The Conjecture of Sato and Tate and its Partial Proof due to Clozel, Harris, Shepherd-Barron and Taylor

Number Theory and Computation Seminar

Robert L. Miller
University of Washington

November 7, 2008

Elliptic Curves

Let E be an elliptic curve over $\mathbb{Q}$, defined by a polynomial with coefficients in $\mathbb{Z}$:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

For p a prime, there are different possibilities for the reduction $E(\mathbb{F}_p)$ of E mod p, obtained by reducing the coefficients a_i mod p to obtain a defining polynomial with coefficients in $\mathbb{F}_p$.

- If $E(\mathbb{F}_p)$ is smooth, then we say E has *good reduction* at p, and p is a good prime for E.
- If $E(\mathbb{F}_p)$ is singular, then we say E has *bad reduction* at p, and p is a bad prime for E.

Elliptic Curves

Suppose p is a bad prime for E, say with singular point $P = (x_0, y_0)$. Then writing the Taylor expansion at (x_0, y_0) gives (note that $\partial f/\partial x = \partial f/\partial y = 0$ at the singular point):

$$f(x, y) - f(x_0, y_0) =$$

$$= (y - y_0)^2 + \lambda_1(x - x_0)(y - y_0) + \lambda_2(x - x_0)^2 - (x - x_0)^3 =$$

$$= [(y - y_0) - \alpha(x - x_0)]\,[(y - y_0) - \beta(x - x_0)] - (x - x_0)^3$$

- If $\alpha = \beta$ (unique tangent line at P), then we say $E(\mathbb{F}_p)$ has a *cusp* at P, and E has additive reduction at p.
- If $\alpha \neq \beta$ (two distinct tangent lines at P), then we say $E(\mathbb{F}_p)$ has a *node* at P, and E has multiplicative reduction at p. If $\alpha, \beta \in \overline{\mathbb{F}_p}$ are actually in $\mathbb{F}_p$, then the reduction is said to be split multiplicative (otherwise non-split).

Elliptic Curves

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

- $b_2 = a_1^2 + 4a_2$
- $b_4 = 2a_4 + a_1a_3$
- $b_6 = a_3^2 + 4a_6$
- $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_3^2a_2 - a_4^2$
- $c_4 = b_2^2 - 24b_4$
- $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$
- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ (discriminant)
- $j = \frac{c_4^3}{\Delta}$ (j-invariant)
- $\omega = \frac{dx}{2y+a_1x+a_3}$ (invariant differential)

Elliptic Curves

- $E/\mathbb{F}_p$ is singular iff $\Delta = 0$.
- $E/\mathbb{F}_p$ has a node iff $\Delta = 0$ and $c_4 \neq 0$.
- $E/\mathbb{F}_p$ has a cusp iff $\Delta = 0$ and $c_4 = 0$.

Now we are ready to define the $a_p(E)$:

- For any p, define $a_p = p + 1 - \#E(\mathbb{F}_p)$.
- If E has bad reduction at p, then

$$a_p = \begin{cases} 0 & \text{additive reduction} \\ 1 & \text{split multiplicative reduction} \\ -1 & \text{non-split multiplicative reduction} \end{cases}$$

Elliptic Curves

Theorem (Hasse)

$$|a_p| \leq 2\sqrt{p}$$

Let K be a finite field of order q, and E/K an elliptic curve. If F is the q-th power Frobenius map, then for $P \in E(\overline{K})$, we have $P \in E(K)$ iff $F(P) = P$, i.e. $E(K) = \ker(1 - F)$. Since $\# \ker(1 - F) = \deg(1 - F)$ and F is of degree q, a version of Cauchy-Schwarz finishes the proof:

$$|\deg(1 - F) - \deg(1) - \deg(F)| \leq 2\sqrt{\deg(1)\deg(F)}$$

Note that one can show that (for F Frobenius acting on E, F_p acting on $T_p(E)$) $\operatorname{tr}(F_p) = 1 + \deg(F) - \deg(1 - F) = a_p$.

Elliptic Curves

Theorem (Hasse)

$$|a_p| \leq 2\sqrt{p}$$

As a consequence, $-1 \leq \frac{a_p}{2\sqrt{p}} \leq 1$. Define the angle $\phi_p \in [0, \pi]$ as the arc-cosine of $\frac{a_p}{2\sqrt{p}}$.

Conjecture

Suppose E does not have complex multiplication. As $p \to \infty$, the ϕ_p approach the Sato-Tate distribution

$$\frac{2}{\pi} \sin^2 \phi \; d\phi.$$

The Tate Module

Given our elliptic curve E, recall that $E \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda = \langle 1, \tau \rangle$. Using this one concludes that $E[n] = \{P \in E(\mathbb{C}) \mid [n]P = P + \cdots + P = 0\}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. (Note that since addition is defined by polynomials, $E[n] \subset E(\overline{\mathbb{Q}})$.) Let ℓ be a prime, and consider the sequence:

$$\begin{tikzcd} E[\ell] & E[\ell^2] \arrow[l, "\cdot\ell"'] & E[\ell^3] \arrow[l, "\cdot\ell"'] & \cdots \arrow[l, "\cdot\ell"'] \end{tikzcd}$$

Define the ℓ-adic Tate module by

$$T_\ell(E) = \varprojlim_n E[\ell^n]; \; V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

This gives an ℓ-adic Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V_\ell(E))$.

Compatible Families

Definition

An ℓ-adic representation ρ is *rational (integral)* if there is a finite set of primes such that ρ is unramified away from those primes p, and the coefficients of the characteristic polynomial $P_{p,\rho}(T)$ of Frobenius at such primes are elements of $\mathbb{Q}$ ($\mathbb{Z}$).

Definition

For ρ an ℓ-adic Galois representation and ρ' an ℓ'-adic Galois representation, which we assume are both rational, we say these are *compatible* if there is a finite set S of primes such that ρ and ρ' are unramified away from S and the characteristic polynomials of Frobenius away from S are all equal.

Compatible Families

Definition

For each prime ℓ, suppose we have a rational ℓ-adic representation ρ_ℓ. The system (ρ_ℓ) is *compatible* if $\rho_\ell, \rho_{\ell'}$ are compatible for any two primes ℓ, ℓ'. The system is *strictly compatible* if there is a finite set S (the exceptional set) of primes such that

- For $v \notin S$ and $v \nmid \ell$, ρ_ℓ is unramified at v and $P_{v,\rho}(T)$ has rational coefficients.
- For $v \notin S$ and $v \nmid \ell\ell'$,

$$P_{v,\rho_\ell}(T) = P_{v,\rho_{\ell'}}(T)$$

The Tate module provides a strictly compatible family of ℓ-adic Galois representations, with $S = \{p : p \mid \Delta\}$. We say that a family (ρ_ℓ) is *irreducible* if each ρ_ℓ is.

L-functions

Given a strictly compatible family $\rho = (\rho_\ell)$ of rational ℓ-adic representations with exceptional set S, one can define an L-function. For $v \notin S$, $P_{v,\rho}(T) = P_{v,\rho_\ell}(T)$ does not depend on $\ell \nmid v$. For s a complex variable, define:

$$L_\rho(s) = \prod_{v \notin S} \frac{1}{P_{v,\rho}((Nv)^{-s})}$$

If the Galois group acts through a finite group, then one can show that this is an Artin L-function. For the Tate module of an elliptic curve, this is the normal L-function of E (excluding the bad primes, which is fine for us, since we are talking about asymptotic distributions: normally what one does is to quotient out the nontrivial action of inertia first).

Equidistribution

Let:

- X be a compact topological space,
- $C(X)$ be the space of continuous complex valued functions on X, with its norm $||f|| = \sup_{x \in X} |f(x)|$, and
- μ be a Radon measure (locally finite, inner regular) on X.

Recall that $\mu(f) = \int_X f \ d\mu$.

Definition

We say that a sequence (x_n) in X is μ-equidistributed if the sequence of measures

$$\mu_n = \frac{\delta_{x_1} + \cdots + \delta_{x_n}}{n}$$

converges weakly to μ, i.e. $\mu_n(f) \to \mu(f)$ as $n \to \infty$ for any $f \in C(X)$.

The Haar Measure

Given a locally compact topological group G, we can require a measure μ on G to be:

- countably additive and regular,
- left translation invariant: $\mu(aS) = \mu(S)$ for $a \in G$ and S a Borel subset of G, and
- such that $\mu(U) > 0$ for all nonempty open Borel sets U.

It turns out that this uniquely characterizes a measure up to a multiplicative constant, called the Haar measure on G. We can normalize by requiring that $\mu(G) = 1$.

The Haar Measure

Theorem

Suppose X is the set of conjugacy classes of G, and μ is a measure on G (hence on X by $G \to X$). A sequence (x_n) in X is μ-equidistributed iff

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = \mu(\chi)$$

for any irreducible character χ of G.

This theorem is a consequence of the Peter-Weyl theorem, which implies that the irreducible characters of G generate a dense subspace of $C(X)$. If μ is the Haar measure with $\mu(G) = 1$, then $\mu(\chi) = 0$ unless χ is the trivial character in which case $\mu(\chi) = 1$.

L-functions

Let x_v for $v \in \Sigma$ be a sequence in X where Σ is a denumerable set, and $v \to Nv$ a function into integers ≥ 2. Suppose the following hold:

- The following product converges for $\Re(s) > 1$, and extends meromorphically to $\Re(s) \geq 1$ with neither zero nor pole except simple pole at $s = 1$: (think $\zeta_K(s)$)

$$\prod_{v \in \Sigma} \frac{1}{1 - (Nv)^{-s}}.$$

L-functions

Let x_v for $v \in \Sigma$ be a sequence in X where Σ is a denumerable set, and $v \longrightarrow Nv$ a function into integers ≥ 2. Suppose the following hold:

- If ρ is an irreducible representation of G with character χ, the following product converges for $\Re(s) > 1$, and extends meromorphically to $\Re(s) \geq 1$ with neither zero nor pole except possibly for $s = 1$:

$$L(\rho, x_v, s) = \prod_{v \in \Sigma} \frac{1}{\det(1 - \rho(x_v)(Nv)^{-s})}.$$

Denote the order of $L(\rho, x_v, s)$ at $s = 1$ by $-c_\chi$.

L-functions

Theorem

With the above assumptions, for χ an irreducible character of G,

- *As $n \to \infty$*

$$\#\{v \in \Sigma : Nv \leq n\} \simeq \frac{n}{\log n}.$$

- $$\sum_{Nv \leq n} \chi(x_v) = c_\chi \frac{n}{\log n} + o\left(\frac{n}{\log n}\right).$$

In particular,

$$\frac{1}{\#\{Nv \leq n\}} \sum_{Nv \leq n} \chi(x_v) \to c_\chi \text{ as } n \to \infty$$

Back to the Conjecture...

Let E be an elliptic curve defined over a number field K and let Σ be the set of finite places of K at which E has good reduction. Fixing $v \in \Sigma$, we can consider the eigenvalues of Frobenius at v, which must be complex conjugates $\pi_v, \overline{\pi}_v$. (Here was are considering Frobenius on the Tate module $T_\ell(E)$, but as we have seen, the choice of $\ell \nmid v$ does not matter.) Define $\phi_v \in [0, \pi]$ by

$$\pi_v = (Nv)^{1/2} e^{i\phi_v}.$$

By normalizing Frobenius we obtain determinant 1 unitary transformations: this corresponds to using Hasse's bound to normalize the a_p, since $(Np)^{1/2} = \sqrt{p}$.

Connecting Things...

Let $G = SU(2)$ (unitary determinant 1 matrices), and note that any conjugacy class possesses a unique representative of the form $\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}$ with $0 \leq \phi \leq \pi$. Thus $x_v = \phi_v$ is interpreted as a sequence in X, the conjugacy classes of G. The Haar measure on $G = SU(2)$ when considered on X is the measure

$$\frac{2}{\pi} \sin^2 \phi d\phi.$$

If ρ is the natural representation of G (2x2 matrices, after all...), then the irreducible characters of G are the mth symmetric powers ρ^m of ρ.

The Conjecture

We had made two assumptions earlier, which allowed us to conclude equidistribution with respect to the Haar measure. One was related to what turns out to be the zeta function ζ_K of the number field K, and is true. The other was related to the irreducible representations of G, in this case ρ^m. It was that the following L-function converges for $\Re(s) > 1$, and extends meromorphically to $\Re(s) \geq 1$ with neither zero nor pole except possibly for $s = 1$:

$$L_{\rho^m}(s) = \prod_{v \in \Sigma} \prod_{a=0}^{m} \frac{1}{1 - e^{i(m-2a)\phi_v}(Nv)^{-s}}.$$

Note that we also need that

$$\frac{1}{\#\{Nv \leq n\}} \sum_{Nv \leq n} \chi(x_v) \to 0 \text{ as } n \to \infty$$

for nontrivial characters χ of G (Chebotarev's Density Theorem).

The Conjecture

If this is true, then we have that the ϕ_v are uniformly distributed with respect to the image of the Haar measure on $X \simeq [0, \pi]$, given by

$$\frac{2}{\pi} \sin^2 \phi d\phi.$$

Thus the desired properties for $L_{\rho^m}(s)$ would imply the Sato-Tate conjecture, which is precisely that the angles ϕ_v are uniformly distributed with respect to $\frac{2}{\pi} \sin^2 \phi d\phi$.

Symmetric Powers

Briefly, the symmetric algebra $S^2(V)$ is $V \otimes V / \langle v \otimes w - w \otimes v \rangle$, and in this fashion we can form $S^k(V)$ for general $k \geq 1$. Taking the *m*th symmetric power of ρ amounts to taking the image of $\rho \otimes \cdots \otimes \rho$ in the quotient $T^m(G^*) \to S^m(G^*)$. We have that up to conjugacy

$$\rho(x_v) = \mathrm{Diag}(e^{i\phi_v}, e^{-i\phi_v}).$$

One can show that up to conjugacy

$$\rho^m(x_v) = \mathrm{Diag}(e^{mi\phi_v}, e^{(m-2)i\phi_v}, \cdots, e^{-(m-2)i\phi_v}, e^{-mi\phi_v}).$$

Note that for the strictly compatible family of Galois representations $(V_\ell(E))$ the symmetric powers are also strictly compatible. By a theorem of Serre, E having no complex multiplication implies that these are irreducible.

To Prove the Conjecture

It remains to show that the following L-functions converge for $\Re(s) > 1$, and extends meromorphically to $\Re(s) \geq 1$ with neither zero nor pole except possibly for $s = 1$:

$$L_{\rho^m}(s) = \prod_{v \in \Sigma} \prod_{a=0}^{m} \frac{1}{1 - e^{i(m-2a)\phi_v}(Nv)^{-s}}.$$

The Langlands Program

Goal is relating irreducible strictly compatible families of rational ℓ-adic $\mathrm{Gal}(\overline{K}/K)$ characters χ of degree d (with values in a number field F) to cuspidal automorphic forms ω for $\mathrm{GL}(d)$ over K that are eigenforms for the appropriate Hecke operators (with eigenvalues in F).
Say they are linked (χ is cuspidal automorphic) if for every nonexceptional place v the value $\chi(v)$ is equal to the eigenvalue of the appropriate Hecke operator attached to v acting on ω. If this is the case, then certain L-functions turn out to be equal, since the eigenvalues determine the representations.
This is more than enough for our ρ^m in order to prove Sato-Tate. We need only the property of *potential automorphy* for odd m, since although cuspidal automorphy provides nice holomorphic continuations, potential automorphy provides meromorphic continuations, which is all we need.

Aside on Automorphic Forms

- G - a Lie group.
- M - a smooth G-module.
- ω - section of any vector bundle over M admitting a compatible action of G.
- $\Gamma \subset G$ - a discrete subgroup.

Use ω to construct a representation of the group G on the vector space consisting of all translates of ω by G. We require ω to further be invariant under Γ.

Generalization of modular forms, where $G = \mathrm{PSL}_2(\mathbb{R})$, $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, $M = \mathcal{H}$, and $\omega = f$ is the holomorphic function on $\mathcal{H}$.

Our Symmetric Powers

- $m = 0$: then ρ is trivial, and the L-function is the Riemann zeta-function.
- $m = 1$: then this is linked to the invariant differential ω under the action of $\Gamma_1(N)$. Here we view the upper half plane as a homogeneous space under the action of $\mathrm{PSL}_2(\mathbb{R})$. (Thanks to Taylor-Wiles)
- $2 \leq m \leq 4$: then this is linked to a differential ω_n on the homogeneous space $\mathrm{GL}_{n+1}/\mathrm{SO}_{n+1} \cdot \mathbb{R}^+$ with appropriate invariance properties.
- $m > 4$: in this case, there are only weaker conclusions, but still enough to conclude Sato-Tate for certain types of elliptic curves: potential automorphy.

Potential Automorphy

The essential idea here is to take a compatible family of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ representations and "lift" this family to a finite extension $F/\mathbb{Q}$, by restricting to the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

A compatible family of Galois representations over $\mathbb{Q}$ is *strongly potentially cuspidal automorphic* if there is some totally real Galois number field $K/\mathbb{Q}$ such that its lifting is cuspidal automorphic.

So it remains to prove that odd symmetric powers of the Tate module representation are potentially automorphic.

Galois Deformation Theory

Suppose we have an irreducible ℓ-adic Galois representation

$$\rho : G_K \to \mathrm{GL}_d(\mathcal{O}_\ell) \subset \mathrm{GL}_d(\overline{\mathbb{Q}_\ell}),$$

where $\mathcal{O}_\ell$ is the ring of integers of $\overline{\mathbb{Q}_\ell}$. By passing from $\mathcal{O}_\ell$ to its residue field $\overline{\mathbb{F}_\ell}$, we obtain the associated *residual representation*

$$\overline{\rho}_\ell : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}_\ell}).$$

Taking an equivalent ρ results in a residual representation whose semisimplification is equivalent to that of the original residual representation.

Galois Deformation Theory

The question is given a prime ℓ and a representation $r : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}_\ell})$, to consider the possible liftings $\rho : G_K \to \mathrm{GL}_d(\mathcal{O}_\ell)$ so that $r = \overline{\rho}_\ell$.
In particular, Barry Mazur defines a Galois deformation theorem to be one which assumes certain conditions on the residual representation r, on the possible global liftings ρ, and on the local data of the restriction of ρ to all the decomposition groups, and which concludes that for such r, if there is any lifting ρ which satisfies the conditions given and is strongly potentially automorphic, then every lifting satisfying the conditions is also strongly potentially automorphic.

Galois Deformation Theory

Theorem (Taylor, June '08)

Let $n = 2m, m \in \mathbb{N}$ and let $\ell > \max\{3, n\}$ be a prime, and suppose $r : G_{\mathbb{Q}} \to GSp_n(\mathbb{Z}_\ell)$ be an irreducible representation such that

- *r ramifies at only finitely many primes.*
- *$r|_{G_{\mathbb{Q}_\ell}}$ is crystalline and $\dim_{\mathbb{Q}_\ell} gr^i(r \otimes_{\mathbb{Q}_\ell} B_{DR})^{G_{\mathbb{Q}_\ell}} = 0$ unless $0 \leq i < n$ in which it has dimension 1.*
- *There is a prime $q \neq \ell$ such that $r|^{ss}_{G_{\mathbb{Q}_q}}$ is unramified and $r|^{ss}_{G_{\mathbb{Q}_q}}(F_q)$ has eigenvalues $\{\alpha q^i : 0 \leq i < n\}$ for some α.*
- *The image of $r \mod \ell$ contains $Sp_n(\mathbb{F}_\ell)$.*
- *$r \mod \ell$ arises from a cuspidal automorphic representation π_0 of $GL_n(\mathbb{A})$ for which $\pi_{0,\infty}$ has trivial infinitesimal character and $\pi_{0,q}$ is an unramified twist of the Steinberg representation.*

Then r arises from a representation π with the same properties as

Galois Deformation Theory

Corollary

For E an elliptic curve with multiplicative reduction at some prime (this condition is imposed by 3 above), and for odd m, the representation ρ^m is potentially automorphic.

This implies that there is some known cuspidal automorphic representation which gives the same residual representation as ρ^m. Since this implies Sato-Tate, all that is left is to find this representation explicitly.

The Dwork Pencil

$$Y_t : X_0^{n+1} + X_1^{n+1} + \cdots + X_n^{n+1} = (n+1)tX_0X_1\ldots X_n$$

for $t \in \mathbb{Q} - \mathbb{Z}[1/(n+1)]$. Note that for $n = 2$, this is an elliptic curve. In general, it is a Calabi-Yau manifold. Define

$$H = \{(\zeta_0, ..., \zeta_n) \in \mu_{n+1}^{n+1} | \prod_j \zeta_j = 1\}/\Delta(\mu_{n+1}),$$

which acts on the family by multiplying X_i by ζ_i. Then define

$$V_{t,\ell} = H_{\text{ét}}^{n-1}(Y_t(\overline{\mathbb{Q}}), \mathbb{Q}_\ell)^H.$$