An Invitation to the Arithmetic Langlands

Geometric Langlands Reading Seminar 1

Daebeom Choi

January 26, 2024

University of Pennsylvania

Table of contents

A Naive Introduction to the Langlands Program

Solving Equations

Fundamental Problem in Number Theory

Let $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$. Find all rational/integral solutions of

$$f(x_1, \cdots, x_n) = 0.$$

This is known to be a very hard problem. For example,

$$f(x_1, x_2, x_3) = x_1^n + x_2^n - x_3^n = 0$$

seems like a hard problem.

Solving Equations

Fundamental Problem in Number Theory

Let $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$. Find all rational/integral solutions of

$$f(x_1, \cdots, x_n) = 0.$$

This is known to be a very hard problem. For example,

$$f(x_1, x_2, x_3) = x_1^n + x_2^n - x_3^n = 0$$

seems like a hard problem.

Easier Problem

Let $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$.

1. When does $f(x_1, \cdots, x_n) = 0$ have a solution in $\mathbb{F}_p$?
2. How many solutions are there?

Quadratic Reciprocity

Let's begin with the simplest nontrivial case: $f(x) = x^2 - m$.

$m = 5$

Let $f(x) = x^2 - 5$. Then

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff p \equiv \pm 1 \bmod 5 \text{ or } p = 2, 5.$$

Quadratic Reciprocity

Let's begin with the simplest nontrivial case: $f(x) = x^2 - m$.

$m = 5$

Let $f(x) = x^2 - 5$. Then

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff p \equiv \pm 1 \bmod 5 \text{ or } p = 2, 5.$$

Quadratic Reciprocity

Let $f(x) = x^2 - m$, m square-free. Then there exists a congruence class S mod $4m$ such that, if $p \nmid 4m$, then

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff p \in S \bmod 4m.$$

Harder Case

What happens if we consider a cubic polynomial?

Cubic Equation

Let $f(x) = x^3 + x^2 - 2x - 1$. Then the list of primes for which $f(x) = 0 \bmod p$ has a solution includes

$$p = 7, 13, 29, 41, 43, 71, 83, 97, 113, 127, \cdots$$

Harder Case

What happens if we consider a cubic polynomial?

Cubic Equation

Let $f(x) = x^3 + x^2 - 2x - 1$. Then the list of primes for which $f(x) = 0 \bmod p$ has a solution includes

$$p = 7, 13, 29, 41, 43, 71, 83, 97, 113, 127, \cdots$$

Indeed,

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff p \equiv \pm 1 \bmod 7 \text{ or } p = 7.$$

Class Field Theory

The essence of the class field theory is that this is always possible if the Galois group of f is abelian.

Class Field Theory

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial **whose Galois group is abelian**. Then, there exists a number N, called the **conductor** of f, and a congruence class S mod N such that

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff p \in S \bmod N$$

apart from a finite number of exceptions.

Note that the Galois group of $x^3 + x^2 - 2x - 1$ is C_3.

Class Field Theory

The essence of the class field theory is that this is always possible if the Galois group of f is abelian.

Class Field Theory

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial **whose Galois group is abelian**. Then, there exists a number N, called the **conductor** of f, and a congruence class S mod N such that

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff p \in S \bmod N$$

apart from a finite number of exceptions.

Note that the Galois group of $x^3 + x^2 - 2x - 1$ is C_3.

Naive form of the Langlands Program

Extend this to **arbitrary** monic irreducible $f(x)$.

An Example

Let $f(x) = x^3 - x^2 + 1$, whose Galois group is S_3. The list of primes for which $f(x) = 0 \mod p$ has a solution includes

$$5, 7, 11, 17, 19, 23, 37, 43, 53, 59, 61, 67, 79, 83, 89, 97, \cdots$$

Can you guess the pattern?

An Example

Let $f(x) = x^3 - x^2 + 1$, whose Galois group is S_3. The list of primes for which $f(x) = 0 \bmod p$ has a solution includes

$$5, 7, 11, 17, 19, 23, 37, 43, 53, 59, 61, 67, 79, 83, 89, 97, \cdots$$

Can you guess the pattern?

Answer

Let

$$F(q) = q \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{23n}) = \sum_{n=1}^{\infty} a_n q^n.$$

Then

$$\exists x \in \mathbb{F}_p \text{ s.t. } f(x) = 0 \iff a_p = 2 \text{ or } 0 \text{ or } p = 23.$$

Note: $a_p = -1, 0$ or 2. Therefore this is equivalent to $a_p \neq -1$.

The list of primes for which $f(x) = 0 \bmod p$ does **not** have a solution includes

$$2, 3, 13, 29, 31, 41, 47, 71, 73, \cdots$$

and

$$\begin{aligned} F(q) = & q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25} + q^{26} \\ & + q^{27} - q^{29} - q^{31} + q^{39} - q^{41} - q^{46} - q^{47} + q^{48} + q^{49} \\ & - q^{50} - q^{54} + q^{58} + 2q^{59} + q^{62} + q^{64} - q^{69} - q^{71} - q^{73} + \cdots \end{aligned}$$

The list of primes for which $f(x) = 0 \bmod p$ does **not** have a solution includes

$$2, 3, 13, 29, 31, 41, 47, 71, 73, \cdots$$

and

$$\begin{aligned} F(q) = & q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25} + q^{26} \\ & + q^{27} - q^{29} - q^{31} + q^{39} - q^{41} - q^{46} - q^{47} + q^{48} + q^{49} \\ & - q^{50} - q^{54} + q^{58} + 2q^{59} + q^{62} + q^{64} - q^{69} - q^{71} - q^{73} + \cdots \end{aligned}$$

Less Naive form of the Langlands Program

For **arbitrary** monic irreducible $f(x)$, $\exists$ a special function F whose coefficients contain the information whether $f(x) = 0$ is solvable or not apart from a finite number of exceptions.

The list of primes for which $f(x) = 0 \bmod p$ does **not** have a solution includes

$$2, 3, 13, 29, 31, 41, 47, 71, 73, \cdots$$

and

$$\begin{aligned} F(q) =& q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25} + q^{26} \\ &+ q^{27} - q^{29} - q^{31} + q^{39} - q^{41} - q^{46} - q^{47} + q^{48} + q^{49} \\ &- q^{50} - q^{54} + q^{58} + 2q^{59} + q^{62} + q^{64} - q^{69} - q^{71} - q^{73} + \cdots \end{aligned}$$

Less Naive form of the Langlands Program

For **arbitrary** monic irreducible $f(x)$, $\exists$ a special function F whose coefficients contain the information whether $f(x) = 0$ is solvable or not apart from a finite number of exceptions.

Langlands-Tunnell Theorem, 1981

We can do this if $\deg f \leq 4$.

One more Example, but with two variables

Let

$$f(x, y) = y^2 + y - x^3 + x^2.$$

Let n_p be the number of solutions of $f(x, y) = 0$ in $\mathbb{F}_p$, and $b_p := p - n_p$.

p	2	3	5	7	11	13	17	19	23	29	31
b_p	-2	-1	1	-2	1	4	-2	0	-1	0	7

One more Example, but with two variables

Let

$$f(x,y) = y^2 + y - x^3 + x^2.$$

Let n_p be the number of solutions of $f(x,y) = 0$ in $\mathbb{F}_p$, and $b_p := p - n_p$.

p	2	3	5	7	11	13	17	19	23	29	31
b_p	-2	-1	1	-2	1	4	-2	0	-1	0	7

Let

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum_{n=1}^{\infty} a_n q^n$$

Eichler Reciprocity

$$a_p = b_p$$

p	2	3	5	7	11	13	17	19	23	29
b_p	-2	-1	1	-2	1	4	-2	0	-1	0

$$\begin{aligned} F(q) = & q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} \\ & + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 0q^{19} + 2q^{20} + 2q^{21} \\ & - 2q^{22} - q^{23} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 0q^{29} + 2q^{30} + \cdots \end{aligned}$$

p	2	3	5	7	11	13	17	19	23	29
b_p	-2	-1	1	-2	1	4	-2	0	-1	0

$$\begin{aligned} F(q) = & q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} \\ & + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 0q^{19} + 2q^{20} + 2q^{21} \\ & - 2q^{22} - q^{23} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 0q^{29} + 2q^{30} + \cdots \end{aligned}$$

Taniyama-Shimura-Weil Conjecture, or the Modularity Theorem, proved by Taylor-Wiles, Breuil-Conrad-Diamond-Taylor

We can do this for any elliptic curve over $\mathbb{Q}$.

p	2	3	5	7	11	13	17	19	23	29
b_p	-2	-1	1	-2	1	4	-2	0	-1	0

$$\begin{aligned} F(q) = & q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} \\ & + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 0q^{19} + 2q^{20} + 2q^{21} \\ & - 2q^{22} - q^{23} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 0q^{29} + 2q^{30} + \cdots \end{aligned}$$

Taniyama-Shimura-Weil Conjecture, or the Modularity Theorem, proved by Taylor-Wiles, Breuil-Conrad-Diamond-Taylor

We can do this for any elliptic curve over $\mathbb{Q}$.

Another Naive Form of the Langlands Program

Extend this to general equations.

Galois Representations and Modular Forms

Dedekind Domain

Dedekind Domain

A **Dedekind domain** is a Noetherian 1-dimensional normal domain.

Examples

1. If K is a finite extension of $\mathbb{Q}$, then the **ring of integers** $\mathcal{O}_K$, the integral closure of $\mathbb{Z}$, is a Dedekind domain.
2. If X is a smooth affine curve over a field k, then the **ring of global sections** $\Gamma(X, \mathcal{O}_X)$ is a Dedekind domain.

Dedekind Domain

Dedekind Domain

A **Dedekind domain** is a Noetherian 1-dimensional normal domain.

Examples

1. If K is a finite extension of $\mathbb{Q}$, then the **ring of integers** $\mathcal{O}_K$, the integral closure of $\mathbb{Z}$, is a Dedekind domain.
2. If X is a smooth affine curve over a field k, then the **ring of global sections** $\Gamma(X, \mathcal{O}_X)$ is a Dedekind domain.

Existence and Uniqueness of Prime Factorization

In a Dedekind domain D, every nonzero ideal I can be uniquely represented as a product of prime ideals:

$$I = P_1^{e_1} \cdots P_r^{e_r},$$

where $P_1, \ldots, P_r$ are distinct nonzero prime ideals of D.

Especially, if K is a finite extension of $\mathbb{Q}$ and p is a prime

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}.$$

In this case, e_i is the **ramification index** of P_i. Note that $\mathcal{O}_K/P_i$ is a finite extension of $\mathbb{F}_p$. $f_i = [\mathcal{O}_K/P_i : \mathbb{F}_p]$ is the **inertia degree** of P_i.

Especially, if K is a finite extension of $\mathbb{Q}$ and p is a prime

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}.$$

In this case, e_i is the **ramification index** of P_i. Note that $\mathcal{O}_K/P_i$ is a finite extension of $\mathbb{F}_p$. $f_i = [\mathcal{O}_K/P_i : \mathbb{F}_p]$ is the **inertia degree** of P_i.

Why should we care?

Let $K = \mathbb{Q}[x]/f(x)$ for a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}.$$

Factorization

Apart from a finite number of primes p,

$$f(x) = p_1(x)^{e_1} \cdots p_r(x)^{e_r}$$

in $\mathbb{F}_p$, where p_i is a monic irreducible polynomial in $\mathbb{F}_p[x]$ of degree f_i.

Good News!

Almost Everywhere Unramifiedness

Apart from a finite number of primes p, $e_i = 1$.

Galois Action

If K is a Galois extension, then e_i and f_i are constant.

Fundamental Equality

$$\sum_{i=1}^{r} e_i f_i = [K : \mathbb{Q}].$$

In particular, if K is Galois, apart from a finite number of primes p,

$$f\,r = [K : \mathbb{Q}]$$

Frobenius Endomorphism

All in all, to know the prime factorization, if K is Galois, apart from a finite number of primes p, it is enough to know f. Let

$$p\mathcal{O}_K = P_1^{e} \cdots P_r^{e}.$$

Frobenius Endomorphism

All in all, to know the prime factorization, if K is Galois, apart from a finite number of primes p, it is enough to know f. Let

$$p\mathcal{O}_K = P_1^e \cdots P_r^e.$$

Frobenius element

Apart from a finite number of primes p, , there exists a natural element $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$, the **Frobenius element**, defined up to conjugacy, s.t.

1. Maps P_i to P_i for some i.
2. Induces the Frobenius endomorphism on $\mathcal{O}_K/P_i$.
3. The order of Fr_p is f.

Interim Summary

To solve the equation, it is enough to find **Frobenius**.

Return to the Example

One natural way to recognize the Frobenius is by using a representation.

Return to $x^3 - x^2 + 1$! Its Galois group is S_3. This

1. Has three conjugacy classes, and
2. Admits a unique faithful 2-dim representation

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \simeq S_3 \to \mathrm{GL}_2(\mathbb{C}).$$

Return to the Example

One natural way to recognize the Frobenius is by using a representation.

Return to $x^3 - x^2 + 1$! Its Galois group is S_3. This

1. Has three conjugacy classes, and
2. Admits a unique faithful 2-dim representation

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \simeq S_3 \to \mathrm{GL}_2(\mathbb{C}).$$

We can distinguish conjugacy classes by the trace of ρ.

Conjugacy Class	$\mathrm{tr}(\rho(c))$
id	2
(1 2)	0
(1 2 3)	-1

Reciprocity in terms of the Galois representation

Let

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \sum_{n=1}^{\infty} a_n q^n.$$

Then, apart from a finite number of primes p,

$$a_p = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

Reciprocity in terms of the Galois representation

Let

$$F(q) = q \prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \sum_{n=1}^{\infty} a_n q^n.$$

Then, apart from a finite number of primes p,

$$a_p = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

A refined form of Langlands Program - Version 1

For a Galois representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n$, there exists a special function $F(q) = \sum_n a_n q^n$ such that

$$a_p = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

apart from a finite number of primes p.

Examples of Galois representations

Let K be a Galois extension of $\mathbb{Q}$. Then there exists a natural projection

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}).$$

Since $\mathrm{Gal}(K/\mathbb{Q})$ is a finite group, its representation theory over $\mathbb{C}$ is well known. We can produce a lot of representations

$$\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C}).$$

Examples of Galois representations

Let K be a Galois extension of $\mathbb{Q}$. Then there exists a natural projection

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}).$$

Since $\mathrm{Gal}(K/\mathbb{Q})$ is a finite group, its representation theory over $\mathbb{C}$ is well known. We can produce a lot of representations

$$\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C}).$$

By composing them, we have representations

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

with a finite image. They are called **Artin representations.**

Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\bar{\mathbb{Q}})$

1. Is an abelian group, and
2. $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\bar{\mathbb{Q}})$.

Hence, its l^n-torsion $E(\bar{\mathbb{Q}})[l^n]$ is also a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module.

Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\bar{\mathbb{Q}})$

1. Is an abelian group, and
2. $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\bar{\mathbb{Q}})$.

Hence, its l^n-torsion $E(\bar{\mathbb{Q}})[l^n]$ is also a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module.

Fact: $E(\bar{\mathbb{Q}})[l^n]$ is isomorphic to $(\mathbb{Z}/l^n\mathbb{Z})^2$ as an abelian group.

Hence, the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ defines a representation

Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\bar{\mathbb{Q}})$

1. Is an abelian group, and
2. $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\bar{\mathbb{Q}})$.

Hence, its l^n-torsion $E(\bar{\mathbb{Q}})[l^n]$ is also a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module.

Fact: $E(\bar{\mathbb{Q}})[l^n]$ is isomorphic to $(\mathbb{Z}/l^n\mathbb{Z})^2$ as an abelian group.

Hence, the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ defines a representation

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z}),$$

By taking limit $n \to \infty$, we obtain

$$\rho_{E,l} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l).$$

This is the **l-adic Tate module** of E.

Lefschetz Fixed Point Theorem

Let n_p be the number of points of E in $\mathbb{F}_p$, and $b_p := p - n_p$. Then

$$\mathrm{tr}(\rho_{E,l}(\mathrm{Fr}_p)) = b_p$$

apart from a finite number of primes p.

Lefschetz Fixed Point Theorem

Let n_p be the number of points of E in $\mathbb{F}_p$, and $b_p := p - n_p$. Then

$$\mathrm{tr}(\rho_{E,l}(\mathrm{Fr}_p)) = b_p$$

apart from a finite number of primes p.

Modularity Theorem, refined version

For any elliptic curve E over $\mathbb{Q}$, , there exists a special function ,

$$F_E(q) = \sum_n a_n q^n$$

such that

$$a_p = \mathrm{tr}(\rho_{E,l}(\mathrm{Fr}_p)).$$

apart from a finite number of primes p, for any choice of prime l.

Upper Half Plane with the $SL_2(\mathbb{Z})$ action

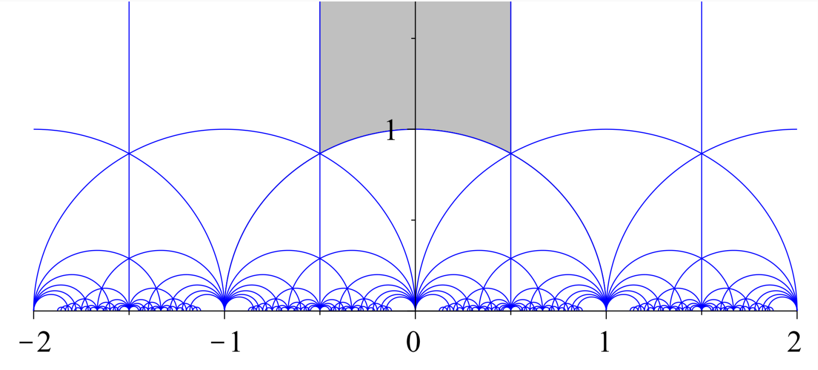

Figure 1: Fundamental domains of the $SL_2(\mathbb{Z})$ action on $\mathbb{H}$, PC: Wikipedia

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az+b}{cz+d}.$$

Modular Group

The **Modular Group**, $\mathrm{SL}_2(\mathbb{Z})$, has some special subgroups, such as

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N \right\}.$$

Modular Group

The **Modular Group**, $\mathrm{SL}_2(\mathbb{Z})$, has some special subgroups, such as

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \right\}.$$

A **congruence subgroup** is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(N)$ for some N. For instance,

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\},$$

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod N \right\}.$$

For any

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathsf{GL}_2^+(\mathbb{R}),$$

a natural number k and a function $F : \mathbb{H} \to \mathbb{C}$, we define $F|_k\gamma$ by

$$\begin{aligned} F|_k\gamma(z) &:= (\det \gamma)^{\frac{k}{2}}(cz+d)^{-k}F(\gamma z) \\ &= (\det \gamma)^{\frac{k}{2}}(cz+d)^{-k}F\left(\frac{az+b}{cz+d}\right). \end{aligned}$$

This is the **slash operator**.

For any

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathsf{GL}_2^+(\mathbb{R}),$$

a natural number k and a function $F : \mathbb{H} \to \mathbb{C}$, we define $F|_k\gamma$ by

$$\begin{aligned} F|_k\gamma(z) &:= (\det\gamma)^{\frac{k}{2}}(cz+d)^{-k}F(\gamma z) \\ &= (\det\gamma)^{\frac{k}{2}}(cz+d)^{-k}F\left(\frac{az+b}{cz+d}\right). \end{aligned}$$

This is the **slash operator**.

Note that this is defined in a way that the following holds:

$$F|_k\gamma(z)(dz)^{\otimes\frac{k}{2}} = F(\gamma z)(d(\gamma z))^{\otimes\frac{k}{2}}.$$

Modular Forms

Modular form

A **weak modular form** of weight k and level N is a holomorphic function $F : \mathbb{H} \to \mathbb{C}$ s.t. $F|_k \gamma = F$ for any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N)$, i.e.

$$F(\gamma z) = (cz + d)^k F(z).$$

Modular Forms

Modular form

A **weak modular form** of weight k and level N is a holomorphic function $F : \mathbb{H} \to \mathbb{C}$ s.t. $F|_k \gamma = F$ for any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N)$, i.e.

$$F(\gamma z) = (cz + d)^k F(z).$$

Note that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \Gamma_1(N)$, so $F(z) = F(z+1)$. Hence

$$F(z) = F_0(q) \text{ where } q = e^{2\pi i z}$$

for a holomorphic function F_0 on a punctured disc.

The same holds for $F|_k \gamma(z)$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so $F|_k \gamma(z) = F_0^{\gamma}(q)$.

Modular Forms

Modular form

A **weak modular form** of weight k and level N is a holomorphic function $F : \mathbb{H} \to \mathbb{C}$ s.t. $F|_k\gamma = F$ for any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N)$, i.e.

$$F(\gamma z) = (cz + d)^k F(z).$$

Note that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \Gamma_1(N)$, so $F(z) = F(z+1)$. Hence

$$F(z) = F_0(q) \text{ where } q = e^{2\pi i z}$$

for a holomorphic function F_0 on a punctured disc.

The same holds for $F|_k\gamma(z)$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so $F|_k\gamma(z) = F_0^\gamma(q)$.

F is a **modular form** if F_0^γ holomorphic, and a **cusp form** if $F_0^\gamma(0) = 0$.

Examples of Modular Forms

Eisenstein Series: weight $2k$, level 1, non-cusp form.

$$E_{2k}(z) = \frac{1}{2\zeta(2k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^{2k}} = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.$$

Examples of Modular Forms

Eisenstein Series: weight $2k$, level 1, non-cusp form.

$$E_{2k}(z) = \frac{1}{2\zeta(2k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^{2k}} = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.$$

Modular Discriminant: weight 12, level 1, cusp form.

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Examples of Modular Forms

Eisenstein Series: weight $2k$, level 1, non-cusp form.

$$E_{2k}(z) = \frac{1}{2\zeta(2k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^{2k}} = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.$$

Modular Discriminant: weight 12, level 1, cusp form.

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Our Examples: weight 1/level 23, weight 2/level 11. Cusp forms.

$$F(q) = q \prod_{n=1}^{\infty} (1-q^n)(1-q^{23n}), F_E(q) = q \prod_{n=1}^{\infty} (1-q^n)^2(1-q^{11n})^2$$

A refined form of Langlands Program - Version 2

For an irreducible Galois representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2$, there exists a cusp form $F(q) = \sum_n a_n q^n$ such that

$$a_p = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

apart from a finite number of primes p.

Caution: This is **trivially false** for various reasons.

In the rest of presentation, we will improve the preceeding formulation:

1. Make this statement works in both direction.
2. Generalize this from GL_2 to arbitrary reductive group.

Modular Curves

Consider

$$Y(N) := \Gamma(N)\backslash\mathbb{H}, \;\; Y_0(N) := \Gamma_0(N)\backslash\mathbb{H}, \;\; Y_1(N) := \Gamma_1(N)\backslash\mathbb{H}.$$

Note that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is the moduli space of curves elliptic curves. In the same vein, these are moduli space of elliptic curves with a level structure.

Modular Curves

Consider

$$Y(N) := \Gamma(N)\backslash\mathbb{H},\ \ Y_0(N) := \Gamma_0(N)\backslash\mathbb{H},\ \ Y_1(N) := \Gamma_1(N)\backslash\mathbb{H}.$$

Note that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is the moduli space of curves elliptic curves. In the same vein, these are moduli space of elliptic curves with a level structure.

$$\begin{aligned} Y_1(N) = \text{ moduli space of pairs } &(E, P) \\ E &: \text{an elliptic curve} \\ P &: \text{a point of order } N. \end{aligned}$$

Modular Curves

Consider

$$Y(N) := \Gamma(N)\backslash\mathbb{H},\ \ Y_0(N) := \Gamma_0(N)\backslash\mathbb{H},\ \ Y_1(N) := \Gamma_1(N)\backslash\mathbb{H}.$$

Note that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is the moduli space of curves elliptic curves. In the same vein, these are moduli space of elliptic curves with a level structure.

$$\begin{aligned} Y_1(N) &= \text{moduli space of pairs } (E, P) \\ &\quad E : \text{an elliptic curve} \\ &\quad P : \text{a point of order } N. \end{aligned}$$

Exercise: Find a simillar description for $Y(N), Y_0(N)$.

They have natural compactification

$$Y(N) \subseteq X(N), Y_0(N) \subseteq X_0(N) \text{ and } Y_1(N) \subseteq X_1(N).$$

Geometric Description of Modular Forms

Let $S_k(N)$ (resp. $M_k(N)$) be the $\mathbb{C}$-vector space of cusp (resp. modular) forms. Recall that the slash operator is defined such that

$$F|_k\gamma(z)(dz)^{\otimes\frac{k}{2}} = F(\gamma z)(d(\gamma z))^{\otimes\frac{k}{2}}$$

and we require

$$F|_k = F, \text{ i.e. } F(z)(dz)^{\otimes\frac{k}{2}} = F(\gamma z)(d(\gamma z))^{\otimes\frac{k}{2}}$$

for a modular form F.

Geometric Description of Modular Forms

Let $S_k(N)$ (resp. $M_k(N)$) be the $\mathbb{C}$-vector space of cusp (resp. modular) forms. Recall that the slash operator is defined such that

$$F|_k\gamma(z)(dz)^{\otimes\frac{k}{2}} = F(\gamma z)(d(\gamma z))^{\otimes\frac{k}{2}}$$

and we require

$$F|_k = F, \text{ i.e. } F(z)(dz)^{\otimes\frac{k}{2}} = F(\gamma z)(d(\gamma z))^{\otimes\frac{k}{2}}$$

for a modular form F.

Geometric Description of $S_2(N)$

$$S_2(N) \simeq \Gamma\left(X_1(N), \Omega^1_{X_1(N)}\right).$$

Exactly the same statement holds for $\Gamma_0(N)$ and $X_0(N)$.

We can obtain simillar description for a general weight k. Let

$$\pi : \mathcal{E} \to X_1(N)$$

be the universal family of elliptic curves, and

$$\lambda := \pi_* \Omega^1_{\mathcal{E}/X_1(N)}$$

be the **Hodge line bundle**.

We can obtain simillar description for a general weight k. Let

$$\pi : \mathcal{E} \to X_1(N)$$

be the universal family of elliptic curves, and

$$\lambda := \pi_* \Omega^1_{\mathcal{E}/X_1(N)}$$

be the **Hodge line bundle**.

Geometric Description of $M_k(N)$

$$M_k(N) \simeq \Gamma\left(X_1(N), \lambda^{\otimes k}\right).$$

This explains the last condition in the defintion:

$$F|_k\gamma(z) = F|_k\gamma(z+1) \text{ for } \gamma \in \mathrm{SL}_2(\mathbb{Z}), \text{ so } F|_k\gamma(z) = F_0^\gamma(q).$$

F is a **modular form** if F_0^γ holomorphic, and a **cusp form** if $F_0^\gamma(0) = 0$.

The points in $D_N := X_1(N) \setminus Y_1(N)$ are called **cusps**.

The last condition corresponds to the regularity of the section at cusps.

This explains the last condition in the defintion:

$$F|_k\gamma(z) = F|_k\gamma(z+1) \text{ for } \gamma \in \mathrm{SL}_2(\mathbb{Z}), \text{ so } F|_k\gamma(z) = F_0^\gamma(q).$$

F is a **modular form** if F_0^γ holomorphic, and a **cusp form** if $F_0^\gamma(0) = 0$.

The points in $D_N := X_1(N) \setminus Y_1(N)$ are called **cusps**.

The last condition corresponds to the regularity of the section at cusps.

Geometric Description of $S_k(N)$

$$S_k(N) \simeq \Gamma\left(X_1(N), \lambda^{\otimes k}(D_N)\right).$$

Hecke Operator

Let n be an integer prime to N. Let

$$\begin{tikzcd} & X_1(nN) \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ X_1(N) & & X_1(N) \end{tikzcd}$$

where

$$\alpha(E, P) = (E, nP),\ \beta(E, P) = (E/NP, P).$$

This is the **Hecke correspondence** T_n of $X_1(N)$.

Hecke Operator

Let n be an integer prime to N. Let

$$\begin{tikzcd} & X_1(nN) \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ X_1(N) & & X_1(N) \end{tikzcd}$$

where

$$\alpha(E, P) = (E, nP),\ \beta(E, P) = (E/NP, P).$$

This is the **Hecke correspondence** T_n of $X_1(N)$.

The definition of T_n is a bit more complicated for a general n.

The **Hecke operator** T_n on $S_k(N)$ is

$$T_n = \alpha_* \beta^* : S_k(N) \to S_k(N).$$

Hecke Algebra for $N = 1$

On $S_k(1)$, $\{T_n\}_{n\in\mathbb{N}}$ is

1. Simultaneously diagonalizable.
2. If F is a common eigenfunction of $\{T_n\}_{n\in\mathbb{N}}$ such that

$$F(q) = q + \sum_{n=2}^{\infty} a_n q^n,$$

   then $T_pF = a_pF$.
3. If F and G are nonzero common eigenfunctions of T_n with the same eigenvalues, then they coincide up to a constant.

Hecke Algebra for $N = 1$

On $S_k(1)$, $\{T_n\}_{n\in\mathbb{N}}$ is

1. Simultaneously diagonalizable.
2. If F is a common eigenfunction of $\{T_n\}_{n\in\mathbb{N}}$ such that
$$F(q) = q + \sum_{n=2}^{\infty} a_n q^n,$$
then $T_p F = a_p F$.
3. If F and G are nonzero common eigenfunctions of T_n with the same eigenvalues, then they coincide up to a constant.

Essentially nothing holds for general N.

Fixing the Problem

The origin of the problem:

$$\text{if } f(z) \in S_k(N), \text{ then } f(dz) \in S_k(dN), \text{ which has the same info}$$

Oldforms

An element $f \in S_k(N)$ given by

$$f(z) = g(dz)$$

For some $d \mid N$ and $g \in S_k(N/d)$, is called an **oldform**.

Let $S_k(N)^{\text{old}}$ be the subspace spaned by oldforms.

Fixing the Problem

The origin of the problem:

$$\text{if } f(z) \in S_k(N), \text{ then } f(dz) \in S_k(dN), \text{ which has the same info}$$

Oldforms

An element $f \in S_k(N)$ given by

$$f(z) = g(dz)$$

For some $d \mid N$ and $g \in S_k(N/d)$, is called an **oldform**.

Let $S_k(N)^{\text{old}}$ be the subspace spaned by oldforms.

There is a natural inner product on $S_k(N)$, given by

$$\langle f, g \rangle = \int_{\Gamma_1(N)\backslash\mathbb{H}} f(z)\overline{g(z)}y^{k-2}dxdy.$$

The **newform** is defined as an element of $S_k(N)^{\mathrm{new}} = (S_k(N)^{\mathrm{old}})^{\perp}$.

Hecke Algebra for $S_k(N)^{\mathrm{new}}$

On $S_k(N)^{\mathrm{new}}$, $\{T_n\}_{n\in\mathbb{N}}$ is

1. Simultaneously diagonalizable.
2. If F is a common eigenfunction of $\{T_n\}_{n\in\mathbb{N}}$ such that

$$F(q) = q + \sum_{n=2}^{\infty} a_n q^n,$$

   then $T_p F = a_p F$.
3. If F and G are nonzero common eigenfunctions of T_n with the same eigenvalues, then they coincide up to a constant.

The **Hecke eigenform** is an element of $S_k(N)^{\mathrm{new}}$ that satisfies (2) above.

A refined form of Langlands Program - Version 3

There exists a one-to-one correspondence between

1. irreducible Galois representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2$
2. Hecke eigenform F

such that, apart from a finite number of primes p,

$$a_p(F) = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

Caution: Still, this is **trivially false** for various reasons.

- We did not specify the base field of ρ,
- We need more than cusp forms for it to be true,

among many others. Nevertheless, this serves as a good starting point!

Good news: Now we know enough to formulate some theorems!

Deligne-Serre ($k = 1$), Eichler-Shimura ($k = 2$), Deligne ($k > 2$)

For any Hecke eigenform $F \in S_k(N)^{\text{new}}$ and a prime l, there exists an irreducible Galois representation

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}_l})$$

such that

$$a_p(F) = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

apart from a finite number of primes p,

Hence, at least one direction of the conjecture is true!

A special case of the Artin's conjecture, Khare-Wintenberger 09

If $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ is an irreducible representation such that $\det \rho(c) = -1$, where c is the complex conjugation, then there exists a weight 1 Hecke eigenform F such that

$$a_p(F) = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

apart from a finite number of primes p.

A special case of the Artin's conjecture, Khare-Wintenberger 09

If $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ is an irreducible representation such that $\det \rho(c) = -1$, where c is the complex conjugation, then there exists a weight 1 Hecke eigenform F such that

$$a_p(F) = \mathrm{tr}(\rho(\mathrm{Fr}_p)).$$

apart from a finite number of primes p.

Modularity Theorem, a rigorous statement

If E is an elliptic curve over $\mathbb{Q}$, there exists a weight 2 Hecke eigenform F of $\Gamma_0(N)$ such that

$$a_p(F) = \mathrm{tr}(\rho_{E,l}(\mathrm{Fr}_p)).$$

apart from a finite number of primes p and any prime l.

Adelization and Automorphic Representations

Adelization

Goal: Provide a ‘natural’ description of the congruence subgroups.

Adelization

Goal: Provide a 'natural' description of the congruence subgroups.

We use p-adic numbers to do this. Recall that

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} \text{ and } \mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right].$$

They have natural topology, which makes them a topological ring, and a local basis at 0 is given by

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset \cdots \supset p^{n-1}\mathbb{Z}_p \supset p^n\mathbb{Z}_p \supset p^{n+1}\mathbb{Z}_p \supset \cdots$$

Adelization

Goal: Provide a 'natural' description of the congruence subgroups.

We use p-adic numbers to do this. Recall that

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} \text{ and } \mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right].$$

They have natural topology, which makes them a topological ring, and a local basis at 0 is given by

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset \cdots \supset p^{n-1}\mathbb{Z}_p \supset p^n\mathbb{Z}_p \supset p^{n+1}\mathbb{Z}_p \supset \cdots$$

We also topologize algebraic groups over $\mathbb{Q}_p$, e.g. $\mathrm{GL}_n(\mathbb{Q}_p)$ has a basis

$$\mathrm{GL}_n(\mathbb{Z}_p) \supset 1_n + p\mathrm{M}_n(\mathbb{Z}_p) \supset \cdots \supset 1_n + p^{n-1}\mathrm{M}_n(\mathbb{Z}_p) \supset 1_n + p^n\mathrm{M}_n(\mathbb{Z}_p) \cdots$$

The **Adele** (over $\mathbb{Q}$) is defined by

$$\mathbb{A}_{\mathbb{Q}} := \mathbb{R} \times \prod_p{}' \mathbb{Q}_p = \{(a_\infty, a_2, a_3, \cdots) \mid a_p \in \mathbb{Z}_p \text{ for almost every } p\}.$$

The **Adele** (over $\mathbb{Q}$) is defined by

$$\mathbb{A}_{\mathbb{Q}} := \mathbb{R} \times \prod_{p}{}' \mathbb{Q}_p = \{(a_\infty, a_2, a_3, \cdots) \mid a_p \in \mathbb{Z}_p \text{ for almost every } p\}.$$

It is a locally compact topological ring whose basis at 0 is given by

$$U \times \prod_{i=1}^{r} p_i^{e_i} \mathbb{Z}_{p_i} \times \prod_{p \nmid N} \mathbb{Z}_p$$

where $N = p_1^{e_1} \cdots p_r^{e_r}$ and U is any open subset containing 0.

The **Adele** (over $\mathbb{Q}$) is defined by

$$\mathbb{A}_{\mathbb{Q}} := \mathbb{R} \times \prod_p{}' \mathbb{Q}_p = \{(a_\infty, a_2, a_3, \cdots) \mid a_p \in \mathbb{Z}_p \text{ for almost every } p\}.$$

It is a locally compact topological ring whose basis at 0 is given by

$$U \times \prod_{i=1}^{r} p_i^{e_i} \mathbb{Z}_{p_i} \times \prod_{p \nmid N} \mathbb{Z}_p$$

where $N = p_1^{e_1} \cdots p_r^{e_r}$ and U is any open subset containing 0.

The 'diagonal embedding' $\mathbb{Q} \to \mathbb{A}_{\mathbb{Q}}$ is discrete and cocompact.

Exercise: $\mathbb{Q} \backslash \mathbb{A}_{\mathbb{Q}} \simeq \mathbb{R}/\mathbb{Z} \times \prod_p \mathbb{Z}_p$, $\mathbb{Q} \backslash \mathbb{A}_{\mathbb{Q}} / \prod_p \mathbb{Z}_p \simeq \mathbb{R}/\mathbb{Z}$.

Although it looks scary, its appropriate quotient is just a manifold!

Have $\mathrm{GL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R}) \simeq \mathbb{H}$ in mind! Let

$$\mathrm{GL}_2(\mathbb{Q}_p) \supset \mathrm{GL}_2(\mathbb{Z}_p), \mathrm{GL}_2(\mathbb{R}) \supset \mathrm{O}_2(\mathbb{R})$$

be the maximal compact subgroups.

Have $\mathrm{GL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R}) \simeq \mathbb{H}$ in mind! Let

$$\mathrm{GL}_2(\mathbb{Q}_p) \supset \mathrm{GL}_2(\mathbb{Z}_p), \mathrm{GL}_2(\mathbb{R}) \supset \mathrm{O}_2(\mathbb{R})$$

be the maximal compact subgroups. Then

$$Z(\mathbb{A}_{\mathbb{Q}})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})/\mathrm{O}_2(\mathbb{R}) \times \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \simeq \mathrm{SL}_2(\mathbb{Z})\backslash \mathbb{H}.$$

Where Z is the center of GL_2, i.e. the diagonal matrices.

Have $\mathrm{GL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R}) \simeq \mathbb{H}$ in mind! Let

$$\mathrm{GL}_2(\mathbb{Q}_p) \supset \mathrm{GL}_2(\mathbb{Z}_p), \mathrm{GL}_2(\mathbb{R}) \supset \mathrm{O}_2(\mathbb{R})$$

be the maximal compact subgroups. Then

$$Z(\mathbb{A}_\mathbb{Q})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})/\mathrm{O}_2(\mathbb{R}) \times \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \simeq \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}.$$

Where Z is the center of GL_2, i.e. the diagonal matrices.

Similarly, for $N = p_1^{e_1} \cdots p_r^{e_r}$, let $K(N) = K_\infty \times \prod_p K_p(N)$ where

$$K_\infty = \mathrm{O}_2(\mathbb{R}),\ K_{p_i}(N) = 1_n + p_i^{e_i}\mathrm{M}_n(\mathbb{Z}_{p_i}),\ K_p(N) = \mathrm{GL}_2(\mathbb{Z}_p) \text{ for } p \neq p_i.$$

Then

$$Z(\mathbb{A}_\mathbb{Q})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})/K(N) \simeq \mathrm{GL}_2(\mathbb{Q}) \cap \prod_p K_p\backslash\mathbb{H} \simeq \Gamma(N)\backslash\mathbb{H}.$$

Have $\mathrm{GL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R}) \simeq \mathbb{H}$ in mind! Let

$$\mathrm{GL}_2(\mathbb{Q}_p) \supset \mathrm{GL}_2(\mathbb{Z}_p), \mathrm{GL}_2(\mathbb{R}) \supset \mathrm{O}_2(\mathbb{R})$$

be the maximal compact subgroups. Then

$$Z(\mathbb{A}_\mathbb{Q})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})/\mathrm{O}_2(\mathbb{R}) \times \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \simeq \mathrm{SL}_2(\mathbb{Z})\backslash \mathbb{H}.$$

Where Z is the center of GL_2, i.e. the diagonal matrices.

Similarly, for $N = p_1^{e_1} \cdots p_r^{e_r}$, let $K(N) = K_\infty \times \prod_p K_p(N)$ where

$$K_\infty = \mathrm{O}_2(\mathbb{R}),\ K_{p_i}(N) = 1_n + p_i^{e_i}\mathrm{M}_n(\mathbb{Z}_{p_i}),\ K_p(N) = \mathrm{GL}_2(\mathbb{Z}_p) \text{ for } p \neq p_i.$$

Then

$$Z(\mathbb{A}_\mathbb{Q})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})/K(N) \simeq \mathrm{GL}_2(\mathbb{Q}) \cap \prod_p K_p \backslash \mathbb{H} \simeq \Gamma(N)\backslash \mathbb{H}.$$

Upshot: Modular forms lives in $Z(\mathbb{A}_\mathbb{Q})\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})/K(N)$.

This extends to reductive groups: Let

$$G : \text{ a reductive group}$$
$$K_\infty : \text{ a maximal compact subgroup of } G(\mathbb{R})$$
$$K_{\text{fin}} : \text{ a compact open subgroup of } \prod_p G(\mathbb{Q}_p).$$

This extends to reductive groups: Let

$$\begin{aligned} G &: \text{ a reductive group} \\ K_\infty &: \text{ a maximal compact subgroup of } G(\mathbb{R}) \\ K_{\text{fin}} &: \text{ a compact open subgroup of } \prod_p G(\mathbb{Q}_p). \end{aligned}$$

Punchline: For $K = K_\infty K_{\text{fin}} \subseteq G(\mathbb{A}_\mathbb{Q})$,

$Z(\mathbb{R})\backslash G(\mathbb{R})/K$ is a locally symmetric space,

$Z(\mathbb{A}_\mathbb{Q})G(\mathbb{Q})\backslash G(\mathbb{A}_\mathbb{Q})/K$ is a quotient of $Z(\mathbb{R})\backslash G(\mathbb{R})/K$ by $G(\mathbb{Q}) \cap K_{\text{fin}}$.

This extends to reductive groups: Let

$$
\begin{aligned}
G &: \text{ a reductive group} \\
K_\infty &: \text{ a maximal compact subgroup of } G(\mathbb{R}) \\
K_{\text{fin}} &: \text{ a compact open subgroup of } \prod_p G(\mathbb{Q}_p).
\end{aligned}
$$

Punchline: For $K = K_\infty K_{\text{fin}} \subseteq G(\mathbb{A}_\mathbb{Q})$,

$Z(\mathbb{R})\backslash G(\mathbb{R})/K$ is a locally symmetric space,

$Z(\mathbb{A}_\mathbb{Q})G(\mathbb{Q})\backslash G(\mathbb{A}_\mathbb{Q})/K$ is a quotient of $Z(\mathbb{R})\backslash G(\mathbb{R})/K$ by $G(\mathbb{Q}) \cap K_{\text{fin}}$.

Let $M = Z(\mathbb{R})\backslash G(\mathbb{R})/K$ and $\Gamma_K = G(\mathbb{Q}) \cap K_{\text{fin}}$.

$\Gamma_K\backslash M$ is a generalization of the modular curve, 'parameterized' by K.

$$Z(\mathbb{A}_\mathbb{Q})G(\mathbb{Q})\backslash G(\mathbb{A}_\mathbb{Q}) \text{ “} = \text{”} \varprojlim_K \Gamma_K\backslash M.$$

Automorphic Representations

Let $\chi : Z(\mathbb{A}_\mathbb{Q}) \to \mathrm{U}(1)$ be a character and $F : G(\mathbb{Q})\backslash G(\mathbb{A}_\mathbb{Q}) \to \mathbb{C}$.

Let $L_0^2(G,\chi)$ be the set of functions satisfying

1. [Central Character] $F(gz) = \chi(z)F(g)$ for $z \in Z(\mathbb{A}_\mathbb{Q})$
2. [L^2 condition]
$$\int_{Z(\mathbb{A}_\mathbb{Q})G(\mathbb{Q})\backslash G(\mathbb{A}_\mathbb{Q})} |F(g)|^2 dg < \infty$$
3. [Cuspidality]
$$\int_{U(\mathbb{Q})\backslash U(\mathbb{A}_\mathbb{Q})} F(ug)dg = 0$$
for any unipotent radical U of a parabolic subgroup P.

The **cuspidal automorphic representation** of $G(\mathbb{A}_\mathbb{Q})$ is an irreducible subrepresentation of $L_0^2(G,\chi)$.

Recall that

$$Z(\mathbb{A}_\mathbb{Q})G(\mathbb{Q})\backslash G(\mathbb{A}_\mathbb{Q}) \text{ ``}=\text{'' } \varprojlim_K \Gamma_K\backslash M.$$

Hence, $L_0^2(G,\chi)$ reduced to the spectral theory of $\Gamma_K\backslash M$. In this vein,

Cuspidal automorphic representations $\approx$ Laplacian eigenspace of $\Gamma_K\backslash M$.

Recall that

$$Z(\mathbb{A}_{\mathbb{Q}})G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}}) \text{ “}=\text{” } \varprojlim_{K} \Gamma_K\backslash M.$$

Hence, $L_0^2(G,\chi)$ reduced to the spectral theory of $\Gamma_K\backslash M$. In this vein,

Cuspidal automorphic representations $\approx$ Laplacian eigenspace of $\Gamma_K\backslash M$.

Example: Let $G = \mathrm{GL}_2$ and $F \in S_k(N)$. Then

$$g \mapsto F|_k g(i) = (\det g)^{\frac{k}{2}}(ci+d)^k f\left(\frac{ai+b}{ci+d}\right),$$

originally defined on $\mathrm{GL}_2^+(\mathbb{R})$, descends to $Y_1(N)$.

Recall that

$$Z(\mathbb{A}_{\mathbb{Q}})G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}}) \text{ ``} = \text{''} \varprojlim_{K} \Gamma_K\backslash M.$$

Hence, $L_0^2(G, \chi)$ reduced to the spectral theory of $\Gamma_K\backslash M$. In this vein,

Cuspidal automorphic representations $\approx$ Laplacian eigenspace of $\Gamma_K\backslash M$.

Example: Let $G = \mathrm{GL}_2$ and $F \in S_k(N)$. Then

$$g \mapsto F|_k g(i) = (\det g)^{\frac{k}{2}}(ci + d)^k f\left(\frac{ai + b}{ci + d}\right),$$

originally defined on $\mathrm{GL}_2^+(\mathbb{R})$, descends to $Y_1(N)$.

This is a Laplacian eigenfunction with eigenvalue $\frac{k(1-k)}{4}$.

Hence, a modular form gives rise to an automorphic representation.

Hecke Operators

For any reductive group G, there exists a theory of Hecke operators for $L^2_0(G, \chi)$, but describing it here is a bit intricate.

Hecke Operators

For any reductive group G, there exists a theory of Hecke operators for $L^2_0(G, \chi)$, but describing it here is a bit intricate.

If $G = \mathrm{GL}_n$, the situation is much simpler:

For each prime p, there exists n operators

$$T_{p,1}, \cdots, T_{p,n}$$

and we can define the 'eigenvalues' of these operators for a cuspidal automorphic representation π. These eigenvalues are denoted by $a_{p,i}(\pi)$.

Our Final Version of the Langlands Program, for GL_n

There exists a one-to-one correspondence between

1. Irreducible Galois representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$.
2. Cuspidal automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$.

such that

$$\det(X 1_n - \rho(\mathrm{Fr}_p)) = X^n + \sum_{i=1}^{n} (-1)^i a_{p,i}(\pi) X^{n-i}.$$

Unfortunately, the Langlands program for a reductive group is **not** a correspondence between $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G(\overline{\mathbb{Q}}_l)$ and cuspidal automorphic representations of G.

Unfortunately, the Langlands program for a reductive group is **not** a correspondence between $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G(\overline{\mathbb{Q}}_l)$ and cuspidal automorphic representations of G.

Langlands Dual

Let G be a reductive group with the root datum $(X^*, \Delta, X_*, \Delta^\vee)$. The **Langlands dual** G^{L} of G is the reductive group corresponding to $(X_*, \Delta^\vee, X^*, \Delta)$.

If G is semisimple, then this coincides with the Dynkin dual.

G	GL_n	SL_n	SO_{2n}	SO_{2n+1}	$\mathrm{Spin}(2n)$
G^{L}	GL_n	PGL_n	SO_{2n}	Sp_{2n}	$\mathrm{SO}_{2n}/\{\pm 1_{2n}\}$

Our Final Version of the Langlands Program, for G

Let G be a reductive algebraic group. There exists a one-to-one correspondence between

1. Galois representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G^{\mathsf{L}}(\overline{\mathbb{Q}}_l)$.
2. Automorphic representation π of G.

Of course, we need to specify the relationship between the Hecke eigenvalues and the image of the Frobenius element, but this is challenging for a general reductive group.

This description is very incomplete, since:

1. It does not explain the choice of prime l on the Galois side: this is related to the l-independence and the theory of motives.

This description is very incomplete, since:

1. It does not explain the choice of prime l on the Galois side: this is related to the l-independence and the theory of motives.
2. Not every Galois representation corresponds to an automorphic representation. This is related to geometric Galois representation and the Fontain-Mazur conjecture.

This description is very incomplete, since:

1. It does not explain the choice of prime l on the Galois side: this is related to the l-independence and the theory of motives.
2. Not every Galois representation corresponds to an automorphic representation. This is related to geometric Galois representation and the Fontain-Mazur conjecture.
3. Not every automorphic representation corresponds to a Galois representation. This is related to the notion of algebraic automorphic representations, the Weil group, and the Langlands group.

This description is very incomplete, since:

1. It does not explain the choice of prime l on the Galois side: this is related to the l-independence and the theory of motives.
2. Not every Galois representation corresponds to an automorphic representation. This is related to geometric Galois representation and the Fontain-Mazur conjecture.
3. Not every automorphic representation corresponds to a Galois representation. This is related to the notion of algebraic automorphic representations, the Weil group, and the Langlands group.
4. It does not mention local-global compatability, as we have not discussed the local Langlands program.

among many others.

This description is very incomplete, since:

1. It does not explain the choice of prime l on the Galois side: this is related to the l-independence and the theory of motives.
2. Not every Galois representation corresponds to an automorphic representation. This is related to geometric Galois representation and the Fontain-Mazur conjecture.
3. Not every automorphic representation corresponds to a Galois representation. This is related to the notion of algebraic automorphic representations, the Weil group, and the Langlands group.
4. It does not mention local-global compatability, as we have not discussed the local Langlands program.

among many others.

However, this is good enough for the Geometric Langlands Program!