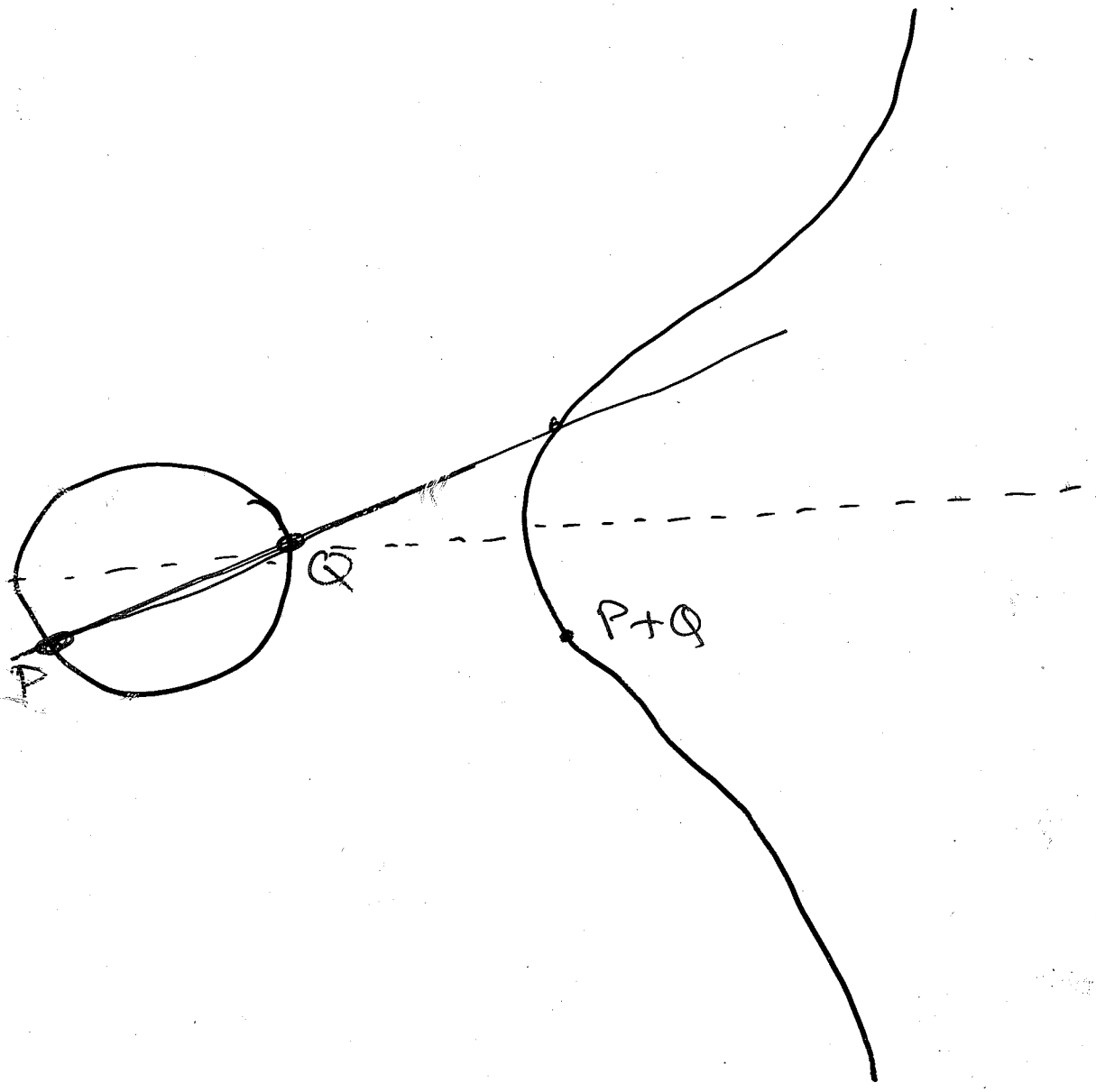


E elliptic curve defined over $\mathbb{Q}$, i.e. a non-singular projective cubic plane curve.

If we want, affine equation

$$y^2 = x^3 + ax + b \qquad a, b \in \mathbb{Q}$$

The group law is figured in the above picture.

One will assume that E is <u>without complex multiplication</u>, no endomorphisms compatible with the above group structure except the trivial ones:

$$\mathrm{End}_{\bar{\mathbb{Q}}} E = \mathbb{Z}$$

Take any equation of E over $\mathbb{Z}$ and reduce mod. the primes, this reduction is well-defined up to a finite number of p's.

Write $\#E(\mathbb{F}_p) = 1 + p - a_p$

It has been known for a long time that $|a_p| \leq 2\sqrt{p}$ so we can put

$$a_p = 2\sqrt{p}\cos\theta_p \qquad \theta_p \in [0, \pi]$$

A slightly more sophisticated way to define this is to speak of the <u>eigenvalues of Frobenius</u> (acting on the ℓ-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to E). These eigenvalues are $\alpha_p = 2\sqrt{p}\, e^{i\theta_p}$ and $\bar{\alpha}_p = 2\sqrt{p}\, e^{-i\theta_p}$.

The Sato-Tate conjecture predicts the repartition of the θ_p inside $[0,\pi]$.

Conjecture ST (Early 60') The sequence θ_p is equidistributed in $[0,\pi]$ with respect to the measure $\mu = \frac{2}{\pi}\sin^2\theta\, d\theta$.

That means that for any continuous function f on $[0,\pi]$ we have

$$\frac{1}{\mathrm{Card}\{p \le N\}} \sum_{p \le N} f(\theta_p) \xrightarrow[(N\to\infty)]{} \mu(f).$$

Now this is proved, according to work of Clozel, Harris, Shepherd-Barron, Taylor, under a slightly stronger hypothesis.

Th Assume that $j(E) = -1728 \frac{4a^3}{4a^3+27b^2}$ is not integral (this is equivalent to the fact that E has somewhere multiplicative reduction and this implies that E has no CM).

Then the Sato-Tate conjecture is true for E.

We have an analogous conjecture for E defined over any number field F and the analogous theorem when F is totally real.

It has been known, essentially since the first statement of this conjecture, that it can be reduced to some conjectural properties of certain L-functions.

Let me first explain the meaning of the Sato-Tate measure μ.

$$[0,\pi] \xrightarrow{\sim} \text{Set of conjugacy classes of } SU(2)$$

$$\theta \longrightarrow \begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix}^{\sim}$$

$$\arccos \frac{\mathrm{tr}\, g}{2} \longleftarrow g$$

And it is not difficult to check that μ is the direct image of the normalized Haar measure on this group. This can be viewed as a particular case of H. Weyl integration formula for class functions on a compact group G:

$$\int_G f(g)\,dg = \frac{1}{|W(G,T)|} \int_T \det\left(1 - \mathrm{Ad}(t^{-1})\right)\Big|_{\mathfrak{g}/\mathfrak{t}} f(t)\,dt.$$

So the ST conjecture is equivalent to the equidistribution of the conjugacy classes of the $\Theta_p = \begin{pmatrix} e^{i\theta_p} & \\ & e^{-i\theta_p} \end{pmatrix} \in SU(2)$

ie the fact that for any class function χ on G we have

$$\frac{1}{\#\{p \leq N\}} \sum_{p \leq N} \chi(\Theta_p) \longrightarrow \int_G \chi(g)\,dg$$

A result of Serre (in "Abelian ℓ-adic representations and Elliptic curves"), also known by other people (Tate ...).

K compact group, assume we are given for each prime p a conjugacy class Θ_p in K.

For any irreducible representation r of K define

$$L(s,r) = \prod_p \det\left(1 - p^{-s} r(\Theta_p)\right)^{-1}$$

cv for $\mathrm{Re}\, s > 1$

Prop Suppose that, for any non-trivial r, $L(s,r)$ admits an holomorphic continuation to some open set containing $\{\mathrm{Re}\, s \geq 1\}$ and that this continuation does not vanish on $\mathrm{Re}\, s = 1$. Then the $\widetilde{(H)}_p$ are equidistributed in the conjugacy classes of K.

Classical example ! $\quad K = (\mathbb{Z}/N\mathbb{Z})^*$

$\widetilde{(H)}_p = \dot{p}$

The proof in the general case is not very different from the classical one (Hadamard-de la Vallée Poussin methods)

Sketch

• One has to show the above convergence for χ the character of an irreducible nontrivial representation r. Note that $\mu(\chi) = 0$.

$$L(s,r) = \prod_p \prod_{i=1}^{n} \frac{1}{1 - p^{-s}\lambda_{i,p}}$$

where the $\lambda_{i,p}$ are the eigenvalues of $r(\widetilde{(H)}_p)$.

$$-\frac{L'}{L} = \sum_P \sum_i \frac{p^{-s}\log p}{1-p^{-s}\lambda_{i,p}}$$

$$= \sum_P \sum_i \sum_{m\geq 1} p^{-ms}\lambda_{i,p}^m \log p$$

$$= \sum_P \sum_{m\geq 1} p^{-ms}\chi(\Theta_p^m)\log p$$

$$= \sum_P p^{-s}\chi(\Theta_p)\log p$$

+ Something holomorphic on $\mathrm{Re}\, s \geq 1$

Now we apply the Wiener-Ikehara tauberian theorem, this gives:

$$\sum_{p\leq N} \chi(\Theta_p)\log p = o(N).$$

and, using a classical lemma of analytic number theory, we get

$$\sum_{p\leq N} \chi(\Theta_p) = o\left(\frac{N}{\log N}\right)$$

but $\#\{p \leq N\} \sim \frac{N}{\log N}$ QED.

Wiener - Ikehara theorem

Let $F(s) = \sum a_n / n^s$ be a Dirichlet series. Suppose there is another one $F^+(s) = \sum a_n^+ / n^s$ with positive real coefficients such that:

(a) $|a_n| \leq a_n^+$ for all n

(b) F^+ converges for $\mathrm{Re}\, s > 1$

(c) F^+ (resp F) can be extended to a meromorphic function on $\mathrm{Re}\, s \geq 1$ having no poles except (resp except possibly) for a simple pole with residue c^+ (resp c, possibly 0).

Then $$\sum_{n \leq N} a_n = cN + o(N)$$

A classical lemma (simple consequence of Abel's summation)

$$\sum_{n \leq N} b_n = o(N) \implies \sum_{n \leq N} \frac{b_n}{\log n} = o\left(\frac{N}{\log N}\right)$$

In our case the irreductible representations of $SU(2)$ are the mth. symetric powers of the standard 2-dimensional one and the corresponding L-functions are :

$$L(s, \mathrm{Sym}^m E) = \prod_p \left(1-\beta_p^{-m} p^{-s}\right)^{-1}\left(1-\beta_p^{-m+2} p^{-s}\right)^{-1} \cdots \left(1-\beta_p^{m} p^{-s}\right)^{-1}$$

with $\beta_p = e^{i\theta_p}$.

For $m=1$ this is nothing else but the L-function of the elliptic curve E (with an unusual normalization). Because E is modular (according to Taylor-Wiles + Breuil, Conrad, Diamond) this is the L-function associated to a modular form f of weight 2

$$L^*(s, E) = * L\left(s+\tfrac{1}{2}, f\right).$$

For such an L-function the holomorphic continuation + non-vanishing results have been known for a long time (Ogg, Rankin).

What happens if $m > 1$?

Conjecturally, $\mathrm{Sym}^m E$ should correspond to some automorphic representation of $GL_{m+1}(\mathbb{A})$.

▶ Classical modular form (of weight 2)

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ • $(c \equiv 0 \ (N))$.

Such a classical object gives rise to an automorphic form on

$$GL_2(\mathbb{A}) = \coprod GL_2(\mathbb{Q}_p) \times GL_2(\mathbb{R})$$

(i.e. something on $GL_2(\mathbb{Q}) \backslash GL_2(\mathbb{A})$)

which can be defined, using the decomposition

$$GL_2(\mathbb{A}) = GL_2(\mathbb{Q})\, GL_2(\mathbb{R})^+ K_N$$

(where $K_N \subset \prod GL_2(\mathbb{Z}_p)$ is defined by $c \equiv 0 \ (N)$)

by the formula

for $g = \gamma g_\infty k \qquad g_\infty = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$

$$\phi(g) = f(g_\infty(i))(zi+t)^{-2}\det g_\infty$$

This is a cuspidal automorphic form (ie satisfying some growth conditions I do not want to make explicit here). In Langlands' theory one rather considers the $GL_2(\mathbb{A})$-representation that ϕ generates (as a sub-representation of $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}))$) which is an irreducible (cuspidal) automorphic representation π of $GL_2(\mathbb{A})$. It decomposes as a tensor product $\pi = \otimes \pi_v$ of representations of the local groups $GL_2(\mathbb{Q}_p)$ and $GL_2(\mathbb{R})$.

▶ All those definitions make sense for GL_n.

Conjecture For any $m \geq 2$ $\rho_m = \mathrm{Sym}^m H^1_{\acute{e}t}$ corresponds to an automorphic cuspidal representation of $GL_{m+1}(\mathbb{A})$.

This means that for all p except a finite number, π_p is the spherical principal series of $GL_{m+1}(\mathbb{Q}_p)$ induced by the $m+1$ unramified characters ξ_i of $\mathbb{Q}_p^*$ which send $p \longrightarrow$ normalized eigenvalues of Frobenius $\{\beta_p^{-m}, \dots, \beta_p^m\}$

If the conjecture were true, then the L-function we are interested in would coincide with the L-function of an automorphic representation of GL_n, which is known to satisfy the required properties.

▶ In fact what we can prove at the moment is weaker: "potential automorphy" result.

Th For m odd, there exists a Galois totally real extension $F/\mathbb{Q}$ and a cuspidal automorphic representation π of $GL_{m+1}(\mathbb{A}_F)$ which corresponds to $\rho_m \mid Gal(\overline{\mathbb{Q}}/F)$.

This is in fact enough according to some (Brauer-type) arguments invented by Taylor some time ago.

The Brauer induction theorem allows us to write the trivial representation of $Gal(F/\mathbb{Q})$ as a virtual sum of induced representations

$$1_{Gal(F/\mathbb{Q})} = \sum m_i \, \mathrm{Ind}_{Gal(F/F_i)}^{Gal(F/\mathbb{Q})} \chi_i$$

with F/F_i solvable and χ_i a 1-dim. representations.

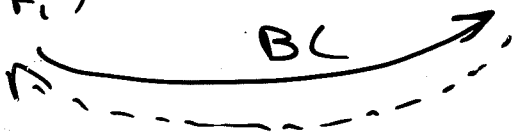
Then we can write $\rho = \rho_m$ as

$$\rho = \sum m_i \operatorname{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} \left(\rho|_{G_{F_i}} \otimes \chi_i \right)$$

Then the usual properties of L-functions give

$$L(s, \rho) = \prod L_{F_i}\left(s, \rho|_{G_{F_i}} \otimes \chi_i\right)^{m_i}.$$

But, for solvable extensions, we have relations ("Base change") between automorphic representations of $GL_n(\mathbb{A}_{F_i})$ and $GL_n(\mathbb{A}_F)$



$\rightsquigarrow$ get the fact that the L_{F_i} above are holomorphic and $\neq 0$ on $\mathrm{Re}\, s \geq 1$; so this is still true for the above product.

- There is also a trick for even symetric powers, based on the decomposition:

$$\rho_m \otimes \rho_1 \simeq \rho_{m+1} \oplus \rho_{m-1}$$

From that we get the formula:

$$L(s, \rho_{m+1}) = \frac{L(s, \rho_m \otimes \rho_1)}{L(s, \rho_{m-1})}$$

If m is odd, the Rankin-type L-function $L(s, \rho_m \otimes \rho_1)$ has the good properties and this allows to prove what we want by induction for even symetric powers.

The method to prove the potential automaphy of $\rho = \rho_m$ follows the Taylor-Wiles ideas: two things have to be checked.

① The fact that the reduction mod ℓ $\bar{\rho}$ of ρ is automorphic (at least potentially) i.e. is the reduction of some ρ' which is potentially automorphic.

② An "automorphy lifting theorem" (ALT) which says roughly the following:

$\bar{\rho}$ automorphic $\Longrightarrow$ ρ automorphic.
(+ many hypothesis on $\bar{\rho}, \rho$)

---

3 Preprints

[CHT] Clozel, Harris, Taylor: Automorphy for some ℓ-adic lifts of automorphic modulo ℓ representations.

[HSBT] Harris, Shepherd-Barron, Taylor: A family of Calabi-Yau varieties and potential automorphy.

[T] Taylor: Automorphy for some ℓ-adic ------ II.

Those results are technically complicated. There are several ALT-type theorems which are needed in the proof. Let me state at least one properly.

Theorem Let F be a totally real field, $n \geq 2$, $\ell > n$ a prime which is unramified in F. Let

$$\rho : \mathrm{Gal}(\bar{F}/F) \longrightarrow GL_n(\bar{\mathbb{Q}}_\ell)$$

be a continuous irreducible representation. Assume

(1) $\rho^\vee \simeq \rho \chi^{n-1}$ (χ cyclotomic ch.)

(2) ρ is unramified except at a finite # of places.

(3) The restrictions of ρ to the local Galois groups at places dividing ℓ are crystalline of weights $0, 1, \dots, n-1$.

(4) $\exists$ a finite place v where ρ is a generalized special representation and $q_v^i \equiv 1$ mod ℓ $\forall i \leq n$

(5) $\mathrm{Im}\bar{\rho}$ is "big enough".

(6) $\bar{\rho}$ is irreducible and associated to an automorphic representation of generalized Steinberg type at v and with trivial infinitesimal character at ∞.

Then ρ is automorphic of the same type.