ST and ST

Joan-C. Lario

29 Gener 2013

Introducció

$E/\mathbb{Q}\colon y^2 = x^3 + ax + b, \quad$ amb $a,\ b \in \mathbb{Z}$

$$\Delta = -16(4a^3 + 27b^2) \neq 0$$

Per a cada primer p amb $(p, \Delta) = 1$, considerem

$$\widetilde{E}/\mathbb{F}_p\colon y^2 \equiv x^3 + ax + b \pmod{p}$$

Definim l'error

$$\#\widetilde{E}(\mathbb{F}_p) = \#\mathbb{P}^1(\mathbb{F}_p) - a_p$$

Teorema (Hasse 1933, néé conjectura Artin 1924)

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

Distribució dels errors

$$p \mapsto \frac{a_p}{\sqrt{p}} \in [-2,2] \qquad p \mapsto \theta_p \in [0,\pi]$$

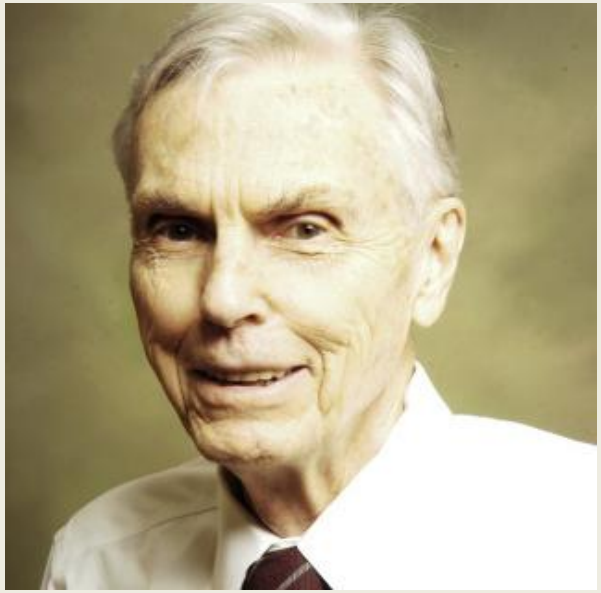
$$\frac{a_p}{\sqrt{p}} = 2\cos\theta_p$$

1962: Mikio Sato (Nagashima, Kanji Namba) a la Tokyo University of Education amb un Hitachi HIPAC 103 fan càlculs.

1963: John Tate ("Algebraic cycles and poles of zeta functions", Proc. Purdue University), a la pàgina 107 diu:

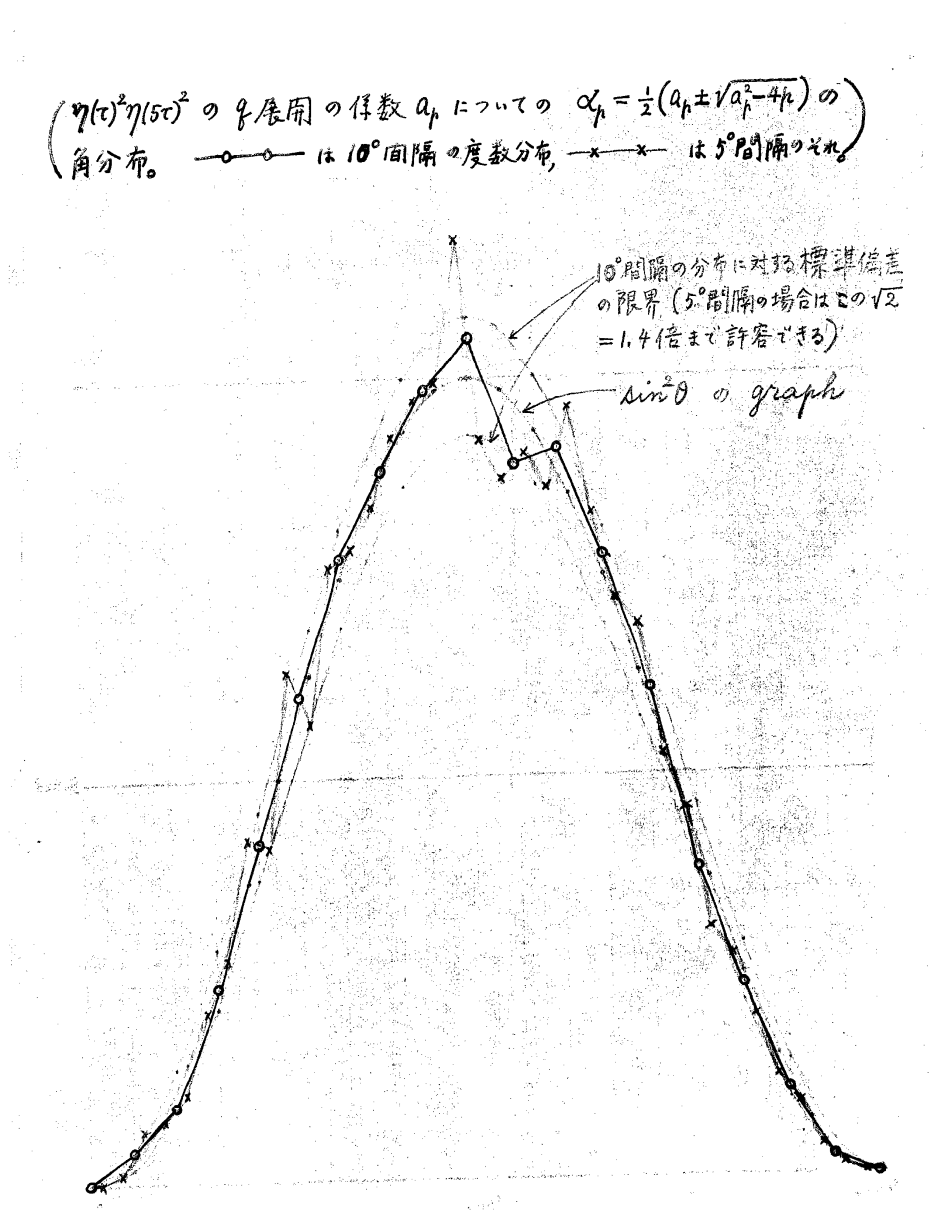
"I understand that M. Sato has found this $\sin^2$ distribution law experimentally with machine computations".

Protagonistes (Sato-Tate, Serre-Taylor, ...)

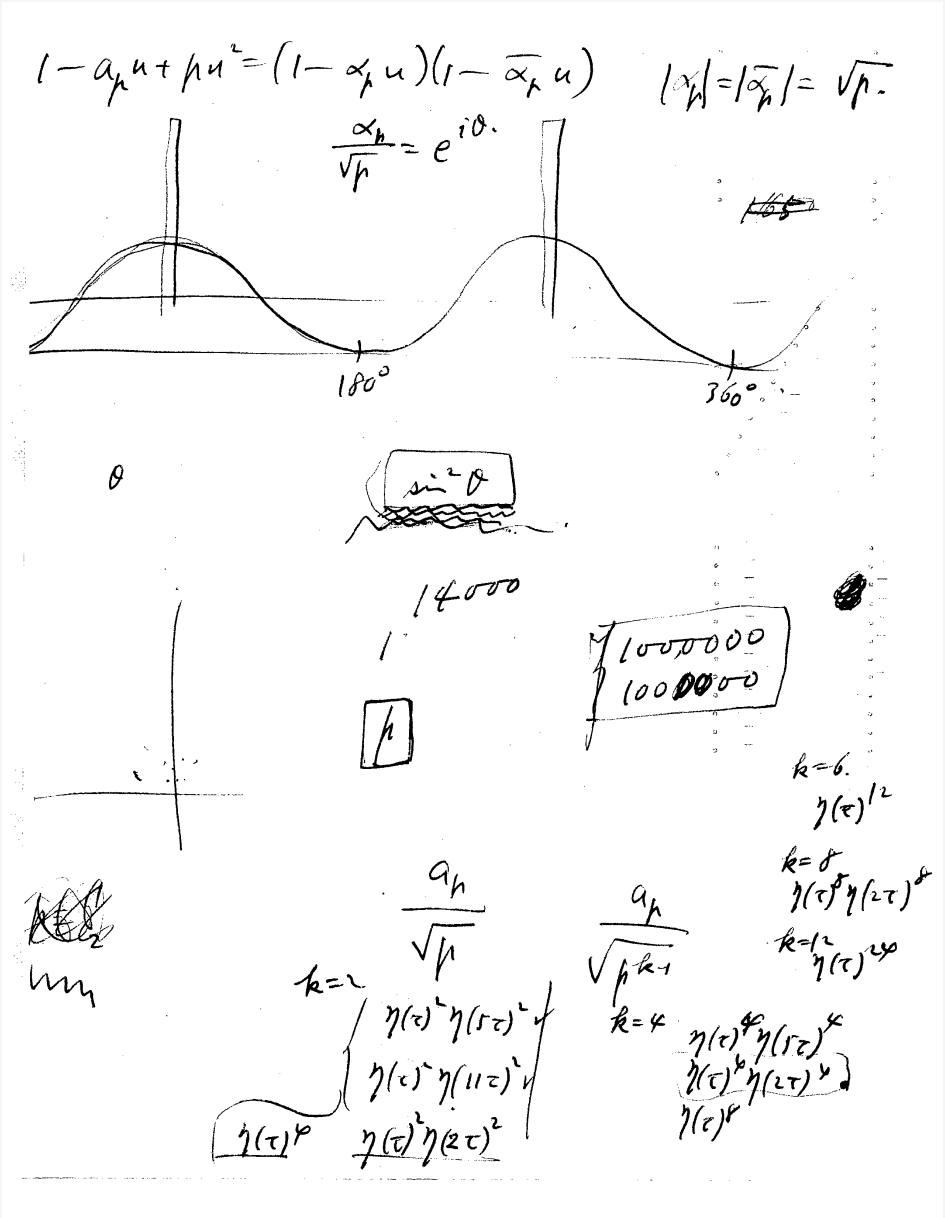



Hitachi HIPAC103 (1962)

13 Abril 1963, des d'Osaka



Abril 1963, tornant d'Osaka



Sato-Tate: corbes el·líptiques

Retornem a les corbes el·líptiques (sense CM):

$$a_p/\sqrt{p} = 2\cos\theta_p\,, \quad 0 \le \theta_p \le \pi\,.$$

Conjectura (Sato-Tate)

Donat un interval $[\alpha,\beta] \subseteq [0,\pi]$, *es té*

$$\lim_{x\to\infty} \frac{\#\{p \le x\colon \theta_p \in [\alpha,\beta]\}}{\#\{p \le x\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta\, d\theta$$

Sato-Tate: corbes el·líptiques

Retornem a les corbes el·líptiques (sense CM):

$$a_p/\sqrt{p} = 2\cos\theta_p\,, \quad 0 \le \theta_p \le \pi\,.$$

Conjectura (Sato-Tate)

Donat un interval $[\alpha,\beta] \subseteq [0,\pi]$, *es té*

$$\lim_{x\to\infty} \frac{\#\{p \le x\colon \theta_p \in [\alpha,\beta]\}}{\#\{p \le x\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta\, d\theta$$

$$= \frac{\beta-\alpha}{\pi} - \frac{1}{2\pi}(\sin 2\beta - \sin 2\alpha)\,.$$

Alternatives: Sato-Tate per a formes modulars

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

$$= q - 24q^2 + 252q^3 - 1472q^4 + \cdots + \tau(n)q^n + \ldots$$

Teorema (Deligne 1970, conjectura Ramanujan 1917)

$$|\tau(p)| \leq 2\,p^{11/2}$$

p	2	3	5	...	997
$\tau(p)\,p^{-11/2}$	-0.53033	0.598734	0.691213	...	0.688016

$$\tau(p) = 2p^{11/2}\cos\theta_p\,, \quad \theta_p \rightsquigarrow \frac{2}{\pi}\sin^2(\theta)$$

Alternatives: curses de convergència

$$\pi(x;N,a) = \#\{p \text{ primer} : p \leq x, p \equiv a \bmod N\}$$

$$\pi(x;4,1) \sim \pi(x;4,3) \sim \frac{1}{2}\frac{x}{\log x}$$

Diríem: $\pi(x) = 50\%\,\pi(x;4,1) + 50\%\,\pi(x;4,3)$

Alternatives: curses de convergència

$$\pi(x;N,a) = \#\{p \text{ primer} : p \leq x, p \equiv a \bmod N\}$$

$$\pi(x;4,1) \sim \pi(x;4,3) \sim \frac{1}{2}\frac{x}{\log x}$$

Diríem: $\pi(x) = 50\%\,\pi(x;4,1) + 50\%\,\pi(x;4,3)$

Però noooooooo (Txebyshev, 1853):

$$\pi(x;4,3) > \pi(x;4,1)$$

per a tot $x < 26833$ excepte $x = 5,\ 17,\ 41,\ 461$.

Tate s'inspira en Dirichlet

Euler: $\sum_p \frac{1}{p}$ divergeix. Dirichlet: $\sum_{p \equiv a \bmod N} \frac{1}{p}$ divergeix.

Tate s'inspira en Dirichlet

Euler: $\sum_p \frac{1}{p}$ divergeix. Dirichlet: $\sum_{p\equiv a \bmod N} \frac{1}{p}$ divergeix.

$G = (\mathbb{Z}/N\mathbb{Z})^*$, caràcters χ, funcions $L(\chi, s) = \prod_p (1 - \chi(p)/p^s)^{-1}$.

$$\sum_{p\equiv a \bmod N} \frac{1}{p^s} = \sum_\chi \frac{\chi(a^{-1})}{\varphi(N)} \sum_p \frac{\chi(p)}{p^s} = \sum_\chi \frac{\chi(a^{-1})}{\varphi(N)} \log L(\chi, s) + O(1) =$$

$$= \frac{1}{\varphi(N)} \left(\log L(\chi_0, s) + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \log L(\chi, s) \right) + O(1)$$

Punts clau:

Quan $\chi \neq \chi_0$, les funcions $L(\chi, s)$ s'estenen holomorfament a $\Re(s) \geq 1$.
A més, $L(\chi, 1) \neq 0$.

Estratègia de Serre-Tate

Sigui X espai topològic compacte, μ_* mesura de Radon (forma lineal contínua en $C(X)$). Una successió $\{x_n\}_{n\geq 1}$ de punts de X està μ_*-equidistribuïda si per a cada funció $f \in C(X)$ es té

$$\mu_*(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i)\,.$$

Cas important: G grup compacte, $X = G/\sim$ classes de conjugació, μ_* la imatge directa de la mesura de Haar normalitzada de G.

Proposició

Una successió $\{x_n\}_{n\geq 1}$ de X està μ_*-equidistribuïda si i només si per a cada caràcter irreductible χ de G, $\chi \neq 1$, es té

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = 0.$$

Mesura de Haar

G grup topològic localment compacte.
$\mathscr{B}(G)$ àlgebra de Borel $=$ σ-àlgebra dels subconjunts compactes de G.
$\mu\colon \mathscr{B}(G) \to \mathbb{R}^+ \cup \{\infty\}$ mesura invariant per translació

$$\mu(S) = \mu(gS) \text{ per a tot } g \in G.$$

Existència i unicitat (llevat d'homotecia): Haar 1933, André Weil 1940, Cartan 1940, Alfsen 1963.

G	μ
$(\mathbb{R}^n, +)$	Lebesgue
$(\mathbb{R}_{>0}, \cdot)$	$\mu(S) = \int_S \frac{1}{t}\, dt$
$\mathrm{GL}(n, \mathbb{R})$	$\mu(S) = \int_S \frac{dX}{\lvert \det X \rvert^n}$

Unimodular: left Haar $=$ right Haar.
Compacte implica unimodular.

Sigui G grup compacte, $X = G/\sim$ classes de conjugació. Triem $\{x_p\}_{p\in\Sigma}$. Per a cada representació irreductible ρ, considerem

$$L(\rho, s) = \prod_{p\in\Sigma} \det\left(1 - \rho(x_p)p^{-s}\right)^{-1} \quad (\Re(s) > 1).$$

Teorema

Si per a tota ρ no-trivial, la funció $L(\rho, s)$ s'estén a una funció holomorfa en $\Re(s) \geq 1$ sense zeros en $\Re(s) = 1$, aleshores $\{x_p\}_{p\in\Sigma}$ està μ_*-equidistribuïda.

Si χ és el caràcter de ρ, cal comprovar

$$\lim_{N\to\infty} \frac{1}{\#\{p \leq N\}} \sum_{p\leq N} \chi(x_p) = 0 = \mu(\chi).$$

Prova del teorema (Hadamard, de la Vallée Poussin)

Posem $L = L(\rho, s) = \prod_p \prod_{i=1}^{n} \frac{1}{1 - p^{-s}\lambda_{i,p}}$ i la derivada logarítmica

$$\begin{aligned} -\frac{L'}{L} &= \sum_p \sum_i \frac{p^{-s}\log p}{1 - p^{-s}\lambda_{i,p}} \\ &= \sum_p \sum_i \sum_{m\geq 1} p^{-ms}\lambda_{i,p}^m \log p \\ &= \sum_p \sum_{m\geq 1} p^{-ms}\chi(x_p^m)\log p \\ &= \sum_p p^{-s}\chi(x_p)\log p + \text{ funció holomorfa en } \Re s > 1 \end{aligned}$$

(Wiener-Ikehara): implica $\sum_{p\leq N} \chi(x_p)\log p = o(N)$.

(sumació d'Abel): implica $\sum_{p\leq N} \chi(x_p) = o\left(\frac{N}{\log N}\right)$.

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

Un teorema tauberià

Teorema (Wiener-Ikehara)

Si la sèrie de Dirichlet $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ *satisfà:*

(i) $a(n) \geq 0$;

(ii) *convergeix en* $\Re s > b$;

(iii) *té un pol simple en* $s = b$ *amb residuo* c,

aleshores

$$\sum_{n \leq x} a(n) \sim \frac{c}{b} x^b .$$

Cas el·líptic sense CM

$G = \mathrm{SU}(2) = \{A \in \mathscr{M}_2(\mathbb{C}) : \overline{A} = A^{-t} \text{ i } \det A = 1\}$.

$X =$ classes de conjugació de $G = \{\begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix}^{\sim}\}$.

$$\begin{array}{ccc} [0,\pi] & \longrightarrow & X \\ \theta & \longrightarrow & \begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix}^{\sim} \\ \arccos \frac{\mathrm{tr}\, g}{2} & \longleftarrow & g \end{array}$$

Les representacions irreductibles de G són la standard 2-dimensional i les seves potències potències simètriques. De manera que cal bregar amb les funcions L següents, per $m \geq 1$:

$$L_m(s) := L(\mathrm{Sym}^m E, s) = \prod_p \prod_{i=0}^{m} (1 - \beta_p^{-m+2i} p^{-s})^{-1}$$

on $\beta_p = e^{i\theta_p}$ (recordem $a_p/\sqrt{p} = 2\cos\theta_p$).

El programa de Langlands

Conjectura (Langlands)

Per cada $m \geq 1$, la representació $\rho_m = \mathrm{Sym}^m E$ correspon a una representació automorfa cuspidal π_m de $\mathrm{GL}_{m+1}(\mathbb{A})$.

En tal cas, se sap que $L(\pi_m, s) = L(\rho_m, s)$ és bona en $s = 1 \Rightarrow$ Conjectura de Sato-Tate certa per a la corba el·líptica E sense CM.

El programa de Langlands

Conjectura (Langlands)

Per cada $m \geq 1$, *la representació* $\rho_m = \mathrm{Sym}^m E$ *correspon a una representació automorfa cuspidal* π_m *de* $\mathrm{GL}_{m+1}(\mathbb{A})$.

En tal cas, se sap que $L(\pi_m, s) = L(\rho_m, s)$ és bona en $s = 1 \Rightarrow$ Conjectura de Sato-Tate certa per a la corba el·líptica E sense CM.

(Wiles-Taylor-Wiles): El cas $m = 1$ és ok! $L(\rho_1, s) = L(f, s + \frac{1}{2})$

El programa de Langlands

Conjectura (Langlands)

Per cada $m \geq 1$, *la representació* $\rho_m = \mathrm{Sym}^m E$ *correspon a una representació automorfa cuspidal* π_m *de* $\mathrm{GL}_{m+1}(\mathbb{A})$.

En tal cas, se sap que $L(\pi_m, s) = L(\rho_m, s)$ és bona en $s = 1 \Rightarrow$ Conjectura de Sato-Tate certa per a la corba el·líptica E sense CM.

(Wiles-Taylor-Wiles): El cas $m = 1$ és ok! $L(\rho_1, s) = L(f, s + \frac{1}{2})$

(Taylor): Per $m \geq 2$ tenim automorfia potencial.

Teorema de la automorfia potencial

Sigui K un cos de nombres totalment real.

Sigui E/K una corba el·líptica sense CM.

Teorema (Taylor)

Sigui $\rho_m = \mathrm{Sym}^m(E)$ amb $m \geq 1$ senar. Existeix una extensió L/K normal i totalment real tal que $\rho_m|\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ és automorfa. Es pot triar L de manera que funcioni simultàniament per a qualsevol conjunt de nombres senars m.

- Anem a veure com d'aquest TAP s'arriba a Sato-Tate.

Prova de Taylor et al. (sketch)

- Taylor (2008), "Automorphy for some l-adic lifts of automorphic mod l Galois representations. II", Publ. Math. Inst. Hautes Études Sci. 108: 183–239.
- Clozel; Harris; Taylor (2008), "Automorphy for some l-adic lifts of automorphic mod l Galois representations", Publ. Math. Inst. Hautes Études Sci. 108: 1-181.
- Harris; Shepherd-Barron; Taylor (2009), A family of Calabi-Yau varieties and potential automorphy, preprint.
- Barnet-Lamb; Geraghty; Harris; Taylor (2009), A family of Calabi-Yau varieties and potential automorphy. II, preprint.

Step 1

Siguin E/K com abans i $m \geq 1$ senar. Pel teorema de automorfia potencial (TAP), existeix L/K tal que la restricció $\rho_m|L$ és automorfa.

Teorema (Harris, Shepherd-Barron, Taylor)

Per a cada subextensió $K \subseteq F \subseteq L$ tal que L/F sigui resoluble, aleshores la restricció $\rho_m|F$ és automorfa.

Aplicar la teoria del *base change* de Arthur-Clozel per a extensions cícliques de manera inductiva:

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = L$$

amb F_{i+1}/F_i cíclica per $0 \leq i \leq m-1$.

Step 2

Posem $G = \mathrm{Gal}(L/K)$. Pel teorema d'inducció de Brauer,

$$1_G = \sum_i a_i \operatorname{Ind}_{H_i}^G \psi_i$$

on a_i són enters i ψ_i els caràcters 1-dimensionals dels subgrups nilpotents $H_i \subseteq G$. Aleshores,

$$L(s, \rho_m \otimes 1_G) = \prod_i L(s, \rho_m \otimes \operatorname{Ind}_{H_i}^G \psi_i)^{a_i}$$

Per la reciprocitat de Frobenius,

$$\rho_m \otimes \operatorname{Ind}_{H_i}^G \psi_i = \operatorname{Ind}_{H_i}^G \left(\rho_m | L^{H_i} \otimes \psi_i \right).$$

Fent servir la reciprocitat d'Artin i la invariabilitat per inducció, s'arriba

$$L(s, \rho_m) = \prod_i L(s, \rho_m | L^{H_i} \otimes \psi_i)^{a_i}$$

Step 1 implica que ρ_m és automorfa per m **senar**.

Step 3

Un teorema de Jaquet-Shalika assegura que les funcions L cuspidals automorfes admeten prolongació holomorfa a $\Re s \geq 1$ i en $\Re s = 1$ no s'anul.len. Això s'aplica a $L(s, \rho_m)$ per m senar. Per al cas parell, es procedeix per inducció (matemàtica:-):

$$\mathrm{Sym}^{m-1}\rho \oplus \mathrm{Sym}^{m+1}\rho = \mathrm{Sym}^{m}\rho \otimes \mathrm{Sym}^{1}\rho$$

$$\frac{\sin m\theta}{\sin\theta} + \frac{\sin(m+2)\theta}{\sin\theta} = \left(\frac{\sin(m+1)\theta}{\sin\theta}\right)\left(\frac{\sin 2\theta}{\sin\theta}\right)$$

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

El TAP per al conjunt de nombres senars $\{1, m\}$, més un teorema de Shahidi sobre la no anul·lació de funcions L de Rankin-Selberg, completen la prova.


0.6
0.4
0.2
0
1
2
2.5
3
ST end ST