ARITHMETIC OF L-FUNCTIONS

CHAO LI

NOTES TAKEN BY PAK-HIN LEE

Abstract. These are notes I took for Chao Li's course on the arithmetic of L-functions offered at Columbia University in Fall 2018 (MATH GR8674: Topics in Number Theory).

WARNING: I am unable to commit to editing these notes outside of lecture time, so they are likely riddled with mistakes and poorly formatted.

Contents

Last updated: December 14, 2018. Please send corrections and comments to phlee@math.columbia.edu.

1. Lecture 1 (September 10, 2018)

1.1. **Motivation: arithmetic of elliptic curves.**

Let us begin with some motivation by studying the arithmetic of elliptic curves. Consider an elliptic curve $E : y^2 = x^3 + Ax + B$, where $A, B \in \mathbf{Q}$.

Example 1.1. The elliptic curve $y^2 = x^3 - x$ intersects with the x-axis at $(-1, 0)$, $(0, 0)$ and $(1, 0)$.

Given two points P, Q on E, the straight line through P and Q intersects E at a third point R. Declaring that $P + Q + R = 0$ defines an abelian group law on E and on the set of rational points $E(\mathbf{Q})$. There are some degenerate cases; for example, the tangent line through $P' \in E$ defines the relation $2P' + R' = 0$.

A fundamental result in the arithmetic of elliptic curves is that the group of rational points cannot be too huge.

Theorem 1.2 (Mordell)**.** *$E(\mathbf{Q})$ is finitely generated.*

Definition 1.3. The *algebraic rank* of E is defined as $r_{\mathrm{alg}}(E) := \operatorname{rank} E(\mathbf{Q}) \in \mathbf{Z}_{\geq 0}$.

In particular, $r_{\mathrm{alg}}(E) = 0$ if and only if $E(\mathbf{Q})$ is finite.

Example 1.4. For $E : y^2 = x^3 - x$, $E(\mathbf{Q}) = \mathbf{Z}/2 \times \mathbf{Z}/2$ is generated by the two 2-torsion points $(0, 0)$ and $(1, 0)$. Thus $r_{\mathrm{alg}}(E) = 0$.

Example 1.5. For $E : y^2 = x^3 - 25x$, one can check that $P = (-4, 6) \in E(\mathbf{Q})$, and $2P = (\frac{1681}{144}, -\frac{62279}{1728}) \in E(\mathbf{Q})$. In fact, $E(\mathbf{Q}) \simeq \mathbf{Z} \times \mathbf{Z}/2 \times \mathbf{Z}/2$, with generators $(-4, 6)$, $(0, 0)$, $(5, 0)$ respectively, and thus $r_{\mathrm{alg}}(E) = 1$.

The greatest mystery in the study of elliptic curves is the following question. Given $E/\mathbf{Q}$, how do we determine $r_{\mathrm{alg}}(E)$? No algorithm exists yet! In fact, we have very little knowledge; we don't even know which integers can show up as $r_{\mathrm{alg}}(E)$.

To show how limited our knowledge is:

Example 1.6. Consider $E^{(n)} : y^2 = x^3 - n^2x$. The smallest n for each value of $r_{\mathrm{alg}}(E^{(n)})$ is

$r_{\mathrm{alg}}(E^{(n)})$	0	1	2	3	4	5	6
n	1	5	34	1254	29274	48272239	6611714866

but we don't know of any n which gives $r_{\mathrm{alg}}(E^{(n)}) = 7$.

1.2. **Understanding $r_{\mathrm{alg}}(E)$: BSD conjecture.**

In order to attack the problem of understanding $r_{\mathrm{alg}}(E)$, the deep connections with the arithmetic L-function come into play.

Analogous to the Riemann zeta function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1},$$

we can define the L-function associated to $E/\mathbf{Q}$:

$$L(E, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p L_p(E, s),$$

where the Euler factor is defined by

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \text{if } p \text{ is good,} \\ (1 - a_p p^{-s})^{-1} & \text{if } p \text{ is bad,} \end{cases}$$

and

$$a_p = \begin{cases} p + 1 - |E(\mathbf{F}_p)| & \text{if } p \text{ is good,} \\ \pm 1 & \text{if } p \text{ is multiplicative,} \\ 0 & \text{if } p \text{ is additive.} \end{cases}$$

Later we will give some motivation for defining the L-function this way. The whole point is that these L-functions are much easier to study; for example, a_p is a more tractable number, depending on the number of points of E mod p.

$L(E,s)$ converges when $\operatorname{Re} s > \frac{3}{2}$. Analogous to the Riemann zeta function, we expect $L(E,s)$ to admit analytic continuation and satisfy a functional equation. In fact, there is the miraculous theorem:

Theorem 1.7 (Modularity theorem: Wiles, Taylor, BCDT)**.** *There exists a cuspidal eigenform $f_E \in S_2(N_E)$ such that*

$$f_E(s) = \sum_{n \geq 1} a_n q^n$$

where the a_n's are as before.

Example 1.8. Consider $E : y^2 = x^3 - x$, which has conductor $N_E = 32$. Solving this equation mod p, we see that

p	2	3	5	7	11	13	17	19	23	29	31
a_p	0	0	-2	0	0	6	2	0	0	-10	0

Notice that $a_p \neq 0$ if and only if $p \equiv 1 \pmod 4$. Under the modularity theorem, the corresponding modular form is

$$\begin{aligned} f_E &= q \prod_{n \geq 1} (1 - q^{4n})^2 (1 - q^{8n})^2 \\ &= q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} + \cdots . \end{aligned}$$

The modularity theorem is truly miraculous; why does the number of solutions mod p have anything to do with modular forms? For us, we have the

Corollary 1.9. $L(E,s) = L(f_E,s)$. *In particular, $L(E,s)$ has analytic continuation to $\mathbf{C}$ and satisfies a functional equation under $s \leftrightarrow 2 - s$.*

Definition 1.10. The *analytic rank* of E is defined as $r_{\text{an}}(E) := \operatorname{ord}_{s=1} L(E,s) \in \mathbf{Z}_{\geq 0}$.

Conjecture 1.11 (BSD)**.** $r_{\text{alg}}(E) = r_{\text{an}}(E)$.

Remark. BSD leads to an algorithm for computing r_{alg} and r_{an}.

Theorem 1.12 (Gross–Zagier, Kolyvagin, 1980's)**.**

(1) *If $r_{\text{an}}(E) = 0$, then $r_{\text{alg}}(E) = 0$.*
(2) *If $r_{\text{an}}(E) = 1$, then $r_{\text{alg}}(E) = 1$.*

But little is known in the higher rank case!

1.3. **Bridge: Selmer groups.** Let us outline how this theorem is proved.

$$\begin{tikzcd}
E(\mathbf{Q}) \arrow[rr, leftrightarrow, dotted, "\text{very far}"] \arrow[dr, dash, "(*)"'] & & L(E,s) \arrow[dl, dash, "(**)"] \\
& \mathrm{Sel}_{p^\infty}(E) &
\end{tikzcd}$$

where the connection $(*)$ is made by p^∞-descent, and $(**)$ is by explicit reciprocity laws.

Recall the p^n-descent sequence

$$0 \to E(\mathbf{Q})/p^n E(\mathbf{Q}) \to \mathrm{Sel}_{p^n}(E) \to Ш(E)[p^n] \to 0$$

where $\mathrm{Sel}_{p^n}(E)$ is a finite group and $Ш(E)$ is the Tate–Shafarevich group.

Conjecture 1.13. *$Ш(E)$ is finite.*

Taking inverse limit over n and tensoring with $\mathbf{Q}_p$, we get an injection

$$E(\mathbf{Q}) \otimes \mathbf{Q}_p \hookrightarrow \mathrm{Sel}_{p^\infty}(E)$$

which is an isomorphism if $Ш(E)$ is finite. So

$$\text{finiteness of } Ш(E) \implies r_{\mathrm{alg}}(E) = \dim_{\mathbf{Q}_p} \mathrm{Sel}_{p^\infty}(E).$$

$\dim_{\mathbf{Q}_p} \mathrm{Sel}_{p^\infty}(E)$ is called the Selmer rank of E.

In summary, the algebraic object $\mathrm{Sel}_{p^\infty}(E)$ gives an upper bound for $r_{\mathrm{alg}}(E)$, which is sharp if $Ш(E)$ is finite. Moreover, $\mathrm{Sel}_{p^\infty}(E)$ is easier to understand due to its local nature.

Strategy for proving Theorem 1.12:

(1) $r_{\mathrm{an}} = 0 \implies \mathrm{Sel}_{p^\infty}(E) = 0$.
(2) $r_{\mathrm{an}} = 1 \implies \dim \mathrm{Sel}_{p^\infty}(E) \le 1$. Then show $r_{\mathrm{alg}}(E) \ge 1$ by finding a point of infinite order.

The connection between r_{an} and Selmer groups is obtained by bounding Selmer groups from above using Euler systems (due to Kolyvagin), and the explicit point construction is by considering Heegner points (due to Gross–Zagier).

The key in bounding Selmer groups is to construct Galois cohomology classes with *controlled local ramification.* There are currently three ways to do this:

- Kolyvagin: Heegner points in ring class fields
- Bertolini–Darmon: Heegner points on different Shimura curves
- Kato: Kato classes in cyclotomic fields (in case (1) only)

We will focus on the second approach by Bertolini–Darmon, and generalize to more general motives.

Let me briefly indicate where the ramification comes from in each case:

- Kolyvagin: tamely ramified extensions
- Bertolini–Darmon: ramified groups
- Kato: wildly ramified extensions

1.4. **Bloch–Kato conjecture for Rankin–Selberg motives.** The second part of the course will be on some recent results on Bloch–Kato conjecture for certain Rankin–Selberg motives.

For elliptic curves, the Bloch–Kato conjecture takes the following form:

Conjecture 1.14 (Bloch–Kato)**.** $\dim \mathrm{Sel}_{p^\infty}(E) = r_{\mathrm{an}}(E)$.

This is exactly as predicted by BSD and the finiteness of Ш.

Bloch–Kato gives an alternative definition of Selmer groups $H^1_f(\mathbf{Q}, \rho_E)$ where $\rho_E : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_p)$ is the Galois representation on the rational Tate module $T_p(E) \otimes \mathbf{Q}_p$. The Bloch–Kato Selmer groups H^1_f are $\mathbf{Q}_p$-vector spaces associated to arbitrary p-adic Galois representations coming from geometry, which coincide with the usual Selmer groups in the case of elliptic curves. Now we can generalize the earlier picture

$$\begin{tikzcd}
 & f_E \in S_2(N) \arrow[dl] \arrow[dr] & \\
H^1_f(\mathbf{Q}, \rho_E) \cong \mathrm{Sel}_{p^\infty}(E) & & L(f_E, s)
\end{tikzcd}$$

Let Π be a conjugate self-dual cohomological cuspidal automorphic representation on $\mathrm{GL}_n(\mathbf{A}_K)$ where K is a CM quadratic extension of a totally real field F. By the global Langlands correspondence (due to many people, e.g. Chenevier–Harris), we can associate to Π a Galois representation $\rho_\Pi : G_K \to \mathrm{GL}_n(\overline{\mathbf{Q}_p})$.

Now consider Π on $\mathrm{GL}_n(\mathbf{A}_K)$ and Π' on $\mathrm{GL}_{n+1}(\mathbf{A}_K)$, which give the Rankin–Selberg motive $H^1_f(K, \rho_\Pi^\vee \otimes \rho_{\Pi'}^\vee)$ and the Rankin–Selberg L-function $L(\Pi \times \Pi', s)$. The Bloch-Kato conjecture in this case asserts that

Conjecture 1.15 (Bloch–Kato)**.** $\dim H^1_f(K, \rho_\Pi^\vee \otimes \rho_{\Pi'}^\vee) = \mathrm{ord}_{s=\frac{1}{2}} L(\Pi \times \Pi', s)$.

Theorem 1.16 (Liu–Tian–Xiao–Zhang–Zhu)**.** *Assume* Π *and* Π' *have trivial infinitesimal character and* p *satisfies certain assumptions.*

(1) *If* $\mathrm{ord}_{s=\frac{1}{2}} L(\Pi \times \Pi', s) = 0$, *then* $H^1_f(K, \rho_\Pi^\vee \otimes \rho_{\Pi'}^\vee) = 0$.

(2) *Assume* $\mathrm{cl}_{\mathrm{GGP}}(\Pi \times \Pi') \in H^1_f(K, \rho_\Pi^\vee \otimes \rho_{\Pi'}^\vee)$ *is nonzero. Then* $\dim H^1_f(K, \rho_\Pi^\vee \otimes \rho_{\Pi'}^\vee) = 1$.

Remark. By the Beilinson conjecture, $\mathrm{cl}_{\mathrm{GGP}}(\Pi \times \Pi') \neq 0 \iff \mathrm{ord}_{s=\frac{1}{2}} L(\Pi \times \Pi', s) = 1$.

2. Lecture 2 (September 12, 2018)

2.1. ***L*-functions of elliptic curves.** Recall: for an elliptic curve $E/\mathbf{Q}$, we define

$$L(E, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p L_p(E, s)$$

where the Euler factor at p is

$$L_p(E, s) = \begin{cases} (1 - a_p p^{-s} + p \cdot p^{-2s})^{-1} & \text{if } p \nmid N = N_E, \\ (1 \pm p^{-s})^{-1} & \text{if } p \parallel N, \\ 1 & \text{if } p^2 \mid N. \end{cases}$$

A uniform way to write this is as follows: define $\chi(p) = \begin{cases} 1 & \text{if } p \nmid N, \\ 0 & \text{if } p \mid N, \end{cases}$, so then

$$L_p(E, s) = (1 - a_p p^{-s} + \chi(p) p \cdot p^{-2s})^{-1}.$$

Some easy consequences are:

(1) $a_1 = 1$.
(2) $a_{mn} = a_m a_n$ if $(m, n) = 1$.
(3) $a_{p^r} = a_p a_{p^{r-1}} - \chi(p) p a_{p^{r-2}}$ if $r \geq 2$.

This exactly matches the relations for Hecke operators T_n.

Remark. $L(E, s)$ is an example of a "motivic L-function", i.e., one associated to Galois representations coming from geometry. Recall the ℓ-adic Tate module $T_\ell E = \varprojlim_n E[\ell^n]$, which is a $\mathbf{Z}_\ell$-module of rank 2. The action of $G_{\mathbf{Q}}$ on $V_\ell E = T_\ell E \otimes \mathbf{Q}_\ell$ gives rise to a 2-dimensional Galois representation

$$\rho_E : G_{\mathbf{Q}} \to \mathrm{Aut}(V_\ell E) \simeq \mathrm{GL}_2(\mathbf{Q}_\ell).$$

Then for $p \neq \ell$,

$$L_p(E, s) = \det\left(1 - p^{-s} \,\mathrm{Fr}_p \mid (V_\ell E)^{I_p}\right)^{-1}$$

where $I_p \subset G_{\mathbf{Q}_p}$ is the inertia subgroup. Notice that

$$\dim(V_\ell E)^{I_p} = \begin{cases} 2 & \text{if } p \nmid N, \\ 1 & \text{if } p \parallel N, \\ 0 & \text{if } p^2 \mid N. \end{cases}$$

In particular, $a_p = \mathrm{tr}(\mathrm{Fr}_p \mid (V_\ell E)^{I_p})$.

Proposition 2.1. *$L(E, s)$ converges when* $\mathrm{Re}\, s > \frac{3}{2}$.

Proof. By counting the number of solutions to $y^2 = x^3 + Ax + B$, we have the trivial bound $|E(\mathbf{F}_p)| \leq 2p + 1$. However, 50% chance of being a square in $\mathbf{F}_p$ gives the heuristic $|E(\mathbf{F}_p)| \overset{?}{\sim} p + 1$. This is made precise by

Theorem 2.2 (Hasse)**.** *$|p + 1 - |E(\mathbf{F}_p)|| \leq 2\sqrt{p}$.*

This implies

$$\left|\frac{a_n}{n^s}\right| = O\left(\frac{1}{n^{\mathrm{Re}\, s - \frac{1}{2}}}\right)$$

and so $\sum \frac{a_n}{n^s}$ converges if $\mathrm{Re}\, s - \frac{1}{2} > 1$. □

Remark. Hasse's theorem can be seen in a high-brow manner using the Weil conjectures, since $a_p = \alpha + \beta$ with $|\alpha| = |\beta| = p^{1/2}$.

Expected properties of $L(E, s)$ (more generally *any* motivic L-function):

(1) Euler product.
(2) $L(E, s)$ has analytic continuation to all of $\mathbf{C}$.
(3) $L(E, s)$ has a functional equation.

(2) and (3) are more difficult and is one of the motivations of the *Langlands program.*

$$\begin{matrix} L(E,s) & & L(f_E,s) \\ \text{motivic } L\text{-function} & \longleftrightarrow & \text{automorphic } L\text{-function} \end{matrix}$$

Automorphic L-functions are associated to modular forms or automorphic forms, for which (2) and (3) are easier.

2.2. **L-functions of modular forms.** Let $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \pmod N \right\} \subseteq \mathrm{SL}_2(\mathbf{Z})$. Let $S_k(N)$ be the space of cusp forms of level $\Gamma_0(N)$ and weight k. Recall $f \in S_k(N)$ if:

(1) $f : \mathcal{H} \to \mathbf{C}$ is holomorphic.
(2) $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \Gamma_0(N)$.
(3) f is holomorphic and vanishes at all cusps.

Every $f \in S_k(N)$ has a Fourier expansion $f(\tau) = \sum_{n\geq 1} a_n(f)q^n$.

Definition 2.3. The L-function of a cusp form $f \in S_k(N)$ is defined as

$$L(f,s) := \sum_{n\geq 1} \frac{a_n}{n^s},$$

where $a_n = a_n(f)$.

Remark. In this generality, $L(f,s)$ may not have an Euler product. It has an Euler product if and only if f is eigenform for all T_n's.

Proposition 2.4. *$L(f,s)$ converges when* $\operatorname{Re} s > \frac{k}{2} + 1$*. In fact,* $|a_n| = O(n^{k/2})$.

Remark.

- This is the trivial bound for $E/\mathbf{Q}$ (for weight $k = 2$).
- If f is an eigenform, there is a sharper bound $|a_p| = O(p^{\frac{k-1}{2}})$ (due to Deligne).

Proof. Notice

$$a_n = \int_0^1 e^{-2\pi i n(x+iy)} f(x+iy)\, dx$$

for any y. Taking $y = \frac{1}{n}$, we have

$$|a_n| = e^{2\pi} \left| \int_0^1 f\left(x + i \cdot \frac{1}{n}\right)\, dx \right|.$$

On the other hand, $|f(\tau)|(\operatorname{im}\tau)^{\frac{k}{2}}$ is invariant under Γ. Since f is a *cusp* form, the function $|f(\tau)|(\operatorname{im}\tau)^{\frac{k}{2}}$ is extended to $\Gamma\backslash\mathcal{H}^*$, so it is bounded on $\mathcal{H}$. This implies $|f(x+iy)| = O(y^{-\frac{k}{2}})$.

For $y = \frac{1}{n}$, we have $|f(x + i \cdot \frac{1}{n})| = O(n^{\frac{k}{2}})$ and so $a_n = O(n^{\frac{k}{2}})$. □

The next goal is to prove (2) and (3) for $L(f,s)$.

2.3. **Proofs of analytic continuation and functional equation.** Starting point: $L(f,s)$ has an explicit integral representation (Mellin transform of f).

Definition 2.5. The Mellin transform of f is

$$g(s) = \int_0^\infty f(it) t^s \, \frac{dt}{t}.$$

Proposition 2.6. *$g(s) = (2\pi)^{-s}\Gamma(s)L(f,s)$ when $\operatorname{Re} s > \frac{k}{2}+1$.*

Proof. Recall $\Gamma(s) = \int_0^\infty e^{-t}t^s \, \frac{dt}{t}$. Changing t by $2\pi n t$,

$$\Gamma(s) = (2\pi n)^s \int_0^\infty e^{-2\pi n t} t^s \, \frac{dt}{t},$$

so

$$n^{-s} = (2\pi)^s \Gamma(s)^{-1} \int_0^\infty e^{-2\pi n t} t^s \, \frac{dt}{t}.$$

Summing over n gives

$$\begin{aligned} L(f,s) = \sum_{n\geq 1} \frac{a_n}{n^s} &= (2\pi)^s\Gamma(s)^{-1} \sum_{n \geq 1} a_n \int_0^\infty e^{-2\pi n t} t^s \, \frac{dt}{t} \\ &= (2\pi)^s\Gamma(s)^{-1} \int_0^\infty \sum_{n\geq 1} a_n e^{-2\pi n t} t^s \, \frac{dt}{t} \\ &= (2\pi)^s\Gamma(s)^{-1} \int_0^\infty f(it) t^s \, dt \\ &= (2\pi)^s\Gamma(s)^{-1} g(s). \end{aligned}$$

Therefore $g(s) = (2\pi)^{-s}\Gamma(s)L(f,s)$. □

Definition 2.7. The complete L-function of f is

$$\Lambda(f,s) := N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f,s) = N^{\frac{s}{2}} g(s).$$

To get a functional equation, we need some extra symmetry on f.

Definition 2.8 (Atkin–Lehner involution)**.** Define an operator $W_N : S_k(N) \to S_k(N)$ by

$$(W_N f)(\tau) = \left(\frac{i}{\sqrt{N}\tau}\right)^k f\left(-\frac{1}{N\tau}\right).$$

One can check that $W_N^2 = 1$.

Theorem 2.9 (Hecke)**.** *Let $f \in S_k(N)$. Assume $W_N f = \epsilon f$, where $\epsilon \in \{\pm 1\}$. Then*

1. *$\Lambda(f,s)$ has analytic continuation to all of $\mathbf{C}$.*
2. *There is a function equation*

$$\Lambda(f,s) = \epsilon \Lambda(f, k-s).$$

ϵ is called the sign of the functional equation, and plays an important role in the BSD conjecture. Since $N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)$ doesn't have any zeros, we have the

Corollary 2.10. *$L(f,s)$ has analytic continuation to all of $\mathbf{C}$.*

Remark. This theorem applies to any newform $f \in S_k(N)$, so $\Lambda(f,s) = \pm\Lambda(f,k-s)$.

Proof of Theorem 2.9.

$$\begin{aligned}\Lambda(f,s) &= N^{\frac{s}{2}}\int_0^\infty f(it)t^s\,\frac{dt}{t}\\ &= \int_0^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\,\frac{dt}{t}\quad\left[\text{by } t\mapsto\frac{t}{\sqrt{N}}\right]\\ &= \underbrace{\int_0^1 f\left(\frac{it}{\sqrt{N}}\right)t^s\,\frac{dt}{t}}_{(*)}+\underbrace{\int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\,\frac{dt}{t}}_{(**)}.\end{aligned}$$

The term $(**)$ clearly converges, whereas

$$\begin{aligned}(*) &= \int_0^1 (W_N f)\left(\frac{i}{\sqrt{N}t}\right)t^{s-k}\,\frac{dt}{t}\quad[\text{by definition of } W_N]\\ &= \int_1^\infty (W_N f)\left(\frac{it}{\sqrt{N}}\right)t^{k-s}\,\frac{dt}{t}\quad[\text{by } t\mapsto t^{-1}].\end{aligned}$$

Therefore,

$$\Lambda(f,s)=\int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\,\frac{dt}{t}+\int_1^\infty (W_N f)\left(\frac{it}{\sqrt{N}}\right)t^{k-2}\,\frac{dt}{t}.$$

The theorem follows since $W_N f=\epsilon f$. □

3. Lecture 3 (September 17, 2018)

3.1. **Rank part of BSD.** Recall: For an elliptic curve $E/\mathbf{Q}$,

$$L(E,s)=\prod_p L_p(E,s).$$

By the modularity theorem, we have shown:

(1) $L(E,s)$ has analytic continuation to $\mathbf{C}$.
(2) $L(E,s)$ satisfies a functional equation under $s\leftrightarrow 2-s$.

The complete L-function satisfies $\Lambda(E,s)=\epsilon\Lambda(E,2-s)$ where $\epsilon\in\{\pm1\}$.

At the center of the functional equation $s=1$, we have

$$\operatorname{ord}_{s=1}\Lambda(E,s)=\begin{cases}\text{even} & \text{if } \epsilon=+1,\\ \text{odd} & \text{if } \epsilon=-1.\end{cases}$$

Since $\operatorname{ord}_{s=1}\Lambda(E,s)=\operatorname{ord}_{s=1}L(E,s)$,

$$r_{\text{an}}(E)=\begin{cases}\text{even} & \text{if } \epsilon=+1,\\ \text{odd} & \text{if } \epsilon=-1.\end{cases}$$

Question. What is the relation between $r_{\text{an}}(E)$ and $r_{\text{alg}}(E)$?

Heuristically, we can try plugging $s=1$ into $\prod_p L_p(E,s)$, although this doesn't converge! Note that

$$L_p(E,1)=(1-a_p\cdot p^{-1}+\chi(p)p\cdot p^{-2})^{-1}$$

$$
\begin{aligned}
&= \left(\frac{p - a_p + \chi(p)}{p}\right)^{-1} \\
&= \frac{p}{p - a_p + \chi(p)} \\
&= \begin{cases} \frac{p}{p+1-a_p} & \text{if } p \text{ is good,} \\ \frac{p}{p\pm 1} & \text{if } p \text{ is multiplicative,} \\ \frac{p}{p} & \text{if } p \text{ is additive,} \end{cases} \\
&= \frac{p}{|\widetilde{E}(\mathbf{F}_p)|}
\end{aligned}
$$

where $\widetilde{E}$ is the smooth part of the reduction of E mod p, so

$$L(E,1) \text{“="} \prod_p \frac{p}{|\widetilde{E}(\mathbf{F}_p)|}.$$

If $E(\mathbf{Q})$ has “more” points (i.e., $r_{\mathrm{alg}}(E)$ is “large”), then $|\widetilde{E}(\mathbf{F}_p)|$ is “large” for each p, and hence $L(E,1)$ becomes “more” zero (i.e., $r_{\mathrm{an}}(E)$ is “large”).

In fact, Birch and Swinnerton-Dyer did numerical computation for $\{y^2 = x^3 - n^2 x\}$ in 1958. They computed

$$\prod_{p<X} \frac{|\widetilde{E}(\mathbf{F}_p)|}{p} \overset{\text{“looks like”}}{\sim} c(\log X)^r$$

where $r = r_{\mathrm{alg}}(E)$. This leads to:

Conjecture 3.1 (BSD: rank part)**.** *$r_{\mathrm{an}}(E) = r_{\mathrm{alg}}(E)$.*

However, all these are heuristics.

Question. How to compute $r_{\mathrm{an}}(E)$? $L^{(r)}(E,1)$?

3.2. **Computing the leading term $L^{(r)}(E,1)$.** Recall:

$$\Lambda(f,s) = \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)(t^s + \epsilon t^{k-s})\frac{dt}{t}$$

where $W_N f = \epsilon f$ for the Atkin–Lehner involution. Let us apply this to $f = f_E \in S_2(N)$.

3.2.1. *Rank zero.* For $r = 0$ (hence $\epsilon = +1$),

$$
\begin{aligned}
\Lambda(E,1) &= 2\int_1^\infty f\left(\frac{it}{\sqrt{N}}\right) t \cdot \frac{dt}{t} \\
&= 2\int_1^\infty \sum_{n\geq 1} a_n e^{-\frac{2\pi n t}{\sqrt{N}}}\, dt \\
&= 2\sum_{n\geq 1} a_n \int_1^\infty e^{-\frac{2\pi n t}{\sqrt{N}}}\, dt \\
&= 2\sum_{n\geq 1} \frac{\sqrt{N}}{2\pi} \cdot \frac{a_n}{n} \cdot e^{-\frac{2\pi n}{\sqrt{N}}}.
\end{aligned}
$$

Then the incomplete L-function is

$$\begin{aligned} L(f,1) &= \frac{2\pi}{\sqrt{N}}\Lambda(f,1) \\ &= 2\sum_{n\geq 1}\frac{a_n}{n}e^{-\frac{2\pi n}{\sqrt{N}}}. \end{aligned}$$

This is a formula we can use to compute whether an elliptic curve has analytic rank 0.

Remark. $L(f,1)$ can be viewed as a "weighted sum" of the divergent series

$$L(f,1)\text{``}{=}\text{''}\sum\frac{a_n}{n}.$$

3.2.2. *Rank one.* For $r=1$ (hence $\epsilon=-1$),

$$\begin{aligned} \Lambda'(f,1) &= 2\int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)\log t\,dt \\ &= 2\int_1^\infty \sum_{n\geq 1} a_n e^{-\frac{2\pi n t}{\sqrt{N}}}\log t\,dt \\ &= 2\sum_{n\geq 1} a_n\int_1^\infty e^{-\frac{2\pi n t}{\sqrt{N}}}\log t\,dt \\ &= 2\sum_{n\geq 1}\frac{\sqrt{N}}{2\pi}\cdot\frac{a_n}{n}\int_1^\infty e^{-\frac{2\pi n t}{\sqrt{N}}}\frac{dt}{t}, \end{aligned}$$

where we have used integration by parts to obtain the exponential integral

$$\int_1^\infty e^{-ct}\log t\,dt = \frac{1}{c}\int_1^\infty e^{-ct}\frac{dt}{t}.$$

Then the incomplete L-function has derivative

$$\begin{aligned} L'(f,1) &= \frac{2\pi}{\sqrt{N}}\Lambda'(f,1) \\ &= 2\sum_{n\geq 1}\frac{a_n}{n}\int_1^\infty e^{-\frac{2\pi n t}{\sqrt{N}}}\frac{dt}{t}. \end{aligned}$$

3.2.3. *General rank.* More generally, for any $r\geq 1$, we define

$$E_r(x) := \frac{1}{(r-1)!}\int_1^\infty e^{-xt}(\log r)^{r-1}\frac{dt}{t}.$$

Then the leading term is

$$L^{(r)}(f,1) = 2r!\sum_{n\geq 1}\frac{a_n}{n}E_r\left(\frac{2\pi n}{\sqrt{N}}\right).$$

This shows that the analytic rank is easy to compute in practice.

Remark. ϵ is easy to compute. Breaking the integral into $\int_A^\infty + \int_{A^{-1}}^\infty$ gives

$$L(f,1) = \sum_{n\geq 1}\frac{a_n}{n}\left(e^{-\frac{2\pi n}{A\sqrt{N}}} + \epsilon e^{-\frac{2\pi n A}{\sqrt{N}}}\right).$$

Now plugging in different values of A (e.g. $A = 1$ and $A = 1.01$) gives the only choice for ϵ.

3.3. **Rank zero: What is $L(E, 1)$?**

Example 3.2. Consider $E : y^2 = x^3 - x$, which has conductor $N = 32$ (and complex multiplication by $\mathbf{Q}(i)$). The corresponding modular form is

$$\begin{aligned} f &= q \prod_{n \geq 1} (1 - q^{4n})^2 (1 - q^{8n})^2 \\ &= q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} + \cdots . \end{aligned}$$

In fact, $a_p \neq 0 \iff p \equiv 1 \pmod 4$. Then

$$L(E, 1) = 2 \sum \frac{a_n}{n} e^{-\frac{2\pi n}{\sqrt{32}}} = 0.65551438837 \cdots .$$

Example 3.3. Consider $E : y^2 = x^3 + 1$, which has conductor $N = 36$ (and complex multiplication by $\mathbf{Q}(\sqrt{-3})$). The corresponding modular form is

$$\begin{aligned} f &= q \prod_{n \geq 1} (1 - q^{6n})^4 \\ &= q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} + \cdots . \end{aligned}$$

In fact, $a_p \neq 0 \iff p \equiv 1 \pmod 3$. Then

$$L(E, 1) = 2 \sum \frac{a_n}{n} e^{-\frac{\pi n}{3}} = 0.701091052663 \cdots .$$

Question. What are these transcendental numbers?

Answer. There are natural transcendental numbers associated to elliptic curves: elliptic integrals, or periods of elliptic curves in modern language.

Definition 3.4. Suppose E has minimal Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Define the *Néron differential*

$$\omega_E := \frac{dx}{2y + a_1 x + a_3} \in H^0(E, \Omega^1_E)$$

and the *Néron period* is

$$\Omega(E) := \int_{E(\mathbf{R})} \omega_E \in \mathbf{R}.$$

Example 3.5. For $E : y^2 = x^3 - x$, this equation is already minimal and the Néron differential is

$$\omega_E = \frac{dx}{2y} = \frac{dx}{2\sqrt{x^3 - x}}.$$

The real locus $E(\mathbf{R})$ consists of two circles (including the point at infinity), which correspond to two homologous circles in the complex torus $E(\mathbf{C})$. Then

$$\Omega(E) = \int_{E(\mathbf{R})} \omega_E = 2 \int_{\text{circle}} \frac{dx}{2\sqrt{x^3 - x}} = 4 \int_1^\infty \frac{dx}{2\sqrt{x^3 - x}} = 5.24411510858 \cdots .$$

Observe the miraculous coincidence:

$$\frac{L(E,1)}{\Omega(E)} \approx \frac{1}{8} \in \mathbf{Q}!$$

Similarly,

Example 3.6. For $E : y^2 = x^3 + 1$, the Néron differential is $\omega_E = \frac{dx}{2\sqrt{x^3+1}}$. The real locus $E(\mathbf{R})$ is only one circle, which corresponds to a circle in $E(\mathbf{C})$. Then

$$\Omega(E) = \int_{-1}^{\infty} \frac{dx}{\sqrt{x^3+1}} = 4.20654631\cdots$$

and

$$\frac{L(E,1)}{\Omega(E)} \approx \frac{1}{6} \in \mathbf{Q}.$$

The upshot is the following

Conjecture 3.7. *For every elliptic curve $E/\mathbf{Q}$,*

$$\frac{L(E,1)}{\Omega(E)} \in \mathbf{Q}.$$

We will prove this next time and explain what happens for $L^{(r)}(E,1)$.

4. Lecture 4 (September 19, 2018)

4.1. **Rationality of $\frac{L(E,1)}{\Omega(E)}$.** To prove $\frac{L(E,1)}{\Omega(E)} \in \mathbf{Q}$, we need to relate $L(E,1)$ to a "period". In general, a period of an algebraic variety $X/\mathbf{Q}$ is a quantity of the form

$$\text{period} = \int_{i\text{-cycle}} \text{closed } i\text{-form},$$

where an i-cycle lives in $H_i(X(\mathbf{C}), \mathbf{Q})$ and a closed i-form lives in $H^i_{\mathrm{dR}}(X/\mathbf{Q})$.

Example 4.1. For $X = \mathbf{G}_m$ and $\omega = \frac{dt}{t}$,

$$\int_{S^1} \frac{dt}{t} = 2\pi i.$$

Note that $2\pi i$ is the period of the exponential function (inverse of log).

Example 4.2. For an elliptic curve,

$$\int_{E(\mathbf{R})} \omega_E = \text{period of the Weierstrass } \wp\text{-function (inverse of elliptic integral)}.$$

Our goal is to show that $L(E,1) = L(f_E,1)$ is related to periods of the (compactified) modular curve $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$. Recall the Mellin transform interpretation of $L(f,s)$:

$$L(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} f(it)t^s \,\frac{dt}{t}.$$

Applying this to $s = 1$ (without worrying about convergence),

$$L(f,1) = 2\pi \int_0^{\infty} f(it)\,dt \overset{\tau=it}{=} -2\pi i \int_0^{i\infty} f(\tau)\,d\tau.$$

Then $\omega_f = 2\pi i f(\tau)\,d\tau$ can be interpreted as a 1-form on $X_0(N)$, and

$$L(f,1) = -\int_0^{i\infty} \omega_f$$

is an integral along the path $0 \to i\infty$ on $X_0(N)$.

Problem: $0 \to i\infty$ is not a closed path. But it is not too far from being one, as shown in the following

Theorem 4.3 (Manin–Drinfeld)**.** *Take any cusps $\alpha, \beta \in X_0(N)$. Then $\alpha \to \beta$ belongs to $H_1(X_0(N)(\mathbf{C}), \mathbf{Q})$, i.e., there exist closed loops $\gamma_i \in H_1(X_0(N)(\mathbf{C}), \mathbf{Z})$ and $c_i \in \mathbf{Q}$ such that*

$$\int_\alpha^\beta \omega_f = \sum_i c_i \int_{\gamma_i} \omega_f$$

for all $f \in S_2(N)$.

Remark. In other words, a rational multiple of $L(f,1)$ is indeed a period.

Remark. This theorem implies (in fact, is equivalent to saying) $\alpha - \beta$ gives a torsion point on $J_0(N) = \mathrm{Jac}(X_0(N))$.

Idea of proof. Use Hecke operators T_p for $p \nmid N$:

$$\begin{aligned} T_p \int_0^{i\infty} &= \int_0^{i\infty} + \sum_{k=0}^{p-1} \int_{\frac{k}{p}}^{i\infty} \\ &= (1+p) \int_0^{i\infty} - \sum_{k=0}^{p-1} \int_{\frac{k}{p}}^{0}. \end{aligned}$$

Note that for $p \nmid N$, $\frac{k}{p} \to 0$ is a closed loop on $X_0(N)$. Then

$$(1 + p - T_p) \int_0^{i\infty} = \sum \int_{\gamma_i}$$

with $1 + p - T_p$ acting as an integer (the number of points mod p). It remains to choose p such that this is nonzero, which is possible because a modular form with T_p acting by $1+p$ for all p must be an Eisenstein series. □

Now we are ready to prove the

Theorem 4.4 (Birch)**.** $\dfrac{L(E,1)}{\Omega(E)} \in \mathbf{Q}$.

Proof. The modularity theorem gives a nontrivial map $\varphi : X_0(N) \to E$ (defined over $\mathbf{Q}$) such that $\varphi^*(\omega_E) = c \cdot 2\pi i f(\tau)\,d\tau$ for some $c \in \mathbf{Q}^\times$. Then

$$L(f,1) \underset{\mathbf{Q}^\times}{\sim} \text{period of } 2\pi i f(\tau)\,d\tau,$$

$$\Omega(E) = \text{period of } \omega_E.$$

Both are real periods, so we conclude $L(f,1) \underset{\mathbf{Q}^\times}{\sim} \Omega(E)$. □

Conjecture 4.5. $c = 1$.

4.2. **What is $\frac{L(E,1)}{\Omega(E)}$?** More generally, what is $\frac{L^{(r)}(E,1)}{\Omega(E)}$ for $r = r_{\mathrm{an}}(E)$?

Example 4.6. Consider $E : y^2 = x^3 - 25x$, with $N = 800 = 32 \cdot 25$, $r = 1$ and $E(\mathbf{Q}) \cong \mathbf{Z} \times \mathbf{Z}/2 \times \mathbf{Z}/2$ generated by $(-4,6), (0,0), (5,0)$ respectively. The corresponding modular form is

$$f = q - 3q^9 - 6q^{13} - 2q^{17} + \cdots .$$

We can use the formula from last time to compute that

$$L'(f,1) = 2\sum \frac{a_n}{n} E_1\left(\frac{2\pi n}{\sqrt{800}}\right) = 2.22737037954\cdots .$$

However,

$$\Omega(E) = 2\int_5^\infty \frac{dx}{\sqrt{x^3 - 25x}} = 2.34523957\cdots$$

and

$$\frac{L'(f,1)}{\Omega(E)} = 0.949741 \cdots \notin \mathbf{Q}!$$

Of course, Theorem 4.4 is trivially true, since $\frac{L(f,1)}{\Omega(E)} = 0$.

Idea: Use *arithmetic complexity* of the rational points of infinite order.

Definition 4.7. For $x = \frac{a}{b} \in \mathbf{Q}^\times$ with $(a,b) = 1$, define its *height* by

$$h(x) := \log \max\{|a|, |b|\}.$$

Definition 4.8. For $P \in E(\mathbf{Q})$, define its *naive height* by

$$h(P) := \begin{cases} h(x(P)) & \text{if } x(P) \neq 0, \\ -\infty & \text{if } x(P) = 0. \end{cases}$$

Problem: This depends on the Weierstrass equation of E.

Definition 4.9 (Tate)**.** Define the *canonical height* (or *Néron–Tate height*) by

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h([2^n]P)}{4^n} \in \mathbf{R}_{\geq 0}.$$

Example 4.10. Let us return to the previous example $E : y^2 = x^3 - 25x$. Then

$P = (-4,6)$	$h(P) = 1.856786\cdots$
$2P = (\frac{1681}{144}, \cdots)$	$\frac{h(2P)}{4} = 1.8778407\cdots$
$4P = (\frac{11183412793921}{223416132416}, \cdots)$	$\frac{h(4P)}{16} = 1.89946579\cdots$

In fact, $\hat{h}(P) = 1.89948217253\cdots$. Observe that

$$\frac{L'(f,1)}{\Omega(E)\hat{h}(P)} = \frac{1}{2} \in \mathbf{Q}!$$

Remark. $\hat{h}(P)$ does not depend on the Weierstrass equation and is uniquely characterized by the following:

(1) $\hat{h} : E(\mathbf{Q}) \to \mathbf{R}_{\geq 0}$.
(2) $\hat{h}(2P) = 4\hat{h}(P)$.
(3) $\hat{h}(P) - h(P)$ is bounded for $P \in E(\mathbf{Q})$.

Definition 4.11. Let $r \geq 2$. Define the *Néron–Tate height pairing* $\langle -, - \rangle : E(\mathbf{Q}) \times E(\mathbf{Q}) \to \mathbf{R}_{\geq 0}$ by

$$\langle P, Q \rangle := \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right).$$

In particular, $\langle P, P \rangle = \hat{h}(P)$.

Definition 4.12. The *regulator* of E is defined to be

$$R(E) := \det\left(\langle P_i, P_j \rangle_{r \times r}\right),$$

where $\{P_i\}_{1 \leq i \leq r}$ are generators of $E(\mathbf{Q})/E(\mathbf{Q})_{\text{tors}}$.

Remark.

(1) $\hat{h}(P) = 0 \iff P \in E(\mathbf{Q})_{\text{tors}}$, so $\langle -, - \rangle$ is perfect on $E(\mathbf{Q})/E(\mathbf{Q})_{\text{tors}}$ and $R(E) \neq 0$.
(2) When $r = 0$, $R(E) = 1$.
(3) When $r = 1$, $R(E) = \hat{h}(P)$.

Conjecture 4.13. $\dfrac{L^{(r)}(E,1)}{\Omega(E)R(E)} \in \mathbf{Q}^\times$.

This is the first step towards the full BSD conjecture

Remark.

- When $r = 0$, this is true (proved).
- When $r = 1$, this is true by the $r = 0$ case and Gross–Zagier formula.
- When $r \geq 2$, no example is known! But there is enormous numerical evidence.

4.3. **Full BSD conjecture.** Our goal is to find a formula for $\dfrac{L^{(r)}(E,1)}{\Omega(E)R(E)}$. Recall the three examples we did earlier:

E	N	r	$\frac{L^{(r)}(E,1)}{\Omega(E)R(E)}$
$y^2 = x^3 - x$	32	0	$\frac{1}{8}$
$y^2 = x^3 + 1$	36	0	$\frac{1}{6}$
$y^2 = x^3 - 25x$	800	1	$\frac{1}{2}$

Idea: Instead of looking at $\int_{E(\mathbf{R})} \omega_E$ only, we should look at $\int_{E(\mathbf{Q}_p)} |\omega_E|$.

Fact.

$$\int_{E(\mathbf{Q}_p)} |\omega_E| = [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)] \cdot \frac{|\widetilde{E}(\mathbf{F}_p)|}{p},$$

where $E^0(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p) : P \mod p \in \widetilde{E}(\mathbf{F}_p)\}$. (Recall that $\frac{|\widetilde{E}(\mathbf{F}_p)|}{p} = L_p(E,1)^{-1}$.)

Definition 4.14. The *local Tamagawa number* is defined to be

$$c_p(E) := [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)].$$

Remark.

- $c_p(E) = \Phi(\mathbf{F}_p)$ where $\Phi_{\mathbf{F}_p}$ is the component group scheme of the Néron model of E at p.
- $c_p = 1$ if $p \nmid N$.

This is easily computed using Tate's algorithm.

Now we can complete the table above:

E	N	r	$\frac{L^{(r)}(E,1)}{\Omega(E)R(E)}$	$\prod c_p$	$\frac{L^{(r)}(E,1)}{\Omega(E)\cdot\prod_p c_p\cdot R(E)}$	$E(\mathbf{Q})_{\text{tors}}$
$y^2 = x^3 - x$	32	0	$\frac{1}{8}$	$c_2 = 2$	$\frac{1}{16}$	$\mathbf{Z}/2 \times \mathbf{Z}/2$
$y^2 = x^3 + 1$	36	0	$\frac{1}{6}$	$c_2 \cdot c_3 = 3 \cdot 2 = 6$	$\frac{1}{36}$	$\mathbf{Z}/2 \times \mathbf{Z}/3$
$y^2 = x^3 - 25x$	800	1	$\frac{1}{2}$	$c_2 \cdot c_5 = 2 \cdot 4 = 8$	$\frac{1}{16}$	$\mathbf{Z}/2 \times \mathbf{Z}/2$

Next time, we will complete the full formula using the data we see.

5. Lecture 5 (September 24, 2018)

5.1. Full BSD conjecture.

Last time we saw from a few examples with $r = 0, 1$ that

$$\frac{L^{(r)}(E,1)}{\Omega(E) \cdot \prod_p c_p(E) \cdot R(E)} \overset{?}{=} \frac{1}{|E(\mathbf{Q})_{\text{tor}}|^2}.$$

Let's rewrite this as

$$\frac{L^{(r)}(E,1)}{r!} \overset{?}{=} \underbrace{\Omega(E) \cdot \prod_p c_p(E)}_{\text{period}} \cdot \underbrace{\frac{R(E)}{|E(\mathbf{Q})_{\text{tor}}|^2}}_{\text{regulator}}.$$

Remark. $\frac{R(E)}{|E(\mathbf{Q})_{\text{tor}}|^2}$ is more canonical: for any $\Lambda \subseteq E(\mathbf{Q})$ of rank r, $\frac{R(\Lambda)}{[E(\mathbf{Q}):\Lambda]^2}$ is independent of the choice of Λ.

Notice the similarity with the class number formula: for any number field $K/\mathbf{Q}$,

$$\operatorname{res}_{s=1} \zeta_K(s) = \underbrace{\frac{2^{r_1}(2\pi)^{r_2}}{|d_K|^{1/2}}}_{\text{period}} \cdot \underbrace{\frac{R(K)}{|\mathcal{O}_{K,\text{tor}}^{\times}|}}_{\text{regulator}} \cdot \underbrace{h(K)}_{\text{class number}}.$$

Missing in the formula of BSD above is an analogue of $h(K) = |\text{Cl}(K)|$; this will be provided by the size of the Tate–Shafarevich group $\text{Ш}(E)$.

Conjecture 5.1 (Full BSD conjecture)**.** *Let $E/\mathbf{Q}$ be an elliptic curve. Then*

(1) *(rank part) $r_{\text{alg}}(E) = r_{\text{an}}(E)$.*

(2) *(formula part)*

$$\frac{L^{(r)}(E,1)}{r!} = \Omega(E) \cdot \prod_p c_p(E) \cdot \frac{R(E)}{|E(\mathbf{Q})_{\text{tor}}|^2} \cdot |\text{Ш}(E)|.$$

This can be seen as a vast generalization of the class formula formula.

Remark. (1) is known when $r_{\text{an}}(E) \leq 1$ (Gross–Zagier, Kolyvagin). (2) is known for many (but not all) $E/\mathbf{Q}$ with $r_{\text{an}}(E) \leq 1$; the main ingredient is Skinner–Urban's work on the Iwasawa main conjecture and Kato's Euler systems.

5.2. **Tate–Shafarevich group.**

Definition 5.2. The Tate–Shafarevich group of E is defined to be

$$Ш(E) := \ker \left(H^1(\mathbf{Q}, E) \to \prod_v H^1(\mathbf{Q}_v, E) \right).$$

In other words, an element of $Ш(E)$ is represented by a genus 1 curve $C/\mathbf{Q}$ such that $\mathrm{Jac}(C) \simeq E$ and $C(\mathbf{Q}_v) \neq \emptyset$ for all places v of $\mathbf{Q}$. $Ш(E)$ measures the failure of local-global principle for $\mathbf{Q}$-points (for C).

Example 5.3 (Lind, 1940)**.** The curve $C : 2y^2 = x^4 - 17$ has points over all $\mathbf{Q}_p$ and $\mathbf{R}$, but has no $\mathbf{Q}$-points. This corresponds to the elliptic curve

$$E = \mathrm{Jac}(C) : y^2 = x^3 + 17x$$

which has $r = 0$ and $Ш(E) \simeq (\mathbf{Z}/2)^2$.

To check the BSD formula, we compute that

$$\begin{aligned} L(E,1) &= 3.6523\cdots, \\ \Omega(E) &= 1.82618\cdots, \\ \textstyle\prod_p c_p(E) &= c_2 \cdot c_{17} = 1 \cdot 2 = 2, \\ E(\mathbf{Q})_{\mathrm{tor}} &= \mathbf{Z}/2\mathbf{Z}, \end{aligned}$$

and hence

$$\frac{L(E,1)}{\Omega(E)\prod_p c_p} = \frac{2}{1 \cdot 2} = 1 \quad \text{and} \quad \frac{|Ш(E)|}{|E(\mathbf{Q})_{\mathrm{tor}}|^2} = \frac{4}{4} = 1.$$

Example 5.4 (Selmer, 1951)**.** The curve $C : 3x^3 + 4y^3 + 5z^3 = 0$ has points over all $\mathbf{Q}_p$ and $\mathbf{R}$, but no $\mathbf{Q}$-points. This corresponds to the elliptic curve

$$E = \mathrm{Jac}(C) : x^3 + y^3 + 60z^3 = 0,$$

(with Weierstrass equation $y^2 = x^3 - 24300$), which has $Ш(E) = (\mathbf{Z}/3)^2$.

Remark. In general, there is no algorithm to compute $Ш(E)$. The full BSD formula helps to compute $|Ш(E)|$.

Remark. To see why $|Ш(E)|$ is an analogue of the class number, note that the class group $\mathrm{Cl}(K)$ can also be described in terms of Galois cohomology. Setting $S = \mathrm{Res}_{\mathcal{O}_K/\mathbf{Z}}\, \mathbf{G}_m$, we have

$$\mathrm{Cl}(K) \cong \ker \left(H^1(\mathbf{Q}, S) \to \prod_v H^1(\mathbf{Q}_v, S) \right)$$

measuring the failure of any ideal that is locally principal but not globally principal. We know $\mathrm{Cl}(K)$ is finite (using geometry of numbers), but we don't know the finiteness of $Ш(E)$.

Conjecture 5.5. *$Ш(E)$ is finite.*

Remark.

1. This conjecture is true if $r_{\mathrm{an}}(E) \leq 1$ (Gross–Zagier, Kolyvagin).
2. No example is known where $r_{\mathrm{an}}(E) \geq 2$!

Remark (Cassels–Tate pairing). There exists an alternating pairing $Ш(E) \times Ш(E) \to \mathbf{Q}/\mathbf{Z}$ whose kernal is the divisible part of $Ш(E)$, so

$$Ш(E) \text{ is finite} \implies Ш(E) \simeq G \times G \implies |Ш(E)| \text{ is a square!}$$

Remark. Delaunay (2001) developed Cohen–Lenstra heuristics for $Ш(E)$ as "random" finite abelian groups with nondegenerate alternating pairing $(H, (-,-))$ (with frequency $\frac{1}{\mathrm{Aut}(H,(-,-))}$). It predicts that the probability of $p \mid |Ш(E)|$ is given by:

- $r = 0$:
$$f_0(p) = 1 - \prod_{k \geq 1} \left(1 - \frac{1}{p^{2k-1}}\right).$$
- $r = 1$:
$$f_1(p) = 1 - \prod_{k \geq 1} \left(1 - \frac{1}{p^{2k}}\right).$$

For example,

p	$f_0(p)$	$f_1(p)$
2	0.58	0.31
3	0.36	0.12
5	0.21	0.04

None of this is support by actual data. However, we don't even know if given p there exists $E/\mathbf{Q}$ such that $p \mid |Ш(E)|$ (not to mention positive probability!).

Remark. It is known that for $p = 2, 3, 5, 7, 13$, $Ш(E)[p^\infty]$ can be arbitrarily large. The proof uses the fact that $X_0(p)$ has genus 0, so $p = 11$ is not allowed here.

5.3. **Tamagawa numbers.** There is a reformulation of the BSD formula, due to Bloch, in terms of Tamagawa numbers, which is similar to the case of linear algebraic groups.

Definition 5.6. Let G be a semisimple algebraic group over $\mathbf{Q}$. Take a top differential ω (defined over $\mathbf{Q}$) of G. Then $|\omega|_v$ (volume form) gives a Haar measure μ_v on $G(\mathbf{Q}_v)$. Then the *Tamagawa measure* is $\mu = \prod_v \mu_v$ on $G(\mathbf{A})$, and the *Tamagawa number* of G is

$$\tau(G) := \mu(G(\mathbf{Q}) \backslash G(\mathbf{A})).$$

Theorem 5.7 (Weil's conjecture)**.** *If G is simply-connected, then $\tau(G) = 1$.*

This is proved by Langlands, Lai, Kottwitz, etc.

Example 5.8. Let $G = \mathrm{SL}_{2/\mathbf{Q}}$. Then

$$\tau(G) = \mu_\infty(\mathrm{SL}_2(\mathbf{Z}) \backslash \mathrm{SL}_2(\mathbf{R})) \cdot \prod_p \mu_p(\mathrm{SL}_2(\mathbf{Z}_p)).$$

But

$$\mu_p(\mathrm{SL}_2(\mathbf{Z}_p)) = \frac{|\mathrm{SL}_2(\mathbf{F}_p)|}{p^3} = 1 - p^{-2} = \zeta_p(2)^{-1},$$

so

$$\tau(G) = 1 \implies \mu_\infty(\mathrm{SL}_2(\mathbf{Z}) \backslash \mathrm{SL}_2(\mathbf{R})) = \zeta(2) = \frac{\pi^2}{6}$$
$$\implies \mathrm{Vol}(\mathrm{SL}_2(\mathbf{Z}) \backslash \mathcal{H}) = \frac{\pi}{3}.$$

Example 5.9. Let $G = \mathrm{SL}_{n/\mathbf{Q}}$. Then

$$\begin{aligned}\tau(G) = 1 &\iff \mu_\infty(\mathrm{SL}_n(\mathbf{Z})\backslash\mathrm{SL}_n(\mathbf{R})) = \zeta(2)\cdots\zeta(n)\\ &\iff \mathrm{Vol}(\mathrm{SL}_n(\mathbf{Z})\backslash\mathcal{H}^n) = n2^{n-1}\cdot\frac{\zeta(2)\cdots\zeta(n)}{\mathrm{Vol}(S^1)\cdots\mathrm{Vol}(S^{n-1})}.\end{aligned}$$

We can do this for E too (next time).

6. Lecture 6 (September 26, 2018)

6.1. **Bloch's reformulation of BSD formula.** Last time we saw that for $G = \mathrm{SL}_n$, the Tamagawa number is $\tau(G) = 1$; this special case is due to Minkowski and Siegel using geometry of numbers, before the formulation of Weil's conjecture for semisimple algebraic groups. But for more general algebraic groups, $\tau(G)$ may not be well-defined.

Example 6.1. Let $G = \mathbf{G}_m$. Then

$$\mu_p(G(\mathbf{Z}_p)) = \frac{|\mathbf{G}_m(\mathbf{F}_p)|}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}.$$

Notice $\prod_p(1-\frac{1}{p})$ doesn't converge! To fix this, the idea is to regularize this product by changing the local measure to be

$$\left(1-\frac{1}{p}\right)^{-1}\mu_p = \zeta_p(1)\mu_p,$$

and take

$$\tau(G) = \frac{\mu(G(\mathbf{Q})\backslash G(\mathbf{A}))}{\zeta^*(1)},$$

where $\zeta^*(1)$ is the leading coefficient of $\zeta(s)$ at $s = 1$. Then $\tau(\mathbf{G}_m) = 1$.

Fro a general linear algebraic group, there exists an L-function $L(G, s)$ such that for all $p \notin S$ (a finite set of bad primes),

$$\frac{|G(\mathbf{F}_p)|}{p^{\dim G}} = L_p(G, 1)^{-1}.$$

Example 6.2. Let $G = \mathbf{G}_m$. Then $L(G, s) = \zeta(s)$.

Example 6.3. Let $G = \mathrm{GL}_n$. Then $L(G, s) = \zeta(s)\zeta(s+1)\cdots\zeta(s+n-1)$.

Definition 6.4. For any algebraic group G, define the modified Tamagawa measure

$$\mu^* := \prod_{v\notin S} L_v(G, 1)\mu_v \cdot \prod_{v\in S}\mu_v$$

and the Tamagawa number

$$\tau(G) := \frac{\mu^*(G(\mathbf{Q})\backslash G(\mathbf{A}))}{L_S^*(G, 1)}.$$

Then we have the following generalization of Weil's conjecture.

Theorem 6.5 (T. Ono, Oesterlé, Kottwitz). *For any connected linear algebraic group $G/\mathbf{Q}$,*

$$\tau(G) = \frac{|\mathrm{Pic}(G)_{\mathrm{tor}}|}{|Ш(G)|}.$$

Here $\text{Ш}(G) = \ker\left(H^1(\mathbf{Q}, G) \to \prod_v H^1(\mathbf{Q}_v, G)\right)$ is the Tate–Shafarevich *set.*

Remark. If G is linear, $\text{Ш}(G)$ is known to be finite (Borel–Serre, 1966).

Remark. Suppose G is simply connected and semisimple. Then indeed $|\text{Pic}(G)_{\text{tor}}| = 1$. The verification that $|\text{Ш}(G)| = 1$ is a hard theorem due to Harder (1965), Kneser (1966), and Chernousov (1989) for E_8, which completed Kottwitz's proof of the Tamagawa number conjecture.

Bloch's idea is to look at elliptic curves. Suppose $r_{\text{alg}}(E) = r$. Take a generator $P_i \in E(\mathbf{Q})$. Using the fact that $E \simeq \widehat{E} = \text{Ext}^1(E, \mathbf{G}_m)$, P_i gives rise to an extension of groups

$$0 \to \mathbf{G}_m \to X_{P_i} \to E \to 0.$$

If $\{P_i\}$ is a basis of $E(\mathbf{Q})$, then

$$0 \to \mathbf{G}_m^r \to X \to E \to 0.$$

Theorem 6.6 (Bloch)**.** *The Tamagawa number conjecture for X is equivalent to the BSD formula for E.*

In fact, $\text{Ш}(X) = \text{Ш}(E)$, and Bloch's theorem gives an interpretation of the regulator $R(E)$ also as a volume.

6.2. **p-Selmer groups.** Selmer groups are more accessible than the Mordell–Weil group $E(\mathbf{Q})$ and the Tate–Shafarevich group $\text{Ш}(E)$, and will be used to prove the BSD conjecture.

Start with

$$0 \to E[p] \to E \xrightarrow{p} E \to 0.$$

Taking $H^*(\mathbf{Q}, -)$, we get a long exact sequence

$$0 \to E(\mathbf{Q})[p] \to E(\mathbf{Q}) \xrightarrow{p} E(\mathbf{Q}) \to H^1(\mathbf{Q}, E[p]) \to H^1(\mathbf{Q}, E) \xrightarrow{p} H^1(\mathbf{Q}, E) \to \cdots$$

and hence

$$0 \to \frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \to H^1(\mathbf{Q}, E[p]) \to H^1(\mathbf{Q}, E)[p] \to 0.$$

We want to understand $E(\mathbf{Q})$, but $H^1(\mathbf{Q}, E[p])$ is an infinite-dimensional $\mathbf{F}_p$-space. Instead we look at the local picture:

$$\begin{tikzcd}
0 \arrow[r] & \frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \arrow[r, "\delta"] \arrow[d] & H^1(\mathbf{Q}, E[p]) \arrow[r] \arrow[d, "\text{loc}_v"] & H^1(\mathbf{Q}, E)[p] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v \frac{E(\mathbf{Q}_v)}{pE(\mathbf{Q}_v)} \arrow[r, "\delta_v"] & \prod_v H^1(\mathbf{Q}_v, E[p]) \arrow[r] & \prod_v H^1(\mathbf{Q}_v, E)[p] \arrow[r] & 0
\end{tikzcd}$$

Here $H^1(\mathbf{Q}_v, E[p])$ is finite for each v!

Definition 6.7. The p-Selmer group is

$$\text{Sel}_p(E) := \{x \in H^1(\mathbf{Q}, E[p]) : \text{loc}_v(x) \in \text{im}(\delta_v) \text{ for all } v\}.$$

In other words, we have a pullback diagram

$$\begin{tikzcd}
\mathrm{Sel}_p(E) \arrow[r] \arrow[d] & H^1(\mathbf{Q}, E[p]) \arrow[d] \\
\prod_v \frac{E(\mathbf{Q}_v)}{pE(\mathbf{Q}_v)} \arrow[r] & \prod_v H^1(\mathbf{Q}_v, E[p])
\end{tikzcd}$$

which induces a natural map $\frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \to \mathrm{Sel}_p(E)$.

By construction, we have a "p-descent exact sequence"

$$0 \to \frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \to \mathrm{Sel}_p(E) \to Ш(E)[p] \to 0.$$

$\mathrm{Sel}_p(E)$ is described locally, and hence more accessible than $E(\mathbf{Q})$ and $Ш(E)$ which contain global information.

Theorem 6.8. $\mathrm{Sel}_p(E)$ *is finite.*

Idea of proof. $\mathrm{Sel}_p(E) \subseteq H^1(\mathbf{Q}, E[p])$ can be thought of as a subspace "cut out" by local conditions $\mathrm{im}(\delta_v) \subseteq H^1(\mathbf{Q}_v, E[p])$ for all v. View a class $x \in H^1(\mathbf{Q}, E[p])$ as a number field $L/\mathbf{Q}$. Then the local condition at $v \notin S$ (finite set of bad primes) imply that L is unramified at v (control on the ramification). The theorem follows because there are only finitely many number fields $L/\mathbf{Q}$ with exponent p and unramified outside S! □

Since $\dim_{\mathbf{F}_p} E(\mathbf{Q})/pE(\mathbf{Q}) = r_{\mathrm{alg}}(E) + \dim_{\mathbf{F}_p} E(\mathbf{Q})[p]$, we obtain the

Corollary 6.9 (p-descent)**.**

$$\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E) = r_{\mathrm{alg}}(E) + \dim_{\mathbf{F}_p} E(\mathbf{Q})[p] + \dim_{\mathbf{F}_p} Ш(E)[p].$$

In particular, $\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E) \geq r_{\mathrm{alg}}(E) + \dim_{\mathbf{F}_p} E(\mathbf{Q})[p]$.

Remark. $\mathrm{Sel}_p(E)$ is most computable when $p = 2$.

Example 6.10 (Heath-Brown, 1994)**.** For the family $\{y^2 = x^3 - n^2x\}$, Heath-Brown proved that the probability that $\dim \mathrm{Sel}_2(E) = d + \dim E(\mathbf{Q})[2] = d + 2$ is given by

$$P(d) := \prod_{k\geq 0} \left(1 + \frac{1}{2^k}\right)^{-1} \prod_{k=1}^{d} \frac{2}{2^k - 1}.$$

For example,

d	$P(d)$
0	0.2097
1	0.4194
2	0.2796
3	0.0799
4	0.0107

Remark. Poonen–Rains developed Cohen–Lenstra heuristics (for all $E/\mathbf{Q}$):

$$\mathrm{Prob}(\dim \mathrm{Sel}_p = d) \overset{?}{=} \prod_{k\geq 0}\left(1+\frac{1}{p^k}\right)^{-1}\prod_{k=1}^{d}\frac{p}{p^k-1}. \tag{6.1}$$

This has the following consequences:

(1)
$$\mathrm{Average}(|\mathrm{Sel}_p(E)|) = p+1.$$
This is proved by Bhargava–Shankar for $p = 2, 3, 5$.

(2)
$$\mathrm{Prob}(r_{\mathrm{alg}}(E)\geq 2) \leq \frac{1}{p}+\frac{1}{p^2} \implies \mathrm{Prob}(r_{\mathrm{alg}}(E)\geq 2) = 0.$$
This is consistent with Goldfeld's conjecture; in fact, (6.1) implies that 50% of E have $r_{\mathrm{alg}} = 0$ and 50% have $r_{\mathrm{alg}} = 1$.

Remark.

(1) $\mathrm{Sel}_p(E) = 0 \implies r_{\mathrm{alg}}(E) = 0$.
(2) Assume $\text{Ш}(E)[p^\infty] < \infty$. Then $\dim \mathrm{Sel}_p(E) = 1 \implies r_{\mathrm{alg}}(E) = 1$.

The implication in (2) is still open in general, but Skinner–Zhang proved many cases, and combining with Bhargava they get that at least 20% of $E/\mathbf{Q}$ have $r_{\mathrm{alg}} = 1$.

Next time we will state a reformulation of BSD in terms of Selmer groups.

7. Lecture 7 (October 8, 2018)

Last time we defined the p-Selmer group $\mathrm{Sel}_p(E) \subseteq H^1(\mathbf{Q}, E[p])$, which is a finite-dimensional $\mathbf{F}_p$-vector space inside an infinite-dimensional global H^1. It fits into a p-descent sequence

$$0 \to \frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \to \mathrm{Sel}_p(E) \to \text{Ш}(E)[p] \to 0.$$

Thus bounds on $\mathrm{Sel}_p(E)$ lead to bounds on the algebraic rank of E. However, one disadvantage with this sequence is that only the p-torsion of $\text{Ш}(E)$ is present. Taking limit over all p-powers will allow us to see the p-primary part of $\text{Ш}(E)$.

7.1. p^∞-Selmer group.

Consider the p^n-descent sequence

$$0 \to \frac{E(\mathbf{Q})}{p^nE(\mathbf{Q})} \to \mathrm{Sel}_{p^n}(E) \to \text{Ш}(E)[p^n] \to 0.$$

Taking $\varinjlim_n$ with respect to the maps $\mathbf{Z}/p^n \hookrightarrow \mathbf{Z}/p^{n+1}$ and $E[p^n] \hookrightarrow E[p^{n+1}]$, we obtain

$$0 \to E(\mathbf{Q}) \otimes \frac{\mathbf{Q}_p}{\mathbf{Z}_p} \to \mathrm{Sel}_{p^\infty}(E) \to \text{Ш}(E)[p^\infty] \to 0.$$

Definition 7.1. The p^∞-Selmer group is $\mathrm{Sel}_{p^\infty}(E) := \varinjlim_n \mathrm{Sel}_{p^n}(E)$.

Remark. We have an exact sequence

$$0 \to \frac{E(\mathbf{Q})[p^\infty]}{p^nE(\mathbf{Q})[p^\infty]} \to \mathrm{Sel}_{p^n}(E) \to \mathrm{Sel}_{p^\infty}(E)[p^n] \to 0.$$

In particular, if $E(\mathbf{Q})[p] = 0$, then $\mathrm{Sel}_{p^\infty}(E) \simeq \mathrm{Sel}_{p^\infty}(E)[p^\infty]$.

Notice that $\mathrm{Sel}_{p^\infty}(E) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^r \times$ (finite group).

Definition 7.2.

$$\begin{aligned} r_p(E) &:= \mathrm{corank}(\mathrm{Sel}_{p^\infty}(E)) \\ &= \text{number of copies of } \frac{\mathbf{Q}_p}{\mathbf{Z}_p}. \end{aligned}$$

Corollary 7.3.

(1) $r_p(E) \geq r_{\mathrm{alg}}(E)$.
(2) $r_p(E) = r_{\mathrm{alg}}(E) \iff Ш(E)[p^\infty]$ *is finite.*

In particular, BSD and the finiteness of Ш imply

Conjecture 7.4 (Bloch–Kato)**.** $r_p(E) = r_{\mathrm{an}}(E)$ *for all* p.

Remark.

(1) $r_p(E)$ is more accessible than $r_{\mathrm{alg}}(E)$ due to its local nature.
(2) By a theorem of Bloch–Kato, $\mathrm{Sel}_{p^\infty}(E)$ can be defined in terms of the p-divisible group $E[p^\infty]_{/\mathbf{Q}}$ or $V_p(E)_{/\mathbf{Q}}$. **Warning:** In general $\mathrm{Sel}_p(E)$ may not only depend $E[p]$.

Bloch–Kato generalizes this conjecture to any p-adic Galois representation V coming from geometry.

Our target theorem is

Theorem 7.5 (Gross–Zagier, Kolyvagin)**.**

(1) $r_{\mathrm{an}}(E) = 0 \implies r_p(E) = 0$.
(2) $r_{\mathrm{an}}(E) = 1 \implies r_p(E) \leq 1$ *and* $r_{\mathrm{alg}}(E) \geq 1$.

Remark. (1) and (2) imply that BSD and Bloch–Kato are true when $r_{\mathrm{an}}(E) \leq 1$, and that $Ш(E)[p^\infty]$ is finite for all p.

The goal today is to illustrate how to bound $\mathrm{Sel}_{p^\infty}(E)$ from above in the simplest case.

7.2. **Tate's local duality.** In rough terms, local duality allows us to quantify different local conditions in $H^1(\mathbf{Q}_v, E[p^\infty])$.

Definition 7.6. Let M be a finite $G_{\mathbf{Q}}$-module (e.g. $M = E[p^n]$). Define the *Cartier dual* of M

$$M^\vee(1) := \mathrm{Hom}_{\mathrm{ab.gp}}(M, \mathbf{G}_m).$$

The natural pairing $M \times M^\vee(1) \to \mathbf{G}_m$, together with the cup product, gives a pairing

$$\langle -, - \rangle_v : H^i(\mathbf{Q}_v, M) \times H^{2-i}(\mathbf{Q}_v, M^\vee(1)) \to H^2(\mathbf{Q}_v, \mathbf{G}_m) \simeq \mathbf{Q}/\mathbf{Z}.$$

Theorem 7.7 (Tate)**.**

(1) $\langle -, - \rangle_v$ *is perfect.*
(2) *(Euler characteristic)*

$$\frac{|H^1(\mathbf{Q}_v, M)|}{|H^0(\mathbf{Q}_v, M)| \cdot |H^2(\mathbf{Q}_v, M)|} = |M \otimes \mathbf{Z}_v|.$$

Apply this to $M = E[p^n]$. Then $M^\vee(1) = E[p^n]$ and $\langle -, - \rangle_v$ is precisely the Weil pairing.

Corollary 7.8. *We have an isomorphism*

$$H^0(\mathbf{Q}_v, E[p^n]) \xrightarrow{\sim} H^2(\mathbf{Q}_v, E[p^n])^\vee$$

and a perfect pairing

$$H^1(\mathbf{Q}_v, E[p^n]) \times H^1(\mathbf{Q}_v, E[p^n]) \to \mathbf{Q}/\mathbf{Z}.$$

Corollary 7.9. *If $v \neq p$, then*

$$|H^1(\mathbf{Q}_v, E[p^n])| = |H^0(\mathbf{Q}_v, E[p^n])|^2 = |E(\mathbf{Q}_v)[p^n]|^2.$$

Example 7.10. Let $n = 1$. Then

$$\dim_{\mathbf{F}_p} H^1(\mathbf{Q}_v, E[p]) = 2 \dim_{\mathbf{F}_p} E(\mathbf{Q}_v)[p].$$

Definition 7.11. Define $\mathcal{L}_v \subseteq H^1(\mathbf{Q}_v, E[p^n])$ to be the image of

$$\frac{E(\mathbf{Q}_v)}{p^n E(\mathbf{Q}_v)} \xrightarrow{\delta_v} H^1(\mathbf{Q}_v, E[p^n]).$$

Then

$$\mathrm{Sel}_{p^n}(E) = \{x \in H^1(\mathbf{Q}, E[p^n]) : \mathrm{loc}_v(x) \in \mathcal{L}_v \text{ for all } v\}$$

Theorem 7.12 (Tate)**.** *$\mathcal{L}_v$ is its own annihilator under $\langle -, - \rangle_v$.*

It would be helpful if we could characterize the local conditions $\mathcal{L}_v$ without reference to the local points $E(\mathbf{Q}_v)$. This is possible in some cases.

7.3. **Local conditions at good primes.** The goal is to pin down $\mathcal{L}_v$ in terms of only $E[p^n]$.

7.3.1. *Case $v \neq p$.*

Definition 7.13 ("Unramified" or "finite" condition)**.** Assume $|M|$ is invertible in $\mathbf{Z}_v$. Define

$$H^1_f(\mathbf{Q}_v, M) \left(= H^1_{\mathrm{ur}}(\mathbf{Q}_v, M)\right) := H^1(\mathbf{F}_v, M^{I_v}) \subseteq H^1(\mathbf{Q}_v, M),$$

i.e., the extension classes which are unramified.

The inflation-restriction sequence gives

$$0 \to H^1(\mathbf{F}_v, M^{I_v}) \to H^1(\mathbf{Q}_v, M) \to H^1(I_v, M)^{\mathrm{Frob}_v = 1} \to 0.$$

This leads to a different kind of condition.

Definition 7.14 ("Singular" condition)**.**

$$H^1_{\mathrm{sing}}(\mathbf{Q}_v, M) := H^1(I_v, M)^{\mathrm{Frob}_v = 1} \left(= \frac{H^1(\mathbf{Q}_v, M)}{H^1_f(\mathbf{Q}_v, M)} \right).$$

Proposition 7.15. *$H^1_f(\mathbf{Q}_v, M)$ and $H^1_f(\mathbf{Q}_v, M^\vee(1))$ are annihilators of each other under $\langle -, - \rangle_v$.*

Corollary 7.16. *$H^1_f(\mathbf{Q}_v, M) \times H^1_{\mathrm{sing}}(\mathbf{Q}_v, M^\vee(1)) \to \mathbf{Q}/\mathbf{Z}$ is a perfect pairing.*

Apply this to $M = E[p^n]$.

Proposition 7.17. *If $v \neq p$ and E has good reduction at v, then*

$$\mathcal{L}_v = H^1_f(\mathbf{Q}_v, E[p^n]) \left(= H^1_{\text{ét}}(\mathbf{Z}_v, \mathcal{E}[p^n])\right).$$

where $\mathcal{E}$ is the Néron model of E, so that $\mathcal{E}(\mathbf{Z}_v) = E(\mathbf{Q}_v)$.

7.3.2. *Case $v = p$.* The situation is more involved, but the last proposition suggests the following

Definition 7.18 (Flat condition)**.** Let $\mathcal{M}$ be a finite flat group scheme over $\mathbf{Z}_p$. Define

$$H^1_f(\mathbf{Q}_p, \mathcal{M}) := H^1_{\mathrm{fppf}}(\mathbf{Z}_p, \mathcal{M}) \subseteq H^1(\mathbf{Q}_p, \mathcal{M}).$$

Proposition 7.19. *$H^1_f(\mathbf{Q}_p, \mathcal{M})$ and $H^1_f(\mathbf{Q}_p, \mathcal{M}^\vee(1))$ are annihilators of each other under $\langle -, - \rangle_p$.*

Analogously with the case $v \neq p$, we have the

Proposition 7.20. *If $v = p$ and E has good reduction at p, then*

$$\mathcal{L}_v = H^1_f(\mathbf{Q}_p, \mathcal{E}[p^n]).$$

Remark. If $n = 1$ and $p > 2$, Raynaud shows that $E[p]$ has a unique extension to $\mathbf{Z}_p$, so $H^1_f(\mathbf{Q}_p, \mathcal{E}[p])$ is determined by $E[p]$.

7.4. **Kolyvagin's method.** The starting point is a simple application of global class field theory: for $s_1, s_2 \in H^1(\mathbf{Q}, E[p])$, we have $\sum_v \langle s_1, s_2 \rangle_v = 0$. This condition can be used to bound Selmer ranks.

Theorem 7.21. *Let $S = \{$bad primes for $E\} \cup \{p\}$. Assume we can construct $c(\ell) \in H^1(\mathbf{Q}, E[p])$ for all $\ell \notin S$ satisfying:*

1. *For $v \notin S \cup \{\ell\}$, $\mathrm{loc}_v(c(\ell)) \in H^1_f(\mathbf{Q}_v, E[p])$.*
2. *For $v = p$, $\mathrm{loc}_p(c(\ell)) \in H^1_f(\mathbf{Q}_p, E[p])$.*
3. *For $v \in S - \{p\}$, $\mathrm{loc}_v(c(\ell)) = 0$ (e.g. when $E(\mathbf{Q}_v)[p] = 0$).*
4. *For $v = \ell$, $H^1_f(\mathbf{Q}_\ell, E[p]) = \mathbf{F}_p$ and $0 \neq \mathrm{loc}_\ell(c(\ell)) \in H^1_{\mathrm{sing}}(\mathbf{Q}_\ell, E[p])$.*

Then $\mathrm{Sel}_p(E) = 0$.

Next time we will explain this.

8. Lecture 8 (October 10, 2018)

8.1. **Kolyvagin's method.** Last time we defined, for good primes v, the unramified conditions

$$H^1_f(\mathbf{Q}_v, E[p]) \subseteq H^1(\mathbf{Q}_v, E[p])$$

and for $v \neq p$, the singular conditions $H^1_{\mathrm{sing}}(\mathbf{Q}_v, E[p])$. We have $\langle H^1_f, H^1_f \rangle_v = 0$, and that $\langle -, - \rangle_v$ is perfect on $H^1_f \times H^1_{\mathrm{sing}}$.

Theorem 8.1. *Let $S = \{$bad primes$\} \cup \{p\}$. Assume we can construct classes $c(\ell) \in H^1(\mathbf{Q}, E[p])$ for all $\ell \notin S$ such that:*

1. *For $v \notin S \cup \{\ell\}$, $\mathrm{loc}_v(c(\ell)) \in H^1_f(\mathbf{Q}_v, E[p])$.*
2. *For $v = p$, $\mathrm{loc}_p(c(\ell)) \in H^1_f(\mathbf{Q}_p, E[p])$.*
3. *For $v \in S - \{p\}$, $\mathrm{loc}_v(c(\ell)) = 0$.*
4. *For $v = \ell$, $H^1_f(\mathbf{Q}_v, E[p]) = \mathbf{F}_p$ and $\mathrm{loc}_\ell(c(\ell)) \neq 0 \in H^1_{\mathrm{sing}}(\mathbf{Q}_v, E[p])$.*

Then $\mathrm{Sel}_p(E) = 0$.

Proof. Assume $\mathrm{Sel}_p(E) \neq 0$, and take $0 \neq s \in \mathrm{Sel}_p(E)$. By Chebotarev density, we can find $\ell \notin S$ such that $0 \neq \mathrm{loc}_\ell(s) \in H^1_f(\mathbf{Q}_\ell, E[p])$. Then

$$\langle s, c(\ell)\rangle = \sum \langle s, c(\ell)\rangle_v \overset{\text{by (1)-(3)}}{=} \langle s, c(\ell)\rangle_\ell \overset{\text{by (4)}}{\neq} 0$$

since $s \in H^1_f$ and $c(\ell) \in H^1_{\mathrm{sing}}$. This is a contradiction, since $\langle s, c(\ell)\rangle = 0$ by global class field theory. Thus $\mathrm{Sel}_p(E) = 0$. □

Remark. The proof shows that we only need $c(\ell)$ for "many" (a positive proportion of) $\ell \notin S$.

By the theorem, the key to bound Selmer groups is the construction of the classes $\{c(\ell)\}_{\ell\notin S}$ with controlled ramification. Next, we will carry out the construction via *Heegner points*.

Remark. The existence of $\{c(\ell)\}$ should be related to $r_{\mathrm{an}}(E) = 0$.

$$\begin{tikzcd}
\mathrm{Sel}_p(E) \arrow[rr, leftrightarrow, dotted, "\text{BSD/BK}"] \arrow[dr, leftrightarrow, "\text{Kolyvagin's method}"'] & & L(E,s) \arrow[dl, leftrightarrow, "\text{explicit reciprocity law (Bertolini–Darmon)}"] \\
& \{c(\ell)\} &
\end{tikzcd}$$

8.2. **Heegner points on** $X_0(N)$**.** Recall the modular curve $Y_0(N) := \Gamma_0(N)\backslash\mathcal{H}$, where $\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} : N \mid c\right\} \subseteq \mathrm{SL}_2(\mathbf{Z})$, and the compactified modular curve $X_0(N) := \Gamma_0(N)\backslash\mathcal{H}^*$. More precisely, what we are defining here are the complex points $Y_0(N)(\mathbf{C})$ and $X_0(N)(\mathbf{C})$.

In the simplest case, $Y_0(1) = \mathrm{SL}_2(\mathbf{Z})\backslash\mathcal{H}$. For $\tau \in \mathcal{H}$, consider the elliptic curve $E_\tau := \mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau$. It is easy to check that $E_\tau \simeq E_{\tau'}$ if and only if τ and τ' are in the same $\mathrm{SL}_2(\mathbf{Z})$-orbit, so

$$Y_0(1)(\mathbf{C}) = \{\text{elliptic curves } E/\mathbf{C}\}.$$

To describe $Y_0(N)$, consider pairs $\left(E_\tau, C_\tau = \frac{\frac{1}{N}\mathbf{Z}+\mathbf{Z}\tau}{\mathbf{Z}+\mathbf{Z}\tau} \simeq \mathbf{Z}/N\right)$. Analogously as above, $(E_\tau, C_\tau) \simeq (E_{\tau'}, C_{\tau'})$ if and only if τ and τ' are in the same $\Gamma_0(N)$-orbit, and hence

$$\begin{aligned} Y_0(N)(\mathbf{C}) &= \{(E, C) : E \text{ elliptic curve over } \mathbf{C},\ C \subseteq E \text{ cyclic group of order } N\} \\ &= \{E \to E' = E/C\text{: cyclic } N\text{-isogeny}\}. \end{aligned}$$

This moduli interpretation gives a model of $X_0(N)$ (and $Y_0(N)$) over $\mathbf{Q}$.

We want to construct points on $X_0(N)$ and use the modular parametrization $X_0(N)_{/\mathbf{Q}} \to E_{/\mathbf{Q}}$. However, $X_0(N)(\mathbf{Q})$ tends to be small (as a curve of genus at least 2 except for small value of N). To overcome this problem, we instead construct algebraic points on $X_0(N)$ lying in small degree number fields.

As a naive try, we consider the uniformization $\mathcal{H}^* \to X_0(N)(\mathbf{C})$. Although $\mathcal{H}^*$ contains many algebraic points, this map is highly transcendental and will not send algebraic points to algebraic points! The miracle, though, is that this may still work in special cases, namely for imaginary quadratic points. To see this, we use the moduli interpretation. Recall elliptic curves E over $\mathbf{C}$ can be divided into two possibilities:

(1) $\mathrm{End}(E) = \mathbf{Z}$.

(2) $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{O}_K$, where $K = \mathbf{Q}(\sqrt{-|d_K|})$ is an imaginary quadratic field and $\mathcal{O} \subseteq \mathcal{O}_K$ is a finite index subring.

Definition 8.2. An elliptic curve E in case (2) is said to have *complex multiplication (CM).*

Example 8.3. The elliptic curve $E : y^2 = x^3 + nx$ has CM by $\mathcal{O} = \mathbf{Z}[i]$, where

$$[i](x, y) = (-x, iy).$$

Example 8.4. The elliptic curve $E : y^2 = x^3 + n$ has CM by $\mathcal{O} = \mathbf{Z}[\zeta_3]$, where

$$[\zeta_3](x, y) = (\zeta_3 x, y).$$

The theory of complex multiplication tells us that CM elliptic curves are defined over number fields. Recall that for a number field K, the Hilbert class field H_K is the maximal unramified abelian extension of K, with $\mathrm{Gal}(H_K/K) \simeq \mathrm{Cl}(K)$.

Theorem 8.5 (Main Theorem of CM)**.** *There is a bijection*

$$\{\textit{elliptic curves with CM by } \mathcal{O}_K\} \xrightarrow{\sim} \{\mathbf{C}/\mathfrak{a} : \mathfrak{a} \in \mathrm{Cl}(K)\}.$$

Moreover, each such elliptic curve can be defined over the Hilbert class field H_K.

Definition 8.6. A *Heegner point* is a point $x_K = (E \xrightarrow{\phi} E') \in X_0(N)(\mathbf{C})$, where ϕ is a cyclic N-isogeny, such that $\mathrm{End}(E) = \mathrm{End}(E') = \mathcal{O}_K$.

We know that $x_K \in X_0(N)(H_K)$.

Remark. A Heegner point $x_K \in X_0(N)$ exists $\iff$ there exists $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(K)$ such that $\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{b}$ is a cyclic N-isogeny $\iff$ $\mathfrak{b}/\mathfrak{a} \simeq \mathcal{O}_K/\mathfrak{a}\mathfrak{b}^{-1}$ is isomorphic to $\mathbf{Z}/N$ $\iff$ there exists an ideal $\mathcal{N} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \simeq \mathbf{Z}/N$.

Definition 8.7. We say that K satisfies the *Heegner hypothesis* for $X_0(N)$ if every prime dividing N splits in K.

If this is true, then taking a prime $\mathfrak{p}$ above every $p \mid N$ and $\mathcal{N} = \prod \mathfrak{p}^{\mathrm{ord}_p(N)}$ gives $\mathcal{O}/\mathcal{N} = \mathbf{Z}/N$, and so x_K exists. By Chebotarev density, there are infinitely many K satisfying the Heegner hypothesis for a given N.

8.3. **Heegner points on elliptic curves.**

Definition 8.8. Fix a modular parametrization $\varphi : X_0(N) \to E$ sending $\infty \in X_0(N)$ to $0 \in E$. Define a Heegner point on E to be

$$y_K := \sum_{\sigma \in \mathrm{Gal}(H_K/K)} \sigma(\varphi(x_K)) \in E(K).$$

It is not necessary to further trace down to $\mathbf{Q}$. Using the moduli interpretation, one can check the

Proposition 8.9. $\overline{y_K} = -\epsilon(E) y_K$ *in* $E(K)/E(K)_{\mathrm{tor}}$*, where* $\epsilon(E) \in \{\pm 1\}$ *is the sign of the functional equation.*

In particular, $y_K \in E(\mathbf{Q}) + E(K)_{\mathrm{tor}}$ if and only if $\epsilon(E) = -1$.

Example 8.10. For the elliptic curve $E = X_0(32) : y^2 = x^3 + 4x$, $K = \mathbf{Q}(\sqrt{-7})$ satisfies the Heegner hypothesis for $X_0(32)$. Then $H_K = K = \mathbf{Q}(\sqrt{-7})$ since $\mathrm{Cl}(K) = 0$. Using $\mathcal{H}^* \to E = \Gamma_0(32)\backslash\mathcal{H}^*$, we find

$$x_K = y_K = \left(\frac{\sqrt{-7}-1}{2}, \frac{\sqrt{-7}+3}{2}\right) \in E(K).$$

Moreover, y_K has infinite order, and $\epsilon(E) = +1$.

Heegner used this construction to prove the following

Theorem 8.11. *The elliptic curve $E : y^2 = x^3 - n^2x$ has $r_{\mathrm{alg}} \geq 1$ when n is a prime $\equiv 5 \pmod 8$.*

Example 8.12. For the elliptic curve $E : y^2 + y = x^3 - x$ with conductor $N = 37$, $K = \mathbf{Q}(\sqrt{-7})$ satisfies the Heegner hypothesis for $X_0(37)$. Then $y_K = (0, 0) \in E(K)$ has infinite order, and this agrees with $\epsilon(E) = -1$.

Next time we will relate the Heegner point y_K with $L(E, 1)$ via the Gross–Zagier formula, and prove that $r_{\mathrm{an}}(E) = 1 \implies r_{\mathrm{alg}}(E) \geq 1$.

9. Lecture 9 (October 15, 2018)

Last time we introduced the Heegner hypothesis: an imaginary quadratic field K satisfies the Heegner hypothesis for $X_0(N)$ if

$$\text{every } p \mid N \text{ splits in } K, \tag{Heeg}$$

and used this to construct Heegner points $x_K \in X_0(N)(H_K)$ and $y_K \in E(K)$.

9.1. Gross–Zagier formula.

Let E_K be the base change of E from $\mathbf{Q}$ to K. Then $L(E_K, s)$ satisfies a functional equation

$$L(E_K, s) \leftrightarrow L(E_K, 2 - s)$$

with sign of functional equation $\epsilon(E_K)$. There is a simple formula for computing $\epsilon(E_K)$.

Proposition 9.1. *Assume $(d_K, N) = 1$. Then $\epsilon(E_K) = \chi_K(-N)$, where $\chi_K : \mathbf{Z}/|d_K| \to \{\pm 1\}$ is the quadratic character associated to $K/\mathbf{Q}$.*

Corollary 9.2. *If K satisfies* (Heeg)*, then $\epsilon(E_K) = -1$. More generally,*

$$\epsilon(E_K) = -\prod_{p \text{ inert in } K} (-1)^{\mathrm{ord}_p N}.$$

To summarize, we have a diagram

$$\begin{tikzcd}
& \epsilon(E_K) = -1 \arrow[r, Rightarrow] & r_{\mathrm{an}}(E_K) = \mathrm{odd} \arrow[ldd, dotted, leftrightarrow, "?"] \\
(\mathrm{Heeg}) \arrow[ru, Rrightarrow] \arrow[rd, Rrightarrow] & & \\
& y_K \in E(K) &
\end{tikzcd}$$

so it is natural ask to ask if there is a relationship between $y_K \in E(K)$ and $r_{\mathrm{an}}(E_K) = \mathrm{odd}$.

Theorem 9.3 (Gross–Zagier)**.**

$$L'(E_K,1)=\frac{\int_{E(\mathbf{C})}\omega\wedge\overline{i\omega}}{|d_K|^{1/2}|\mathcal{O}_K^\times//\{\pm1\}|^2}\langle y_K,y_K\rangle_{\mathrm{NT}}.$$

Here $\omega\in H^0(E_{\mathbf{Q}},\Omega^1)$ is such that $\varphi^*\omega=2\pi i f_E(z)\,dz$, where f_E is the normalized newform associated to E.

Remark. Since

$$\left(\int_{E(\mathbf{C})}\omega\wedge\overline{i\omega}\right)\cdot\deg\varphi=\int_{X_0(\mathbf{C})}8\pi^2 f(z)\overline{f(z)}\,dx\,dy=(f,f)$$

is the Petersson inner product, we can rewrite the Gross–Zagier formula as

$$L'(E_K,1)=\frac{(f,f)}{|d_K|^{\frac{1}{2}}|\mathcal{O}_K^\times/\{\pm1\}|^2}\cdot\frac{\langle y_K,y_K\rangle_{\mathrm{NT}}}{\deg\varphi}.$$

Remark. The Heegner point y_K depends on the choice of $\mathcal{N}\subseteq\mathcal{O}_K$, but is determined up to sign and torsion. It also depends on $\varphi:X_0(N)\to E$, but $\dfrac{\langle y_K,y_K\rangle_{\mathrm{NT}}}{\deg\varphi}$ is canonical!

The proof of the Gross-Zagier formula is a computation. To understand it conceptually, we need to rephrase the formula.

Corollary 9.4. *$L'(E_K,1)=0\iff\langle y_K,y_K\rangle_{\mathrm{NT}}=0\iff y_K$ is of infinite order. Thus $r_{\mathrm{an}}(E_K)=1\implies r_{\mathrm{alg}}(E_K)\geq 1$.*

Remark. Comparison with the BSD formula gives

$$|\text{Ш}(E_K)|^{\frac{1}{2}}\overset{?}{=}\frac{[E(K):\mathbf{Z}y_K]}{\prod_p c_p(E)\cdot|\mathcal{O}_K^\times|^2\cdot c}$$

where c is the Manin constant (conjectured to be 1): $\varphi^*\omega_E=c\cdot 2\pi i f_E(z)\,dz$. In particular, this gives the conjectural implication

$$\begin{cases}p\nmid y_K\\ E(K)[p]=0\end{cases}\overset{?}{\Longrightarrow}\text{Ш}(E_K)[p^\infty]=0.$$

9.2. **Back to $E/\mathbf{Q}$.** Now we explain how the result above descends to $\mathbf{Q}$.

Definition 9.5. Let $E^{(K)}/\mathbf{Q}$ be the quadratic twist of E by K, i.e., the unique elliptic curve over $\mathbf{Q}$ that is isomorphic to E over K but not isomorphic to E over $\mathbf{Q}$. Explicitly, if E has Weierstrass equation $y^2=x^3+Ax+B$, then

$$E^{(K)}:d_Ky^2=x^3+Ax+B.$$

Remark. Consider $\rho_E:G_{\mathbf{Q}}\to\mathrm{Aut}(V_pE)$. Then $\rho_{E^{(K)}}=\rho_E\otimes\chi_K$ where $\chi_K:G_{\mathbf{Q}}\twoheadrightarrow G_{K/\mathbf{Q}}\simeq\{\pm1\}$.

Proposition 9.6. *$L(E_K,s)=L(E,s)L(E^{(K)},s)$.*

Proof. Check by definition, or

$$L(E_K,s)=L(\mathrm{Ind}_{G_K}^{G_{\mathbf{Q}}}\rho_E,s)=L(\rho_E\oplus\rho_E\otimes\chi_K,s)=L(\rho_E,s)L(\rho_E\otimes\chi_K,s).\qquad\square$$

Corollary 9.7. *$r_{\mathrm{an}}(E_K)=r_{\mathrm{an}}(E)+r_{\mathrm{an}}(E^{(K)})$.*

By BSD, this predicts an identity on algebraic ranks, which is also easy to see directly.

Proposition 9.8. $r_{\mathrm{alg}}(E_K) = r_{\mathrm{alg}}(E) + r_{\mathrm{alg}}(E^{(K)})$.

Proof. Looking at the action of complex conjugation, we have

$$E(K) \otimes \mathbf{Q} \simeq E(\mathbf{Q}) \otimes \mathbf{Q} \oplus E^{(K)}(\mathbf{Q}) \otimes \mathbf{Q}$$

into the eigenspaces for $c = \pm 1$. □

Theorem 9.9. *If* $r_{\mathrm{an}}(E) = 1$*, then* $r_{\mathrm{alg}}(E) \geq 1$.

Proof. By a theorem of Waldspurger (next time), one can choose K satisfying (Heeg) such that $r_{\mathrm{an}}(E^{(K)}) = 0$. Then $r_{\mathrm{an}}(E_K) = 1 + 0 = 1$, hence $r_{\mathrm{alg}}(E_K) \geq 1$. But $\epsilon(E) = -1$, so $y_K^c = -\epsilon(E) y_K = y_K$ in $E(K)/E(K)_{\mathrm{tor}}$. Therefore $P = y_K^c + y_K \in E(\mathbf{Q})$ is of infinite order, and $r_{\mathrm{alg}}(E) \geq 1$. □

Corollary 9.10. *If* $r_{\mathrm{an}}(E) = 1$*, then*

$$\frac{L'(E,1)}{\Omega(E)R(E)} \in \mathbf{Q}^\times.$$

Proof. Choose K as before. Then $L'(E_K, 1) = L'(E,1)L(E^{(K)}, 1)$, where $\dfrac{L(E^{(K)}, 1)}{\Omega(E^{(K)})} \in \mathbf{Q}^\times$. The result follows from the Gross–Zagier formula using $\dfrac{\int_{E(\mathbf{C})} \omega \wedge \overline{i\omega}}{|d_K|^{\frac{1}{2}}} \overset{\mathbf{Q}^\times}{\sim} \Omega(E)\Omega(E^{(K)})$. □

Corollary 9.11. *If* $\epsilon(E) = -1$ *and* $y_K^c + y_K \in E(\mathbf{Q})$ *is torsion, then* $r_{\mathrm{an}}(E) \geq 3$.

Using this we can construct $E/\mathbf{Q}$ with $r_{\mathrm{an}}(E) = 3$.

Remark. There is no example of $E/\mathbf{Q}$ with provably correct $r_{\mathrm{an}}(E) = 4$.

Theorem 9.12 (Goldfeld, 1976)**.** *If there exists* $E_{\mathbf{Q}}$ *with* $r_{\mathrm{an}}(E) \geq 3$*, then the class number of* $\mathbf{Q}(\sqrt{-D})$ *has an explicit lower bound*

$$h(D) \gg C_{\delta,E} \cdot (\log |D|)^{1-\delta}$$

for all $\delta > 0$*, where* $C_{\delta,E}$ *is an effective constant.*

Example 9.13 (Gauss elliptic curve)**.** Consider $E : y^2 + y = x^3 - 7x + 6$ with $N = 5077$. Buhler–Gross–Zagier computed that $y_K^c + y_K$ is torsion, hence $r_{\mathrm{an}}(E) \geq 3$. Together with Goldfeld, this solves Gauss' class number problem.

9.3. Gross–Zagier formula for Shimura curves.

Fix an imaginary quadratic field $K/\mathbf{Q}$. For $(N, d_K) = 1$, define $N = N^+ N^-$ where every $p \mid N^+$ splits in K and every $p \mid N^-$ is inert in K.

Example 9.14. The Heegner hypothesis (Heeg) implies that $N = N^+$.

Assume N^- is square-free. Then $\epsilon(E_K) = -(-1)^{\#\{p|N^-\}}$, so

$$\epsilon(E_K) = \begin{cases} +1 & \text{if } \#\{p \mid N^-\} \text{ is odd}, \\ -1 & \text{if } \#\{p \mid N^-\} \text{ is even}. \end{cases}$$

Definition 9.15. K satisfies the *generalized Heegner hypothesis* (Heeg*) if N^- is a square-free product of an even number of primes.

Next time we will construct y_K for K satisfying this.

10. Lecture 10 (October 17, 2018)

Last time we introduced the generalized Heegner hypothesis:

$$\begin{cases} N = N^+N^-, \text{ with } N^- \text{ a square-free product of an } \textit{even} \text{ number of primes,} \\ p \mid N^+ \implies p \text{ split in } K, \\ p \mid N^- \implies p \text{ inert in } K. \end{cases} \tag{Heeg*}$$

Our goal is to construct Heegner points in this setting and fill in a similar diagram as last time

$$\begin{tikzcd}
(\text{Heeg*}) \arrow[r, Rightarrow] \arrow[dr, Rightarrow, "?"] & \epsilon(E_K) = -1 \arrow[r, Rightarrow] & r_{\text{an}}(E_K) = \text{odd} \arrow[dl, dotted, leftrightarrow, "?"'] \\
& \text{Heegner points } y_K &
\end{tikzcd}$$

10.1. **Gross–Zagier formula for Shimura curves.** Since $\#\{p \mid N^-\}$ is even, we can construct the following

Definition 10.1. Let $B = B_N$ be the unique quaternion algebra over $\mathbf{Q}$ that is ramified exactly at $\{p \mid N\}$, i.e.,

$$B_v \cong \begin{cases} M_2(\mathbf{Q}_v) & \text{if } v \nmid N^-, \\ \text{division quaternion algebra over } \mathbf{Q}_v & \text{if } v \mid N^-. \end{cases}$$

Example 10.2. Every quaternion algebra over $\mathbf{Q}$ is of the form $B = \mathbf{Q}\{1, i, j, ij\}$ where $i^2 = a$, $j^2 = b$, $ij = -ji$.

- If $a = 1$, then we recover the matrix algebra $B \simeq M_2(\mathbf{Q})$ via $i \mapsto \left(\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right)$, $j \mapsto \left(\begin{smallmatrix} & 1 \\ b & \end{smallmatrix}\right)$ and $ij \mapsto \left(\begin{smallmatrix} & 1 \\ -b & \end{smallmatrix}\right)$.
- If a is a prime $p \equiv 1 \pmod 4$ and b is a prime q such that $\left(\dfrac{q}{p}\right) \neq 1$, then B is exactly ramified at $\{p, q\}$.

As an analogue of $M_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : N \mid c\right\}$,

Definition 10.3. An *Eichler order* of level N^+ is a subring $\mathcal{O} \subseteq \mathcal{O}_B$ (maximal order in B) of finite index, such that

$$\mathcal{O}_p = \begin{cases} M_0(N^+)_p & \text{if } p \nmid N^-, \\ \mathcal{O}_{B_p} & \text{if } p \mid N^-, \end{cases}$$

where $\mathcal{O}_{B_p}$ is the maximal order of B_p.

Now we can define the analogue of $\Gamma_0(N)$.

Definition 10.4. $\Gamma(N^+, N^-) = \{\gamma \in \mathcal{O}^\times : \gamma\overline{\gamma} = 1\}$.

Example 10.5. If $N^- = 1$, then $\Gamma(N^+, 1) = \Gamma_0(N^+)$.

Definition 10.6. Using $\Gamma(N^+, N^-) \hookrightarrow B^\times(\mathbf{R}) \simeq \mathrm{GL}_2(\mathbf{R})$, the condition $\gamma\overline{\gamma} = 1$ implies that $\Gamma(N^+, N^-)$ has image in $\mathrm{SL}_2(\mathbf{R})$. We define the *Shimura curve*

$$X(N^+, N^-) := \Gamma(N^+, N^-)\backslash\mathcal{H}.$$

Example 10.7.

- If $N^- = 1$, then $X(N^+, N^-) = Y_0(N)$.
- If $N^- \neq 1$, then $X(N^+, N^-)$ is already compact.

Remark. This is an example of a Shimura variety. One can rewrite $X(N^+, N^-)$ adelically as follows. Consider the compact open subgroup $K_p = \mathcal{O}_p^\times \subseteq B^\times(\mathbf{Q}_p)$. Take $K_f = \prod_p K_p \subseteq B^\times(\mathbf{A}_f)$, again a compact open subgroup. Then $K_f \cap B_1^\times(\mathbf{Q}) = \Gamma(N^+, N^-)$ and

$$\begin{aligned} X(N^+, N^-) &= \Gamma(N^+, N^-)\backslash\mathcal{H} \\ &\cong B^\times(\mathbf{Q})\backslash B^\times(\mathbf{A}_f) \times \mathcal{H}^\pm / K_f. \end{aligned}$$

Notice $\mathcal{H} = \mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R})$.

Now we are ready to construct Heegner points using the moduli interpretation of Shimura curves, similarly as in the case of modular curves:

- In the level 1 case,
$$X(1, N^-)(\mathbf{C}) = \{\text{abelian surface } A/\mathbf{C} \text{ with } \mathcal{O}_B \hookrightarrow \mathrm{End}(A)\}$$
by sending $\tau \in \mathcal{H}$ to $\mathbf{C}^2/\mathcal{O}_B \cdot \left(\begin{smallmatrix}\tau\\1\end{smallmatrix}\right)$ via $\mathcal{O}_B \hookrightarrow M_2(\mathbf{C})$.
- In the general case,
$$X(N^+, N^-)(\mathbf{C}) = \{A \to A' \text{: cyclic } \mathcal{O}_B\text{-isogeny of degree } (N^+)^2\}.$$

Example 10.8. If $N^- = 1$, then $A_\tau = E_\tau \times E_\tau$.

Let K be an imaginary quadratic field satisfying (Heeg*), with Hilbert class field H_K.

Definition 10.9. Define Heegner points $x_K = (A \to A') \in X(N^+, N^-)(H_K)$ if $A \sim E^2$, $A' \sim E'^2$ and $\mathrm{End}(E) = \mathrm{End}(E') = \mathcal{O}_K$.

Definition 10.10. Using the modular parametrization $\varphi : X(N^+, N^-) \to E$, define

$$y_K = \sum_{\sigma \in \mathrm{Gal}(H_K/K)} \varphi(\sigma(x_K)) \in E(K).$$

Theorem 10.11 (Yuan–Zhang–Zhang)**.** *Assume K satisfies* (Heeg$*$)*. Then*

$$L'(E_K, 1) = \frac{(f, f)}{|d_K|^{\frac{1}{2}} |\mathcal{O}_K^\times/\{\pm 1\}|^2} \cdot \frac{\langle y_K, y_K \rangle_{\mathrm{NT}}}{\deg \varphi}.$$

Although this looks exactly the same as the original Gross–Zagier formula, the proof is much more complicated.

10.2. **Waldspurger's formula.** To study the case $\epsilon(E_K) = +1$, we need a formula of Waldspurger which was proved around the same time as Gross–Zagier and concerns the central value $L(E_K, 1)$.

Assume the hypothesis:

$$N^- \text{ is a square-free product of an } \textit{odd} \text{ number of primes.} \qquad \text{(Wald)}$$

This implies $\epsilon(E_K) = +1$. The goal is to construct "y_K" such that $y_k \longleftrightarrow L(E_K, 1)$. But $\#\{p \mid N^-\}$ is odd, so we *cannot* make a quaternion algebra B that is exactly ramified at $\{p \mid N^-\}$. Instead, we consider the

Definition 10.12. Let $B = B_{N^-\infty}$ be the unique quaternion algebra over $\mathbf{Q}$ ramified at $\{p \mid N^-\} \cup \{\infty\}$.

In particular, $B(\mathbf{R}) \simeq \mathbf{H}$ (where $i^2 = j^2 = -1$, $ij = -ji$), so

$$B_1^\times(\mathbf{R}) \cong \mathrm{SU}_2 = \left\{ \begin{pmatrix} x & -y \\ \overline{y} & \overline{x} \end{pmatrix} \in M_2(\mathbf{C}) : |x|^2 + |y|^2 = 1 \right\}$$

is compact and does not act on $\mathcal{H}$.

Definition 10.13. Let $\mathcal{O} \subseteq \mathcal{O}_B$ be an Eichler order of level N^+. Define the *Shimura set*

$$X(N^+, N^-) := B^\times(\mathbf{Q}) \backslash B^\times(\mathbf{A}_f)/K_f$$

where $K_f = \prod_p \mathcal{O}_p^\times$. (This is a 0-dimensional Shimura variety.)

Remark. A quaternion algebra $B/\mathbf{Q}$ is called *indefinite* if $B(\mathbf{R}) \simeq M_2(\mathbf{R})$, and *definite* if $B(\mathbf{R}) \simeq \mathbf{H}$.

Remark. Recall that for a number field F,

$$F^\times \backslash \mathbf{A}_{F,f}^\times / \prod_p \mathcal{O}_{F,p}^\times \xrightarrow{\sim} \mathrm{Cl}(\mathcal{O}_F).$$

Similarly, for a definite quaternion algebra B,

$$X(1, N^-) \cong \mathrm{Cl}(\mathcal{O}_B) = \{\text{right ideal classes of } \mathcal{O}_B\}.$$

Next we introduce Heegner points on this 0-dimensional Shimura variety.

Definition 10.14. Fix an embedding $K \hookrightarrow B$ (with $K \cap \mathcal{O} = \mathcal{O}_K$). Then we have

$$\mathrm{Cl}(\mathcal{O}_K) = K^\times \backslash \mathbf{A}_{K,f}^\times / \prod_p \mathcal{O}_{K,p}^\times \to X(N^+, N^-) = \mathrm{Cl}(\mathcal{O})$$
$$I \mapsto I\mathcal{O}.$$

A point $x_K \in \mathrm{Cl}(\mathcal{O}_K)$ (or its image) is called a *CM point* (or *Gross point*) on $X(N^+, N^-)$. ($\mathrm{Cl}(\mathcal{O}_K)$ permutes these CM points.)

Definition 10.15. Let $f \in S_2^{\mathrm{new}}(N)$, which transfers under the Jacquet–Langlands correspondence to a function $\varphi : X(N^+, N^-) \to \mathbf{C}$ with the same Hecke eigenvalues as f. (This is the analogue of $X(N^+, N^-) \to E$ in the indefinite case.) Define *Waldspurger's toric period*

$$y_K = \sum_{x_K \in \mathrm{Cl}(\mathcal{O}_K)} \varphi(x_K)(|\operatorname{Aut}(x_K)|) \in \mathbf{C}$$

where $\operatorname{Aut}(x) = \{\gamma \in B^\times(\mathbf{Q}) : \gamma x = x\}/\{\pm 1\}$, and

$$\deg \varphi = \sum_{x \in X(N^+, N^-)} |\varphi(x)|^2 (|\operatorname{Aut}(x)|).$$

Finally, we can state the

Theorem 10.16 (Waldspurger). *Assume K satisfies* (Wald). *Then*

$$L(E_K, 1) = \frac{(f, f)}{|d_K|^{\frac{1}{2}} |\mathcal{O}_K^\times / \{\pm 1\}|^2} \cdot \frac{|y_K|^2}{\deg \varphi}.$$

Corollary 10.17. $L(E_K, 1) \neq 0 \iff y_K \neq 0.$

11. Lecture 11 (October 22, 2018)

Last time we stated Waldspurger's formula: if K satisfies (Wald) for $N = N^+N^-$, then

$$L(E_K, 1) = \frac{(f, f)}{|d_K|^{\frac{1}{2}} |\mathcal{O}_K^\times/\{\pm 1\}|^2} \cdot \frac{|y_K|^2}{\deg \varphi}$$

where y_K is the toric period.

11.1. Examples of Waldspurger's formula.

Example 11.1. Let $E = X_0(11)$, with Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$ and corresponding newform

$$\begin{aligned} f = f_E &= q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2 = \eta(z)^2 \eta(11z)^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots . \end{aligned}$$

Then $K = \mathbf{Q}(\sqrt{-5})$ satisfies (Wald) (note 11 is inert in K), with $N^+ = 1$ and $N^- = 11$. Let $B = B_{11,\infty}$ with maximal order $\mathcal{O} = \mathcal{O}_B$, so that $X(N^+, N^-) = X(1, 11) = \mathrm{Cl}(\mathcal{O}_B)$.

We make use of the following two formulas:

(1) (Eichler's mass formula) If N^- is prime, then $\displaystyle\sum_{x \in \mathrm{Cl}(\mathcal{O}_B)} \frac{1}{|\operatorname{Aut}(x)|} = \frac{N^- - 1}{12}$.

(2) $\displaystyle\prod_x |\operatorname{Aut}(x)| = \operatorname{denom}\left(\frac{N-1}{12}\right)$.

In our case, Eichler's mass formula gives $\frac{10}{12} = \frac{5}{6} = \frac{1}{2} + \frac{1}{3}$, so the second formula confirms that $|\mathrm{Cl}(\mathcal{O}_B)| = 2$ with $|\operatorname{Aut}(x_1)| = 2$ and $|\operatorname{Aut}(x_2)| = 3$.

Consider the modular parametrization $\varphi : X(N^+, N^-) \to \mathbf{C}$ with Hecke eigenvalues equal to those of f. It is easy to check that $x_1 \mapsto -1$ and $x_2 \mapsto 1$. Then $y_K = -2 + 3 = 1$ (which implies $r_{\mathrm{an}}(E_K) = 0$) and $\deg \varphi = 2 + 3 = 5$. Now we compute that

$$\begin{aligned} L(E_K, 1) &= L(E, 1) L(E^{(K)}, 1) \\ &= (0.25384 \cdots)(0.65240 \cdots), \\ (f, f) &= 3.70309 \cdots , \\ \implies \frac{L(E_K, 1)}{(f, f)} &= 0.044721 \cdots = \frac{1}{10\sqrt{5}}. \end{aligned}$$

This matches up with $\displaystyle\frac{1}{|d_K|^{\frac{1}{2}}} \cdot \frac{|y_K|^2}{\deg \varphi} = \frac{1}{\sqrt{20}} \cdot \frac{1}{5} = \frac{1}{10\sqrt{5}}$, as predicted by Waldspurger's formula.

Question. How does y_K vary when K varies?

Answer. They fit into another modular form of weight $\frac{3}{2}$.

Definition 11.2. Let $\mathrm{Cl}(\mathcal{O}) = \{x_1, \cdots, x_n\}$ (right ideal classes of $\mathcal{O}$). For each i, define the *left order* of x_i

$$R_i = \{\gamma \in B : \gamma x_i = x_i\},$$

and

$$S_i = \{\gamma \in \mathbf{Z} + 2R_i : \mathrm{tr}(\gamma) = 0\},$$

which is a rank 3 $\mathbf{Z}$-module together with a quadratic form given by the norm $\mathbf{N}$.

Definition 11.3. Define a weight $\frac{3}{2}$ θ-series by

$$g_i := \frac{1}{2}\sum_{v \in S_i} q^{\mathbf{N}v}.$$

Thus the D-th Fourier coefficient of g_i encodes the maps $x_{\mathbf{Q}(\sqrt{-D})} \in \{\text{CM points}\} \mapsto x_i \in X(N^+, N^-)$ under $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O})$.

Definition 11.4. Associated to f, define

$$g := \sum_{i=1}^{n} \varphi(x_i) g_i = \sum_{n \geq 1} b_n q^n.$$

Theorem 11.5. $y_K = b_{|d_K|}$.

Example 11.6. Let $E = X_0(11)$ and $\mathrm{Cl}(\mathcal{O}_B) = \{x_1, x_2\}$ as before. Then we can compute that

$$g_1 = \frac{1}{2} \sum_{\substack{x,y,z \in \mathbf{Z} \\ x \equiv y \pmod 2}} q^{x^2+11y^2+11z^2} = \frac{1}{2} + q^4 + q^{11} + 2q^{12} + q^{16} + 2q^{20} + \cdots,$$

$$g_2 = \frac{1}{2} \sum_{\substack{x,y,z \in \mathbf{Z} \\ x \equiv y \pmod 3 \\ y \equiv z \pmod 2}} q^{\frac{x^2+11y^2+33z^2}{3}} = \frac{1}{2} + q^3 + q^{12} + 3q^{15} + 3q^{16} + 3q^{20} + \cdots,$$

and hence $g = -g_1 + g_2 = q^3 - q^4 - q^{11} + 2q^{16} + q^{20} + \cdots$. In particular, $y_K = 1$ for $K = \mathbf{Q}(\sqrt{-5})$! Indeed, for $E = X_0(11)$,

$$\text{BSD formula for } E_K \iff |\text{Ш}(E/K)| \overset{?}{=} |b_{|d_K|}|^2.$$

In particular, $\text{Ш}(E/\mathbf{Q}(\sqrt{-5})) = 0$!

The first two non-trivial examples are given by

$$g = q^3 - q^4 - q^{11} + 2q^{16} + q^{20} + \cdots + 3q^{67} + \cdots + 4q^{91} + \cdots.$$

Indeed, $\text{Ш}(E/\mathbf{Q}(\sqrt{-67})) = (\mathbf{Z}/3)^2$ and $\text{Ш}(E/\mathbf{Q}(\sqrt{-91})) = (\mathbf{Z}/2)^4$.

Remark. By studying Fourier coefficients of weight $\frac{3}{2}$ forms, one can show there are a lot of K such that $y_K \neq 0$, which implies that $r_{\mathrm{an}}(E^{(K)}) = 0$ for many K. Recall that this is the input for deducing BSD over $\mathbf{Q}$ from BSD over K.

11.2. **Back to Kolyvagin.** Recall that we have constructed Heegner points on modular curves, Shimura curves or Shimura sets. Our next goal is to construct classes $c(\ell) \in H^1(K, E[p])$ such that $\mathrm{loc}_\ell(c(\ell))$ is ramified, i.e., its image in $H^1_{\mathrm{sing}}(K_\ell, E[p])$ is nonzero.

As a naive try, say K satisfies (Heeg*). Then we have Heegner points $y_K \in E(K)$. Using the connecting homomorphism

$$\delta : \frac{E(K)}{pE(K)} \to H^1(K, E[p]),$$

we obtain $\delta(y_K) \in H^1(K, E[p])$.

Problem: If $\ell \notin S = \{x \mid Np\infty\}$, then $\delta(y_K)$ is *unramified* at ℓ.

The idea is to find another elliptic curve $E(\ell)$ such that $E[p] \xrightarrow{\sim} E(\ell)[p]$ and $E(\ell)$ has conductor $N\ell$. If so, choose K satisfying (Heeg*) for $N\ell$. This gives $y_K(\ell) \in E(\ell)(K)$ and $c(\ell) := \delta(y_K(\ell)) \in H^1(K, E(\ell)[p]) \cong H^1(K, E[p])$. Then it is possible that $c(\ell)$ is ramified at ℓ, as $\ell \mid N\ell$.

To summarize, we can produce ramification by raising the level under congruences mod p.

Question. Given $f \in S_2^{\text{new}}(N)$, when can we find $g \in S_2^{\text{new}}(N\ell)$ such that $f \equiv g \pmod p$ (i.e., $a_q(f) \equiv q_q(g) \pmod p$ for almost all primes q)?

In general this is not possible. For example, when the level is small, the number of modular forms is limited. We can reformulate this question in terms in Galois representations. Consider $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{Z}_p})$ and the residual representation $\overline{\rho_f} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}_p})$.

Question. When can we find $g \in S_2^{\text{new}}(N\ell)$ such that $\overline{\rho_f} \cong \overline{\rho_g}$?

Under this reformulation, we immediately see a necessary condition. Since $\overline{\rho_f}|_{G_{\mathbf{Q}_\ell}} \cong \overline{\rho_g}|_{G_{\mathbf{Q}_\ell}}$ and ρ_f is unramified at ℓ, we want $\overline{\rho_g}$ to be unramified (even though ρ_g is ramified at ℓ), so g has multiplicative reduction at ℓ. By Tate's uniformization, Frob_ℓ is sent to $\pm \begin{pmatrix} \ell & * \\ 0 & 1 \end{pmatrix}$. Taking $\mathrm{tr}(\mathrm{Frob}_\ell)$, we get $a_\ell(f) \equiv \pm(\ell+1) \pmod p$.

Definition 11.7. $\ell \nmid Np$ is called a *level-raising prime* for $f \pmod p$ if

$$a_\ell(f) \equiv \pm(\ell+1) \pmod p.$$

Ribet shows this is almost a sufficient condition:

Theorem 11.8 (Ribet, 1990)**.** *If $\overline{\rho_f}$ is irreducible, and ℓ is a level-raising prime for f* $\pmod p$*, then there exists $g \in S_2^{\ell\text{-new}}(N\ell)$ such that $\overline{\rho_f} \simeq \overline{\rho_g}$.*

Example 11.9. Let $E = X_0(11)$ and $p = 2$. It is clear that

$$a_\ell(f) \equiv \pm(\ell+1) \pmod 2 \iff a_\ell(f) \text{ is even},$$

so $\ell = 7$ is level-raising. The corresponding $g \in S_2^{\text{new}}(77)$ is the newform with label $77a$:

	2	3	5	7	11	13	17	19
$f = f_E$	-2	-1	1	-2	1	4	-2	0
$g = 77a$	0	-3	-1	-1	-1	-4	2	-6

12. Lecture 12 (October 24, 2018)

Last time we stated the

Theorem 12.1 (Ribet)**.** *Let $f \in S_2(N)$ such that $\overline{\rho_f}$ is irreducible, and ℓ be a level-raising prime for f* $\pmod p$*, i.e., $a_\ell(f) \equiv \pm(\ell+1)$* $\pmod p$*. Then there exists $g \in S_2^{\ell\text{-new}}(N\ell)$ such that $\overline{\rho_f} \simeq \overline{\rho_g}$.*

12.1. **Geometric interpretation of Ribet's theorem: Ihara's lemma.** Recall that the modular curve $X_0(N)_{/\mathbf{Q}}$ has the moduli interpretation

$$\{(E, C) : E \text{ elliptic curve}, C \subseteq E[N] \text{ cyclic subgroup of order } N\}.$$

There is a correspondence

$$\begin{tikzcd} & X_0(N\ell) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ X_0(N) & & X_0(N), \end{tikzcd}$$

where

$$\pi_1 : (E, C) \mapsto (E, C[N]), \quad \pi_2 : (E, C) \mapsto (E/C[\ell], C/C[\ell])$$

which make sense since $C \simeq \mathbf{Z}/N\ell$.

Example 12.2. When $N = 1$, $X_0(\ell)$ parametrizes isogenies $(E \to E')$ of degree ℓ, and

$$\pi_1 : (E \to E') \mapsto E, \quad \pi_2 : (E \to E') \mapsto E'.$$

The Hecke operator can be defined as

$$T_\ell := \pi_{2*}\pi_1^* = \pi_{1*}\pi_2^* \in \mathrm{End}(J_0(N)).$$

Consider the map $\pi_1^* + \pi_2^*$, which fits into the diagram

$$\begin{tikzcd} H^0(X_0(N), \Omega^1)^{\oplus 2} \arrow[r, "\pi_1^*+\pi_2^*"] \arrow[d, equal] & H^0(X_0(N\ell), \Omega^1) \arrow[d, equal] \\ S_2(N)^{\oplus 2} \arrow[r] & S_2(N\ell). \end{tikzcd}$$

Concretely, $\pi_1^*(f(z)) = f(z)$ (via $z \mapsto z$) and $\pi_2^*(f(z)) = \ell f(\ell z)$ (via $z \mapsto \ell z$). These are ℓ-old forms, so

$$S_2^{\ell\text{-new}}(N\ell) = \mathrm{coker}(\pi_1^* + \pi_2^*).$$

To deal with mod p congruences (which require $\mathbf{Z}_p$-structures), we look at

$$\pi_1^* + \pi_2^* : H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)^{\oplus 2} \to H^1_{\text{ét}}(X_0(N\ell), \mathbf{Z}_p).$$

After inverting p, this is injective and the Hecke eigenvalues on $\mathrm{coker}(\pi_1^* + \pi_2^*)_{\mathbf{Q}_p}$ are exactly given by those on $S_2^{\ell\text{-new}}(N\ell)$.

Definition 12.3. Let $\mathbf{T}$ be the Hecke algebra generated by T_q for all $q \nmid N\ell$. Let $\chi_f : \mathbf{T} \to \overline{\mathbf{Z}_p}$ be the Hecke eigenvalues associated to f. Let $\mathfrak{m} = \mathfrak{m}_f := \ker(\mathbf{T} \xrightarrow{\chi_f} \overline{\mathbf{Z}_p} \twoheadrightarrow \overline{\mathbf{F}_p})$ be the maximal ideal of $\mathbf{T}$ encoding congruences with f.

To prove Ribet's theorem, it suffices to prove that the map

$$\pi_1^* + \pi_2^* : H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)^{\oplus 2}_{\mathfrak{m}} \to H^1_{\text{ét}}(X_0(N\ell), \mathbf{Z}_p)_{\mathfrak{m}}$$

(localization at $\mathfrak{m} = \mathfrak{m}_f$) has cokernel containing a point in characteristic 0, i.e., $\mathrm{coker}(\pi_1^*+\pi_2^*)$ is not torsion.

Theorem 12.4 (Ihara's lemma)**.** *Assume $\overline{\rho_f}$ is irreducible. Then*

$$\pi_1^* + \pi_2^* : H^1_{\text{ét}}(X_0(N), \mathbf{F}_p)^{\oplus 2}_{\mathfrak{m}} \to H^1_{\text{ét}}(X_0(N\ell), \mathbf{F}_p)_{\mathfrak{m}}$$

is injective.

Proof that Ihara implies Ribet. If $\operatorname{coker}(\pi_1^*+\pi_2^*)_{\mathbf{Z}_p}$ is torsion, then Ihara's lemma implies that $\operatorname{coker}(\pi_1^*+\pi_2^*)_{\mathbf{Z}_p}$ is trivial, so $(\pi_1^*+\pi_2^*)_{\mathbf{Z}_p}$ is an isomorphism. To get a contradiction, look at the dual map

$$(\pi_{1*}, \pi_{2*}) : H^1_{\text{ét}}(X_0(N\ell), \mathbf{Z}_p)_{\mathfrak{m}} \to H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)^{\oplus 2}_{\mathfrak{m}}$$

which is also an isomorphism by duality. The composition

$$H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)^{\oplus 2}_{\mathfrak{m}} \xrightarrow{\sim} H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)^{\oplus 2}_{\mathfrak{m}}$$

is an isomorphism, with 2×2 matrix given by

$$\begin{pmatrix} \ell+1 & T_\ell \\ T_\ell & \ell+1 \end{pmatrix}_{\mathfrak{m}} \equiv \begin{pmatrix} \ell+1 & \pm(\ell+1) \\ \pm(\ell+1) & \ell+1 \end{pmatrix} \pmod{p}.$$

This is a contradiction to the composition being an isomorphism. □

12.2. **Geometry of modular curves in characteristic** p**.** Recall that $X_0(N)$ has moduli interpretation (E, C) with $C \subseteq E[N]$. The group $E[N]$ still behaves well in characteristic $p \nmid N$ (i.e., is étale). In particular, if $p \nmid N$, then

$$E[N](\overline{\mathbf{F}_p}) \simeq (\mathbf{Z}/N)^2.$$

But $E[p]$ behaves differently in characteristic p:

$$E[p](\overline{\mathbf{F}_p}) \simeq \begin{cases} \mathbf{Z}/p & \text{if } E \text{ is ordinary,} \\ 0 & \text{if } E \text{ is supersingular.} \end{cases}$$

Equivalently,

$$\operatorname{End}(E_{/\overline{\mathbf{F}_p}}) \simeq \begin{cases} \mathcal{O} \subseteq \mathcal{O}_K & \text{if } E \text{ is ordinary,} \\ \mathcal{O} \subseteq \mathcal{O}_{p,\infty} & \text{if } E \text{ is supersingular,} \end{cases}$$

where K is an imaginary quadratic field, and $\mathcal{O}_{p,\infty}$ is the maximal order in $B_{p,\infty}$.

To define an integral model of $X_0(N)$, we need to change the moduli interpretation.

Theorem 12.5 (Igusa, Deligne–Rapoport, Katz–Mazur)**.** *$X_0(N)$ has a model over $\mathbf{Z}$. It is flat, projective and of relative dimension 1 over $\mathbf{Z}$.*

(1) *If $p \nmid N$, then $X_0(N)_{\mathbf{Z}_p}$ has the same moduli interpretation as before; $X_0(N)_{\mathbf{F}_p}$ is smooth, and has Newton stratum*

$$X_0(N)_{\mathbf{F}_p} = X_0(N)^{\text{ord}}_{\mathbf{F}_p} \cup X_0(N)^{\text{ss}}_{\mathbf{F}_p}$$

according to whether E is ordinary or supersingular, where the supersingular locus $X_0(N)^{\text{ss}}_{\mathbf{F}_p}$ is a finite set of points.

(2) *If $p \parallel N$, then $X_0(N)_{\mathbf{Z}_p}$ has moduli interpretation*

$$S_{/\mathbf{Z}_p} \mapsto \left\{ (E, C) : \begin{array}{l} E_{/S} \textit{ elliptic curve, } C \subseteq E[p] \textit{ finite flat} \\ \textit{group scheme over } \mathbf{Z}_p \textit{ of rank } N \end{array} \right\};$$

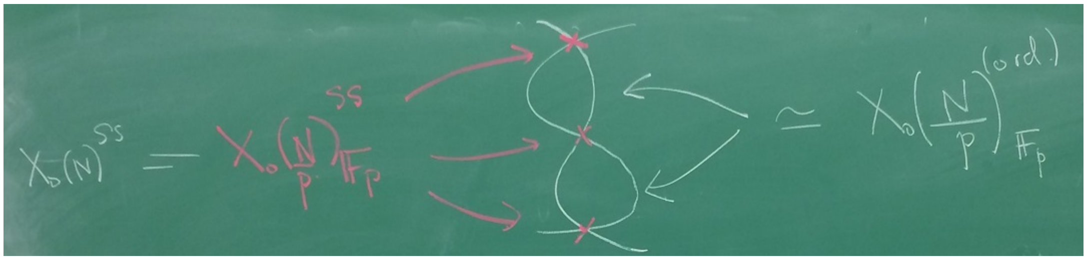
$X_0(N)_{\mathbf{F}_p}$ is no longer smooth but is semistable, with two irreducible components isomorphic to $X_0(N/p)_{\mathbf{F}_p}$ and intersecting along $X_0(N/p)^{\text{ss}}_{\mathbf{F}_p} = X_0(N)^{\text{ss}}$.

(3) *If $p^2 \mid N$, then $X_0(N)_{\mathbf{Z}_p}$ has moduli interpretation in terms of Drinfeld level structure:*

$$C = \bigoplus_{a \in \mathbf{Z}/p} [aP], \quad P \in E[p]$$

as a Cartier divisor on E; $X_0(N)_{\mathbf{F}_p}$ is not smooth and not semistable.

Remark. If $p \parallel N$, the picture looks like



$X_0(N)^{ss} = X_0(\frac{N}{p})^{ss}_{\mathbb{F}_p}$
$\simeq X_0(\frac{N}{p})^{(ord)}_{\mathbb{F}_p}$

Let us describe the gluing datum. Over $\mathbf{F}_p$, we have

$$\begin{tikzcd}
X_0(N/p) \arrow[dr, "\alpha_1"] & & X_0(N/p) \arrow[dl, "\alpha_2"'] \\
& X_0(N) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
X_0(N/p) & & X_0(N/p)
\end{tikzcd}$$

where (assuming $N/p = 1$ for simplicity)

$$\pi_1 : (E \overset{\deg p}{\to} E') \mapsto E, \quad \pi_2 : (E \overset{\deg p}{\to} E') \mapsto E',$$

$$\alpha_1 : E \mapsto (E \overset{\mathrm{Frob}_p}{\to} E^{(p)}), \quad \alpha_2 : E \mapsto (E^{(p)} \overset{\mathrm{Ver}_p}{\to} E).$$

Notice

$$\pi_1 \circ \alpha_1 = \mathrm{Id}, \quad \pi_2 \circ \alpha_2 = \mathrm{Id},$$

$$\pi_1 \circ \alpha_2 = \mathrm{Frob}_p, \quad \pi_2 \circ \alpha_1 = \mathrm{Ver}_p\,.$$

The two copies of $X_0(N/p)$ are glued via $E \leftrightarrow E^{(p)}$, as $(E^{(p)})^{(p)} \simeq E$ if E is supersingular.

Next time we will describe $X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$ explicitly and prove Ihara's lemma.

13. Lecture 13 (October 29, 2018)

Last time we saw that the special fiber $X_0(N)_{\mathbf{F}_p}$ is smooth if $p \nmid N$. Our goal is to describe the supersingular locus $X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$, which is a finite set.

13.1. **The supersingular locus.**

Proposition 13.1. *$X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p} \simeq X(N,p)$, the Shimura set associated to $B_{p,\infty}$, which is in turn isomorphic to $\mathrm{Cl}(\mathcal{O})$ for the Eichler order $\mathcal{O}$ of level N in $B_{p,\infty}$.*

Remark. This is an instance of "switching invariants": $X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$ is indefinite at ∞ and split at p, while $X(N,p)$ is definite at ∞ and ramified at p.

Idea of proof. Given $(E,C) \in X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$, we have $\mathrm{End}(E) \simeq \mathcal{O}_{p,\infty}$ (maximal order in $B_{p,\infty}$), under which the subring $\mathrm{End}(E,C)$ corresponds to $\mathcal{O}$ (Eichler order of level N).

Given any point $(E',C') \in X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$, look at $I = \mathrm{Hom}((E,C),(E',C'))$, which is a rank 4 $\mathbf{Z}$-module and admits a right action of $\mathcal{O} = \mathrm{End}(E,C)$: for $f \in I$ and $g \in \mathcal{O}$, $f \cdot g := f \circ g$. This construction gives a map

$$\begin{aligned} X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p} &\to X(N,p) = \mathrm{Cl}(\mathcal{O}) \\ (E',C') &\mapsto I = \mathrm{Hom}((E,C),(E',C')). \end{aligned}$$

One can check this is a bijection. □

Last time we saw that Ihara's lemma implies Ribet's theorem for level-raising congruences. Recall

Theorem 13.2 (Ihara's lemma)**.** *Assume $\overline{\rho_f}$ is irreducible (so that the maximal ideal $\mathfrak{m} = \mathfrak{m}_f \subseteq \mathbf{T}$ is "non-Eisenstein"). Then*

$$H^1_{\text{ét}}(X_0(N), \mathbf{F}_p)^{\oplus 2}_{\mathfrak{m}} \to H^1_{\text{ét}}(X_0(N\ell), \mathbf{F}_p)_{\mathfrak{m}}$$

is injective.

Idea of proof. Use p-adic comparison theorem between $H^1_{\text{ét}}(X_0(N), \mathbf{F}_p)$ and $H^1_{\mathrm{dR}}(X_0(N)_{/\mathbf{F}_p})$ and reduce to showing that

$$\pi_1^* + \pi_2^* : H^0(X_0(N)_{\mathbf{F}_p}, \Omega^1)^{\oplus 2} \to H^0(X_0(N\ell)_{\mathbf{F}_p}, \Omega^1)$$

is injective.

Suppose $(\omega_1, \omega_2) \in \ker(\pi_1^* + \pi_2^*)$. By looking at the Hecke action of T_ℓ, we see that if $(E',C') \in T_\ell(E,C)$, then

$$(E',C') \in \mathrm{div}^0(\omega_i) \iff (E,C) \in \mathrm{div}^0(\omega_i)$$

for $i = 1,2$. Thus $\mathrm{div}^0(\omega_i)$ is supported on the whole $X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$ (if $(E,C) \in X_0(N)^{\mathrm{ord}}_{\mathbf{F}_p}$, then $\{T_\ell^n(E,C) : n \geq 1\}$ is infinite).

But there is an explicit differential form (Hasse invariant) $A \in H^0(X_0(N)_{\mathbf{F}_p}, \omega^{p-1})$ of weight $p-1$ with simple zeros at exactly $X_0(N)^{\mathrm{ss}}_{\mathbf{F}_p}$. If $p - 1 > 2$, this is a contradiction!

If $p = 3$ (resp. $p = 2$), then $\omega_i = c \cdot A$ (resp. $\omega_i = c \cdot A^2$). Both cases are impossible, since the Hecke action on A is given by an Eisenstein ideal: $T_q \equiv q + 1 \pmod{p}$. □

13.2. **Geometry of Shimura curves.** We want to carry over the geometry of modular curves to the case of Shimura curves. Recall the Shimura curve $X(N^+, N^-)$ has moduli interpretation $\{(A, \iota, C)\}$ where:

- A is an abelian surface,
- $\iota : \mathcal{O}_{N^-} \hookrightarrow \mathrm{End}(A)$,
- $C \subseteq A[N]$ of order $(N^+)^2$ and cyclic as $\mathcal{O}_{N^-}$-module.

Analogous to $X_0(N) = X(N,1)$, we can extend this moduli interpretation to characteristic $p \nmid N = N^+N^-$. But at $p \mid N$, changes need to be made (especially more difficult when $p \mid N^-$)!

Let us begin with the classification of abelian surfaces with special endomorphisms in characteristic p. Let $A_{/\overline{\mathbf{F}_p}}$ be an abelian surface with $\mathcal{O}_{N^-}$-action. Then A is either:

- *ordinary*: $A[p] \simeq (\mathbf{Z}/p)^2 \iff A$ is isogenous to E^2 for an ordinary elliptic curve E.

- *supersingular*: $A[p] = 0 \iff A$ is isogenous to E^2 for a supersingular E.

If A is supersingular, we say that A is *superspecial* if A is isomorphic to E^2 for a supersingular E. Similarly to the case of elliptic curves, we have

$$\mathrm{End}(A) = \begin{cases} \mathcal{O} \subseteq M_2(\mathcal{O}_K) & \text{if } A \text{ is ordinary,} \\ \mathcal{O} \subseteq M_2(\mathcal{O}_{p,\infty}) & \text{if } A \text{ is supersingular,} \end{cases}$$

where K is an imaginary quadratic field.

Remark. By definition, every superspecial A is supersingular. When $p \nmid N^-$, the converse is true: A is superspecial if and only if A is supesingular.

The geometry of Shimura curves is summarized in the

Theorem 13.3 (Buzzard, Drinfeld). *Assume $p^2 \nmid N$. Then $X(N^+, N^-)$ has a model over $\mathbf{Z}_p$ which is flat and projective.*

(1) *If $p \nmid N$, then $X(N^+, N^-)_{\mathbf{F}_p}$ is smooth, with a distinguished finite set of marked points $X(N^+, N^-)^{\mathrm{ss}}_{\mathbf{F}_p}$. Moreover,*

$$X(N^+, N^-)^{\mathrm{ss}}_{\mathbf{F}_p} \simeq X(N^+, pN^-),$$

which is a definite Shimura set (note that pN^- has an odd number of prime factors).

Remark. In this case, $X(N^+, N^-)^{\mathrm{ss}}_{\mathbf{F}_p} = X(N^+, N^-)^{\mathrm{s.sp}}_{\mathbf{F}_p}$.

(2) *If $p \parallel N^+$, then $X(N^+, N^-)_{\mathbf{F}_p}$ is not smooth but is semistable, with two irreducible components each isomorphic to $X(N^+/p, N^-)$ and intersecting along*

$$X(N^+, N^-)^{\mathrm{ss}}_{\mathbf{F}_p} = X(N^+/p, N^-)^{\mathrm{ss}}_{\mathbf{F}_p} \overset{(1)}{=} X(N^+/p, pN^-).$$

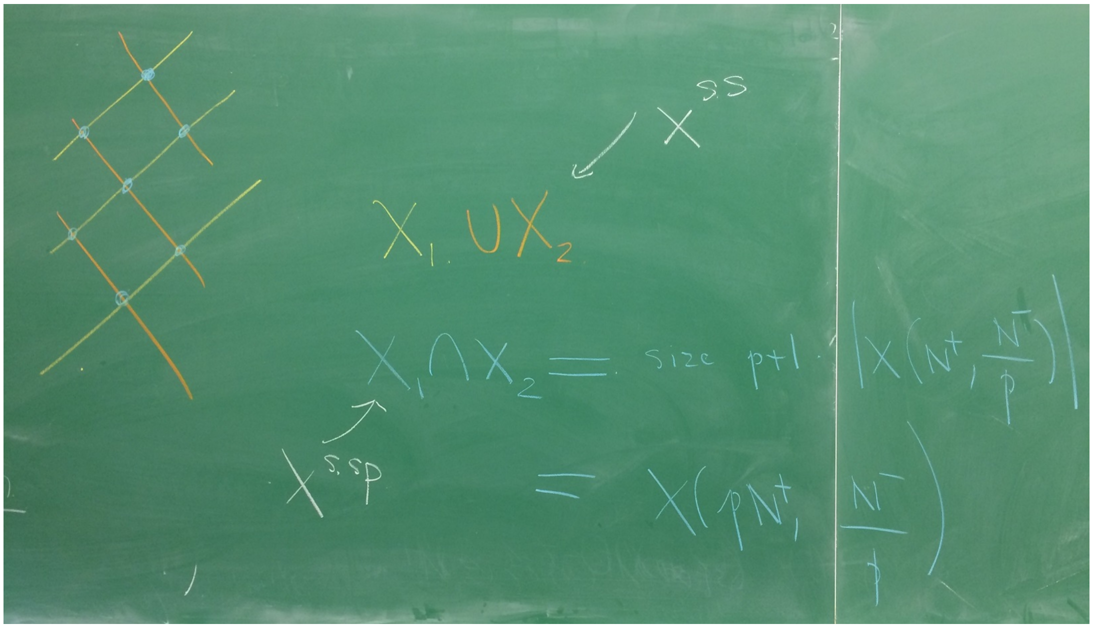
Remark. Cases (1) and (2) are analogous to the situation for $X_0(N)$.

(3) *If $p \mid N^-$, then $X(N^+, N^-)_{\mathbf{F}_p}$ is not smooth but is semistable. Its geometry is described by Ceredink–Drinfeld p-adic uniformization:*

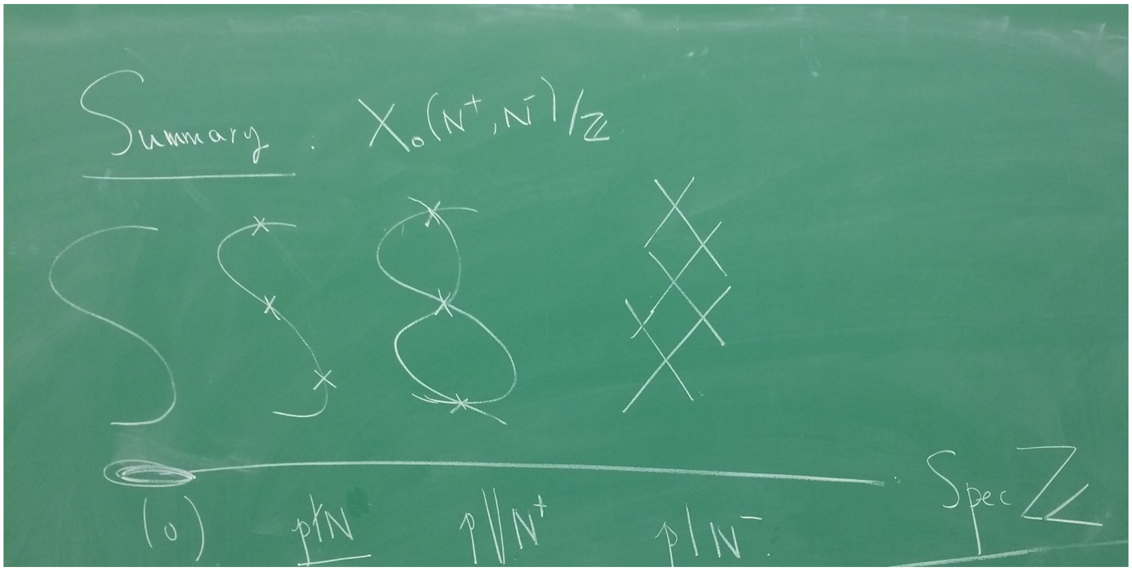
$$X(N^+, N^-)_{\mathbf{F}_p} = X_1 \cup X_2,$$

where each X_i is a family of $\mathbf{P}^1$'s indexed by the Shimura set $X(N^+, N^-/p)$ (switching invariants). Each $\mathbf{P}^1$ in X_1 intersects with exactly $p+1$ $\mathbf{P}^1$'s in X_2 (and vice versa), forming $\mathbf{P}^1(\mathbf{F}_p)$. Finally,

$$X_1 \cap X_2 = (p+1) \cdot |X(N^+, N^-/p)| = X(pN^+, N^-/p).$$


X^{ss}
$X_1 \cup X_2$
$X_1 \cap X_2 =$ size $p+1 \cdot \left|X(N^+, \frac{N^-}{p})\right|$
$X^{s.sp}$
$= X(pN^+, \frac{N^-}{p})$

The geometry of $X(N^+, N^-)$ is summarized in the picture:



- For $p \nmid N$, $X(N^+, N^-)^{\mathrm{ss}}_{\mathbf{F}_p} = X(N^+, pN^-)$.
- For $p \mid N^-$, the irreducible components of $X(N^+, N^-)_{\mathbf{F}_p}$ are $X(N^+, N^-/p)$.

14. Lecture 14 (October 31, 2018)

14.1. **Inertia action on cohomology.** The motivation is to understand

$$H^1_{\mathrm{sing}}(K_\ell, E[p]) = H^1(I_\ell, E[p])^{\mathrm{Fr}_\ell = 1},$$

where I_ℓ is the inertia subgroup at ℓ. Thus we need to understand the action of I_ℓ on $E[p] = H^1_{\text{ét}}(E, \mathbf{F}_p)(1)$.

In general, let us switch notation to the local situation. Suppose X is a smooth projective variety over $\mathbf{Q}_p$, and $K = \widehat{\mathbf{Q}_p^{\mathrm{ur}}}$ is the completion of the maximal unramified extension of $\mathbf{Q}_p$

(so $I_p = \mathrm{Gal}(\overline{K}/K)$). Let $\mathcal{O} = \mathcal{O}_K \left(= \widehat{\mathbf{Z}_p^{\mathrm{ur}}}\right)$ and $k = \mathcal{O}/p = \overline{\mathbf{F}_p}$. Let $\Lambda = \mathbf{Z}/\ell$ or $\mathbf{Q}_\ell$ be the coefficient ring.

Recall the wild inertia subgroup $P \subseteq I$ is defined as $P = \mathrm{Gal}(\overline{K}/K^t)$ where $K^t = \bigcup_{p\nmid n} K(p^{1/n})$ is the maximal tamely ramified extension of K. Then $I/P \simeq \prod_{\ell \neq p} \mathbf{Z}_\ell(1)$.

$$\begin{tikzcd}
\mathbf{Q}_p \arrow[r, dash] & K \arrow[r, dash] \arrow[rr, dash, bend left, "I"] & K^t \arrow[r, dash, bend left] \arrow[r, dash, bend right, "P"'] & \overline{K}
\end{tikzcd}$$

Definition 14.1. Define the *tame ℓ-adic character* to be the map $t : I \to \mathbf{Z}_\ell(1)$ given by

$$\sigma \mapsto \left\{ \frac{\sigma(p^{1/\ell^m})}{p^{1/\ell^m}} \right\} \in \{\mu_{\ell^m}\}_{m\geq 1} = \mathbf{Z}_\ell(1).$$

Theorem 14.2 (Grothendieck)**.** *Let $V = H^i_{(\text{ét})}(X_{\overline{K}}, \Lambda)$ with $\Lambda = \mathbf{Q}_\ell$, which has an action of $I = \mathrm{Gal}(\overline{K}/K)$. Then there exists an open subgroup $J \subseteq I$ and a nilpotent matrix $N : V(1) \to V$ such that for all $\sigma \in J$, the action of σ on V is given by* $\exp(t(\sigma)N)$ *(hence unipotent).*

Definition 14.3. The operator N is called the *monodromy* operator.

Remark. The geometric analogue is

$$\begin{tikzcd}
\mathbf{Z}_\ell(1) & I = \mathrm{Gal}(\overline{K}/K) \arrow[l] \arrow[d, leftrightarrow] \\
& \pi_1(D - \{0\}) \simeq \mathbf{Z} \arrow[ul, leftrightarrow]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Spec}\, k \arrow[r, hook] & \mathrm{Spec}\, \mathcal{O} & \mathrm{Spec}\, K \arrow[l, hook'] \\
\{z = 0\} & D = \{|z| < 1\} & D - \{0\} \\
\text{point} & \text{disk} & \text{punctured disk}
\end{tikzcd}$$

After going around a loop in $\mathrm{Spec}\, K$, we get an automorphism of $H^i(X_{\overline{K}}, \Lambda)$ (monodromy in geometry).

Example 14.4. Let $X/\mathbf{Q}_p$ be an elliptic curve with multiplicative reduction. Then by Tate's uniformization theorem, the action of $\sigma \in I$ on $V = H^1(X_{\overline{K}}, \Lambda)$ (or $T_\ell X$) is given by

$$\begin{pmatrix} 1 & t(\sigma) \\ & 1 \end{pmatrix} = \exp \begin{pmatrix} 0 & t(\sigma) \\ & 0 \end{pmatrix},$$

so $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

14.2. **Nearby cycle sheaves and monodromy filtration.** Our goal is to describe $H^i(X_{\overline{K}}, \Lambda)$ and N using the geometry of $X_k = X_{\overline{\mathbf{F}_p}}$. Let $X_{\mathcal{O}}$ be a proper integral model of X_K.

$$\begin{tikzcd}
X_k \arrow[r, hook, "i"] \arrow[d] & X_{\mathcal{O}} \arrow[d] & X_{\overline{K}} \arrow[l, hook', "j"'] \arrow[d] \\
\mathrm{Spec}\, k \arrow[r, hook] & \mathrm{Spec}\, \mathcal{O} & \mathrm{Spec}\, \overline{K} \arrow[l, hook']
\end{tikzcd}$$

Definition 14.5. The *nearby cycle sheaf* is

$$R\Psi\Lambda := i^* Rj_* \Lambda \in \mathcal{D}(X_k).$$

Then

$$\begin{aligned} H^i(X_{\overline{K}},\Lambda) &= H^i(X_{\mathcal{O}}, Rj_*\Lambda) \quad \text{(for any map } j\text{)} \\ &= H^i(X_k, i^*Rj_*\Lambda) \quad \text{(proper base change)} \\ &= H^i(X_k, R\Psi\Lambda), \end{aligned}$$

so the slogan is

cohomology of generic fiber = cohomology of special fiber for nearby cycle sheaf.

Thus the nearby cycle sheaf sees the cohomology of "nearby" fibers.

Example 14.6. If $X_{\mathcal{O}} \to \operatorname{Spec} \mathcal{O}$ is smooth, then $R\Psi\Lambda \cong \Lambda$ and $H^i(X_{\overline{K}},\Lambda) \simeq H^i(X_k,\Lambda)$. In this case, $N = 0$ (unramified).

In general, there is an action

$$N : R\Psi\Lambda(1) \to R\Psi\Lambda$$

which is nilpotent. More precisely, $N^{n+1} = 0$ for $n = \dim X$.

Definition 14.7.

(1) The *kernel filtration* is given by $F_i := \ker N^{i+1}$:

$$0 \subseteq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = R\Psi\Lambda.$$

(2) The *image filtration* is given by $G^j := \operatorname{im} N^j$:

$$R\Psi\Lambda \supseteq G^1 \supseteq G^2 \supseteq \cdots \supseteq G^n \supseteq 0.$$

(3) The *monodromy filtration* is given by $M_r := \sum_{i-j=r} F_i \cap G^j$:

$$0 \subseteq M_{-n} \subseteq \cdots \subseteq M_n \subseteq R\Psi\Lambda.$$

The monodromy filtration is characterized by the properties:

(1) $N(M_r(1)) \subseteq M_{r-2}$.
(2) $N^r : \operatorname{gr}^M_r R\Psi\Lambda(r) \xrightarrow{\sim} \operatorname{gr}^M_{-r} R\Psi\Lambda$ is an isomorphism, where $\operatorname{gr}^M_r = M_r/M_{r-1}$.

14.3. Rapoport–Zink weight spectral sequence.

Definition 14.8. $X_{\mathcal{O}}$ is *semistable* if

(1) $X_{\mathcal{O}}$ is regular and flat over $\mathcal{O}$.
(2) X_k is a divisor of $X_{\mathcal{O}}$ with normal crossings, i.e., its singularities are given by $\mathcal{O}[x_1, \cdots, x_n]/(x_1 \cdots x_s - p)$ for some $s \leq n$.

We further say that $X_{\mathcal{O}}$ is *strictly semistable* if

(3) all irreducible components of X_k are smooth ("simple" normal crossings).

For example, the nodal curve is semistable, but not strictly semistable. The union of two curves intersecting transversally is strictly semistable.

Definition 14.9. Assume $X_{\mathcal{O}}$ is strictly semistable. Then $X_k = X_1 \cup \cdots \cup X_m$ where each X_i is a smooth irreducible component (of codimension 1 in $X_{\mathcal{O}}$). Define for any subset $J \subseteq \{1, \cdots, m\}$,

$$X_J := \bigcap_{i \in J} X_i.$$

For any $p \geq 0$, let

$$X^{(p)} := \coprod_{\substack{J \subseteq \{1, \cdots, m\} \\ |J| = p+1}} X_J,$$

which is a smooth projective variety over k of codimension p in X_k.

For any $p \geq 0$, we have

- pullback: $H^q(X^{(p)}, \Lambda) \to H^q(X^{(p+1)}, \Lambda)$,
- pushforward: $H^q(X^{(p)}, \Lambda)(-1) \to H^{q+2}(X^{(p-1)}, \Lambda)$.

Theorem 14.10 (Rapoport–Zink, Saito). *Assume $X_{\mathcal{O}}$ is strictly semistable. Then we have a spectral sequence*

$$E_1^{p,q} = H^{p+q}(X_k, \mathrm{gr}^M_{-p} R\Psi\Lambda) \Rightarrow H^{p+q}(X_{\overline{K}}, \Lambda),$$

which degenerates at E_2 if $\Lambda = \mathbf{Q}_\ell$. Moreover,

$$E_1^{p,q} = \bigoplus_{\substack{i \geq 0 \\ i \geq -p}} H^{q-2i}(X^{(p+2i)}, \Lambda)(-i)$$

where the differentials on E_1 are sums of pushforwards and pullbacks, and $N : E_1^{p,q} \to E_1^{p+2,q-2}$ is given by $\otimes t$.

Remark. The terminology of "weight" spectral sequence comes from the

Conjecture 14.11 (Weight monodromy). *Let $\Lambda = \mathbf{Q}_\ell$. Then $\mathrm{gr}^M_{-r} H^i(X_{\overline{K}}, \Lambda)$ is pure of weight $i + r$ (i.e., the action of Fr_p has eigenvalues of absolute value $p^{\frac{i+r}{2}}$).*

15. Lecture 15 (November 7, 2018)

16. Lecture 16 (November 12, 2018)

17. Lecture 17 (November 14, 2018)

18. Lecture 18 (November 19, 2018)

18.0. **Rankin–Selberg L-functions for $\mathrm{GL}_n \times \mathrm{GL}_{n-1}$.** As a motivation, recall that the way we proved the rank part of BSD is by going through

$$L(E, s) = L(f, s).$$

- The left-hand side is a special case of a "motivic L-function" $L(\rho_E, s)$, where ρ_E is the motive associated to E.
- The right-hand side is an "automorphic L-function" $L(\pi, s)$, where π is an automorphic representation on $\mathrm{GL}_2(\mathbf{A})$ associated to $f \in \pi$.

The global Langlands correspondence states that every motivic L-function arises as an automorphic L-function. In this way, arithmetic questions about motives (e.g. counting points on algebraic varieties) can be studied using analytic properties of automorphic representations, which are often easier.

Our goal is to study generalizations to the arithmetic of $L(s, \pi \times \pi')$, where π (resp. π') is a cuspidal automorphic representation on $\mathrm{GL}_n(\mathbf{A})$ (resp. $\mathrm{GL}_{n-1}(\mathbf{A})$), for $\mathbf{A} = \mathbf{A}_K$ the ring of adeles of a number field $K/\mathbf{Q}$.

Example 18.1. Let $n = 2$. Taking π to be the automorphic representation corresponding to f and π' to be the trivial representation gives $L(f, s)$.

Today we will define $L(s, \pi \times \pi')$ and state its basic properties. Similarly to the case of the Riemann zeta function, the three basic properties are analytic continuation, functional equation, and Euler product (which relates to the problem of counting points on varieties). The study follows the template of Tate's thesis.

18.1. **Global zeta integrals.**

Definition 18.2 (Global zeta integrals)**.** Let $f \in \pi$ and $\varphi \in \pi'$. Define

$$Z(f, \varphi, s) := \int_{[\mathrm{GL}_{n-1}]} f\begin{pmatrix} g & \\ & 1 \end{pmatrix} \varphi(g) |\det g|^{s-\frac{1}{2}}\, dg,$$

where $[\mathrm{GL}_{n-1}] = \mathrm{GL}_{n-1}(K)\backslash\mathrm{GL}_{n-1}(\mathbf{A})$.

Example 18.3. Let $n = 2$, and $f \in S_2^{\mathrm{new}}(N)$. Recall the L-function

$$L(f, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p L_p(f, s)$$

and the completed L-function

$$\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s) = \int_0^\infty f(it)t^s\, \frac{dt}{t}.$$

Let us rewrite this in adelic language. Every point $x + iy \in \mathcal{H}$ corresponds to $\begin{pmatrix} y & x \\ & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{R})$, and f corresponds to $f\begin{pmatrix} y & \\ & 1 \end{pmatrix} = f(iy)y$. Then $\Lambda(f, s)$ generalizes to

$$\int_{[\mathrm{GL}_1]} f\begin{pmatrix} y & \\ & 1 \end{pmatrix} |y|^{s-1}\, dy,$$

so that $L(f, s) = Z(f, \mathbb{1}, s + \frac{1}{2})$.

The basic properties of the global zeta integrals are summarized in the

Theorem 18.4 (Properties of global zeta integrals)**.**

1. *$Z(f, \varphi, s)$ converges to an analytic function on $s \in \mathbf{C}$.*
2. *$Z(f, \varphi, s)$ satisfies a functional equation*
$$Z(f, \varphi, s) = Z(\widetilde{f}, \widetilde{\varphi}, 1 - s),$$
where $\widetilde{f}(g) = f({}^t g^{-1})$ and similarly for $\widetilde{\varphi}$.
3. *Suppose $f = \bigotimes f_v \in \pi = \bigotimes_v \pi_v$ and $\varphi = \bigotimes \varphi_v \in \pi' = \bigotimes_v \pi'_v$. Then $Z(f, \varphi, s)$ has an Euler product*
$$Z(f, \varphi, s) = \prod_v Z_v(f_v, \varphi_v, s)$$
where Z_v is to be defined.

Sketch of proof.

1. This is clear, since f is a cusp form and hence rapidly-decreasing along cusps.

(2) Use the automorphism $g \mapsto {}^t g^{-1}$.

(3) Euler product uses the uniqueness of Whittaker models, which will be explained in the following. □

Before defining the Whittaker models, we need to introduce the Whittaker(–Fourier) expansion. Fix an additive character $\psi : K\backslash\mathbf{A} \to \mathbf{C}^\times$.

Definition 18.5. For $f \in \pi$, define

$$W_f(g) = \int_{[N_n]} f(ng)\psi^{-1}(n)\,dn,$$

where N_n is the maximal unipotent subgroup of GL_n consisting of all the upper-triangular unipotent matrices, and

$$\psi\begin{pmatrix} 1 & x_{12} & & * \\ & 1 & x_{23} & \\ & & \ddots & x_{n-1,x} \\ & & & 1 \end{pmatrix} = \psi(x_{12} + x_{23} + \cdots + x_{n-1,n}).$$

Theorem 18.6 (Jacquet, Piatetski-Shapiro, Shalika)**.**

$$f(g) = \sum_{\gamma \in N_{n-1}(K)\backslash \mathrm{GL}_{n-1}(K)} W_f\left(\begin{pmatrix} \gamma & \\ & 1 \end{pmatrix} g\right).$$

Example 18.7. For $n = 2$,

$$W_f(g) = \int_{[\mathbf{G}_a]} f\left(\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} g\right)\psi^{-1}(x)\,dx$$

is the familiar Fourier coefficient, and

$$\begin{aligned} f(g) &= \sum_{\gamma \in K^\times} W_f\left(\begin{pmatrix} \gamma & \\ & 1 \end{pmatrix} g\right) \\ &= \sum_{\gamma \in K^\times} W_{f,\psi_\gamma}(g) \end{aligned}$$

where $\psi_\gamma(x) = \psi(\gamma x)$. Here $W_{f,\psi_\gamma}(g)$ is the generalization of $a_n \cdot q^n$.

Remark. If $n > 2$, difficulty for the theorem arises because N_{n-1} is not abelian. One has to carry out a subtle induction on n.

Now we define the Whittaker model.

Definition 18.8. Let

$$\mathrm{Ind}_{N_n}^{\mathrm{GL}_n}(\psi) = \{W \in C^\infty(\mathrm{GL}_n(\mathbf{A})) : W(ng) = \psi(n)W(g), n \in N_n(\mathbf{A}), g \in \mathrm{GL}_n(\mathbf{A})\},$$

called the space of *(global) Whittaker functions.*

By definition, $W_f(g) \in \mathrm{Ind}_{N_n}^{\mathrm{GL}_n}(\psi)$.

Definition 18.9. The *(global) Whittaker model* is

$$W(\pi, \psi) = \{W_f(g) : f \in \pi\}.$$

We have a $\mathrm{GL}_n(\mathbf{A})$-equivariant map

$$\begin{aligned}\pi &\to W(\pi,\psi)\\ f &\mapsto W_f.\end{aligned}$$

This provides a way of understanding automorphic representations in terms of concrete functions.

Now we can use Whittaker functions to prove the Euler product; this technique is called "unfolding".

$$\begin{aligned}
Z(f,\varphi,s) &= \int_{[\mathrm{GL}_{n-1}]} f\begin{pmatrix} g & \\ & 1\end{pmatrix}\varphi(g)|\det g|^{s-\frac{1}{2}}\,dg\\
&= \int_{[\mathrm{GL}_{n-1}]}\left(\sum_{\gamma\in N_{n-1}(K)\backslash \mathrm{GL}_{n-1}(K)} W_f\left(\begin{pmatrix}\gamma & \\ & 1\end{pmatrix}\begin{pmatrix} g & \\ & 1\end{pmatrix}\right)\right)\varphi(g)|\det g|^{s-\frac{1}{2}}\,dg\\
&= \int_{N_{n-1}(K)\backslash \mathrm{GL}_{n-1}(\mathbf{A})} W_f\begin{pmatrix} g & \\ & 1\end{pmatrix}\varphi(g)|\det g|^{s-\frac{1}{2}}\,dg\\
&= \int_{N_{n-1}(\mathbf{A})\backslash \mathrm{GL}_{n-1}(\mathbf{A})} W_f\begin{pmatrix} g & \\ & 1\end{pmatrix}W_\varphi(g)|\det g|^{s-\frac{1}{2}}\,dg,
\end{aligned}$$

where the last step is by the property of Whittaker functions. Note that $N_{n-1}(\mathbf{A})\backslash\mathrm{GL}_{n-1}(\mathbf{A})$ is factorizable!

Analogous to the global situation, we make the following definitions.

Definition 18.10. Let

$$\mathrm{Ind}_{N_n}^{\mathrm{GL}_n}(\psi_v) = \{W\in C^\infty(\mathrm{GL}_n(K_v)) : W(ng)=\psi_v(n)W(g), n\in N_n(K_v), g\in\mathrm{GL}_n(K_v)\}$$

be the space of *local Whittaker functions.*

Definition 18.11. A *local Whittaker model* is a nontrivial $\mathrm{GL}_n(K_v)$-equivariant map

$$\pi_v \to \mathrm{Ind}_{N_n}^{\mathrm{GL}_n}(\psi_v),$$

i.e., a nonzero element in $\mathrm{Hom}_{\mathrm{GL}_n(K_v)}(\pi_v, \mathrm{Ind}_{N_n}^{\mathrm{GL}_n}(\psi_v))$.

Theorem 18.12 (Uniqueness of local Whittaker model: Gelfand–Kazhdan)**.** *Let π_v be a smooth irreducible admissible representation of $\mathrm{GL}_n(K_v)$. Fix a nontrivial additive character $\psi_v : K_v\to\mathbf{C}^\times$. Then*

$$\dim \mathrm{Hom}_{\mathrm{GL}_n(K_v)}(\pi_v, \mathrm{Ind}_{N_n}^{\mathrm{GL}_n}(\psi_v)) \le 1.$$

The proof uses Bessel distributions.

As a consequence, if $f=\bigotimes f_v$ is factorizable, then

$$W_f(g) = \prod_v W_{f_v}(g_v).$$

Definition 18.13 (Local zeta integrals)**.**

$$Z_v(f_v,\varphi_v,s) := \int_{N_{n-1}(K_v)\backslash \mathrm{GL}_{n-1}(K_v)} W_{f_v}\begin{pmatrix} g_v & \\ & 1\end{pmatrix} W_{\varphi_v}(g_v)|\det g_v|^{s-\frac{1}{2}}\,dg_v.$$

Corollary 18.14.

$$Z(f,\varphi,s)=\prod_v Z_v(f_v,\varphi_v,s).$$

18.2. **Relation between $Z(f,\varphi,s)$ and $L(s,\pi\times\pi')$.**

Theorem 18.15 (Properties of local zeta integrals)**.**

1. *$Z_v(f_v,\varphi_v,s)$ converges for $\operatorname{Re} s\gg 0$.*
2. *$Z_v(f_v,\varphi_v,s)\in \mathbf{C}(q^{-s})$ and hence has meromorphic continuation to $\mathbf{C}$.*
3. *$\{Z_v(f_v,\varphi_v,s) : f_v\in\pi_v,\varphi_v\in\pi'_v\}$ is a $\mathbf{C}[q^{\pm s}]$-ideal in $\mathbf{C}(q^{-s})$ and hence has a generator $P_{\pi_v,\pi'_v}(q^{-s})^{-1}$, where $P\in\mathbf{C}[X]$ and $P(0)=1$.*

Definition 18.16. Define the local L-factor to be

$$L(\pi_v\times\pi'_v,s):=P_{\pi_v,\pi'_v}(q^{-s})^{-1}.$$

Theorem 18.17 (Local functional equation)**.**

$$Z_v(f_v,\varphi_v,s)=\omega_{\pi'}(-1)^{n-1}\gamma(s,\pi_v\times\pi'_v,\psi_v)\cdot Z_v(\widetilde{f_v},\widetilde{\varphi_v},1-s),$$

where $\gamma(s,\pi_v\times\pi'_v,\psi_v)$ is defined using the uniqueness of local Whittaker models.

Definition 18.18.

$$\epsilon(s,\pi_v\times\pi'_v,\psi_v):=\gamma(s,\pi_v\times\pi'_v,\psi_v)\cdot\frac{L(s,\pi_v\times\pi'_v)}{L(1-s,\widetilde{\pi}_v\times\widetilde{\pi}'_v)}.$$

18.3. **Global L-functions.**

Definition 18.19.

$$\begin{aligned}L(s,\pi\times\pi')&=\prod_{v\nmid\infty}L(s,\pi_v\times\pi'_v),\\ \Lambda(s,\pi\times\pi')&=\prod_v L(s,\pi_v\times\pi'_v),\\ \epsilon(s,\pi\times\pi')&=\prod_v\epsilon(s,\pi_v\times\pi'_v,\psi_v).\end{aligned}$$

By the product formula, $\epsilon(s,\pi\times\pi')$ is independent of the choice of ψ.

Theorem 18.20.

1. *$L(s,\pi\times\pi')$ has analytic continuation to $\mathbf{C}$.*
2. *There is a functional equation*

$$\Lambda(s,\pi\times\pi')=\epsilon(s,\pi\times\pi')\Lambda(s,\widetilde{\pi}\times\widetilde{\pi}').$$

The proof uses $Z(f,\varphi,s)$ and $Z_v(f_v,\varphi_v,s)$.

19. Lecture 19 (November 26, 2018)

19.1. **General Waldspurger formula.** Recall the Waldspurger hypothesis: let $E/\mathbf{Q}$ be an elliptic curve, and $K/\mathbf{Q}$ be an imaginary quadratic field satisfying

$$\#\{p \mid N : p \text{ inert in } K\} \text{ is odd, i.e., } \#\{p \mid N^-\} \text{ is odd.} \tag{Wald}$$

Thus (Wald) implies that $\epsilon(E_K) = +1$. The Waldspurger formula states that

$$\frac{L(E_K, 1)}{(f, f)} = \frac{1}{|d_K|^{1/2}} \cdot \frac{|y_K|^2}{\deg \varphi},$$

where y_K is a toric period on a certain definite quaternion algebra and φ is the modular parametrization of E. As a consequence, $L(E_K, 1) \neq 0$ if and only if $y_K \neq 0$. This is crucial in proving $r_{\text{an}}(E) = 0 \implies r_{\text{alg}}(E) = 0$.

This formula is actually much more general. Notice that under the association

$$\begin{aligned} \text{elliptic curve } E &\rightsquigarrow \text{newform } f \in S_2^{\text{new}}(N) \\ &\rightsquigarrow \begin{array}{l}\text{automorphic representation } \pi \text{ on } \mathrm{GL}_2(\mathbf{A}) \\ \text{(with central character),}\end{array} \end{aligned}$$

we have

$$L(E_K, s) \sim L(\pi_K, s) = L(\pi_K \otimes \mathbb{1}_K, s)$$

where $\mathbb{1}_K : K^\times \backslash \mathbf{A}^\times \to \mathbf{C}^\times$ is the trivial character, and $\sim$ means the L-functions differ by a shift.

In general, take a number field F with ring of adeles $\mathbf{A} = \mathbf{A}_F$, a quadratic extension K/F, a quaternion algebra B/F (including $M_2(F)$), a cuspidal automorphic representation π on $G := B^\times/F^\times$, and a character χ on $H := K^\times/F^\times$. Then an embedding $K \hookrightarrow B$ induces an embedding $H \hookrightarrow G$ (as algebraic groups over F).

Now we are ready to generalize the toric period y_K:

Definition 19.1. The *automorphic H-period* is defined to be

$$\wp_H(f) := \int_{[H]} f(h)\chi(h)\, dh \in \mathbf{C}$$

for $f \in \pi$, where $[H] = H(F)\backslash H(\mathbf{A}_F)$.

Notice $\wp_H : f \mapsto \wp_H(f)$ defines a linear functional

$$\wp_H \in \mathrm{Hom}_{H(\mathbf{A})}(\pi \otimes \chi, \mathbf{C}) = \prod_v{}' \mathrm{Hom}_{H(F_v)}(\pi_v \otimes \chi_v, \mathbf{C}).$$

Theorem 19.2 (Tunnell, Saito)**.**

(1) *(Multiplicity one)*

$$\dim \mathrm{Hom}_{H(F_v)}(\pi_v \otimes \chi_v, \mathbf{C}) \leq 1.$$

(2) *(ϵ-dichotomy) Let $G^0(F_v) = \mathrm{PGL}_2(F_v)$ and $G^1(F_v) = B_v^\times/F_v^\times$. Suppose π_v^0 is an irreducible representation of $G^0(F_v)$, and $\pi_v^1 = \mathrm{JL}(\pi_v^0)$ is its Jacquet–Langlands transfer to $G^1(F_v)$ (which is nonzero only when π_v^0 is discrete series). Then*

$$\dim \mathrm{Hom}_{H(F_v)}(\pi_v^0 \otimes \chi_v, \mathbf{C}) + \dim \mathrm{Hom}_{H(F_v)}(\pi_v^1 \otimes \chi_v, \mathbf{C}) = 1.$$

Moreover, $\mathrm{Hom}_{H(F_v)}(\pi_v^0 \otimes \chi_v, \mathbf{C}) \neq 0$ *if and only if the local root number*

$$\epsilon\left(\frac{1}{2}, \pi_v^0 \otimes \chi_v\right) = \chi_v(-1)\eta_v(-1),$$

where $\eta = \eta_{K/F}$*.*

Example 19.3. Let π be an automorphic representation coming from an elliptic curve $E/\mathbf{Q}$, and $\chi = \mathbb{1}_K$. Then

$$\epsilon\left(\frac{1}{2}, \pi_v \otimes \chi_v\right) = \epsilon_v(E/K).$$

There are two cases:

- If $v \nmid N$, then $\epsilon_v(E/K) = +1$ and $\pi_v^1 = 0$. These imply $\dim \mathrm{Hom}_{H(F_v)}(\pi_v^0 \otimes \chi_v, \mathbf{C}) = 1$.
- If $v \mid N$, then

$$\epsilon_v(E/K) = \begin{cases} +1 & \text{if } v \text{ splits in } K, \\ (-1)^{\mathrm{ord}_v N} & \text{if } v \text{ is inert in } K. \end{cases}$$

  Moreover, $\chi_v(-1) = +1$ and $\eta_v(-1) = +1$ (as $v \nmid d_K$). So $\dim \mathrm{Hom}_{H(F_v)}(\pi_v^0 \otimes \chi_v, \mathbf{C}) = 1$ when $v \mid N^+$, and $\dim \mathrm{Hom}_{H(F_v)}(\pi_v^1 \otimes \chi_v, \mathbf{C}) = 1$ when $v \mid N^-$.

Thus (Wald) implies

$$\dim \mathrm{Hom}_{H(\mathbf{A})}(\pi \otimes \chi, \mathbf{C}) = 1.$$

This is the representation-theoretic interpretation of the Waldspurger condition.

Theorem 19.4 (Waldspurger's nonvanishing criterion)**.** *The following are equivalent:*

1. $\wp_H \neq 0$.
2. $\mathrm{Hom}_{H(\mathbf{A})}(\pi \otimes \chi) \neq 0$ *and* $L(\pi \otimes \chi, \frac{1}{2}) \neq 0$.

This is enough for the rank part of BSD. Indeed, Waldspurger also proves a refined formula for $L(\pi \otimes \chi, \frac{1}{2})$ in terms of the period $\wp_H$. One constructs a canonical element

$$\alpha_v \in \mathrm{Hom}_{H(F_v)}(\pi_v \otimes \chi_v, \mathbf{C}) \otimes \mathrm{Hom}_{H(F_v)}(\widetilde{\pi}_v \otimes \widetilde{\chi}_v, \mathbf{C})$$

using matrix coefficients: for $f \in \pi_v$ and $\widetilde{f} \in \widetilde{\pi}_v$,

$$\alpha_v(f, \widetilde{f}) := \int_{H(F_v)} \langle \pi_v(h) f, \widetilde{f} \rangle \chi_v(f)\, dh.$$

Remark. If π_v is unramified and $f, \widetilde{f}$ are spherical such that $\langle f, \widetilde{f} \rangle = 1$, then

$$\alpha_v(f, \widetilde{f}) = \frac{\zeta_{F_v}(2) L(\frac{1}{2}, \pi_v \otimes \chi_v)}{L(1, \eta_v) L(1, \pi_v, \mathrm{Ad})} =: \mathcal{L}_v\left(\frac{1}{2}, \pi \otimes \chi\right).$$

Theorem 19.5 (Waldspurger formula)**.** *Let* $f = \bigotimes f_v \in \pi$ *and* $\widetilde{f} = \bigotimes \widetilde{f}_v \in \widetilde{\pi}$*. Then*

$$\frac{\wp_H(f)\wp_H(\widetilde{f})}{(f, \widetilde{f})} = \frac{1}{4} \cdot \underbrace{\frac{\zeta_F(2) L(\frac{1}{2}, \pi \otimes \chi)}{L(1, \eta) L(1, \pi, \mathrm{Ad})}}_{\mathcal{L}(\frac{1}{2}, \pi \otimes \chi)} \cdot \prod_v \frac{\alpha_v(f_v, \widetilde{f}_v)}{\mathcal{L}(\frac{1}{2}, \pi_v \otimes \chi_v) \cdot (f_v, \widetilde{f}_v)}.$$

Remark. $L(\frac{1}{2}, \pi \otimes \chi)$ may be thought of as the ratio of $\wp_H(f)\wp_H(\widetilde{f})$ by "$\prod_v \alpha_v(f_v, \widetilde{f}_v)$" in a 1-dimensional space!

19.2. **Gan–Gross–Prasad conjectures.** In the situation of the Waldspurger formula, $G = \mathrm{PGL}_2 \cong \mathrm{SO}_3$ and $H = K^\times/F^\times \cong \mathrm{SO}_2$. The Gan–Gross–Prasad conjectures generalize this to many pairs of classical groups.

The case of interest to us is as follows. Let $G = \mathrm{U}_n = \mathrm{U}(V)$ and $H = \mathrm{U}_{n-1} = \mathrm{U}(W)$, where V (resp. W) is a hermitian space of dimension n (resp. $n-1$) with respect to a quadratic extension K/F. Assume $V = W \perp K \cdot u$ where $(u,u) = 1$, so that $H \hookrightarrow G$ via $g \mapsto \begin{pmatrix} g & \\ & 1 \end{pmatrix}$.

Let π (resp. π') be a cuspidal tempererd automorphic representation on G (resp. H). Our goal is to relate

$$L\left(\frac{1}{2}, \pi_K \times \pi'_K\right) \longleftrightarrow \text{automorphic } H\text{-period } \wp_H,$$

where $L(s, \pi_K \times \pi'_K)$ is the Rankin–Selberg L-function for $\mathrm{GL}_n \times \mathrm{GL}_{n-1}$ from last time.

Conjecture 19.6 (Gan–Gross–Prasad)**.** *Write* $\Pi = \pi \times \pi'$.

(1) *(Multiplicity one)*

$$\dim \mathrm{Hom}_{H(F_v)}(\Pi_v, \mathbf{C}) \leq 1.$$

(2) *(ϵ-dichotomy)*

$$\sum_{(H^i, \Pi'_v)} \dim \mathrm{Hom}_{H^i(F_v)}(\Pi'_v, \mathbf{C}) = 1,$$

where (H^i, Π'_v) runs over the Vogan L-packet of Π_v*. Moreover, there is a description in terms of* $\epsilon(\Pi_v)$*.*

(3) *(Nonvanishing) The following are equivalent:*
   (a) $\wp_H \neq 0$.
   (b) $\mathrm{Hom}_{H(\mathbf{A})}(\Pi, \mathbf{C}) \neq 0$ *and* $L(\frac{1}{2}, \Pi) \neq 0$.

(4) *(Ichino–Ikeda formula) Let $f \in \Pi$ and $f' \in \widetilde{\Pi}$. Then*

$$\frac{\wp_H(f)\wp_H(\widetilde{f})}{(f, \widetilde{f})} = \frac{1}{|S_\Pi|} \cdot \mathcal{L}\left(\frac{1}{2}, \Pi\right) \cdot \prod_v \frac{\alpha_v(f_v, \widetilde{f_v})}{\mathcal{L}(\frac{1}{2}, \Pi_v)(f_v, \widetilde{f_v})}$$

where S_Π is the component group of the L-parameter of Π*.*

These are all known:

(1) by Aizenbud–Gourevitch–Rallis–Schiffman for $v \nmid \infty$, and by Sun–Zhu for $v \mid \infty$;
(2) by Beuzart-Plessis;
(3) by W. Zhang, Jacquet–Rallis, Z. Yun, H. Xue, Chaudouard–Zydor;
(4) by W. Zhang, Beuzart-Plessis.

20. Lecture 20 (November 28, 2018)

20.1. **Bloch–Kato Selmer groups.** As motivation, recall that for an elliptic curve $E/\mathbf{Q}$ we have defined the p-Selmer group

$$\mathrm{Sel}_p(E) \subseteq H^1(\mathbf{Q}, E[p]),$$

which sits in a short exact sequence

$$0 \to \frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \to \mathrm{Sel}_p(E) \to Ш(E)[p] \to 0.$$

$\mathrm{Sel}_p(E)$ is cut by *local* conditions: at v of $\mathbf{Q}$,

$$\mathrm{im}\left(\delta_v : \frac{E(\mathbf{Q})}{pE(\mathbf{Q})} \to H^1(\mathbf{Q}_v, E[p])\right).$$

More generally, we have the p^∞-Selmer group

$$\mathrm{Sel}_{p^\infty}(E) := \varinjlim \mathrm{Sel}_{p^n}(E) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{r_p} \times \text{finite}$$

and the $\mathbf{Q}_p$-Selmer group

$$\mathrm{Sel}_{\mathbf{Q}_p}(E) := \varprojlim \mathrm{Sel}_{p^n}(E) \otimes \mathbf{Q}_p = \mathbf{Q}_p^{r_p}.$$

Our goal is to define an analogue of $\mathrm{Sel}_{\mathbf{Q}_p}(E)$ for more general Galois representations $\rho : G_K \to \mathrm{Aut}(V)$ on finite-dimensional $\mathbf{Q}_p$-vector spaces V. This will be the Bloch–Kato Selmer group $H^1_f(K, V)$.

Remark. In the case of elliptic curves, $V = V_pE$ is the rational Tate module. In particular, $\mathrm{Sel}_{\mathbf{Q}_p}(E)$ is invariant under isogenies of E.

Let K be a number field.

Definition 20.1. A p-adic Galois representation $\rho : G_K \to \mathrm{Aut}(V)$ *comes from geometry* if V is a subquotient of $H^i(X_{\overline{K}}, \mathbf{Q}_p)(n)$ for some i, n, and smooth projective variety X/K.

Remark. Let K be a v-adic local field.

(1) If $v \nmid p$ and X/K has good reduction, then $H^i(X, \mathbf{Q}_p)$ is *unramified* as a G_K-representation.
(2) If $v \mid p$, then $H^i(X, \mathbf{Q}_p)$ is *de Rham* as a G_K-representation.

To define de Rham representation, we recall the p-adic comparison theorem.

Theorem 20.2 (Faltings)**.**

$$H^i(X, \mathbf{Q}_p) \otimes_{\mathbf{Q}_p} B_{\mathrm{dR}} \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/K) \otimes_K B_{\mathrm{dR}},$$

where B_{dR} is Fontaine's p-adic period ring.

Using $B_{\mathrm{dR}}^{G_K} = K$, we know that

$$(H^i(X, \mathbf{Q}_p) \otimes_{\mathbf{Q}_p} B_{\mathrm{dR}})^{G_K} \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/K).$$

Definition 20.3. Define

$$D_{\mathrm{dR}}(V) := (V \otimes_{\mathbf{Q}_p} B_{\mathrm{dR}})^{G_K}.$$

Say V is *de Rham* if $\dim_K D_{\mathrm{dR}}(V) = \dim_{\mathbf{Q}_p} V$.

Returning to the global situation where K is a number field, we make the

Definition 20.4. V is *geometric* if

(1) V is unramified at almost all places v.
(2) V is de Rham at $v \mid p$.

So V comes from geometry $\implies$ V is geometric. The converse is conjecturally true, so the condition of V being geometric provides a working definition.

Conjecture 20.5 (Fontaine–Mazur)**.** *V comes from geometry if and only if V is geometric.*

Remark. If $v \mid p$ and X/K has good reduction, then $H^i(X, \mathbf{Q}_p)$ is *crystalline* at v (defined analogously using B_{crys} instead of B_{dR}).

Theorem 20.6 (Faltings)**.**

$$H^i(X, \mathbf{Q}_p) \otimes_{\mathbf{Q}_p} B_{\mathrm{crys}} \xrightarrow{\sim} H^i_{\mathrm{crys}}(X_k/W(k)) \otimes_{W(k)} B_{\mathrm{dR}},$$

where k is the residue field of K and $W(k)$ is the Witt ring of k.

Using $B_{\mathrm{crys}}^{G_K} = W(k)[\frac{1}{p}]$, the notion of crystalline representations is defined similarly. Now we are ready to define the local conditions for Bloch–Kato Selmer groups.

Definition 20.7 (Local conditions)**.** Define $H^1_f(K_v, V) \subseteq H^1(K_v, V)$ as follows:

(1) If $v \nmid p$, define the *unramified* subspace

$$H^1_f(K_v, V) := H^1(k_v, V^{I_v}) = \ker\left(H^1(K_v, V) \to H^1(I_v, V)^{\mathrm{Fr}_v = 1}\right).$$

(2) If $v \mid p$, define the *finite* subspace

$$H^1_f(K_v, V) := \ker\left(H^1(K_v, V) \to H^1(K_v, V \otimes_{\mathbf{Q}_p} B_{\mathrm{crys}})\right).$$

Similarly to the case of elliptic curves, they satisfy the following properties:

(1) If $v \nmid p$, then

$$\dim H^1_f(K_v, V) = \dim H^0(K_v, V).$$

Also, local duality works: under the local Tate pairing

$$(\cdot, \cdot)_v : H^1(K_v, V) \times H^1(K_v, V^*(1)) \to H^2(K_v, \mathbf{Q}_p(1)) \simeq \mathbf{Q}_p,$$

$H^1_f(K_v, V)$ and $H^1_f(K_v, V^*(1))$ are exact annihilators.

(2) If $v \mid p$, then

$$\dim_{\mathbf{Q}_p} H^1_f(K_v, V) = \dim_{\mathbf{Q}_p} H^0(K_v, V) + \dim_{\mathbf{Q}_p} D_{\mathrm{dR}}(V)/D^+_{\mathrm{dR}}(V),$$

where the last term computes the number of negative Hodge–Tate weights of V. Also, local duality works.

Example 20.8. Let $E/\mathbf{Q}$ be an elliptic curve and $V = V_p(E)$. Then

(1) If $v \nmid p$, then $H^1_f(K_v, V) = 0$, since the Tate module has no nontrivial Galois invariants. This implies $H^1(K_v, V) = 0$.

(2) If $v \mid p$, then $\dim_{\mathbf{Q}_p} H^1_f(K_v, V) = 1$, since $\mathrm{HT}(V) = \mathrm{HT}(E) = \{0, -1\}$. This implies $\dim H^1(K_v, V) = 2$.

Finally, we can define the Bloch–Kato Selmer groups.

Definition 20.9. The *Bloch–Kato Selmer group* is defined to be

$$H^1_f(K, V) := \{s \in H^1(K, V) : \mathrm{loc}_v(s) \in H^1_f(K_v, V) \text{ for all } v\}.$$

It is a deep theorem that this agrees with the original definition for elliptic curves.

Theorem 20.10 (Bloch–Kato)**.** *Let E/K be an elliptic curve (or abelian variety) and $V = V_p(E)$. Then*

$$H^1_f(K_v, V) = \mathrm{im}\left(A(K_v) \otimes \mathbf{Q}_p \to H^1(K_v, V)\right).$$

Thus $H^1_f(K_v, V) = \mathrm{Sel}_{\mathbf{Q}_p}(E)$.

20.2. Bloch–Kato conjecture.

Definition 20.11. Define

$$L(s,V) := \prod_{v\nmid\infty} L_v(s,V)$$

where

$$L_v(s,V) = \begin{cases} \det\left(1-\mathrm{Fr}_v^{-1}\, q_v^{-s} : V^{I_v}\right)^{-1} & \text{at } v\nmid p, \\ \det\left(1-\phi_v^{-1} q_v^{-s} : D_{\mathrm{crys},v}(V)\right)^{-1} & \text{at } v \mid p. \end{cases}$$

Example 20.12. Let $E/\mathbf{Q}$ be an elliptic curve. Then

$$L(s,V) = L(s+1,E),$$

with center at $s=0$.

Conjecture 20.13 (Langlands)**.** *Let V be a geometric Galois representation. Then V should come from an automorphic representation. So $L(s,V)$ has meromorphic continuation to $s\in\mathbf{C}$ (analytic if V does not contain $\mathbf{Q}_p(1)$) and satisfies a functional equation*

$$\Lambda(s,V) = \epsilon(s,V)\Lambda(-s,V^*(1)).$$

Conjecture 20.14 (Bloch–Kato)**.**

$$\mathrm{ord}_{s=1} L(s,V) = \dim H^1_f(K,V^*(1)) - \dim H^0(K,V^*(1)).$$

Here $H^1_f(K,V^*(1))$ is the Bloch–Kato Selmer group, and $H^0(K,V^*(1))=0$ if V is irreducible. The Bloch–Kato conjecture vastly generalizes BSD to any motives.

20.3. Rankin–Selberg motives.

Let K/F be a CM extension over a totally real number field, and π (resp. π') be an automorphic representation on $\mathrm{GL}_{n,K}$ (resp. $\mathrm{GL}_{n-1,K}$). Set $\Pi = \pi\times\pi'$.

Our goal is to construct a geometric Galois representation $V_\Pi = V_\pi \otimes V_{\pi'}$, which has dimension $n(n-1)$.

Definition 20.15. Let π be a cuspidal automorphic representation on $\mathrm{GL}_n(\mathbf{A}_K)$. Say

(1) π is *cohomological* (or *regular algebraic* in Henniart's terminology) if the infinitesimal character $\chi_\infty \in X^*(T)$ of π_∞ is regular, i.e.,

$$\langle \chi_\infty, \alpha^\vee\rangle \neq 0$$

for all $\alpha\in\Phi(\mathrm{GL}_n)$. (The Hodge–Tate weights are distinct.)

(2) π is *conjugate self-dual* if $\pi^c \cong \widetilde{\pi}$.

Next time we will construct V_Π under these assumptions.

21. Lecture 21 (December 3, 2018)

21.1. BBK for Rankin–Selberg motives.

Recall:

Conjecture 21.1 (Bloch–Kato)**.** *For a geometric p-adic Galois representation V,*

$$\mathrm{ord}_{s=0} L(s,V) = \dim H^1_f(K,V^*(1)).$$

Remark. Suppose K/F is a CM extension of a totally real field, and $V^c \cong V^*(1)$. Then

$$L(s,V) = L(s,V^c) = L(s,V^*(1)),$$

so we have a functional equation relating

$$L(s,V) \longleftrightarrow L(-s,V)$$

with center $s=0$.

Now let π be a cuspidal tempered automorphic representation on $\mathrm{GL}_n(\mathbf{A}_K)$. The construction of V_π is provided by

Theorem 21.2 (Chenevier–Harris, Shin and many people)**.** *Assume π is cohomological and conjugate-self-dual (i.e., $\pi^c \simeq \widetilde{\pi}$). Then there exists $\rho_\pi : G_K \to \mathrm{Aut}(V_\pi)$ (over a p-adic field) such that:*

1. *V_π is geometric, i.e., de Rham at $v \mid p$ with distinct Hodge–Tate weights.*
2. *If π_v is unramified, then V_π is unramified at v if $v \nmid p$, and cyrstalline at v if $v \mid p$. Furthermore, suppose π_v corresponds to the Satake parameter $C_{\pi_v} = \begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix} \in \mathrm{GL}_n(\mathbf{C})$ with $|\mu_i| = 1$. Then the eigenvalues of Fr_v (at $v \nmid p$) or ϕ_v (at $v \mid p$) are given by $\{\mu_i q^{\frac{1-n}{2}}\}$. In other words,*

$$V_\pi|_{G_v} = \mathrm{LLC}\left(\pi_v \otimes |\cdot|_v^{\frac{1-n}{2}}\right)$$

under the local Langlands correspondence.

3. *More generally, $V_\pi|_{G_v}$ is compatible with $\mathrm{LLC}(\pi_v)$.*

In particular, we have $V_\pi^c = V_\pi^*(1-n)$.

Idea of proof. When n is odd, or n is even with π_∞ satisfying extra regularity conditions, V_π can be constructed in the cohomology of a certain unitary Shimura variety, by

1. point-counting on Igusa varieties (Shin),
2. comparison of Lefschetz trace formula and Arthur–Selberg trace formula.

When n is even, the extra assumption is removed by Chenevier–Harris by congruences (eigenvarieties). □

Definition 21.3 (Rankin–Selberg motive)**.** Let π (resp. π') be an automorphic representation on $\mathrm{GL}_n(\mathbf{A}_K)$ (resp. $\mathrm{GL}_{n-1}(\mathbf{A}_K)$) as before, and $\Pi = \pi \times \pi'$. Define the *Rankin–Selberg motive*

$$V_\Pi := (V_\pi \otimes V_{\pi'})(n-1).$$

It can be checked easily that $V_\Pi^c = V_\Pi^*(1)$ and

$$L_v\left(s - \frac{1}{2}, V_\Pi\right) = \det\left(1 - q_v^{-s} C_{\pi_v} \otimes C_{\pi'_v}\right)^{-1} = \prod_{i,j}\left(1 - q_v^{-s}\mu_i\mu'_j\right)^{-1}$$

for the Satake parameters C_{π_v} and $C_{\pi'_v}$.

Now we can state the main theorem, due to Yifeng Liu, Yichao Tian, Liang Xiao, Wei Zhang and Xinwen Zhu.

Theorem 21.4 (LTXVV, rank 0)**.** *Assume π and π' have trivial infinitesimal character (with Hodge–Tate weights $\{0,-1,-2,\cdots,-(n-1)\}$ and $\{0,-1,-2,\cdots,-(n-2)\}$ respectively). Let V_Π be the Rankin–Selberg motive. Then for almost all p,*

$$L\left(\frac{1}{2},\Pi\right)\neq 0 \implies H^1_f(K,V_\Pi^*(1))=0,$$

i.e., the Bloch–Kato conjecture holds in rank 0.

This is a vast generalization of our previous theorem for elliptic curves.

21.2. **Rank one case.** We would like to prove the implication

$$\operatorname{ord}_{s=\frac{1}{2}} L(s,\Pi)=1 \implies \dim H^1_f(K,V_\Pi^*(1))=1.$$

In the elliptic curve case, this crucially relies on the Gross–Zagier formula:

$$L'(E_K,1)\sim \text{height of Heegner point } y_K.$$

A generalization is given by the arithmetic Gan–Gross–Prasad conjecture:

$$L'\left(\frac{1}{2},\Pi\right)\sim \text{“height” of GGP cycle } \Delta_\Pi.$$

Unfortunately the definition of heights for cycles is conditional on the standard conjectures.

Realistically, our goal is to construct Δ_Π using the Shimura variety associated to $\mathrm{U}_n\times\mathrm{U}_{n-1}$.

Definition 21.5. Let V be a hermitian space with respect to K/F of dimension n, and $\mathrm{U}_n=U(V)$ be the associated unitary group. Assume $\mathrm{U}_n(\mathbf{R})=\mathrm{U}(n-1,1)\times\mathrm{U}(n,0)\times\cdots\times\mathrm{U}(n,0)$ (with $[F:\mathbf{Q}]$ factors in total). Define the Hodge cocharacter

$$h:\mathbf{C}^\times\to \mathrm{U}_n(\mathbf{R})=\mathrm{U}(n-1,1)\times\mathrm{U}(n,0)\times\cdots\times\mathrm{U}(n,0)$$

$$z\mapsto\left(\begin{pmatrix}\frac{\bar z}{z} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix},\mathrm{Id},\cdots,\mathrm{Id}\right)$$

and

$$\begin{aligned}\mathcal{H} &:= \text{orbit of } h \text{ under } \mathrm{U}_n(\mathbf{R})\text{-conjugation}\\ &\cong \mathrm{U}(n-1,1)/(\mathrm{U}(n-1)\times\mathrm{U}(1)),\end{aligned}$$

which is a hermitian symmetric domain with $\dim_{\mathbf{C}}\mathcal{H}=n-1$.

Write $\mathbf{A}_f=\mathbf{A}_{F,f}$.

Definition 21.6. Let $K\subseteq \mathrm{U}_n(\mathbf{A}_f)$ be an open compact subgroup. Define the Shimura variety

$$\mathrm{Sh}_K(\mathrm{U}_n)(\mathbf{C})=\mathrm{U}_n(F)\backslash\mathrm{U}_n(\mathbf{A}_f)\times\mathcal{H}/K.$$

Assume K has no torsion elements. Then Sh_K is a quasi-projective smooth variety over F of dimension $n-1$.

Remark. Technically it is easier to work with the Shimura variety associated to $\mathrm{GU}(V)$ instead of $\mathrm{U}(V)$, where

$$\mathrm{GU}(V)(R) = \{g \in \mathrm{GL}_{K\otimes R}(V \otimes_{\mathbf{Q}} R) : \langle gv_1, gv_2\rangle = \chi(g)\langle v_1, v_2\rangle, \chi(g) \in R^\times\}$$

for each $\mathbf{Q}$-algebra R. There is an extension

$$1 \to \mathrm{U}(V) \to \mathrm{GU}(V) \xrightarrow{\chi} \mathbf{G}_m \to 1.$$

Consider the Hodge cocharacter

$$\begin{aligned} \mathbf{C}^\times &\to \mathrm{GU}(V)(\mathbf{R}) \\ z &\mapsto \left(\begin{pmatrix} \overline{z} & & & \\ & z & & \\ & & \ddots & \\ & & & z \end{pmatrix}, z \cdot \mathrm{Id}, \cdots, z \cdot \mathrm{Id} \right). \end{aligned}$$

Then $\mathrm{Sh}_K(\mathrm{GU}(V))$ is of *PEL type*, with

$$\mathrm{Sh}_K(\mathrm{GU}(V))(\mathbf{C}) = \{(A, \iota, \lambda, \eta)\}$$

where:

- A is an abelian variety of dimension $n-1$,
- $\iota : \mathcal{O}_K \to \mathrm{End}(A)$,
- $\lambda : A \xrightarrow{\sim} A^\vee$ is an $\mathcal{O}_K$-linear polarization,
- η is a K-orbit of isomorphisms
$$H^1(A, \mathbf{Q}) \otimes \mathbf{A}_f \simeq V(\mathbf{A}_f)$$
of symplectic $\mathbf{A}_f$-modules (up to similitude) and of $\mathcal{O}_K$-modules.

Remark. If $F \neq \mathbf{Q}$, then $\mathrm{Sh}_K(\mathrm{GU}(V))$ is projective. If $F = \mathbf{Q}$, then $\mathrm{Sh}_K(\mathrm{GU}(V))$ has a canonical toroidal compactification. Denote them by X_V.

Definition 21.7 (GGP cycle)**.** Let $V = W \oplus K \cdot u$ with $(u, u) = 1$. Then the embedding $\mathrm{GU}(W) \hookrightarrow \mathrm{GU}(V)$ induces $\delta : X_W \hookrightarrow X_V$ (of dimensions $n-2$ and $n-1$ respectively). Consider

$$(\mathrm{Id}, \delta) : X_W \hookrightarrow X_W \times X_V =: X$$

(of dimensions $n-2$ and $2n-3$ respectively). The GGP cycle is defined as

$$\Delta := \mathrm{im}(\mathrm{Id} \times \delta) \subseteq \mathrm{CH}^{n-1}(X).$$

Given Π, define $\Delta_\Pi = \Delta[\Pi_f] \subseteq \mathrm{CH}^{n-1}(X)$ to be the Π_f-isotypic component.

Remark. Local ϵ-dichotomy ensures there is a unique choice of (W, V) such that Δ_Π is possibly nonzero.

Conjecture 21.8 (Arithmetic GGP)**.**

$$L'\left(\frac{1}{2}, \Pi\right) \sim \text{“height” of } \Delta_\Pi.$$

Remark. The arithmetic GGP is a special case of Beilinson's conjecture:

Conjecture 21.9 (Beilinson). *Let X/K be a smooth projective variety. Then*

$$\mathrm{ord}_{s=center} L(s, H^{2i-1}(X)) = \dim \mathrm{CH}^i(X)_0,$$

where $\mathrm{CH}^i(X)_0 := \ker(\mathrm{CH}^i(X) \xrightarrow{\mathrm{cl}} H^{2i}(X))$.

Remark. We have the implication

$$L'\left(\frac{1}{2}, \Pi\right) \neq 0 \implies \Delta_\Pi \neq 0.$$

Then we can consider its image $\mathrm{AJ}(\Delta_\Pi)$ under the Abel–Jacobi map:

$$\begin{tikzcd}
\mathrm{CH}^{n-1}(X) \arrow[r, "\mathrm{cl}"] \arrow[dr, "\mathrm{AJ}"'] & H^{2n-2}(X, \overline{\mathbf{Q}_p})(n-1)[\Pi_f] \arrow[d] \\
 & H^1(K, H^{2n-3}(X_{\overline{K}}, \overline{\mathbf{Q}_p}))(n-1)[\Pi_f]
\end{tikzcd}$$

where the vertical map comes from the Hochschild–Serre spectral sequence and the fact that $H^{2n-2}(X_{\overline{K}}, \overline{\mathbf{Q}_p})(n-1)[\Pi_f] = 0$. Note that H^{2n-3} is the exact middle dimension.

Remark. When $n = 2$, $\mathrm{AJ}(\Delta_\Pi)$ is the analogue of y_K under the Kummer map $E(K) \to H^1(K, V_p(E))$.

Theorem 21.10 (LTXZZ, rank 1). *For almost all p,*

$$\mathrm{AJ}(\Delta_\Pi) \neq 0 \implies \dim H^1_f(K, V_\Pi^*(1)) = 1.$$

Next time we will sketch the proof of this.

22. Lecture 22 (December 5, 2018)

22.1. **Proof strategies.** Recall:

Theorem 22.1 (LTXZZ). *Let Π be the Rankin–Selberg motive as before.*

- *(Rank 0) If $L(\frac{1}{2}, \Pi) \neq 0$, then $H^1_f(K, V_\Pi^*(1)) = 0$.*
- *(Rank 1) If $\mathrm{AJ}(\Delta_\Pi) \neq 0$, then $\dim H^1_f(K, V_\Pi^*(1)) = 1$.*

The strategy is analogous to the elliptic curve case. The key is two explicit reciprocity laws for GGP cycles on unitary Shimura varieties. Roughly speaking, for certain "level-raising primes" v, we can find a congruence

$$\Pi \text{“}\equiv\text{”} \Pi' \pmod p$$

where Π is unramified at v and Π' is ramified at v.

The first reciprocity law concerns the case $\epsilon(\Pi) = +1$. Recall that the Ichino–Ikeda formula expresses the central L-value $L(\frac{1}{2}, \Pi)$ in terms of the automorphic period $\wp_{\mathrm{U}_{n-1}}(\varphi)$ for $\varphi \in \Pi$. Then the reciprocity law states that

$$\wp_{\mathrm{U}_{n-1}}(\varphi) \equiv \partial_v \mathrm{AJ}(\Delta_{\Pi'}) \pmod p,$$

where $\mathrm{AJ}(\Delta_{\Pi'}) \in H^1(K, V_\Pi)$ with $V_\Pi = H^{2n-3}(X)[\Pi_f]$, and $\partial_v : H^1(K_v, V_\Pi) \to H^1_{\mathrm{sing}}(K_v, V_\Pi)$. Similarly, we can formulate the second reciprocity law for $\epsilon(\Pi) = -1$:

$$\mathrm{loc}_v \mathrm{AJ}(\Delta_\Pi) \equiv \wp_{\mathrm{U}_{n-1}}(\Pi') \pmod p.$$

Then we use Kolyvagin's method to bound $H^1_f(K, V_\Pi)$.

New ingredients are needed for the explicit reciprocity laws. For $X = X_V \times X_W$ (of dimensions $n-1$ and $n-2$ respectively), the Künneth formula gives

$$H^{2n-3}(X)[\Pi_f] = H^{n-1}(X_V) \otimes H^{n-2}(V_W)[\Pi_f],$$

since cohomology is concentrated at middle degree. Now we have

$$\mathrm{loc}_v \, \mathrm{AJ}(\Delta_\Pi) \in H^1(k_v, H^{n-1}(X_{V,k_v}) \otimes H^{n-2}(X_{W,k_v}))(n-1)[\Pi_f],$$

so we need to understand the geometry of Shimura varieties in characteristic p.

22.2. **Geometry of unitary Shimura varieties at good reduction.** Recall that for $\ell \nmid N$, $X_0(N)_{\mathbf{F}_\ell}$ has a distinguished set of supersingular points $X_0(N)^{\mathrm{ss}}_{\mathbf{F}_\ell}$. What makes the explicit reciprocity law work is the identification

$$X_0(N)^{\mathrm{ss}}_{\mathbf{F}_\ell} \simeq X(N, \ell)$$

with the Shimura set associated to $B_{\ell,\infty}$ (ramified at ℓ and ∞).

Definition 22.2 (Switching invariants)**.** Let v be a place of F. Assume v is inert in K. Each hermitian space V gives rise to V_v for the local quadratic extension K_v/F_v. Then the *Hasse invariant* is

$$\epsilon(V_v) := \begin{cases} +1 & \text{if } \mathrm{disc}(V_v) \text{ has even valuation,} \\ -1 & \text{if } \mathrm{disc}(V_v) \text{ has odd valuation.} \end{cases}$$

Given V such that $\epsilon(V_v) = +1$ and $\mathrm{sign}(V_\infty) = \{(n-1,1), (n,0), \cdots, (n,0)\}$, define a new hermitian space $V^\bullet$ by

$$\epsilon(V^\bullet_v) = -1, \quad \mathrm{sign}(V^\bullet_\infty) = \{(n,0), (n,0), \cdots, (n,0)\}.$$

Theorem 22.3. *Assume v is inert in K, and the level defining the unitary Shimura variety $X = X_V$ is given by a hyperspecial subgroup in $\mathrm{GU}(V)(F_v)$ (i.e., the stabilizer of a self-dual lattice in V_v).*

(1) *(Kottwitz, Lan) X has an integral model over $\mathcal{O}_{K_v}$, given by the solution to a moduli problem $\{(A, \iota, \lambda, \eta)\}$. The special fiber is smooth projective and has dimension $n-1$.*

(2) *(Vollaard–Wedhorn) Let $X^{\mathrm{ss}} \subseteq X_k$ be the supersingular locus (i.e., where A/k_v is a supersingular abelian variety). Then the normalization of X^{ss}, denoted by $\widetilde{X^{\mathrm{ss}}}$, is a disjoint union of copies of a smooth projective variety DL_n of dimension $\lfloor \frac{n-1}{2} \rfloor$, indexed by the definite Shimura set*

$$X^\bullet = \mathrm{GU}(V^\bullet)(\mathbf{Q}) \backslash \mathrm{GU}(V^\bullet)(\mathbf{A}_f)/K^\bullet,$$

where the level at v for $X^\bullet$ is given by the stabilizer of

$$\begin{cases} \textit{a self-dual lattice (i.e., } \Lambda^\vee = \Lambda\textit{)} & \textit{if } n \textit{ is odd,} \\ \textit{an almost self-dual lattice (i.e., } \Lambda^\vee \overset{\mathrm{codim}\,1}{\supseteq} \Lambda\textit{)} & \textit{if } n \textit{ is even.} \end{cases}$$

As a summary, we have the following picture

$$\begin{tikzcd}
\underset{\dim n-1}{X} & \underset{\dim \lfloor \frac{n-1}{2} \rfloor}{X^{\mathrm{ss}}} \arrow[l, hook'] & \widetilde{X^{\mathrm{ss}}} \arrow[l] \arrow[d, "\mathrm{DL}_n\text{-fibration}"] \\
 & & \underset{\dim 0}{X^{\bullet}}
\end{tikzcd}$$

22.3. **Tate's conjecture.** Recall that we have a cycle class map

$$\mathrm{CH}^r(X) \xrightarrow{\mathrm{cl}} H^{2r}(X, \mathbf{Q}_p)(r).$$

Conjecture 22.4 (Tate)**.** *Assume X/k_v is smooth projective over the finite field k_v. Then*

$$\mathrm{CH}^r(X) \otimes \mathbf{Q}_p \xrightarrow{\mathrm{cl}} H^{2r}(X, \mathbf{Q}_p)(r)^{\mathrm{Fr}_v=1}$$

is surjective.

Remark. This is known when X is an abelian variety and $r = 1$, due to Tate.

Tate conjecture says that we can understand $H^{2r}(X)(r)^{\mathrm{Fr}=1}$ via algebraic cycles.

As before, let π be an automorphic representation on $\mathrm{GL}_n(\mathbf{A}_K)$, V_π be the associated Galois representation of dimension n, and $X = X_V$ be the associated Shimura variety of dimension $n-1$.

Definition 22.5. Assume n is odd. Let v be inert in K. Say v is *odd generic* for $\pi \pmod p$ if the eigenvalues $\{\alpha_1, \cdots, \alpha_n\}$ of Fr_v acting on $V_\pi \pmod p$ satisfy $\frac{\alpha_i}{\alpha_j} \neq 1, q_v$ for all $i \neq j$.

Theorem 22.6 (Xiao–Zhu)**.** *Assume v is odd generic. Then Tate conjecture holds for $H^{n-1}(X_{\overline{k_v}})(\frac{n-1}{2})[\pi_f]^{\mathrm{Fr}_v=1}$. In fact, this space is exactly generated by $\widetilde{X^{\mathrm{ss}}}$.*

In particular, this and Poincaré duality together imply that

$$\begin{aligned} H^{n-1}(X_{\overline{k_v}})(\tfrac{n-1}{2})[\pi_f]^{\mathrm{Fr}_v=1} &\xrightarrow{\sim} H^{n-1}(\widetilde{X^{\mathrm{ss}}})(\tfrac{n-1}{2})[\pi_f] \\ &\simeq H^0(X^\bullet)[\pi_f]^*, \end{aligned}$$

which is a space of automorphic forms!

22.4. **Second reciprocity.**

Definition 22.7. Let n be even. Say v is *even level-raising* for $\pi \pmod p$ if $\frac{\alpha_i}{\alpha_j} \neq 1, q_v$ for all $i \neq j$, except that $\alpha_{\frac{n}{2}} = q_v^{\frac{n}{2}}$ and $\alpha_{\frac{n}{2}+1} = q_v^{\frac{n}{2}-1}$.

This is analogous to the Steinberg representation for GL_2.

Definition 22.8. Say p is *nice* if p is a good prime for $\Pi = \pi \times \pi'$, $p \geq 5$, and:

(1) V_π and $V_{\pi'}$ mod p are irreducible and with adequate images;
(2) p is isolated for Π.

Fact. p is nice for almost all p.

Definition 22.9. Assume n is even. Say v is *admissible* for $\Pi = \pi \times \pi'$ (on GL_n and GL_{n-1} respectively) mod nice p if:

(1) v is odd generic for π';
(2) v is even level-raising for π;
(3) Fr_v acting on V_Π has eigenvalue 1 with multiplicity 1.

Fact. v is admissible for a positive proportion of v.

Theorem 22.10 (Second explicit reciprocity)**.** *Assume p is nice and v is admissible. If* $\mathrm{loc}_v \mathrm{AJ}(\Delta_\Pi) \not\equiv 0 \pmod{p}$*, then there exists* $\Pi^\bullet$ *on* $\mathrm{GU}(V^\bullet) \times \mathrm{GU}(W^\bullet)$ *and* $\varphi^\bullet \in \Pi^\bullet$ *such that*

$$\mathrm{loc}_v \mathrm{AJ}(\Delta_\Pi) \equiv \wp_{\mathrm{GU}(W^\bullet)}(\varphi^\bullet) \pmod{p}.$$

23. Lecture 23 (December 10, 2018)

23.1. **Tate conjecture via geometric Satake.** Recall that a new ingredient in proving explicit reciprocity is the Tate conjecture for unitary Shimura varieties. Let $X = X_{V,\bar{k}}$ be the special fiber associated to $\mathrm{GU}(1, n-1)$. Assume n is odd, so that $\dim X = n-1$ is even.

Last time we saw the diagram

$$\begin{tikzcd} \underset{\dim n-1}{X} & \underset{\dim \frac{n-1}{2}}{\widetilde{X^{\mathrm{ss}}}} \arrow[l] \arrow[d] \\ & \underset{\substack{\dim 0 \\ \text{Shimura set}}}{X^\bullet} \end{tikzcd}$$

where the fibers of the vertical map are Deligne–Lusztig varieties of dimension $\frac{n-1}{2}$.

Theorem 23.1 (Xiao–Zhu)**.** *Assume v is odd generic for π. Then*

$$H^{n-1}(\widetilde{X^{\mathrm{ss}}})(\tfrac{n-1}{2})[\pi_f] \simeq H^{n-1}(X)(\tfrac{n-1}{2})^{\mathrm{Fr}_v=1}[\pi_f].$$

Remark. This even holds with coefficients $\Lambda = \mathbf{F}_p$. Let $\mathfrak{m}_\pi \subseteq \mathbf{T}$ correspond to π. Then

$$H^{n-1}(\widetilde{X^{\mathrm{ss}}}, \Lambda)(\tfrac{n-1}{2})_{\mathfrak{m}_\pi} \xrightarrow{\sim} H^{n-1}(X, \Lambda)(\tfrac{n-1}{2})^{\mathrm{Fr}_v=1}_{\mathfrak{m}_\pi}.$$

This follows from the torsion-free result of Caraiani–Scholze.

The proof strategy is:

(1) (Injectivity) Show the image of components of $\widetilde{X^{\mathrm{ss}}}$ are linearly independent in $H^{n-1}(X)$.
(2) (Compare dimensions) Prove dimensions are equal using comparison of Lefschetz trace formula for $X^\bullet$ and X.

(1) is more difficult: by looking at the intersection pairing

$$(\cdot,\cdot) : H^{n-1}(X) \times H^{n-1}(X) \to H^{2(n-1)}(X) \simeq \mathbf{Q}_p,$$

it suffices to show the matrix under $(\cdot,\cdot)$ for $H^{n-1}(\widetilde{X^{\mathrm{ss}}})$ is nondegenerate. This intersection matrix is very difficult to compute, and the idea is to compute the determinant abstractly using the representation theory of $\widehat{G}$.

- On the generic fiber, we have an action of Hecke correspondence $\mathcal{H}_v$ at v. For G split, the Satake isomorphism gives

$$\mathcal{H}_v \xrightarrow{\sim} \mathbf{C}[X_*(T)]^W \xrightarrow{\sim} \mathbf{C}[\widehat{G}]^{\widehat{G}}.$$

- On the special fiber, we can realize

$$\begin{tikzcd}
 & \widetilde{X^{\mathrm{ss}}} \arrow[dl] \arrow[dr] & \\
X^{\bullet} & & X
\end{tikzcd}$$

  as an "exotic Hecke correspondence" between $X^{\bullet}$ and X. This has meaning in terms of "spectral operators", which comes from the representation theory of $\widehat{G}$.

23.2. **Geometric Satake.** Let F be a local non-archimedean field with residue field k and ring of integers $\mathcal{O} = \mathcal{O}_F \subseteq F$. Let $G/\mathcal{O}$ be a reductive group.

Definition 23.2. The *spherical Hecke algebra* is $\mathcal{H} := C_c^{\infty}(G(\mathcal{O})\backslash G(F)/G(\mathcal{O}))$.

The Satake isomorphism states that

$$\mathcal{H} \xrightarrow{\sim} \overline{\mathbf{Q}_p}[\widehat{G}]^{\widehat{G}}$$

with an action by σ-conjugation: for σ the Frobenius, $g \cdot h = gh\sigma(g^{-1})$.

Remark. We can rewrite this as $\mathcal{H} \xrightarrow{\sim} \overline{\mathbf{Q}_p}[\widehat{G}\sigma]^{\widehat{G}}$, where $\widehat{G}\sigma \subseteq \widehat{G} \rtimes \langle\sigma\rangle$.

To geometrize the classical Satake isomorphism, we need to introduce:

Definition 23.3. The *local Hecke stack* is

$$\mathrm{Hk}^{\mathrm{loc}} := L^+G\backslash LG/L^+G,$$

where $LG(k) = G(F)$ and $L^+G(k) = G(\mathcal{O})$. For every perfect k-algebra R, define the disk $D_R = \operatorname{Spec} W_{\mathcal{O}}(R)$ and the punctured disk $D_R^* = \operatorname{Spec} W_{\mathcal{O}}(R)[\frac{1}{\varpi}]$. Then

$$\mathrm{Hk}^{\mathrm{loc}}(R) = \{\mathcal{E}_1 \xrightarrow{\beta} \mathcal{E}_2 : \mathcal{E}_1 \text{ and } \mathcal{E}_2 \text{ are } G\text{-bundles on } D_R \text{ and } \beta|_{D_R^*} \text{ is an isomorphism}\}.$$

Let $\mathrm{Perv}(\mathrm{Hk}^{\mathrm{loc}})$ be the category of perverse sheaves on $\mathrm{Hk}^{\mathrm{loc}}$.

Theorem 23.4 (Mirkovic–Vilonen if $\operatorname{char} F > 0$; X. Zhu if $\operatorname{char} F = 0$)**.** *There is an equivalence of monoidal categories*

$$\mathrm{Rep}(\widehat{G}) \xrightarrow{\sim} \mathrm{Perv}(\mathrm{Hk}^{\mathrm{loc}})$$
$$V_\mu \mapsto IC_\mu$$

which sends the highest weight representation of weight μ to the IC sheaf on $\mathrm{Gr}_\mu \subseteq \mathrm{Gr}$.

23.3. **Spectral operators.**

Definition 23.5. The *moduli of local shtukas* is

$$\mathrm{Sht}^{\mathrm{loc}} := \{(\mathcal{E}_1 \xrightarrow{\beta} \mathcal{E}_2) \in \mathrm{Hk}^{\mathrm{loc}} \text{ with } \sigma^*\mathcal{E}_1 \xrightarrow{\sim} \mathcal{E}_2\}.$$

By definition, we have a forgetful map $\mathrm{Sht}^{\mathrm{loc}} \to \mathrm{Hk}^{\mathrm{loc}}$.

Definition 23.6. Define

$$\mathrm{Hk}(\mathrm{Sht}^{\mathrm{loc}}) := \left\{ \begin{tikzcd} \mathcal{E}_1 \arrow[r, "\beta"] \arrow[d, "\alpha"'] & \mathcal{E}_2 \arrow[r, "\sim"] \arrow[d, "\sigma^*\alpha"] & \sigma^*\mathcal{E}_1 \\ \mathcal{E}_1' \arrow[r, "\beta'"] & \mathcal{E}_2' \arrow[r, "\sim"] & \sigma^*\mathcal{E}_1' \end{tikzcd} \right\}.$$

Then there is a diagram

$$\begin{tikzcd} & \mathrm{Hk}(\mathrm{Sht}^{\mathrm{loc}}) \arrow[dl, "\overleftarrow{h}"'] \arrow[dr, "\overrightarrow{h}"] & \\ \mathrm{Sht}^{\mathrm{loc}} & & \mathrm{Sht}^{\mathrm{loc}} \end{tikzcd}$$

Let $\mathrm{Sht}^{\mathrm{loc}}_{\mu} \subseteq \mathrm{Sht}^{\mathrm{loc}}$ be given by the locus where $\mathrm{inv}(\beta) \leq \mu$, and $\mathrm{Sht}^{\mathrm{loc}}_{\mu_1|\mu_2} \subseteq \mathrm{Hk}(\mathrm{Sht}^{\mathrm{loc}})$ be where $\mathrm{inv}(\beta) \leq \mu_1$ and $\mathrm{inv}(\beta') \leq \mu_2$. Then we have a correspondence

$$\begin{tikzcd} & \mathrm{Sht}^{\mathrm{loc}}_{\mu_1|\mu_2} \arrow[dl] \arrow[dr] & \\ \mathrm{Sht}^{\mathrm{loc}}_{\mu_1} & & \mathrm{Sht}^{\mathrm{loc}}_{\mu_2} \end{tikzcd}$$

Example 23.7.

- $\mathrm{Sht}^{\mathrm{loc}}_0 = [\mathrm{Spec}\, k/G(\mathcal{O})] = [\mathrm{point}/G](k)$ (where $G(\mathcal{O})$ is considered as a discrete group).
- $\mathrm{Sht}^{\mathrm{loc}}_{0|0} = [G(\mathcal{O})\backslash G(F)/G(\mathcal{O})] = \mathrm{Hk}^{\mathrm{loc}}(k)$.

Definition 23.8. The category $\mathrm{Perv}^{\mathrm{Corr}}(\mathrm{Sht}^{\mathrm{loc}})$ is defined by:

(1) objects: perverse sheaves on $\mathrm{Sht}^{\mathrm{loc}}$;

(2) morphisms: cohomological correspondences supported on $\mathrm{Hk}(\mathrm{Sht}^{\mathrm{loc}})$, i.e.,

$$\mathrm{Hom}^{\mathrm{Corr}}(\mathcal{F}_1, \mathcal{F}_2) := \mathrm{Hom}(\overleftarrow{h}^*\mathcal{F}_1, \overrightarrow{h}^!\mathcal{F}_2).$$

The identification $\mathrm{Rep}(\widehat{G}) = \mathrm{Coh}([\bullet/\widehat{G}])$ induces a pullback map

$$\mathrm{Rep}(\widehat{G}) \to \mathrm{Coh}([\widehat{G}\sigma/\widehat{G}])$$
$$V \mapsto \widetilde{V} := \{V \otimes \mathcal{O}_{\widehat{G}\sigma}\}$$

with image inside the subcategory $\mathrm{Coh}_{\mathrm{free}}([\widehat{G}\sigma/\widehat{G}])$ of free sheaves.

Theorem 23.9 (Xiao–Zhu)**.** *There is a functor S such that the diagram*

$$\begin{tikzcd} V \arrow[d, mapsto] & \mathrm{Rep}(\widehat{G}) \arrow[r, "\sim", "Satake"'] \arrow[d, "pullback"'] & \mathrm{Perv}(\mathrm{Hk}^{\mathrm{loc}}) \arrow[d, "pullback"] \\ \widetilde{V} = \{V \otimes \mathcal{O}_{\widehat{G}\sigma}\} & \mathrm{Coh}_{\mathrm{free}}([\widehat{G}\sigma/\widehat{G}]) \arrow[r, "\exists S"] & \mathrm{Perv}^{\mathrm{Corr}}(\mathrm{Sht}^{\mathrm{loc}}) \end{tikzcd}$$

commutes.

Remark. Let $V_0 = \mathbb{1}$ be the trivial representation of $\widehat{G}$. Then

$$\mathrm{End}(V_0) = \Gamma([\widehat{G}\sigma/\widehat{G}], \mathcal{O}) = \overline{\mathbf{Q}_p}[\widehat{G}\sigma]^{\widehat{G}} \left(\overset{\text{Satake}}{\simeq} \mathcal{H}\right)$$

is the space of twisted conjugation-invariant functions on $\widehat{G}$. More generally, define

$$\begin{aligned} J(V) &= \Gamma([\widehat{G}\sigma/\widehat{G}], \widetilde{V}) \\ &= (\overline{\mathbf{Q}_p}[\widehat{G}\sigma \otimes V])^{\widehat{G}} \\ &= \{f : \widehat{G} \to V : f(gh\sigma^{-1}(g)) = g \cdot f(h)\}. \end{aligned}$$

Write $J := J(V_0)$ $(\simeq \mathcal{H})$.

23.4. **Computing intersection numbers.** Notice there is a map $X = \mathrm{Sh}(G, \mu) \to \mathrm{Sht}^{\mathrm{loc}}_{\mu}$ and a diagram

$$\begin{tikzcd}
 & \widetilde{X^{\mathrm{ss}}} \arrow[dl] \arrow[d] \arrow[dr] & \\
X^{\bullet} \arrow[d] & \mathrm{Sht}^{\mathrm{loc}}_{0|\mu} \arrow[dl] \arrow[dr] & X \arrow[d] \\
\mathrm{Sht}^{\mathrm{loc}}_{0} & & \mathrm{Sht}^{\mathrm{loc}}_{\mu}.
\end{tikzcd}$$

Then $\widetilde{X^{\mathrm{ss}}}$ can be identified via

$$H^0(X^{\bullet}) \underset{J}{\otimes} \mathrm{Hom}(\widetilde{V_0}, \widetilde{V_\mu}) \to H^{n-1}(X).$$

Here $\mathrm{Hom}(\widetilde{V_0}, \widetilde{V_\mu}) = J(V_\mu)$ can be thought of as an "exotic correspondence" via the S-operator. Finally, the intersection matrix is given by

$$J(V_\mu) \times J(V_\mu^*) \to J.$$

Returning to the case $G = \mathrm{U}(n)$ for n odd, $\mu(t) = \begin{pmatrix} t & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$ and V_μ is the standard representation of GL_n, the upshot is:

Theorem 23.10.

(1) *$J(V_\mu)$ is a free module of rank 1 over J.*

(2) *The intersection matrix (1×1) is given by*

$$\prod_{i=1}^{\frac{n-1}{2}} (X_i + X_i^{-1} - 2),$$

where $X_i(t) = \mathrm{diag}(1, \cdots, t, \cdots, 1, \cdots, 1, \cdots, t^{-1}, \cdots, 1)$ with t (resp. t^{-1}) at the i-th (resp. $(n-1-i)$-th) position.

Corollary 23.11. *After localizing at $\mathfrak{m}_\pi$, we get*

$$\prod_{i=1}^{\frac{n-1}{2}}(\mu_i + \mu_i^{-1} - 2)$$

where $\{\mu_i\}$ are the Satake parameters of π. This is nonzero because $\mu_i \neq 1$!