The p-adic Local Langlands Correspondence

Eran Assaf
The Hebrew University of Jerusalem
eran.assaf@mail.huji.ac.il

1. Elliptic Curves

1.1 Definition

Let $f(x) \in \mathbb{Q}[x]$ be a cubic polynomial with rational coefficients and distinct roots. Then

$$E = E(\mathbb{C}) = \{(x,y) \in \mathbb{C}^2 \mid y^2 = f(x)\}$$

is an ***elliptic curve defined over*** $\mathbb{Q}$, and we denote by $E(\mathbb{Q}) = E \cap \mathbb{Q}^2$ its rational points.

We note that the requirement that f has distinct roots is equivalent to $\Delta(f) \neq 0$, where $\Delta(f)$ is its discriminant, defined as

$$\Delta(f) = a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2$$

where $x_1, \ldots, x_n$ are the roots of f, n is its degree and a_n is the leading coefficient.
The first result in understanding the rational solutions to the equation $y^2 = f(x)$ was

1.2 Theorem (Mordell, 1922)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then E is an abelian group, and it subgroup of rational points, $E(\mathbb{Q})$, is finitely generated.

However, we have not yet determined the rank of this group.
To this end, more complicated methods are needed.

2. L-function and The Birch-Swinnerton-Dyer Conjecture

Let p be a prime. Assume $f(x) \in \mathbb{Z}[x]$, we can then consider its reduction $\overline{f(x)} \in \mathbb{F}_p[x]$. Let

$$E(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p^2 \mid y^2 = f(x)\}$$

For any elliptic curve E, there is a number $N = N(E)$, called the ***conductor*** of E, measuring the effect of reduction at the different primes.
For any prime p, there is also a number a_p, which depends on $E(\mathbb{F}_p)$.

2.1 Definition

Let E be an elliptic curve defined over $\mathbb{Q}$. We call the ***Hasse-Weil Zeta function*** or the ***L-function*** attached to E the following infinite product

$$L(E,s) = \prod_{p^2 \nmid N} L_p(E,s)^{-1}$$

where

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s}) & p \nmid N \\ (1 - a_p p^{-s}) & p \mid N, \quad p^2 \nmid N \end{cases}$$

This product converges for $\Re(s) > \frac{3}{2}$.
Hasse conjectured (1954) that this function admits an analytic continuation to the whole complex plane, and that it satisfies a functional equation relating $L(E,s)$ with $L(E,2-s)$.
This allows one to conjecture

2.2 conjecture (Birch, Swinnerton-Dyer 1965)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$rank(E(\mathbb{Q})) = ord_{s=1} L(E,s)$$

3. Modular Forms

Let $\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ be the complex upper half plane. Let $\Gamma \leq GL_2^+(\mathbb{R})$ be a discrete subgroup. Form the quotient space $\Gamma \backslash \mathcal{H}$. It is compactified by adding finitely many points of $\partial \mathcal{H}$, called ***cusps***.

3.1 Definition

A ***modular form of weight*** k ***with respect to*** Γ is a function $f : \mathcal{H} \to \mathbb{C}$ satisfying:
(i) f is holomorphic on $\mathcal{H}$.
(ii) For any $z \in \mathcal{H}$ and any $\gamma \in \Gamma$, one has $f(\gamma z) = j(\gamma, z)^k \cdot f(z)$.
(iii) f is holomorphic at the cusps.
If f vanishes at the cusps, we say that f is a ***cusp form***.

From now on, for an integer N, we will consider

$$\Gamma = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \mod N \right\}$$

3.2 Definition

We say that a modular form with respect to $\Gamma_0(N)$ is a modular form ***of level*** N. Let $S_k(N)$ denote the space of cusp forms of weight k and level N.

Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, $f(z+1) = f(z)$ hence there is a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \quad q = e^{2\pi i z}$$

4. L-functions of Modular Forms

Modular forms can be viewed as functions on $\mathbb{Z}$-lattices in $\mathbb{C}$.
Hecke introduced natural operators on these functions, T_n for all $n \in \mathbb{N}$.

4.1 Definition

We say that $f \in S_k(N)$, which is an eigenvector for all the T_n, is a ***newform*** if it is not in the image of the natural map $S_k(N') \to S_k(N)$ for any $N' \mid N$. We say that f is ***normalized*** if $a_1 = 1$.

For normalized newforms, one may form

$$L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p L_p(f,s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{k-1-2s})^{-1} \cdot \prod_{p \mid N} (1 - a_p p^{-s})^{-1}$$

This looks, particularly when $k = 2$, very much like the Hasse-Weil zeta function!
Moreover, in this case one obtains a holomorphic continuation of $L(f,s)$ to $\mathbb{C}$ and a functional equation relationg $L(f,s)$ to $L(f,k-s)$.
It therefore remains to show the following.

4.2 The Modularity Theorem (Breuil, Conrad, Diamond, Taylor, Wiles 2001)

Let E be an elliptic curve defined over $\mathbb{Q}$. Let N be the conductor of E. Then there exists a cusp eigenform of weight 2 and level N, $f \in S_2(N)$ such that

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

and this verifies Hasse's conjecture (as well as Fermat's Last Theorem).

5. The Langlands Correspondence

Let $\mathbb{A} = \mathbb{R} \times \prod_p' \mathbb{Q}_p$ be the Adéle ring. Cusp forms give rise to certain representations of $GL_2(\mathbb{A})$, called ***cuspidal automorphic representations***. We denote it by $f \mapsto \pi_f$.
For such a representation π, write $\pi = \widehat{\bigotimes}_p \pi_p$ with π_p a representation of $GL_2(\mathbb{Q}_p)$.
For all p, there are $L_p(\pi,s) = L(\pi_p,s)$ and let $L(\pi,s) = \prod_p L_p(\pi,s)$. Then $L(\pi_f,s) = L(f,s)$
The Hasse-Weil zeta function can be viewed as an L-function associated to a representation ρ of the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, $L(\rho_E,s) = L(E,s)$.
For every local factor at a prime p, $L_p(\rho_E,s) = L_p(E,s)$ and $L_p(\pi,s) = L_p(f,s)$.

5.1 Langlands Conjecture for $GL_2(\mathbb{Q})$ (Langlands, 1969)

Fix a prime l. There is a natural bijection $\rho \mapsto \pi$ between the following categories:
{2-dimensional l-adic continuous irreducible representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ }
$\leftrightarrow$
{cuspidal automorphic representations of $GL_2(\mathbb{A})$, algebraic at infinity}
such that $L(\pi,s) = L(\rho,s)$.

The compatibility with Euler products should even give more.

5.2 Local Langlands Correspondence (Harris, Taylor, Henniart 2001)

Fix primes l,p such that $l \neq p$. Let F be a finite extension of $\mathbb{Q}_p$. There is a natural bijection $\rho \mapsto \pi$ between the following categories:
{n-dimensional l-adic continuous representations of $Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ which are Frobenius semisimple}
$\leftrightarrow$
{irreducible smooth l-adic representations of $GL_n(F)$}
such that $L_p(\pi,s) = L_p(\rho,s)$.

6. p-adic Local Langlands Correspondence

6.1 Definition

Let $F/\mathbb{Q}_p$ be a finite extension. A ***p-adic Galois representation*** is a continuous action of the absolute Galois group $Gal(\overline{F}/F)$ of F on a finite dimensional $\mathbb{Q}_p$-vector space.

6.2 Definition

Let $G = GL_n(F)$ for some $n \in \mathbb{N}$. A ***Unitary G-Banach space representation*** is a C-Banach space V, with a continuous action of G such that the norm is G-invariant.

Roughly speaking, the p-adic Langlands programme suggests the following:

6.3 Conjecture (p-adic Langlands philosophy)

There is a natural bijection $\rho \mapsto \Pi(\rho)$ between the following categories:
{n-dimensional p-adic representations of $Gal(\overline{F}/F)$ }
$\leftrightarrow$
{unitary Banach space representations of $GL_n(F)$}

When $n = 2$ and $F = \mathbb{Q}_p$, this conjecture can be made precise, the bijection is functorial and has been proved by Colmez, Berger, Breuil and others.
In all other cases, $n > 2$ or $F \neq \mathbb{Q}_p$, very little is known.
In our research, we attempt to find good candidates for $\Pi(\rho)$ either when $n = 2$ and $F \neq \mathbb{Q}_p$ or when considering different reductive groups, such as $U_3(F)$.