The Arithmetic of Curves: Overview

Diophantine equations:

We generalize the ring $\mathbb{Z}$ to any $\mathcal{O} = \mathcal{O}_{K,S} = \begin{pmatrix} K: \text{\# field} \\ S: \text{finite set of primes} \end{pmatrix} = \mathcal{O}_K[S^{-1}]$

$$X = \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ f_m(x_1, \dots, x_n) = 0 \end{cases} \quad (*)$$

$X(\mathcal{O}) = \{(x_1, \dots, x_n) \in \mathcal{O}^n \text{ satisfying } X\} = \mathrm{Hom}(\mathcal{O}[X], \mathcal{O})$

where $\mathcal{O}[X] = \mathcal{O}[x_1, \dots, x_n]/(f_1, \dots, f_m)$

This is the affine case.

- Projective case: Assume f_i's are homogeneous.

$$X(K) = \{(x_1, \dots, x_n) \neq (0, \dots, 0) \in K^n \text{ satisfying } (*)\}/K^\times \qquad (K = \text{\# field}).$$

Note: $X(K) = X(\mathcal{O}_K) = X(\mathcal{O}_{K,S})$ in the projective case.

Def A curve is a variety over K defined by $(*)$, for which $X(\mathbb{C})$ is a one-dimensional complex manifold.

We assume also that X is equipped with a model $\mathcal{X}$ over $\mathrm{Spec}(\mathcal{O}_K)$, allowing us to talk about $X(\mathcal{O}_{K,S})$.

Basic questions

1) Is $X(\mathcal{O}_{K,S})$ finite or infinite?

2) If $\#X(\mathcal{O}_{K,S}) < \infty$, give upper bounds on this cardinality in terms of X, S, K.

3) Height functions:

$$h: X(\mathcal{O}_{K,S}) \to \mathbb{R}_{\geq 0}$$

If $\#X(\mathcal{O}_{K,S}) = \infty$, understand the asymptotics of a counting function

$$N(X, B) = \#\{P \in X(\mathcal{O}_{K,S}) \mid h(P) < B\}.$$

4) If $\#X(\mathcal{O}_{K,S}) < \infty$, understand $\max_{P \in X(\mathcal{O}_{K,S})} \{h(P)\}$.

5) Give effective algorithms to compute $X(\mathcal{O}_{K,S})$.

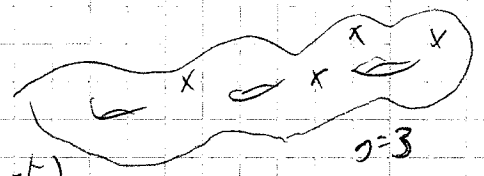
• Topological appearance of $X(\mathbb{C})$

Assume X smooth.

Then $X(\mathbb{C}) \simeq S_g \setminus \{P_1, \dots, P_s\}$

where g = genus of X, S_g is a complex surface of genus g

and $\{P_1, \dots, P_s\}$ is a finite set of points.



Can define $\chi(X) := 2-2g-s$ (Euler Characteristic).

• $\chi(X) > 0 \Rightarrow g=0$, $s=0,1$.

Theorem: Assume $s=0$ (projective case).

TFAE:

1) $X(k) \neq \emptyset$

2) $X \simeq \mathbb{P}^1$ over K

3) $X(K_v) \neq \emptyset$ for all completions K_v of K.

1 ⇒ 2 Riemann-Roch $\infty \in X(k)$, then $\mathcal{L}(\infty) \neq 0 \Rightarrow \phi \in \mathcal{L}(\infty)$, $\phi: X \to \mathbb{P}^1$.

2 ⇒ 3 obvious

3 ⇒ 1 Hasse-Minkowski

Note in case $s=1$ (affine) then $X \simeq \mathbb{A}^1 / \mathcal{O}$ Spec $\mathcal{O}$

$\Rightarrow \mathcal{O}[X] \simeq \mathcal{O}[x] \Rightarrow X(\mathcal{O}) \simeq \mathcal{O}$

• $\chi(X) = 0 \Rightarrow (g,s) = (0,2)$ (affine) or $(1,0)$ (projective)

If $X(\mathcal{O}) \neq \emptyset$, then X has the structure of a group scheme over $\mathcal{O}$.

In the affine case, $X/\mathcal{O} \simeq \mathbb{G}_m/\mathcal{O}$ $(= \mathcal{O}^\times)$ (typical example)

In the projective case, $X/\mathcal{O}$ = Elliptic curve / Spec $(\mathcal{O})$.

Theorem: $X(\mathcal{O})$ is finitely generated.

→ Affine case: Dirichlet theorem ($\mathcal{O}^\times$ fin. gen.)

→ Projective case: Mordell-Weil theorem.

In this course, we will concentrate on $\chi(X) < 0$.

Theorem: If $\chi(X) < 0$, then $\#X(\mathcal{O}) < \infty$.

→ Affine case: Siegel's theorem. ($S \neq \emptyset$)

First interesting case: $X = \mathbb{P}_1 - \{0, 1, \infty\}$ / $\mathrm{Spec}(\mathcal{O})$

$\mathcal{O}(X) = \mathcal{O}[x, \frac{1}{x}, \frac{1}{x-1}]$.

Then $X(\mathcal{O}) = \mathrm{Hom}(\mathcal{O}(X), \mathcal{O})$

$f \in \mathrm{Hom}(\mathcal{O}(X), \mathcal{O}) \to f(x) \in \mathcal{O}^\times$ and $1 - f(x) \in \mathcal{O}^\times$ ⇒ S-unit equation

→ Projective case: Faltings' theorem. (next two lectures about this)

Prelude: dimension 0 (schemes of dim 0 over $\mathrm{Spec}\,\mathcal{O}$)

An $\mathcal{O}$-algebra R is called finite flat (f.f.) if R is f.g. free $\mathcal{O}$-module.

An $\mathcal{O}$-algebra R is called étale if $R/\mathfrak{p}$ is reduced (no nilpotents) for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$

Let $Ш(\mathcal{O}, d) = \{$iso. classes of f.f. étale algebras / $\mathcal{O}$ of rank $d\}$

Theorem (Hermite): $(\mathcal{O} = \mathcal{O}_{K,S})$.

$\#Ш(\mathcal{O}, d) < \infty$

Pf (Sketch)

Given $R \in Ш(\mathcal{O}, d)$, consider $L = R \otimes_{\mathcal{O}} K$.

L is a K-algebra of degree d, unramified outside S.

One can then bound the discriminant of L/K.

One then shows that there are finitely many fields of bounded degree & discriminant.

Unramified Coverings.

Let π be a finite morphism $\pi : X \to Y$ / Spec $\mathcal{O}$.

We will say π is unramified if $\pi : X(\mathbb{C}) \to Y(\mathbb{C})$ is unramified (for (some) $\mathcal{O} \hookrightarrow \mathbb{C}$) — does not depend on this.

Lemma: if $\pi : X \to Y$ is unramified, then there exists a finite extension L/K, and a finite set $S' \supseteq \tilde{S}$ s.t. ($\tilde{S}$: places of L above S).

$$\pi\left(X(\mathcal{O}_{L,S'})\right) \supseteq Y(\mathcal{O}_{K,S})$$

Pf Fact: if $\pi : X \to Y$ is unramified, then $\exists\, S' \supseteq S$, S' finite s.t.

$\pi : X \to Y$ / $\mathcal{O}_{K,S'}$ is étale, as a covering of schemes over Spec $(\mathcal{O}_{K,S'})$

In particular, for all $P \in Y(\mathcal{O}_{K,S'})$, $\pi^*(P)$ (fiber of P) is (spec of) an étale $\mathcal{O}_{K,S'}$-algebra.

Hence $\pi^*(P) \in \mathrm{III}(\mathcal{O}_{K,S'}, d)$ where $d = \deg \pi$.

By Hermite's thm, there are finitely many such algebras, and can let

$L = \underset{R \in \mathrm{III}(\mathcal{O}_{K,S'},d)}{\text{Composition}} \left(\mathrm{Frac}(R)\right)$ is finite over K by Hermite. //

Def X is **mordellic** if $X(\mathcal{O}_{L,S})$ is finite $\forall\, [L:K] < \infty$, $\forall$ finite set of places S.

Corollary: if $\pi : X \to Y$ is unramified, then X mordellic $\Leftrightarrow$ Y mordellic.

(The interesting application is ($\Rightarrow$)).

$$Y(\mathcal{O}_{K,S}) \subset \pi\left(X(\mathcal{O}_{L,S'})\right) \quad \Rightarrow \checkmark.$$ //

Exercises:

1) Show Faltings $\Rightarrow$ Siegel (mordellic case $\mathbb{P}^1 - \{0, 1, \infty\}$)

2) If $\chi(X) = 0$ and X is a gp scheme / $\mathcal{O}_{K,S}$, show that $X(\mathcal{O})/nX(\mathcal{O})$ is fin-gen.

3) Let $X = x^7 + y^7 + z^7 = 0$ (Fermat curve of deg 7).

$Y = u^3v + v^3w + w^3u = 0$ (Klein quartic, $X(7)$).

a) Show that $g(X) = 15$, $g(Y) = 3$.

b) Show that $\pi(x,y,z) = (x^3z, y^3x, z^3y)$ is an unramified covering $X \to Y$ of degree 7.

c) Show that if $P \in Y(\mathbb{Q})$, $\exists\, A \in X(\mathbb{Q})$ s.t. $\pi(A) = P$

Faltings' Theorem, (I)

References:

- Szpiro, Deligne "Bourbaki Seminar lecture"
- Faltings-Wüstholz, "Rational Points"
- Cornell-Silverman → (further background).

Theorem (Faltings): Let X/K be a smooth projective curve of genus $g \geq 2$. Then $|X(K)| < \infty$

Pf: Fix from now on a finite set S of places of K s.t. X has a smooth model over Spec $\mathcal{O}_{K,S}$ (will call it X, not $\mathcal{X}$).

We proceed by a series of reductions.

1) First Reduction: the Shafarevich Problem.

Recall $Ш(\mathcal{O}, d)$ defined before. It is finite (by Hermite).

Def
(1) $Ш(\mathcal{O}, M_g)$ = iso. classes of smooth curves of genus g over Spec $\mathcal{O}$. (i.e. they have good reduction over any prime of $\mathcal{O}$, also).
(2) $Ш(\mathcal{O}, A_g)$ = iso classes of abelian varieties of dimension g.
(3) $Ш(\mathcal{O}, I_g)$: isogeny classes of abelian varieties of dimension g.

Conjecture: $Ш(\mathcal{O}, -)$ is finite (by Shafarevich).

Theorem (Kodaira, Parshin): The Shafarevich conjecture for curves implies Faltings' Theorem.

Idea of pf: the Kodaira-Parshin construction: given $P \in X(K)$, it constructs a curve X_P which is a covering of X, $X_P \xrightarrow{\pi_P} X$ s.t.
- X_P is ramified only at P.
- The genus of X_P is > 1 and depends only on X. Let $g' = \text{genus}(X_P)$ (not on P!)
- X_P is smooth over Spec $(\mathcal{O}[\frac{1}{2}])$

So get a map $X(K) \longrightarrow Ш(\mathcal{O}[\frac{1}{2}], M_{g'})$

* Outline of the construction over $\mathrm{Spec}(k)$ (it's easier).

Embed $X \hookrightarrow \mathrm{Jac}(X)$, abelian variety of dimension g, by $Q \mapsto [(Q)-(P)]$

$$\begin{array}{ccc} \tilde{X} & \dashrightarrow & \mathrm{Jac}(X) \\ \pi \downarrow & & \downarrow [2] \\ X & \hookrightarrow & \mathrm{Jac}(X) \end{array}$$

$\tilde{X}$ the pullback of the diagram

Write $\pi^{-1}(P) = \tilde{P} + D$ where $\begin{cases} D \text{ is an effective divisor of deg } = 2^{2g}-1 \\ \tilde{P} \in \tilde{X}(k) \end{cases}$

$\tilde{J}_D :=$ generalized Jacobian of $(\tilde{X}, D)$ is s.t.

$$\tilde{J}_D(L) = \left\{ \begin{array}{l} L\text{-rational divisors of deg } 0 \\ \text{of } \tilde{X} \text{ supported outside } D \end{array} \right\} \Big/ \left\{ \begin{array}{l} \text{principal divisors } \mathrm{div}(f) \\ \text{s.t. } f(D') = 1 \ \forall D' \text{ of deg } 0 \\ \text{supported on } D \end{array} \right\}$$

Have the exact sequence $1 \to G_m^{2g-2} \to \tilde{J}_D \to \mathrm{Jac}(\tilde{X}) \to 1$

What we do now: when X_P is again the pullback of the diagram.

$$\begin{array}{ccc} X_P & \dashrightarrow & \tilde{\tilde{J}}_D \\ \downarrow & & \downarrow [2] \\ \tilde{\tilde{X}} & \hookrightarrow & \tilde{J}_D \end{array}$$

Exercise: Compute g'.

Call $R_1 : X(K) \to Ш(\mathcal{O}[\tfrac{1}{2}], M_{g'})$ just defined.

The key point is that R_1 has finite fibers (Theorem by De Franchis)

De Franchis says $\mathrm{Mor}(Y, X)$ is finite if $g(X) \geq 2$.

So among $Y \cong X_P$ done.

2) Second reduction: From curves to Abelian varieties.

Consider $R_2 : Ш(\mathcal{O}, M_g) \to Ш(\mathcal{O}, A_g)$

$$X \longmapsto \mathrm{Jac}(X).$$

By a theorem of Torelli, R_2 has finite fibers. (as an abelian variety can only carry finitely-many polarizations) then X is determined by its Jacobian + data from the principal polarization.

3) Third reduction: From Abelian varieties to Isogeny classes

Let $R_3 : Ш(\mathcal{O}, A_{g'}) \longrightarrow Ш(\mathcal{O}, I_{g'})$

Theorem (Faltings): Let A be an abelian variety over K. Then there are finitely many isomorphism classes of abelian varieties over K that are K-isogenous to A. (i.e. R_3 has finite fibers).

This result is the technical part of Faltings' proof

The key ingredient is "Faltings Height", ...

Will take this part as a black box.

4) Fourth reduction: From isogeny classes to ℓ-adic representations.

Given A an abelian variety over K, consider

$G_K \circlearrowright A[\ell^n] \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ $\qquad (G_K = Gal(\bar{K}/K))$

Define the Tate module $\overset{G}{\circlearrowright} T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$

$V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$

Then $V_\ell(A)$ is a $2g$-dimensional $\mathbb{Q}_\ell$-vectorspace equipped with two commuting actions:

$E = \mathbb{Q}_\ell$-algebra generated by $End_K(A) \circlearrowright V_\ell(A)$

$\Pi = \mathbb{Q}_\ell$-algebra generated by $G_K \circlearrowright V_\ell(A)$.

(they commute because $End_K(A)$ is invariant under Π).

The iso. class of the G_K-module $V_\ell(A)$ depends only on the isogeny class of A. (because we tensor by $\mathbb{Q}_\ell$).

$R_4 : Ш(\mathcal{O}, I_{g'}) \xrightarrow{V_\ell} \{$iso. classes of $2g$-dim ℓ-adic reps of $G_K\}$

- Basic facts about $V_\ell(A)$

1) $V_\ell(A)$ is semisimple over E (the category of abelian varieties up to isogeny is semisimple (i.e. all exact sequences are split)).

(Weil) 2) $V_\ell(A)$ is unramified outside S where $S =$ {primes invertible in $\mathcal{O}$} $\cup \{v \mid \ell\}$

(Weil) 3) $V_\ell(A)$ is a rational representation i.e. given $v \notin S$, $Frob_v \circlearrowright V_\ell(A)$ and $Frob_v$ has characteristic polynomial in $\mathbb{Z}[T]$ with roots $\alpha_1, \dots, \alpha_{2g'}$ satisfying $|\alpha_i| \leq \sqrt{N(v)}$ (in particular $Trace(Frob_v) \leq 2g'\sqrt{N(v)}$)

Thanks to these previous facts, R_4 actually lands in

$$\left\{ \begin{array}{l} \text{iso classes of } 2g'\text{-dim'l Galois reps of } G_K \\ \text{such that } \bullet \text{ unramified outside } S \\ \qquad\quad \bullet \text{ rational} \end{array} \right\}$$

There's another property that Faltings proved about $V_\ell(A)$:

4) $V_\ell(A)$ is semisimple over Π (deeper than checking it over E).

Tomorrow: prove (4) and that R_4 has finite fibers.

and then R_4 lands in iso classes of unramified outside S rational semisimple over Π

and finally prove that this last set is finite, to conclude the proof.

Finiteness - to - 1 by

So far:

$X(K) \xrightarrow{R_1} Ш(\mathcal{O}, M_{g'})$ (Kodaira-Parshin) De Franchis: $\#\mathrm{Mor}(X,Y) < \infty$

$\xrightarrow{R_2} Ш(\mathcal{O}, A_{g'})$ (Passage to Jac) Torelli's theorem.

$\xrightarrow{R_3} Ш(\mathcal{O}, I_{g'})$ (Natural map) — Faltings' Finiteness Thm

$\xrightarrow{R_4} \mathrm{Rep}_S(G_K, d) = \left\{ \begin{array}{l} \text{isom. classes of} \\ \text{rational, semisimple, } \ell\text{-adic} \\ \text{representation of } G_K, \text{ of} \\ \text{dimension } d = 2g', \text{ unramif. outside } S \end{array} \right\}$ ← Tate Conjecture

(Tate module) Tate Weil

Ending the proof:

Step 1: Show that the ℓ-adic Tate module is semisimple for Π

Step 2: Show R_4 is injective (Tate Conjecture)

Step 3: $\mathrm{Rep}_S(G_K, d)$ is finite.

Step 1: Semisimplicity:

(Exercise: show that if we commit semisimplicity, then $\mathrm{Rep}_S(G_K, d)$ can be infinite.)

Key Theorem (call it Theorem E): Let $W \subset V_\ell(A)$ be a Π-stable subspace. Then $\exists\, u \in E \left(= \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell\right)$ s.t. $u(V_\ell(A)) = W$

Pf: Consider $W \cap T_\ell(A)$ and $W_n = \text{image in } A[\ell^n]$. (note that W_n is Π-stable)

Consider $A \xrightarrow{\alpha_n} A/W_n$ where β_n = isogeny satisfying $\alpha_n \circ \beta_n = \ell^n$, $\beta_n \circ \alpha_n = \ell^n$

$\beta_n : A_n$

Note that $\beta_n(A_n[\ell^n]) = W_n$

By Faltings' finiteness theorem, $\exists$ infinite $I = \{n_0, \dots, i, \dots\}$ s.t. $A_{n_0} \xrightarrow[\nu_i]{\sim} A_i$

Have:

$$\begin{array}{ccc} A_{n_0} & \xrightarrow{\nu_i} & A_i \\ & {\scriptstyle \alpha_{n_0}} \nwarrow \quad \swarrow {\scriptstyle \beta_i} & \\ & A & \end{array}$$

Define $U_i := \beta_i \circ \nu_i \circ \alpha_{n_0} \in \mathrm{End}_K(A)$.

Assume that the u_i converge in $\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell$, and $u|_{A[\ell^i]} = u_i|_{A[\ell^i]}$ (compactness so can take a subsequence that does converge).

Let $u = \lim u_i$

Then $u(A[\ell^i]) = u_i(A[\ell^i]) \subseteq \beta_i(A_i[\ell^i]) = W_i$ (with index indep of i)

So $u(T_\ell(A)) \subseteq W \cap T_\ell(A) \Rightarrow u(V_\ell(A)) = W$.

(first: finite index; second: because $\mathbb{Q}_\ell$)

Corollary: $V_\ell(A)$ is semisimple.

Pf: Let $W \subset V_\ell(A)$ be any Π-stable subspace. Need to produce a Π-stable complement.

By Thm E, $\exists\, u \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell : u(V_\ell(A)) = W$.

Consider uE, and let u_0 be an idempotent in uE.

Let $W' = \ker u_0$. This is a Π-stable complement.

Step 2: R_ℓ is injective

Remark 1: Enough to show that

$$\mathrm{Hom}_K(A,B)\otimes\mathbb{Q}_\ell \longrightarrow \mathrm{Hom}_\Pi\big(V_\ell(A),V_\ell(B)\big)$$ is surjective (injective is clear)

This is called the Tate Conjecture.

Pf: $\exists\, i: V_\ell(A)\overset{(\Pi)}{\simeq} V_\ell(B)$. Then $\exists\, u\in \mathrm{Hom}_K(A,B)\otimes_{\mathbb{Z}}\mathbb{Q}_\ell$ mapping to i.

Then $\det(u)\neq 0$. Can clear denominators and assume $u\in \mathrm{Hom}_K(A,B)\otimes\mathbb{Z}_\ell$

Write $u=\ell^n u_i$, $u_i\in \mathrm{Hom}_K(A,B)$

The u_i are congruent for $i\gg 0$ so done. //

Remark 2: Enough to show

$$\mathrm{End}_K(A)\otimes\mathbb{Q}_\ell \xrightarrow{\sim} \mathrm{End}_\Pi(V_\ell(A)) \quad \text{(injective is easy)}$$

Pf: Replace by A by $A\times B$ and note that $\mathrm{End}_K(A\times B)=\mathrm{End}_K(A)\oplus\mathrm{Hom}(A,B)$

$$\oplus\,\mathrm{Hom}_K(B,A)\oplus\mathrm{End}_K(B)$$

Theorem: $\mathrm{End}_K(A)\otimes\mathbb{Q}_\ell \longrightarrow \mathrm{End}_\Pi(V_\ell(A))$ is surjective.

Pf: Let $\varphi\in\mathrm{End}_\Pi(V_\ell(A))$

Consider $\mathrm{graph}(\varphi)=W=\{(x,\varphi(x))\in V_\ell(A)\times V_\ell(A)\}\subseteq V_\ell(A\times A)$

W is Π-stable (as $\varphi\in\mathrm{End}_\Pi$). $\quad M_{2\times 2}(\mathrm{End}_K(A)\otimes\mathbb{Q}_\ell)$

By Theorem E, $\exists\, u\in\mathrm{End}_K(A\times A)\otimes\mathbb{Q}_\ell$ s.t. $u\big(V_\ell(A\times A)\big)=W$.

Let $\alpha\in E^\circ$ = commutant of E in $\mathrm{End}(V_\ell(A))$ (centralizer)

Then $\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}$ commutes with u, hence $\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}$ preserves $W=\mathrm{image}(u)$.

So α commutes with φ (exercise)

Hence $\varphi\in(E^\circ)^\circ = E$ (fact about semisimple algebras). //

Final step: $\mathrm{Rep}_S(G_K, d)$ is finite.

Proposition: (Effective Chebotarev Theorem):

There exist a finite set T of places of K, disjoint from S, such that for all $\rho_1, \rho_2 \in \mathrm{Rep}_S(G_K, d)$,

$$\mathrm{Trace}\left(\rho_1(\mathrm{Frob}_v)\right) = \mathrm{Trace}\left(\rho_2(\mathrm{Frob}_v)\right) \ \forall v \in T \Rightarrow \rho_1 \cong \rho_2$$

Pf: Let L = compositum of all extensions of degree at most ℓ^{2d^2} which are unramified outside S.

By Hermite, $[L:K] < \infty$.

By classical Chebotarev, $\exists\, v_1, \dots, v_N$ places of K s.t. $\{\mathrm{Frob}(v_1), \dots, \mathrm{Frob}(v_N)\}$ generate $\mathrm{Gal}(L/K)$. Let $T = \{v_1, \dots, v_N\}$.

Consider now $\rho_1, \rho_2 \in \mathrm{Rep}_S(G_K, d)$, consider:

$$j: \rho_1 \oplus \rho_2 : \Pi \longrightarrow M_d(\mathbb{Z}_\ell) \times M_d(\mathbb{Z}_\ell)$$

Let $M = \mathrm{Image}(j)$.

The rank of M as a $\mathbb{Z}_\ell$-module is $\mathrm{rk}_{\mathbb{Z}_\ell} M \le 2d^2$.

$$\overline{j} = \overline{\rho_1 \oplus \rho_2} : \begin{array}{ccc} \Pi & \longrightarrow & M/\ell M \\ G_K & \longrightarrow & (M/\ell M)^\times \end{array}$$

$\overline{j}$ is unramified outside S (j has).

$$\#(M/\ell M)^\times \le \#\, M/\ell M = \ell^{2d^2}$$

So $\overline{j}: G_K \longrightarrow (M/\ell M)^\times$ factors through $\mathrm{Gal}(L/K)$

$$G_K \twoheadrightarrow \mathrm{Gal}(L/K) \hookrightarrow (M/\ell M)^\times$$

Therefore, by the choice of T, $\{\overline{j}(\mathrm{Frob}(v_1)), \dots, \overline{j}(\mathrm{Frob}(v_N))\}$ generates $M/\ell M \Rightarrow$ (by Nakayama's Lemma) $\Rightarrow j(\mathrm{Frob}(v_1)), \dots, j(\mathrm{Frob}(v_N))$ generate M as a $\mathbb{Z}_\ell$-module.

Hence, if $\mathrm{Trace}\left(\rho_1(\mathrm{Frob}(v))\right) = \mathrm{Trace}\left(\rho_2(\mathrm{Frob}(v))\right)\ \forall v \in T \Rightarrow$

$\Rightarrow \mathrm{Trace}\left(\rho_1(\sigma)\right) = \mathrm{Trace}\left(\rho_2(\sigma)\right)\ \forall \sigma \in \Pi$.

As ρ_1, ρ_2 are semi-simple, $\rho_1 \simeq \rho_2$ because they are determined by their traces.

To conclude, then:

There are only finitely many possibilities for $\mathrm{Tr}(\rho(\mathrm{Frob}_v)) \leq d\,N(v)^{1/2}$

So done. Here it's crucial the rationality of the rep.

Modular Curves & Mazur's Theorem.

Question: what curves are also moduli spaces?

One class of them are the modular curves.

Modular Curves: (Moduli space of elliptic curves (coarse) $/\operatorname{Spec}\mathbb{Z}[1/6]$ $= \operatorname{Spec}\mathbb{Z}[1/6][j]$)

Fix a prime $p \geq 5$, and let $\mathbb{Z} = \mathbb{Z}[1/p]$.

$Y_1(p)$ = curve over $\operatorname{Spec}\mathbb{Z}$ classifying pairs (E, P) where $\begin{cases} E \text{ ell. curve} \\ P \text{ a point of order } p \text{ on } E. \end{cases}$

What this means is that for any $\mathbb{Z}$-algebra R,

$Y_1(p)(R) = \{(E,P)/R$, up to R-isomorphism$\}$. $\circlearrowleft (\mathbb{Z}/p\mathbb{Z})^\times$ by $\alpha : (E,P) \mapsto (E, \alpha P)$

Also, let $Y_0(p) := Y_1(p)/(\mathbb{Z}/p\mathbb{Z})^\times$

Fact: $Y_1(p)$ and $Y_0(p)$ are smooth over $\operatorname{Spec}\mathbb{Z}$.

Exercise: compute the genus of $Y_1(p)$ and $Y_0(p)$.

Theorem (Mazur): if $p = 11$ or $p > 13$, then $Y_1(p)(\mathbb{Q}) = \emptyset$

Remark: this is a Theorem about curves in two different ways:

1) It says sth about the infinite collection of curves $Y_1(p)$ as p varies.

2) It also implies that the torsion on all elliptic curves over $\mathbb{Q}$ is uniformly bounded.

We will outline the proof of this theorem.

Description of $Y_1(p)$ over $\mathbb{C}$

$Y_1(p)(\mathbb{C}) = \{(E,P)/\mathbb{C}\} = \dfrac{\mathbb{H}}{\Gamma_1(p)}$, $\quad \Gamma_1(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod p\}$

$Y_0(p)(\mathbb{C}) = \dfrac{\mathbb{H}}{\Gamma_0(p)}$, $\quad \Gamma_0(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod p\}$

• Compactifications

Cusps: $X_0(p)$: compactification of $Y_0(p)$ obtained by adjoining cusps.

$$X_0(p)(\mathbb{C}) = \mathcal{H}^* / \Gamma_0(p), \quad \mathcal{H}^* : \mathbb{P}_1(\mathbb{Q}) \cup \mathcal{H}.$$

$$\text{i.e. } X_0(p)(\mathbb{C}) = \mathcal{H}/\Gamma_0(p) \cup \{0, \infty\} \quad (+ \text{ analytic structure}).$$

Local parameter at ∞:

Is given by $q = e^{2\pi i \tau}$.

Algebraically, consider the Tate curve $\mathbb{Z}[[q]]^\times / q^{\mathbb{Z}} =: E_{Tate}$ / $\mathrm{Spec}\left(\mathbb{Z}[[q]][\frac{1}{q}]\right)$

$\Delta = q \cdot \prod (1-q^n)^{24}$

So E_{Tate} is an elliptic curve over $\mathbb{Z}[[q]][\frac{1}{q}]$

The q-expansion principle identifies:

$$\widehat{\mathcal{O}}_{X_0(p),\infty} = \mathbb{Z}[[q]].$$

Definition: A morphism of varieties $j: X \to Y$ is a formal immersion at $x \in X(\mathbb{Z})$ if it induces a surjection:

$$j^\sharp : \widehat{\mathcal{O}}_{Y, j(x)} \twoheadrightarrow \widehat{\mathcal{O}}_{X,x}$$

Mazur's criterion: Suppose there is a quotient $J_\#(p)$ of $J_0(p) = \mathrm{Jac}(X_0(p))$, (Jacobian variety of $X_0(p)$, abelian)

with the property that:

1) $j_\# : X_0(p) \to J_0(p) \twoheadrightarrow J_\#(p)$ (the map $J_\#$) is a formal immersion at ∞.

$x \mapsto (x) - (\infty)$, $\Phi_\#$

2) $J_\#(p)(\mathbb{Q})$ is finite.

Then $Y_1(p)(\mathbb{Q}) = \emptyset$.

Sketch of pf:

Let $\tilde{x} \in Y_1(p)(\mathbb{Q})$, and let (E, P) be the corresponding "point" to $\tilde{x}$.

E has potentially multiplicative reduction at 3.

For otherwise $\mathcal{E}/\mathbb{F}_3$ ($\mathcal{E}$ Néron model) is either an elliptic curve (good red.) or an extension of a finite group Φ of ord. $2^a 3^b$ by $\mathbb{G}_a$ (case of additive red.) $\to$!!

2) Let $x \in X_0(p)$ be the image of $\tilde{x}$ in $X_0(p)$. Then x reduces to either 0 or ∞ modulo 3.

Assume WLOG that $x/\mathbb{F}_3 = \infty/\mathbb{F}_3$ (if it reduces to 0, can replace $(E, \langle P \rangle) \rightsquigarrow \left(E/\langle P \rangle, E[p]/\langle P \rangle\right)$)

3) Consider the image $\Phi_\#\left((x)-(\infty)\right) \in \underbrace{J_\#^1(p)}_{\text{the connected component of the identity}}(\mathbb{Q}_3) \cap J_\#(p)(\mathbb{Q})$

Now $J_\#^1(p)(\mathbb{Q}_3)$ is torsion-free, $J_\#(p)(\mathbb{Q})$ is torsion $\Rightarrow \Phi_\#\left((x)-(\infty)\right) = 0$.

Therefore, $j_\#(x) = 0$

(Aside, $J_\#^1(p)(\mathbb{Q}_3)$ is, by definition, $1 \to J_\#^1(p)(\mathbb{Q}_3) \to J_\#(p)(\mathbb{Q}_3) \to J_\#(p)(\mathbb{F}_3) \to 1$)

4) By the formal immersion property, $x = \infty$:

Let $\operatorname{spec} R$ = affine nbhd of x, $x: R \to \mathbb{Z}_3$ factors through:

$$\begin{array}{ccc} x: R & \longrightarrow & \mathbb{Z}_3 \\ & \searrow \quad \nearrow & \\ & \mathcal{O}_{X_0(p),\infty} & \\ & \cong \mathbb{Z}[[q]]\left[\frac{1}{q}\right] & \end{array}$$

the map $\alpha: \mathbb{Z}[[q]] \to \mathbb{Z}_3$

$\downarrow$ formal immersion $\Rightarrow j_\#^\sharp$ surjective.

We've shown in (3) that $x^\sharp \circ j_\#^* = \alpha \circ j_\#^* \Rightarrow x = \infty$

Problem: Construct a good quotient $J_\#(p)$ of $J_0(p)$.

Key ingredient: connection between $J_0(p)$ and modular forms.

Def $S_2(p, R)$ = space of regular differentials on $X_0(p)/R$, where R is a $\mathbb{Z}$-algebra.

It is called the space of modular forms of weight 2 in $\Gamma_0(p)$.

(because $S_2(p, \mathbb{C}) = \{f: \mathcal{H} \to \mathbb{C}$ holomorphic, $f(z)dz$ $\Gamma_0(p)$-invariant, f holomorphic at ∞ and $0\} \ni f(z) = \sum_{n \geq 0} a_n q^n \dfrac{dq}{q}$)

Eichler-Shimura decomposition.

Let $\ell \neq p$ a prime. $X_0(p\ell)$ — two different maps — (E, C_1, C_2) (ord p, ord ℓ)

$X_0(p)$ $\quad$ $X_0(p)$ $\quad$ (E, C_1) $\quad$ $(E/C_2, \overline{C}_1)$

This correspondence T_ℓ gives rise to an endomorphism of $J_0(p)$.

$\uparrow$ $\mathrm{End}_{\mathbb{Q}}(J_0(p))$

Let $\mathbb{T} :=$ subring of $\mathrm{End}_{\mathbb{Q}}(J_0(p))$ generated by all T_ℓ $(\ell \nmid p)$.
It's called the Hecke algebra.

Claim: $\mathbb{T} \otimes \mathbb{Q}$ is a semisimple commutative algebra over $\mathbb{Q}$.

$$\dim_{\mathbb{Q}} \mathbb{T} \otimes \mathbb{Q} = \dim_{\mathbb{Q}} S_2(p, \mathbb{Q}) \left(= \text{genus}(X_0(p)) \right)$$

↑ dim of reg. diff. = genus, true always.

If There's a perfect pairing $\mathbb{T} \otimes \mathbb{Q} \times S_2(p, \mathbb{Q}) \longrightarrow \mathbb{Q}$

$$(T, f) \longmapsto a_1(Tf).$$

↖ the first Fourier coeff of the q-expansion of Tf

Exercise: show that this is perfect.

Corollary: $\mathbb{T} \otimes \mathbb{Q} \simeq \prod_{f \text{ normalized eigenforms}} K_f$ where K_f = field generated by Fourier coeffs of f.

(an eigenform is a modular form which is an eigenvector for $\mathbf{T}$ (all at the same time))

normalized $\rightsquigarrow a_1 = 1$.

Also, $f \in S_2(p, \bar{\mathbb{Q}}) \rightsquigarrow f = \sum_{a_1=1} a_n q^n$ then a_ℓ = eigenvalue of T_ℓ on f.

$\mathbb{T}$ is an order in $K_{f_1} \times \cdots \times K_{f_t}$ where $f_1, \ldots, f_t$ is a system of eigenforms.

The Eichler–Shimura construction allows us to associate $f \rightsquigarrow A_f$,
to an eigenform $f \rightsquigarrow$ a quotient of $J_0(p)$ def/$\mathbb{Q}$.

How?

$$I_f := \ker\left(\mathbb{T} \longrightarrow K_f\right)$$

$$A_f := J_0(p)/I_f$$

Note: A_f are simple.

Properties of A_f:

1) $\mathrm{End}_{\mathbb{Q}}(A_f) \simeq \mathcal{O}_f$ where $\mathcal{O}_f \subset K_f$ = ring generated by $a_n(f)$.

This comes from the action of $\mathbb{T}$ on A_f, which factors through $\mathbb{T}/I_f \simeq \mathcal{O}_f$.

2) $\dim A_f = [K_f : \mathbb{Q}]$

3) $V_\ell(A_f)$ is a module over $K_f \otimes \mathbb{Q}_\ell$ of rank 2.

Then $J_0(p) \underset{\mathbb{Q}}{\sim} \prod_{f_j} A_{f_j}$

f_j eigenforms in $S_2(\Gamma_1, \overline{\mathbb{Q}})/\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

L-Series

- Hasse-Weil L-series: $L(A,s) = \prod_{\ell \text{ primes}} \det\left(1 - \mathrm{Frob}_\ell \, V_p(A)^{I_\ell} \ell^{-s}\right)^{-1}$

  of the Hasse-Weil L-series of an Abelian variety A.

- Hecke L-series: $L(f,s) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_{p \text{ good}} \left(1 - a_p(f) p^{-s} + p^{1-2s}\right)^{-1} \cdot \prod_{\text{bad}} (\,)$

  of an eigenform

Can write

$$p^{s/2} \Gamma(s) L(f,s) = \int_0^{i\infty} g(it) t^{s-1} dt$$

(Mellin transform of g)

Exercise: Show that the Euler product defining $L(A,s)$ converges for $\mathrm{Re}(s) > 3/2$

Hecke proved: $L(f,s)$ has analytic continuation & functional equation.

In particular, $L(f,1)$ makes sense.

Theorem (Eichler-Shimura): $L(A_f, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s)$

We know that $L(A_f, s)$ has analytic continuation thanks to this.

Conjecture (Birch-Swinnerton-Dyer): $\#A(\mathbb{Q}) < \infty \Leftrightarrow L(A,1) \neq 0$.

Theorem (Gross-Zagier + Kolyvagin):

If $L(A_f, 1) \neq 0$, then $A_f(\mathbb{Q}) < \infty$

Construction of $J_0^{\#}(p)$

$$I_e := \ker\left(\mathbb{T} \longrightarrow \prod_{L(f_1)\neq 0} \mathbb{T}/K_f\right)$$

Define $J_0^{\#}(p) := \dfrac{J_0(p)}{I_e} \sim \prod_{L(f,1)\neq 0} A_f$ and can check that $J_0^{\#}(p)(\mathbb{Q}) < \infty$.

Also, we can define also I_e as $\mathrm{Ann}_{\mathbb{T}}(e)\cdot A$, $e \in H_1(X_0(p), \mathbb{Q})$

where $e \hookrightarrow \mathrm{path}(0 \to i\infty)$.

The quotient $J_0^{\#}(p)$ is also called J_e or $J_e(1)$, and called the Winding quotient.

$\longleftarrow$

Fermat's Last Theorem.

Consider $x^p + y^p = z^p$, p prime ≥ 3.

Theorem (Wiles): $x^l + y^l = z^l$ has no non-trivial rational solution for $p \geq 3$.

Motivation for the approach

H. Chapdelaine: there's a 1-1 corresp. between

$$\left\{\begin{array}{l}\text{Strategies for studying}\\ \text{Primitive solutions}\\ \text{to } x^p+y^p=z^p,\ \gcd(x,y,z)=1\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{unramified coverings of}\\ \mathbb{P}^1\setminus\{0,1,\infty\} \text{ of}\\ \text{"signature" } (p,q,r)\end{array}\right\}$$

via $\Sigma_{p,q,r} = \left\{ \dfrac{a^p}{c^r},\ (a,b,c) \text{ primitive solution} \right\} \subseteq \mathbb{P}^1(\mathbb{Q})$ $\swarrow \pi$

Then $\pi^{-1}(\Sigma_{p,q,r}) \subseteq X(L)$ where L has ramification bounded indep of the solution.

- What are some coverings of $\mathbb{P}^1\setminus\{0,1,\infty\}$ of signature (p,p,p)?

1) $X = x^p + y^p + z^p$ and $\pi : X \to \mathbb{P}^1(\mathbb{Q})$ π has signature (p,p,p)

$$(x,y,z) \mapsto \frac{x^p}{z^p}$$

So one would study sol'ns to the Fermat eq by studying the Fermat curve.

$\downarrow$ more interesting example -

2) Modular curves : $X(n)$ = moduli space of (E, P_1, P_2) where (P_1, P_2) a basis of $E[n]$.

$$\begin{array}{c} X(2p) \\ \downarrow \pi \\ X(2) \end{array}$$

open set of $X(2)$.

Over $\mathbb{Z}[\frac{1}{2}]$, $X(2) = \operatorname{Spec}\left(\mathbb{Z}[\frac{1}{2}][\lambda, \frac{1}{\lambda}, \frac{1}{\lambda-1}]\right)$

Its universal cover is $y^2 = x(x-1)(x-\lambda)$ (Legendre curve).

Let $\lambda = \frac{a^p}{c^p} \in \sum_{ppp}$, $a^p + b^p = c^p$, $a, b, c \in \mathbb{Z}$, $\gcd(a,b,c) = 1$

$\pi^{-1}(\lambda)$ is defined over the field of p-division points of the curve $y^2 = x(x-1)\left(x - \frac{a^p}{c^p}\right)$

It is better to work with a twist of this curve:

$E_{a,b,c}$: $y^2 = x(x-a^p)(x-c^p)$ where $a \equiv 0 \ (4)$, $c \equiv -1 \ (4)$.

↑ Frey curve associated to the solution $a^p + b^p = c^p$.

We will consider the rep. of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ given by

$$\rho_{abc} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\left(E_{a,b,c}[p]\right) \simeq GL_2(\mathbb{F}_p)$$

- What do we know about ρ_{abc} ?

Theorem (Frey, Serre) : local properties of ρ_{abc} :

1) Unramified outside $2, p$.

2) $\rho_{abc}|_{D_2} \simeq \begin{pmatrix} \chi_{cyc}\,\psi & * \\ 0 & \psi^{-1} \end{pmatrix}$ ($D_2 = \mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2)$)

where $\chi_{cyc} : \mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2) \longrightarrow \mathrm{Aut}(\mu_p)$ cyclotomic character

ψ unramified character

$\neq 1$?

Jargon: ρ_{abc} is "ordinary" at 2.

3) ρ_{abc} is either ordinary at p or "finite", where "finite" means that it comes from the Galois action on the points of a finite-flat group scheme over $\mathbb{Z}_p$.

Proof of (Frey & Serre)

First, $\Delta_{E_{abc}} = 2^8 (abc)^{2p}$, $N = \mathrm{rad}(abc) = \prod_{\ell \mid abc} \ell$.

1) If $\ell \nmid 2abc \Rightarrow E_{abc}$ has good reduction at $\ell \Rightarrow \rho_{abc}$ is unramified at ℓ.

2) If $\ell \mid abc$, $\ell \neq 2, p \Rightarrow E_{a,b,c}$ has mult. reduction at ℓ.

$E(\mathbb{Q}_\ell^{ur}) \simeq (\mathbb{Q}_\ell^{unr})^\times / q^{\mathbb{Z}}$, q = Tate parameter $\in \ell\mathbb{Z}_\ell$

($\mathbb{Q}_\ell^{ur}$: maximal unramified ext of $\mathbb{Q}_\ell$)

← it's called the Tate model.

Also, $\Delta = q \prod (1-q^n)^{24}$

Δ is a p^{th} power for $\neq 2$

$\mathrm{ord}_\ell(q) = \mathrm{ord}_\ell(\Delta) \equiv 0 \ (p)$

$E(\overline{\mathbb{Q}_\ell})[p]$ (the points in) are defined over $\mathbb{Q}_\ell^{unr}(\zeta^a q^{b/p})$ where $0 \le a, b < p-1$, ζ a primitive root of 1.

(i.e. $\mathbb{Q}_\ell^{unr}(q^{1/p})$)

3) If $\ell = 2$, use the Tate model (exercise).

4) If $\ell = p$, $p \mid abc \Rightarrow E_{abc}$ has multiplicative reduction $\Rightarrow \rho_{abc}$ ordinary at p

$p \nmid abc \Rightarrow E_{abc}$ has good reduction. (Tate model)

Theorem (Mazur): Global properties of ρ_{abc} ($p > 13$)

ρ_{abc} is irreducible

Pf Exercise, use what we've seen lately for Mazur's theorem (the other one) to show it. (Hint: E_{abc} has points of multiplicative reduction)

So far:

non-trivial solutions of $x^p + y^p = z^p$ $\xrightarrow{R_1}$ { elliptic curves of squarefree conductor $N = \mathrm{rad}(abc)$ ← depends on the solution }

$\xrightarrow{R_4}$ { mod p representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ s.t. irreducible, unramified outside $2, p$, ordinary at 2 and ordinary or finite at p, odd ← check it (odd means that $\det(\rho(c)) = -1$) }

Remarks (cf Faltings' Theorem)

- Work with mod p reps, not ℓ-adic.
- We don't know that $R_{\mathbb{Q}}$ is finite-k-1.
- We want to show that $X(\mathbb{Q}) = \emptyset$, so enough to show that the last set (of reps) is empty.

Key new ingredient: connection between Galois reps and modular forms.

From Modular Forms to Galois Representations

Let $f = \sum a_n q^n \in S_2(N, \mathbb{C})$ be an eigenform of weight 2 on the group $\Gamma_0(N)$; K_f = field of Fourier coeffs

$\mathcal{O}_f$: ring generated over $\mathbb{Z}$ by the Fourier coeffs.

Let $\mathfrak{p}$ be a prime (ideal) of $\mathcal{O}_f$, and $K_{f,\mathfrak{p}}$, $\mathcal{O}_{f,\mathfrak{p}}$ the corresp. completions.

Theorem: There exists a Galois representation $\rho_{f,\mathfrak{p}}: G_{\mathbb{Q}} \to GL_2(K_{f,\mathfrak{p}})$ s.t.:

1) $\rho_{f,\mathfrak{p}}$ is unramified outside $N\mathfrak{p}$ (conductor).

2) $\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)$ has a characteristic polynomial of the form $X^2 - a_\ell(f)X + \ell$ ($a_\ell(f)$: ℓ^{th} coeff.)

Pf Use the Eichler-Shimura construction, which associates $f \rightsquigarrow A_f$ ($\dim A_f = 2$).

$V_p(A_f)$ is a $\mathcal{O}_f$-module, and so can consider $V_p(A_f) \otimes_T K_{f,\mathfrak{p}}$ (using $T \to K_{f,\mathfrak{p}}$).

$\cong K_{f,\mathfrak{p}}^2$ as $G_{\mathbb{Q}}$

Mod p reps: Denote $\rho_{f,\mathfrak{p}}: G_{\mathbb{Q}} \to GL_2(K_{f,\mathfrak{p}})$

Conjecture of $G_{\mathbb{Q}} \Rightarrow \rho_{f,\mathfrak{p}}(G_{\mathbb{Q}}) \sim GL_2(\mathcal{O}_{f,\mathfrak{p}})$

$\downarrow$ reduce mod $\mathfrak{p}$

$GL_2(\mathcal{O}_{f,\mathfrak{p}}/\mathfrak{p})$

Denote the $\overline{\rho_{f,\mathfrak{p}}}: G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{f,\mathfrak{p}}/\mathfrak{p})$

$\uparrow$ finite field.

What is conjectured is that one should be able to reverse this process: go from Galois reps to Modular Forms.

Conjecture (Serre): Let $\rho: G_{\mathbb{Q}} \to GL_2(\mathbb{F}_q)$ ($q = p^r$, p odd) be an irreducible Galois representation (complex conjugation $\rho(c) \sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$)

which is
- "ordinary" at p (for finite)
- "ordinary" at ℓ for all $\ell \mid N$ (N some fixed integer)
- unramified outside N.

Then $\exists\, f \in S_2(\Gamma_0(N))$, $\mathfrak{p} \lhd \mathcal{O}_f$ s.t. $\rho = \overline{\rho_{f,\mathfrak{p}}}$.

If that was true, then could make a reduction

$$\xrightarrow{R5} \left\{ SL_2\left(\Gamma_0(N)\right)/\mathbb{F}_p \right\} = \phi$$

!!

Remark: Serre's conjecture is almost a theorem (Khare-Wintenberger, 2006)

Theorem (Ribet): It is enough to show that $E_{abc} \overset{\text{Frey curves}}{\sim} A_f$ for some modular form on $\Gamma_0(N)$, $N = \mathrm{rad}(abc)$.

Theorem (Wiles): For all semistable (sqfree conductor) E, $\exists\, f \in S_2(\Gamma_0(N))$ such that $E \sim A_f$.

Importance of Wiles' Theorem:

1. It proves FLT.
2. Modularity of elliptic curves is key in understanding their arithmetic properties.
3. General method for relating Galois reps and modular forms.
   1) Proof of Artin Conjecture ($\Leftarrow$ in some cases) (Buzzard, Taylor) ($L(\rho, s)$ has analytic cont. where ρ an Artin rep.)
   2) Serre's conjecture (Khare, Wintenberger)
   3) Fontaine-Mazur conjecture
   4) Sato-Tate conjecture (Taylor, Harris, Clozel, ...).

Elliptic Curves & Modular Forms.

E an elliptic curve. Will study $E(K)$ or $\{E(L)\}_{L \supseteq K}$.

Mordell-Weil Thm: The group $E(K)$ is finitely-generated,

ie $E(K) \simeq \mathbb{Z}^r \oplus T$, $\#T < \infty$.

We know a lot about T. For instance, $\#T \leq C_{[K:\mathbb{Q}]}$

The difficulty stems then in understanding r.

Some words about the proof of M-W thm:

$$\begin{array}{c} E \\ \downarrow [n] \\ E \end{array} \Big/ \operatorname{Spec} \mathcal{O}_K\left[\frac{1}{\Delta n}\right]$$

Vocabulary of descent:

$$1 \to E[n] \to E \xrightarrow{n} E \to 1$$

Taking the G_K-invariants, get:

$$0 \to E(K)[n] \to E(K) \xrightarrow{n} E(K) \xrightarrow{\delta} H^1(G_K, E[n]) \to H^1(G_K, E)[n] \to 0$$

So have an injection:

$$0 \to \frac{E(K)}{nE(K)} \to H^1(G_K, E[n]) \to H^1(G_K, E)[n] \to 0$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$0 \to \frac{E(K_v)}{nE(K_v)} \to H^1(G_{K_v}, E[n]) \to H^1(G_{K_v}, E)[n] \to 0$$

The n^{th} Selmer gp of E/K is $Sel_n(E/K) := \operatorname{Ker}\left[H^1(K, E[n]) \to \prod_v H^1(K_v, E)[n]\right]$

(1) $Sel_n(E/K) \subseteq H^1_{n\Delta}(K, E[n])$ = classes unramified outside $n\Delta$.

Recall: $\delta(P)(\sigma) = \tilde{P}^\sigma - \tilde{P}$ where $n\tilde{P} = P$.

(2) $H^1_{n\Delta}(K, E[n]) < \infty$ by the theorem of Hermite.

$\Rightarrow \frac{E(K)}{nE(K)}$ is finite. (weak MW)

The extra ingredient of the proof is the heights.

We have an exact sequence:

$$0 \to \frac{E(K)}{nE(K)} \to Sel_n(E/K) \to Ш(E/K)[n] \to 0$$

where $Ш(E,K) = \ker\left[H^1(K,E) \to \prod_v H^1(K_v, E)\right]$

Question:

- When is $r > 0$?
- Computation of r, and a system of generators for $E(K)/T$.

Birch - Swinnerton-Dyer conjecture

Suppose now $K = \mathbb{Q}$.

For every $p \nmid \Delta$, define $N_p := \#E(\mathbb{F}_p)$.

Consider $\prod_{p<X} \frac{N_p}{p} \sim C_E (\log X)^r$ (heuristical observations)

We associate to E the Hasse-Weil L-function:

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

($a_p = p+1-N_p$; $a_p = 0$ or ± 1)

Facts:

- $L(E,s)$ converges for $\mathrm{Re}(s) > 3/2$. (exercise, use $|a_p| < 2\sqrt{p}$).
- Expand $L(E,1)$ formally and get $\prod_p \frac{p}{N_p}$

Conjecture (BSD):

$L(E,K)$ has analytic continuation, and $\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}\left(E(K)\right)$

From now on: $K = \mathbb{Q}$.

Theorem (Wiles, ...) $L(E,s)$ has an analytic continuation.

Theorem (Gross-Zagier + Kolyvagin): If $\mathrm{ord}_{s=1} L(E,s) \leq 1$ then BSD is true.

Key for these Thms: Connection with modular forms.

Theorem (Wiles, BCDT (Taylor, Diamond)): If $E/\mathbb{Q}$ is an elliptic curve of conductor N, then $\exists$ normalized eigenform of weight 2 on $\Gamma_0(N)$ such that E is isogenous to A_f (quotient of $J_0(N)$ associated to f by the Eichler-Shimura construction).

Consequences:

1) $L(E,s) = L(A_f, s) = L(f,s) = \sum_{n=1}^{\infty} a_n(f)\, n^{-s}$

$(2\pi)^s \Gamma(s) L(E,s) = \int_0^{i\infty} f(y) \left(\frac{y}{i}\right)^s \frac{dy}{y}$ $\Rightarrow$ analytic continuation of $L(E,s)$

2) There is a morphism

$$X_0(N) \longrightarrow J_0(N) \twoheadrightarrow A_f \xrightarrow{J_0(N) \twoheadrightarrow A_f \text{ isogeny, but assume for now (WLOG, actually) that they are equal.}} E$$

$$P \longmapsto (P) - (\infty)$$

$$\Phi : X_0(N) \to E$$

Φ is called the modular parametrization attached to E.

Computing Φ

Assume N squarefree. Let ω_E = Neron differential $\left(\frac{dx}{y}\right)$

Fact: $\Phi^*(\omega_E) = \omega_f = 2\pi i f(z)\, dz = \sum_{n=1}^{\infty} a_n q^n \frac{dq}{q}$

($\uparrow$ up to a small constant (1, 2, 2).)

For $\tau \in \mathcal{H}$, get an analytic formula for $\Phi(\tau)$: (related to $\#E(\mathbb{F}_p)$!)

$$\int_0^{\Phi(\tau)} \omega_E = \int_0^{\tau} \omega_f = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n, \quad q = e^{2\pi i \tau}.$$

(we know this because $L(E,s) = \sum a_n n^{-s}$)

$X_0(N) \to E$

Find rational or algebraic points on $X_0(N) \rightsquigarrow$ points on E.

- CM points and Heegner points.

Fix $K \subseteq \mathbb{C}$, K a quadratic imaginary field, $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$.

Theorem: If $\tau \in \mathcal{H} \cap K$, then $\Phi(\tau) \in E(K^{ab})$ (K^{ab} = max'l abelian extension of K)

Tomorrow: For certain K, τ we obtain a point $Q_1 \in X_0(N)(H)$ (Hilbert class field)

$$P_K := \mathrm{Trace}_K^H(\Phi(Q_1)) \in E(K).$$

- Gross-Zagier: $L'(E/K,1) = * \cdot \hat{h}(P_K)$ (non-zero factor)

$\Downarrow$

$L(E/K,1) \neq 0 \Leftrightarrow P_K$ of infinite order.

- Kolyvagin: If P_K has infinite order then $E(K)/\langle P_K \rangle$ is finite.

- **Heegner hypothesis**: all primes $\ell \mid N$ are split in $K/\mathbb{Q}$.

Let A be an elliptic curve with $\mathrm{End}(A) \simeq \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ ($D = \mathrm{disc}(K) < 0$)

Theory of complex multiplication $\Rightarrow A$ is defined over H = Hilbert class field of K.

Heegner hypothesis $\Rightarrow \exists\, \mathcal{N} \lhd \mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$

$A[\mathcal{N}]$ is cyclic of order N, so $(A, A[\mathcal{N}]) \in X_0(N)(H)$. $:= Q_1$

modular parametrization

Define $P_1 := \Phi(Q_1) \in E(H)$ and $P_K := \mathrm{Trace}_K^H(P_1) = \sum_{\sigma \in \mathrm{Gal}(H/K)} P_1^{\sigma} \in E(K)$

Theorem A (Gross-Zagier). (analytic)

$$\hat{h}(P_K) = * \cdot L'(E/K,1)$$

($*$ constant)

Remarks: 1) The proof is a direct, lengthy calculation. //

2) $L(E/K,s) = L(E/\mathbb{Q},s) \cdot L(E/\mathbb{Q}, \chi_K, s)$ where $\sum_{n=1}^{\infty} a_n \chi_K(n) n^{-s}$

χ_K is the quadratic character $\mathrm{Gal}(K/\mathbb{Q}) \to \pm 1$ $\left(\simeq (\mathbb{Z}/D\mathbb{Z})^{\times}\right)$

3) Heegner hypothesis $\Rightarrow$ the sign in the functional equation for $L(E/K,s)$ is $-1 \Rightarrow L(E/K,s)$ vanishes to odd order.

Rk 4) $\operatorname{sign}\left(L(E/\mathbb{Q}, s)\right) = -w_N$ where w_N = sign of Atkin-Lehner at N acting on f.

Theorem B (Kolyvagin): If P_K is of infinite order, then

1) $E(K)$ has rank one.
2) $\#Ш(E,K) < \infty$.

Proof of GZK:

$\operatorname{ord}_{s=1} L(E,s) \leq 1 \Rightarrow \exists K$ satisfying the Heegner hypothesis, and for which $\operatorname{ord}_{s=1} L(E^K, s) = 1$ (it's an analytic theorem on non-vanishing of twists of L-series). ⇐ (proved by Waldspurger, BFH, MM, ...)

By GZ, P_K is of ∞ order.

By Kolyvagin, $E(K)/\langle P_K \rangle < \infty$ and $\#Ш(E/K) < \infty$

Extra information about P_K: $P_K \in E(\mathbb{Q})/\text{tors}$ if $w_N = 1$

$P_K \in E(K)^-$ if $w_N = -1$

$\Rightarrow \operatorname{rank}\left(E(\mathbb{Q})\right) = \operatorname{ord}_{s=1} L(E,s)$, and $\#Ш(E/\mathbb{Q}) < \infty$

Kolyvagin's Theorem: bounding $E(K)$, $Ш$ in terms of P_K:

Main Point: P_K is part of a norm-coherent system of points.

Given n w/ $(n, N) = 1$. Let A_n := E.C. with $\operatorname{End}(A_n) = \mathbb{Z}\left[n \frac{1+\sqrt{D}}{2}\right]$ (order of conductor n)

CM theory ⇒ A_n is defined over H_n = ring class field of conductor n. ($\mathcal{O}_n$)

$$\operatorname{Gal}(H_n/K) \simeq A_K^\times / \left(K^\times \cdot \prod_\ell (\mathcal{O}_n \otimes \mathbb{Z}_\ell)^\times \cdot \mathbb{C}^\times\right)$$

ramified only at $\ell \mid n$.

Define Q_n corresponding to $(A_n, A_n[\mathfrak{N}]) \in X_0(N)(H_n)$ — trace $P_n = \Phi(Q_n)$.

If $\ell \nmid N_n$ is inert in K,

$$\boxed{\mathrm{Trace}_{H_n}^{H_{n\ell}} P_{n\ell} = a_\ell \cdot P_n} \mod \mathrm{Gal}(H_n/K)$$

$\leftarrow$ eff. divisor of deg $\ell+1$

Why? $\sum_{\sigma \in \mathrm{Gal}(H_{n\ell}/H_n)} Q_{n\ell}^{\sigma} \equiv T_\ell Q_n \mod \mathrm{Gal}(H_n/K)$.

Kolyvagin's Proof

Uses a p-descent. Fix a "descent prime" p in the following way:

1) $p \neq 2$
2) $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq Gl_2(\mathbb{Z}/p\mathbb{Z})$

- E has no CM $\Rightarrow$ by a theorem of Serre, $\forall$ is possible for ∞-many p.

Rk: can modify argument to make it work with CM curves.

Thm (Kolyvagin$_p$): If the image of P_K in $E(K)/pE(K)$ is nonzero, then $Sel_p(E/K) \simeq \mathbb{Z}/p\mathbb{Z}$.

In particular, $E(K)$ has rank 1, and $Ш(E/K)[p] = 0$.

We will only prove Kolyvagin$_p$:

Generalities on Selmer groups: (following Wiles)

K any number field,

M a finite module equipped with a continuous action of G_K.

$H^1(G_K, M) = H^1(K, M) = \text{Continuous 1-cocycles} / \text{coboundaries}$.

Given a prime v of K, v is said to be good for M if:

1) M is unramified at v (I_v acts trivially on M). } almost all primes are good.
2) $v \nmid \#M$.

If v is a good prime, have:

$$0 \to H^1(K_v^{unr}/K_v, M) \xrightarrow{inf} H^1(K_v, M) \xrightarrow{\partial_v} H^1(I_v, M)^{G_{K_v}}.$$

and call ∂_v: "residue map at v".

We call $H^1(\mathbb{F}_v, M)^{G_{K_v}}$: "singular part" of $H^1(K_v, M)$.
and $H^1(K_v^{un}/K_v, M)$ = "finite part" of $H^1(K_v, M)$
and denote them by $H^1_{sing}(K_v, M)$, $H^1_{fin}(K_v, M)$.

Def A set of Selmer conditions (for M and K) is a collection of subgroups $\{\mathcal{L}_v \subseteq H^1(K_v, M)\}_v$ s.t. $\mathcal{L}_v = H^1_{fin}(K_v, M)$ for all but finitely many places v.

Def: The Selmer group attached to $(M, K, \mathcal{L})$ is:

$$\{c \in H^1(K, M) : res_v(c) \in \mathcal{L}_v\} =: H^1_{\mathcal{L}}(K, M)$$

(connecting hom. in the Kummer sequence)

Main Example: $M = E[p]$, $\mathcal{L}_v = \delta_v\left(E(K_v)/pE(K_v)\right)$.

Then $H^1_{\mathcal{L}}(K, M) = Sel_p(E/K)$.

General Fact: any Selmer group $H^1_{\mathcal{L}}(K, M)$ is finite.

(Use thm of Hermite - Minkowski).

Problem: bound the size of $H^1_{\mathcal{L}}(K, M)$.

Duality: $M^* = Hom(M, \mathbb{G}_m) = Hom(M, \mu_{\#M})$ is called the Kummer dual.

Have a cup product: (Brauer group of K_v)

$$H^1(K_v, M) \times H^1(K_v, M^*) \longrightarrow H^2(K_v, \mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}$$

& called the "Tate pairing", denoted $\langle \cdot, \cdot \rangle$

Theorem (Tate): The pairing $\langle \cdot, \cdot \rangle_v$ is non-degenerate (on left & right), bilinear.

If v is good, then $H^1_{fin}(K_v, M)$ and $H^1_{fin}(K_v, M^*)$ are orthogonal complements under this pairing.

Corollary: if $\{\mathcal{L}_v\}$ is a set of Selmer conditions for $H^1(K_v, M)$, can define $\mathcal{L}_v^* := \mathcal{L}_v^{\perp}$ is also a set of Selmer conditions.

Def the Dual Selmer group : $H^1_{\mathcal{L}^*}(K, M^*)$

Theorem (Riemann-Roch for Selmer groups) (R. Greenberg) :

$$\frac{\#H^1_{\mathcal{L}}(K,M)}{\#H^1_{\mathcal{L}^*}(K,M^*)} = \frac{\#H^0_{\mathcal{L}}(K,M)}{\#H^0_{\mathcal{L}^*}(K,M^*)} \cdot \prod_v \frac{\#d_v}{\#H^0(k_v,M)}$$

Rk :

1) If v is good, then $\#H^1_{fin}(k_v, M) = \#H^0(k_v, M)$ (exercise).
   ⇒ the infinite product is in fact finite.

2) Flesh out the analogy with Riemann-Roch

Important case : $M = E[p]$, $E[p]^* = E[p]$ (Weil Pairing),
and if $\mathcal{L}_v = \delta_v(E(k_v)/p)$.

Lemma : $Sel_p(E/K)$ is equal to its dual.

Hence, we get by the previous theorem : (assume $p \neq 2$)

$$1 = \prod_v \frac{E(k_v)/pE(k_v)}{E[p](k_v)}$$

Exercise : prove this directly, for $K = \mathbb{Q}$. $\left(\begin{matrix} v = p & \sim p \\ v = \infty & \sim \frac{1}{p} \end{matrix}\right)$

Let S be a finite set of good primes $\ell \neq pN$.

Def

1) The relaxed selmer group $Sel_p(E/k)_{(S)} = \{ c \in H^1(K, E_p) \text{ s.t. } \forall v \notin S, res_v(c) \in \delta(E(k_v)/p) \}$

2) The restricted selmer group $Sel_p(E/k)_{[S]} = \{ c \in Sel_p(E/k) \text{ s.t. } res_v(c) = 0 \ \forall v \in S \}$

Easy lemma : $Sel_p(E/k)_{(S)}$ is the dual of $Sel_p(E/k)_{[S]}$.

Applying the Theorem,

$$\frac{\#Sel_p(E/k)_{(S)}}{\#Sel_p(E/k)_{[S]}} = \prod_{v\in S} \frac{\#H^1(k_v, E[p])}{\#E[p](k_v)} \overset{v\nmid p}{=} \prod_{v\in S} \frac{\#H^1(k_v, E[p])}{\#E(k_v)/pE(k_v)} =$$

$$= \prod_{v\in S} \#H^1_{sing}(k_v, E[p]).$$

Definition. A set S **controls** $Sel_p(E/k)$ if $Sel_p(E/k)_{[S]} = 0$.

(i.e. $Sel_p(E/k) \hookrightarrow \bigoplus_{v\in S} H^1_{fin}(k_v, E[p])$ is injective).

Exercise: what does MR for Selmer groups say when $M = \mathbb{Z}/p\mathbb{Z}$ (w/ trivial Galois action) ($M^* = \mu_p$). (~ class field theory).

Suppose S controls $Sel_p(E/k)$. Then

a) $\#Sel_p(E/k)_{(S)} = \prod_{v\in S} H^1_{sing}(k_v, E[p])$.

b) $0 \to Sel_p(E/k) \to Sel_p(E/k)_{(S)} \xrightarrow{\partial = \bigoplus_{v\in S} res_v} \prod_{v\in S} H^1_{sing}(k_v, E[p])$ is exact

($Sel_p(E/k)_{(S)}$ and $\prod_{v\in S} H^1_{sing}(k_v, E[p])$ have the same cardinality.)

Problem: bound the cokernel of ∂. (by manufacturing unramified classes)

Kolyvagin classes

$M = E[p]$ (E def/$\mathbb{Q}$), K a quadratic imaginary field

Def: A prime ℓ is called a **Kolyvagin prime** relative to (E, K, p) if

1) $\ell \nmid 2ND_K p$
2) ℓ inert in K.
3) $p \mid a_\ell(E)$ (where $a_\ell(E) = \ell + 1 - \#E(\mathbb{Z}/\ell\mathbb{Z})$).
4) $p \mid \ell + 1$

Lemma: There are infinitely-many Kolyvagin primes.

(ℓ is Kolyvagin $\Leftrightarrow Frob_\ell\left(K(E[p])/\mathbb{Q}\right) =$ complex conjugation) ← exercise

of) The classes $K(\ell) : \overleftarrow{\quad}$ assume ℓ is a Kolyvagin prime

Let $n_\ell := \#\,\mathrm{Gal}\left(H_\ell / H\right)$ (H my class field) $= \#\,G_\ell$. n_ℓ class field n_1, $\#G_\ell = \frac{\ell+1}{w}$, $w \mid 6$.

G_ℓ is cyclic, $= \langle \sigma_\ell \rangle$

$$D_\ell := \sum_{j=0}^{n_\ell - 1} j\, \sigma_\ell^j \in \mathbb{Z}[G_\ell]$$

(called the "Kolyvagin derivative")

Let $N_1 = \sum_{\sigma \in \mathrm{Gal}(H/K)} \sigma$, $N_\ell = \sum_{j=0}^{n_\ell - 1} \sigma_\ell^j$

Have that $(\sigma_\ell - 1) D_\ell = n_\ell - N_\ell$

Recall the Heegner point $P_\ell \in E(H_\ell)$.

$Q_\ell := N_1 \cdot D_\ell \cdot P_\ell \in E(H_\ell)$

Claim $Q_\ell \in \left(\dfrac{E(H_\ell)}{p E(H_\ell)} \right)^{\mathrm{Gal}(H_\ell/K)}$.

Pf $(\sigma_\ell - 1) Q_\ell = (\sigma_\ell - 1) D_\ell \cdot N_1 (P_\ell) = (n_\ell - N_\ell) N_1 P_\ell \equiv -N_1 N_\ell P_\ell =$ ($p \mid n_\ell$)

$= -N_1 \cdot a_\ell P_1 \equiv 0 \pmod p$ ($p \mid a_\ell$)

(for the other elts of Gal, it's even easier). //

Def $\overline{K(\ell)_0} \in H^1(G_K, E(H_\ell))[p]$ defined as

$$\overline{K(\ell)_0}(\sigma) = \frac{(\sigma - 1) Q_\ell}{p} \in E(H_\ell)$$

(can divide by p because $E(H_\ell)$ has no p-torsion)

Exercise: prove that $E(H_\ell)[p] = 0$.

Define $\overline{K(\ell)} \in H^1(K, E)$ which maps to $\overline{K(\ell)_0}$.

Define $K(\ell)$ be any lift of $\overline{K(\ell)}$ to $H^1(K, E[p])$

Theorem:

1) $\kappa(\ell) \in Sel_p(E/k)_{(\ell)}$

2) $\partial_\ell \kappa(\ell) \neq 0 \Leftrightarrow P_k \neq 0$ in $E(k_\ell)/pE(k_\ell)$

3) $\partial_\ell \kappa(\ell) \in H^1_{sing}(k_\ell, E[p])^{-\varepsilon}$ where ε = - sign in Functional equation for $L(E/\mathbb{Q}, s)$

Proof

1) Because H_ℓ/k is ramified only at ℓ.

2) $\partial_\ell \kappa_\ell(\ell) \neq 0 \Leftrightarrow \overline{\kappa(\ell)}(\sigma_\ell) \neq 0$ in $E(k_\ell)/p$

$\Leftrightarrow \underbrace{(\sigma_\ell - 1) D_\ell N_1 P_\ell}_{r} \neq 0$ in $E(k_\ell)/p$

$= \frac{n_\ell - N_1 P_\ell}{r} - \frac{a_\ell P_k}{r} \neq 0$ in $E(k_\ell)/p$

Impose more condition on ℓ (to simplify computation), say require $p^2 \mid \ell+1$, $p \| a_\ell$ (note $p^2 \mid \ell+1 \Rightarrow p^2 \mid n_\ell$).

Then $\Leftrightarrow \frac{a_\ell}{p} P_k \neq 0$ in $E(k_\ell)/p \Leftrightarrow P_k \neq 0$ in $E(k_\ell)/p$.

3) Exercise

Let ℓ_1, ℓ_2 be two Kolyvagin primes.

$\kappa(\ell_1 \ell_2)$ is constructed in the same way, but use $Q_{\ell_1 \ell_2} = D_{\ell_2} D_{\ell_1} N_1 P_{\ell_1 \ell_2}$

Theorem:

1) $\kappa(\ell_1 \ell_2) \in Sel_p(E/k)_{(\ell_1 \ell_2)}$

2) $\partial_{\ell_2}(\kappa(\ell_1 \ell_2)) \neq 0 \Leftrightarrow res_{\ell_2} \kappa(\ell_1) \neq 0$ in $H^1_{fin}(k_{\ell_2}, E[p])$.

3) $\kappa(\ell_1 \ell_2) \in H^1(k, E[p])^{\varepsilon}$

Pf Similar

• Proof of Kolyvagin's Theorem

Control Lemma: There exists a set $S = \{\ell_1, \dots, \ell_t\}$ of Kol. primes such that.

1) S controls $Sel_p(E/K)$
2) The image of P_K in $E(K_{\ell_i})/p$ is nonzero.
3) $res_{\ell_j}(\kappa(\ell_1)) \neq 0$ for $j = 1, \dots, t$.

Pf Chebotarev. applied to $K(E[p^2], \frac{1}{p}P_K)$ and the field cut out by a basis $\langle s_1, \dots, s_m \rangle$ for $Sel_p(E/K)$. //

End of pf:

$$0 \to Sel_p(E/K)^{-\varepsilon} \to Sel_p(E/K)^{-\varepsilon}_{(S)} \xrightarrow{\partial^{-\varepsilon}} \bigoplus_{\ell \in S} H^1_{sing}(K_\ell, E[p])^{-\varepsilon}$$

Step 1: $\partial(\kappa(\ell_1)), \dots, \partial(\kappa(\ell_t))$ are linearly indep in over $\mathbb{F}_p$.

Hence the $\operatorname{coker}(\partial^{-\varepsilon}) = 1 \Rightarrow Sel_p(E/K)^{-\varepsilon} = 1$

Step 2: $\partial(\kappa(\ell_1\ell_2)), \partial(\kappa(\ell_1\ell_3)), \dots, \partial(\kappa(\ell_i\ell_j)), \dots$

are also linearly indep in $\mathbb{F}_p$.

Hence $\dim_{\mathbb{F}_p} \operatorname{coker}(\partial^{\varepsilon}) \leq 1 \Rightarrow \dim_{\mathbb{F}_p}(Sel_p(E/K))^{\varepsilon} \leq 1$

$\Rightarrow Sel_p(E/K)^{\varepsilon} = \langle \delta(P_K) \rangle$.

Question: What about other number fields?

F = totally real field. Then a lot of this generalizes.

Shimura Curves:

Let S be a finite set of places of F containing all the archimedean ones.

Assume $\#S$ is odd.

Theorem: There exists a curve X_S over F having the following properties:

1) (Analytic properties) For all $v \in S$, let $B_{S\setminus\{v\}}$:= the quaternion algebra ramified at $S\setminus\{v\}$

Define $R(v) := \begin{cases} \text{Maximal order in } B_{S\setminus\{v\}} & \text{if } v \text{ archimedean.} \\ \text{Maximal } \mathcal{O}_F[\frac{1}{v}]\text{-order in } B_{S\setminus\{v\}} & \text{if } v \text{ is non-archimedean.} \end{cases}$

We have also $\iota_v : B \otimes_F F_v \xrightarrow{\sim} M_2(F_v)$, and write:

$\Gamma(v) := \iota_v(R(v)^\times_1) \subseteq SL_2(F_v)$

Denote by $\mathbb{C}_v$ the completion of $\overline{F_v}$ ($\mathbb{C}_v = \mathbb{C}$ if v archimedean).

Also, $\Gamma(v) \underset{\text{discrete}}{\subseteq} \mathcal{H}_v := \begin{cases} \mathbb{P}_1(\mathbb{C}) \setminus \mathbb{P}_1(\mathbb{R}) & \text{if } v \text{ archimedean} \\ \mathbb{P}_1(\mathbb{C}_v) - \mathbb{P}_1(F_v) & \text{if } v \text{ non-archimedean} \end{cases}$

Then: $X_S(\mathbb{C}_v) \xrightarrow{\sim} \Gamma(v)\backslash\mathcal{H}_v$ as $\begin{cases} \text{Riemann surfaces if } (v \text{ arch.}) \\ \text{Rigid analytic curves } (v \text{ non-arch}) \end{cases}$

2) (CM points) If K is a quadratic subfield of $B_{S\setminus\{v\}}$ such that

$\iota_v(K^\times) \subseteq \mathcal{H}_v$ has a fixed point $\tau_K \in \mathcal{H}_v$

Then τ_K corresponds to a point on $X_S(\mathbb{C}_v)$ defined over an abelian extension of K. (K CM)

not a theorem so far!

3) (Shimura Taniyama Conjecture): conductor = ideal of F

Let E be an elliptic curve / F with $N_{E/F} = \prod_{\substack{v \in S \\ v \text{ non-arch.}}} v$

Then there is a nonconstant morphism

$\Phi_E : J_S \to E$ def. over F, where $J_S = \mathrm{Jac}(X_S)$.

(a lot can be proved in this direction, but not all)

More Facts:

Supersingular points on $X_S/\mathcal{O}_{F/v} \longleftrightarrow B_{S\cup\{v\}}$.

Example

- Now take $F=\mathbb{Q}$, $S=\{\infty\}$. Then $X_S = X_0(1)$
- $F=\mathbb{Q}$, $S=\{\infty, 2, 3\}$ cf. John Voight's lecture.
- $F=\mathbb{Q}(\zeta_q^+)$, $S=\{\infty_1, \infty_2, \infty_3\}$

p-adic uniformization

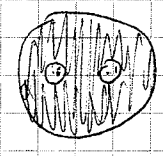
$F=\mathbb{Q}$, $S=\{-\}$, $p\in S$, and study $X_S/\mathbb{C}_p$.

$X_S(\mathbb{C}_p) = \Gamma\backslash\mathcal{H}_p$, $\Gamma \subseteq SL_2(\mathbb{Q}_p)$

$J(\mathbb{C}_p) \longrightarrow E(\mathbb{C}_p)$

Def: A rigid analytic function on $\mathcal{H}_p$ is a function $f: \mathcal{H}_p \to \mathbb{C}_p$ whose restriction to every good subset A (Affinoid) is a uniform limit of rational functions with poles outside A.

(An Affinoid is a subset of $\mathbb{C}_p$ with certain properties of closedness:
eg. typical example: $\{z\in\mathbb{C}_p : |z|\le 1\}$.
To get an Affinoid in $\mathcal{H}_p$, for instance $\{z\in\mathbb{C}_p : |z|\le 1 \text{ and } |z-a|\ge 1-\varepsilon\}$ for $a=0,1,\dots,p-1$)



$(p=2)$

Boundary measures: A measure on $\mathbb{P}_1(\mathbb{Q}_p)$ μ is a finitely additive bounded function

$\{\text{compact open } U\subseteq \mathbb{P}_1(\mathbb{Q}_p)\} \longrightarrow \mathbb{C}_p$

$\mu \in \mathrm{Meas}(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{C}_p)$, $f_\mu(z) = \int_{\mathbb{P}_1(\mathbb{Q}_p)} \frac{d\mu(t)}{z-t} = \lim_{\mathbb{P}_1(\mathbb{Q}_p)=\bigcup U_\alpha} \sum_{U_\alpha} \frac{\mu(U_\alpha)}{z-t_\alpha}$, $t_\alpha\in U_\alpha$.

Have $\mathrm{Meas}(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{C}_p) \xrightarrow{\sim}$ rig. analytic/diff. on $\mathcal{H}_p$ (fun exercise)

$\mu \longmapsto f_\mu(z)\,dz$

↑ finite dimensional $\mathbb{C}_p$-vectorspace equipped with a Hecke action.

Coleman integral

$$\int_{\tau_1}^{\tau_2} f_\mu(\tau)\, d\tau := \int_{\mathbb{P}_1(\mathbb{Q}_p)} \log_p\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu(t)$$

(choose a branch of $\log_p : \mathbb{C}_p^\times \to \mathbb{C}_p$)

Suppose that $\mu \in \mathrm{Meas}\left(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{Z}\right)^{\Gamma}$ (i.e. μ is $\mathbb{Z}$-valued)

can define the multiplicative integral:

$$\prod_{\tau_1}^{\tau_2} f_\mu(\tau)\, d\tau := \prod_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu(t) = \lim_{U_\alpha} \prod \left(\frac{t_\alpha - \tau_2}{t_\alpha - \tau_1}\right)^{\mu_f(U_\alpha)} \in \mathbb{C}_p^\times$$

Having $\Phi(f)$ defined, then

$$\Phi_E\left((\tau_2)-(\tau_1)\right) = \exp\left(\int_{\tau_1}^{\tau_2} f(\tau)\, d\tau\right) \in \mathbb{C}_p$$

(exp: Tate uniformization)

Remark about the theorem of GZ-K.

The proof of GZ-K works almost without change for A_f, i.e.

$$\prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, 1) = L(A_f, 1) \neq 0 \Rightarrow \#A_f(\mathbb{Q}) < \infty$$

(This was also done by Kolyvagin & Logachev)

Def If F is a totally real field, then E/F is said to be arithmetically uniformizable if $\exists\, X/F$ Shimura curve s.t. $J(X) \to E/F$ (non-constant)

Note: A.U. $\Rightarrow$ modular. (not the converse!).

Theorem (Zhang, Kolyvagin-Logachev): If E is A.U., then

$$\mathrm{ord}_{s=1} L(E/F, s) \leq 1 \Rightarrow \mathrm{rank} = \mathrm{ord}_{s=1}$$

"Mysteries":

1) F a real quadratic field, E having everywhere good reduction of a (quadratic) twist of such a curve. Then one can show E is not A.U.

- $\mathrm{ord}_{s=1} L(E/F, s) = 0 \Rightarrow \#E(F) < \infty$ (Tian, Zhang, + Logo).
- $\mathrm{ord}_{s=1} L(E/F, s) = 1 \Rightarrow ???$

More history:

2) F = imaginary quadratic field (Matt Greenberg, talk about this).

Heegner points, revisited

$X_0(N) \longrightarrow E$ / $\mathbb{Q}$.

If ℓ split in K $\forall \ell \mid N$ (Heegner hyp) then $\exists$ Heegner points.

H = ring class field of K, $(\mathrm{disc}(H), N) = 1$

Have that
$$L(E/H, s) = \prod_{\chi : \mathrm{Gal}(H/K) \to \mathbb{C}^\times} L(E/K, \chi, s)$$

Also,
$$L(E/K, \chi, s) \longleftrightarrow L(E/K, \overline{\chi}, 2-s)$$
$$\| \qquad\qquad\qquad \| \qquad\qquad\qquad \| \qquad\qquad\qquad \|$$
$$L(E/K, \chi, s) \qquad L(E/K)^{\|} \qquad L(E/K, \chi, 2-s)$$

$\Rightarrow$ each of the factors of the product vanishes at odd order.

Hence, by parity, $\mathrm{ord}_{s=1} L(E/H, s) \geq [H:K]$ "$\overset{\text{BSD}}{\Longrightarrow}$" $\mathrm{rank}(E(H)) \geq [H:K]$

One can prove that if $\mathrm{ord}_{s=1} L(E/H, s) = [H:K]$ (equality!) Then BSD is satisfied (i.e. $\mathrm{rank}(E(H)) = [H:K]$).

Mystery: If K is a real quadratic fld, the analysis of signs goes through, ook.

Simplest case: K = r. quad. fld, $N = p \cdot M$, $p \nmid M$

Modified Heegner hyp: 1) All $\ell \mid M$, ℓ split in K.

2) p is inert in K.

Conjectural formula for these "Stark-Heegner points".

$\hookrightarrow$ 1

p-adic construction

work in $\mathcal{H}_p$ instead of $\mathcal{H}$. But Shimura curves will not contain these "Stark Heegner points".

We expect that there are ∞ many real quadratic fields of class number 1.

Let $\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) : M \mid c \right\}$.

$\Gamma \subset \mathcal{H}$ and $\Gamma \subset \mathcal{H}_p$. (by Möbius transformations).

The action of Γ on $\mathcal{H}_p \times \mathcal{H}$ is discrete (not on each of the factors, though).

Goal: Define a map $\Phi : \Gamma \backslash (\mathcal{H}_p \cap K) \longrightarrow E(\mathbb{C}_p)$

conjecture: $\Gamma \backslash (\mathcal{H}_p \cap K) \longrightarrow E(K^{ab}) \longrightarrow E(\mathbb{C}_p)$

(E ec. / $\mathbb{Q}$ of conductor $N = pM$...)

The definition of Φ is analytic.

Step 1: Modular symbols: $f(z)dz$ classical modular form on $\Gamma_0(N) \backslash \mathcal{H}$ associated to E.

Given $r, s \in \mathbb{P}_1(\mathbb{Q})$, define $I_f\{r \to s\} := \frac{\mathrm{Re}\left(\int_r^s f(z)dz\right)}{\Omega^+} \in \mathbb{Z}$ (by choosing Ω^+ appropriately)

(Picture of f as $\overset{r}{\bullet} \overset{s}{\bullet} \twoheadrightarrow E$).

Step 2:

Proposition: $\exists$ a unique system of measures on $\mathbb{P}^1(\mathbb{Q}_p)$, indexed by pairs $(r, s) \in \mathbb{P}^1(\mathbb{Q})$ and denoted $\mu\{r \to s\}$ - satisfying:

(1) $\mu\{r \to s\}(\mathbb{P}_1(\mathbb{Q}_p)) = 0$; $\mu\{r \to s\}(\mathbb{Z}_p) = I_f\{r \to s\}$.

(2) (Γ-invariance): $\mu\{\gamma r \to \gamma s\}(\gamma U) = \mu\{r \to s\}(U)$

($\forall r, s \in \mathbb{P}_1(\mathbb{Q})$, $\forall \gamma \in \Gamma$, $\forall U \subseteq \mathbb{P}_1(\mathbb{Q}_p)$).

(3) $\mu\{r \to s\} + \mu\{s \to t\} = \mu\{r \to t\}$.

Proof Use the fact that Γ acts "transitively" (only two orbits) on the open balls in $\mathbb{P}_1(\mathbb{Q}_p)$.

Step 3: Define $\ell_{r\to s}(z) := \int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{1}{z-t}\, d\mu_{\{r\to s\}}(t)$

Properties: $\ell_{\gamma r\to \gamma s}\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 \ell_{r\to s}(z) \quad \forall\, \gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma.$

Coleman integrals: choose a $\log: \mathbb{C}_p^\times \to \mathbb{C}_p$

$$\int_{\tau_1}^{\tau_2} \ell_{r\to s}(z)\, dz = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_{\{r\to s\}}(t).$$

Have also the multiplicative corresponding integral, $\oint_{\tau_1}^{\tau_2} \ell_{r\to s}(z)\, dz$.

Notation: write $\int_{\tau_1}^{\tau_1} \ell_{r\to s}(z)\, dz = \int_{\tau_1}^{\tau_2}\int_r^s \omega_f$

where think of ω_f as the "matrix Hilbert modular form on $\Gamma \backslash (\mathcal{H}_p \times \mathcal{H}_p)$ of weight $(2,2)$".

Properties:

- $\int_{\tau_1}^{\tau_2}\int_r^s \omega_f + \int_{\tau_2}^{\tau_3}\int_r^s \omega_f = \int_{\tau_1}^{\tau_3}\int_r^s \omega_f$ (1st var)
- $\int_{\tau_1}^{\tau_2}\int_r^s \omega_f + \int_{\tau_1}^{\tau_2}\int_s^t \omega_f = \int_{\tau_1}^{\tau_2}\int_r^t \omega_f$ (2nd var)
- $\int_{\gamma\tau_1}^{\gamma\tau_2}\int_{\gamma r}^{\gamma s} \omega_f = \int_{\tau_1}^{\tau_2}\int_r^s \omega_f$ [also have the mult integral in the same way, and $\log\left(\prod\int \omega_f\right) = \int\int \omega_f$]

Step 4: Choose $\log: \mathbb{C}_p^\times \to \mathbb{C}_p$ s.t. $\log(q) = 0$, where

q = Tate period of E.

Theorem (Rapoport, Greenberg, Stevens): There is a unique function $\mathcal{H}_p \times \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}_p$ denoted by $(\tau, r, s) \mapsto \int_r^s \omega_f$ satisfying:

1) $\int_{\tau_1}^{\tau_2}\int_r^s \omega_f = \int_{\tau_1}^{\tau_1}\int_r^s \omega_f = \int_{\tau_1}^{\tau_2}\int_r^s \omega_f$
2) (Γ-invariance) $\int_{\gamma\tau}^{\gamma\tau}\int_{\gamma r}^{\gamma s} \omega_f = \int_\tau^\tau \int_r^s \omega_f \quad \forall\, \gamma \in \Gamma.$
3) $\int_\tau^\tau \int_r^s \omega_f + \int_\tau^\tau \int_s^t \omega_f = \int_\tau^\tau \int_r^t \omega_f.$

Step 5: $\tau \in \mathcal{H}_p \cap K$. A simple calculation shows that $\mathrm{Stab}_{\mathrm{Gal}}(\tau) \simeq \langle \gamma_\tau \rangle$ (gen. by one element)

$$J_\tau = \int_r^\tau \int_r^{\gamma_\tau r} \omega_t \in \mathbb{C}_p$$

$$J_\tau^X = \int_x^\tau \int_x^{\gamma_\tau x} \omega_t \in \mathbb{C}_p^\times / q^{\mathbb{Z}}$$

$\Phi(\tau) = P_\tau = \Phi_{\mathrm{Tate}}(J_\tau^X) \in E(K_p)$ (Exercise: Show that J_τ does not depend on r)

Conjecture: The collection of $\Phi(\tau)$ as τ ranges over $\mathcal{H}_p \cap K$ behave "in all respects" like Heegner points.

Evidence: Lots of numerical evidence (check Darmon's website).

Theorem (Darmon, Bertolini): If $\tau_1, \dots, \tau_h$ are a complete set of points of conductor 1 ($h = h(K)$), then

$\Phi(\tau_1) + \cdots + \Phi(\tau_h) = P_K \in E(K)$ modulo $E(K_p)_{\mathrm{tors}}$.

and $P_K \neq 0 \iff L'(E/K, 1) \neq 0$.

Conj (Uniform boundedness for the torsion) (Ogg '79 Ronconi 1901, Lev: 1966):

$\forall d \geq 1$, $\exists B(d)$ s.t. $\forall E/K$ $[K:\mathbb{Q}]=d$,

$\#(E(K)_{tors}) \leq B(d)$

This is now a theorem by Merel (1995).

Thm 2 (Merel): p prime. Let E/K an e.c., $[K:\mathbb{Q}]=d \geq 1$.

Suppose $\exists P \in E(K)$ a p-torsion pt. Then $p \leq d^{3d^2}$.

By Faltings & Frey, Thm 2 $\Rightarrow$ Thm 1. ($\Leftarrow$ proven by Mazur & Kamienny)

Remarks:

1) For $d=1$, this is Mazur's theorem.

2) Oesterlé improved the bound d^{3d^2}

3) The bound $B(d)$ is not explicit at all. However, in ~1999 Parent bounded the p^r-torsion $r \in \mathbb{Z}_{\geq 1}$ $\rightsquigarrow$ explicit $B(d)$ which is exponential in d.

Conjecture: there is a polynomial bound.

§1. Mazur's method.

1.1. Let E/K $[K:\mathbb{Q}]=d$ (>1), $P \in E(K)$ p-torsion pt.

Then (E,P) defines a point $\tilde{x} \in Y_1(p)(K)$.

$$\begin{array}{ccc} X_1(p)(K) & \ni & \tilde{x}=(E,P) \\ \downarrow & & \uparrow \\ X_0(p)(K) & \ni & x=(E,\langle P\rangle) \end{array}$$

Let $\sigma_1,\dots,\sigma_d : K \hookrightarrow \mathbb{C}$; $\underline{x}=(\sigma_1(x),\dots,\sigma_d(x)) \in X_0(p)^{(d)}$

if ℓ smooth over $\mathbb{Z}=\mathbb{Z}[1/p]$.

(d): d^{th} symmetric power of $X_0(1)$

Then $X_0(p)^{(d)}/G_d =: X_0(p)^{(d)}$

1.2.

$$X_0(p)^{(d)} \longrightarrow J_0(p) \longrightarrow J_e \quad \text{(winding quotient)}$$

$$(Q_1, \dots, Q_d) \longmapsto [(Q_1)+\cdots+(Q_d)-d(\infty)]$$

Thm (Mazur - Kamienny):

If $\phi_e^{(d)}$ is a formal immersion at $\infty^{(d)}$ = image of $(\infty, \dots, \infty)$ in $X_0(p)^{(d)}$.

then $Y_1(p)(K) = \phi$ for all #field K, $[K:\mathbb{Q}]=d$.

We will see that $\exists$ a formal immersion for $p>7$, for $d=1$ and $d>1$.

(the case $d=1$ will finish Mazur's theorem).

Need a criterion for formal immersion. (Recall $\varphi: X \to Y$ FI if $\varphi^\sharp : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is surjective at $x \in X$)

Criterion (differential criterion):

if $k(y) \xrightarrow{\sim} k(x)$ and $\mathrm{Cot}_y Y \to \mathrm{Cot}_x X$.

↑ ok in this setting.

we know $\mathrm{Cot}(J_e/\mathbb{Z}) \overset{?}{\hookrightarrow} \mathrm{Cot}(J_0(p)/\mathbb{Z})$ $\quad (\mathcal{O} = \mathbb{Z}[1/p])$

↑ ✓ due to Mazur & Raynaud

Then $\mathrm{Cot}(J_0(p)/\mathbb{Z}) \xrightarrow{\Phi^*}_{\sim} S_2(p, \mathbb{Z})$. (where $\Phi: X_0(p) \to J_0(p)$)

↑ due to Grothendieck-Serre duality.

Can take $S_2(p|\mathbb{Z}) \hookrightarrow \mathbb{Z}[\![q]\!]$

↑ q-expansion principle

Then $\mathrm{Cot}(J_e/\mathbb{Z}) \longrightarrow \mathrm{Cot}_{\infty^{(d)}} X_0(p)^{(d)}$?

q a formal parameter of $X_0(p)$ at ∞, $\hat{\mathcal{O}}_{X_0(p),\infty} \simeq \mathbb{Z}[\![q]\!]$

$q_1, \dots, q_d$ $\qquad X_0(p)^d$

$\downarrow$

$X_0(p)^{(d)}$

If $\sigma_1, \dots, \sigma_d$ are the symmetric functions on $q_1, \dots, q_d$, there are formal powers for $X_0(p)^{(1)}$

Hence $\mathrm{Cot}_{\infty^{(d)}} X_0(p)^{(d)}/\mathbb{Z}$ is a free $\mathbb{Z}$-module of rank d,

with a basis given by $d\sigma_1, \dots, d\sigma_d$.

Lemma: Let $\omega \in \mathrm{Cot}\, J_0(p)/\mathbb{Z}$ s.t. $\phi^*(\omega)$ has a q-exp $\sum_{m\geq 1} a_m q^m \frac{dq}{q}$,

then $\Phi^{(d)*}(\omega) = a_1 d\sigma_1 + a_2 d\sigma_2 + \cdots + (-1)^{d-1} a_d d\sigma_d$

Pf

$$\begin{array}{ccc} X_0(p)^d & & \\ \pi \downarrow & \Rightarrow & \pi^* \Phi^{(d)*}(\omega) = \sum_{i=1}^{d} \sum_{m\geq 1} a_m q_i^m \frac{dq_i}{q_i} = \sum_{m\geq 1} a_m m^{-1} d s_m \\ X_0(p)^{(d)} & & \end{array}$$

$s_m = \sum_{i=1}^{d} a_i^m$

It's an exercise (use Newton Formula) $\Rightarrow m^{-1} d s_m = (-1)^m d\sigma_m$.

- Ending of the case $d=1$:

Let $\omega \in \mathrm{Cot}\, J_e$ s.t. $\phi^*\omega \in S_2(p, \mathbb{Z})$ is an eigenform.

Then by the q-expansion principle, its q-exp is not identically 0.

So since ω is an eigenform $a_1(\omega) \neq 0$ (ow. $a_m(\omega) = 0$ $\forall m$).

So $a_1(\omega)$ generates $\mathrm{Cot}_\infty X_0(p) \simeq \mathbb{Z}$

$\| \phi_e^{(d-1)*}(\omega)$

Theorem (Mazur - Kurokawa): TFAE:

1) $\phi_e^{(d)}$ is a $\mathbb{P}^1$ at $\infty^{(d)}$

by the lemma ⟸ 2) There exist $f_1, \dots, f_d \in S_2(p, \mathbb{Z})[I_e]$ ($I_e f_i = 0$; I_e is an ideal of the Hecke algebra that stabilizes $S_2(p, \mathbb{Z})$)

such that $\left(a_1(f_i), \dots, a_d(f_i)\right)_{i=1\dots d}$ are $\mathbb{Z}$-linearly independent.

3) The image of $T_1, \dots, T_d$ in $\mathbb{T}/I_e$ are $\mathbb{Z}$-linearly independent. ($\mathbb{T}/I_e$: Hecke algebra)

((3) is because $S_2(p, \mathbb{Z}) \simeq \mathrm{Hom}(\mathbb{T}, \mathbb{Z})$, $f \mapsto (t \mapsto a_1(tf))$)

Write now $X = X_0(p)(\mathbb{C}) \simeq \Gamma_0(p) \backslash \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$

$e \in H_1^*(X, \mathbb{Z})$, "almost equal" to $\{0, \infty\}$.

Recall $\mathbb{T} \hookrightarrow \mathrm{End}\, J_0(p)$, and $\mathbb{T}$ acts also on $H_1(X, \mathbb{Z})$.

Moreover, $\mathbb{T}e$ is a $\mathbb{T}/I_e$-module, free of rank 1.

So condition (1)–(3) of prev. theorem are also equivalent to

4) $T_1 e, \dots, T_d e$ are $\mathbb{Z}$-linearly independent in $\mathbb{T}e$.

$\Longleftrightarrow$

§2. Heart of Merel's proof

$$H_1(X,\mathbb{R}) \xrightarrow{\sim} \mathrm{Hom}\left(S_2(\Gamma,\mathbb{C}),\mathbb{C}\right) \quad \text{iso of } \mathbb{R}\text{-vectorspaces}$$
$$c \longmapsto \left(\omega \mapsto \int_c \omega\right)$$

Defined in Dormon's lectures $e :=$ pullback of $\left(\omega \mapsto -\int_0^{i\infty} \omega\right)$

There is a difference between e and $-\{0,\infty\}$, due to the "Eisenstein part" of $H_1(Y, \text{cusps}; \mathbb{Z})$ on which T_n acts by $\sum_{d \mid n,\ (d,p)=1} d$ ($\sigma^1(n) = \sum_{d\mid n} d$, $\times \sigma^1(n)$)

Recall that we want to prove that for $p \geq d^{3d^2}$, $T_1 e = e, T_2 e, \dots, T_d e$ are $\mathbb{Z}$-linearly indep.

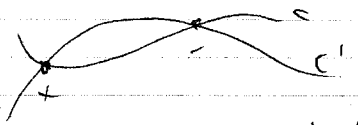
It suffices to prove that

$e, t_1 e, \dots, t_d e$ are $\mathbb{Z}$-l.i., where $t_i = T_r - \sigma^1(r)$

This is better because $t_r e = -t_r\{0,\infty\}$.

Idea of the proof:

Use the "intersection product" $\bullet : H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$



Suppose $\lambda_1 e + \lambda_2 t_2 e + \cdots + \lambda_c t_c e = 0$, $c \leq d$

Strategy: find $x_c \in H_1(X,\mathbb{Z})$ s.t. $\begin{cases} t_c e \cdot x_c \neq 0 \\ t_r e \cdot x_c = 0 \ \forall r < c \end{cases} \Rightarrow \lambda_c = 0 \Rightarrow$ ok

$\downarrow$

To find $\mathfrak{X}_c$, the key fact is

- If a presentation of $H_1(X, \mathbb{Z})$ by generators $\xi(\kappa)$ and relations.
- We know how to compute $\xi(\kappa) \cdot \xi(\kappa')$.

We need to express $t_r e$ in terms of the $\xi(\kappa)$'s.

2.1. Manin Symbols

relative homology

Let $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, and take a geodesic from α to β which leads to a homology class $\{\alpha, \beta\} \in H_1(X, \text{cusps}; \mathbb{Z})$

It's an exercise that $\{\alpha, \beta\}$ is a sum of the type $\{\frac{b}{d}, \frac{a}{c}\}$ where $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$ (use continuous fractions).

Also, if $\Gamma_0(p)\alpha = \Gamma_0(p)\beta$, then $\{\alpha, \beta\} \in H_1(X, \mathbb{Z})$.

$\{\frac{b}{d}, \frac{a}{c}\}$ depends only on the class of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(p) \backslash SL_2(\mathbb{Z})$

So get a map (surjective) $\mathbb{Z}[\Gamma_0(p) \backslash SL_2(\mathbb{Z})] \twoheadrightarrow H_1(X, \text{cusps}; \mathbb{Z})$.

$$\Gamma_0(p)\, g \longmapsto \left\{\frac{b}{d}, \frac{a}{c}\right\} = \{g0, g\infty\}.$$

We have an isomorphism

$$\Gamma_0(p) \backslash SL_2(\mathbb{Z}) \longrightarrow \mathbb{P}^1(\mathbb{F}_p) \quad \text{so write } \xi(c/d) = \xi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto (c, d)$$

Now for $\kappa \neq \mathbb{F}_p^*$, $\xi(\kappa) \overset{\text{exercise}}{=} \{0, 1/\kappa\} \Rightarrow \xi(\kappa) \in H_1(X, \mathbb{Z})$

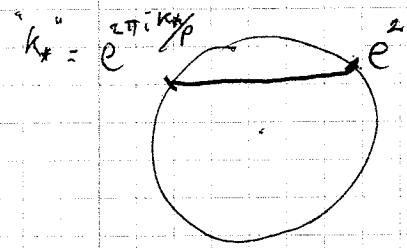
(conj by $\Gamma_0(p)$)

Also these elements $\xi(\kappa)$ are generators, together with

$$\xi(0) := -\xi(\infty) := \{0, \infty\}.$$

"Lemme des Cordes" (Mercel)

Let $\kappa, \kappa' \in \{1, \dots, p-1\}$, denote by $\kappa_* \in \{1, \dots, p-1\}$ s.t. $\kappa \cdot \kappa_* \equiv -1 \ (p)$



ℓ_κ the chord from $e^{2\pi i \kappa/p}$ to $e^{\pi i \kappa/p}$ in the unit circle.

Then $\xi(\kappa) \cdot \xi(\kappa') = \ell_{\kappa'} \wedge \ell_{\kappa_*}$ (# of intersection $(-1, 0, +1)$)

2.2. "Black Box"

$$t_r e = -\sum_{\binom{u\ v}{w\ t}\in X_r} \xi\left(\frac{w}{t}\right) \quad , \quad X_r := \left\{ \binom{u\ v}{w\ t} = M \in M_2(\mathbb{Z}) \;\middle|\; \begin{array}{l} \det M = r \\ u > v \geq 0 \\ 0 < w < t \end{array} \right\}$$

(when) $t_r e = -tr\{0,\infty\} = \sum_{d|r} \left\{\frac{b}{d}, \infty\right\}$ $\rightsquigarrow$ cont. fractions

and also $(p-1)\, e \bullet \xi(\kappa) = \frac{\kappa_\ell - \kappa}{r}(p-1) - 12\, S(\kappa, p)$ Dedekind sums.

2.3 - End of the proof

$\lambda_1 e + \cdots + \lambda_d t_d e = 0$

- $\underline{\lambda_1 = 0}$

Will look for $\xi(\kappa)$ s.t. $e \cdot \xi(\kappa) \neq 0$ (1)

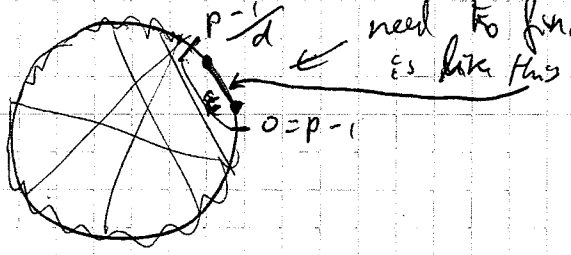
$t_r e \cdot \xi(\kappa) = 0 \quad \forall r > 1$ (2)

(2) $\Leftrightarrow$ $-\sum_{\binom{u\ v}{w\ t}} \xi\left(\frac{w}{t}\right) \cdot \xi(\kappa) = 0$ $\rightarrow$ it suffices to find some $\xi(\kappa)$ s.t. $\xi\left(\frac{w}{t}\right)\xi(\kappa) = 0 \;\forall \binom{u\ v}{w\ t} \in X_r$.

So let $\ell \in \{1, \dots, p-1\}$ $e \equiv \frac{v}{t} \;(p)$, $\left(\ell_* \equiv -\frac{t}{w} \;(p)\right)$

Claim: $\ell_{\text{mod } p} \geq \frac{p-1}{d}$

Solley using the "lemme des cordes",



i.e. find $\kappa \in \mathcal{E}$ s.t. κ_ℓ is in $\mathcal{E}$

and also s.t. $e \cdot \xi(\kappa) \neq 0$.

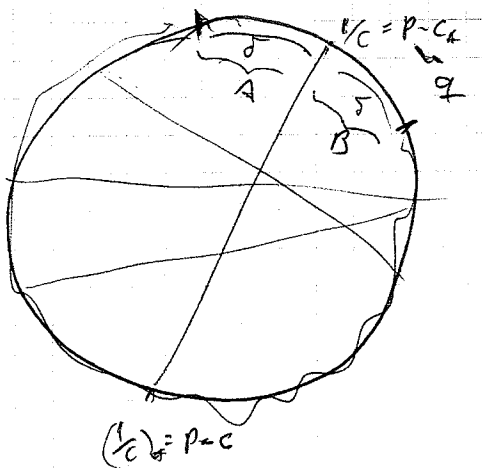
It is possible to do so by an analytic lemma for $p > d^{3d^2}$

- for λ_c, $c > 1$: Suppose $\lambda_2 t_2 e + \cdots + \lambda_c t_c e = 0 \quad 1 < c \leq d$.

want $\xi(\kappa)$ s.t. $\begin{cases} t_r e \cdot \xi(\kappa) = 0 \;\forall r < c \\ t_c e \cdot \xi(\kappa) \neq 0. \end{cases}$

Note that $\xi(\frac{v}{c})$ occurs ONLY in $t_c e$

So to finish, look for $\xi(\kappa)$ s.t



$$\xi\left(\tfrac{1}{c}\right)\cdot\xi(\kappa)\neq 0$$

$$\xi\left(\tfrac{w}{t}\right)\cdot\xi(\kappa)=0 \quad \forall \binom{w}{t}\in\mathbb{Z}^2,\ r\leq c,\ \tfrac{w}{t}\neq\tfrac{1}{c}$$

Exercise: $|\ell-q|\geq\delta=\dfrac{p-d^2}{d(d-1)}$

(define ℓ s.t $\ell=\frac{w}{t}$)

Suffices to find $\kappa\in A$ s.t κ_A^i is in B

This is possible using the same analytic lemma. Takes $p>d^{3d^2}$.