

Here $\left(\frac{W}{\cdot}\right)$ is the Kronecker symbol $\left(\frac{W/|W|}{\cdot}\right)\prod_{p|W}\left(\frac{p}{\cdot}\right)$.

Thus for $E/\mathbb{Q}$ as above, $\mathbb{Q}(\sqrt{\Delta_E}) \subset \mathbb{Q}(\zeta_D)$ if and only if $D_{\Delta_{\mathrm{sqf}}} \mid D$.

Definition 30 (Serre number)**.** For any squarefree integer W we define a Serre number

$$M_W := \begin{cases} 2\,|W| & \text{if } W \equiv 1 \mod 4 \\ 4\,|W| & \end{cases} = \mathrm{lcm}(2, D_W)$$

Remark 31. So $\mathbb{Q}(E[M_{\Delta_{\mathrm{sqf}}}]) = \mathbb{Q}(E[2])\mathbb{Q}(E[D_{\Delta_{\mathrm{sqf}}}])$!

Definition 32 (Serre Subgroup)**.** For a squarefree integer W,

$$H_{M_W} = \ker\left(\left(\frac{W}{\det(\cdot)}\right)\varepsilon(\cdot)\right) \subseteq \mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z}),$$

where

$$\varepsilon : \mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to \{\pm 1\}$$

is just the extension of the sign representation of S_3 as before, we call this the signature character.

Remark 33. So $\mathrm{Gal}(\mathbb{Q}(E[M_{\Delta_{\mathrm{sqf}}}])) \subset H_{M_{\Delta_{\mathrm{sqf}}}}$!

Definition 34. For our elliptic curve E, the Serre subgroup $H_E \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the preimage under the projection $\pi : \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/M_{\Delta_{\mathrm{sqf}}}\mathbb{Z})$ of $H_{M_{\Delta_{\mathrm{sqf}}}}$.

If N is exceptional for E then note that any multiple of N is exceptional for E by Chinese remainder theorem. It will be useful to define a notion of minimality to reduce down to the core of where the exceptionality occurs.

Definition 35. We say N is minimal exceptional for E if it is exceptional and for every $d \mid N$ such that $1 \neq d \neq N$, d is not exceptional.

Example 36. If E is a Serre curve, then $N_{\Delta_{\mathrm{sqf}}}$ is minimal exceptional.

We finish with a statement, which we will prove next time.

Lemma 37. *If N is minimal exceptional for our elliptic curve $E/\mathbb{Q}$, then*

$$N \in \{p \ : \ p \text{ is prime}\} \cup \left\{M_{\Delta_{\mathrm{sqf}}(E)}\right\} \cup \{4, 8, 9\}.$$

Moreover, if 8 is minimal exceptional then $[\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : \rho_{E,8}(G_{\mathbb{Q}})] = 2$.

Lecture 4 (Anni)

Recall from last time Lemma 37. You can show:

- For $\ell \geq 5$: If $\rho_{E,\ell}$ is surjective, then ρ_{e,ℓ^n} is surjective for all n.
- Unfortunately ρ_{E,ℓ^n} being surjective does not imply $\rho_{E,\ell^{n+1}}$ being surjective for $\ell^n \in \{2, 3, 4\}$.

There are results in these exceptional cases: $2, 4, 8$ (Dokchitser–Dokchitser), and 3 Elkies. We'll try to ignore these small primes in the interests of time because they are ugly. Now we prove the lemma from last time.

Lemma 38 (Lemma 37)**.** *If N is minimal exceptional for our elliptic curve $E/\mathbb{Q}$, then*

$$N \in \{p \ : \ p \text{ is prime}\} \cup \left\{M_{\Delta_{\mathrm{sqf}}(E)}\right\} \cup \{4, 8, 9\}.$$

Moreover, if 8 is minimal exceptional then $[\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : \rho_{E,8}(G_{\mathbb{Q}})] = 2$.

Proof. Suppose N is exceptional but is not prime. Write

$$G_N := \mathrm{im}\left(\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \subsetneq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})\right).$$

If N is minimal exceptional then for all $d \mid N$ not 1 or N we have

$$G_d = \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}).$$

Therefore there is a surjection

$$G_N \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$$

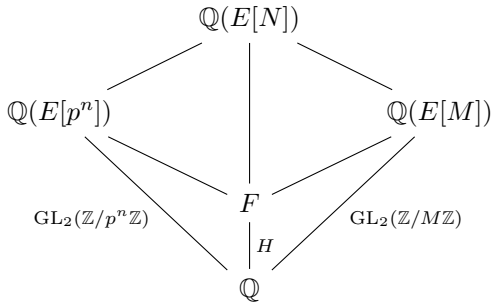
for every proper nontrivial divisor $d \mid N$. The Weil pairing is surjective, so

$$\det : G_N \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}^\times.$$

We want to find options for $G_N \subsetneq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that

- $G_N \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ for all $d \mid N$ with $d \neq 1, N$;
- $\det : G_N \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}^\times$.

Case 1: N is not a prime power. In this case, let $p \mid N$ be the smallest prime and $M = N/p^{v_p(N)}$ be the prime-to-p part of N. In particular M is odd. Consider the diagram



Then $\mathbb{Q} \subsetneq \mathbb{Q}(E[p^n]) \cap \mathbb{Q}(E[M]) =: F$ because $G_N \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $H = \mathrm{Gal}(F/\mathbb{Q})$. If H is not a simple group then replace it (by the Jordan–Hölder theorem) with any non-trivial simple quotient (and F by the appropriate fixed field).

We then appeal to a result of Serre.

Lemma 39 (Serre)**.** *Let $N_1, N_2 \in \mathbb{Z}_{>1}$ be coprime integers. Then $\mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/N_2\mathbb{Z})$ have no common simple non-abelian quotients.*

Thus we may assume that H is abelian, common quotient of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Lemma 40. *We have the following.*

- *The commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is* $\begin{cases} \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) & p \neq 2 \\ \ker \varepsilon \cap \mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z}) & p = 2 \end{cases}$
- *$\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is its own commutator for $p \geq 5$.*

So, since M is odd, $F \subseteq \mathbb{Q}(\zeta_M)$. If $p > 2$ then also $F \subseteq \mathbb{Q}(\zeta_{p^n})$. However then $F \subseteq \mathbb{Q}(\zeta_M) \cap \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}$. This is a contradiction, so $p = 2$. The

$$\mathbb{Q} \neq F \subseteq \mathbb{Q}(\sqrt{\Delta_E}, \zeta_{2^n}) \cap \mathbb{Q}(\zeta_M).$$

If $n = 1$ then $F = \mathbb{Q}(\sqrt{\Delta_E})$, so N is a multiple of $M_{\Delta_{\mathrm{sqf}}(E)}$, the Serre number, and therefore by minimality must be the Serre number.

If $n \geq 2$ then $\#\mathrm{Gal}(F/\mathbb{Q}) = 2^\alpha$, so must be $\mathbb{Z}/2\mathbb{Z}$ by simplicity. If $n = 2$ then $F \in \left\{\mathbb{Q}(\sqrt{\Delta_E}), \mathbb{Q}(\sqrt{-\Delta_E})\right\}$, else if $n \geq 3$ then $F \in \left\{\mathbb{Q}(\sqrt{\Delta_E}), \mathbb{Q}(\sqrt{-\Delta_E}), \mathbb{Q}(\sqrt{2\Delta_E}), \mathbb{Q}(\sqrt{-2\Delta_E})\right\}$. In all of these cases $M_{\Delta_{\mathrm{sqf}}(E)} \mid N$, so since N is assumed to be minimal exceptional (and the Serre number is always exceptional), $N = M_{\Delta_{\mathrm{sqf}}(E)}$ in this case.

Case 2: $N = p^n$ is a prime power for some $n \geq 2$, $p \geq 5$. Then

$$G_{p^n} \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/p^{n-1}\mathbb{Z}),$$

so the commutator (which we denote with ') satisfies

$$G'_{p^n} \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/p^{n-1}\mathbb{Z})' \cong \mathrm{SL}_2(\mathbb{Z}/p^{n-1}\mathbb{Z}).$$

But it is a result of Serre that if

$$G'_{p^n} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/p^{n-1}\mathbb{Z})$$

Then in fact $G'_{p^n} \cong \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Since the determinant map surjects and $G_{p^n} \supseteq G'_{p^n} = \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$, we must have $G_{p^n} = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, which is a contradiction of our assumptions and so this case cannot occur.

Case 3. $N = p^n$ **is a prime power for some** $n \geq 2$ **and** $p \in \{2, 3\}$**.** Ask me later. □

We are now in a good place to prove Lemma 27, which we restate below for the readers convenience.

Lemma 41 (Lemma 27)**.** *Let $E/\mathbb{Q}$ be such that:*

(1) E has no exceptional primes; and
(2) E is not exceptional at 4 and 9; and
(3) $[\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : \rho_{E,8}(G_{\mathbb{Q}})] \neq 2$; and
(4) $\exists p$ prime such that $p > 3$, $p \mid M_{\Delta_{\mathrm{sf}(E)}}$.

Then E is a Serre curve.

Proof. We want to show that all of our exceptional behaviour (or entanglement, if you will), is seen in the Serre group

$$G_{M_{\Delta_{\mathrm{sqf}(E)}}} = \mathrm{Gal}(\mathbb{Q}(E[M_{\Delta_{\mathrm{sqf}(E)}}])/\mathbb{Q} = H_{M_{\Delta_{\mathrm{sqf}(E)}}}.$$

More precisely, that for all N we have

$$G_N = \begin{cases} \pi^{-1}_{N, M_{\Delta_{\mathrm{sqf}(E)}}}(H_{M_{\Delta_{\mathrm{sqf}(E)}}}) & \text{if } M_{\Delta_{\mathrm{sqf}(E)}} \mid N \\ \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) & \text{otherwise.} \end{cases}$$

We will need a (strict) application of the Goursat lemma.

Lemma 42. *For $N \in \mathbb{Z}_{>1}$, $N = N_1N_2$ with $N_1 = 2^r3^s$ and $N_2 > 1$ coprime to N_1. Let $G_a \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $G_a \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})'$. Assume that $G_b \subset G_a$ is such that both*

- *$G_b \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$ for $i \in \{1, 2\}$; and*
- *$\det : G_b \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}^\times$.*

Then $G_a = G_b$

Using the lemma, $N = M_{\Delta_{\mathrm{sqf}(E)}}$, $G_a = H_{M_{\Delta_{\mathrm{sqf}(E)}}}$, $G_b = G_{M_{\Delta_{\mathrm{sqf}(E)}}}$. Then

$$G_{M_{\Delta_{\mathrm{sqf}(E)}}} \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \left(\ker(\varepsilon) \cap \mathrm{SL}_2(\mathbb{Z}/2^r3^s\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/M'\mathbb{Z})\right),$$

where

$$M_{\Delta_{\mathrm{sqf}(E)}} = M'2^r3^s = N_2N_1.$$

Moreover $G_{M_{\Delta_{\mathrm{sqf}(E)}}}$ surjects onto $\mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$ for both $i \in \{1, 2\}$ by hypothesis. □

Statistics. $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$ and $\gcd(A^3, B^2)$ being 12th power free. Then let

$$H(E) := \max\left\{|A|^3, |B|^2\right\}$$

be the naive height. Then it is a result of Duke that if we order these curves by height, then almost all E have no exceptional primes.

Theorem 43 (Duke 1997)**.** *Let*

$$C(X) = \left\{ [E/\mathbb{Q} \ : \ H(E) \leq X^6]/\cong \right\},$$

and

$$\mathcal{E}(X) = \{E \in C(X) \ : \ \exists p \text{ exceptional for } E\}.$$

Then

$$\lim_{X\to\infty} \frac{\#\mathcal{E}(X)}{\#C(X)} = 0.$$

In fact, more precisely,

$$\#\mathcal{E}(X) \ll X^4 \log^B(X),$$
$$\#C(X) = \frac{4}{\zeta(10)} X + O(X^3).$$

Note that Duke's count of $\#\mathcal{E}(X)$ is not effective, it was then follows by the following effective result.

Theorem 44 (Grant 2000)**.** *In fact for all* $\varepsilon > 0$

$$\#\mathcal{E}(X) = CX^3 + O(X^{2+\varepsilon}),$$

for some explicit C*, and the main contribution comes from* 2 *and* 3*.*

We won't look into the proofs, it is technical. We promised to show that almost all curves are Serre curves, so let us do that now.

If N is minimal exceptional then $N \in \{\text{prime}\} \cup \left\{M_{\Delta_{\text{sqf}}(E)}\right\} \cup \{4, 8, 9\}$. Let $C_{ns}(X) \subset C(X)$ be defined by

$$C_{ns}(X) := \{E \in C(X) \ : \ E \text{ is not a Serre curve}\}.$$

Then there exists N minimal exceptional for $E \in C_{ns}(X)$, and let

$$\varepsilon_N(X) = \begin{cases} \{E \in C(X) \ : \ 4 \text{ or } 9 \text{ is minimal exceptional}\} & \text{if } N \in \{4, 9\} \\ \{E \in C(X) \ : \ 8 \text{ is exceptional}\} & \text{if } N = 8 \\ \{E \in C(X) \ : \ G_N \subsetneq H_N\} & \text{if } N \in \{6, 12, 24\}. \end{cases}$$

Note that

$$C_{ns}(X) \subseteq \mathcal{E}(X) \cup \bigcup_{N\in\{4,6,8,9,12,24\}} \mathcal{E}_N(X).$$

Theorem 45 (Jones, 2006)**.** *Let* $C_{\text{serre}}(X) = \{E \in C(X) \ : \ E \text{ is a Serre curve}\}$*. Then*

$$\lim_{X\to\infty} \frac{C_{\text{serre}}(X)}{\#C(X)}.$$

Proof. Note that

$$\lim_{X\to\infty} \frac{C_{ns}(X)}{\#C(X)} = 0.$$

We have

$$C_{ns}(X) \subseteq \mathcal{E}(X) \cup \bigcup_{N\in\{4,6,8,9,12,24\}} \mathcal{E}_N(X)$$

and we decompose

$$\mathcal{E}_N(X) = \bigcup_{(t,d)\in\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}^\times} \mathcal{E}_{N,(t,d)}(X),$$

where

$$\mathcal{E}_{N,(t,d)}(X) = \{E \in \mathcal{E}_N(X) \ : \ \nexists \tau \in G_N \ : \ \mathrm{tr}(\tau) = t, \ \det(\tau) = d\}\,.$$

Then we count these subsets (with the large sieve). This allows us to obtain the following result.

Lemma 46 (Jones, Duke)**.**

$$\#\mathcal{E}_N(X) \ll N^{16}\varphi(N)X^4\log(X)^{-2}$$

□

Lecture 5 (Anni)

3. Interlude: Galois Groups

Let $F \in \mathbb{Z}[X]$ be monic and of degree d (with **big** coefficients!).

Question 47. *How can one prove that the Galois group of the splitting field $\mathbb{Q}(F)$ satisfies*

$$\mathrm{Gal}(\mathbb{Q}(F)/\mathbb{Q}) \cong S_d?$$

Answer 48. Pick a prime p and let $F_p \in \mathbb{F}_p[X]$ be the reduction of F mod p. If F_p is separable then there is a $\tau \in \mathrm{Gal}(\mathbb{Q}(F)/\mathbb{Q})$ such that the cycle type of τ is the same as the factorisation pattern of F_p.

Definition 49. We say that a prime p is of:

(1) type I for F if F_p is irreducible over $\mathbb{F}_p$;
(2) type II for F if $F_p = f_0 \dots f_s$ where the f_i are distinct irreducible polynomials with $\deg(f_0) = 2$ and $\deg(f_i)$ is odd for all other i.
(3) type III for F if $F_p = f_0 \dots f_t$ where the f_i are distinct irreducible polynomials with $\deg(f_0) > d/2$ and prime.
(4) type IV if $F_p = f_0 f_1$ where the f_i are distinct irreducible polynomials and $\deg(f_0) = 1$

Lemma 50 (Buzzard, Conrey–Farmer, Serre, Maeda)**.** *If $f \in \mathbb{Z}[X]$ has primes of type I, II, and (III or IV), then*

$$\mathrm{Gal}(\mathbb{Q}(F)/\mathbb{Q}) \cong S_d.$$

Lemma 51 (Ghitza, McAndrew, Durzat)**.** *If these conditions hold then:*

- *Type I occurs with density $1/d$;*
- *Type II occurs with density $> 1/4\sqrt{d}$;*
- *Type III occurs with density $> 1/d$ if $d > 10$ the density $> 1/3\log(d)$;*
- *Type IV occurs with density $1/(d-1)$.*

4. Inverse Galois Problem

Question 52 (Noether)**.** *Given a finite group G, is there a Galois number field $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?*

- Consider $G = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ or $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ for $M \in \mathbb{Z}_{>1}$ and p prime. Then take a Serre curve $E/\mathbb{Q}$ (there are plenty of them as a result of our earlier lectures!), and we are done – take $K = \mathbb{Q}(E[p])$ or $\mathbb{Q}(E[M])$! Okay so maybe for M you need to change curve to change the Serre number, but you can do this.

- Consider $G = \mathrm{GL}_2(\mathbb{F}_{p^d})$ for p prime and $d > 1$. Can we use abelian varieties? No: the Weil pairing is an obstruction, since the determinant will be in $\mathbb{F}_p$. So we use modular forms!

Let $f \in S_k(\Gamma_0(N))^{\mathrm{new}}$ be a (weight k level N) newform (normalised eigenform for the Hecke operators, cuspidal, not coming from any level $m \mid N$). An important property is that f has a q-expansion

$$f(z) = q + \sum_{n \geq 2} a_n q^n$$

where $q = e^{2\pi i z}$. Under these hypotheses, $K_f := \mathbb{Q}(\{a_n\})$ is a number field called the Hecke eigenvalue field.

Theorem 53 (Deligne, Serre, Shimura)**.** *There is a unique continuous semisimple representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda),$$

where $\mathbb{F}_\lambda = \mathcal{O}_{K_f}/\Lambda \supset \mathbb{F}_\ell$, ℓ *a prime, which is:*

- *unramified outside of* $N\ell$*; and*
- $\forall p \nmid N\ell$ *the characteristic polynomial of* $\rho_{E,\lambda}(\mathrm{Frob}_p)$ *is* $x^2 - a_p + p^{k-1}$*, where* a_p *is the coefficient of the* q*-expansion.*

Now, if I want to realise $\mathrm{GL}_2(\mathbb{F}_{\ell^d})$ as a Galois group over $\mathbb{Q}$ then I want to find f, N, k such that $\mathbb{F}_\lambda \cong \mathbb{F}_{\ell^d}$ and $\rho_{f,\lambda}$ is surjective.

Theorem 54 (Wiese 2013)**.** *Assume Maeda's conjecture. Then*

(1) For any d *even, the set of primes* p *such that there is* $K/\mathbb{Q}$ *ramified at* p *and*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{F}_{p^d})$$

has density 1*.*

(2) For every d *odd, the set of primes* p *such that there is* $K/\mathbb{Q}$ *ramified precisely at these primes and*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_{p^d})$$

has density 1*.*

Proof. Maeda's conjecture implies that there are f_{n_i}, newforms of level 1 and increasing weight such that $K_{f_{n_i}}$ satisfy

(1) $\mathrm{Gal}(K_{f_{n_i}}^{\mathrm{gal}}/\mathbb{Q}) \cong S_d$;
(2) the dimension of the modular forms space for f_{n_i} goes to infinity;
(3) $K_{f_{n_i}}$ have no CM;

Then $\left\{p \,:\, \exists i,\ \exists \mathfrak{p} \mid p \text{ in } K_{f_{n_i}} \text{ of residue degree } d\right\}$ has density 1.

For each k, $\mathbb{P}_{\rho_{f,\mathfrak{p}}}$ is surjective almost always (Ribet, 1985). □

Let T_m be the mth Hecke operator acting on $S_k(1)^{\mathrm{new}}$, and let $F_{m,k}$ be the characteristic polynomial of T_m.

Conjecture 55 (Maeda's Conjecture, 1997)**.** *If* $m > 1$ *then*

(1) $F_{m,k}$ *is irreducible over* $\mathbb{Q}$
(2) $\mathrm{Gal}(\mathbb{Q}(F_{m,k})/\mathbb{Q}) \cong S_d$*, where* $d = \dim S_k(1)$

In particular, there is only one Galois orbit of newforms in level 1*.*

Currently the best result towards Maeda's conjecture is the following.

Theorem 56 (Ghitza–McAndrew 2012)**.** *Let $k < 12000$, and let*
$n \in \{2, \dots, 10000\} \cup \{p \text{ prime } : \ 2 \leq p \leq 4000000\} \cup \{p \text{ prime } : \ p \not\equiv \pm 1 \mod 5 \text{ or } \pm 1 \mod 7\}$
Then $F_{n,k}$ satisfies Maeda's conjecture.