Frey's curve and its modularity

Guo Haoyang

May 2025

Contents

1 Backgrounds and history

The Fermat's last theorem asserts that the equation $x^n + y^n = z^n$ has no non-zero integer solutions for all $n \geq 3$.
How does this equation link to an elliptic curve?
Frey proposed that $E_{a,b,c}$ should not be modular in 1984. Thereafter, Serre formalized his suggestion as ϵ-conjecture, based on Galois representations and modular forms [Sut22]

2 Frey's curve

2.1 Basic introduction

Frey consider an elliptic curve in the Weierstraβ form $E_{A,B} : y^2z = x(x - Az)(x + Bz)$.
If Fermat's last theorem does not hold, $x^n + y^n = z^n$ has integer solutions. The assumed existence of solutions provide a candidate, a curve with substitution: $A = a^p$ and $B = b^p$.

Definition 2.1: Frey-Hellegouarch's curve

Let p be an odd prime number and (a, b, c) be a tuple of integer solutions of $x^p + y^p = z^p$(or, $a^p + b^p = c^p$).
The Frey curve is

$$E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$$

To compute the minimal Weierstrass equation ([Las82]).
Note that this curve has very symmetric discriminant: for a polynomial f of roots $\alpha_1, \ldots, \alpha_n$, the discriminant is $\Delta_f = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)^2$. Here, if we think of $f(x) = x(x - a^p)(x + b^p)$, which has roots $0, a^p, -b^p$, then the discriminant of $f(x) = x(x - a^p)(x + b^p)$ is

$$\Delta_f = (0 - a^p)^2(0 + b^p)^2(a^p + b^p)^2$$

Since the discriminant of E satisfies $\Delta_{E_{a,b,c}} = 16\Delta_f$, $\Delta_{E_{a,b,c}} = 16(abc)^{2p}$
Let's consider the minimal Weierstrass equation of $E_{a,b,c}$, $E'_{a,b,c}$. E' is an elliptic isomorphic to $E \Leftrightarrow$ the transformation of E into E' is under the form $x' = u^2x + r$, $y' = u^3y + u^2sxy + t$. After that, the discriminant of E, Δ_E and the discriminant of E', $\Delta_{E'}$ has a factor u^{12} varying, i.e. $\Delta_E = u^{12}\Delta_{E'}$.
So, to prove FLT is true $\Leftrightarrow$ to prove every such curve does not exist. Needs revised: 1.links between FLT and this curve 2.How do

2.2 Motivation of arising

2.3 Why is this curve 'strange'?

[Sut22]

2.4 Non-modularity of Frey's curve

Now, let's go back to Frey's suggestion: why such a curve should not exist.

3 Some Galois representations

3.1 Galois representations associated to elliptic curves

There are three kinds of representations we would explore: the Artin representations, mod-l representations and the p-adic representations.

Definition 3.1: mod-l Galois representations

Let $E/\mathbb{Q}$ be an Elliptic curve and l be an odd prime. The **mod-l Galois representation** is defined as:

$$\begin{aligned}\overline{\rho}_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\to \mathrm{Aut}(E[l](\mathbb{Q})) \\ \sigma &\mapsto \Big(\overline{\rho}_{E,l}(\sigma) : [x:y:z] \mapsto [\sigma(x):\sigma(y):\sigma(z)]\Big)\end{aligned}$$

where $E[l]$ is the collection of l-torsion points in $E/\mathbb{Q}$.
For each power of l, l^n, the corresponding **mod-l^n Galois representation** is similarly defined as

$$\overline{\rho}_{E,l^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[l^n](\mathbb{Q}))$$

Remark From the structure of N-torsion points $E[N]$ of elliptic curves E/K: when $\mathrm{char}K = 0$ or $\mathrm{char}K > 0$ with $\mathrm{char}K \not| N$, $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times Z/N\mathbb{Z}$. Since $\mathrm{char}\mathbb{Q} = 0$, here $\mathrm{Aut}(E[l]) \cong \mathrm{Aut}(\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$, and $\mathrm{Aut}(E[l^n]) \cong \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ the last $\cong$ for both are up to choices of basis.

So, the above-mentioned definition makes the notion falls into a representation over a ring of characteristic l, but this is not satisfactory enough, since 'it is easier to deal with representations whose matrices have coefficients in a ring of characteristic 0 ([Sil09]). So, the next step is to try to fit representations over a ring of characteristic l for arbitrary l into a representation over characteristic 0 ring.
Inspired by the l-adic integers, let's consider the limit case: take $E[l^n]$ to be its limit case $T_l(E) := \varprojlim_n E[l^n]$, the l-adic *Tate module*. Then, we get

Definition 3.2: l-adic Galois representations

Let $E/\mathbb{Q}$ and l be the same as in Definition 3.1. The **l-adic Galois representation** is defined as:

$$\rho_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_l(E))$$

Remark By the structure theorem of $T_l(E)$ for E/K, $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ non-canonically if $l \neq \mathrm{char}K$; $T_l(E) \cong \{0\}$ or $\mathbb{Z}_l$ if $l = \mathrm{char}K$. After choosing a $\mathbb{Z}_l$-basis, $\mathrm{Aut}(T_l(E)) \cong \mathrm{Aut}(\mathbb{Z}_l \times \mathbb{Z}_l) \cong \mathrm{GL}_2(\mathbb{Z}_l)$.
In general, this representation is defined for all field K and E/K, so $\rho_{E,l}$ should be $\rho_{E,l} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$.

To proceed with a representation over a field of characteristic 0, there is a satisfied one, $\mathbb{Q}_l$, at hand. ([Sil09])
By the inclusion $\mathbb{Z}_l \hookrightarrow \mathbb{Q}_l$, we have a representation $\widetilde{\rho}_{E,l} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_l) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_l)$, as desired. The only drawback of this representation is it depends on some choices of $\mathbb{Q}_l$-basis. To avoid choosing basis, consider

$$\widetilde{\rho}_{E,l} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E)) \hookrightarrow \mathrm{Aut}(T_l(E)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

3.2 Galois group actions

Let K/F be a finite extension of number fields and $\mathcal{O}_K, \mathcal{O}_F$ be their corresponding rings of integers. So, $\mathcal{O}_K, \mathcal{O}_F$ both are integral closure of $\mathbb{Z}$ in K, F, respectively. We have the diagram

$$\begin{array}{ccccc} \mathbb{Q} & \hookrightarrow & F & \hookrightarrow & K \\ {\scriptstyle \mathrm{Frac}}\uparrow & & \uparrow{\scriptstyle \mathrm{Frac}} & & \uparrow{\scriptstyle \mathrm{Frac}} \\ \mathbb{Z} & \hookrightarrow & \mathcal{O}_F & \hookrightarrow & \mathcal{O}_K \end{array}$$

Now, let $\mathfrak{p} \trianglelefteq \mathcal{O}_F$ be a prime ideal. $\mathcal{O}_F, \mathcal{O}_K$ are discrete valuation rings (hence they are PID and then $\mathfrak{p}$ is maximal), $\mathcal{O}_F/\mathfrak{p}$ is the residue field. Every discrete valuation ring is a Dedekind domain, so every ideal of $\mathcal{O}_K$ has the unique factorization into prime ideals of $\mathcal{O}_K$. Consider the extended ideal of $\mathfrak{p}$ in $\mathcal{O}_K$, denoted $\mathfrak{p}\mathcal{O}_K$ or $\mathfrak{p}^{\mathrm{e}}$ (not necessarily prime here), we obtain

$$\mathfrak{p}^{\mathrm{e}} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

where each $\mathfrak{P}_i \trianglelefteq \mathcal{O}_K$ is a prime ideal. In addition, these ideals are called '**lie over/above**' $\mathfrak{p}$, written $\mathfrak{P}_i|\mathfrak{p}$.
In the above-settled notation, $e(\mathfrak{P}_i : \mathfrak{p})$ for the **ramification index** of $\mathfrak{P}_i$: $e(\mathfrak{P}_i : \mathfrak{p}) := e_i$, and $f(\mathfrak{P}_i : \mathfrak{p})$ or f_i for the **residue class degree/ inertia degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$: $f(\mathfrak{P}_i : \mathfrak{p}) := [\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_F/\mathfrak{p}]$, which is the residue degree

of the field extension.
K/L is called **ramified** at $\mathfrak{p}$ if $\exists i$, $e_i > 1$. Otherwise, K/F is called **unramified** at $\mathfrak{p}$.
Let $\mathscr{I}(\mathcal{O}_K)$ be the group generated by fractional ideals of $\mathcal{O}_K$ and $\{\mathfrak{P} \trianglelefteq \mathcal{O}_K : \mathfrak{P}|\mathfrak{p}\}$ be the collection of all prime ideals $\mathfrak{P} \trianglelefteq \mathcal{O}_F$ over $\mathfrak{p}$ (i.e. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$).
When the extension K/F is Galois(using the setting above, we can assume K/F is a normal extension), some interesting properties appear:

(1) ([Mil20]) Consider the same setting as above, $\forall i$, e_i and f_i are identical, respectively. So,

$$\mathfrak{p}^{\mathrm{e}} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e \quad [1]$$

(2) To study the sets $\mathscr{I}(\mathcal{O}_K)$ and $\{\mathfrak{P} \trianglelefteq \mathcal{O}_K : \mathfrak{P}|\mathfrak{p}\}$, as well as the group $\mathrm{Gal}(K/F)$ itself. As group theory suggested, we do group actions. Basically, we study:

• $\mathrm{Gal}(K/F) \curvearrowright \mathscr{I}(\mathcal{O}_K)$. For every fractional ideal J of $\mathcal{O}_K$ and $\forall \sigma \in \mathrm{Gal}(K/F)$, we define the action to be

$$^{\sigma}J := \sigma(J)$$

This is indeed an action and it does not arouse our great interest unless we study one of its orbit as next:

• $\mathrm{Gal}(K/F) \curvearrowright \{\mathfrak{P} \trianglelefteq \mathcal{O}_K : \mathfrak{P}|\mathfrak{p}\}$, which is a special case of the precious type. The definition of action is exactly the same as above. The extra property of this case is this action is *transitive*.

• $\mathrm{Gal}(K/F) \curvearrowright H \leq \mathrm{Gal}(K/F)$. Here we turn to study the subgroups H of $\mathrm{Gal}(K/F)$, the action is defined to be conjugation to make it non-trivial: $\forall \sigma \in \mathrm{Gal}(K/F)$,

$$^{\sigma}H := \sigma H \sigma^{-1}$$

In the following setting, we have two best understood configurations for K/F: One is $\overline{\mathbb{Q}}/\mathbb{Q}$, another one is $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$. In group actions, stabilizers and orbits are always investigated. So, then we consider a subgroup of $\mathrm{Gal}(K/F)$, the decomposition subgroup (see [DS05]), which is exactly the stabilizer of $\mathrm{Gal}(K/F)$ for the actions of the first two types.

Definition 3.3: Decomposition subgroup

Given the setting as above, the **decomposition subgroup** of $\mathfrak{P}_i$, denoted $D_{\mathfrak{P}_i|\mathfrak{p}}$, is the collection of elements of $\mathrm{Gal}(K/F)$ that fixes $\mathfrak{P}_i$

$$D_{\mathfrak{P}_i|\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(K/F) : \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} = \mathrm{Stab}_{\mathrm{Gal}(K/F)}(\mathfrak{P}_i)$$

Because the action is transitive, two stabilizers are conjugate to each other. Hence, two decomposition subgroups are conjugate to each other. Namely, for two $\mathfrak{P}_i, \mathfrak{P}_j$, $\exists \sigma \in \mathrm{Gal}(K/F)$, $D_{\mathfrak{P}_i|\mathfrak{p}} = \sigma D_{\mathfrak{P}_j|\mathfrak{p}} \sigma^{-1}$.

Naturally, $D_{\mathfrak{P}_i}$ has an action on each $\mathcal{O}_K/\mathfrak{P}_i$: fix an $x + \mathfrak{P}_i$ and a $\sigma \in D_{\mathfrak{P}_i}$,

$$^{\sigma}(x + \mathfrak{P}_i) := \sigma(x) + \mathfrak{P}_i$$

The kernel of this action is called **inertia subgroup**.

Definition 3.4: inertia subgroup

The **inertia subgroup** of $\mathfrak{P}_i$ is the kernel of the action $D_{\mathfrak{P}_i|\mathfrak{p}} \curvearrowright \mathcal{O}_K/\mathfrak{P}_i$, denoted $I_{\mathfrak{P}_i|\mathfrak{p}}$, i.e.

$$I_{\mathfrak{P}_i|\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/F) | \ \forall x \in \mathcal{O}_K, \sigma(x) - x \in \mathfrak{P}_i\}$$

Remark The notation of $I_{\mathfrak{P}_i|\mathfrak{p}}$ varies: sometimes it is $I_{\mathfrak{p}}$ or I_K. Because for two different prime ideals $\mathfrak{P}_i, \mathfrak{P}_j$, they are isomorphic. Fix $\sigma \in \mathrm{Gal}(K/F)$. Since Galois group acts transitively on prime ideals above $\mathfrak{p}$, $I_{\mathfrak{P}_i} = I_{\sigma(\mathfrak{P}_j)}$. The action on prime ideals and action on subgroups are reconciled by:

$$I_{\sigma(\mathfrak{P}_j)} = \ ^{\sigma}I_{\mathfrak{P}_j} = \sigma I_{\mathfrak{P}_j} \sigma^{-1}$$

which follows from that $(\tau - \mathrm{id}_K)(x) \in \mathfrak{P}_j \Leftrightarrow \sigma(\tau - \mathrm{id}_K)\sigma^{-1}(x) \in \sigma(\mathfrak{P}_j)$ and $I_{\mathfrak{P}_j} \to I_{\mathfrak{P}_i} \quad \tau \mapsto \sigma\tau\sigma^{-1}$ is an isomorphism. Therefore, there is no difference to pick an $I_{\mathfrak{P}}$ ranging over every prime ideal $\mathfrak{P}|\mathfrak{p}$ up to isomorphism.

[1] the e for $\mathfrak{p}^{\mathrm{e}}$ represents for extended ideal, while the e for $(\mathfrak{P}_1 \cdots \mathfrak{P}_n)^e$ just means the degree.

Without any confusion, we make this symbol global as $I_{\mathfrak{p}}$, $I_{K/F}$ or I_K.
$I_{\mathfrak{P}_i|\mathfrak{p}}$ is a normal subgroup of $D_{\mathfrak{P}_i|\mathfrak{p}}$ since sth. Thus, the quotient $D_{\mathfrak{P}_i}/I_{\mathfrak{P}_i}$ is studied. It has nice structure

$$D_{\mathfrak{P}_i}/I_{\mathfrak{P}_i} \xrightarrow{\sim} \mathrm{Gal}\big((\mathcal{O}_K/\mathfrak{P}_i)/F\big)$$

In the language of valuation, $\sigma(x) - x \in \mathfrak{P}_i \Leftrightarrow v_{\mathfrak{P}_i}(\sigma(x) - x) \geq 1 > 0$. This inspires us to define a sequence of groups that have valuation greater than some integer n.

Lemma 3.1: Equivalent conditions for valuation

Let K/F be a Galois extension now and i be an integer ≥ -1. $\forall \sigma \in \mathrm{Gal}(K/F)$. TFAE:
(i) σ acts transitively on $\mathcal{O}_K/\mathfrak{p}_K^{j+1}$
(ii) $\forall a \in \mathcal{O}_K$, $v_K(\sigma(a) - a) \geq j + 1$
(iii) $v_K(\sigma(x) - x) \geq j + 1$

For each j, define G_i to be the set of $\sigma \in \mathrm{Gal}(K/F)$ satisfying conditions (i), (ii) and (iii) at the same time. Under this notion, $G_0 = I_{\mathfrak{P}_i|\mathfrak{p}}$ If $\mathfrak{P}_i^0 := \mathcal{O}_K$, then $G_{-1} = \mathrm{Gal}(K/F)$. For j sufficiently large, $G_j = \{1\}$. Show this is a group and equality The group G_i is the i-th **ramification group** of $\mathrm{Gal}(K/F)$.

Definition 3.5: Frobenius element

3.3 Reductions

Reductions reveal the local properties of elliptic curves. It means doing the p-module (mod p) operations on the coefficients of an elliptic curve E, and the curve E after mod p, $E_{\mathrm{mod}\ p}$ is some local pieces in the following sense: [Com22]
Suppose that E has coefficients in $\mathbb{Q}$. By rearranging the coefficients and mod-p operations, the coefficients are in $\mathbb{F}_p$. So, we get an elliptic curve $E(\mathbb{F}_p)$. But mod-p operation only yields the roughest 'projection' of E in the sense that it loses much information of E and only keeps the p-many. Continuing the mod-p^n operations, all the $\mathbb{Z}/p^n\mathbb{Z}$ can be embedded into $\mathbb{Z}_p$ by the surjection $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$. As a field, all the $E_{\mathrm{mod}\ p^n}(\mathbb{Q})$ is a piece of $E(\mathbb{Q}_p)$.
This process passes the coefficients from a global field to a local one.
Let

Definition 3.6: Good and Bad reductions

Let p be a prime number and $E/\mathbb{Q}$ be an elliptic curve. E has a **good reduction** at $p \Leftrightarrow E_{\mathrm{mod}\ p}/\mathbb{Q}$ is smooth (has no singularity).
E has a **bad reduction** at $p \Leftrightarrow E$ has some singularities.

A reduction is good or bad can be known from its discriminant: If E has a good reduction at l, then $l \nmid \Delta$; if E has a bad reduction at l, then $l|\Delta$.
From the Δ, it is possible to further classify bad reductions:

- **Multiplicative reduction**: $l \| \Delta$ ($l|\Delta$, but $l^1 \nmid \Delta$). In this case, $E_{\mathrm{mod}\ l}/\mathbb{Q}$ has nodes.
- **Additive reduction**: $l^1|\Delta$. The reduced elliptic curve has cusp points. When this happens, the reduced elliptic curve does not preserve the group structure as $E_{\mathrm{mod}\ l}(\mathbb{Q})$ (meaning $E_{\mathrm{mod}\ l}(\mathbb{Q})$ is not a group anymore). [2]

Example (0) $E : y^2 = x^3 + x + 1$ is a good reduction at $l = 5$, because $\Delta_{E_{\mathrm{mod}\ 5}} = -31$. $5 \nmid -31$.
(1) $E : y^2 = x^3 - x$ is a multiplicative bad reduction. The global discriminant would lose the effect. It only works for field of characteristic $\neq 2, 3$.
(2) $E : y^2 = x^3$ at any l.
In view of these reduction cases, we would like to study those elliptic curves still having group structure after reduction. Such classes of elliptic curves are called **semi-stable**. (See [**MIT17_783S13_lec24**])

[2] There is one subtlety that this criteria lose the power when the field that coefficients are in has characteristic $= 2, 3$.

Definition 3.7: Semi-stable elliptic curve

An elliptic curve $E/\mathbb{Q}$ is semi-stable $\Leftrightarrow$ E does not have additive reduction at any prime.

For the structure of $E[l](\overline{\mathbb{Q}_p})$,

$$E[l](\overline{\mathbb{Q}_p}) \cong (\mathbb{Z}/l\mathbb{Z})^2$$

The cases for $E[l](\mathbb{Q}_p)$ is a bit more complicated: consider two cases $l \neq p$, $l = p$. Notice that $\mathbb{Q}_p = \overline{\mathbb{Q}_p}^{\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}$. This notation implies an action $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p) \curvearrowright E[l](\overline{\mathbb{Q}_p})$, which can be translated into a representation

$$\overline{\rho}_{E,l}\big|_{\overline{\mathbb{Q}_p}} : \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Aut}(E[l](\overline{\mathbb{Q}_p}))$$

When $l \neq p$, $E[l](\mathbb{Q}_p)$, since $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acting on $E[l](\overline{\mathbb{Q}_p})$ componentwise, $E[l](\mathbb{Q}_p) \cong E[l](\mathbb{Q}_p)^{\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}$. So, $E[l](\mathbb{Q}_p)$ is an $\mathbb{F}_l$-subspace of $E[l](\overline{\mathbb{Q}_p})$. So,

$$E[l](\mathbb{Q}_p) \cong (\mathbb{Z}/l\mathbb{Z})^d, \quad d \in \{0, 1, 2\}$$

- When $d = 2$,
- When $d = 1$, $E[l](\mathbb{Q}_p)$ is a 1-dim subspace of $E[l](\overline{\mathbb{Q}_p})$, meaning that $\overline{\rho}_{E,l}\big|_{\overline{\mathbb{Q}_p}}$ is reducible.
- When $d = 0$, there is no non-trivial l-torsion point on $E[l](\mathbb{Q}_p)$.

When $l = p$, things get complicated.

3.4 Galois group representation: second encounter

Let $\overline{\rho}_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[l])$ be the mod-l Galois representation. From last chapter, we get some properties of the Galois group actions/ Galois representations. More properties are going to be derived:

Theorem 3.1: (Frey Serre)

The mod-l Galois representation is *absolutely irreducible*, *odd*, *unramified* outside $2l$ and *flat* at l.

Let $K/\mathbb{Q}$ be a number field extension. Let $\{\mathfrak{P}_i\}_i$ be the collection of prime ideals over a prime p(precisely speaking, over a prime ideal $\langle p\rangle$). There is an exact sequence

$$1 \longrightarrow I_{\mathfrak{P}_i|\langle p\rangle} \longrightarrow D_{\mathfrak{P}_i|\langle p\rangle} \longrightarrow \mathrm{Gal}(\mathfrak{k}_K/\mathfrak{k}_\mathbb{Q}) \longrightarrow 1$$

where $\mathfrak{k}_K$ and $\mathfrak{k}_\mathbb{Q}$ are residue field of K and $\mathbb{Q}$ respectively.
When K gets to the limit case, $\overline{\mathbb{Q}}$, then the above-mentioned exact sequence comes to

$$1 \longrightarrow I_p \longrightarrow D_p \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \longrightarrow 1$$

The case for $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ also bears a lot resemblence,

$$1 \longrightarrow I_p \longrightarrow D_p \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \longrightarrow 1$$

- $D_p \cong \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, because D_p is the image of the map $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- Some remarks on the map $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. First, $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p$. The residue field of $\mathbb{Q}_p$ is $\overline{\mathbb{F}_p}$ because *

For $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, it has a simplier characterisation of its structure: $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}} = \prod_l \mathbb{Z}_l$

- Studying I_p is a throny issue. The aid of next little sections is indispensible.

3.4.1 Maximal ramification extension of $\mathbb{Q}_p$

In this section, fix a local field K and let κ_K be its perfect residue field. There are two categories: $\mathscr{A}$ is the category of finite extension of K and $\mathscr{B}$ is the category of finite extension of κ_K. Then, there is a functor $F : \mathscr{A} \to \mathscr{B}$ sending

each $L \in \mathrm{Ob}(\mathscr{A})$ to its residue field κ_L

each K-linear map $f : L \to L'$ between two fintie unramified extensions of K to κ_K-linear map *

$$F(f) : \kappa_L \to \kappa_{L'} \quad x + \mathfrak{m}_L \to f(x) + \mathfrak{m}_{L'}$$

This comes from $f(\mathcal{O}_L) \subseteq \mathcal{O}_{L'}$ and $f(\mathfrak{m}_L) \subseteq \mathfrak{m}_{L'}$ (f is a local ring map), for $\forall y \in f(\mathcal{O}_L)$, $y = f(x)$ for some $x \in \mathcal{O}_L$, $v'(y) = (v' \circ f)(x) \overset{*}{=} v(x) \geq 0$, where v' is a valuation on L' and v is a valuation on L. $*$ comes from the uniqueness of valuation and $v' \circ f$ is a valuation on L. Similar argument for $\mathfrak{m}_L$ and $\mathfrak{m}_{L'}$. These two properties make this map well-defined.

Lemma 3.1 *The two categories, $\mathscr{A}$ and $\mathscr{B}$ are equivalent.*

Proof: This functor is essentially surjective and fully faithful:

Essentially surjective: $\forall$ finite extension κ/κ_K, there is a finite nuramified extension of K by the following construction. Since κ_K is perfect. From the primitive element theorem, there is an $\alpha \in \kappa$, such that $\kappa = \kappa_K[\alpha]$ with the minimal polynomial of α, $g(x) \in \kappa_K[x]$. Let $G(x) \in K[x]$ be a lift of $g(x)$. Local compactness of K implies it is complete. Hence, by the Hensel's lemma for complete DVR, α can be lifted to the unique root β of $G(x)$ in $\overline{K}$. Let $L := K(\beta)$. Then $\mathcal{O}_L/\mathfrak{m}_L = \kappa$?. Irreducibility of g implies the irreducibility of G, ?. Therefore, $[L : K] = \deg G = \deg g = [\kappa : \kappa_K]$.

Fully faithful: □

Now, the maximal unramified extension of $\mathbb{Q}_p$, denoted $\mathbb{Q}_p^{\text{ur}}$, is defined as $\mathbb{Q}_p^{\text{ur}} := \bigcup_{K/\mathbb{Q}_p \text{ finite, unramified}} K$.

The residue field of $\mathbb{Q}_p^{\text{ur}}$ is $\overline{\mathbb{F}_p}$. Moreover, $\text{Gal}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p) \cong \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. ? This can be used to characterise the I_p. Since $I_p = \ker\left(\text{Gal}(\overline{\mathbb{Q}_p}/Q_p) \to \text{Gal}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p)\right)$, I_p are the elements of morphisms between $\overline{\mathbb{Q}_p}$ fixing the field $\mathbb{Q}_p^{\text{ur}}$. Hence,

$$I_p \cong \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\text{ur}})$$

3.4.2 Finer decomposition of I_p

Let K/F be a finite Galois extension of local fields. $e := e(K/F)$ and $f := f(K/F)$. Then, we have $[K : F] = ef$. Hence,

$$|I_{K/F}| = \left|\frac{\text{Gal}(K/F)}{\text{Gal}(k_K/k_F)}\right| = \frac{[K : F]}{[k_K; k_F]} = e$$

the settings and theorem being used needs revised where e is the ramification degree of K/L. So, $I_{K/F}$ characterise the ramification of the extension K/L. There is a finer classification of the ramification depending on the interaction of e and p.

When $(e, p) = 1$, the ramification of K/F is called **tame rafication**.

When $(e, p) \neq 1$, i.e. $p|e$, the ramification of K/F is called **wild ramification**. If the base field $F = \mathbb{Q}_p$, this means the ramification conflicits with the p-adic structure. In this case, $|I_p|$ is finite. There exists a Sylow-p subgroup of $I_{K/F}$, denoted $P_{K/F}$. These groups form another short exact sequence:

$$1 \longrightarrow P_{K/F} \longrightarrow I_{K/F} \longrightarrow I_{K/F}\Big/P_{K/F} \longrightarrow 1$$

Taking them into limit cases, $P_p := \varinjlim_K P_{K/F}$ and $I_p := \varinjlim_K I_{K/F}$, and $I_p^{\text{tame}} := I_p/P_p$. The limit preserves the morphisms. Hence, a new exact sequence is

$$1 \longrightarrow P_p \longrightarrow I_p \longrightarrow I_p^{\text{tame}} \longrightarrow 1$$

By virtue of the structure of I_p in Galois group, $I_p \cong \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\text{ur}})$, and the structure theorem concrete theorem, I_p can be further decomposed into a short exact sequence:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\text{tame}}) & \longrightarrow & \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\text{ur}}) & \longrightarrow & \text{Gal}(\mathbb{Q}_p^{\text{tame}}/\mathbb{Q}_p^{\text{ur}}) & \longrightarrow & 1 \\
 & & \| & & \sim\big| & & \| & & \\
1 & \longrightarrow & P_p & \longrightarrow & I_p & \longrightarrow & I_p^{\text{tame}} & \longrightarrow & 1
\end{array}$$

where P_p is the pro-p subgroup which controls the wild ramification of what

I_p^{tame} is resiponsible for the tame ramification.

3.4.3 Ramification filtrations

From now on, the goal is to deeply understand the structure of those above-mentioned special groups. For $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the properties of $\mathbb{Q}$ are well-known and the extensions $K/\mathbb{Q}$ are studied well. However, the extension $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ seems more mysterious and we want to get more information on $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.
For $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, we have good news for both, but here we briefly follow the second path.
Ramification groups are 'simpler pieces'. More precisely, the ramification groups can be thought of as finer structure of inertia groups ([Tay02]). There is a continuous surjection

$$t : I_{\overline{\mathbb{Q}_p}} \twoheadrightarrow \prod_l \mathbb{Z}_l \qquad \text{s.t.} \quad \mathrm{Frob}_p \circ \sigma \circ \mathrm{Frob}_p^{-1} \mapsto p^{-1} t(\sigma)$$

The kernel $\ker t$ is a pro-p subgroup of $I_{\overline{\mathbb{Q}_p}}$, called the wild inertia subgroup of
The ramification groups G_i give a filtration of I has the following properties:

3.5 Level, weight and characters

3.5.1 Level

This basically comes from chapter 1 of [Ser03].

3.5.2 Weight

This basically comes from chapter 2 of [Ser03].

3.5.3 Characters

3.6 Conductors

In studying elliptic curves, we usually list the conductors of elliptic curves by a 'number', conductor.
Let K be a local field of residue characteristic $p > 0$ [3]. Let L/K be a finite Galois extension with normalized valuation (The setting follows [Sil94]) Let

- $I_{\overline{K}/K}$ be the absolute inertia group of K.
- $V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ be the Tate-l module
- $V_l(E)^{I_{\overline{K}/K}}$ be the subspace of $V_l(E)$ fixed by $I_{\overline{K}/K}$

Definition 3.8: Conductor for $\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve. The **conductor** of E, N_E is defined to be the product:

$$N_E = \prod_p p^{e_p}$$

where $e_p \neq 0$ only when the reduction of E at p is bad.
The exponent e_p is defined to be a sum of two parts: $e_p = \varepsilon_p + \delta_p$.

- ε_p is the tame parts, and
- δ_p is the wild part

Remark This comes from [Buh01]). In general, like for conductors for number field K, the conductor is defined to be product of ideals. As [Sil94] entrenched, the conductor $\mathfrak{f}_{E/K} := \prod_{\mathfrak{p}} \mathfrak{p}^{f_{E/K_{\mathfrak{p}}}}$. The definition here actually fits the general definition. Because we can think both sides as principal ideals in $\mathbb{Z}$,

$$(N) = \left(\prod_p p^{e_p} \right)$$

We can further write $\left(\prod_p p^{e_p}\right) = \prod_p (p)^{e_p} = \prod_{(p)} (p)^{e_p}$. For the last $=$, taking prime number is equivalent to taking prime ideals in $\mathbb{Z}$.

[3] This is always true. Since every local field is isomorphic to any one of the three cases: (1) $\mathbb{R}$ or $\mathbb{C}$, (2) finite extension K over $\mathbb{Q}_p$, (3) $\mathbb{F}_q((t))$, where $q = p^n$ For case (1), they do not have discrete valuation ring, so the concept does not apply here. For case (2), the DVR is the integral closure of $\mathbb{Z}_p$ in K. ?? For case (3), the DVR of $\mathbb{F}_q((t))$ is $\mathbb{F}_q[[t]]$ and the maximal ideal of this DVR is (t). $\mathbb{F}_q[[t]]/(t) \cong \mathbb{F}_q$

The smallest possible conductor is 11 ([Rib08]).
The most useful fact is that we can explicitly get the exponents of conductors, and they have very simple form.

Theorem 3.2: Explicit exponent conductor

$$\varepsilon_p := \begin{cases} 0 & E \text{ is a good reduction} \\ 1 & E \text{ is a multiplicative bad reduction} \\ 2 & E \text{ is an additive bad reduction} \end{cases}$$

If E/K

Example Compute the conductor of Frey-Hellegouarch's curve.

4 Serre's conjectures

4.1 Serre's modualrity conjecture

Definition 4.1: Modular Galois representations

An l-adic Galois representation ρ is **modular** (of weight k and level N) if there is a modular form $(f_q = \sum a_n q^n \in \mathcal{S}_k(\Gamma_1(N)))$ with $a_n \in \mathbb{Z}$ such that: $\forall$ prime $p \not| lN$,

$$\mathrm{tr}(\rho(\sigma_p)) = a_p$$

Definition 4.2: Odd representation

Now we are able to study the Galois representation of semi-stable elliptic curves:

Theorem 4.1: Invariants of semi-stable elliptic curves

$N(\rho_{E,p})$, $k(\rho_{E,p})$ and $\epsilon(\rho_{E,p})$ are given by:
(1) $N(\rho_{E,p}) = \prod_{l \neq p, \mathrm{ord}_l(\Delta_E) \not\equiv 0 \bmod p} l$
(2) $k(\rho_{E,p}) = \begin{cases} 2 & \mathrm{ord}_p(\Delta_E) = 0 \\ p+1 & \text{otherwise} \end{cases}$
(3) $\epsilon(\rho_{E,p}) = 1$

4.2 Serre's ϵ conjecture

Serre's ϵ conjectureepsilon Every irreducible modular Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ is modular. There is a more precise version of this conjecture that assigns an optimal weight and an optimal level to .
For the Frey's curve $E_{a,b,c}$, the optimal level is 2. But there are no modular forms of level 2 and weight 2 since

$$\dim \mathcal{S}_2(\Gamma_1(2)) = \dim \mathcal{S}_2(\Gamma_0(2)) = g(X_0(2))$$

Theorem 4.2: Ribet's level lowering theorem

Corollary 4.1: Non-modularity of Frey's curve

References

[Las82] Michael Laska. "An Algorithm for Finding a Minimal Weierstrass Equation for an Elliptic Curve". In: *Mathematics of Computation* 38.157 (1982), pp. 257–260. ISSN: 00255718, 10886842. URL: https://www.ams.org/journals/mcom/1982-38-157/S0025-5718-1982-0637305-2/S0025-5718-1982-0637305-2.pdf.

[Sil94] Joseph H. Silverman. "The Néron Model". In: *Advanced Topics in the Arithmetic of Elliptic Curves*. New York, NY: Springer New York, 1994, pp. 289–407. ISBN: 978-1-4612-0851-8. DOI: 10.1007/978-1-4612-0851-8_5. URL: https://doi.org/10.1007/978-1-4612-0851-8_5.

[Buh01] Joe P. Buhler. "Elliptic Curves, Modular Forms and Applications". In: *Arithmetic Algebraic Geometry*. Ed. by Karl Rubin Brian Conrad. Vol. 9. IAS/Park City Mathematics Series. Providence, RI: American Mathematical Society, 2001, pp. 60–62. ISBN: 978-0-8218-2173-3.

[Tay02] Richard L. Taylor. *Galois Representations*. Plenary lecture at the International Congress of Mathematicians. Beijing, China, August 20-28, 2002. 2002. URL: http://virtualmath1.stanford.edu/~rltaylor/longicm02.pdf.

[Ser03] Jean-Pierre Serre. *Représentations modulaires de Galois*. Lecture notes, Collège de France. 2003. URL: https://www.college-de-france.fr/media/jean-pierre-serre/UPL5835292064138487263_Serre_Repr.modulaires_Galois.pdf (visited on 08/20/2023).

[DS05] Fred Diamond and Jerry Shurman. "Galois Representations". In: *A First Course in Modular Forms*. New York, NY: Springer New York, 2005, pp. 371–411. ISBN: 978-0-387-27226-9. DOI: 10.1007/978-0-387-27226-9_9. URL: https://doi.org/10.1007/978-0-387-27226-9_9.

[Rib08] Kenneth A. Ribet. *Projective Arithmetic on Curves: Methods and Applications*. Technical Report. University of California, Berkeley, 2008. URL: https://math.berkeley.edu/~ribet/parc.pdf.

[Sil09] Joseph H. Silverman. "The Geometry of Elliptic Curves". In: *The Arithmetic of Elliptic Curves*. New York, NY: Springer New York, 2009, pp. 41–114. ISBN: 978-0-387-09494-6. DOI: 10.1007/978-0-387-09494-6_3. URL: https://doi.org/10.1007/978-0-387-09494-6_3.

[Sut13] Andrew Sutherland. *Supersingular Elliptic Curves in Cryptography*. Lecture Notes. Archived at MIT DSpace: http://hdl.handle.net/1721.1/97521. Massachusetts Institute of Technology, 2013. URL: https://dspace.mit.edu/bitstream/handle/1721.1/97521/18-783-spring-2013/contents/lecture-notes/MIT18_783S13_lec24.pdf.

[Mil20] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[Com22] Johan Commelin. *Good Reduction in Arithmetic Geometry*. Lecture notes, University of Regensburg. From the author's research notes on p-adic Hodge theory. 2022. URL: https://math.commelin.net/files/good_reduction.pdf (visited on 08/20/2023).

[Sut22] Andrew Sutherland. *Lecture 25: Isogeny Cryptography*. Course slides for 18.783 (Elliptic Curves), Massachusetts Institute of Technology. 2022. URL: https://math.mit.edu/classes/18.783/2022/LectureSlides25.pdf (visited on 08/20/2023).