Fermat's Last Theorem

Lecture II

Nuno Freitas

Second Portuguese number theory meeting

4 – 8 Sep 2023

Recap from Lecture I

Motivation

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^n + y^n + z^n = 0, \qquad a, b, c \in \mathbb{Z}, \qquad n \geq 3$$

satisfy $abc = 0$.

Theorem (Wiles, Taylor–Wiles)

All semistable elliptic curves over $\mathbb{Q}$ are modular.

Weierstrass equations

Elliptic curves are a special kind of plane cubic curves, which are commonly described using Weierstrass equations.

Definition

An **elliptic curve** *E defined over a field K is a* **non-singular** *plane cubic given by an equation of the form*

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

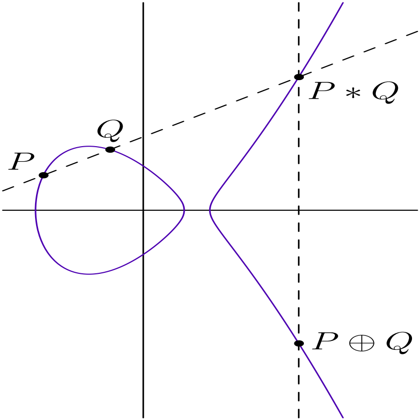
where $a_1, a_2, a_3, a_4, a_6 \in K$. This is a **Weierstrass equation***.*

The homogenisation of E is

$$Y^2Z + a_1XYZ + a_3YZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and its **unique** point at infinity is $\infty = [0 : 1 : 0]$.

The group law



Theorem

Let E be an elliptic curve defined over a field K. Then, $E(\overline{K})$ is an abelian group under the operation $\oplus$, with identity $\infty = [0 : 1 : 0]$.

The Mordell-Weil theorem

Theorem (Mordell-Weil)

Let $E/\mathbb{Q}$ be an elliptic curve.

Then the abelian group $E(\mathbb{Q})$ is finitely generated, *i.e.,*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

where $r \geq 0$ is the **rank** *of $E(\mathbb{Q})$, and $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.*

Question: Does this mean that in practice we can determined $E(\mathbb{Q})$? By "determine" we mean find the abstract group structure, *i.e.* find the structure of $E(\mathbb{Q})_{\mathrm{tors}}$ and r.

We will start by studying the torsion part $E(\mathbb{Q})_{\mathrm{tors}}$.

Torsion subgroup: The Lutz-Nagell Theorem

We have an easy process to compute points of order 2.

How about points of finite order > 2 ?

Theorem (Lutz-Nagell)

Let E over $\mathbb{Q}$ be an elliptic curve given by an **integral** *short Weierstrass equation*

$$Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{Z}, \quad \Delta = -4A^3 - 27B^2$$

If $P = (x, y) \in E(\mathbb{Q})$ has **finite order***, then*

1. *the coordinates $x, y \in \mathbb{Z}$, and*
2. *either $y = 0$ or $y^2 \mid \Delta_E$.*

Corollary

The torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.

Torsion subgroup: The Lutz-Nagell Theorem

Example

Consider $E : Y^2 = X^3 + 4$ satisfying $\Delta = -27(4)^2 = -3(12)^2$.

If $P = (x, y)$ has finite order then, either $y = 0$ or $|y| \mid 12$, hence

$$y \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}.$$

$\lvert y \rvert$	0	1	2	3	4	6	12
y^2	0	1	4	9	16	36	144
$y^2 - 4$	-4	-3	0	5	12	32	140
x	–	–	0	–	–	–	–

So the only two possibilities are $P = (0, 2)$ or $-P = (0, -2)$.

One checks $2P = -P$ so P has order 3 (the line $y = 2$ intersects E at P with multiplicity 3, so $P + P + P = 0$).

Torsion subgroup: The Lutz-Nagell theorem

Example

Let E be given by $Y^2 = X^3 + 8$, with $\Delta = -27 \cdot 8^2 = -3(24)^2$.

If $P = (x, y)$ has finite order then $y = 0$ or $|y| \mid 24$.

$\|y\|$	0	1	2	3	4	6	12	24
y^2	0	1	4	9	16	36	144	576
$y^2 - 8$	-8	-7	-4	1	8	28	136	568
x	-2	–	–	1	2	–	–	–

For $y = 0$, one gets $T = (-2, 0)$ which has order 2.

For $y = 3$, we get $P = (1, 3)$ satisfying $2P = (-7/4, -13/8)$.

Since $2P$ is **not** integral, it **cannot** have finite order.

For $y = 4$, we get $Q = (2, 4)$ yielding $2Q = (-7/4, 13/8) = -2P$, hence Q is **not** of finite order.

Reduction modulo p

Reduction mod p

Consider an elliptic curve $E/\mathbb{Q}$ given by an integral short Weierstrass equation

$$E \;:\; Y^2 = X^3 + AX + B, \qquad A, B \in \mathbb{Z}.$$

We can reduce the coefficients A, B modulo p to get a curve

$$\overline{E} : Y^2 = X^3 + \overline{A}X + \overline{B}, \qquad \overline{A}, \overline{B} \in \mathbb{F}_p.$$

This may be a **singular** curve and not an elliptic curve.

Reduction mod p

Example

Let $E/\mathbb{Q}$ be the curve

$$Y^2 = X^3 + 20, \qquad \Delta_E = -2^8 3^3 5^2$$

(a) Let $p = 7$. The reduced curve is the elliptic curve

$$E/\mathbb{F}_7 : Y^2 = X^3 + 6$$

(b) Let $p = 5$. The reduced curve is the singular curve

$$E/\mathbb{F}_5 : Y^2 = X^3$$

(c) Let $p = 3$. The reduced curve is the singular curve

$$E/\mathbb{F}_3 : Y^2 = X^3 - 1 = (X - 1)^3$$

Reduction mod p

Fortunately, getting singular curves after reduction happens only for **finitely** many primes.

Lemma

Let $E/\mathbb{Q}$ be an elliptic curve given by an **integral** *equation $Y^2 = X^3 + AX + B$. Then for all primes $p \nmid \Delta_E$, the reduced curve $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$.*

Proof.

The discriminant $\Delta_E = -16(4A^3 + 27B^2) \in \mathbb{Z}$ is non-zero.

The discriminant of $\overline{E}$ is $\Delta_{\overline{E}} = \Delta_E \pmod{p}$ which is $0 \in \mathbb{F}_p$ if and only if $p \mid \Delta_E$.

Therefore, for all $p \nmid \Delta_E$ we have that $\overline{E}$ is an elliptic curve. □

Reduction mod p

Definition

Let $E/\mathbb{Q}$ be an elliptic curve given by an **integral** *model.*
Let p be a prime.

We say that E has **good reduction at p** *if $p \nmid \Delta_E$.*
If $E/\mathbb{Q}$ is given by a **minimal** *model (i.e. $|\Delta_E|$ minimal) and it does not have good reduction at p, then it has* **bad reduction** *at p.*

Example

(1) Let $n \geq 1$ be an integer, and $E_n : Y^2 = X^3 - n^2 X$ the congruent number curve associated to n.

The discriminant of E_n is $\Delta = 64n^6$. Therefore E has good reduction at p for all prime $p \nmid 2n$.

(2) The curve $E : Y^2 = X^3 + c$, with $c \in \mathbb{Z}$ has discriminant $\Delta = -2^4 3^3 c^2$. So it has good reduction at p if $p \nmid 6c$.

Reduction mod p

"Definition"

- The **conductor** N_E of E measures the arithmetic complexity of E; we compute it using Tate's algorithm;
- E has **multiplicative reduction** at p if and only if $p \| N_E$.
- E has **additive reduction** at p if and only if $p^2 \mid N_E$.
- A prime p is **a prime of good reduction** when $p \nmid N_E$.
- We say that E is **semistable** if N_E is squarefree, i.e., all primes of bad reduction are of multiplicative reduction.

Reduction mod p

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve, and p a prime of **good reduction***. Then there is a well defined reduction map*

$$r_p : E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$$
$$P \mapsto \overline{P}$$

which is a group homomorphism whose kernel does not contain points with rational coordinates. Furthermore, r_p **is injective on torsion points***, i.e.,*

$$\ker(r_p) \cap E(\mathbb{Q})_{\mathrm{tors}} = \{\infty\}.$$

In particular,

$$\#E(\mathbb{Q})_{\mathrm{tors}} \mid \#\overline{E}(\mathbb{F}_p).$$

Reduction mod p

Example

Let $E : Y^2 = X^3 + 4$, with $\Delta = -432 = -2^4 \cdot 3^3$. Then E has good reduction at any prime $p \geq 5$.

Reduction mod 5 gives $\overline{E} : Y^2 = X^3 - 1$.

x	0	1	-1	2	-2
x^3	0	1	-1	-2	2
$x^3 - 1$	-1	0	-2	2	1
y	± 2	0	$-$	$-$	± 1

$$\overline{E}(\mathbb{F}_5) = \{\infty, (1,0), (0, \pm 2), (-2, \pm 1)\}.$$

So $\#\overline{E}(\mathbb{F}_5) = 6$, hence $\#E(\mathbb{Q})_{\text{tors}} = 1, 2, 3$ or 6.

We see there are no points of order 2.

We already know $P = (0, 2)$ has order 3.

So $E(\mathbb{Q})_{\text{tors}}$ is a group of order 3 generated by P.

Reduction mod p

Example

Let $E : Y^2 = X^3 + 8$, with $\Delta = -27 \cdot 8^2$. Then E has good reduction at all primes $p \geq 5$.

The point $T = (-2, 0)$ is a 2-torsion point on E.

For the prime $p = 5$, we find

$$\overline{E}_5(\mathbb{F}_5) = \{\infty, (1, \pm 2), (2, \pm 1), (-2, 0)\}.$$

So $\#\overline{E}_5(\mathbb{F}_5) = 6$ and $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 6$.
Since $\#E(\mathbb{Q})_{\mathrm{tors}}$ is a multiple of 2, it must be 2 or 6.

Looking at other primes, we find

- $p = 7 \rightsquigarrow \#\overline{E}_7(\mathbb{F}_7) = 12$, **no information** *as* $6 \mid 12$;
- $p = 11 \rightsquigarrow \#\overline{E}_{11}(\mathbb{F}_{11}) = 12$, **no information** *as* $6 \mid 12$;
- $p = 13 \rightsquigarrow \#\overline{E}_{13}(\mathbb{F}_{13}) = 16$; *since* $6 \nmid 16$ *it follows that* $E(\mathbb{Q})_{\mathrm{tors}} = \langle T \rangle$ *has order 2.*

Reduction mod p

Example

Let E be the curve given by $Y^2 = X^3 + 18X + 72$ satisfying

$$\Delta = -4(18)^3 - 27(72)^2 = -2^5 \cdot 3^3 \cdot 7 = -(2^2 3)^2 (2 \cdot 7)$$

Using Lutz-Nagell's Theorem to look for torsion points would require us to check 13 values of y.

Instead, we use reduction mod 5 and 11, obtaining

$$\#\overline{E}_5(\mathbb{F}_5) = 5 \quad \#\overline{E}_{11}(\mathbb{F}_{11}) = 8,$$

which implies that

$$E(\mathbb{Q})_{\mathrm{tors}} = \{\infty\}.$$

Torsion subgroup : Mazur theorem

Theorem (Mazur)

The only possible torsion subgroups of $E(\mathbb{Q})$ are

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & \text{for } 1 \leq n \leq 10 \text{ and } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} & \text{for } 1 \leq n \leq 4. \end{array}$$

The Birch and Swinnerton-Dyer Conjecture (BSD)

The Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$.

The Mordell-Weil Theorem asserts that $E(\mathbb{Q})$ is finitely generated.

More precisely,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r,$$

where r is the rank of E.

Question: Does this mean that in practice we can determined $E(\mathbb{Q})$? By "determine" we mean find the abstract group structure, *i.e.* **find the structure of $E(\mathbb{Q})_{\mathrm{tors}}$ and r.**

The torsion subgroup can be computed thanks to the result of Mazur, combined with the Lutz-Nagell Theorem.

The rank r, however, remains **highly** mysterious.

The Birch and Swinnerton-Dyer Conjecture

For example, it is unclear whether given a positive integer r there exists a curve E such that $\mathrm{rank}(E) = r$.

The experts opinion on this has not been constant over the years.

Recent work due to Park–Poonen–Voight–Wood conjectures that the possible set of ranks is bounded and that there are only finitely many E with rank above 21.

The **highest established** rank known to date is 20. It belongs to a curve discovered by Elkies-Klagsbrun in 2020.

The current record is a curve with rank at least 28 due to Elkies, but this is proved only **conditionally** to the Generalized Riemman Hipothesis.

Since the mid 60s, much effort has gone into understanding ranks of elliptic curves, leading to one of the most influential conjectures in number theory, namely the **Birch and Swinnerton-Dyer Conjecture.**

The Birch and Swinnerton-Dyer Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve with discriminant Δ_E

Let p be a prime.

Let $\overline{E}_p$ be the reduction of E modulo p.

If p is a prime of **good** reduction, $\overline{E}_p$ is an elliptic curve over $\mathbb{F}_p$.

In that case, we define the **trace of Frobenius at p** by

$$a_p = p + 1 - \#\overline{E}_p(\mathbb{F}_p).$$

Theorem (Hasse's Inequality)

Let $q = p^k$ be a prime power and $E/\mathbb{F}_q$ be an elliptic curve. Then

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

In particular, for $q = p$, we get

$$|a_p| \leq 2\sqrt{q}.$$

The Birch and Swinnerton-Dyer Conjecture

For primes p of good reduction we defined

$$a_p = p + 1 - \#\overline{E}_p(\mathbb{F}_p).$$

Extend the definition of a_p to the primes of **bad** reduction:

$$a_p := \begin{cases} 0 & \text{if } E \text{ has additive reduction at } p, \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

Definition

Let E be an elliptic curve defined over $\mathbb{Q}$ with minimal discriminant Δ. The **L-series attached to E** *is defined by*

$$L(E,s) := \prod_{p \mid \Delta} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}.$$

The Birch and Swinnerton-Dyer Conjecture

Definition

Let E be an elliptic curve defined over $\mathbb{Q}$.

The **L-series attached to E** *is defined by*

$$L(E,s) := \prod_{p|\Delta} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}.$$

This product converges for $s \in \mathbb{C}$ s.t. $\Re(s) \geq 3/2$, and has a **meromorphic continuation** to the whole complex plane.

In fact, it makes sense to evaluate $L(E,s)$ at $s=1$, although the above formula does not apply. **This is a corollary of modularity!!**

The Birch and Swinnerton-Dyer Conjecture

The following is the weak version of BSD, which was formulated in the mid 60s based on numerical evidence gathered using EDSAC, one of the early computers available at Cambridge University.

Conjecture (Birch–Swinnerton-Dyer)

Let $E/\mathbb{Q}$ be an elliptic curve, and let $r = \mathrm{rank}(E)$. Then,

(i) $L(E,1) = 0$ *if and only if* $r > 0$.

(ii) *If* $L(E,1) = 0$, *then* $r = \mathrm{ord}_{s=1} L(E,s)$, *the order of vanishing of* $L(E,s)$ *at* $s = 1$.

The central rôle played by this conjecture in the arithmetic theory of elliptic curve is highlighted by the fact that it is one of the Millennium Prize Problems of the Clay Mathematical Institute.

The Birch and Swinnerton-Dyer Conjecture

Example (Congruence number curve for $n = 1$)

One can show that $E : Y^2 = X^3 - X$ has rank $r = 0$.

By evaluating the L-series of this curve to several digit precision using Sage or Magma , we see that

$$L(E, 1) = 0.655514388573...,$$

which is consistent with the BSD Conjecture.

Example (Congruence number curve for $n = 5$)

One can show that $E : Y^2 = X^3 - 25X$ has rank $r = 1$.

The L-series of this curve computed to several digit precision is

$$L(E, 1) = 0.0000000000....$$

Galois representations attached to elliptic curves

The n-torsion representation

Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve, with $A, B \in \mathbb{Q}$.

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $P = (x, y) \in E(\overline{\mathbb{Q}})$, set

$$\sigma(P) = (\sigma(x), \sigma(y)).$$

Since $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ is a ring homomorphism (hence is $\mathbb{Q}$-linear),

$$\sigma(y^2) = \sigma(x^3 + Ax + B) \iff \sigma(y)^2 = \sigma(x)^3 + A\sigma(x) + B$$

because $\sigma(A) = A$ and $\sigma(B) = B$. Hence

$$P \in E(\overline{\mathbb{Q}}) \implies \sigma(P) \in E(\overline{\mathbb{Q}}).$$

Moreover,

$$(\tau\sigma)(P) = \tau(\sigma(P)) \;\; \forall \tau, \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

So, this defines an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E(\overline{\mathbb{Q}})$.

The n-torsion representation

Furthermore, Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)**-action sends lines to lines.**

So it is **compatible** with the **group structure** on E.

In particular, Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) **preserves the subgroup** $E[n]$**.**

Fix a basis of $E[n]$: same as to giving an isomorphism

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

Then, the action of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) gives rise to a group homomorphism

$$\overline{\rho}_{E,n} : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong \mathsf{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

called the **n-torsion Galois representation attached to E.**

The n-torsion representation

Since $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is finite it follows that the $\ker(\overline{\rho}_{E,n})$ is normal of finite index inside $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Moreover,

$$\sigma \in \ker(\overline{\rho}_{E,n}) \iff P^\sigma = P \text{ for all } P \in E[n]$$

Thus, letting $K_n = K(E[n])$, we have

$$\ker(\overline{\rho}_{E,n}) = \mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$$

therefore

$$\mathrm{Im}(\overline{\rho}_{E,n}) \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\,\mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \simeq \mathrm{Gal}(K_n/\mathbb{Q})$$

The 2-torsion representation

Let $y^2 = f(x) = x^3 + ax^2 + bx + c$ be an elliptic curve over $\mathbb{Q}$.

We have $E[2] = \{\infty, P_1, P_2, P_3\}$ where $P_i = (\theta_i, 0)$ and θ_i are the roots of f. We have $P_3 = P_1 \oplus P_2$ and

$$K_2 := \mathbb{Q}(E[2]) = \mathbb{Q}(\theta_1, \theta_2, \theta_3).$$

If θ_i are all in $\mathbb{Q}$ then $K_2 = \mathbb{Q}$ and $\overline{\rho}_{E,2}$ is trivial.

Suppose, $\theta_1 \in \mathbb{Q}$ and $\theta_2, \theta_3 \notin \mathbb{Q}$. Then

$$f(x) = (x - \theta_1)(x^2 + ux + v), \quad K_2 = \mathbb{Q}(\theta_2) = \mathbb{Q}(\theta_3) = \mathbb{Q}(\sqrt{d})$$

where $d = u^2 - 4v$ is not a square in $\mathbb{Q}$.

We will write $\overline{\rho}_{E,2}$ with respect to the basis $\{P_1, P_2\}$.

The n-torsion representation

We will write $\overline{\rho}_{E,2}$ with respect to the basis $\{P_1, P_2\}$.

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If $\sigma(\sqrt{d}) = \sqrt{d}$ then

$$\sigma(P_1) = P_1, \quad \sigma(P_2) = P_2, \quad \overline{\rho}_{E,2}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2).$$

If $\sigma(\sqrt{d}) = -\sqrt{d}$ then σ swaps θ_2 and $\theta_3$hence

$$\sigma(P_1) = P_1, \quad \sigma(P_2) = P_3 = P_1 \oplus P_2, \quad \overline{\rho}_{E,2}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2).$$

Therefore,

$$\mathrm{Im}(\overline{\rho}_{E,2}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}).$$

Galois representations attached to elliptic curves

If f is irreducible with discriminant Δ_f not a square in $\mathbb{Q}^\times$ one can show that

$$\mathrm{Im}(\overline{\rho}_{E,2}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3.$$

If f is irreducible with discriminant Δ_f a square in $\mathbb{Q}^\times$ one can show that

$$\mathrm{Im}(\overline{\rho}_{E,2}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \simeq \mathbb{Z}/3\mathbb{Z} \simeq A_3 \subset S_3.$$

Theorem

Suppose that $E/\mathbb{Q}$ has a n-torsion point P defined over $\mathbb{Q}$. Then with respect to a bases of the form $\{P, Q\}$, we have

$$\mathrm{Im}(\overline{\rho}_{E,n}) \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

Recall the conductor of an elliptic curve.

"Definition"

- The **conductor** N_E of E measures the arithmetic complexity of E; we compute it using Tate's algorithm;
- E has multiplicative reduction at p if and only if $v_p(N_E) = 1$.
- E has additive reduction at p if and only if $v_p(N_E) \geq 2$.
- A prime p is **a prime of good reduction** when E mod p is an elliptic curve; in this case we have $p \nmid N_E$.
- We say that E is **semistable** if N_E is squarefree, i.e., all primes of bad reduction are of multiplicative reduction.

Recall also that for a prime $\ell \nmid N_E$ of good reduction we have defined the **trace of Frobenius at ℓ** by

$$a_\ell(E) = (\ell + 1) - \#\overline{E}(\mathbb{F}_\ell).$$

Galois representations attached to E.

Definition

Let ρ be a representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let p be a prime. We say that ρ is **unramified** at p if $\rho(I_p) = 1$ where $I_p \subset G_{\mathbb{Q}}$ is an inertia subgroup at p. We say it is **ramified** otherwise.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Then the p-torsion representation

$$\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is unramified at all primes $\ell \nmid pN_E$.

Moreover, for $\ell \nmid pN_E$ we have

1. $\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_\ell)) \equiv a_\ell(E) \pmod{p}$;
2. $\det(\overline{\rho}_{E,p}(\mathrm{Frob}_\ell)) \equiv \ell \pmod{p}$,

where Frob_ℓ is a Frobenius element at ℓ.

Mazur's Irreducibility Theorem

Theorem (Mazur)

Let $p \geq 5$ be a prime and E an elliptic curve defined over $\mathbb{Q}$. Suppose that

1. E is semistable;
2. the 2-torsion points $E[2]$ are defined over $\mathbb{Q}$.

Then, the Galois representation $\overline{\rho}_{E,p}$ is **irreducible.**

Here **irreducible** means that the image of $\overline{\rho}_{E,p}$ cannot be conjugated in $\mathrm{GL}_2(\mathbb{F}_p)$ into a subgroup of upper triangular matrices

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

p-adic representations attached to E

Fix a prime p and consider the p^n-torsion sequence:

$$E[p] \xleftarrow{[p]} E[p^2] \xleftarrow{[p]} E[p^3] \longleftarrow \quad \dots$$

taking the inverse limit we have the **Tate module at** p

$$T_p(E) = \varprojlim_n \{E[p^n]\} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

From the compatibility of the action of $G_{\mathbb{Q}}$ with $[p]$ we have an action on $T_p(E)$. Since $Aut(E[p^n])$ and $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ are isomorphic we also have

$$Aut(T_p(E)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}_p),$$

hence there is a continuous homomorphism

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p).$$

Moreover, reduction modulo p leads to

$$\overline{\rho}_{E,p} = \rho_{E,p} \pmod{p}.$$

p-adic representations attached to E

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime number.
The Galois representation

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$$

arising on the Tate module of E is irreducible.

Moreover, it is unramified at all primes $\ell \nmid pN_E$.

For each $\ell \nmid pN_E$ the characteristic polynomial of $\rho_{E,p}(\mathrm{Frob}_\ell)$ is

$$x^2 - a_\ell(E)x + \ell,$$

where Frob_ℓ be a Frobenius element at ℓ. In particular,

$$a_\ell(E) = \mathrm{Tr}(\rho_{E,p}(\mathrm{Frob}_\ell))$$

is the **trace of Frobenius**.