The local anatomy of Frey's curves

Guo Haoyang

May 2025

Contents

1 Background and history

2 Construction of Frey's curves

3 Understanding the properties of Frey's curves

The Frey curve is defined on $\mathbb{Z}$, but it is actually defined on $\mathbb{P}^2$, on which coordinates in $\mathbb{Q}$ can be converted equivalently to coordaintes $\mathbb{Z}$. Another reason is, $E(\mathbb{Q})$ has more structure than $E(\mathbb{Z})$. The latter one is finite by Siegel's theorem.
Let's consider of the rational points of an elliptic curve E, $E(\mathbb{Q})$. This is an abelian group by the Mordell-Weil theorem. So, from the structure theorem of an abelian group,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \otimes E_{\text{tors}}(\mathbb{Q})$$

where r is the rank of E. Further, $E_{\text{tors}}(\mathbb{Q}) = \bigcup_{l\geq 1} E(\mathbb{Q})[l]$, where $E(\mathbb{Q})[l]$ is the collection of l-torsion points in $E(\mathbb{Q})$. This is the first parameter and l is always for the l-torsion points in the following contents.
The reason why $E(\mathbb{Q})[l]$ is more interesting than $E(\mathbb{Q})$ is probably because that the automorphisms between $E(\mathbb{Q})[l]$ is more abundant than the automorphisms between $E(\mathbb{Q})$. Usually, Aut((Q)) only has [1] and [−1]. Its order always divides 24 and is too small to arouse great interest.

3.1 Galois representation of a curve: Global information

From the structure of N-torsion points $E(K)[N]$ and $E(\overline{K})[N]$ of elliptic curves E/K: when $\text{char}K = 0$ or $\text{char}K > 0$ with $\text{char}K \not| N$, $E(\overline{K})[N] \cong \mathbb{Z}/N\mathbb{Z} \times Z/N\mathbb{Z}$. Galois groups $\text{Gal}(\overline{K}/K)$ permute the points in $E(K)$($E(K)[l]$ as well !!). This permutation can be regarded as an action(and indeed it is) on $E(K)$, especially on $E(K)[l]$. When $K = \mathbb{Q}$, consider $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
The action of $G_{\mathbb{Q}}$ on $E(\mathbb{Q})[l]$ is equivalent to the representation $G_{\mathbb{Q}} \to \text{Aut}(E(\mathbb{Q})[l])$. Usually, $E(\mathbb{Q})[l]$ is too small, and its structure is poor. Instead, we embeds this into $\text{Aut}(E(\overline{\mathbb{Q}})[l])$, i.e. $G_{\mathbb{Q}} \to \text{Aut}(E(\mathbb{Q})[l]) \hookrightarrow \text{Aut}(E(\overline{\mathbb{Q}})[l])$. So, this type of representation is called mod-l representation. [1]

Definition 3.1: mod-l Galois representations

Let $E/\mathbb{Q}$ be an Elliptic curve and l be an odd prime. Let $N = l^n$, some positive integer power of l. The **mod-N Galois representation** is defined as:

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

Remark Since $\text{char}\mathbb{Q} = 0$, the structure theorem of $E(\overline{\mathbb{Q}})[N]$ implies that

$$\text{Aut}(E(\overline{\mathbb{Q}})[l]) \cong \text{Aut}(\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}) \overset{\dagger}{\cong} \text{GL}_2(\mathbb{Z}/l\mathbb{Z}) \cong \text{GL}_2(\mathbb{F}_l), \quad \text{Aut}(E(\overline{\mathbb{Q}})[l^n]) \overset{\dagger}{\cong} \text{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$$

†: $\cong$ for both are up to choices of basis.

$l = 2?$.
To recover the information of $E(\mathbb{Q})[l]$,

$$E(\mathbb{Q})[l] = E(\overline{\mathbb{Q}})[l]^{G_{\mathbb{Q}}}$$

because all the rational points should be fixed by the Galois group $G_{\mathbb{Q}}$.

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 $T_l(E) := \varprojlim_n E(K)[l^n]$, the l-adic *Tate module*.
The Weierstrass uniformization theorem helps understanding the structure of l^n-torsion points $E(\mathbb{C})[l^n]$ and the

[1] Here mod-l does not mean the modular arithmetic on the coordinates, it just stress the representation is on the l-torsion points.

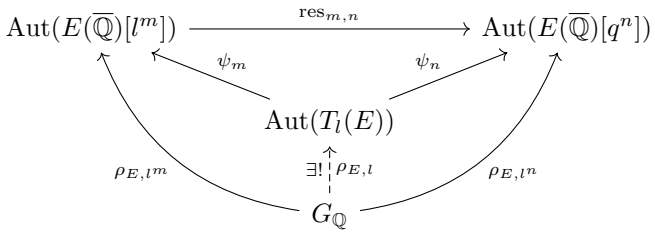
l-adic Tate modules $T_l(E)$:
Then, we get

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 This is well-defined because: first, $\mathrm{Aut}(E(\overline{\mathbb{Q}})[l^m]) \to \mathrm{Aut}(E(\overline{\mathbb{Q}}[l^n]$ by $\sigma \mapsto \sigma|_{E(\overline{Q})[l^n]}$ is a group homomorphism when $m > n$. Then, by the universal property of $T_l(E)$, change of lim and aut



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, $\mathrm{Aut}(T_l(E)) \cong \mathrm{Aut}(\mathbb{Z}_l \times \mathbb{Z}_l) \cong \mathrm{GL}_2(\mathbb{Z}_l)$.

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 $\widetilde{\rho}_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_l)$, as desired. The only drawback of this representation is it depends on some choices of $\mathbb{Q}_l$-basis. To avoid choosing basis, consider

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

3.2 Reduction of a curve: Local information

Minimal Weierstrass equation.
But, given a Weierstrass model(the coefficients are in the ring of integer of K), how do we know whether this is the minimal Weierstrass equation?
First of all, since the coefficients are in $\mathcal{O}(K)$, so Δ must also be in $\mathcal{O}(K)$. Namely, $v(\Delta) \geq 0$. If such an E is not minimal, then make a substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ with $u \in \mathcal{O}(K)$. The new form has coefficients $a_i' = u^{-i}a_i$ comparing to the coefficients before changing the variables. As a consequence, the discriminant after the substitution is $\Delta' = u^{-12}\Delta$. So, $v(\Delta') = v(\Delta) - 12v(u)$. This shows the $v(\Delta)$ decreases a multiple of 12 each time. So,

- $a_i \in \mathcal{O}(K)$ and $(0 \leq)v(\Delta) < 12$, then the equation is minimal.

For corresponding c_4' and c_6' in the new equation, since $c_4' = u^{-4}c_4$ and $c_6' = u^{-6}c_6$, we also have:

- $a_i \in \mathcal{O}(K)$ and $v(c_4) < 4$, then the equation is minimal.
- $a_i \in \mathcal{O}(K)$ and $v(c_6) < 6$, then the equation is minimal.

Generally, given an elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ in the Weierstrass form over $\mathbb{Q}$. Since $\mathbb{Q} \hookrightarrow \mathbb{Q}_q$, this E can be regarded as a curve over $\mathbb{Q}_q$ for every prime q. (Here, q is used to distinguish it from p in a Frey curve.) So, we change the perspective of view from a global field into a local one. $\mathbb{Q}_q$ is too abstract to operate.
But, $\mathbb{Q}_q$ has connection to $\mathbb{Z}_q$ and $\mathbb{F}_q$. Hensel's lemma gives us the motivation to manipulate something related to $\mathbb{Q}_q$: Finding a solution of a polynomial $f(x) \in \mathbb{Q}_q$. The Hensel's lemma allows us to first go down to $\mathbb{F}_q$ to find an approximate solution and then lift it to $\mathbb{Q}_q$ under a non-vanishing derivative condition. The reduction here is trying to do a geometric analogy of Hensel's lemma.
More generally, if E' is defined over a local field K, then by some substitution, the curve E' is a curve over the ring of integers $\mathcal{O}(K)$. !!

$$E'(K) \to \tilde{E}'(\kappa) \quad P \mapsto \tilde{P}$$

3.2.1 Type of reduction

Definition 3.3: Reduction Type

Let E/K be an elliptic curve over some local field K and $\tilde{E}$ be the reduction of E as above.
(1) E has a **good(or stable) reduction** $\Leftrightarrow$ $\tilde{E}$ is non-singular.
(2) E has a **bad(or semistable) reduction** of $E \Leftrightarrow \tilde{E}$ is singular.
(2.1) E has a **multiplicative(or semistable) reduction** $\Leftrightarrow \tilde{E}$ has a node.
(2.2) E has an **additive(or unstable) reduction** $\Leftrightarrow \tilde{E}$ has a cusp.

Direct calculation of reduction might be cumbersome. Here is an characterization for different reduction types:

Proposition 3.1: Characterization of reductions

Still, let E/K be a elliptic curve over a local field (e.g. $K = \mathbb{Q}_q$) with a minimal Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

The reduction type is characterized by Δ and c_4 [a] as follows:
(1) E has a good reduction $\Leftrightarrow v(\Delta) = 0$ (for $K = \mathbb{Q}_q$, this is $v_q(\Delta) = 0$). In this case, $\tilde{E}/\kappa$ is an elliptic curve.
(2) E has a multiplicative reduction $\Leftrightarrow v(\Delta) > 0$ and $v(c_4) = 0$. In this case, the non-singular part $\tilde{E}(\overline{\kappa})_{\text{ns}} \cong \overline{\kappa}^{\times}$ is a multiplicative group.
(3) E has an additive reduction $\Leftrightarrow v(\Delta) > 0$ and $v(c_4) > 0$. In this case, the non-singular part $\tilde{E}(\overline{\kappa})_{\text{ns}} \cong \overline{\kappa}^{+}$ is an additive group.

[a] $c_4 = b_2^2 - 24b_4$ and $b_2 = a_1^2 - 4a_2$, $b_4 = a_1a_3 + 2a_4$

Remark Let $\mathcal{O}(K)$ be the ring of integer of K and $\mathfrak{m}$ be the unique maximal ideal of $\mathcal{O}(K)$. Then, $v(\Delta) = 0 \Leftrightarrow \Delta \in \mathcal{O}(K)^{\times}$ is a unit, and $v(\Delta) > 0 \Leftrightarrow \Delta \in \mathfrak{m}$.
For $K = \mathbb{Q}_q$, this corollary can be illustrated by the following diagram:

Reduction types	Conditions	Group structures
Good reduction	$\Delta \in (\mathbb{Z}_q)^{\times}, \Leftrightarrow q \not\mid \Delta$	$\tilde{E}/\mathbb{F}_q$ is an elliptic curve
Multiplicative reduction	$\Delta \in q\mathbb{Z}_q, c_4 \in (\mathbb{Z}_q)^{\times}, \Leftrightarrow q \mid \Delta$ and $q \not\mid c_4$	$\tilde{E}(\overline{\mathbb{F}_q})_{\text{ns}} \cong \overline{\mathbb{F}_q}^{\times}$ is a multiplicative group
Additive reduction	$\Delta, c_4 \in q\mathbb{Z}_q, \Leftrightarrow q \mid \Delta$ and $q \mid c_4$	$\tilde{E}(\overline{\mathbb{F}_q})_{\text{ns}} \cong \overline{\mathbb{F}_q}^{+}$ is an additive group

Now let's try to apply these criteria to For Frey curve of the form $E : y^2 = x(x - a^p)(x + b^p)$ and get the reduction type at different prime q. This curve has

$$\Delta = 16(abc)^{2p} \qquad c_4 = 16(a^{2p} + a^pb^p + b^{2p})$$

As this corollary suggests, first E should be converted into the minimal model. Here is the minimality check by virtue of the criteria mentioned above:
Suppose $q \neq 2$ at first. This separates the influence of 2 in Δ and c_4 apart. So, there are two cases for the prime q(now q is odd), $q \not\mid abc$ and $q \mid abc$.

- When $q \not\mid abc$, $v_q(\Delta) = 0 < 12$. E is minimal.
- When $q \mid abc$, by assumption Where, a, b, c are coprime. So, q cannot divide a and b at the same time. Hence, $v_q(c_4) = v_q(a^{2p} + a^pb^p + b^{2p}) \leq \min\{v_q(a^{2p}), v_q(a^pb^p), v_q(b^{2p})\} = 0$, implying that $v_q(c_4) = 0$. So, E is minimal as well.

For $q = 2$, usually E is not the minimal one, for $v_2(\Delta) = 4 + 2p \cdot v_2(abc)$ is usually very large. A minimal model might have the form

$$y^2 + xy = x^3 + \cdots$$

When $q \neq 2$, the minimality checks yields that E is already the minimal Weierstrass form, which gives more convenience to stuy the reduction E module a prime q, for $\Delta^{\min} = \Delta$ and $c_4^{\min} = c_4$:
Split the cases into $q \not\mid abc$ and $q \mid abc$.
(1.1) When $q \not\mid abc$, $q \not\mid \Delta$. $v_q(\Delta) = 0$, so the reduced curve $\tilde{E}$ is good.

(1.2) When $q|abc$, $q|\Delta$. The above-mentioned analysis also applies here: $v_q(c_4) = 0$, so the reduction is multiplicative. When $q = 2$, E also has multiplicative reduction [**darmon1995fermat**].

3.2.2 Reduction over $\mathbb{Q}$

Back to the $K = \mathbb{Q}_q$ cases, as a curve over $\mathbb{Q}_q$, the reduction step first map it to $\mathcal{O}(\mathbb{Q}_q) = \mathbb{Z}_q$ and then goes to the residue field $\mathbb{F}_q \cong \mathbb{Z}_q/q\mathbb{Z}_q$. First, as a consequence of changing perspective, the l-torsion points, $E(\mathbb{Q}_q)[l]$ over different q, may have new information: the natural inclusion

$$E(\mathbb{Q})[l] \hookrightarrow E(\mathbb{Q}_q)[l]$$

might have some l-torsion points that are not rational. The change of perspective also brings some new problem. Second, module the coefficients of $E(\mathbb{Q}_q)$ by q, to get the reduced elliptic curve $\tilde{E}(\mathbb{F}_q)$:

$$E(\mathbb{Q}_q) \to \tilde{E}(\mathbb{F}_q) \overset{\text{induces}}{\Rightarrow} E(\mathbb{Q}_q)[l] \to \tilde{E}(\mathbb{F}_q)[l]$$

The bottleneck on the understanding of the 'local behavior' of the l-torsion point $\tilde{E}(\mathbb{F}_q)[l]$ is the entanglement between q (arithmetic) and l (geometry).

- When $l \neq q$, the reduction map

$$E(\mathbb{Q}_q)[l] \to \tilde{E}(\mathbb{F}_q)[l]$$

is an injection. This is good, because all information of $E(\mathbb{Q}_q)[l]$ is faithfully reflected by $\tilde{E}(\mathbb{F}_q)[l]$, which apparently has a simpler structure than $E(\mathbb{Q}_q)[l]$.
- While $l = q$, the reduction map $E(\mathbb{Q}_q)[l] \to \tilde{E}(\mathbb{F}_q)[l]$ has non-trivial kernel.

To have a geometric intuition for what happened. We need the notion of distance between two points on an elliptic curve over $\mathbb{Q}_q$. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be the Weierstrass form defined over $\mathbb{Q}_q$. Let $t = -\frac{x}{y}$ and define

$$E_n(\mathbb{Q}_q) := \{P \in E(\mathbb{Q}_q) : v_q(t(P)) \geq n\} \cup \{O\}$$

$E_n(\mathbb{Q}_q)$ is the 'disk' with the radius p^{-n}. The sequence of $E_n(\mathbb{Q}_q)$ forms a filtration.

$$E_0(\mathbb{Q}_q) \supseteq E_1(\mathbb{Q}_q) \supseteq E_2(\mathbb{Q}_q) \supseteq \cdots$$

The norm of a point $P \neq O$ is defined to be

$$\|P\| := p^{-v_q(t(P))}$$

The distance of two points P and Q is defined to be

$$d(P, Q) := p^{-v_q(t(P-Q))}$$

By virtue of the distance defined here, there are two examples for $l \neq q$ and $l = q$ showing the intuition of what is happening:

Example (1) ($l \neq q$) $E : y^2 = x^3 - x^2$ over $\mathbb{Q}_5$. Consider the 2-torsion points, $E(\mathbb{Q}_5)[2]$.
Since all 2-torsion points P satisfying $P + P = O$, P has the coordinate $[x : y : 1]$ (or the affine form (x, y)) with $y = 0$. The solution of $x^3 - x^2 = 0$ over $\mathbb{Q}_5$ is $0, \pm 1$. Hence, $E(\mathbb{Q}_5)[2] = \{(0, 0), (\pm 1, 0)\}$.
Let $P = (0, 0)$, $Q = (-1, 0)$ and $R = (1, 0)$. The above-defined distance yields that

$$\|P\| = \|Q\| = \|R\| = d(P, Q) = d(P, R) = d(Q, R) = p^0 = 1$$

which means that not only these points have a certain large distance from O, but they also keep some distance from each other.
(2) ($l = q$) $E : y^2 = x^3 + x^2$ In the first example, when $l \neq q$, the points in $E(\mathbb{Q}_q)[l]$ are very far from each other and from the O. So, they do not merge together after the reduction. In the second example, when $l = q$, the points in $E(\mathbb{Q}_q)[l]$ cluster around O. These points merge after the reduction map, and this is the reason why the situation gets complicated. To know the delicate behavior near O, we need a method to stretch those points apart.

This situation also happens in the Hensel's lemma. Hensel's lemma require the $l \neq q$. Otherwise, it fails to get a solution. !!
So, we need some sort of probe to test each cases. The probe is the Galois group action. More precisely, the action of some subgroups of Galois group.

3.3 Studying local information: decomposing Galois groups

From now on, we have three parameters, l for l-**torsion points**, p from **the Frey curve** $y^2 = x(x-a^p)(x+b^p)$, and q a prime number for **the local field** $\mathbb{Q}_q$.
The absolute Galois group is so big that little information on it has been known yet. But, one can decompose it into small groups to study how those little pieces acting on the l-torsion points, either $E(\mathbb{Q})[l]$ or $\tilde{E}(\mathbb{F}_q)[l]$. $E(\mathbb{Q})[l]$ can be viewed as a subgroup of $E(\mathbb{Q}_q)[l]$. This does not mean that $\mathrm{Aut}(E(\mathbb{Q})[l])$ can be embedded as a subgroup of $\mathrm{Aut}(E(\mathbb{Q}_q)[l])$, nor as a restriction.
More than this problem, the absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}}$, cannot even act on $E(\mathbb{Q}_q)[l]$. Even though the coordinates of points in $E(\mathbb{Q}_q)[l]$ are in $\overline{\mathbb{Q}}$ (since those points are on the l-th cyclotomic polynomials of E, ψ_l.), the elements $\sigma \in G_{\mathbb{Q}}$ might send P outside $E(\mathbb{Q}_q)$.
To mimic the action of $G_{\mathbb{Q}}$ on $E(\overline{\mathbb{Q}})[l]$, a counterpart for $E(\overline{\mathbb{Q}_q})[l]$ can be chosen to $G_{\mathbb{Q}_q} = \mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q)$. This action $G_{\mathbb{Q}_q} \curvearrowright E(\overline{\mathbb{Q}_q})[l]$ can be packed into the representation

$$\overline{\rho}_{E,l,q} : G_{\mathbb{Q}_q} \to \mathrm{Aut}(E(\overline{\mathbb{Q}_q})[l])$$

As before,$E(\overline{\mathbb{Q}_q})[l] \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ and $\mathbb{Q}_q = \overline{\mathbb{Q}_q}^{G_{\mathbb{Q}_q}}$ implies that $E(\mathbb{Q}_q)[l] = E(\overline{\mathbb{Q}_q})[l]^{G_{\mathbb{Q}_q}}$. Hence, no matter $l \neq q$ or $l = q$, $E(\mathbb{Q}_q)[l]$ is always an invariant $\mathbb{F}_l$-subspace of $(\mathbb{Z}/l\mathbb{Z})^2$. So,

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

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

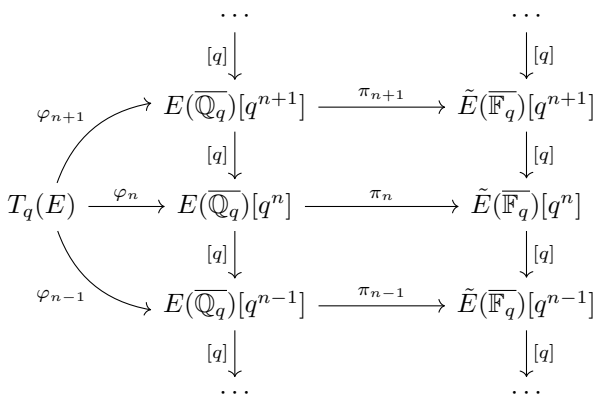
For $\tilde{E}(\mathbb{F}_q)[l]$, the corresponding Galois group action is $G_{\mathbb{F}_q} \curvearrowright \tilde{E}(\mathbb{F}_q)[l]$. We study a similar representation

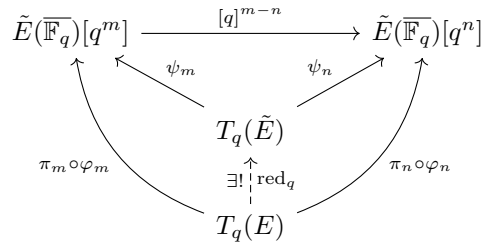
$$\overline{\rho}_{E,l,q} : G_q \to \mathrm{Aut}(\tilde{E}(\overline{\mathbb{F}_q})[l])$$

and have similar $E(\mathbb{Q}_q)[l] = E(\overline{\mathbb{Q}_q})[l]^{G_{\mathbb{Q}_q}}$. But, the situation diverges for $l \neq q$ and $l = q$. When $l \neq q$, $\tilde{E}(\overline{\mathbb{F}_q})[l] \cong (\mathbb{Z}/l\mathbb{Z})^2$ and the analysis for $\tilde{E}(\mathbb{F}_q)[l]$ is the same as $E(\mathbb{Q}_q)[l]$. This can be derived directly from the fact that the reduction map is an isomorphism. But, for $l = q$, since $q|l$, the structure theorem fails.

$T_l(E) = \varprojlim_n E(\mathbb{Q}_q)[l^n]$.
The goal is to recover $E(\mathbb{Q}_q)$ from $\tilde{E}(\mathbb{F}_q)$ when $l = q$. ? The reduction map $\pi : E(\mathbb{Q}_q) \twoheadrightarrow \tilde{E}(\mathbb{F}_q)$ induces many maps on each q^n- torsion points,

$$\pi_1 : E(\overline{\mathbb{Q}_q})[q] \twoheadrightarrow \tilde{E}(\overline{\mathbb{F}_q})[q], \ldots, \pi_n : E(\overline{\mathbb{Q}_q})[q^n] \twoheadrightarrow \tilde{E}(\overline{\mathbb{F}_q})[q^n], \ldots$$





By the universal property of $T_q(\tilde{E})$ (the right hand side), there is a unique surjective map $\mathrm{red}_q : T_q(E) \twoheadrightarrow T_q(\tilde{E})$. The kernel of this red_q encodes all lost information for each reduction map π_n. So, to know the structure of $T_q(E)$, it suffices to know this kernel. All these parts can be formed into a short exact sequence:

$$0 \longrightarrow \ker \mathrm{red}_q \longrightarrow T_q(E) \longrightarrow T_q(\tilde{E}) \longrightarrow 0$$

skip to Galois representation
Analogous to the definition 3.2, here are two well-defined $G_{\mathbb{Q}_q}$ representation sof $T_q(E)$,

$$\rho_{E/\mathbb{Q}_q,q} : G_{\mathbb{Q}_q} \to \mathrm{Aut}(T_q(E)) \qquad \rho_{\tilde{E}/\mathbb{F}_q,q} : G_{\mathbb{F}_q} \to \mathrm{Aut}(T_q(\tilde{E}))$$

There is an induced map $\mathrm{Aut}(T_q(E)) \to \mathrm{Aut}(T_q(\tilde{E}))$, because $E(\overline{\mathbb{Q}_q})[q^n] \to E(\overline{\mathbb{F}_q})[q^n]$ induces $\mathrm{Aut}(E(\overline{\mathbb{Q}_q})[q^n]) \to \mathrm{Aut}(E(\overline{\mathbb{F}_q})[q^n])$ and Aut is interchangable with the inverse limit. Further, there is a commutative diagram of group homomorphisms:

$$\begin{array}{ccc} G_{\mathbb{Q}_q} & \twoheadrightarrow & G_{\mathbb{F}_q} \\ \downarrow{\scriptstyle \rho_{E/\mathbb{Q}_q,q}} & & \downarrow{\scriptstyle \rho_{E/\mathbb{F}_q,q}} \\ \mathrm{Aut}(T_q(E)) & \twoheadrightarrow & \mathrm{Aut}(T_q(\tilde{E})) \end{array}$$

construct the above morphisms.
This diagram also enlighten us: the property of the following Tate-q module can be converted to the property of the morphism between absolute Galois groups.
Since $T_q(E)$ is a $\mathbb{Z}_q$-module (or consider the $\mathbb{Q}_q$ vector space $T_q(E) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$), all tools in representation theory can be applied (such as trace, determinant).

3.3.1 Group structures

Now our goal turns to study the action $G_{\mathbb{Q}_q}$ on $T_q(E)$ by decomposing $G_{\mathbb{Q}_q}$ and observing how those small pieces of $G_{\mathbb{Q}_q}$ determine the behavior of $T_q(E)$.
Following the decomposition of $G_{\mathbb{Q}_q} \twoheadrightarrow G_{\mathbb{F}_q}$, there is a short exact sequence

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

• $D_p \cong \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, 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: $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}} = \prod_l \mathbb{Z}_l$ because
• Studying I_p is a throny issue. The aid of next little sections is indispensible.

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

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

3.3.3 Group structure: 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,

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

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 $I_p^{\mathrm{tame}} := I_p/P_p$. The limit preserves the morphisms. Hence, a new exact sequence is

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

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

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

where P_p is the pro-p subgroup which controls the wild ramification of what
I_p^{tame} is responsible for the tame ramification.

3.3.4 Group structure: 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:

3.3.5 Representation information

Theorem 3.1: Néron-Ogg-Shafarevich criterion($\mathbb{Q}_q$ version)

Let $E/\mathbb{Q}_q$ be an elliptic curve and l be a prime not dividing the characteristic of the residue field of $\mathbb{Q}_q$, i.e. q. Then, $E(\mathbb{Q}_q)$ has a good reduction $\Leftrightarrow$ the l-adic Tate module is unramified.

Remark This criterion characterizes the reduction type by the arithmetic properties what, and Tate module ramified?.

Proof: □

3.4 The equivalency among all different perspectives

3.5 From local to global

In the previous few sections, we examined an elliptic curve E over a global field $\mathbb{Q}$ on different q. More precisely, we tried to embed $E/\mathbb{Q}$ to different $\mathbb{Q}_q$ as $E/\mathbb{Q}_q$ and then reduce them to different $_q$. The perspective goes from global to local. After each piece of information has been collected locally at q, we tries to glue them together. This collection should only care about the 'bad information', for the good reductions of each $E(\mathbb{Q}_q)$ are locally (at each q) as good as the $E(\mathbb{Q}_q)$. More precisely, for those good reductions, $E(\mathbb{Q}_q) \cong \tilde{E}(\mathbb{F}_q)$, so there is no information loss and we do not need to care this q so much. What we only need to care is those primes q that $\tilde{E}(\mathbb{F}_q)$ has singularities. To reflect how bad q is, a little distinguishing should be put between multiplicatively bad and additively bad. For the multiplicative cases and the additive cases, put a weight 1 on the power and a weight 2 on the power, respectively. For the good reduction case, the weight should be 0 to remove the influence on the global information. Since we want q^0 'acts' trivially on the global information, the way of 'gluing' should be simply the product of different q to the power of its 'weight'. This product is called the *conductor* of what?

4 Visualizing Frey's curves

In this section, we try to put Frey's curves on different fields to see what strange things might happen.
First, let's embed E on $\mathbb{R}$ (corresponding to the completion with respect to $|\cdot|_\infty$):
Then, let's do this embedding on $\mathbb{Q}_q$ for some prime q. This case is harder because $\mathbb{Q}_q$ is strange (totally disconnected and not well-ordered).
The uniformization theorem (actually, its corollary) provides a way to visualize an elliptic curve, $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Is there a counterpart of this in the q-adic field $\mathbb{Q}_q$. Naturally, one might guess that $E(\mathbb{Q}_q) \cong \mathbb{Q}_q/\Lambda$ and find a lattice $\Lambda = \mathbb{Z}_q\nu_1 + \mathbb{Z}_q\nu_2$. But, this is impossible because .
Tate raised a fresh perspective of $E(\mathbb{C})$. Viewing $E(\mathbb{C})$ as a plane module a lattice relies on addition. It is also possible to regard it as something in multiplication using the exponential map

$$\exp : \mathbb{C} \to \mathbb{C} \quad z \mapsto e^{2\pi i z}$$

Uniformizing the Under this map, the lattice Λ has the form $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\tau \notin \mathbb{R}$. Let $q := e^{2\pi i \tau}$. Since exp is a group homomorphism,

$$n_1 + n_2\tau \mapsto e^{2\pi i(n_1 + n_2\tau)} = e^{2\pi i n_1} \cdot e^{2\pi i n_2 \tau} = e^{2\pi i n_2 \tau}$$

Λ is mapped to the $\{e^{2\pi i n\tau} : n \in \mathbb{Z}\} =: q^{\mathbb{Z}}$.
Another visualization of $\mathbb{Q}_q$ is the Bruhat-Tits tree [Mor13].

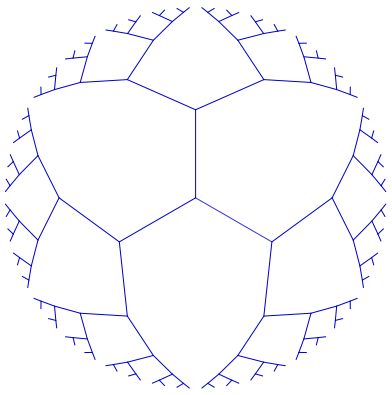


Figure 1: Bruhat-Tits Tree for $\mathrm{PGL}_2(\mathbb{Q}_q)$, $q = 2$

5 Some examples

References

[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.

[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.

[Mor13] Dave Witte Morris. *Introduction to Bruhat-Tits Buildings*. Lecture notes from the University of Chicago. Oct. 2013. URL: https://deductivepress.ca/dmorris/talks/BruhatTits.pdf.