The Arithmetic of Curves: Overview

Describing equation:

We generalise the way to an \( \mathcal{O} = \mathcal{O}_{K, S} \): \( \mathbb{F}_{\mathcal{O}} \) is the field of fractions of \( \mathcal{O} \).

\[
X = \left\{ (x_i, y) : \right. \begin{array}{l}
\sum_{i} x_i = 0 \\
\sum_{i} x_i = 0
\end{array}
\]

\( X(\mathcal{O}) = \left\{ (x_i, y) \in \mathcal{O}^n : \sum_{i} x_i = 0 \right\} \)

where \( \mathcal{O}[X] = \mathcal{O}[x_i, y] / (\mathcal{O}[x_i, y] \cap \mathcal{O}[x_i, y]) \)

This is the affine case.

**Projective Case:** Assume \( f_i \)'s are homogeneous.

\[
X(K) = \left\{ (x_i, y) \in K^n \text{ satisfying } (\star) \right\}
\]

**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 \( (\star) \), for which \( X(C) \) is a one-dimensional complex manifold.

We assume also that \( X \) is equipped with a model \( \mathcal{X} \) over \( \text{Spec}(\mathcal{O}_K) \), 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 \( \mathcal{O}_{K, S}, K \).

3) Height function:

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

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

\[
N(X, B) = \# \left\{ p \in X(\mathcal{O}_{K, S}) : h(p) \leq B \right\}
\]

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 $X(0)$

Assume $X$ smooth.

Then $X(0) \cong \{ y \in \mathbb{P}^1 \mid \rho_i \neq \rho_j \}$

where $g = \text{genus of } X$, $\mathbb{P}^1$ is a complex surface of genus $g$,
and $\{\rho_1, \ldots, \rho_t\}$ is a finite set of points.

Can define $X(0) := 2 - 2g - s$ (Euler Characteristic).

* $X(0) > 0 \implies g = 0$, $s = 0, 1$.

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

**FACT:**

1. $X(k) \neq \emptyset$
2. $X \cong \mathbb{P}^1$ over $k$
3. $(X_k) \neq \emptyset$ for all completions $K_v$ of $K$.

\[ 1 \implies 2 \quad \text{Riemann-Roch} \quad \omega \in X(k), \text{an } L(\omega) \neq 0 \implies \varphi(L(\omega), \phi: X \to \mathbb{P}^1). \]

\[ 2 \implies 3 \quad \text{obvious} \]

\[ 3 \implies 1 \quad \text{Hasse-Minkowski} : \]

Note in case $s = 1$ (affine) then $X \cong \mathbb{A}^1$.

\[ \emptyset \cong X \cong 0 \]

* $X(0) = 0 \implies (g, s) = (0, 2)$ or $\begin{cases} (1, 0) \\ \text{affine} \\ \text{projective} \end{cases}$

If $X(0) \neq \emptyset$, then $X$ has the structure of a group scheme over $\mathcal{O}$.

In the affine case, $X/\mathcal{O} \cong \text{Elliptic curve} / \text{Spec}(\mathcal{O})$.

In the projective case, $X/\mathcal{O} \cong \text{Elliptic curve} / \text{Spec}(\mathcal{O})$. 
Theorem: $X(\mathcal{O})$ is finitely generated.

→ Affine case: Divisibility theorem $(\mathcal{O}^\times \to \text{Spec } \mathcal{O})$.

→ Projective case: Mordell–Weil theorem.

In this course, we will concentrate on $X(\mathcal{O}) \leq 0$.

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

→ Affine case: Siegel’s theorem $(s \neq 0)$

First preliminary case: $X = \mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}_1 \mathcal{O}_2 / \text{Spec } \mathcal{O}$

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

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

$f \in \text{Hom}(\mathcal{O}(X), \mathcal{O})$ \iff $f(x) \in \mathcal{O}^\times$ and $1 - f(x) \in \mathcal{O}^\times = \text{finite}$

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

Prelude: dimension 0 (scheme of dim 0 over Spec $\mathcal{O}$).

An $\mathcal{O}$-algebra $R$ is called finite if $R$ is

$\mathcal{O}$-generated free $\mathcal{O}$-module.

For $\mathcal{O}$-algebra $R$, called étale if $R/\mathcal{O}$ is reduced for all $K \in \text{Spec } \mathcal{O}$.

Let $\mathcal{W}(\mathcal{O}, d) = \text{iso. classes of } \mathcal{O}$-algebras $R$ of rank $d$.

Theorem (Hensel): $(\mathcal{O} = \mathcal{O}_K, s)$.

$\# \mathcal{W}(\mathcal{O}, d) < \infty$.

\[ \#$\mathcal{W}(\mathcal{O}, d) < \infty$.

\[ \text{Given } R \in \mathcal{W}(\mathcal{O}, d), \text{ consider } L = \bigotimes_{\mathcal{O}} R \otimes 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 $d$ and discriminant.
Unramified Coverings.

Let \( \pi: X \to Y \) be a finite morphism.

We will say \( \pi \) is unramified if \( \pi: X(\mathcal{O}) \to Y(\mathcal{O}) \) is unramified.

Lemma: if \( \pi: X \to Y \) is unramified, then there exists a finite extension 
\( \mathcal{O}_K \), and a finite set \( S \subseteq \mathcal{O}_K \) s.t. \( \mathcal{O}_K(\xi) = \pi^{-1}(\eta) \) for all \( \eta \in \pi(X) \).

Let \( \eta \in \pi(X) \).

Fact: if \( \pi: X \to Y \) is unramified, then \( \exists S \subseteq \mathcal{O}_K \), \( S \) finite s.t.
\( \pi: X \to Y \) is étale as a covering of schemes
\[ \pi^* : \text{Spec} (\mathcal{O}_K) \to \text{Spec} (\mathcal{O}_K) \]

In particular, for all \( \mathcal{O}_K \in \mathcal{Y}(\mathcal{O}_K) \), \( \pi^* : (\mathcal{O}_K \to \mathcal{O}_K) \) is an étale \( \mathcal{O}_K \)-algebra.

Hence \( \pi^* : (\mathcal{O}_K \to \mathcal{O}_K) \) is an étale \( \mathcal{O}_K \)-algebra.

By Hensel's Theorem, there are finitely many such algebras, and we can let
\[ \mathcal{O} = \text{Compositum} \left( \text{Frac}(\mathcal{K}) \right) \]
finite over \( \mathcal{K} \) by Hensel.

Exercise:

1. Show that there are no Siegel (weakly, weakly, weakly, weakly, weakly).
2. If \( X(\mathcal{O}_K) = \emptyset \) and \( X \) is a \( g \)th scheme \( \mathcal{O}_K \), show that \( X(\mathcal{O}_K) \) is \( g \)-gen.
3. Let \( X = \mathbb{P}^2 + \mathbb{P}^2 + \mathbb{P}^2 \) (Fermat curve of degree 7).
\[ Y = \mathbb{P}^3 \times \mathbb{P}^3 \times \mathbb{P}^3 \to (\mathbb{K} \times \mathbb{K}) \times \mathbb{K} \] (Klein quartic, \( X(\mathbb{K}) \)).

a) Show that \( X(\mathbb{Q}) = 15 \), \( g(Y) = 3 \).

b) Show that \( \pi: (7,7) \to (\mathbb{Z}/7, \mathbb{Z}/7, \mathbb{Z}/7) \) is an unramified covering of degree 7.

c) Show that for \( \mathcal{O} \neq Y(\mathcal{O}) \), \( \mathcal{O} \times \mathcal{O}(\mathcal{O}) \) is a \( \mathcal{O}(\mathcal{O}) \) s.t. \( \pi(\mathcal{O}) = \mathcal{O} \).
Faltings' Theorem (I)

References:
- S. 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 \( |X(k)| < \infty \).

Proof: Fix from now on a finite set \( S \) of places of \( k \) set \( X \) has a smooth model over \( \text{Spec} \, \mathcal{O}_k \) (will call it \( X, \text{red} \).

We proved by a series of reductions.

1) First reduction: The Shafarevich Problem.

Recall \( H(1,d) \) defined before. It is finite (by Harnack).

Def. (1) \( H(1,M_g) = \) isomorphism classes of smooth curves of genus \( g \) over \( \text{Spec} \, \mathcal{O}_k \).

(2) \( H(1,A_g) = \) isomorphism classes of abelian varieties of dimension \( g \).

(3) \( H(1,J_g) = \) isomorphism classes of Jacobian varieties of dimension \( g \).

Conjecture: \( H(1,-) \) is finite (by Shafarevich).

Theorem (Kodaira-Pearson): The Shafarevich conjecture for curves implies Faltings' theorem.

Idea of proof: the Kodaira-Pearson construction: given \( P \in X(k) \), it constructs a curve \( X_P \) which is a covering of \( X \), \( X_P \rightarrow X \).

St.: \( X_P \) is ramified only at \( P \).

- The genus of \( X_P \) \( > 1 \) and depends only on \( P \), let \( g \equiv \text{genus}(X_P) \).

- \( X_P \) is smooth over \( \text{Spec} \, (\mathcal{O}[1/2]) \).

So get a map \( X(k) \rightarrow H(1/2, M_g) \).
Outline of the construction over $\text{Spec}(k)$ & its end.

Bidual $X \to \text{Jac}(X)$, abelian variety of dimension $g$, by $Q = \left( Q_1 \cdot Q_2 \right)$

\[ \sim \]

In the pullback of the diagram

\[ X \longrightarrow \text{Jac}(X) \]

\[ \Pi \]

\[ \text{J}_{\mathbb{Z}} \]

\[ X \longrightarrow \text{Jac}(X) \]

write $\Pi^{-1}(P) = \tilde{P} + D$, where $D$ is an effective divisor of \( \deg = 2g^2 - 1 \)

\( \tilde{P} \in \tilde{X}(k) \)

\[ \tilde{f}_D^{\text{gen}} \text{ is generalized Jacobian of } (X, D) \text{ is s.t.} \]

\[ \tilde{f}_D(L) = \{ \text{L-rational divisors of } \deg = 0 \} / \text{principal divisors div}(g) \]

\( \tilde{f}_D \) supported outside $D$, \( \tilde{f}_D \) supported on $D$.

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

What we do now is $X_p \longrightarrow \tilde{f}_D \to \text{J}_{\mathbb{Z}}$.

When $X_p$ is again the pullback of the diagram

\[ X \to \tilde{f}_D \]

$\tilde{f}_D$ is called $\tilde{f}_D^{\text{gen}}$. Compute $g^1$. Exercise: compute $g^1$.

Call $R_1 : X(K) \longrightarrow \text{III}(\text{Olit}, \text{Hg})$ just defined.

The key point is that $R_1$ has finite fibers (Theorem by De Franchis). De Franchis says $\text{H} \quad (Y, X) \leq K$ finite. $g(X) \geq 2$.

So every $Y \leq X$ done.

2) Second reduction: From curves to Abelian varieties.

Consider $R_2 : \text{III}(\text{O}, \text{Ag}) \to \text{III}(\text{O}, \text{Ag})$

\[ X \longrightarrow \text{Jac}(X). \]

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 polarization.
3) Third reduction: From Abelian varieties to Isogeny classes.

Let \( \mathbb{R}_3 : \text{III}(0, A_3) \to \text{III}(0, \text{Is}) \).

**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., \( \mathbb{R}_3 \) has finite fibers).

*This result is the technical part of Faltings' proof.*

*The key ingredient is "Faltings Height."*

... will take this part of a black box.

4) Fourth reduction: From isogeny classes to \( \ell \)-adic representations.

Given \( A \) an abelian variety over \( K \), consider \( G_K \).

Let \( G_K = \text{Gal}(\overline{K}/K) \).

Define the Tate module \( V_\ell(A) = \bigoplus A[\ell^n] \cong \mathbb{Z}_\ell^{2g} \).

Then \( V_\ell(A) \) is a \( \mathbb{Z}_\ell \)-dualizable \( \mathbb{Q}_\ell \)-vector space equipped with a free \( \mathbb{Q}_\ell \)-action:

- \( E = \mathbb{Q}_\ell \)-algebra generated by \( \text{End}_K(A) \subset V_\ell(A) \).
- \( T = \mathbb{Q}_\ell \)-algebra generated by \( G_K \subset V_\ell(A) \).

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

\( \mathbb{R}_4 : \text{III}(0, \text{Is}) \to \{ \text{isom. classes of } \ell \text{-adic reps of } G_K \} \).

- **Some 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 split).
  2. \( V_\ell(A) \) is unramified outside \( S \) where \( S \) is finite, invertible in \( Q_4 \) for \( \ell \).
  3. \( V_\ell(A) \) is a rational representation i.e., given \( U \in S \), \( \text{Frob}_U(V_\ell(A)) = V_\ell(A) \), and \( \text{Frob}_U \) has characteristic polynomial in \( Z[T] \) with roots \( a_1, \ldots, a_{2g} \).

\( \text{Gal}(\overline{K}/K) \) is a finite extension of \( \mathbb{Q}_\ell \) containing \( \mathbb{Q}_p \) for some \( p \).

\( \text{Gal}(\overline{K}/K) \) is a finite extension of \( \mathbb{Q}_\ell \) containing \( \mathbb{Q}_p \) for some \( p \).
Thanks to these previous facts, $R_\mu$ actually lands in

\[ \text{the closure of Zariski-dense lattices of } G_K \]

such that unramified outside $S$ is rational.

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

4) $V_\mu(A)$ is semisimple over $\mathbb{T}$ (deeper than Chevalley for $E$).

Tomorrow: prove (4) as the $R_\mu$ are finite fibers.

and then $R_\mu$ lands in its closure unramified outside $S$.

Finally, prove that the last set is finite, to conclude the proof.

So far:

\[ X(K) \xrightarrow{R_\mu} \text{Hilb}(\text{disc}(20)) \xrightarrow{\text{moduli}} \mathbf{D}(\text{Fal}) \xrightarrow{\text{Faltings}} \mathbf{D}(\text{Finiteness}) \]

for $1 \leq y < \infty$.

Looking at the pullback:

\[ \text{Faltings' Finiteness Theorem} \]

\[ \text{Isom. classes of Tate} \]

\[ \text{Tate} \]

\[ \text{Conjecture} \]

\[ \text{Weil} \]

**Step 1:** Show that the Ladevèze map is semisimple for $\mathbb{T}$

**Step 2:** Show $R_\mu$ is injective (Tate Conjecture)

**Step 3:** $\text{Rep}_S(G_K, \mathbb{A})$ is finite.
Step 1: Semisimplicity.  

(Exercise: Show that if we omit semisimplicity, then $\text{Rep}_S(G_k, A)$ can be infinite.)

**Key Theorem (call it Theorem E):** Let $W \in V_k(A)$ be a $TT$-stable subspace. Then $\exists \sigma \in \text{End}_k(A) \otimes \mathbb{Q}_p$ s.t. $\mu(V_k(A)) = W$.

Consider $W \cap T_k(A)$ and $W_n = \text{range in } A[l^n]$. (note that $W_n$ is $TT$-stable)

Consider $A \to \bigoplus_{n} A/l^n$, where $\beta_n = \text{reduction s.t. } \alpha_n \beta_n = \ell^n$ (hence $A \cong \bigoplus_{n} A_l^n$)

Note that $\beta_n(A[l^n]) = W_n$ is finite.

By Faltings' purity theorem, $\exists \Sigma = \{i_0, i_1, \ldots, i_n\}$ s.t. $A_{i_0} \to A_i$

Define:

$\beta_{i_0} \to A_i$

$\alpha_{i_0} \to A_i^l \beta_i$

Define $\nu_i = \beta_i \circ \nu_i \circ \alpha_{i_0} \in \text{End}_k(A)$

Assume that the $\nu_i$ converge $\text{End}_k(A) \otimes \mathbb{Q}_p$ and $\nu_i(A[l^n]) = W_i$ (compact so can take a subsequence that does converge).

Let $\mathcal{M} = \lim_{i} \nu_i$ with index indep of $i$.

Then $\mu(A[l^n]) = \nu_i(A[l^n]) \leq P_{\varepsilon}(A[l^n]) = W_i$.

So $\mu(T_k(A)) \subseteq W \cap T_k(A) = W$. 

**Corollary:** $V_k(A)$ is semisimple.

(Exercise: Show that if we omit semisimplicity, then $\text{Rep}_S(G_k, A)$ can be infinite.)

Let $W \subseteq V_k(A)$ be any $TT$-stable subspace. Need to produce a $TT$-stable complement.

By Thm E, $\exists \sigma \in \text{End}_k(A) \otimes \mathbb{Q}_p \text{ s.t. } \mu(V_k(A)) = W$.

Consider $\sigma E$, and let $\mu_0$ be an idempotent in $\sigma E$.

Let $W' = \ker \mu_0$. Then $W'$ is a $TT$-stable complement.

\[\]
Remark 1: Enough to show that
\[ \text{Hom}_k(A, B) \otimes \mathbb{Q}_p \to \text{Hom}_k(V_c(A), V_c(B)) \] is surjective (injective & clear).

This is called the Tate Conjecture.

If \( i : V_c(A) \to V_c(B) \), then \( \exists \ u \in \text{Hom}_k(A, B) \otimes \mathbb{Q}_p \) mapping to \( i \).

Then \( \det(u) \neq 0 \). Can clear denominator and assume \( u \in \text{Hom}_k(A, B) \).

Write \( u = \sum_{i} \mu_i \), \( \mu_i \in \text{Hom}_k(A, B) \).
The \( \mu_i \) are transcendental.

Remark 2: Enough to show
\[ \text{End}_k(A) \otimes \mathbb{Q}_p \to \text{End}_k(V_c(A)) \] (injective & clear).

Replace by \( A \) by \( A \times B \) and note that \( \text{End}_k(A \times B) \cong \text{End}_k(A) \otimes \text{Hom}(A, B) \).

\[ \otimes \text{Hom}_k(B, A) \otimes \text{End}_k(B) \]

Theorem: \( \text{End}_k(A) \otimes \mathbb{Q}_p \to \text{End}_k(V_c(A)) \) is surjective.

Let \( \psi \in \text{End}_k(V_c(A)) \).

Consider \( \text{Graph}(\psi) = W = \{(x, \psi(x), V_c(A) \times V_c(A)) \}} \subseteq V_c(A \times A) \).

\( W \) is \( TT \)-stable (as \( \psi \in \text{End}_k(A) \)).

By Theorem E, \( \exists \ u \in \text{End}_k(A \times A) \otimes \mathbb{Q}_p \) s.t. \( u(V_c(A \times A)) = W \).

Let \( \alpha \in E^0 = \text{commutant of } E \text{ in } \text{End}(V_c(A)) \).

Then \( (\alpha \circ \psi) \) commutes with \( U \), hence \( (\alpha \circ \psi) \) preserves \( W = \psi(U) \).

So \( \alpha \) commutes with \( U \) (exercise).

Hence \( \psi \in (E^0)^0 = E \).

Footnote about semisimple algebras.
Final step: \( \text{Reps}_5(G_k, d) \) is finite.

Proposition (Effective Chebotarev Theorem):
There exist a finite set \( T \) of primes of \( K \), disjoint from \( S \), such that for all \( \sigma_1, \sigma_2 \in \text{Reps}_5(G_k, d) \),

\[
\text{Trace} \left( \sigma_1(\text{Frob}_v) \right) = \text{Trace} \left( \sigma_2(\text{Frob}_v) \right) \quad \forall v \in T \Rightarrow \sigma_1 \cong \sigma_2
\]

Let \( L \) be the compositum of all extensions of degree at most \( \ell 2d^2 \) which are unramified outside \( S \).

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

By classical Chebotarev, \( \mathfrak{F}_v \) primes of \( K \) sit \( \{ \text{Frob}(v), \text{Frob}(w) \} \) generate \( \text{Gal} \left( L/K \right) \). Let \( T = \{ \mathfrak{F}_1, \mathfrak{F}_2 \} \).

Consider now \( \sigma_1, \sigma_2 \in \text{Reps}_5(G_k, d) \), consider.

\( j : \sigma_1 \circ \sigma_2 : T \to M_d(\mathbb{Z}_\ell) \times M_d(\mathbb{Z}_\ell) \)

Let \( M = \text{image}(j) \).

The rank of \( M \) as \( \mathbb{Z}_\ell \)-module is \( \text{rk}_{\mathbb{Z}_\ell} M \leq \ell 2d^2 \).

\[
\overline{j} = \sigma_1 \circ \sigma_2 : T \to M/M^* \to (M/M^*)^* \to \text{Gal}(L/K)
\]

\( \overline{j} \) is unramified outside \( S \) (by \( j \) unram).

\( \# (M/M^*)^* \leq \# M/M^* = \ell 2d^2 \)

So \( \overline{j} : G_K \to (M/M^*)^* \) factors through \( \text{Gal}(L/K) \).

Therefore, by the choice of \( T \), \( \overline{j}(\text{Frob}(v)), \overline{j}(\text{Frob}(w)) \) generates \( M/M^* = (\ell, \text{Nakayama's lemma})^* = j(\text{Frob}(v)), j(\text{Frob}(w)) \)
generates \( M \) as \( \mathbb{Z}_\ell \)-module.

Hence, if \( \text{Trace}(\sigma_1(\text{Frob}(v))) = \text{Trace}(\sigma_2(\text{Frob}(v))) \forall v \in T \Rightarrow \)

\( \Rightarrow \text{Trace}(\sigma_1(\sigma_1(\sigma_1))) = \text{Trace}(\sigma_2(\sigma_2(\sigma_2))) \forall v \in T \).

As \( \sigma_1, \sigma_2 \) are semi-simple, \( \sigma_1 \times \sigma_2 \) become their determinants by their trace.
To conclude, there are only finitely many possibilities for $\text{Tr}(\mathcal{P}(\text{Tori})) \leq dN(\nu)^2$.

So done. Here it's around 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:** 
\[
\begin{aligned}
\text{(moduli space of elliptic curves)} &= \text{Spec } \mathbb{Z}[\frac{1}{\nu}][[\frac{1}{\nu}]] \\
\text{Definition} &= \text{Spec } \mathbb{Z}[\frac{1}{\nu}][\frac{1}{\nu}]
\end{aligned}
\]

Fix a prime $p \nmid \nu$ and let $\mathcal{E} = \mathbb{Z}[\frac{1}{\nu}]$.

$Y_1(p)$ is a curve over $\text{Spec } \mathbb{Z}$ classifying pairs $(E, \mathcal{L})$ where $
\begin{aligned}
\mathcal{L} &\text{ a point of } \\
\mathcal{E} &\text{ order } p \text{ on } E.
\end{aligned}
$

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

$Y_1(p)(R) = \{ (E, \mathcal{L}) \}_R, \text{ up to } R \text{-isomorphism, by } \alpha \cdot R \mapsto (E, \alpha \cdot \mathcal{L})$

Also, let $Y_0(p) = Y_1(p)/\langle \mu_p \rangle$

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

**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 5th 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 $\mathbb{Q}$**

$Y_1(p)(\mathbb{Q}) = \{ (E, \mathcal{L})/\mathbb{Q} \} = \frac{\Gamma(\mathbb{Q})}{\Gamma(p)} \cdot Y_1(p) = \{ (a \cdot \mathcal{L}) \}^{S_\mathbb{Q}(\mathcal{L})}

Y_0(p)(\mathbb{Q}) = \frac{\Gamma(\mathbb{Q})}{\Gamma_0(p)} \cdot Y_0(p) = \{ (a \cdot \mathcal{L}) \}^{S_\mathbb{Q}(\mathcal{L})}
Computation

Consider \( X_0(p) \), compactified if \( Y_0(p) \) obtained by adjoining cusps:

\[
X_0(p) = \frac{\mathcal{H}^*}{\Gamma_0(p)} , \quad \Gamma_0 = \Gamma(p) \cup \mathcal{H}.
\]

2. \( X_0(p)(\mathbb{C}) = \mathcal{H} \cup \{0, \infty\} \quad (+ \text{analytic structure})
\]

Local parameter at \( \infty \):

Is given by \( \phi = e^{2\pi i t} \)

Algebraically, consider the Tate curve \( \mathbb{Z}[[q]]/q^2 \) : 

\[
\Delta = q \cdot \Pi \left( 1-q^n \right)^2.
\]

So \( E_{\phi} \) is an elliptic curve over \( \mathbb{Z}[[q]] \)

The \( \phi \)-expansion principle identifies:

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

Definition: A morphism of varieties \( j : X \to Y \) is a formal immersion

at \( x \in X(\mathbb{Z}) \) if it induces a surjection:

\[
\hat{j}^* : \mathcal{O}_{Y,j(x)} \to \mathcal{O}_{X,x}.
\]

Nagura criterion: Suppose there is an isogeny \( \hat{j}_\#(p) \) of \( j_0(p) \):

1) \( \hat{j}_\# : X_0(p) \to \mathcal{O}_{X_0(p)} \)

2) \( \hat{j}_\#(p)(\mathbb{Q}) \) is finite.

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

Sketch of \( R \):

Let \( \mathcal{E} \in Y_1(p)(\mathbb{Q}) \) and let \( (E, \mathcal{L}) \) be the corresponding "pair" for \( X \).

\( E \) has potentially multiplicative reduction at \( p \).

For otherwise, \( E/\mathbb{F}_p \) is either an elliptic curve (good rd.) or an extension

of a finite group \( \mathbb{F}_p \) of order \( 2^a3^b \) by \( \mathbb{F}_p(\alpha) \) (additive rd.) \( \Rightarrow \)
2) Let $x \in X_0(p)$ be the image of $x$ in $X_0(p)$. Then $x$ reduces
to either 0 or $\infty$ modulo 3.

Assume WLOG that $x/1/f_3 = \infty/1/f_3$ (if it reduces to 0, then replace
$(\infty, ((x, f_3)) \to (E/k, (C, f_3)))$

1) Consider the map \( \Phi^\# (x) - (\infty) \in \mathbb{J}^0(1)(\mathbb{Q}) \cap \mathbb{J}^0(1)(B) \).

Now $\mathbb{J}^0(1)(\mathbb{Q})$ is torsion-free

$\mathbb{J}^0(1)(B) \cap \text{torsion} \quad \Rightarrow \quad \Phi^\# (x) - (\infty) = 0$.

Therefore, $\Phi^\# (x) = 0$ (Aside $\mathbb{J}^0(1)(\mathbb{Q})$ is, by definition,

$\mapsto \mathbb{J}^0(1)(B) \to \mathbb{J}^0(1)(B) = \mathbb{J}^0(1)(B)$)

4) By the formal isogeny property, $x = \infty$.

Let spec $R = \text{affine abelian} \quad x: R \to \mathbb{Z}_3$. Define through:

$x: R \to \mathbb{Z}_3$

$\Xi_0(1)/0$

$\mathbb{Z}_3[1/2] / x$

We've shown in $(3)$ that $\Phi^\# (x) \in \mathbb{J}^0(1)(B) \Rightarrow x = \infty$

\underline{Problem:} Construct a good point $\mathbb{J}^0(1)(B)$ of $\mathbb{J}^0(1)$.

\underline{key ingredient:} connection between $\mathbb{J}^0(1)$ and modular forms.

If $\mathbb{S}_2(p, R) =$ space of regular differentials on $X_0(p)/R$, $\text{spec } R$ is not rigid.

It is called the space of modular forms of weight 2 in $\mathbb{J}^0(p)$.

(because $\mathbb{S}_2(p, \mathcal{O}) = \{ f: \mathcal{H} \to C \text{ holomorphic} \}$

$\text{holomorphic}$ \quad \mathcal{O} = \mathcal{O}(2) = \mathbb{Z}_3[1/2] / x$

\underline{Eichler - Shimura decomposition}

Let $p \not\equiv p$ a mod. $X_0(p)$

\[ \xymatrix{ X_0(p) \ar[r] \ar[d] & X_0(p) \ar[d] \ar[r] & (E, C_1) \ar[d] \ar[r] & \mathbb{Z}_3 \ar[r] & 0 } \]

This corresponds to a map to an endomorphism of $\mathbb{J}^0(1)$.

$\mathbb{J}^0(1)$
Let $T := \text{subring of } \text{End}_A(J_0(E))$ generated by all $T \alpha$ (if $p$).

It's called the Hecke algebra.

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

Claim: $T \otimes \mathbb{Q} = \text{lim} \otimes \mathbb{Q} \mathbb{S}_2^p(\mathbb{Q}) / \text{genus}(K_0(p))$.

If there's a perfect pairing $T \otimes \mathbb{Q} \otimes \mathbb{S}_2^p(\mathbb{Q}) \to \mathbb{Q}$

Then $K_f := \text{field generated by Fourier coeffs of } f$.

Exercise: show that this is perfect.

**Corollary:** $T \otimes \mathbb{Q} \otimes \mathbb{K}_f$

(an eigenform is a modular form which is an eigenvector for $T$)

(a subset of $\mathbb{K}_f$)

Now define $\delta = \sum_{\alpha \in \text{End}_A(J_0(E))} \alpha f$ as the eigenvalue of $T \delta f$.

If $f$ is an eigenform, $K_f = \mathbb{K}_f$. This is a system of eigenforms.

The Eichler-Selberg construction allows us to associate $f \mapsto \mathbb{A}_f$ to an eigenform $f$ as a quotient of $J_0(E) \otimes \mathbb{Q}$.

Now $\mathcal{I}_f := \text{Ker}(T \to K_f)$

$\mathcal{A}_f := J_0(E) / \mathcal{I}_f$

**Properties of $\mathcal{A}_f$:**

1. $\text{End}_A(\mathcal{A}_f) = \mathbb{Q}_f$, where $\mathbb{Q}_f$ is the ring generated by $a_n(f)$.

This comes from the action of $T$ on $\mathcal{A}_f$, which factors through $T \to \mathbb{Q}_f$.

2. $\dim \mathcal{A}_f = [K_f : \mathbb{Q}]$

3. $V_\ell(\mathcal{A}_f)$ is a module over $K_f \otimes \mathbb{Q}_f$ of rank 2.
Theorem \( J_0(p) \rightarrow \prod_{\ell \in \mathbb{Z}/p\mathbb{Z}} A_{f_{\ell}} \) 

\[ L_{-\text{series}} \]

- Hasse-Weil \( L \)-series: 
  \[ L(A, s) = \prod_{\ell \in \mathbb{Z}/p\mathbb{Z}} \det (1 - \frac{a_{\ell}}{\ell} + \ell^{-s}) \]

- Hecke \( L \)-series: 
  \[ L(f, s) = \sum_{n=1}^{\infty} a_n(n) n^{-s} = \prod_{\ell} \left(1 - a_{\ell}(f) \ell^{-s} + \ell^{-2s}\right)^{-1} \] 

- Complex multiplication 

\[ \int_{0}^{\infty} \Gamma(s) L(f, s) = \int_{0}^{\infty} f(t) t^{-s} \, dt \] 

(Mellin transform of \( f \))

Exercise: Show that the \( f \)-product defining \( L(A, s) \) converges for \( \text{Re}(s) > \frac{1}{2} \)

Hecke point: \( L(f, s) \) has analytic continuation & functional equation.

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

**Theorem (Eichler-Shimura):** 
\[ L(A_{f, s}) = \prod_{\sigma: K \to \mathbb{C}} L(f, \sigma) \]

We know that \( L(A_{f, s}) \) has analytic continuation thanks to this.

**Conjecture (Birch - Swinnerton-Dyer):** 
\[ \# A(\mathbb{Q}) \sim L(1, A) \]

**Theorem (Gross-Zagier + Kolyvagin):** 

If \( L(A_{f, 1}) \neq 0 \), then \( A_{f}(\mathbb{Q}) \) is finite.
Construction of \( J_0^*(p) \)

\[
J_0 = \ker \left( F \to \Gamma K \right) \quad \text{L(1) to}
\]

Define \( J_0^*(p) : = J_0(p) \quad \text{Ann}_F \left( \frac{1}{p} \right) \quad \text{and we claim the } J_0^*(p)(\mathbb{A}) < \infty.
\]

Also, we can define also \( J_0 \) as \( \text{Ann}_F \left( \frac{1}{p} \right) \quad \text{and } e \in H_1(X(p), \mathbb{Q}) \quad \text{with } e \leftrightarrow \text{path}(0 \to i\infty).
\]

The quotient \( J_0^*(p) \) is also called \( J_0 \) or \( J_0(1) \), and called

the Weil-Deligne quotient.

\[ \text{Fermat's Last Theorem.} \]

Consider \( x^p + y^p = z^p, \quad p \text{ prime } \geq 3. \)

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

Motivation for the approach.

H. Chipaulone: there's a 1-1 correspondence between

Strategies for studying

\[
\begin{align*}
\text{Prim. solutions} & \quad \leftrightarrow \quad \text{unramified coeckings of } \left\{ \begin{array}{c}
\mathbb{P}^1 - \{ 0, 1, \infty \} \quad \text{of } \left( p, r, \gamma \right) \quad \text{is expand} \end{array} \right. \\
\end{align*}
\]

\[ \forall a, \quad \Sigma_{p^r, \pi} = \left\{ \frac{a_r}{c^r}, \quad (a_r, c_r) \quad \text{Prim. solutions} \quad \in \mathbb{P}^1 \right\} \]

Then \( \prod \left( \Sigma_{p^r, \pi} \right) \in X(\mathbb{L}) \) and \( L \) has non-trivial kernel only in the solution.

What are some coeckings \( \pi \) \( \mathbb{P}^1 - \{ 0, 1, \infty \} \) of \( \text{expansion } \left( p, p, p \right) \)?

1. \( X = x^p + y^p + z^p \) and \( \pi : X \to \mathbb{P}^1(\mathbb{Q}) \quad \pi \text{ has syzygy } \left( p, p, p \right) \)

So one would study \( \text{Fermat, eq. by studying the Fermat case.} \)

More interesting example.
2) Modular curves $X(n)$ moduli space of $(E, P, P_2)$ where $X(2P) \rightarrow (P, P_2)$ is a basis of $E[n]$. Let $X(2) \rightarrow \text{Spec } \mathbb{Z}[\frac{1}{2}]$. Over $\mathbb{Z}[\frac{1}{2}]$, $X(2) = \text{Spec } \mathbb{Z}[\frac{1}{2}][x, \frac{1}{x}, \frac{1}{x-1}]$. Its universal cover is $y^2 = x(x-1)(x-3)$ (Legendre curve). Let $A = \frac{a^b}{c^p} \in \prod_{p, p} a^b + b^p = c^p, a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$. $\Gamma^{-1}(A)$ is defined over the field of p-adic points of the curve $y^2 = x(x-1)(x-a^b/c^p)$. It is better to work with a twist of this curve $E_{abc}: y^2 = (x-a^p)(x-c^p)$ where $a \equiv 1 \pmod{4}, c \equiv 1 \pmod{4}$. Every curve associated to the solution $a^b + b^p = c^p$. We will consider the rep. of $G_\mathbb{Q} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ given by $\rho_{abc}: G_\mathbb{Q} \rightarrow \text{Aut}(E_{0, 1, 1, 1}) \cong GL_2(\mathbb{Z}[1])$. What do we know about $P_{abc}$? Theorem (Frey, Serre): local properties of $P_{abc}$:

1) Unramified outside 2, p. 
2) $P_{abc}|_{D_2} \sim (X_{\psi} \psi^{-1})$ 

where $X_{\psi}: \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(1/p)$, \psi \text{ unramified character}.

Jørgen: $P_{abc}$ is "ordinary" at 2.

3) $P_{abc}$ 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 (Fre 2.5 Cor)

First, \( \Delta_{abc} = 2^3 (abc)^{2p} \), \( N = \text{gcd}(abc) = \prod_l \ell \).

1) If \( l \mid 2abc \Rightarrow \Delta_{abc} \text{ has good reduction at } l \Rightarrow \text{fabc is unramified at } l \).

2) If \( l \nmid abc, l \nmid 2p \Rightarrow \Delta_{abc} \) has multi-reduction at \( l \).

\[ E(\mathbb{Q}_l^{unr}) = \left( \mathbb{Q}_l^{unr} \right)^{\times} / \mathbb{Z}_l^{*} \]

if \( q \) is the Tate parameter \( \in \mathbb{Z}_l^{*} \)

\[ \Delta = \prod_{l \mid q} (1 - q) \]

\[ \text{ord}_l(q) = \text{ord}_l(\Delta) \equiv 0 \ (p) \]

The points in \( E(\mathbb{Q}_l^{unr}) \) are defined over \( \mathbb{Q}_l^{unr} \left( \zeta, \zeta^{1/p} \right) \) where \( 0 \leq b, c < p^{-1} \)

\( \zeta \) is a primitive root of \( f \).

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

4) If \( l = p \), place c \( \Rightarrow \) Eabc has multiplicative reduction \( \Rightarrow \) fabc ordinary at \( p \)

\( \text{plabc \Rightarrow \Delta_{abc} \text{ has good reduction. (Tate model)} \}

Theorem (Mazur): Global properties of \( \text{fabc} \) \( (p > 13) \)

\( \text{fabc is irreducible} \)

\( \text{Exerc: use that we've seen lately for Mazur's theorem (the other one) to show it. (Hint: Eabc has primes of multiplicative reduction)} \)

So far:

\[ \begin{cases} \text{non-trivial solution} \Rightarrow R_1 \rightarrow \{ \text{elliptic curve of squarefree conductor, } N = \text{gcd}(abc) \text{ depends on the solution} \} \end{cases} \]

\[ \text{mod } p \text{ representation} \]

\[ \begin{cases} \text{irreducible, unramified outside } Z_p \text{ ordinary at } 2 \text{ and ordinary at } p \text{ over } \mathbb{Q}_l \text{ check it (odd even, that)} \end{cases} \]
From Modular Forms to Galois Representations

Let \( \tau = 2 \pi i \in S_2(N, \mathbb{C}) \) be an eigenform of weight 2 on the group \( \Gamma_0(N) \); \( \mathcal{O}_\tau \) field of Fourier coeffs.

\[ \mathcal{O}_\tau \] ring generated as \( \mathbb{Z} \) by the Fourier coeffs.

Let \( \mathfrak{p} \) be a prime of \( \mathcal{O}_\tau \) above \( \mathfrak{p} \).

*Theorem:* There exists a Galois representation \( \tau_{\mathfrak{p}, \mathfrak{p}} : \Gamma \rightarrow \text{GL}_2(\mathcal{O}_\mathfrak{p}) \) s.t.:

1. \( \tau_{\mathfrak{p}, \mathfrak{p}} \) is unramified outside \( \mathfrak{p} \).
2. \( \tau_{\mathfrak{p}, \mathfrak{p}} \) (Frobenius) has a characteristic polynomial of the form \( X^2 - a_\mathfrak{p}(\tau)X + 1 \).

*Use the Eichler-Shimura construction, which associates to \( \mathcal{O}_\mathfrak{p} \) the Galois representations \( \tau_{\mathfrak{p}, \mathfrak{p}} \) above \( \mathcal{O}_\mathfrak{p} \) via the Frobenius elements:

\[ \tau_{\mathfrak{p}, \mathfrak{p}} : \Gamma \rightarrow \text{GL}_2(\mathcal{O}_\mathfrak{p}) \]

Companion of \( \tau_{\mathfrak{p}, \mathfrak{p}} \) is \( \mathcal{O}_\mathfrak{p} \)-module, and so can consider \( \tau_{\mathfrak{p}, \mathfrak{p}} \) as \( \mathcal{O}_\mathfrak{p} \)-linear representations of \( \Gamma \):

\[ \text{GL}_2(\mathcal{O}_\mathfrak{p}) \]

Note also \( \mathfrak{p} \) is reducing mod \( \mathfrak{p} \)

\[ \mathcal{O}_{\mathfrak{p}} \]

\[ \text{free field.} \]
What is conjectured is that one should be able to prove this complex conjecture from Galois reps to Modular Form:

**Conjecture (Serre)**: Let \( p : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(F_\ell) \) be the Galois representation which is "ordinary" at \( p \) (of finite order) and "ordinary" at \( \ell \) for all \( \ell \) \( \not\mid N \) (where \( N \) is the conductor).

Then \( \exists \ f \in S_2(\Gamma_0(N)), \ p \nmid \Delta \ s.t. \ \phi = \overline{p_f} \).

If that were true, then could prove a result:

\[
\mathbb{R}^5 \rightarrow \left\{ \frac{\text{SL}_2(\Gamma_0(N))}{\mathbb{F}_p} \right\} = \phi
\]

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

**Theorem (Ribet)**: It is enough to show that \( E_{ab} \sim \Phi_f \) for some modular form \( \Phi_f \) on \( \Gamma_0(N) \), \( N \nmid 12 \text{gcd}(abc) \).

**Theorem (Wiles)**: For all semistable \( \ell \)-adic Galois representations \( E \), \( \exists f \in S_2(\Gamma_0(N)) \) such that \( E \sim \Phi_f \).

### Importance of Wiles' Theorem:

1. It proves FLT.
2. Modularity of elliptic curves: a key in understanding their arithmetic properties.
3. General method for relating Galois reps and modular forms:
   1. Proof of Artin Conjecture (Bourbaki, Taylor)
   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 \( E(K) \) on \( \ell(E)^1 \). Mordell-Weil Thm: The group \( E(K) \) is finitely-generated.

\[ E(K) = \mathbb{Z}^n \oplus \mathbb{T}, \quad \#T < \infty. \]

We know a lot about \( T \). For instance, \( \#T \leq C \sqrt{\text{disc} \, E} \).

The difficulty starts there in understanding \( r \).

Some words about the proof of MW Thm:

\[ \xymatrix{ & \mathbb{G}_m \ar[d]^n \ar[r] & E \ar[d]^n & E \ar[r]^n & \mathbb{G}_m } \]

Vocabulary of descent:

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

Taking the \( G_k \)-moments, get:

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

So, have an injection:

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

The \( n^\text{th} \) Selmer gp of \( E/k \) is \( \text{Sel}_n(E/K) := \ker \left[ H^1(K, E[n]) \to H^1(K, E) \right] \)

1. \( \text{Sel}_n(E/K) \subset H^1_{\text{na}}(K, E[n]) \) = classes unramified outside \( n \Delta \).

\[ K_K : \sigma(p) = \bar{p}^\sigma - \bar{p} \quad \text{where} \quad n\bar{p} = p. \]

2. \( H^1_{\text{na}}(K, E[n]) < \infty \) by the theorem of \textbf{be}rm\textbf{t}.

\[ \Rightarrow E(K)[n] \text{ is finite.} \quad \text{(weak MW).} \]
The main ingredient of the proof is the height...

We have an exact sequence:

\[ 0 \rightarrow \mathcal{E}(k) \rightarrow \text{Sel}_n(E/k) \rightarrow \text{Sha}(E/k)[n] \rightarrow 0 \]

where \( \text{Sha}(E/k) = \ker \left[ H^1(K, E) \rightarrow H^1(K, E) \right] \)

Questions:

* When is \( r > 0 \)?

* Computation of \( r \), and a system of equations for \( E(k) \).

**Birch - Swinnerton-Dyer conjecture**

Suppose now \( K = \mathbb{Q} \).

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

Consider \( \prod_{p < X} N_p \sim C_E \left( \log X \right) \) (heuristic observations).

We associate to \( E \) the Hasse-Weil \( L \)-function:

\[ L(E, s) := \prod_{p \nmid \Delta} \left( 1 - \alpha_p p^{-s} + p^{-2s} \right)^{-1} \prod_{p \mid \Delta} \left( 1 - \alpha_p p^{-s} \right)^{-1} \]

where \( \alpha_p = \rho + 1 - N_p \).

The \( L(E, s) \) converges for \( \text{Re}(s) > \frac{3}{2} \). (exercise, use \( |\alpha_p| < 2\sqrt{p} \)).

Expand \( L(E, 1) \) formally and get:

\[ \prod_{p \nmid \Delta} \frac{p}{N_p} \]

**Conjecture (BSD):**

\[ L(E, k) \text{ has analytic continuation, and } \text{ord}_{s=k} L(E/k, s) = \text{rank}(E(k)) \]
From now on, $K = \mathbb{Q}$.

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

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

**Key for these thus:** Connection with modular forms.

**Theorem (Wiles, B.D.T.):** If $E/F$ is an elliptic curve of conductor $N$, then there exists an eigenform of weight 2 on $\Gamma_0(N)$ such that $E \cong \text{isogenous to } \mathbb{A}f$ (quotient of $J_0(N)$ associated to $f$ by the Taniyama conjecture).

**Consequences:**

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

   \[ (2\pi)^s \Gamma(s) L(E, s) = \int_0^\infty f(y)(y/\lambda)^s \frac{dy}{y} \Rightarrow \text{analytic continuation of } L(E, s) \]

2. There is a morphism

   \[ X_0(N) \rightarrow J_0(N) \rightarrow A_f \rightarrow \mathcal{E} \]

   \[ \Phi \] is called the modular parametrisation attached to $E$.

**Computing $\Phi$:**

Assume $N$ squarefree. Let $W_e = N^{-1/2} \sum_{q | N} a_q q^{-1/2}$

\[ \Phi^*(W_e) = \int_{\mathbb{H}} f(q) \frac{dz}{q}, \quad f(q) = \sum_{n=1}^{\infty} a_n q^{-n} \]

For $z \in \mathbb{H}$, get an analytic formula for $\Phi(e)$:

\[ \int_0^\infty \Phi(\tau) = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n \quad q = e^{2\pi i \tau} \]
X₀(N) → E

Find rational or algebraic points on X₀(N) → points on E.

- CM points
- Heegner points

R(X, K ≤ E, K a quadratic imaginary field, K = Q(√(-D)), D > 0.

Theorem: If z ∈ H \cap K, then \( \Phi(z) \in E(K_{ab}) \) (\( K_{ab} \) = maximal abelian extension of K)

Tomorrow: for certain \( K, z \) we can obtain a point \( Q, E₀(N)(H) \)

\( \mathcal{P}_k := \text{Trace}_K^H(\Phi(Q)) \in E(K) \)

- Gross-Zagier: \( L'(E(K), 1) \) \& \( \hat{h}(\mathcal{P}_k) \)

\( L(E/K, 1) \neq 0 \Leftrightarrow \mathcal{P}_k \) of infinite order.

- Kolyvagin: if \( \mathcal{P}_k \) has infinite order, then \( \frac{E(K)}{\mathcal{P}_k} \) is finite.

*Heegner hypothesis: all primes \( l \nmid N \) are split in \( \sqrt{D/Q} \).

Let A be an elliptic curve with \( \text{End}(A) \cong \mathbb{Z} \left[ \frac{1 + \sqrt{D}}{2} \right] \). For all \( K \).

Theory of complex multiplication \( A \) is defined on \( K \).

*Heegner hypothesis \( \Rightarrow \exists N \in \mathbb{Q} \) with \( \mathcal{O}_K = \mathbb{Z}[\sqrt{D}] \)

\( A[N] \) is order of order \( N \), so \( (A, A[N]) \in X₀(N)(H) \).

Define \( \mathcal{P}_k := \Phi(Q) \in E(K) \), and \( \mathcal{P}_k := \text{Trace}_K^H(\mathcal{P}_k) = \sum_{\mathcal{P}_k} H(\mathcal{P}_k) \)

*Gross-Zagier: \( \hat{h}(\mathcal{P}_k) \propto L'(E/K, 1) \)

*Remarks: \( a_\mathcal{P}_k \) The proof is a direct, lengthy calculation

\( b = \sum_{n=1}^\infty \frac{a_n \chi(n)}{n^s} \)

\( c = L(E/K, 1, s) \cdot L(E/K, 1, s) \)

\( d = \chi \cdot \mathbb{R} \cdot \mathbb{Q} \)

*Heegner hypothesis \( \Rightarrow \) the sign in the functional equation for \( L(E/K, s) \)

\( f = L(E/K, 5) \) vanishes to odd order.
Theorem B (Kolyvagin): If \( \mathbb{F}_k \) is of infinite order, then

1) \( E(k) \) has rank one.
2) \( \#\text{III}(E,k) < \infty \).

Proof of GZK:

Orders, \( L(E,s) < 1 \Rightarrow \text{GZK satisfying the Heegner hypothesis, and for which } \text{ord}_{s=1} L(E,k, s) = \frac{1}{2} \) (it's an analytic theorem on non-vanishing of twists of \( L \)-seats). (Proved by Waldspurger, BFH, AM, ...)

By GZ, \( \mathbb{F}_k \) is of \( \infty \) order.

By Kolyvagin, \( E(k) \langle \mathbb{F}_k \rangle < \infty \) and \( \#\text{III}(E/k) < \infty \).

Extra information about \( \mathbb{F}_k \): Prefers \( E(k) / F \) torsion if \( w_N = 1 \)

\[ E \in E(k)^+ \] if \( w_N = -1 \)

\[ \Rightarrow \text{rank } (E(k)) = \text{ord}_{s=1} L(E, s) \Rightarrow \#\text{III}(E/k) < \infty \]

Kolyvagin's theorem: boundary \( E(k) \), \#III in terms of \( \mathbb{F}_k \).

Main Point: \( \mathbb{F}_k \) a part of a norm-coherent system of points. Order of conductor \( n \)

Given \( n \) with \( (n, N) = 1 \). Let \( A_n := \text{c.c. with End}(A_n) = \mathbb{Z}[\frac{n+10}{2}] \)

CM theory \( \Rightarrow A_n \) defined over \( H_n = \text{cycl class field of conductor } n \).

\[ \text{Gal}(H_n/k) = \mathbb{A}_k / (k^+ \times \prod (D_n \otimes \mathbb{Q}) \times \mathbb{C}) \]

ramified only at \( \ell | n \).

Define \( Q_n \) corresponding to \( [A_n, A_n[N]] \) \( \in \text{Ext}(N)(H_n) \) via \( \mathbb{F}_n = \text{Gal}(Q_n) \).
If \( l \nmid \text{ord } N \) is next in \( K \):

\[
\text{Tr} \frac{H^l \mu_N \rho^l}{H^l} = \sum_{\sigma \in \text{Gal}(H^l/K)} a_{\sigma} \rho^l \mod \text{Gal}(H^l/K)
\]

Why?:

\[
\sum_{\sigma \in \text{Gal}(H^l/H_0)} \frac{Q_{\sigma} \rho^l}{\sigma \in \text{Gal}(H^l/H_0)} \mod \text{Gal}(H^l/K)
\]

Kolyvagin's Proof

Uses a \( p \)-descent. Fix a \( \text{"descent prime" } p \) in the following way:

1) \( p \neq 2 \)
2) \( \text{Gal} \left( \frac{\mathbb{Q}(\sqrt{p})}{\mathbb{Q}} \right) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \)

A. For \( p \) odd, modify argument to make it work with CM curves.

B. For \( p = 2 \), use a theorem of Serre, \( E \) is possible for \( A \)-type \( p \).

Then (Kolyvagin's theorem): If the image of \( \rho_\mathbb{Q} \) in \( E(K)/pE(K) \) is nontrivial, then \( \text{Sel}_p E(K) \cong \mathbb{Z}/p \).

In particular, \( E(K) \) has rank 1 and \( \text{Sym}^2 (E(K)/L) = 0 \).

We will only prove Kolyvagin's theorem.

Generalities on Selmer groups: (following Wiles)

\( K \) any number field,
\( M \) a finite module equipped with a continuous action of \( G_K \).

\[ H^1(G_K, M) = H^1(K, M) \leq \text{Continu.} \text{Hom} \]

Given a prime \( v \) of \( K \), \( v \) is said to be good for \( M \) if:
1) \( M \) is unramified at \( v \) (i.e. acts trivially on \( M \)).
2) \( v \nmid \text{ord } M \).
3) \( v \nmid \text{ord } M \).

If \( v \nmid \text{ord } M \), then:

\[ 0 \rightarrow H^1(G_{K,v}, M) \rightarrow H^1(G_K, M) \rightarrow \bigoplus_{v \text{ good}} H^1(G_{K,v}, M) \rightarrow 0 \]

and call \( \Theta_v \) "residue map at \( v \)."
We call $H^1(K_v, M)^{Gen}$, "singular part" of $H^1(K_v, M)$, and $H^1(K_v, M)^{Reg}$, "finite part" of $H^1(K_v, M)$.

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

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

$$\mathcal{L} = \left\{ \gamma \in H^1(K, M) : \text{Res}_v(\gamma) \in \mathcal{L}_v \right\} =: H^1_{\mathcal{L}}(K, M)$$

Example: $M = \mathbb{Q}_p, \mathcal{L}_v = \mathcal{O}_v(E(K_v)/\mathcal{O}_v(E(K_v)))$.

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

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

(See m of Harari - Manin.)

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

Duality: $M^\times : \text{Hom}(M, \mathbb{Q}_p) = \text{Hom}(M, \mathbb{Z}_p)$ is called the Kummer dual.

Have a cup product:

$$H^1(K_v, M) \times H^1(K_v, M^\times) \to H^2(K_v, \mathbb{Q}_p) = \mathbb{Q}/\mathbb{Z}$$

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

Theorem (Tate): The pairing $\langle \cdot, \cdot \rangle$ is not degenerate (on left/right), bilinear.

If $v$ is good, then $H^1_{\text{Gen}}(K_v, M)$ and $H^1_{\text{Reg}}(K_v, M^\times)$ 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 condition.
Def. The dual Selmer group: $H^1_{\text{dual}}(K, M^*)$

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

$$\frac{\# H^1_{\text{dual}}(K, M)}{\# H^1_{\text{dual}}(K, M^*)} = \frac{\# H^0(K, M)}{\# H^0(K, M^*)} \prod_{\nu} \frac{\# H^0(K \nu, M)}{\# H^0(K \nu, M^*)}$$

Rmk:

1) If $v$ is good, then $\# H^1_{\text{dual}}(K \nu, M) = \# H^0(K \nu, M)$ (exercise).
   - The infinite product is a finite product.

2) Flesh out the analogy with Riemann–Roch.

Important case: $M = E_{fp}$, $E_{fp}^* = E_{fp}^0$ (Weil pairing).

$$\prod_{\nu} \ell_{\nu} = \tilde{J}(E(K)/p)$$

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

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

$$1 = \prod_{\nu} \frac{E(K \nu)/E(K)}{E_{fp}(K \nu)}$$

Exercise: prove this directly, for $K = \mathbb{Q}$.

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

Def. 1) The relaxed Selmer group $Sel_p(E/K)(S) = \{ c \in H^1(K, E_p) \mid \forall \nu \not\in S, \text{res}_\nu(c) \in E(K \nu)/E(K) \}$

2) The restricted Selmer group $Sel_p(E/K)_{S^1} = \{ c \in Sel_p(E/K) \mid \text{res}_\nu(c) = 0 \forall \nu \in S \}$

Easy lemma: $Sel_p(E/K)(S)$ is the dual of $Sel_p(E/K)_{S^1}$.
Applying the theorem,
\[ \#\text{Sel}_p(E/k)(s) = \prod_{v \in S} \#\text{Sel}_p(E/k)(E_v^S) \]
\[ = \prod_{v \in S} \#H^1(K_v, E_{LP}) \]
\[ = \prod_{v \in S} \#E(K_v) / E_{LP}(K_v) \]
\[ = \prod_{v \in S} \#H^1_{\text{sing}}(K_v, E_{LP}) \]

Definition: A set \( S \) controls \( \text{Sel}_p(E/k) \) if \( \text{Sel}_p(E/k)(S) = 0 \).

(e.g., \( \text{Sel}_p(E/k) \xrightarrow{\sim} \prod_{v \in S} H^1_{\text{sing}}(K_v, E_{LP}) \) is injective).}

Exercise: What does \( \mathbb{R} \mathbb{P} \) for Selmer groups say when \( M = \mathcal{U}/\mathcal{P} \) (w/twist/cond)

\( M = \mathcal{U}/\mathcal{P} \) \hspace{1cm} (w/twist/cond)

Suppose \( S \) controls \( \text{Sel}_p(E/k) \). Then

1) \( \#\text{Sel}_p(E/k)(s) = \prod_{v \in S} \#H^1_{\text{sing}}(K_v, E_{LP}) \)

2) \( \Phi_0 \xrightarrow{\sim} \text{Sel}_p(E/k)(S) \xrightarrow{\sim} \prod_{v \in S} H^1_{\text{sing}}(K_v, E_{LP}) \) is exact

Problem: bound the cokernel of \( \Phi_0 \) (by multiplying unified claim)

Kolyvagin classes

\( M = E[p] \) (\( E \) defin. \( \mathbb{Q} \)), \( K \): a quadratic imaginary field.

Def: A prime \( p \) is called a Kolyvagin prime relative to \( \mathbb{Q} \) relative to \( (E, K, \mathcal{P}) \) if

1) \( \mathcal{P} \not\equiv \mathcal{P} \pmod{p} \)
2) \( \mathcal{P} \) inert in \( K \).
3) \( p \nmid \alpha_f(E) \) \hspace{1cm} (where \( \alpha_f(E) = p+1 - \#E(\mathbb{F}_p) \))
4) \( p \mid p+1 \)

Lemma: There are infinitely many Kolyvagin primes.

\((E, \text{Kolyvagin} \implies \text{Frob}_p(E[p]/\mathbb{Q}) = \text{complex conjugate})\)
8. The classes \( \overline{\kappa}(\ell) \in H^1(G\ell, E(He)) \) defined as

\[
\overline{\kappa}(\ell) \circ \sigma = \frac{(\sigma-1) \alpha_{\ell}}{\sigma \in G\ell} \circ E(He)
\]

Exercise: prove that \( E(He) \cdot 1 \) = 0.

Define \( \overline{\kappa}(\ell) \in H^1(G\ell, E) \) which maps to \( \overline{\kappa}(\ell) \).

Define \( \kappa(\ell) \) be any lift of \( \overline{\kappa}(\ell) \) to \( H^1(G\ell, E) \).
Theorem:

1) \( K(e) \in \text{Sel}_p(E/K) \)

2) \( \Theta_e K(e) \neq 0 \iff \mathcal{P}_K \neq 0 \text{ in } E(K)/\mathcal{P}_K \)

3) \( \Theta_e K(e) \in H^1_p \left( K_e, E', \mathcal{P}_K \right) \)

\[ E = \mathbb{Q}_p \left( \sqrt{-3} \right) \]

Proof:

1) Since \( \text{He/K} \) is ramified only at \( e \)

2) \( \Theta_e K(e) \neq 0 \iff \mathcal{P}_K \neq 0 \text{ in } E(K)/\mathcal{P}_K \)

\[ \left( \Theta_e - 1 \right) D_{e, N, \mathcal{P}_K} \neq 0 \text{ in } E(K)/\mathcal{P}_K \]

Impose more condition on \( e \) (to simplify computing). Inequality

\[ p^2 \mid l + 1, \quad \mathcal{P}_K \text{ as } \left( \text{where } p^2 \mid l + 1 \right) \]

Then \( \mathcal{P}_K \rightarrow 0 \text{ in } E(K)/\mathcal{P}_K \iff \mathcal{P}_K \text{ to in } E(K)/\mathcal{P}_K \)

3) Extend

Let \( l_1, l_2 \) be any polynomials in \( K \).

\( K_0(l_1, l_2) \) is extended in the same way, but one \( \Theta_{e, l_0} = D_{e, l_0, N, \mathcal{P}_K} \).

Theorem:

1) \( K(e, l_2) \in \text{Sel}_p(E/K) \)

2) \( \Theta_e (K(e, l_2)) \neq 0 \iff \text{Res}_{\mathcal{P}_K} K(e) \to \in H^1_p \left( \mathcal{P}_K, E \left[ \mathcal{P}_K \right] \right) \)

3) \( K(e, l_2) \in H^1 \left( K, E \left[ \mathcal{P}_K \right] \right) \)

End Similar.
Proof of Kolyvagin's Theorem

Control Lemma. There exists a set $S = \{ h_i \}$ of $t$ elements such that,

1) $S$ contains $\mathcal{S}_{p, \varepsilon}$

2) The range of $\rho_k$ in $E(ke_i)^\vee$ is non-zero.

3) $\varepsilon_{p, \varepsilon}(ke_i) > 0$ for $i = 2, \ldots, t$.

Let Chebotar's applied to $\alpha \in \mathcal{S}_{p, \varepsilon}$ and the field cut out by a basis $\langle \alpha \rangle$ for $\mathcal{S}_{p, \varepsilon}$.

End of $\mathcal{S}_{p, \varepsilon}$.

$$0 \rightarrow \mathcal{S}_{p, \varepsilon} \rightarrow \mathcal{S}_{p, \varepsilon} \rightarrow H_{\text{sing}}(ke_i, \mathcal{C}(F))$$

Step 1: $\mathcal{S}_{p, \varepsilon}(k(\ell_1)) \cap \mathcal{S}_{p, \varepsilon}(k(\ell_2))$ are linearly independent over $\mathbb{F}_p$.

Hence the kernel $(\mathcal{S}_{p, \varepsilon}) = 1 \Rightarrow \mathcal{S}_{p, \varepsilon}(k(\ell_1)) < 1$

Step 2: $\mathcal{S}_{p, \varepsilon}(k(\ell_1)), \mathcal{S}_{p, \varepsilon}(k(\ell_2)), \ldots$ are also linearly independent over $\mathbb{F}_p$.

Hence $\dim_{\mathbb{F}_p} \mathcal{S}_{p, \varepsilon}(k(\ell_1)) \leq 1 \Rightarrow \dim_{\mathbb{F}_p} \mathcal{S}_{p, \varepsilon}(k(\ell_1)) \leq 1$

$\Rightarrow \mathcal{S}_{p, \varepsilon}(E(ke_i)) \leq \mathcal{S}_{p, \varepsilon}(k(\ell_1))$. 

\[\varepsilon_{p, \varepsilon}(E(ke_i)) \leq \mathcal{S}_{p, \varepsilon}(k(\ell_1))\]
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 property) For all $v \in S$, let $B_{S,v}$ = the quaternion algebra ramified at $S \setminus v$. Define $R(v)$ = maximal order in $B_{S,v}$ if $v$ archimedean.

   $\Theta = [\frac{2}{v}]$-order in $B_{S,v}$ if $v$ non-archimedean.

   \[ \mathbb{H}_v = \frac{B_{S,v} \otimes \mathbb{C}}{R(v)} \]

   \[ \Gamma(v) = \mathbb{H}_v / \Theta \]

   $\Gamma(v)$ acts on $\mathbb{H}_v$.

   \[ \Gamma(v) \backslash \mathbb{H}_v = \frac{\Gamma(v)}{\Theta} \]

   $ \mathbb{H}_v$ is a Riemann surface for $(\mathbb{H}_v, \Gamma(v))$.

   $X_S(C_v)$ (finite)

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

   \[ P_v(K,x) \subset \mathbb{H}_v \]

   and $x$ is a fixed point in $\mathbb{H}_v$.

   Then $x$ corresponds to a point on $X_S(C_v)$ defined over an algebraic extension of $K$.

3) (Shimura-Taniyama Conjecture):

   Let $E$ be an elliptic curve $\mathbb{Q}$ with $N_{E/F} = \prod_{v \in S} \mathbb{H}_v$ $v$ non-arch.

   Then there is a non-constant map

   \[ \Phi : J_S \to E \]

   $J_S = \text{Jac}(X_S)$.

   (a lot can be proven in this direction; but not all)
Not Fred:
Supersingular points on $X_1^t(0)/\mathbb{F}_p \leftrightarrow B_{1,1,t}$

\begin{itemize}
\item \textbf{Example:}
\item \textbf{New Form:} $F = Q_1, \quad S = 4003$. Then $X_5 = X_0(1)$
\item $F = Q_1, \quad S = 400, 2, 3 \quad \text{c.f. John Voight's lecture}$
\item $F = Q_1(\mathbb{Z}_4^+), \quad S = \{x_0, x_1, x_2, x_3\}$
\end{itemize}

$\mathbb{p}$-adic uniformization

$F = Q_1, \quad S = \{x_0, x_1, \ldots, x_n\}, \quad \mathfrak{p} \in S$, and study $X_S/\mathbb{C}_p$

$X_S(\mathbb{C}_p) = \{ \mathfrak{p}^n \} \quad \mathfrak{p} \in \mathcal{L}_2(\mathbb{Q}_p)$

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

Def: A \textbf{rigid analytic function} on $\mathbb{H}_p$ is a function $f : \mathbb{H}_p \rightarrow \mathbb{C}_p$
whose restriction to every good \textit{affinoid} $A(F, \mathfrak{p})$ is a
uniform limit of rational functions with poles outside $A$.

(An \textit{affinoid} is a subset of $\mathbb{C}_p$ with almost properties of closedness
eg. Fractal example: \textbf{Ly} $\mathbb{C}_p \setminus \{ \mathfrak{p} \}$)

To get an \textit{affinoid} on $\mathbb{H}_p$, for almost $\mathfrak{p} \in \mathbb{C}_p$: $1 \leq \mathfrak{p} \leq 2^{1/2}$, $1 \leq \mathfrak{p} \leq 2^{1/3}$, $1 \leq \mathfrak{p} \leq 2^{1/4}$

\begin{itemize}
\item \textbf{Boundary measures:} A measure on $\mathcal{P}_f(\mathbb{Q}_p)$ $\mu$ is a
\textbf{finite additive bounded function}
\item $\mu : \left\{ \text{compact open} \mathcal{U} \subseteq \mathcal{P}_f(\mathbb{Q}_p) \right\} \rightarrow \mathbb{C}_p$
\item $\mu : \text{Meas}(\mathcal{P}_f(\mathbb{Q}_p), \mathbb{C}_p), \quad \mu_0(t) = \frac{1}{\mathcal{U}(n)} \int_{\mathcal{F}(\mathbb{Q}_p)} \mu\left(\frac{t}{z-\mathfrak{p}}\right) d\mathcal{U}_n$
\item Have $\text{Meas}(\mathcal{P}_f(\mathbb{Q}_p), \mathbb{C}_p) \rightarrow \text{rigid analytic} \mathfrak{p}$ on $\mathfrak{p}$
\item $\mu \rightarrow \int_{\mu} f \, d\mu$ (for exercise)
\end{itemize}

A finite dimensional $\mathbb{C}_p$-vector space equipped with a \textit{Hecke action}. 
\[ \int_{\mathcal{Z}} \frac{d\mu(z)}{d\tau} \, d\mathcal{Z} = \int_{\mathcal{Z}} \cos \left( \frac{t - \frac{d\tau}{d\tau}}{x} \right) d\mu(t) \]

Suppose that \( \mu \in \text{Meas} \left( \mathcal{M}_1(\mathcal{O}_K), \mathcal{Z} \right) \)

one can define the multiplicative integral:

\[ \int_{\mathcal{Z}} f(z) \, d\mathcal{Z} = \int_{\mathcal{Z}} \left( \frac{t - \frac{d\tau}{d\tau}}{x} \right) d\mu(t) = \left( \frac{x}{x - 2} \right) \left( \frac{x}{x - 2} \right)^{\xi} f(u) \]

for \( \mathcal{O}_K \)

**Remark about the theorem of \( GZ = K \).**

The proof of \( GZ = K \) works almost without change for \( \mathcal{A}_K \), i.e.,

\[ \# \mathcal{L}(G, 1) = \mathcal{L}(A_K, 1) \rightarrow \# A_K(\mathbb{A}) < \infty \]

This was also done by Kolyvagin and Logachev.

If \( F \) is a totally real field, then \( \mathcal{E}_F \) is said to be non-compact arithmetically uniformizable if \( \exists X / F \) such that

\[ \text{ord}_{x \in A_K} L(E/F, x) \rightarrow \mathcal{E}_F / \mathbb{F} \]

Note: \( A_K \rightarrow \text{modular} \) (not the current).

**Theorem:** (Lang, Kolyvagin - Logachev). If \( E \in A_K \), then

\[ \text{ord}_{s=1} L(E/F, s) \leq 1 \Rightarrow \text{rank} = \text{ord}_{s=1} \]

**Mystere:**

1) If a real quadratic field, \( E \) has good reduction of

\( \text{(quadratic) twist of such a curve}. \) Then one can show \( E \) in \( (\mathbb{Z}) \).

- \( \text{ord}_{s=1} L(E/F, s) = 0 \Rightarrow \# E(K) < \infty \) (Tata, Zhang, Kolyvagin).
- \( \text{ord}_{s=1} L(E/F, s) = 1 \Rightarrow ? \? ? \).
Heegner points, revisited

\( \chi_a(N) \rightarrow \mathbb{C}/\mathbb{Z} \)

If \( \lambda \) split in \( K \setminus \mathbb{Q}/N \) (Heegner hyp), then \( \exists \) Heegner points.

\[ \mathcal{M} = \text{ring class field of } K, \quad (\text{disc}(\mathcal{M})/N) = 1 \]

Hence, \( \chi_a(N) \in \mathbb{C}/\mathbb{Z} \). \[ \chi \sigma \in \text{Gal}(K/\mathbb{Q}) \rightarrow \mathbb{C}/\mathbb{Z} \]

Also,

\[ L(\mathbb{E}/K, s) = \prod_{\chi} L(\mathbb{E}/K, \chi, s) \]

\[ L(\mathbb{E}/K, \chi, s) \rightarrow L(\mathbb{E}/K, \chi, 2-s) \]

As each of the factors of the product involve a \( \mathcal{M} \)-fold order.

Hence, key points,

\[ \text{ord}_s L(\mathbb{E}/K, s) > [H:K] \implies \text{rank}(\mathcal{E}(K)) = [H:K] \]

One can prove that if \( \text{ord}_s L(\mathbb{E}/K, s) = [H:K] \) (equality). Then \( \text{RSD} \) is satisfied (i.e., \( \text{rank}(\mathcal{E}(H)) = [H:K] \)).

Hypothesis: If \( K \) is a real quadratic field, the analysis of signs goes through, etc.

Simple case. \( K = \mathbb{Q}(\sqrt{-d}) \), \( N = pM, p \nmid M \)

Modified Heegner hyp.

1) All \( \ell \mid M \), \( \ell \) split in \( K \).
2) \( p \nmid \text{disc } \mathcal{O} \).

Conjectural formula for these “Stark–Heegner points.”

\[ \Lambda \]

Explicit construction:

\( \text{work in } \mathbb{F}_p \) instead of \( \mathcal{M} \), and Shime curves will not contain these “Stark–Heegner points.”

We expect that there is \( \infty \) many quadratic fields of class number 1.
Let \( \pi = \frac{1}{2} (\chi, \chi) \in \text{SL}_2(\mathbb{Z}[1/2]) \), where \( \chi \) is an \( \ell \)-adic character.

If \( \chi \in \text{Gal}(L/K) \), then \( \pi \in \text{Gal}(L/K) \).

The action of \( \pi \in \text{Sp}(2g, \mathbb{Z}[1/2]) \) on \( (g, h) \) is direct (not in each of the factors, though).

Goal: Define a map \( \Phi: \mathbb{P}(T_1(K)) \rightarrow \mathbb{E}(T_1(4)) \), where \( \mathbb{E}(K) \) is an \( \mathbb{E}(K) \) in which \( N = pM \).

The definition of \( \Phi \) is analytic.

**Step 1.** Modular symbols: \( \{r(s), \mathcal{A} \} \) are classical modular forms on \( \mathbb{P}(T_1(4)) \).

A symbol \( \{r(s), \mathcal{A} \} \) is associated to \( \mathcal{A} \).

Given \( r, s \in \mathbb{P}(T_1(4)) \), define \( \mathcal{I}_r(s) := \text{Re} \left( \sum_{l=1}^{p} \frac{1}{l} \right) \in \mathbb{Z} \).

**Step 2.**

**Proposition.** There is a unique system of measure on \( \mathbb{P}(T_1(4)) \), denoted \( \mu_{\{r(s), \mathcal{A} \}} \), satisfying:

1. \( \mu_{\{r(s), \mathcal{A} \}}(\mathbb{P}(T_1(4))) = 1 \) and \( \mu_{\{r(s), \mathcal{A} \}}(\mathbb{P}(T_1(4))) = \mathcal{I}_r(s) \).
2. \( \mu_{\{r(s), \mathcal{A} \}}(\mathbb{P}(T_1(4))) = \mu_{\{r(s), \mathcal{A} \}}(\mathbb{P}(T_1(4))) \) for all \( r, s \in \mathbb{P}(T_1(4)) \).
3. \( \mu_{\{r(s), \mathcal{A} \}} + \mu_{\{r(s), \mathcal{A} \}} = \mu_{\{r(s), \mathcal{A} \}} \) only for \( \mathcal{A} = 0 \).

**Proof.** Use the fact that \( \mathcal{A} \) acts multiplicatively on the open balls in \( \mathbb{P}(T_1(4)) \).
Step 3: Define \( f_{\text{res}} (z) \) as
\[
\int \frac{1}{z - \ell} d\mu_{\text{res}} (t)
\]
for \( z \in \mathbb{C} \) and \( \ell \in \mathbb{C} \).

Properties:
\[
\text{For any} \quad \left( \frac{a \cdot z + b}{c \cdot z + d} \right)^2 \quad \text{on} \quad \Gamma.
\]

Column integral:
\[
\int_{\tau_1}^{\tau_2} f_{\text{res}} (z) \, dz = \int_{\tau_1}^{\tau_2} \log \left( \frac{z - \tau_2}{z - \tau_1} \right) \, d\mu_{\text{res}} (t)
\]

Have also the multiplicative consistency integral:
\[
\int_{\tau_1}^{\tau_2} f_{\text{res}} (z) \, dz
\]

Notation: Write
\[
\int_{\tau_1}^{\tau_2} f_{\text{res}} (z) \, dz = \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f
\]

When \( \Delta \) is the modular Hecke operator on \( \mathcal{M}(H \times \mathbb{C}) \) of weight \( (2, 1) \).

Properties:
\[
\int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f + \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f = \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f
\]

Step 4: Choose \( \phi : C_p \to C_p \) s.t. \( \log (q) = 0 \), where
\( q = \text{Tate period of} \quad E \).

Theorem (Ralph Greenberg, Steven): There is a unique function \( f_{\text{res}} (z) \) so that:
\[
\log (q) = \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f
\]

1) \( \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f = \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f 
\]
2) \( \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f = \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f 
\]
3) \( \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f = \int_{\tau_1}^{\tau_2} \int_{\tau_1}^{\tau_2} \omega_f 
\]
Steps: $z \in H_p \cap K$. A simple calculation shows the Stirling's $\sim <x_z>$

$$J_z = \int \int_{\mathbb{C}} \int \int_{\mathbb{C}}$$

$$J_z^x = \int \int_{\mathbb{C}^x \in \mathbb{C}^x}$$

$$\Phi(z) = \Phi \text{ Tate}\left( J_z^x \right) \in \mathbb{E}(K_p)$$

(Exercise show that $J_z$ does)

**Conjecture:** $\Phi(z) \in \mathbb{E}(K_p)$. The collection of $\Phi(z)$ as $z$ varies over $H_p \cap K$ behave in all respects like Heegner points.

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

**Theorem (Darmon, 2000):** If $T_1, T_2$ are a complete set of points of conductor $h = h(K)$, then

$$\Phi(T_1) = \Phi(T_2) = P_e \in \mathbb{E}(K) \mod \mathbb{E}(K_p)_{tor}$$

and $P_e \in \mathbb{E}(K, 1)$ not 0.
Let $E/K$ be an elliptic curve with $[K: A] = d$, $d > 1$, $E/K$ iset $A$, and $E/K$ iset $A$. Suppose $E/K$ is a $p$-torsion point. Then $p < d^{3d^2}$.

By Faltings & Frey, Thm 2 $\Rightarrow$ Thm 1.

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 1999,1999
   - Proved bounds for $p$-torsion in $E/K$ to be explicit $B(d)$
   - Conjecture: there is a polynomial bound.

§1. Mazur's method.

1.1. Let $E/K$ be an elliptic curve with $[K: A] = d$, and $p \in E(K)$ $p$-torsion point.
   Then $(E, p)$ defines a point $x \in Y_1(p)(K)$.

\[ X_1(p)(K) \ni x = (E, p) \]
\[ \downarrow \]
\[ X_0(p)(K) \ni x = (E, \langle p \rangle) \]

Let $\sigma_1, \ldots, \sigma_d : A \to C$.

\[ x = (\sigma_1(x), \ldots, \sigma_d(x)) \in X_0(p)(K) \]

If $x$ is smooth over $\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$, then $\sigma$ is a $d$-th symmetric power of $X_0(1)$. 

by Rebolchi
Then \( X_0(p)^{(d)} \rightarrow X_0(p)^{(d)} \)

1.2. \( V_0(p)^{(d)} \to J_0(p) \to J_0(\text{winding groups}) \)

\[ \{Q_{1}, Q_{d} \} \to [\{Q_{1}\} + (Q_{d}) - d(\infty)] \]

Proof (Mazur–Kamnitzer):

If \( \phi_{e}^{(a)} : \text{a formal immersion at } \infty^{(d)} \) is image of \( (\infty_{1}, \infty_{d}) \) in \( V_0(p)^{(d)} \),

then \( Y_1(p)/K) = \varnothing \) for all \#fields \( K, [K : \mathbb{Q}] = d \).

We will see that \( \exists \) a formal immersion for \( p \gg 1 \), for \( d = 1 \) and \( d > 1 \).

(The case \( d = 1 \) will finish Mazer's theorem.)

Need a criterion for formal immersions (Recall \( \psi : X \to Y \) FI ?

Criterion (differentiable criterion)

\( \psi X \to \text{Cot } Y \to \text{Cot } X \).

We have \( \text{Cot}(J_0/\mathbb{Z}) \rightleftarrows \text{Cot}(J_0(p)/\mathbb{Z}) \quad (\mathcal{S} = \mathcal{A}_3/\mathcal{P}_3) \)

Then \( \text{Cot}(J_0(p)/\mathbb{Z}) \leftarrow \text{Cot}(J_0(p)/\mathbb{Z}) \) due to \( \Phi_{e}^{(a)} : X(p) \to J_0(p) \)

Due to Grothendieck–Serre duality,

By taking \( \text{Cot}(J_0(p)/\mathbb{Z}) \leftarrow \mathcal{S}_q \),

From \( \text{Cot}(J_0/\mathbb{Z}) \rightarrow \text{Cot}(X_0(p)^{(d)}) \quad ? \)

one finds \( \Phi_{e}^{(a)} : X(p) \to J_0(p) \) at \( \infty \), \( \hat{E}_{X_0(p)} \), \( \sim \mathbb{Z} \left[ q \mathcal{II} \right] \)

\( \Phi_{e} \)

Hence \( \text{Cot}(X_0(p)^{(d)}) \) is a free \( \mathbb{Z} \)-module of rank \( d \),

with a basis given by \( \mathcal{A}_1, \ldots, \mathcal{A}_d \).
Lemma: Let $w \in \text{Cot} \, S_0(p)/\mathbb{Z}$ be a $q$-expansion $\sum a_m q^m \in \mathbb{Q}_q$. Then

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

If $\Phi^d \Phi^{(d)} (w)$ is an eigenform (use Newton Formula), then

$$\int_{w} \Phi^d \Phi^{(d)} (w) = \sum_{m \geq 1} a_m q_m \frac{d q_m}{q_m} = \sum_{m \geq 1} a_m q_m^{-1} d q_m = \sum_{m \geq 1} a_m q_m^{-1} d q_m$$

End of the case $d = 1$

Let $w \in \text{Cot} \, S_0(p)/\mathbb{Z}$ be an eigenform. Then by the $q$-expansion principle, its $q$-exp is not identically 0. So since $w$ is an eigenform, $a_1(w) \neq 0$ (on $a_m(w) = 0$ for).

So $a_1(w)$ generates $\text{Cot} \, S_0(p) \subset \mathbb{Z}$

Theorem (Mazur, Kiming): TFAE:

1) $\Phi^d \Phi^{(d)} (w)$ is an $\mathcal{F} \mathcal{L}$ at $\infty$ of $\text{Cot} \, S_0(p)/\mathbb{Z}$

2) There exist $l_1, \ldots, l_d \in S_0(p, \mathbb{Z})$ such that $(a_l(l_1), \ldots, a_l(l_d))$ is $\mathbb{Z}$-linearly independent.

3) The image of $\mathcal{T}_1 \mapsto \mathcal{T}_d$ in $\frac{\mathcal{T}_d}{\mathcal{T}_1}$ are $\mathbb{Z}$-linearly independent.

\begin{align*}
(3) \Rightarrow \text{beaut} \quad S_2(p, \mathbb{Z}) \cong \text{Hom}(\mathcal{T}/\mathcal{T}_1, \mathbb{Z}) \\
\downarrow \otimes (t \mapsto a_l(t t'))
\end{align*}

Write now $X = X_0(p) \subset \text{H}_1^p(\mathbb{Q})$

$e \in H_1^p(X, \mathbb{Z})$, almost equal to $-a_1 \otimes 0$.

Recall $\mathcal{T} \mapsto C_{\mathbb{Q}} \text{Cot}(p)$, $\text{Cot}$ with pole in $\text{H}_1(X, \mathbb{Z})$. 

Moreover, $T_e$ is a $T_{fe}$-module, free of rank 1.

So conditions (1)-(3) of prev. theorem are also equivalent to

4) $T_e$, $T_{fe}$ are $\mathbb{Z}$-linearly independent in $T_e$.

52. Heart of Néron's proof

$H_1(X, \mathbb{R}) \xrightarrow{\sim} \text{Hom}(\mathbb{Z}_2, \mathbb{R})$ of $\mathbb{R}$-vector esp. $e \mapsto (w \mapsto \int_0^w)$

Defined by Dorman's lemma $e := \text{pullback of } (w \mapsto \int_0^w)$

There is a difference between $e$ and $-40, 70$, due to the "Eisenstein part" of $H_1(Y, \text{cups}, \mathbb{Z})$, on which $T_e$ act by $x_0 \cdot (n)$

Recall that we want to prove that for $p > 70^2$, $(\sigma^{-1}(n)) = \mathbb{Z}_d$

$T_e \cdot e, T_{fe} \cdot e, \ldots \cdot T_e \cdot e$ are $\mathbb{Z}$-linearly independent.

It suffices to prove that

$e, T_e, \ldots, T_{fe}$ are $\mathbb{Z}$-linearly independent.

This is better known as $T_e = -t \cdot 40, 70$.

Idea of the proof:

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

Suppose $d_1 e_1 + d_2 e_2 + \ldots + d_k e_k = 0$, $e \in \mathbb{Z}$

Strategy: find $x \in H_1(X, \mathbb{Z})$ s.t. $t e \cdot x \neq 0 \quad t e \cdot x = 0 \quad \forall \in H$
To find \( \varphi \), the key fact is

1. If a presentation of \( H_1(X, \mathbb{Z}) \) is given \( \varphi(\alpha) \) and relative.
2. We know how to compute \( \varphi(\alpha) \cdot \varphi(\beta) \).

We need to express \( \varphi \) in terms of the \( \varphi(\alpha) \).

### 2.1 Moeun Symbols

Let \( \alpha, \beta \in \Pi^1(\mathbb{A}) \), and form a good pair from \( \alpha \) to \( \beta \), which leads to a homotopy class \( [\alpha, \beta] \in H_1(X_{\mathbb{A}}^{tor}, \mathbb{Z}) \).

It is an exercise that \( [\alpha, \beta] \) is a sum of the type \( \frac{b}{a}, \frac{c}{d} \)

where \( a, b, c, d \in \mathbb{Z} \), \( ad - bc = 1 \) (use continued fractions).

Also, if \( \Gamma_0(p) \alpha = \Gamma_0(p) \beta \), then \( \varphi_1 \alpha, \beta \in H_1(X, \mathbb{Z}) \).

\( \frac{b}{a}, \frac{c}{d} \) depends only on the class of \( (a, b) \) in \( \Gamma_0(p) \).

So, get a map (surjective)

\[
\mathbb{Z} \left[ \frac{b}{a}, \frac{c}{d} \right] \rightarrow H_1(X_{\mathbb{A}}^{tor}, \mathbb{Z}),
\]

\( \varphi(\alpha) \rightarrow \left\{ \frac{b}{a}, \frac{c}{d} \right\} : (a, b, c, d). \)

We have an isomorphism

\[
\frac{b}{a}, \frac{c}{d} \rightarrow \mathbb{P}^1(F_p) \quad \text{so that} \quad \varphi(\alpha) = \varphi\left( \frac{a}{b}, \frac{c}{d} \right)
\]

Now for \( \alpha + \mathbb{F}_p^\times \), \( \varphi(\alpha) = \frac{0}{1}, \frac{1}{0} \rightarrow \varphi(\alpha) \in H_1(X, \mathbb{Z}) \).

Also, there exists \( \varphi(\alpha) \) and 

\( \varphi(0) = -\varphi(\infty) \in \mathbb{F}_p \).

"Lemme des Cordes" (Mecq)

Let \( k, k' \in \mathbb{F}_p^\times \), denote by \( k \cdot \mathbb{F}_p^{11, \cdots, \rho^{-1}} \). \( 1 \) \( k \cdot k' = -1 \) (\( \rho \))

\( k' = e^{2 \pi i k' / p} \)

\( e^{2 \pi i k' / p} = \frac{e^{2 \pi i k / p}}{e^{2 \pi i k' / p}} \)

the element from \( e^{2 \pi i k / p} \) to \( e^{2 \pi i k' / p} \) in the unit circle.

Then \( \varphi(k) \cdot \varphi(k') = \varphi(k \cdot k') \quad \text{if \( k' \neq 0 \).} \)
2.2. "Black Box"

\[ t_r e = - \sum_{(\lambda, \nu) \in \mathcal{X}_r} \gamma(\lambda, \nu) \]

where \( \mathcal{X}_r = \{ \lambda + \nu \mid \lambda \in M_0 N_1(\mathbb{R}) \} \)

\( (\lambda, \nu) \)

**Proof**

We have \( t e = - t \sum_{(\lambda, \nu) \in \mathcal{X}_r} \gamma(\lambda, \nu) \). Let \( X_r \) be the set of all \( (\lambda, \nu) \) such that \( \gamma(\lambda, \nu) \neq 0 \).

And also \( \exists \) \( e \cdot \gamma(\lambda, \nu) = \frac{\lambda - \nu}{\nu} (p-1) \cdot \gamma(\lambda, \nu) \)

**2.3. End of the proof**

Let \( e = 0 \) and \( t e = 0 \).

If \( \lambda = 0 \),

we have \( e \cdot \gamma(\lambda, \nu) \neq 0 \).

Hence, \( t e \cdot \gamma(\lambda, \nu) = 0 \) \( \forall \lambda, \nu \).

Let \( e \in \mathcal{X}_r \) s.t.

\( e \cdot \gamma(\lambda, \nu) = 0 \).

Then, \( \gamma(\lambda, \nu) = 0 \) \( \forall \lambda, \nu \).

Choose \( p \rightarrow \frac{p-1}{e} \)

So, there exists a "law of sines".

Let \( k e \in \mathcal{X}_r \)

and also s.t.

\( e \cdot \gamma(\lambda, \nu) \neq 0 \).

It is possible to do so by an arbitrary lemma for \( p > d \).

For \( p > d \):

Suppose \( \alpha t \xi + i + i + t e = 0 \), \( 1 < c < d \).

Then \( \gamma(\lambda, \nu) \) s.t.

\( t e \cdot \gamma(\lambda, \nu) \neq 0 \).

Let \( \gamma(\lambda, \nu) \) occur only in \( t e \).
So to finish, look for \( \xi(x) \) s.t.

\[
\xi\left(\frac{z}{c}\right) \neq 0
\]

\[
\xi\left(\frac{w}{\epsilon}\right) \cdot \xi(x) = 0 \quad \forall \left(\frac{w}{\epsilon}\right) \in \mathbb{R}, x < c
\]

\[
\frac{w}{\epsilon} + \epsilon
\]

Exercise: \( |l - q| \), \( \sigma = \frac{p - d^2}{d(d-1)} \)

\[
(\text{define } \epsilon \equiv \frac{l}{w})
\]

Suffices to find \( k \in A \) or \( k \in B \)

This is possible using the same analytic lemma. Then \( p > d^3d^2 \).