THE SATO-TATE CONJECTURE: ANALYTIC ARGUMENTS

Introduction

An elliptic curve is the set E of solutions of a cubic curve in two variables, for example

$$E: \ y^2 + y = x^3 + x,$$

I will generally consider elliptic curves with rational coefficients, which after a change of variables can be written

$$y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Q}$. These are not all distinct, and one can isolate two invariants: the *discriminant*

$$\Delta = \Delta_E - 16(4A^3 + 27B^2)$$

which is not really an invariant of E, but which has the following property: if $\Delta_E \neq 0$ then E is non-singular, which we always assume. There is also the j-invariant, which really depends on E and not just on the equation:

$$j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}$$

which determines E up to isomorphism over an algebraically closed field.

We may assume $A, B \in \mathbb{Z}$. It then makes sense to reduce the equation modulo a prime p and ask how many solutions E has modulo p:

$$N_p = N_p(E) = |E(\mathbb{F}_p)|.$$

Suppose for the moment we replace E by a line L, given by a *linear* equation

$$L: \ y = ax + b.$$

Then the number of solutions of L in the plane ${\mathbb{F}_p}^2$ obviously equals p, to which we add 1 for the point at infinity:

$$|L(\mathbb{F}_p)| = p + 1.$$

It turns out that $p + 1$ is in a natural sense the optimal number of points for a curve of any genus (or degree). Skipping over quadric curves, we define an integer $a_p = a_p(E)$, for each prime p, by

$$N_p(E) = p + 1 - a_p(E).$$

We only consider p for which E remains nonsingular modulo p, which is somewhat weaker than the condition that $\Delta_E \neq 0 \pmod{p}$. Such a p is called a *prime of good reduction*. One can consider the beginning of arithmetic algebraic geometry to be Hasse's discovery that

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

for any prime of good reduction.

In other words, $p+1$ is a good approximation to N_p to square-root order. This can be compared to the square-root good approximation to $\pi(x)$, the number of primes less than x:

$$\pi(x) = \int_2^x \frac{dx}{logx} + \text{ Error}(x)$$

where the Riemann hypothesis is the assertion that

$$\text{Error}(x) = O(x^{\frac{1}{2}})$$

and indeed Hasse's theorem was generalized by Weil to a version of the Riemann hypothesis valid for all curves over finite fields.

The next question is whether anything can be said about the behavior of the $a_p(E)$ as p varies. Is $a_p(E)$ more likely to be positive or negative? Is it more likely to cluster around 0 or around $\pm 2\sqrt{p}$? The rough answer is that it is as random as possible, but it is not immediately obvious how to make sense of this. We normalize all the a_p simultaneously to allow them to be compared:

$$a_p^{norm}(E) = \frac{1}{2\sqrt{p}} a_p(E) \in [-1, 1].$$

Thus there is a unique $\theta_p = \theta_p(E) \in [0, \pi]$ such that $a_p^{norm}(E) = cos(\theta_p)$. We ask about the distribution of the a_p^{norm} in $[-1, 1]$, or equivalently of the $\theta_p \in [0, \pi]$. Over forty years ago, Sato and Tate independently formulated the following conjecture:

Sato-Tate Conjecture. *Suppose E has no complex multiplication. Then the $a_p^{norm}(E)$ (resp. the θ_p) are equidistributed in $[-1, 1]$ (resp. $[0, \pi]$) with respect to the probability measure*

$$\frac{2}{\pi}\sqrt{1-t^2}dt \quad (\textit{ resp. } \frac{2}{\pi}\sin^2(\theta)d\theta \ ) \ .$$

Regarding the initial hypothesis most E have no complex multiplication. In particular, if $j(E) \in \mathbb{Q} - \mathbb{Z}$, then $j(E)$ has no complex multiplication. In this setting the conjecture has recently been proved:

Theorem (L. Clozel, MH, N. Shepherd-Barron, R. Taylor). *Suppose $j(E)$ is not an integer. Then the Sato-Tate Conjecture is valid for E.*

2. Equidistribution

I reformulate the problem in terms of Galois representations. Let F^+ be a totally real field. Those who prefer can assume $F^+ = \mathbb{Q}$.

Let E be an elliptic curve over F^+. To E we associate a 2-dimensional ℓ-adic representation for any prime ℓ: let $\rho_{E,\ell} : Gal(\overline{\mathbb{Q}}/F^+) \to GL(2, \mathbb{Q}_\ell)$ denote the

representation on $H^1(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$, i.e. the dual of the ℓ-adic Tate module. Assume $F^+ = \mathbb{Q}$ for the time being. Then this representation encodes all information about $|E(\mathbb{F}_p)|$ for almost all p, in the following sense. Remember that in the previous section we mentioned primes of good reduction. Suppose p is a prime of good reduction for E, and suppose also $p \neq \ell$. Then we can recover $a_p(E)$ from $\rho_{E,\ell}$. Let $Frob_p \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element for p. This is defined at the beginning of a course in algebraic number theory. We know that $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is generated by an element ϕ_p with the property that,

$$\forall x \in \overline{\mathbb{F}}_p, \phi_p(x) = x^p.$$

For technical reasons, we let $Frob_p = \phi_p^{-1}$. This is an element of $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, but if we extend the p-adic valuation on $\mathbb{Q}$ to a valuation v on $\overline{\mathbb{Q}}$, the decomposition subgroup $\Gamma_v \subset Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ fixing v is isomorphic to $Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Since E has good reduction at p and $p \neq \ell$, the representation $\rho_{E,\ell}$ is *unramified* at p, which means in particular that it is trivial on the inertia subgroup $I_v \subset \Gamma_v$, hence factors through $\Gamma_v/I_v \simeq Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Thus we can define $\rho_{E,\ell}(Frob_p)$. This depends on the choice of extension v of the p-adic valuation, but any two extensions are conjugate by an element of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular, the characteristic polynomial

$$P_{p,E}(T) = det(I - \rho_{E,\ell}(Frob_p)T) \in \mathbb{Q}_\ell[T]$$

depends only on p. However, it is well known that $P_{p,E}(T)$ has coefficients in $\mathbb{Q}$ and is independent of $\ell \neq p$. Thus the complex function $P_{p,E}(p^{-s})$ is well defined for all primes of good reduction. In fact, we know that

$$P_{p,E}(p^{-s}) = 1 - a_p(E)p^{-s} + p^{1-2s}.$$

Let

$$L_p(E,s) = P_{p,E}(p^{-\frac{1}{2}-s})^{-1} = 1 - a_p^{norm}(E)p^{-s} + p^{-2s}.$$

The complex L-function of E is

$$L(s,E) = \prod_p L_p(E,s),$$

where for primes of bad reduction one has another definition of $L_p(E,s)$. With our chosen normalization, this function converges absolutely for $Re(s) > 1$.

A general conjecture is that $L(s,E)$ extends to an entire function and satisfies a functional equation. This is known for $F^+ = \mathbb{Q}$ (Wiles, Taylor et al.) and meromorphic continuation is known for general totally real F^+ (Taylor). One proves that $L(s,E)$ is an entire function, for $F^+ = \mathbb{Q}$, by proving that it is the L-function of a modular form. For more general F^+, one wants to prove that it is the L-function of a cuspidal automorphic representation. This will be explained next week. In that case one says that E is *automorphic* over F^+.

Suppose it is known that E is automorphic: that there exists a cuspidal automorphic representation Π_E of $GL(2,F^+)$, whatever that means, such that (up to normalization) $L(s,\Pi_E) = L(s,E)$ as Euler products. For $n \geq 1$ let

$$\rho_{E,\ell}^n = Sym^{n-1}\rho_{E,\ell} : Gal(\overline{\mathbb{Q}}/F^+) \to GL(n,\mathbb{Q}_\ell).$$

For almost all p, the elliptic curve E has good reduction at p, which means that the local factor $\Pi_{E,p}$ is unramified. Let α_p, β_p be the Satake parameters of $\Pi_{E,p}$ with unitary normalization. I will return to this next week, but one can express these parameters explicitly in terms of the number of points modulo p:

$$a_p = p^{\frac{1}{2}}(\alpha_p + \beta_p),\ \alpha_p \cdot \beta_p = 1.$$

The theorem of Hasse stated before has a meaning in terms of Π_E.

Hasse, Eichler-Shimura ("Ramanujan conjecture").

$$|\alpha_p| = |\beta_p| = 1.$$

Up to permutation we have $\alpha_p = e^{i\theta_p}, \beta_p = e^{-i\theta_p}$, say, with $0 \leq \theta_p \leq \pi$. I restate the Sato-Tate Conjecture:

Sato-Tate Conjecture. *Assume E has no complex multiplication. Then the θ_p are equidistributed in $[0, \pi]$ with respect to the measure $dST(\theta) := \frac{2}{\pi} sin^2\theta\ d\theta$.*

The Sato-Tate measure is the push-forward of the Haar measure on $SU(2)$ to a measure on the set of conjugacy classes in $SU(2)$, which can be identified with $[0, \pi]$. The conjecture makes sense for the automorphic representation Π_E, without reference to elliptic curves, and also makes sense for modular forms of higher weight.

Let $X = [0, \pi]$. For any $f \in C(X)$ and $x > 0$ define

$$S(f, x) = \sum_{p \leq x} f(\theta_p).$$

The Sato-Tate conjecture asserts the following: for any continuous function $f \in C(X)$, we have

$$\lim_{x \to \infty} \frac{S(f,x)}{S(1,x)} = \lim_{x \to \infty} \frac{\sum_{p \leq x} f(\theta_p)}{\sum_{p \leq x} 1} = \int_X f(\theta) dST(\theta). \tag{E}$$

Now the diagonal matrix $diag(\alpha_p, \beta_p)$ belongs to $SU(2)$. There is an obvious map $\phi : SU(2) \to X$ identifying X with the space of conjugacy classes in $SU(2)$, and $dST(\theta)$ is the image with respect to ϕ of the Haar measure on $SU(2)$ with total mass 1. It suffices to prove (E) for f in an orthogonal basis of $L_2(X)$. Such an orthogonal basis is given by the characters χ_n of the irreducible representations Sym^n of $SU(2)$. For $f = \chi_0$, which is the trivial representation, (E) is obvious. For $f = \chi_n$ with $n > 0$, we have

$$\int_X \chi_n(\theta) dST(\theta) = \int_X \chi_n(\theta) \cdot 1 dST(\theta) =< \chi_n, \chi_0 >= 0$$

because the characters form an orthogonal basis.

In general

$$\chi_n(\theta_p) = \sum_{j=0}^{n} \alpha_p^j \beta_p^{n-j}.$$

which is why it is convenient to use the Satake parameters of $\Pi_{E,p}$. So we need to show

$$\lim_{x\to\infty}\sum_{p\leq x}\chi_n(\theta_p)=o(\pi(x)). \tag{2.1}$$

Now we use a standard argument from analytic number theory. Let

$$L^*(s,E,Sym^n)=L^*(s,\rho_E^{n+1}),$$

normalized to be absolutely convergent for $Re(s)>1$. In other words,

$$L^*(s,E,Sym^n)=\prod_p L_p^*(s,\rho_E^{n+1})$$

where for $p\notin S$,

$$L_p^*(s,\rho_E^{n+1})=\prod_{j=0}^{n}(1-\alpha_p^j\beta_p^{n-j}p^{-s})^{-1}.$$

Comparing this with (1.1), we find

$$\begin{aligned}\frac{d}{ds}log(L^*(s,E,Sym^n))&=-\sum_p\sum_m\frac{\chi_n(\theta_p^m)log\ p}{p^{ms}}\\&=-\sum_p\frac{\chi_n(\theta_p)log\ p}{p^s}+\varphi(s)\end{aligned} \tag{2.2}$$

where $\varphi(s)$ is holomorphic for $Re(s)>\frac{1}{2}$ and the first equality is only up to a finite set of bad factors (irrelevant for the second equality).

With regard to the Sato-Tate conjecture, the main result of the articles [CHT], [HST], and [T] is the following theorem

Theorem 2.3. *For all $n>0$, the function $L^*(s,E,Sym^n)$ is meromorphic, and it is holomorphic on $Re(s)>1$ and continuous and non-vanishing up to $Re(s)\geq 1$.*

Thus for each n,

$$\frac{d}{ds}log(L^*(s,E,Sym^n))=L^{*,\prime}(s,E,Sym^n)/L^*(s,E,Sym^n)$$

is a quotient of meromorphic functions that are holomorphic and non-vanishing for $Re(s)\geq 1$.

Corollary. $\sum_p\frac{\chi_n(\theta_p)logp}{p^s}$ *has no pole for $Re(s)\geq 1$.*

The Wiener-Ikehara tauberian theorem states that if $D(s)=\sum_n\frac{b_n}{n^s}$ is a Dirichlet series convergent for $Re(s)>1$ and non-singular except for a possible first-order pole at $s=1$, with residue α, then

$$\sum_{n<x}b_n=\alpha\cdot x+o(x).$$

For the prime number theorem, this is applied with $b_n = p \cdot log\ p$ if $n = p$ is prime, $b_n = 0$ otherwise, to yield

$$\sum_{p<x} log\ p = \cdot x + o(x).$$

Applying Abel summation, as explained below, this gives the usual estimate $\pi(x) \sim x/log\ x$. In the present situation

$$\sum_{p\leq x} \chi_n(\theta_p) log\ p = o(x).$$

Applying Abel summation to get rid of the logs, we find

$$S(\chi_n, x) = \sum_{p\leq x} \chi_n(\theta_p) = o(x/logx)$$

and since

$$S(1, x) = S(\chi_0, x) = \sum_{p\leq x} 1 = x/logx + o(x/logx)$$

by the prime number theorem the ratio

$$\lim_{x\to\infty} \frac{S(\chi_n, x)}{S(1, x)} = 0$$

for all $n > 1$. This yields the estimate (2.1), and hence equidistribution.

Review of the Abel summation trick.

Proposition. *Let b_n, $n = 2, 3, \ldots$ be complex numbers such that*

$$\Psi(x) = \sum_{n\leq x} b_n = \alpha \cdot x + o(x).$$

Then

$$\Pi(x) = \sum_{n\leq x} \frac{n}{log\ n} = \alpha \cdot x/logx + o(x/logx).$$

Proof. We may as well assume $x = N$ is an integer. Since $b_n = \Psi(n) - \Psi(n-1)$, where we set $\Psi(1) =$, we have

$$\begin{aligned}\Pi(N) &= \sum_{n\leq N} \frac{\Psi(n) - \Psi(n-1)}{log\ n} = \sum_{n=2}^{N} \frac{\Psi(n)}{log\ n} - \sum_{n=1}^{N-1} \frac{\Psi(n)}{log\ (n+1)} \\ &= \Psi(N)/log(N) + \sum_{n=2}^{N-1} \Psi(n) \left(\frac{1}{log\ (n)} - \frac{1}{log\ (n+1)} \right)\end{aligned}$$

So it suffices to show that the sum in the second part is $o(\frac{N}{Log\ N})$. Since $\Psi(x) = O(x)$, by hypothesis, we may replace $\Psi(n)$ by Cn for some constant C. Moreover,

$$\frac{1}{log\ (n)} - \frac{1}{log\ (n+1)} = \frac{log(1+\frac{1}{n})}{log(n)log(n+1)} < \frac{1/n}{log(n)^2}.$$

Thus each term in the sum is bounded above by $\frac{C}{log(n)^2}$, and it suffices to show

$$\sum_{n=2}^{N} \frac{1}{log(n)^2} = o(N/log\ N).$$

We break this up as sum for

$$\sum_{2<n<\sqrt{N}} \frac{1}{log(n)^2} + \sum_{\sqrt{N}<n<N} \frac{1}{log(n)^2},$$

where the first term is bounded above by $\sqrt{N}/(log(2)^2)$ and the second by $\frac{N}{log(\sqrt{N})^2} = \frac{4N}{log(N)^2}$. Each term is clearly $o(N/log(N))$, so we are done.

3. Artin L-functions and Brauer's theorem

It is expected that $L(s, \rho_E^n)$ is the L-function of a cuspidal automorphic representation of $GL(n, \mathbb{Q})$ for all n. I explain what this means in the next lecture. Whatever it means, it would imply that $L(s, \rho_E^n)$ is *entire* as well as non-vanishing for $Re(s) \geq 1$. We cannot prove this, but we can prove a weaker result that implies Theorem 2.3. Here is a version of what we prove:

Theorem 3.1. *For every $n > 1$, there is a totally real Galois extension $F_n/\mathbb{Q}$ such that the L-function of $\rho_{E,F_n}^n = \rho_E^n\ |_{Gal(\overline{\mathbb{Q}}/F_n)}$ is the L-function of a cuspidal automorphic representation of $GL(n, F_n)$.*

Remark. Theorem 3.1 is not yet proved as such. In [HST] we only construct automorphic representations for *even* n. An argument using Rankin-Selberg L-functions suffices to prove that the $L(s, \rho_E^n)$ for odd n still enjoy the expected analytic properties up to $Re(s) = 1$, which is sufficient to imply Theorem 2.3. In a more recent paper I have shown how to obtain automorphic representations for odd n as well, assuming completion of ongoing work on the stable trace formula. So I will not include the Rankin-Selberg argument in the notes, though it may be mentioned during the course.

Theorem 3.1 comes with additional properties that will be mentioned in the subsequent argument. To motivate this theorem, and to explain what it has to do with Theorem 2.3, I will step back and recall the theory of Artin L-functions, which are L-functions of complex representations of $Gal(\overline{\mathbb{Q}}/F)$, for any number field F.

Let

$$\rho : Gal(\overline{\mathbb{Q}}/F) \to GL(V) \simeq GL(n, \mathbb{C})$$

be a continuous representation on an n-dimensional complex vector space V. Thus the image of ρ is necessarily finite, hence factors through $Gal(E/F)$ for some finite extension E of F; in particular ρ is unramified outside the finite set of primes of F that ramify in E. For any prime ideal v of F that is unramified in E, we can define a (geometric) Frobenius element $Frob_v \in Gal(E/F)$ as before. Again, $Frob_v$ is only well defined up to conjugacy, but

$$L_v(s, \rho) = det(I - \rho(Frob_v)Nv^{-s})^{-1}$$

depends only on v. If v is ramified, we let $I_v \subset \Gamma_v$ be the intertia group. Then Γ_v/I_v acts on V^{I_v}, and we define

$$L_v(s,\rho) = det(I - \rho(Frob_v, V^{I_v})Nv^{-s})^{-1};$$

$$L(s,\rho) = \prod_v L_v(s,\rho).$$

This product converges absolutely for $Re(s) > 1$. Perhaps the most important conjecture in algebraic number theory is

Artin Conjecture. *If ρ is irreducible and non-trivial, then $L(s,\rho)$ is entire and satisfies a certain (explicit) functional equation.*

One has known for some time that

Theorem. *In any case, $L(s,\rho)$ is meromorphic, satisfies the expected functional equation, and is continous and non-vanishing for $Re(s) \geq 1$.*

This is essentially a consequence of Brauer's theorem on characters. I need to explain a few facts about Galois representations and their L-functions.

Semisimplification. *The representations ρ and ρ' have the same Jordan-Hölder constituents, if and only if $Tr(\rho) = Tr(\rho')$, and the latter is true if and only if $L(s,\rho) = L(s,\rho')$ as Euler products.*

In particular, we can always replace ρ by its semisimplification (the direct sum of its Jordan-Hölder constituents.

Additivity. $L(s, \rho \oplus \rho') = L(s,\rho)L(s,\rho')$.

Inductivity. *Let F'/F be a finite extension, ρ' a continuous representation of $Gal(\overline{\mathbb{Q}}/F')$, $\rho = Ind_{F'/F}\rho'$ the induced representation of $Gal(\overline{\mathbb{Q}}/F)$. Then*

$$L(s,\rho') = L(s,\rho).$$

If ρ is the trivial representation of $Gal(\overline{\mathbb{Q}}/F)$, then $L(s,\rho) = \zeta_F(s)$ is the Dedekind ζ-function of F. More generally, if ρ is one-dimensional then it factors through $Gal(\overline{\mathbb{Q}}/F)^a b$.

Abelian L-functions. *Suppose* $\dim \rho = 1$ *and ρ is non-trivial. Then $L(s,\rho)$ is entire and satisfies the expected functional equation. Moreover, $L(s,\rho)$ is continuous and non-vanishing for $Re(s) \geq 1$.*

This is due to Hecke (Dirichlet when $F = \mathbb{Q}$) and follows from class field theory.

In particular, in the inductivity situation, if ρ' is abelian and non-trivial. then $L(s, Ind_{F'/F}\rho')$ satisfies the Artin conjecture.

Brauer's Theorem. *Let H be a finite group and $\rho : H \to GL(n,\mathbb{C})$ be any finite-dimensional representation. Then there are solvable subgroups $H_i \subset H$, characters $\chi_i : H_i \to \mathbb{C}^\times$, and integers a_i such that*

$$\rho \equiv \oplus_i a_i Ind_{H_i}^H \chi_i.$$

The decomposition above is not unique, and the integers a_i are certainly not assumed positive. Applied to $\rho : H = Gal(E/F) \to GL(n, \mathbb{C})$, this and additivity implies

$$L(s, \rho) = \prod_i L(s, Ind_{F_i/F} \chi_i)^{a_i},$$

where F_i is the fixed field of H_i and χ_i is the character of $H_i = Gal(E/F_i)$; and again this is

$$\prod_i L(s, \chi_i)^{a_i}.$$

Since each of the $L(s, \chi_i)$ is entire and invertible for $Re(s) \geq 1$, the product is meromorphic and invertible for $Re(s) \geq 1$. The functional equation also follows from this product expression. We have not yet used that the H_i are solvable.

Now we return to the situation of an elliptic curve $E/\mathbb{Q}$ without complex multiplication, and assume $F_n/\mathbb{Q}$ is a finite Galois extension. Let 1 be the trivial representation of $H = Gal(F_n/\mathbb{Q})$. Brauer's theorem applies to 1:

$$1 = \oplus a_i Ind_{H_i}^H \chi_i.$$

Let L_i be the fixed field of H_i in F_n, ρ^n_{E,L_i} the restriction of ρ^n_E to $Gal(\overline{\mathbb{Q}}/L_i)$.

Now in general, if ρ is a representation of H, ρ' a representation of the subgroup $H' \subset H$, then it is easy to see that

$$(Ind_{H'}^H \rho') \otimes \rho = Ind_{H'}^H (\rho' \otimes Res_{H'}^H \rho),$$

where $Res_{H'}^H \rho$ is the restriction of ρ to H. It follows that

$$\rho^n_E = \oplus a_i (Ind_{H_i}^H \chi_i) \otimes \rho^n_E = \oplus a_i Ind_{H_i}^H \chi_i \otimes \rho^n_E)$$

which implies

$$L(s, \rho^n_E) = \prod L(s, \rho^n_{E,L_i} \otimes \chi_i)^{a_i}.$$

The following fact follows from a strengthened version of Arthur-Clozel base-change for certain kinds of automorphic representations of totally real fields.

Theorem 3.2. *Suppose F_n is totally real and Galois over $\mathbb{Q}$, and ρ^n_{E,F_n} is automorphic (of a certain type to be made precise below). Then for any solvable subgroup $H_i \subset H$ with fixed field L_i, and any character χ_i of $Gal(\overline{\mathbb{Q}}/L_i)$, $L(s, \rho^n_{E,L_i} \otimes \chi_i)$ is entire, and is invertible for $Re(s) \geq 1$.*

Thus Theorems 3.1 and (the much older) 3.2 suffice to imply Theorem 2.3, and hence the Sato-Tate conjecture.

4. Rate of convergence to the Sato-Tate distribution (following Mazur)

Return to the elliptic curve E with which we started. The Sato-Tate conjecture concerns the distribution of the error term $a_p(E)$ in the estimate of the number of points on E modulo p. But the determination of the behavior of this error term leads to a question about errors at the next level of approximation: how good an approximation is the Sato-Tate distribution to the real distribution of errors?

In other words, the theorem to be discussed in this course asserts that, for any continuous function on $[-1,1]$,

$$\lim_{C\to\infty}[\frac{\sum_{p\leq C} f(cos(\theta_p))}{\pi(C)} - \frac{2}{\pi}\int_{-1}^{1} f(t)\sqrt{1-t^2}dt] = 0.$$

This is just a reformulation of (E) from §2, with a change of variable (for a change). Here $\pi(c)$ is the number of primes $\leq C$. In an article [M] to be published soon in the Bulletin of the AMS, Mazur asks how the expression in the brackets depends on x, and makes the following conjecture:

Conjecture 4.1. *Let $f(t)$ be a real-valued function on $[-1,1]$ of bounded variation. Put*

$$\Delta_f(C) = |\frac{\sum_{p\leq C} f(cos(\theta_p))}{\pi(C)} - \frac{2}{\pi}\int_{-1}^{1} f(t)\sqrt{1-t^2}dt|.$$

Then for every $\epsilon > 0$ we have

$$Delta_f(C) < C^{-\frac{1}{2}+\epsilon}$$

for $C >> 0$.

He shows this is a consequence of a stronger conjecture due to Akiyama and Tanigawa [AT].

Conjecture 4.2. *Consider the class Φ_α of characteristic functions of intervals $[-1,\alpha] \subset [-1,1]$, and define*

$$D(C) = Max_\alpha \Delta(\Phi_\alpha)(C).$$

Then for every $\epsilon > 0$ we have

$$D(C) < C^{-\frac{1}{2}+\epsilon}$$

for $C >> 0$.

Numerical evidence presented in [M] shows that Conjecture 4.1 is, if anything, conservative, though it is hard on statistical grounds to justify a better bound than a square-root error (real-life statistical error in random sampling).

The deduction of Conjecture 4.1 from 4.2 uses arguments already in [AT]. Conjecture 4.1 has the following very interesting consequence, pointed out in [AT]

Proposition 4.3 (in [AT] in the case $n = 1$, the general proof is identical). *Let $n > 0$ be a positive integer. Suppose $L^*(s, E, Sym^n)$ extends to an entire function and satisfies the expected functional equation. Assume Conjecture 4.1 holds for the polynomial function χ_n. Then $L^*(s, E, Sym^n)$ satisfies the generalized Riemann hypothesis: i.e., all its zeroes lie on the line $Re(s) = \frac{1}{2}$.*

The expected functional equation is established in [CHT], [HST], [T], but we only prove meromorphic continuation to the left of $Re(s) = 1$. Note that the case $n = 0$ is excluded, Conjecture 4.1 doesn't seem to imply the original Riemann hypothesis.

Proof. Define a polynomial s_n on $[-1,1]$ such that $s_n(cos(\theta)) = \chi_n(\theta)$. Our hypothesis is that

$$\Delta_{\chi_n}(C) = |\frac{\sum_{p\leq C} s_n(cos(\theta_p))}{\pi(C)} - \frac{2}{\pi}\int_{-1}^{1} f(t)\sqrt{1-t^2}dt|.$$

Then for every $\epsilon > 0$ we have

$$Delta_f(C) < C^{-\frac{1}{2}+\epsilon}$$

for $C >> 0$. On the other hand, the prime number theorem asserts that $\pi(C) \geq C^{1-\delta}$ for any positive δ for $C >> 0$. Moreover, the integral vanishes because $n \neq 0$. So we obtain

$$|\frac{\sum_{p\leq C} s_n(cos(\theta_p))}{\pi(C)}| < C^{\frac{1}{2}+\epsilon} \tag{4.4}$$

for $C >> 0$.

Now formula (2.2) is roughly equivalent (after some changes of variables) to

$$log(L^*(s,E,Sym^n) = \sum_p s_n(\cos(\theta_p))p^{-s} + \psi(s) \tag{4.5}$$

where $\psi(s)$ is holomorphic for $Re(s) > \frac{1}{2}$. Then GRH for $L^*(s,E,Sym^n)$ follows if we can show that $log(L^*(s,E,Sym^n)$ has no poles to the left of the axis of symmetry, i.e. that the first term on the right hand side of (4.5) is holomorphic for $Re(s) > \frac{1}{2}$. So the Proposition follows from (4.4) and Lemma 4.6 below.

Lemma 4.6. *If for any $\epsilon > 0$, $\sum_p s_n(\cos(\theta_p))$ is $O(C^{\frac{1}{2}+\epsilon})$, then $\sum_p s_n(\cos(\theta_p))p^{-s}$ converges to yield a holomorphic function on $Re(s) > \frac{1}{2}$.*

Proof. For $k = 1, 2, \ldots$ set $a_k = s_n(\cos\theta_p)$ if k is prime, 0 otherwise. Thus our Dirichlet series is $\sum_k a_k k^{-s}$ and for any $\epsilon > 0$ we have $\sum_{k\leq N} a_k = O(N^{\frac{1}{2}+\epsilon})$. Partial summation as in §2 gives

$$\sum_{k<N} a_k k^{-s} = \sum_{k<N} a_k N^{-s} - \sum_{n<N}(\sum_{k<n} a_k)[(n+1)^{-s} - n^{-s}].$$

The first term on the right hand side is thus $O(N^{\frac{1}{2}+\epsilon-s})$ which, if $Re(s) > \frac{1}{2}$ is bounded independent of N for appropriate ϵ. But

$$[(n+1)^{-s} - n^{-s}] \leq n^{-s-1}$$

so the second term is bounded by a constant times

$$\sum_n n^{\frac{1}{2}+\epsilon-s-1} = \zeta(s + \frac{1}{2} - \epsilon).$$

And this is also bounded independently of N if $Re(s) > \frac{1}{2} - \epsilon$.

REFERENCES

[AT] S. Akiyama and Y. Tanigawa, Calculation of values of L-functions associated to elliptic curves, *Math. Computation*, **68** (1999) 1201-1231.

[CHT] L. Clozel, MH, R. Taylor: *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations*

[HST] MH, N. Shepherd-Barron, R. Taylor: *A family of Calabi-Yau varieties and potential automorphy*

[M] B. Mazur, Finding meaning in error terms (in preparation).

[T] R. Taylor: *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations, II*