Arithmetic Geometry for Physicists

Minhyong Kim

Seoul, August, 2017
I. Splitting primes
Splitting primes

Given a polynomial \( f \in \mathbb{Z}[x] \), the set of splitting primes \( Sp(f) \) of \( f \) consists of the primes that

– do not divide the discriminant \( \Delta(f) \) of \( f \);
– divide some value \( f(n) \), \( n = 1, 2, 3, \ldots \).

Recall that

\[
\Delta(ax^2 + bx + c) = b^2 - 4ac; \quad \Delta(x^3 + bx + c) = -4b^3 - 27c^2,
\]

e tc.

In general \( \Delta(f) = a_n \prod_{i<j}(\alpha_i - \alpha_j)^2 \), where \( a_n \) is the leading coefficient and \( \alpha_i \) are the roots of \( f \).

For \( p \nmid \Delta(f) \), \( p \in Sp(f) \) if and only if \( f(x) = 0 \) has a solution in \( \mathbb{F}_p = \mathbb{Z}/p \).
Example A:

\[ g(x) = x^2 - 5. \]
\[ \Delta(g) = 20. \]

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g(n) )</td>
<td>-4</td>
<td>-1</td>
<td>4</td>
<td>11</td>
<td>20</td>
<td>31</td>
<td>44</td>
<td>59</td>
<td>76</td>
<td>95</td>
</tr>
</tbody>
</table>

The primes that occur are

\[ Sp(g) = \{ 11, 31, 59, 19, \ldots \} \]

These are \( p \equiv \pm 1 \mod 5. \)
Splitting primes

Example B:

\[ h(x) = x^3 + x^2 - 2x - 1. \]

\[ \Delta(h) = 49. \]
We compute

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>( h(n) )</td>
<td>-1</td>
<td>7</td>
<td>29</td>
<td>71</td>
<td>139</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( n )</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>( h(n) )</td>
<td>239</td>
<td>13 \cdot 43</td>
<td>13 \cdot 43</td>
<td>7 \cdot 113</td>
</tr>
</tbody>
</table>

So we see that

\[ Sp(h) = \{13, 29, 43, 71, 113, 239, \ldots\} \]

These are \( p \equiv \pm 1 \mod 7 \).
Splitting primes

Example C:

\[ f(x) = 13249 + 140x + 1588x^2 - 2x^3 + 67x^4 + x^6. \]

Values \( f(n) \), where \( n = 1, 2, 3, \ldots, 10 \):

\[
15043 = 7^2 \cdot 307, \quad 21001, \quad 34063 = 23 \times 1481, \\
60337, \quad 110899, \quad 204313 = 173 \cdot 1181, \\
369871 = 59 \cdot 6269, \quad 651553 = 7^2 \cdot 13297, \quad 1112707, \\
1841449 = 23^2 \cdot 59^2, \ldots
\]

Primes dividing the discriminant: 2, 3, 7, 23, 191.

What is \( Sp(f) \)?
Theorem
The splitting primes of $f$ are exactly $p$ such that the coefficient of $q^p$ is 2 in the series

$$F(q) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} \left[ q^{m^2+mn+6n^2} - q^{2m^2+mn+3n^2} \right].$$

Fact:
$F(q)$ is a modular cusp form of weight 1 for the group $\Gamma_0(23)$, with character $\left( \frac{\cdot}{23} \right)$. 
Splitting primes

Recall that an algebraic number field $K$ is a finite field extension of $\mathbb{Q}$.

This means that

$$K \simeq \mathbb{Q}^d$$

with a multiplication extending that of $\mathbb{Q}$.

For example,

$$\mathbb{Q}[i] \simeq \mathbb{Q}^2, \quad (a, b)(c, d) = (ac - bd, ad + bc);$$

$$\mathbb{Q}[\sqrt{-23}] \simeq \mathbb{Q}^2, \quad (a, b)(c, d) = (ac - 23bd, ad + bc).$$

$$\mathbb{Q}[\zeta_5] \simeq \mathbb{Q}^4;$$

where $\zeta_5 = \exp(2\pi i/5)$.

The dimension $d$ is also called the degree of the field $K$ and denoted $[K : \mathbb{Q}]$.

We say $K$ is Galois if $|\text{Aut}(K)| = d$. 
Splitting primes

An algebraic number field $K$ admits a subring $\mathcal{O}_K$ referred to as its ring of algebraic integers. It is the maximal subring of $K$ isomorphic to $\mathbb{Z}^d$.

For example,

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i];$$
$$\mathcal{O}_{\mathbb{Q}[\zeta_5]} = \mathbb{Z}[\zeta_5];$$
$$\mathcal{O}_{\mathbb{Q}[\sqrt{-23}]} = \mathbb{Z}[(1 + \sqrt{-23})/2].$$

Among other things, an algebraic number field provides us with new primes. That is, given a usual prime $p$, we can write

$$(p) = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_s$$

for prime ideals $\mathfrak{P}_i$ in $\mathcal{O}_K$.

For example, in $\mathbb{Z}[\sqrt{-23}]$

$$(3) = (3, \sqrt{-23} + 1)(3, \sqrt{-23} - 1); \quad (23) = (\sqrt{-23})^2; \quad (5) = (5)$$
Splitting primes

We say $p$ is unramified in $K$ if the $\mathfrak{P}_i$ are all distinct. Otherwise $p$ is ramified in $K$.

For example, 3 is unramified and 23 is ramified in $\mathbb{Q}[\sqrt{-23}]$.

Each $k(\mathfrak{P}_i) := \mathcal{O}_K / \mathfrak{P}_i$ is a finite field extension of $\mathbb{F}_p = \mathbb{Z} / p$, and we have the equality

$$\sum_{i}[k(\mathfrak{P}_i) : \mathbb{F}_p] = d = [K : \mathbb{Q}].$$

This is (essentially) because

$$\mathbb{F}_p^d \simeq \mathbb{Z}^d / p\mathbb{Z}^d \simeq \mathcal{O}_K / p\mathcal{O}_K = \mathcal{O}_K / \prod_i \mathfrak{P}_i \simeq \prod_i \mathcal{O}_K / \mathfrak{P}_i.$$ 

In particular, there are at most $d$ such $\mathfrak{P}_i$. 
Splitting primes

Say \( p \) splits (or splits completely) in \( K \) if \( p \) is unramified and

\[(p) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_d\]

for \( d = \dim_{\mathbb{Q}} K \). (⇔ \([k(\mathfrak{p}_i) : \mathbb{F}_p] = 1 \) for all \( i \).)

Denote by \( Sp(K) \) the set of primes that split in \( K \).

Examples:

In \( \mathbb{Q}[\sqrt{-23}] \), 3 splits, but 5 does not.

In \( \mathbb{Q}[\zeta_n] \), \( p \nmid n \) splits if and only if \( p \equiv 1 \pmod{n} \).
Splitting primes

Any algebraic number field can be written $K = \mathbb{Q}[\alpha]$ for a root $\alpha$ of an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$.

In this form,

- $[K : \mathbb{Q}] = \deg(f)$;
- If $p \nmid \Delta(f) \Rightarrow p$ is unramified;
- When $K$ is Galois, an unramified $p$ is split if and only if

$$f(x) \equiv 0 \mod p$$

has a root, i.e. if and only if $p | f(n)$ for some $n$. That is,

$$Sp(K) \approx Sp(f),$$

where the $\approx$ means that $Sp(K) \setminus Sp(f)$ and $Sp(f) \setminus Sp(K)$ are both finite.
Splitting primes

From here, assume $K$ is Galois.

For every prime $p \in \mathbb{Z}$, considering

$$(p) = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_s$$

get a collection of subgroups

$$D(\mathfrak{P}_i) := \{g \in \text{Gal}(K/\mathbb{Q}) \mid g \mathfrak{P}_i = \mathfrak{P}_i\} \subset \text{Gal}(K/\mathbb{Q}),$$

the decomposition groups of the $\mathfrak{P}_i$.

These are all conjugate inside $\text{Gal}(K/\mathbb{Q})$: that is, for all $i,j$, there is an $a_{ij} \in \text{Gal}(K/\mathbb{Q})$ such that

$$D(\mathfrak{P}_i) = a_{ij} D(\mathfrak{P}_i) a_{ij}^{-1}.$$. 
Thus, given a Galois field $K$, each prime $p$ determines a conjugacy class of subgroups

$$\{D(\mathfrak{p})\}_{\mathfrak{p}|p}$$

in $\text{Gal}(K/\mathbb{Q})$.

The action of $D(\mathfrak{p}_i)$ on $k(\mathfrak{p}_i) = \mathcal{O}_K/\mathfrak{p}_i$ induces a homomorphism

$$D(\mathfrak{p}_i) \longrightarrow \text{Gal}(k(\mathfrak{p}_i)/\mathbb{F}_p) = \langle \sigma_{\mathfrak{p}_i} \rangle.$$

where $\sigma_{\mathfrak{p}_i}$ is the $p$-power map $x \mapsto x^p$.

When $p$ is unramified, that is, for most $p$, this map is an isomorphism:

$$D(\mathfrak{p}_i) \simeq \text{Gal}(k(\mathfrak{p}_i)/\mathbb{F}_p).$$
Splitting primes

Thus, we get an element

\[ Fr_{\mathfrak{P}_i}^K \in D(\mathfrak{P}_i) \subset \text{Gal}(K/\mathbb{Q}), \]

corresponding to \( \sigma_{\mathfrak{P}_i}^{-1} \) characterised by the condition

\[ Fr_{\mathfrak{P}_i}^K(a) = a^{1/p} \mod \mathfrak{P}_i \]

for all \( a \in \mathcal{O}_K \).

Can put this together for all \( \mathfrak{P}_i \) to get a conjugacy class of elements

\[ Fr_p^K = \{ Fr_{\mathfrak{P}_i}^K \} \subset \text{Gal}(K/\mathbb{Q}), \]

the Frobenius class of \( p \).

Note that when \( \text{Gal}(K/\mathbb{Q}) \) is abelian, e.g., \( K = \mathbb{Q}(\zeta_n) \), this is a single element.
Splitting Primes

\[ \mathbb{Q} \subset K \supset \mathcal{O}_K \supset \mathbb{Z} \]

\[(p) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_s \]

\[ k(\mathfrak{p}_i) = \mathcal{O}_K / \mathfrak{p}_i \supset \mathbb{F}_p \]

\[ D(\mathfrak{p}_i) = \{ g \in \text{Gal}(K/\mathbb{Q}) : g \mathfrak{p}_i = \mathfrak{p}_i \} \]

\[ D(\mathfrak{p}_i) \subset \text{Gal}(K/\mathbb{Q}) \]

\[ \cong \leftarrow \text{(if unramified)} \]

\[ Fr^K_{\mathfrak{p}_i} \in \text{Gal}(k(\mathfrak{p})) \]

\[ \{ Fr^K_{\mathfrak{p}_i} \}_i \subset \text{Gal}(K/\mathbb{Q}) \]
Splitting primes

Galois theory and splitting primes:

I. \textit{p is split in} \( K \) \textit{if and only if} \( Fr_p^K = 1 \).

This is because \( p \) split is equivalent to \( [k(\mathfrak{P}_i) : \mathbb{F}_p] = 1 \) for all \( i \), which is exactly when all the extensions \( k(\mathfrak{P}_i) \) of \( \mathbb{F}_p \) are trivial.

II. Chebotarev Density Theorem:

\textit{Let} \( C \subset Gal(K/\mathbb{Q}) \) \textit{be a conjugacy class. Then there are infinitely many primes} \( p \) \textit{such that}

\[ Fr_p^K = C. \]

\textit{In fact, the density of this set of primes is}

\[ |C|/|G|. \]

\textit{In particular, the density of} \( Sp(K) \) \textit{is exactly} \( 1/[K : \mathbb{Q}] \).
Remark on classification of algebraic number fields:

Let $K$ and $K'$ be two finite Galois extensions of $\mathbb{Q}$. Then

$$K \simeq K'$$

if and only if

$$Sp(K) \simeq Sp(K').$$

So, in some sense, the classification of $K$ is the same as the classification of the possible $Sp(K)$. 
Splitting primes

Some infinite Galois groups:

\[ \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \lim_{\leftarrow F} \text{Gal}(F/\mathbb{Q}), \]

where \( F \) runs over Galois number fields.

For a number field \( F \),

\[ \text{Gal}(\overline{F}/F) = \text{Gal}(\overline{\mathbb{Q}}/F) = \{ g \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid g|F = \text{Id} \} \]

Let \( S \) be a finite set of primes. Then

\[ \text{Gal}(\mathbb{Q}_S/\mathbb{Q}) = \lim_{\leftarrow F} \text{Gal}(F/\mathbb{Q}), \]

where \( F \) runs over the Galois extensions of \( \mathbb{Q} \) that are unramified outside \( S \).

Similarly,

\[ \text{Gal}(F_S/F) \]

where \( S \) is a finite set of primes in \( \mathcal{O}_F \).
Galois groups like

\[ \text{Gal}(\mathbb{Q}_S/\mathbb{Q}) = \lim_{\leftarrow F} \text{Gal}(F/\mathbb{Q}), \]

are very important in practice, because these are the ones that arise in nature, and which one can tools to understand.

For a prime \( p \notin S \), can define conjugacy class \( Fr_p \subset \text{Gal}(\mathbb{Q}_S/\mathbb{Q}) \).
Splitting primes

Return to the modular form

\[ F(q) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} [q^{m^2+mn+6n^2} - q^{2m^2+mn+3n^2}] \]

\[ = \sum_{n=1}^{\infty} a_n q^n \]

of weight 1, level 23 and character \((\cdot \mod 23)\).

This means that for

\[ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(23), \]

we have

\[ F(\gamma \tau) = \left( \frac{d}{23} \right) (c \tau + d) F(\tau). \]
Splitting primes

It has an associated $L$-series

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

$$= \prod_p \frac{1}{(1 - a_p p^{-s} + \left(\frac{p}{23}\right) p^{-2s})}.$$

This product decomposition is a manifestation of the fact that $F$ is an eigenform for a Hecke algebra.
Deligne and Serre associated to $F$ a continuous representation

$$\rho_F : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{C})$$

with the following properties:

- $G = \text{Im}(\rho_F) \subset GL_2(\mathbb{C})$ is finite, so that
  $$K = [\overline{\mathbb{Q}}]^{\text{Ker}(\rho_F)},$$
  is an algebraic number field such that $\text{Gal}(K/\mathbb{Q}) \cong G$;
- The primes that ramify in $\mathcal{O}_K$ are exactly the primes dividing the level of $F$, i.e., $p = 23$;
- If $p \neq 23$, then the conjugacy class $Fr_p$ in $G \subset GL_2(\mathbb{C})$, satisfies
  $$\text{Tr}(Fr_p) = a_p$$
  and $\det(Fr_p) = \left(\frac{p}{23}\right)$.

This property is essentially equivalent to an equality

$$L(F, s) = L(\rho_F, s).$$
Splitting primes

The $L$-function of the Galois representation is defined as

$$L(\rho_F, s) = \prod_p \frac{1}{\det([I - p^{-s}Fr_p]|(\mathbb{C}^2)^{I(p)})}. $$

Here, strictly speaking, I should pick a prime $\mathfrak{p}|p$ in $K$. Then there is an exact sequence

$$0 \longrightarrow I(\mathfrak{p}) \longrightarrow D(\mathfrak{p}) \longrightarrow \text{Gal}(k(\mathfrak{p})/\mathbb{F}_p) \longrightarrow 0,$$

defining the subgroup $I(\mathfrak{p})$, called the \textit{inertia subgroup}.

The factors corresponding to $p$ on the right are actually

$$\frac{1}{\det([I - p^{-s}Fr_{\mathfrak{p}_3}]|(\mathbb{C}^2)^{I(\mathfrak{p})})}.$$
Splitting primes

The representation and field $K$ has been constructed in such a way that $a_p = 2$ if and only if $Tr(Fr_p) = 2$.

However, the eigenvalues of $Fr_p$ are roots of 1. Hence

$$Tr(Fr_p) = 2$$

if and only if both eigenvalues are 1, i.e. $Fr_p = Id$.

Hence

$$\{p \mid p \nmid 23, \ a_p = 2\} = Sp(K).$$

But also, $K = \mathbb{Q}(\alpha)$ for $\alpha$ a root of

$$f(x) = 13249 + 140x + 1588x^2 - 2x^3 + 67x^4 + x^6.$$

Thus, for $p \nmid \Delta(f)$, $p \in Sp(f) \subset Sp(K)$ if and only if $a_p = 2$. 
To sum:

Cuspidal Hecke eigenform $F$

\[ \longrightarrow K = (\overline{\mathbb{Q}})^{\text{Ker}(\rho_F)} = \mathbb{Q}(\alpha) \]

where $\alpha$ is a root of $f(x)$.

Field was constructed so that we know $p$ such that $Fr_p = 1$ in $\text{Gal}(K/\mathbb{Q}) = \text{Im}(\rho_F)$. 
Splitting primes

Langlands (refined by many other people):

Given any continuous irreducible representation

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\mathbb{C}),$$

we should have

$$L(\rho, s) = L(F, s)$$

for some ‘automorphic form’ $F$.

Actually, $F$ must be replaced in general by an automorphic representation $\pi$ of $GL_n(\mathbb{A}_\mathbb{Q})$ and there should be a way to associate $\rho_\pi$ to $\pi$.

Similar statement for irreducible continuous motivic representation

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\overline{\mathbb{Q}}_p)$$
Even more generally, given a motivic continuous representation
\[ \rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow G^\vee(\bar{\mathbb{Q}}_p), \]
we should have
\[ \rho \simeq \rho_\pi \]
for an automorphic representation \( \pi \) of
\[ G(\mathbb{A}_\mathbb{Q}), \]
where \( G \) and \( G^\vee \) are Langlands dual pairs of reductive groups.

General idea is that homomorphisms like \( \rho \) should parametrise automorphic representations of \( G(\mathbb{A}_\mathbb{Q}) \).
Remark 1:

Galois representations are hard to construct: They are essentially always constructed as

$$H^i_{et}(\tilde{X}, \mathbb{Q}_p)$$

where $X$ is a variety defined over $\mathbb{Q}$. This admits an action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that factors through some

$$\Gamma_S = \text{Gal}(\mathbb{Q}_S/\mathbb{Q})$$

for a finite set $S$ of primes. Here, $\mathbb{Q}_S$ is the field obtained as a compositum of all finite algebraic extensions $F$ that are unramified outside the finite set $S$ of primes.
Remark 2:

Galois representations are arithmetic gauge fields.

In geometry there is a correspondence

\[ \text{Bundle with flat connection on } X \leftrightarrow \text{Locally constant sheaf on } X \leftrightarrow \text{Representation of } \pi_1(X) \]
Splitting primes

When

\[ X = \text{Spec}(\mathbb{Z}[1/N]), \]

for \( N = \prod_{p \in S} p \), then

\[ \pi_1(X) = \text{Gal}(\mathbb{Q}_S/\mathbb{Q}). \]

Thus a representation of \( \text{Gal}(\mathbb{Q}_S/\mathbb{Q}) \) is interpreted as an arithmetic flat connection on \( \text{Spec}(\mathbb{Z}[1/N]) \).
Splitting Primes

Remark 3:

Galois representations are *motives*.

Given $K$ Galois with Galois group $G$,

$$H^0(\text{Spec}(K), \mathbb{C}) \cong \mathbb{C}[G]$$

$$\cong \prod \dim(\rho) \rho,$$

where

$$\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_n(\mathbb{C})$$

run over irreducible representations that occur in $H^0(\text{Spec}(K), \mathbb{C})$. That is, the $\rho$ are *constituent motives* of $\text{Spec}(K)$, manifested as

$$\zeta_K(s) = \prod L(\rho, s)^{\dim(\rho)}.$$
Remark 4:

The group $\Gamma_S$ is essentially a topologically finitely-generated group. Its representations lie in moduli spaces

$$\mathcal{M}(\Gamma_S, G)$$

of representations

$$\rho : \Gamma_S \to G$$

where $G$ is a $p$-adic Lie group. The structure of this moduli space is very similar to a space

$$\mathcal{M}(M, G)$$

of $G$-connections on a three manifold $M$ studied by physicists.
Splitting primes

Remark 5:
In physics:

strings

- gauge fields
- automorphic forms
Interlude: What is arithmetic geometry?
Interlude: What is arithmetic geometry?

*Arithmetic geometry* is the study of arithmetic geometries.

These are schemes of finite type, i.e., schemes that are finite unions of those of the form

$$\text{Spec}(\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)),$$

and maps between them, for example,

$$\text{Spec}(\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)) \longrightarrow \text{Spec}(\mathbb{Z})$$

and

$$\text{Spec}(\mathbb{Z}) \longrightarrow \text{Spec}(\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)).$$
Interlude: What is arithmetic geometry?

Recall that scheme theory associates to a commutative ring $A$ with unity, a (ringed) space

$$\text{Spec}(A),$$

whose underlying set consists of the prime ideals in $A$.

For example,

$$\text{Spec}(\mathbb{C}[x]) = \{(0)\} \cup \mathbb{C}.$$

More generally,

$$\text{Spec}(\mathbb{C}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m))$$

is the variety given as the zero set of the $f_i$, enriched by adding a point for each subvariety.

$$\text{Spec}(\mathbb{Z}) = \{(0)\} \cup \{2, 3, 5, 7, 11, \ldots, 37, \ldots, 691, \ldots, 1112707, \ldots\}$$

$$\text{Spec}(\mathbb{Q}[x]) = \{(0)\} \cup \{\text{irreducible polynomials}\}/\mathbb{Q}^\times$$
Interlude: What is arithmetic geometry?

The basic open subsets in $Y = \text{Spec}(A)$ are of the form

$$U_a := \text{Spec}(A[1/a]) \subset Y.$$ 

There is a sheaf of rings $\mathcal{O}_Y$ on $Y$ called the structure sheaf determined by the values

$$\mathcal{O}_Y(U_a) = A[1/a].$$

A general scheme is a topological space $X$ equipped with a sheaf of rings $\mathcal{O}_X$ such that the pair $(X, \mathcal{O}_X)$ is locally isomorphic to $(\text{Spec}(A), \mathcal{O}_{\text{Spec}(A)})$. 
Interlude: What is arithmetic geometry?

The basic maps of schemes are of the form

\[ \text{Spec}(B) \longrightarrow \text{Spec}(A) \]

determined by a ring homomorphism \( A \longrightarrow B \). At the level of sets, one takes the inverse image of prime ideals.

General maps between schemes are locally of this form.

Suppose \( x \) is a point in \( X \). Then \( x \in \text{Spec}(A) \subset X \) for some \( A \), so that \( x \) corresponds to a prime ideal \( P \) in \( A \).

Thus, we get the map

\[ \text{Spec}(A/P) \longrightarrow \text{Spec}(A) \subset X, \]

which encodes the information of \( x \).
Interlude: What is arithmetic geometry?

The field

\[ k(x) := \text{Frac}(A/P) \]

is called the \textit{residue field} at \( x \), and we have the map

\[ \text{Spec}(k(x)) \longrightarrow \text{Spec}(A/P) \longrightarrow \text{Spec}(A) \longrightarrow X. \]

This map is often identified with the point \( x \).

Example:

\( X = \text{Spec}(\mathbb{Z}[t]). \)

\( x = (t, p) \)

\[ \text{Spec}(\mathbb{F}_p) \hookrightarrow X. \]
**Interlude: What is arithmetic geometry?**

\[ X = \text{Spec}(\mathbb{Z}[t]). \]

\[ x = (t) \]

\[ \text{Spec}(\mathbb{Q}) \hookrightarrow \text{Spec}(\mathbb{Z}) \hookrightarrow X. \]

\[ x = (p) \]

\[ \text{Spec}(\mathbb{F}_p(t)) \hookrightarrow \text{Spec}(\mathbb{F}_p[t]) \hookrightarrow X. \]
Interlude: What is arithmetic geometry?

\[ X = \text{Spec}(\mathbb{Z}[t]). \]

\[ x = (f(t)), \text{ where } f \in \mathbb{Z}[t] \text{ is an irreducible polynomial.} \]

\[ \text{Spec}(F) \hookrightarrow \text{Spec}(\mathbb{Z}[t]/(f(t))) \hookrightarrow X, \]

where \( F = \mathbb{Q}[t]/(f(t)) \) is an algebraic number field.

\[ x = (p, f(t)), \text{ where } f(t) \text{ is degree } d \text{ and irreducible mod } p. \]

\[ \text{Spec}(\mathbb{F}_p^d) = \text{Spec}(\mathbb{F}_p[t]/(f(t))) \hookrightarrow X. \]
Interlude: What is arithmetic geometry?

\[ X = \text{Spec}(\mathbb{Z}[t]). \]
\[ x = (0) \]

\[ \text{Spec}(\mathbb{Q}(t)) \hookrightarrow \text{Spec}(\mathbb{Z}[t]) = X. \]
Algebra or Geometry?

Figure: Mumford’s picture of Spec($\mathbb{Z}[x]$)
Interlude: What is arithmetic geometry?

Another point that arises from $x$ is

$$\text{Spec}(\overline{k(x)}) \rightarrow \text{Spec}(k(x)) \rightarrow X,$$

where $\overline{k(x)}$ is the separable closure of $k(x)$. This map is sometimes called the \textit{geometric point} with image $x$.

For example, $\mathbb{Z} \rightarrow \mathbb{Z}/p = \mathbb{F}_p \hookrightarrow \overline{\mathbb{F}}_p$ gives rise to the geometric point

$$\text{Spec}(\overline{\mathbb{F}}_p) \rightarrow \text{Spec}(\mathbb{F}_p) \hookrightarrow \text{Spec}(\mathbb{Z}).$$

Also,

$$\text{Spec}(\overline{\mathbb{Q}}) \rightarrow \text{Spec}(\mathbb{Q}) \hookrightarrow \text{Spec}(\mathbb{Z}).$$

$$\text{Spec}(\overline{\mathbb{Q}(t)}) \rightarrow \text{Spec}(\mathbb{Q}(t)) \hookrightarrow \text{Spec}(\mathbb{Z}[t]).$$
Interlude: What is arithmetic geometry?

The arrow

$$\text{Spec}(\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)) \rightarrow \text{Spec}(\mathbb{Z})$$

is opposite to the inclusion

$$\mathbb{Z} \leftarrow \mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)$$

but the geometric perspective encourages us to view the scheme as a fibre-bundle over $\text{Spec}(\mathbb{Z})$.

Reducing modulo a prime $p$ gives us an inclusion

$$\mathbb{F}_p \leftarrow \mathbb{F}_p[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m),$$

which in geometric form

$$\text{Spec}(\mathbb{F}_p[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)) \rightarrow \text{Spec}(\mathbb{F}_p)$$

is the fibre of the previous map over the point $p$. 
Interlude: What is arithmetic geometry?

Other important basic morphisms include:

Inclusion of a point:

\[
\text{Spec}(\mathbb{F}_p) \hookrightarrow \text{Spec}(\mathbb{Z});
\]

Inclusion of a point through a tubular neighbourhood:

\[
\text{Spec}(\mathbb{F}_p) \hookrightarrow \text{Spec}(\mathbb{Z}_p) \rightarrow \text{Spec}(\mathbb{Z});
\]

An open embedding:

\[
\text{Spec}(\mathbb{Z}[1/N)) \hookrightarrow \text{Spec}(\mathbb{Z});
\]

Refinements of open embeddings:

\[
\text{Spec}(\mathbb{Z}) \supset \text{Spec}(\mathbb{Z}[1/2]) \supset \text{Spec}(\mathbb{Z}[1/6]) \supset \text{Spec}(\mathbb{Z}[1/30]) \cdots .
\]
Interlude: What is arithmetic geometry?

Note that if $N = \prod_{i=1}^{k} p_i^{e_i}$, then

$$\text{Spec}(\mathbb{Z}[1/N]) = \text{Spec}(\mathbb{Z}[1/p_1, 1/p_2, \ldots, 1/p_k])$$

$$= \text{Spec}(\mathbb{Z}) \setminus \{p_1, p_2, \ldots, p_k\}.$$ 

Sometimes consider limits like

$$\text{Spec}(\mathbb{Q}) = \bigcap_N \text{Spec}(\mathbb{Z}[1/N]).$$

A variety over a finite field looks like

$$\text{Spec}(\mathbb{F}_p[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)) \rightarrow \text{Spec}(\mathbb{F}_p) \leftarrow \text{Spec}(\mathbb{Z}),$$

which is fibred over $\text{Spec}(\mathbb{Z})$ with only one fibre.
Interlude: What is arithmetic geometry?

The arrow

\[ \text{Spec}(\mathbb{Z}) \longrightarrow \text{Spec}(\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)) \]

is opposite to a ring homomorphism

\[ \mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m) \longrightarrow \mathbb{Z}; \]

Hence, it corresponds to an integral solution of the system of equations

\[ f_1 = 0, f_2 = 0, \ldots, f_m = 0. \]

Similarly, an arrow

\[ \text{Spec}(A) \longrightarrow \text{Spec}(\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)) \]

corresponds to solutions with entries in \( A \) (e.g. \( \mathbb{Z}_p, \mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \ldots \)).
Interlude: What is arithmetic geometry?

Equation

\[ y^2 = x^3 - 2 \]

has solution

\[
\left( \frac{2340922881}{58675600}, \frac{113259286337279}{449455096000} \right)
\]
Interlude: What is arithmetic geometry?

Picture 1:

\[ y^2 = x^3 - 2 \]

View of classical algebraic geometry, say à là Weil.
Interlude: What is arithmetic geometry?

Picture 2:

\[ B = \text{Spec}(\mathbb{Q}) \]

\[ X = \text{Spec}(\mathbb{Q}[x, y]/(y^2 - x^3 + 2)) \]

This view emphasised by A. Grothendieck.
Interlude: What is arithmetic geometry?

Picture 3:

\[ B_N = \text{Spec}(\mathbb{Z}[1/N]) \]
\[ \mathfrak{X}_N = \text{Spec}(\mathbb{Z}[1/N][x, y]/(y^2 - x^3 + 2)) \]

where, \( N = 3830 \).
Interlude: What is arithmetic geometry?

We have

$$449455096000 = 2^6 \cdot 5^3 \cdot 383^3$$

and

$$58675600 = 2^4 \cdot 5^3 \cdot 383^2$$

So solution

$$\left( \frac{2340922881}{58675600}, \frac{113259286337279}{449455096000} \right)$$

has coordinates in ring

$$\mathbb{Z}\left[ \frac{1}{2 \cdot 5 \cdot 383} \right] = \mathbb{Z}[1/3830].$$

Should think of it as having ‘poles’ at (2), (5), (383).
Interlude: What is arithmetic geometry?

Can also consider the homogeneous equation

$$zy^2 - x^3 + 2z^3 = 0$$

or the scheme

$$\mathfrak{X} = \text{Proj}(\mathbb{Z}[x, y, z]/(zy^2 - x^3 + 2z^3)).$$

This is a union of three pieces

$$\text{Spec}(\mathbb{Z}[x, y]/(y^2 - x^3 + 2));$$
$$\text{Spec}(\mathbb{Z}[x, z]/(z - x^3 + 2z^3));$$
$$\text{Spec}(\mathbb{Z}[y, z]/(zy^2 - 1 + 2z^3)).$$

Then the point

$$(89426414521128940 : 2456480661369244231 : 65930118577144000)$$

is a map

$$\text{Spec}(\mathbb{Z}) \rightarrow \mathfrak{X}.$$
Interlude: What is arithmetic geometry?

Picture 4:

\[
\text{Spec}(\mathbb{Z}) \quad \begin{array}{cccccc}
2 & 3 & 5 & 7 & 11 & 13 \\
\vdots & & & & & \\
379 & 383 & 389
\end{array}
\]

\[\mathfrak{x}_7 \quad \mathfrak{x}_{13} \quad \cdots \quad \mathfrak{x} \quad \cdots \quad P\]
Interlude: What is arithmetic geometry?

Topology:

Basic open sets in the Zariski topology on $\text{Spec}(A)$ are of the form $\text{Spec}(A[1/a])$. Grothendieck topologies regard suitable maps $\text{Spec}(B) \rightarrow \text{Spec}(A)$ as open sets.

Intersections of open sets are replaced by fibre products

$$\text{Spec}(B) \times_{\text{Spec}(A)} \text{Spec}(B) \rightarrow \text{Spec}(B) \rightarrow \text{Spec}(A),$$

where

$$\text{Spec}(B) \times_{\text{Spec}(A)} \text{Spec}(B) = \text{Spec}(B \otimes_A B).$$
Interlude: What is arithmetic geometry?

The most important one (so far) is the étale topology.

A map

\[ \text{Spec}(B) \longrightarrow \text{Spec}(A) \]

is called étale essentially if \( B \) is locally of the form

\[ A[x]/(f(x)) \]

where \( f \in A[x] \) is a monic polynomial such that \( \Delta(f) \in A^\times \).

The key point is that all fibers

\[ \text{Spec}(B \otimes_A (A/m)) = \text{Spec}((A/m)[x]/(\bar{f})) \longrightarrow \text{Spec}(A/m) \]

have the same number of geometric points.
Interlude: What is arithmetic geometry?

For the map

$$\text{Spec}(\mathbb{C}[x][y]/(y^n - x)) \longrightarrow \text{Spec}(\mathbb{C}[x]),$$

we have

$$\Delta = (-1)^{n-1} n^n x^{n-1}.$$ 

This is *not* a unit in $\mathbb{C}[x]$, so the map is not étale.

However,

$$\text{Spec}(\mathbb{C}[x, x^{-1}][y]/(y^n - x)) \longrightarrow \text{Spec}(\mathbb{C}[x, x^{-1}])$$

is étale.
Interlude: What is arithmetic geometry?

Similarly,

\[ \text{Spec}(\mathbb{F}_p[x, x^{-1}][y]/(y^n - x)) \longrightarrow \text{Spec}(\mathbb{F}_p[x, x^{-1}]) \]

is étale if \( p \nmid n \).

The map

\[ \text{Spec}(\mathbb{Z}[x]/(x^2 + 23)) \longrightarrow \text{Spec}(\mathbb{Z}) \]

is not étale,

But

\[ \text{Spec}(\mathbb{Z}[1/46][x]/(x^2 + 23)) \longrightarrow \text{Spec}(\mathbb{Z}[1/46]) \]

is étale.
Interlude: What is arithmetic geometry?

Together with the notion of an étale open map

\[ Y \longrightarrow X, \]

have the notion of an étale open covering

\[ (U_i \longrightarrow X)_{i \in I}. \]

Can use this to form a complex \( C((U_i), \mathbb{Z}/n) \):

\[
\prod_i C(U_i, \mathbb{Z}/n) \longrightarrow \prod_{i < j} C(U_i \times_X U_j, \mathbb{Z}/n)
\]

\[
\longrightarrow \prod_{i < j < k} C(U_i \times_X U_j \times_X U_k, \mathbb{Z}/n) \longrightarrow \cdots
\]
Étale cohomology with coefficients in $\mathbb{Z}/n$ is then defined as

$$H^i(X, \mathbb{Z}/n) := H^i(\lim_{\to} C^*((U_i), \mathbb{Z}/n)).$$

[This is not always right, but good enough for many purposes.]

Also,

$$H^i(X, \mathbb{Z}_p) := \lim_{\leftarrow} H^i(X, \mathbb{Z}/p^n),$$

and

$$H^i(X, \mathbb{Q}_p) \simeq H^i(X, \mathbb{Z}_p) \otimes \mathbb{Q}_p.$$
Interlude: What is arithmetic geometry?

There is a collection of techniques for computing étale cohomology, for example,

(1) Comparison with complex cohomology;
(2) Comparison with (pro-finite) group cohomology;
(3) Long exact sequences depending on ‘breaking up’ $X$.
(4) Spectral sequences depending on maps between spaces;
(5) Generalisation to sheaves and ‘breaking up sheaves’.
(6) Operations on sheaves;
(7) Various base-change theorems;
(8) Lefschetz trace formula.
(9) etc.
Interlude: What is arithmetic geometry?

For example, if $X$ is a variety over $\bar{\mathbb{Q}}$, then

$$H^i(X, \mathbb{Z}/n) \simeq H^i(X(\mathbb{C}), \mathbb{Z}/n)$$

and the same for all the other coefficients.

On the other hand, suppose $X$ is defined over $\mathbb{Q}$ and $\bar{X}$ is the same variety regarded as being over $\bar{\mathbb{Q}}$.

The difference is between

$$\text{Spec}(\mathbb{Q}[x_1, \ldots, x_n]/(f_1, \ldots, f_m))$$

and

$$\text{Spec}(\bar{\mathbb{Q}}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)).$$
Interlude: What is arithmetic geometry?

Then

\[ H^i(\tilde{X}, \mathbb{Z}/n) \simeq H^i(\tilde{X}(\mathbb{C}), \mathbb{Z}/n). \]

But the left hand side has a natural action of \( \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \).

Thus, we end up with ‘arithmetic symmetry’ acting on complex cohomology.
Interlude: What is arithmetic geometry?

Simple application:

Suppose $X$ is a complex variety and $\sigma \in \text{Aut}(\mathbb{C})$.

Let $X^\sigma$ be obtained from $X$ by changing all the coefficients of the defining equation for $X$ using $\sigma$.

For example, suppose the equations defining $X$ has all coefficients algebraic except for some occurrences of $\pi$. There is a $\sigma$ corresponding to substitution of all occurrences of $\pi$ by $e$.

Then

$$H^i(X, \mathbb{Z}) \simeq H^i(X^\sigma, \mathbb{Z}).$$

Proof: The map $\sigma : X \longrightarrow X^\sigma$ is a continuous isomorphism for the étale topology and induces

$$H^i(X, \mathbb{Z}/n) \simeq H^i(X^\sigma, \mathbb{Z}/n)$$

for all $n$. 

Interlude: What is arithmetic geometry?

But more serious application is when $X$ is defined over $\mathbb{Q}$, so that one ends up with a Galois representation

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(H^i(\tilde{X}, \mathbb{Q}_p)).$$

These are the main examples of Galois representations studied in arithmetic geometry.
Interlude: What is arithmetic geometry?

Example: \( X = \mathbb{G}_m = \text{Spec}(\mathbb{Q}[x, x^{-1}]) \). Then

\[ H^1(\bar{X}, \mathbb{Z}_p) \cong \mathbb{Z}_p(-1) := \text{Hom}(\mathbb{Z}_p(1), \mathbb{Z}_p), \]

as a representation of \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \), where

\[ \mathbb{Z}_p(1) := \lim_{\leftarrow} \mu_{p^n}, \]

and \( \mu_i \) is the group of \( i \)--th root of unity. Thus,

\[ \mathbb{Z}_p(1) \cong \mathbb{Z}_p \]

as a group, but the Galois action is determined by the quotients

\[ \mu_{p^n} \cong \mathbb{Z}/p^n. \]
Interlude: What is arithmetic geometry?

Example: When $E$ is an elliptic curve,

$$H^1(\tilde{X}, \mathbb{Z}_p) \cong T_pE \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1).$$

Here,

$$T_pX = \lim_{\leftarrow n} E[p^n].$$

This is still quite difficult when $E$ doesn’t have complex multiplication. Most of the time

$$Im(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \cong \text{Aut}(H_1(\tilde{E}, \mathbb{Z}_p)).$$

When $E$ has complex multiplication the action can be described relatively explicitly in terms of class field theory and the main theorem of complex multiplication.
Interlude: What is arithmetic geometry?

Most other cases are difficult. Among the best understood are Galois representations associated to modular forms, which are obtained as pieces of the étale cohomology of Kuga-Sato varieties. One proves identities like

\[ a_p = \text{Tr}(Fr_p) \]

by relating the action of \( Fr_p \) to the action of a Hecke correspondence \( T_p \), and using the fact that \( a_p \) is eigenvalue of \( T_p \) on the modular form \( F \).
Interlude: What is arithmetic geometry?

This kind of phenomena persists for the cohomology of Shimura varieties, where the étale cohomology tends to have actions of both Galois groups and Hecke algebra. This often allows associations like

\[ \pi \mapsto \rho_\pi \]

from automorphic representations to Galois representations.

For automorphic representations of groups that do not have associated Shimura varieties, one uses versions of Langlands functoriality to move the computations to Shimura varieties.
Interlude: What is arithmetic geometry?

However, one quite general fact is that the homomorphism

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(H^i(\overline{X}, \mathbb{Z}_p))$$

factors through a quotient

$$\text{Gal}(\mathbb{Q}_S/\mathbb{Q}) \cong \pi_1(\text{Spec}(\mathbb{Z}[1/S]))$$

and defines a point in a moduli space

$$\mathcal{M}(\text{Spec}(\mathbb{Z}[1/S]), GL_n(\mathbb{Z}_p)).$$
Interlude: What is arithmetic geometry?

Reason:
Can ‘spread out’ $X$ into

\[ X \hookrightarrow X_S \]

\[ \downarrow \quad \downarrow \]

\[ \text{Spec}(\mathbb{Q}) \hookrightarrow \text{Spec}(\mathbb{Z}[1/S]) \]

where the right hand side is a fibre bundle.
General theme:

Arithmetic geometries are quite different from the manifolds that come up in physics. However, moduli spaces of $G$-bundles on such spaces are quite close to moduli spaces of physics.

In particular, when

$$X = \text{Spec}(\mathbb{Z}[1/N]),$$

the moduli space

$$\mathcal{M}(X, GL_n(\mathbb{Z}_p))$$

of principal $GL_n(\mathbb{Z}_p)$-bundles on $X$ parametrises Galois representations of the sort standardly studied in number theory, and one might attempt to look at them from the point of view of physics, especially TQFT.
Interlude: What is arithmetic geometry?

\[ \mathcal{M}(X, GL_n(\mathbb{Z}_p))^{\leq w}_{Mot} \xrightarrow{\text{loc}} [\prod' p \ WD(X_v, GL_n(\mathbb{Z}_p))_{\mathbb{C}}]^{\leq w} \]

\[ \mathcal{M}(X, GL_n(\mathbb{Z}_p)) \supset \mathcal{M}(X, GL_n(\mathbb{Z}_p))_{Mot} \xleftarrow{\text{loc}} \prod' p \ WD(X_v, GL_n(\mathbb{Z}_p))_{\mathbb{C}} \]
Interlude: What is arithmetic geometry?

The elements

\[ (((φ_p, N_p))_p \in \prod_p \text{WD}(X_v, GL_n(\mathbb{Z}_p)))_C \]

consist of the following data:

- \( φ_p \in GL_n(\mathbb{C}) \), semi-simple;
- \( N_p \in M_n(\mathbb{C}) \) nilpotent, such that

\[ φ_p^{-1}N_pφ_p = pN_p, \]

and \( N_p = 0 \) for most \( p \);
- There is a \( w \) such that

\[ \|φ_p\| \leq p^w \]

for all \( p \).
Interlude: What is arithmetic geometry?

\[
L(((\phi_p, N_p))_p)) = \prod_p \frac{1}{\det([I - \phi_p]|(\mathbb{C}^n)^{N=0})}.
\]

Will not converge in general. Get a function

\[
L : \left[\prod_p WD(X_v, GL_n(\mathbb{Z}_p))_\mathbb{C}\right]^{\leq w} \rightarrow \mathbb{C}
\]

for \(w = w_0\) sufficiently small, say \(w_0 = -2\).
Interlude: What is arithmetic geometry?

Change

$$(((φ_p, N_p))_p \rightarrow (((φ_p, N_p))_p(s) := ((p^{-s}φ_p, N_p))_p.$$ 

Then

$$(((p^{-s}φ_p, N_p))_p(s) \in \prod_{p} WD(X_v, GL_n(\mathbb{Z}_p))_C]^{<w_0}$$

for $\text{Re}(s) >> 0$.

When $((φ_p, N_p))_p = \text{loc}(ρ)$, then write

$$L(ρ) = L(\text{loc}(ρ))$$

and

$$L(ρ(s)) = L(\text{loc}(ρ)(s)).$$
Interlude: What is arithmetic geometry?

Within region of convergence, if $n \in \mathbb{Z}$,

$$L(\rho(n)) = L(\rho(n)).$$

Here, left hand side refers to $\rho \otimes \mathbb{Z}_p(n)$. 
Interlude: What is arithmetic geometry?

(Part of) Hasse-Weil conjecture:

If

\[ \rho \in \mathcal{M}(X, GL_n(\mathbb{Z}_p))_{\text{Mot}}^{\leq w}, \]

then

\[ L(\rho(s)) \]

extends to analytic function of \( s \).

As a consequence, one can define

\[ L : \mathcal{M}(X, GL_n(\mathbb{Z}_p))_{\text{Mot}} \rightarrow \mathbb{C} \]

by

\[ L(\rho) = L([\rho(-n)](n)) \]

for \( n \)-sufficiently large.
Interlude: What is arithmetic geometry?

Conjectures of Beilinson and Deligne:

\[ L(\rho)/\Omega_\rho \in \bar{\mathbb{Q}}, \]

where \( \Omega_\rho \) is a period.
Interlude: What is arithmetic geometry?

(Part of the) Main conjecture of Iwasawa theory:

There exists a $p$-adic analytic extension given by the vertical arrow:

$$M(X, GL_n(\mathbb{Z}_p)) \subseteq M(X, GL_n(\mathbb{Z}_p))_{Mot}$$

$L_p$ is called the $p$-adic $L$-function.
Interlude: What is arithmetic geometry?

The moduli space $\mathcal{M}(X, \text{GL}_n(\mathbb{Z}_p))$ carries a a determinant line bundle

$$\text{DET} \rightarrow \mathcal{M}(X, \text{GL}_n(\mathbb{Z}_p))$$

whose fibre over $[\rho]$ is

$$\text{DET}_{[\rho]} = \det H^*_c(X, \rho).$$

Kato has conjectured the existence of a canonical trivialisation

$$Z \in \Gamma(\mathcal{M}(X, \text{GL}_n(\mathbb{Z}_p)), \text{DET})$$

more or less equivalent to the main conjecture.

Can one give ‘physics constructions’ of such trivialisations?
Interlude: What is arithmetic geometry?

$L$-functions are believed to be a powerful unified approach to arithmetic geometry.

For example, if $\rho_E = T_p E$ is the representation given by the torsion points of an elliptic curve $E/\mathbb{Q}$, then it is conjectured that

$$\text{ord}_{s=0} L(\rho(s)) = \text{rank} E(\mathbb{Q}).$$

However, even in the best of all possible worlds, $L$-functions carry linearised information about arithmetic schemes.

A wild hope is that a more dynamic quantum theory of spaces like $M(X, G)$ will help with the study of non-linear invariants as well.