Some aspects of Langlands program

Cheng-Chiang Tsai

AS-NTU Basic Notion Seminar, Oct. 12th, 2020

First example

- A classical question: For which integer n do there exist integers a, b such that $a^2 + b^2 = n$?
- Answer: When $n = p$ is a prime, such a, b exist iff $p = 2$ or $p = 4k + 1$.
- For $p = 4k + 3$, e.g. $p = 7$, $a^2 + b^2 = 7$ has no solution. Though if we square 7, then $a^2 + b^2 = 49$ obviously has solutions.
- In general, such a, b exist iff $n \geq 0$, and for every prime p that appears in the prime factorization an **odd** number of times, we have $p = 2$ or $p = 4k + 1$. Identical statement is true when we replace a, b, n by rational numbers.
- A common number-theoretic phenomenon: a question about integers or rational numbers (global) can be fully or partially studied by looking at the $\mathbb{R}$-version and information from each prime number (local).
- So why the difference between $4k + 1$ and $4k + 3$?

Second example

- A slightly modern question: for any fixed prime p, when does there exist an integer x such that p divides $x^3 - x - 1$?
- In other words, when does $x^3 - x - 1 = 0$ has a root in $\mathbb{F}_p = \mathbb{Z}/p$, the field of p elements?
- Even more, we can ask the number of roots in $\mathbb{F}_p$, i.e. the number of $x \in \{0, 1, ..., p-1\}$ such that $x^3 - x - 1$ is divisible by p.
- Answer: No root if p can be written as $p = 2a^2 + ab + 3b^2$. Three roots if $p = a^2 + ab + 6b^3$. Two roots if $p = 23$. One root otherwise.
- For any integral polynomial (not only $x^3 - x - 1$) this has a general type of answer as follows: Consider $q = e^{2\pi iz}$ our favorite periodic holomorphic function on $\mathbb{C}$ and

$$f := q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \frac{1}{2}\left(\sum_{a,b\in\mathbb{Z}} q^{a^2+ab+6b^2} - \sum_{a,b\in\mathbb{Z}} q^{2a^2+ab+3b^2}\right)$$

$$= q - 1q^2 - 1q^3 + 0q^5 + q^6 + 0q^7 + q^8 + 0q^{11} - 1q^{13} - q^{16} + 1q^{23} + \ldots\ldots + 2q^{59} + \ldots$$

  which converges on the upper half plane $\mathfrak{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$.
- At the same time, $x^3 - x - 1 = 0$ has no root in $\mathbb{F}_p$ for $p = 2, 3, 13, ...$, one root for $p = 5, 7, 11, ...$, and three roots for $p = 59, ...$

Modular forms

$$f := q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \frac{1}{2}(\sum_{a,b\in\mathbb{Z}} q^{a^2+ab+6b^2} - \sum_{a,b\in\mathbb{Z}} q^{a^2+ab+6b^2})$$

- In fact, f is not only periodic, but a so-called **modular form**.
- Recall that $SL_2(\mathbb{R})$, the group of 2×2 matrices in $\mathbb{R}$ with determinant 1, is the automorphism group of our upper half plane $\mathfrak{H}$.
- Let us look at the subgroup of $SL_2(\mathbb{R})$ that consists of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in \mathbb{Z}$ and $d-1 \equiv c \equiv 0 \pmod{23}$. The function f satisfies (this is not obvious)

$$f(\frac{az+b}{cz+d}) = (cz+d)f(z)$$

- Another weird(?) example:

$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$

$$= q-2q^2-1q^3+2q^4+1q^5+2q^6-2q^7-2q^9-2q^{10}+1q^{11}-2q^{12}+4q^{13}+\ldots$$

is also a modular form except that the $\pmod{23}$ above is to be changed to $\pmod{11}$.

Third example

$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q-2q^2-1q^3+2q^4+1q^5+2q^6-2q^7-2q^9-2q^{10}+1q^{11}-2q^{12}+4q^{13}+4q^{14}-q^{15}-4q^{16}-2q^{17}+4q^{18}+0q^{19}+2q^{20}+2q^{21}-2q^{22}-1q^{23}-4q^{25}-8q^{26}+5q^{27}+\ldots$

- Let us look at the equation $y^2 - y = x^3 - x^2$ and ask for its solutions in $\mathbb{F}_p = \mathbb{Z}/p$.
- For any fixed value of x, we have a quadratic equation in y which might have $0, 1$ or 2 solutions. In average there seems to be p solutions. Let a_p be the "difference":

$$a'_p = \#\{x, y \in \mathbb{F}_p \mid y^2 - y = x^3 - x^2\}$$
$$a_p = p - a'_p.$$

- Some examples of these a_p:

p	2	3	5	7	11	13	17	19	23	29	31	37
a_p	-2	-1	1	-2	1	4	-2	0	-1	0	7	3

Aha!

Examples summarized

- Let us summarized the three examples:

1. On one side we ask whether $x^2 + y^2 = p$ is possible. On the other we have p modulo 4.
2. On one side we ask the number of roots of $x^3 - x - 1$ in $\mathbb{F}_p = \mathbb{Z}/p$. On the other we have the coefficients of the modular form $f(z) = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n})$, $q = e^{2\pi iz}$.
3. On one side we ask how many solutions are there to $y^2 - y = x^3 - x^2$ in $\mathbb{F}_p$. On the other we have modular form $f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$.

- How are they related?
- Langlands program starts with Langlands correspondence: a correspondence between certain **representations** and certain **Galois monodromies**. Can you see which side is which side?

Galois side I: Galois theory

- In the example $x^2 + y^2 = p$, the basic strategy of number theory since 19th century is that we will factor $x^2 + y^2 = (x + iy)(x - iy)$, $i = \sqrt{-1}$. In particular adding i into our number system whenever we like.
- That is, we have the field extension $\mathbb{Q}(i)/\mathbb{Q}$.
- Explicit algorithm for solving $x^2 + y^2 = p$ consists of two steps: (1) find $x' \in \mathbb{Z}$ such that $(x')^2 + 1 = kp$ where $0 < k < p$. (2) Take $x + iy = \gcd_{\mathbb{Z}[i]}(x' + i, p)$ then $x^2 + y^2 = p$.
- And finding x' is solving for $\sqrt{-1}$ in $\mathbb{F}_p$!
- In other words, we want to ask what $\mathbb{F}_p(i)/\mathbb{F}_p$ looks like: If $(x')^2 + 1 = 0$ has a solution in $\mathbb{F}_p$, then $i \in \mathbb{F}_p$ and $\mathbb{F}_p(i) = \mathbb{F}_p$. Otherwise it will be a quadratic extension.
- That is, $x^2 + y^2 = p$ has solution iff $\mathbb{F}_p(i)/\mathbb{F}_p$ is a trivial extension.

Galois side II: Frobenius

- Galois theory is our first powerful tool to study such extensions: $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma : \mathbb{Q}(i) \xrightarrow{\sim} \mathbb{Q}(i) \mid \sigma|_{\mathbb{Q}} = \mathrm{id}\}$ is a group of order $2 = \dim_{\mathbb{Q}} \mathbb{Q}(i)$; $\sigma(i) = \pm i$.
- There is a way to define an element $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ called **Frobenius element at** p that reflects the generator of $\mathrm{Gal}(\mathbb{F}_p(i)/\mathbb{F}_p)$. In this example Frob_p is trivial when $\mathbb{F}_p(i) = \mathbb{F}_p$ and the (unique) non-trivial element otherwise.
- That is, Frob_p is trivial iff $x^2 + y^2 = p$ has a solution.
- Warning: Frob_p is not always defined (for $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, not defined when $p = 2$), but can be defined for all but finitely many prime numbers p. Same for $K/\mathbb{Q}$ any finite Galois extension.
- In particular, solving $x^3 - x - 1 = 0 \in \mathbb{F}_p$ we can consider the Galois extension $K/\mathbb{Q}$ given by adjointing all roots of $x^3 - x - 1$. We have $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$. Except for $p = 23$ (which divides the discriminant of the polynomial) $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ can be defined.

Galois side III: Trace of a representation

Consider the Galois extension $K/\mathbb{Q}$ given by adjointing all roots of $x^3 - x - 1$. We have $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$

- When Frob_p is trivial, $x^3 - x - 1 = 0$ has three roots in $\mathbb{F}_p$, when $\mathrm{Frob}_p = (12)$ has order 2, $x^3 - x - 1$ has one root, and when $\mathrm{Frob}_p = (123)$ has order 3, $x^3 - x - 1$ has no root.
- The group S_3 is the symmetry group of an equilateral triangle. Putting the triangle at the middle of a 2-dimensional vector space (over $\mathbb{R}$ say) we get an irreducible representation of S_3.
- For this action of S_3, the trivial element has trace 2, the order 2 element (12) has trace 0, and the order 3 element (123) has trace -1, always one less than the number of roots/fixed points!
- This matches with our experiment earlier that

$$f = q - 1q^2 - 1q^3 + 0q^5 + q^6 + 0q^7 + q^8 + 0q^{11} - 1q^{13} + \ldots\ldots + 2q^{59} + \ldots$$

Galois side IV: general Galois representation

- We can form the Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ where $\bar{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ (e.g. the field of algebraic numbers in $\mathbb{C}$). The group $G_{\mathbb{Q}}$ has natural quotient map to any $\mathrm{Gal}(K/\mathbb{Q})$ ($K/\mathbb{Q}$ finite) and thus any representation of $\mathrm{Gal}(K/\mathbb{Q})$ can be viewed as a representation of $G_{\mathbb{Q}}$, called a Galois representation.
- The example of $\mathbb{Q}(i)/\mathbb{Q}$ also can be viewed as a 1-dimensional Galois representation: $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \{\pm 1\}$.
- It **matches** with the function $f : \mathbb{Z} \to \{\pm 1, 0\}$ by

$$f(n) := \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv -1 \pmod 4 \\ 0 & \text{else} \end{cases}$$

  As a toy example (what?) of modular form this seems way too easy.
- The example $y^2 - y = x^3 - x$ over $\mathbb{F}_p$ on the other hand is an elliptic curve E and gives a 2-dimensional Galois representation out of its ℓ-adic cohomology $H^1_{\acute{e}t}(E; \mathbb{Q}_\ell)$. We will skip that complicated story.

Representation side I: $\mathbb{Q}_p$

- You probably remember that $f : \mathbb{Z} \to \{\pm 1, 0\}$ given by

$$f(n) := \begin{cases} 1 & p \equiv 1 \,(\text{mod } 4) \\ -1 & p \equiv -1 \,(\text{mod } 4) \\ 0 & \text{else} \end{cases}$$

  should live in the "representation" side and should generalize to modular forms. Why representations?
- Notice: The first two cases give an isomorphism $(\mathbb{Z}/4)^\times \cong \{\pm 1\}$.
- We mentioned in the beginning that problems about $\mathbb{Q}$ (global) can be studied over $\mathbb{R}$ and at various prime number p (local). At a prime number p, we may consider the norm on $\mathbb{Q}$ given by

$$|\frac{ap^r}{b}|_p := p^{-r}, \ a, b, r \in \mathbb{Z}, ; a, b \not\equiv 0 \,(\text{mod } p)$$

- The key is that it gives a topology in which two elements are very close if their difference is divisible by p many times.
- One may take the completion of $\mathbb{Q}$ by this topology, getting a field called the field of p-**adic numbers** and denoted $\mathbb{Q}_p$.
- For example, $\frac{1}{25} + 1 + 3 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \ldots \in \mathbb{Q}_5$.

Representation side II: Adéles

- It's well known that $\mathbb{R}$ is the completion of $\mathbb{Q}$ under the usual archimedian norm. This different completion $\mathbb{Q}_p$ behaves similar to $\mathbb{R}$ in many ways; for example a good portion of manifold and measure theory works when $\mathbb{R}$ is literally replaced by $\mathbb{Q}_p$.
- A main difference: $\mathbb{Q}_p$ has a subring $\mathbb{Z}_p$ which is the closure (or equivalently completion) of $\mathbb{Z} \subset \mathbb{Q}$ under the norm $|\cdot|_p$. This subring is compact and open inside $\mathbb{Q}_p$.
- We put notation-wise $\mathbb{R} = \mathbb{Q}_\infty = \mathbb{Z}_\infty$, and call $\{\infty\} \cup \{2, 3, 5, 7, ...\}$ the set of **places** of $\mathbb{Q}$.
- Now let us define the so-called ring of adéles

$$\mathbb{A}_\mathbb{Q} := \{(a_v)_{v \text{ place of } \mathbb{Q}} \mid a_v \notin \mathbb{Z}_v \text{ for at most finitely many } v\} \subset \prod_v \mathbb{Q}_v.$$

It comes with a diagonal embedding $\mathbb{Q} \hookrightarrow A_\mathbb{Q}$.

Representation side III: Translation

$\mathbb{A}_{\mathbb{Q}} := \{(a_v)_{v \text{ place of } \mathbb{Q}} \mid a_v \notin \mathbb{Z}_v \text{ for at most finitely many } v\} \subset \prod_v \mathbb{Q}_v$.

- The story begins with the approximation theorems:

$$\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} \cdot \sum_v \mathbb{Z}_v,$$

$$\mathbb{A}_{\mathbb{Q}}^{\times} = \mathbb{Q}^{\times} \cdot \prod_v \mathbb{Z}_v^{\times} \tag{1}$$

  sort of like Chinese Remainder Theorem.
- Consider the subgroup $U \subset \mathbb{Z}_2^{\times}$ given by the closure (under $|\cdot|_2$) of integers that are $\equiv 1 \pmod 4$. We have natural isomorphism $\mathbb{Z}_2^{\times}/U \cong (\mathbb{Z}/4)^{\times}$ is a group of order 2 that we saw three slides ago.
- From (1) we have

$$(\mathbb{Z}/4)^{\times} \cong \mathbb{Z}_2^{\times}/U \cong \mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} / \prod_{v \neq 2} \mathbb{Z}_v \cdot U \tag{2}$$

  That is, we just form a seemingly silly way to write $\mathbb{Z}_2^{\times}/U$ (a group of order 2) as a double quotient of the complicated $\mathbb{A}_{\mathbb{Q}}^{\times}$.

Representation side IV: Automorphic language

- In our consideration, for any ring R let $GL_2(R)$ be the group of 2×2 matrices, for which all entries and its inverse' entries are in R. We have

$$GL_2(\mathbb{A}_{\mathbb{Q}}) \supsetneq \prod_v GL_2(\mathbb{Q}_v) \text{ satisfies } GL_2(\mathbb{A}_{\mathbb{Q}}) = GL_2(\mathbb{Q}) \cdot \prod_v GL_2(\mathbb{Z}_v).$$

- Consider the subgroup $U \subset GL_2(\mathbb{Z}_{23})$ consisting of matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $d-1, c \in 23 \cdot \mathbb{Z}_{23}$, as well as $O_2 \subset GL_2(\mathbb{R})$ the subgroup of rotations. We have

$$\begin{aligned} &(GL_2(\mathbb{Q}) \cap U \cdot \prod_{v \neq 23, \infty} GL_2(\mathbb{Z}_v)) \quad \backslash \quad GL_2(\mathbb{R}) \quad / \quad \mathbb{R}_+ \cdot O_2 \\ \cong \quad & GL_2(\mathbb{Q}) \quad \backslash \quad GL_2(\mathbb{A}_{\mathbb{Q}}) \quad / \quad U \cdot \prod_{v \neq 23} GL_2(\mathbb{Z}_v) \cdot \mathbb{R}_+ \cdot O_2 \end{aligned}$$

The group $GL_2(\mathbb{Q}) \cap U \cdot \prod_{v \neq 23, \infty} GL_2(\mathbb{Z}_v)$ is exactly the those $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in \mathbb{Z}$, $ad - bc = \pm 1$ and $d - 1 \equiv c \equiv 0 \pmod{23}$. The quotient $GL_2(\mathbb{R})/R_+ \cdot O_2$ is exactly the upper half plane. So this is in some sense where our previous modular forms live!

Representation side V: Automorphic forms

- The thing is, we go through translation which seems tedious but actually works generally. Then a modular form, originally a function on upper half plane $\mathfrak{H}$, becomes a function on $GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A}_{\mathbb{Q}})$.
- Such a function is called an **automorphic form** of GL_2.
- The group $GL_2(\mathbb{A}_{\mathbb{Q}})$ acts on the space of such functions by right translation (that is, $g.f(h) := f(hg)$). This is a big space. An **automorphic representation** is an irreducible sub-representation of this space.
- Our first baby case is the GL_1-case; $GL_1(R)$ is the group of 1×1 invertible matrices in R, i.e. $R^\times$. The same construction can be worked out for GL_n, any $n \geq 1$.
- Langlands correspondence: Automorphic representation of GL_n should correspond to n-dimensional Galois representations, with some restriction / decorations on both sides.
- Also generalized systematically when GL_n is replaced by other reductive groups, e.g. Automorphic representations of SO_{2n+1} correspond to $2n$-dimensional symplectic Galois representations.

Langlands correspondence

- The correspondence should interchange most important informations of both sides. For example, we can have on the automorphic side the representation generated by the automorphic form of GL_2 translated from $f = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n})$, and on the other side the 2-dimensional representation of the Galois group of $x^3 - x - 1$.
- The example that everybody talks about: Suppose a, b, c are integers such that $a^p + b^p = c^p$ for some prime $p \geq 3$. Consider the curve

$$y^2 = x(x - a^p)(x + b^p)$$

The 2-dimensional Galois representation associated to this cubic curve will corresponds (by Wiles and Wiles-Taylor) to some modular form. Then there is some trick (by Ribet, Serre, ...) that cooks up another modular form out of the previous one, which has some property too naive that it cannot exist.

Local Langlands correspondence

- For $n = 1$ Langlands correspondence is the so-called class field theory - one of the largest advancement in early 20th century. For $n > 1$ only special cases (can be very powerful!) are known.
- The Langlands correspondence we have talked about are also called global Langlands correspondence; it's about subspace of functions on $G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}})$ as representations of $G(\mathbb{A}_{\mathbb{Q}})$.
- Local Langlands correspondence instead look at representations of $G(\mathbb{Q}_v)$; every irreducible representation of $G(\mathbb{A}_{\mathbb{Q}})$ that we looked at necessarily contains a unique irreducible representation of $G(\mathbb{Q}_v) \subset G(\mathbb{A}_{\mathbb{Q}})$. Hence a local piece of the global datum.
- For example, the $n = 1$ case, i.e. local class field theory is equivalent to that there is a bijection between (1) finite abelian extensions $F/\mathbb{Q}_p$; this reflects 1-dimensional representations of $\mathrm{Gal}(\bar{Q}_p/\mathbb{Q}_p)$, and (2) finite index subgroup of $GL_1(\mathbb{Q}_p) = \mathbb{Q}_p^{\times}$.
- In fact, the bijection is just given by the image of norms from $F^{\times}$ to $\mathbb{Q}_p^{\times}$.
- In general from an explicit representation of $G(\mathbb{Q}_p)$ we hope to get explicit Galois representations for $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and vice versa.

Template for explicit local Langlands

- Say we begin with a local Galois representation $G_{\mathbb{Q}_p}$; this is a homomorphism $\varphi : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to G^\vee$ to some reductive group $G^\vee$ (typically over $\bar{\mathbb{Q}}_\ell$ for a different prime ℓ).
- The highlight is that the wild inertia of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ (a rather large normal pro-p-subgroup) usually has image in a maximal torus $T^\vee$ (a maximal connected commutative multiplicative subgroup, e.g. $(T^\vee)^o$ are the diagonal subgroup when $G^\vee = GL_n$); this always happens when p does not divide the order of the Weyl group $N_{G^\vee}(T^\vee)/T^\vee$.
- In this case, the local Langlands correspodence for $T^\vee$, because of the commutative nature, is given by local class field theory.
- Having things on the Galois side happening largely around a torus T, the main challenge is then to get a desired representation of $G(\mathbb{Q}_p)$ from a character of of $T(\mathbb{Q}_p)$. This is probably one of the most common situation among all different kinds of representation theories.

Induction from a torus

- For example, we can induce from the diagonal torus of GL_n or in general from a split maximal torus of a reductive group. This is called parabolic induction and appears the most frequently - from representations of finite reductive groups, real Lie groups, Lie algebras, automorphic induction (in the form of Eisenstein series), ...
- Or, we can induce from a maximal torus that splits (say, conjugate to diagonal) over an unramified extension of $\mathbb{Q}_p$. The construction this case relies on the similar story over $\mathbb{F}_p$, that starts from the so-called Deligne-Lusztig induction in which the representation is realized as the ℓ-adic cohomology of Deligne-Lusztig variety over $\mathbb{F}_p$.
- Or, we can induce from a maximal torus that is elliptic over an unramified extension. In this case, this is the work on harmonic analysis of p-adic group worked out by many and especially crowned by the construction of supercuspidal representations by Jiu-Kang Yu.
- These constructions (expectedly) give finite length but not irreducible representations, and the question of identifying the components is exactly a problem of the frontier of current researches.

Thank you!