Talk: Shafarevich's Theorem, irred Theorem (Assuming Siegel's thm)

References: MG book, IV §1-2.1

Goals for today:

<u>Shafarevich's Theorem</u>

K number field, S finite set of places of K Then:

$$\{\text{Iso classes of } E/K \text{ elliptic curves w/ good reduction outside } S\} \text{ is finite}$$

<u>Irreducibility Theorem</u>

<u>Thm:</u> Assume E/K has no CM. Then

a) $V_\ell = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is irreducible for all primes ℓ

b) $E[\ell]$ is irreducible for almost all primes ℓ

§ Setup & Basics

K number field, E/K elliptic curve, w/ Weierstrass form $(\mathrm{Char}(K) \neq 2, 3)$

$$E: y^2 = 4x^3 - ax - b$$

Recall: Coefficients a, b are unique up to transformation:

$$a \mapsto u^4 a, \quad b \mapsto u^6 b, \quad u \in K^\times$$

The j-invariant of E is:

$$j(E) = \frac{1728\, a^3}{a^3 - 27b^2} \quad \Big\} \ \Delta = a^3 - 27b^2$$

$j(E)$ is independent of choice of Weierstrass eqn, but $\Delta = \Delta(f) = \Delta(a,b)$ is not.

E & E' have the same j-invariant $\iff E \simeq E'$ over $\overline{K}$

§ Good Reduction

Let v be a place of K. Write:

$\mathcal{O}_K$ - Ring of integers of K

$\mathcal{O}_v$ - Local ring at v

m_v - maximal ideal

k_v - Residue field.

Say E/K has good reduction at v if $\exists$ change of coordinates such that:

- Coefficients of equation f for E are in $\mathcal{O}_K \subseteq \mathcal{O}_v$
- Reduction $\tilde{f} = f \bmod m_v$ defines a <u>non-singular</u> (thus elliptic) curve $\tilde{E}_v / k_v$

Equivalently, $\exists$ equation f for E w/ coefficients in $\mathcal{O}_K$ s.t $\Delta(f) \in \mathcal{O}_v^\times$

RK: E has good reduction at all but finitely many places.

Since E can only have bad reduction at places dividing Δ

If E has good redn at v, then:

$$j(E) = \frac{1728a^3}{\Delta} \in \mathcal{O}_v \quad (\text{Since } \Delta(f) \in \mathcal{O}_v^*)$$

And $j(E) \bmod m_v = j(\tilde{E}_v)$

What about converse?

If $j(E) \in \mathcal{O}_v$, does E have good redn at v?

Ans: No, but E has <u>potential good reduction</u>

i.e $\exists$ fin ext L/K s.t the base change of E to L, $E \otimes_{\operatorname{Spec} K} \operatorname{Spec} L$ has good redn at all primes of L lying above v. (Proof omitted)

§ The Néron-Ogg-Shafarevich Criterion

Define the Tate-module:

$$T_\ell = \varprojlim_n E[\ell^n] \quad \text{and} \quad V_\ell = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

$G_K = \mathrm{Gal}(\bar{K}/K)$ acts on $E[\ell^n]$, T_ℓ, and V_ℓ, and give rise to G_K representations

Suppose $v \nmid \ell$, and let $\bar{v}$ be an extension of v in $\bar{K}$. (i.e fix an alg closure of K_v containing $\bar{K}$)

Let $D_{\bar{v}}$, $I_{\bar{v}}$ be the decomposition and inertia groups respectively.

$$D_{\bar{v}} = \mathrm{Gal}(\bar{K}_{\bar{v}}/K_v), \quad I_{\bar{v}} = \mathrm{Ker}(\mathrm{Gal}(\bar{K}_{\bar{v}}/K_v) \to \mathrm{Gal}(k_{\bar{v}}/k))$$

$$D_{\bar{v}}/I_{\bar{v}} \cong \langle \mathrm{Frob}_{\bar{v}} \rangle$$

Def: A representation $\varphi : G_K \longrightarrow GL(V)$ is <u>unramified at v</u> if the image of the inertia group is zero for any $\bar{v}$ lying above v:

$$\varphi(I_{\bar{v}}) = \{id\}$$

If E has good reduction at v, then reduction at $\bar{v}$ defines an isomorphism of G_K-modules:

$$E[\ell^n] \xrightarrow{\sim} \tilde{E}_v[\ell^n]$$

$\therefore$ The Galois action on $E[\ell^n]$ factors through the inertia group, so

$$E[\ell^n],\ T_\ell,\ V_\ell \text{ are unramified at } v.$$

⌜Moreover, the Frobenius action Frob_v on $\underline{T_\ell}$ corresponds to the Frobenius action F_v on $\tilde{E}_v$.

Why? bc Frob_v is a lift of F_v.

$$\therefore \quad \det(\mathrm{Frob}_v) = \det(F_v) = Nm(v)$$

$$\det(1-\mathrm{Frob}_v) = \det(1-F_v) = \#\tilde{E}_v(k_v)$$

⌟

The converse is also true:

Thm (Néron-Ogg-Shafarevich)

If $V_\ell = T_\ell \otimes \mathbb{Q}_\ell$ is unramified at v for <u>some</u> $v \nmid \ell$, then E has good reduction at v.

↑ some here refers to ℓ

Previous discussion shows if this is true for some ℓ, it is true for all ℓ.

Proof: Omitted

Corollary

If E and E' are isogenous and E has good reduction at v, then so does E'

Pf Given $\phi: E \to E'$ isogeny, pick ℓ coprime to size of kernel, then $\phi: E[\ell^k] \to E'[\ell^k]$ is an isomorphism, so E and E' have isomorphic ℓ-adic representations. $\square$

Alternatively: Even if $\ell \mid \operatorname{Ker}\phi$, $T_\ell \to T_\ell$ is an isogeny (kernel is finite) so upon tensoring with $\mathbb{Q}_\ell$ they are isomorphic: (i.e $V_\ell \cong V_\ell'$ for any ℓ)

§ Proof of Shafarevich's Theorem

Lemma: Let S be a finite set of primes of K, including all primes dividing 2 and 3, and such that $\mathcal{O}_{K,S}$ is a PID.

Then E/K has good reduction outside of S if and only if it can be put into Weierstrass form:

$$E: y^2 = 4x^3 - ax - b$$

Where $a, b \in \mathcal{O}_S$, and $\Delta = a^3 - 27b^2 \in \mathcal{O}_S^\times$. (We want coeffs that reduce at every v simultaneously)

<u>Proof</u> $\Leftarrow$ is clear from earlier discussion.

To show $\Rightarrow$, suppose K has a Weierstrass form

$$y^2 = 4x^3 - a'x - b'$$

For $a, b \in K^\times$.

Let v be a place not in S. Then E has good reduction at v, we can also write:

$$E: y^2 = 4x^3 - a_v x - b_v.$$

Where $a_v, b_v \in \mathcal{O}_v \cap K^\times$, and $\Delta(a_v, b_v) \in \mathcal{O}_v^\times \cap K^\times$

⌜ S containing primes dividing 2 & 3 so we can divide by 2 & 3 to get Weierstrass form ⌟

Since we now have 2 representations of E, there must exist $u_v \in K^\times$ s.t:

$$a_v = u_v^4 a', \quad b_v = u_v^6 b', \quad \Delta(a_v, b_v) = u_v^{12} \Delta(a', b')$$

Note that for all but finitely many v, a', b' will already be $\in \mathcal{O}_v$, and $\Delta(a', b') \in \mathcal{O}_v^\times$. Thus we can take $u_v = 1$ for all but finitely many v.

RK: $u_v \in K^\times$ only matters up to its v-valuation, $v(u_v)$.

Since $\mathcal{O}_{K,S}$ is a PID, it is possible to find an element $u \in K^\times$ such that

$$v(u) = v(u_v) \quad \forall v \notin S.$$

(Just take product of ideals corresponding to places)

Proof of Shafarevich's Theorem

Adding extra primes into S, WLOG S contains primes dividing 2 and 3, and $\mathcal{O}_{K,S}$ is PID.

If E/K has good reduction outside S, then by above lemma, we can write E in the form: $y^2 = 4x^3 - ax - b$

Where $a, b \in \mathcal{O}_{K,S}$, $\Delta(a,b) \in \mathcal{O}_{K,S}^\times$.

Δ can be changed by u^{12}, $u \in \mathcal{O}_{K,S}^\times$, so can consider Δ up to $\mathcal{O}_S^\times / (\mathcal{O}_S^\times)^{12}$.

Note that $\mathcal{O}_S^\times / (\mathcal{O}_S^\times)^{12}$ is finite, let $X \subseteq \mathcal{O}_S^\times$ be a set of representatives.

For each $\Delta \in X$, the equation: $U^3 - 27V^2 = \Delta$

Has finitely many solutions in $\mathcal{O}_S^\times$ (Siegel's thm).

$\therefore$ There are finitely many iso classes of elliptic curves w/ good reduction outside S.

$\square$

Corollary

Given E/K elliptic curve, there are only finitely many elliptic curves (up to isomorphism) that are K-isogenous to E.

Pf follows from corollary of Néron-Ogg-Shafarevich.
(isogenous curves have same places of good/bad reduction)

---

§ Proof of Irreducibility Thm

Lemma:

Let E/K with $\mathrm{End}_K(E) = \mathbb{Z}$ (i.e. No CM over K)

If $\phi' : E' \to E$ and $\phi'' : E'' \longrightarrow E$ are K-isogenies w/ non-isomorphic cyclic kernels, then E' and E'' are not isomorphic over K.

Pf of Lemma

Let n', n'' be size of $\mathrm{Ker}\,\phi'$, $\mathrm{Ker}\,\phi''$

Suppose otherwise and $\exists$ a K-isomorphism $E' \to E''$.

Consider the dual isogeny $\hat{\phi}' \; E \to E'$, this also has cyclic kernel of order n'.

$\phi\hat{\phi} = [n]$ has kernel $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

$\therefore \mathrm{Ker}\,\hat{\phi} = \mathrm{Ker}\,[n] / \mathrm{Ker}\,\phi$

Then the isogeny: $E \to E' \xrightarrow{\sim} E'' \to E$ must have kernel iso to an extension of $\mathbb{Z}/n''\mathbb{Z}$ by $\mathbb{Z}/n'\mathbb{Z}$.

But E has no CM $\rightsquigarrow$ this map must be $[a]$ for some a.

Then $\mathbb{Z}/n''\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z} \Rightarrow n'' = n' = a$. ※. $\square$

Proof of Irreducibility Thm

a) Suppose V_ℓ is reducible, i.e. $\exists$ 1-dim $\mathbb{Q}_\ell$ subspace of V_ℓ, stable under G_K action

Then intersecting w/ T_ℓ will give X, T_ℓ/X rank 1 free $\mathbb{Z}_\ell$ modules, X stable under G_K

Define $X(n) :=$ Image of X under quotient $T_\ell \to T_\ell/\ell^n T_\ell \cong E[\ell^n]$.

$X(n)$ is a cyclic submodule of $E[\ell^n]$, and <u>stable under G_K</u>

$\therefore$ We can define quotient curve $E(n) = E/X(n)$ over <u>K</u>

The isogenies $E \to E(n)$ have cyclic kernel of order ℓ^n.

$\Rightarrow$ $E(n)$ and $E(m)$ are not isomorphic for $n \neq m$. non-CM used here from previous lemma.

$\therefore$ There are infinitely many non-iso curves that are K-isogenous to E.

This contradicts Shafarevich's theorem. ※

b) If $E[\ell]$ is not irred, then $\exists\, X_\ell \subseteq E[\ell]$ 1-dim $\mathbb{Z}/\ell\mathbb{Z}$ subspace that is stable under G_K action.

$\therefore$ Once again, $E \to E/X_\ell$ is an isogeny of cyclic order ℓ.

$\therefore$ By Shafarevich's Theorem, there can only be finitely many such ℓ.

$\square$

Ritual of eternal youth

- Japanese Myth: Eat a mermaid?
- Anger a greek god (e.g Sisyphus.)
- Good skincare/ Stay hydrated
  infinitely

10 Eat A Mermaid

In Japanese mythology, there was a mermaid-like creature known as a ningyo. Described as a cross between a monkey and a carp, they lived in the sea and would normally bring bad luck or stormy weather if caught. (If they washed up on shore, they were said to be an omen of war).

One particular myth involves a girl known as the "Eight Hundred Nun." Her father accidentally brought her ningyo meat, and she ate it and was cursed with immortality. After years of sadness due to her many husbands and children dying, she devoted her life to Buddha and became a nun. Perhaps because of her holiness, she was allowed to die at the age of 800.