An Introduction to the Sato-Tate Conjecture

Edray Herber Goins
Department of Mathematics
Pomona College

Algebra / Number Theory / Combinatorics Seminar
Claremont Colleges

October 2, 2018

Abstract

In 1846, Ernst Eduard Kummer conjectured a distribution of values of a cubic Gauss sum after computing a few values by hand. This was forgotten about for nearly 100 years until John von Neumann and Herman Goldstine attempted to verify the conjecture as a way to test the new ENIAC machine in 1953. They found evidence that the conjecture was false, but trusted Kummer more than they did their digital computer. The conjecture would hold until 1979, when Roger Heath-Brown and Samuel Patterson proved it to be false.

A few years earlier in 1965, Mikio Sato and John Tate independently came up with a conjecture which gave the correct distribution of these cubic Gauss sums – although it was expressed slightly differently in terms of counting points of elliptic curves over finite fields. In this talk, we give an overview of the Sato-Tate Conjecture, present an approach by Jean-Pierre Serre following his paper from 1967, then sketch the 2006 proof of the conjecture following the ideas of Laurent Clozel, Michael Harris, Nicholas Shepherd-Barron and Richard Taylor.

Outline of Talk

Gauss's Theorem

Theorem (Carl Friedrich Gauss, 1798)

Consider the Fermat curve $\mathcal{F}_3 : a^3 + b^3 + c^3 = 0$.

- *If either* $p = 3$ *or* $p \equiv 2 \pmod 3$, *then* $\#\mathcal{F}_3(\mathbb{F}_p) = p + 1$.
- *If* $p \equiv 1 \pmod 3$, *then there exist integers* a_p *and* b_p *such that*

$$\#\mathcal{F}_3(\mathbb{F}_p) = p + 1 - a_p \qquad \text{and} \qquad 4\,p = a_p^2 + 27\,b_p^2.$$

p	$\#\mathcal{F}_3(\mathbb{F}_p)$	a_p	b_p
7	9	-1	1
13	9	5	1
19	27	-7	1
31	36	-4	2
37	27	11	1
43	36	8	2

p	$\#\mathcal{F}_3(\mathbb{F}_p)$	a_p	b_p
61	63	-1	3
67	63	5	3
73	81	-7	3
79	63	17	1
97	117	-19	1
103	117	-13	3

Gauss's Theorem

Corollary

Consider the elliptic curve $E: y^2 - y = x^3 - 7$. For all primes $p \neq 3$,

$$\left(\sqrt{p} - 1\right)^2 \leq \#E(\mathbb{F}_p) \leq \left(\sqrt{p} + 1\right)^2.$$

Proof. We have a bijection

$$\begin{array}{ccc} \mathcal{F}_3: \ a^3 + b^3 + c^3 = 0 & \to & E: \ y^2 - y = x^3 - 7 \\ (a : b : c) & \mapsto & (-3\,c \ : \ -4\,a + 5\,b \ : \ a + b) \end{array}$$

Hence

$$p + 1 - \#E(\mathbb{F}_p) = a_p = \begin{cases} 0 & \text{if } p \equiv 2 \pmod 3, \\ \pm\sqrt{4\,p - 27\,b_p^2} & \text{if } p \equiv 1 \pmod 3. \end{cases}$$

In either case we have $\left|p + 1 - \#E(\mathbb{F}_p)\right| \leq 2\sqrt{p}$. □

Proof of Gauss's Theorem

First assume that $p \equiv 2 \pmod 3$. We have a bijection

$$\begin{array}{rcl} \mathbb{P}^1(\mathbb{F}_p) & \to & \left\{ (a:b:c) \in \mathbb{P}^2(\mathbb{F}_p) \,\middle|\, a^3 + b^3 + c^3 = 0 \right\} \\ (\alpha : \beta) & \mapsto & \left(-\alpha \,:\, -\beta \,:\, \left(\alpha^3 + \beta^3\right)^{(2p-1)/3} \right) \end{array}$$

Now assume $p \equiv 1 \pmod 3$. There exists a nontrivial cubic character $\chi_p : \mathbb{F}_p^\times \to \mathbb{C}^\times$. Upon setting $\chi_p(0) = 0$, define the Gauss sum

$$\tau(\chi_p) = \sum_{\alpha \in \mathbb{F}_p} \chi_p(\alpha)\, \zeta_p^\alpha = -e^{i\theta_p/3}\sqrt{p}$$

for some angle θ_p. Note that for any $\alpha \in \mathbb{F}_p$, we have the formula

$$\# \left\{ a \in \mathbb{F}_p \,\middle|\, a^3 = \alpha \right\} = 1 + \chi_p(\alpha) + \chi_p(\alpha)^2.$$

Proof of Gauss's Theorem

Now define Jacobi sum as

$$J(\chi_p, \chi_p) = \sum_{\alpha+\beta=1} \chi_p(\alpha)\,\chi_p(\beta) = \frac{\tau(\chi_p)^2}{\tau(\chi_p^2)} = -e^{i\theta_p}\sqrt{p}.$$

Writing $J(\chi_p, \chi_p) = c_p + d_p\,\zeta_3$, we have $\left|J(\chi_p, \chi_p)\right|^2 = c_p^2 - c_p\,d_p + d_p^2$.
Choose the rational integers

$$\left.\begin{aligned} a_p &= d_p - 2\,c_p \\ b_p &= d_p/3 \end{aligned}\right\} \quad \Longrightarrow \quad \begin{cases} 4\,p = a_p^2 + 27\,b_p^2 \\ a_p \equiv 2 \pmod 3 \end{cases}$$

Finally, count the number of points:

$$\begin{aligned} \#\mathcal{F}_3(\mathbb{F}_p) &= 3 + \sum_{\alpha+\beta=1} \#\left\{a \in \mathbb{F}_p \,\middle|\, a^3 = \alpha\right\} \times \#\left\{b \in \mathbb{F}_p \,\middle|\, b^3 = \beta\right\} \\ &= p + 1 + J(\chi_p, \chi_p) + J(\chi_p^2, \chi_p^2) \\ &= p + 1 - a_p. \end{aligned}$$

Kummer's Conjecture

Conjecture (Ernst Eduard Kummer, 1846)

For each rational prime $p \equiv 1 \pmod 3$, consider the cubic Gauss sum as

$$\tau_p = \sum_{\alpha \in \mathbb{F}_p} \zeta_p{}^{\alpha^3} = \tau(\chi_p) + \tau(\chi_p^2) = -2\sqrt{p}\,\cos\frac{\theta_p}{3}.$$

Then $\big(1:2:3\big)$ is the proportion of p for which τ_p lies in the intervals

$$\big[-2\sqrt{p},\ -\sqrt{p}\big], \qquad \big[-\sqrt{p},\ \sqrt{p}\big], \qquad \text{and} \qquad \big[\sqrt{p},\ 2\sqrt{p}\big].$$

Recall that

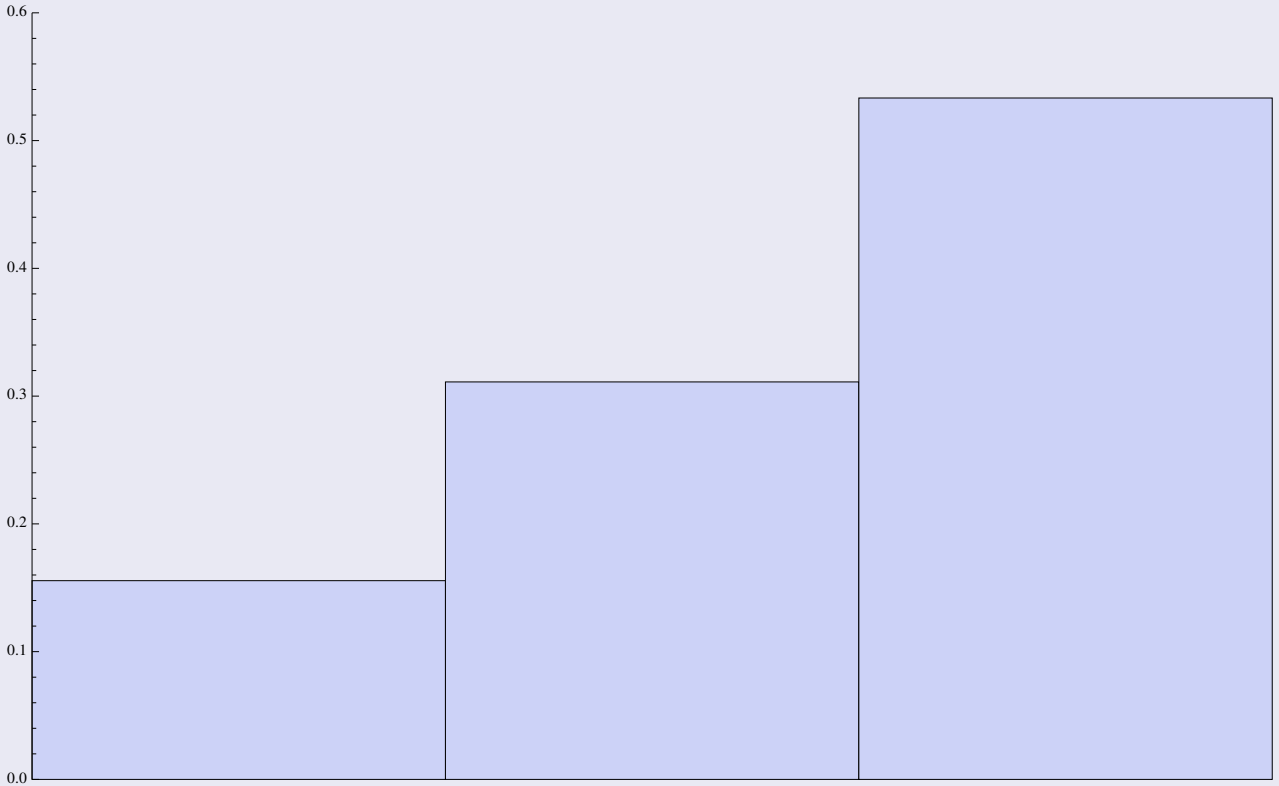
$$2\,\cos\theta_p = -\frac{J(\chi_p,\chi_p) + J(\chi_p^2,\chi_p^2)}{\sqrt{p}} = \frac{a_p}{\sqrt{p}}.$$

Verification of Kummer's Conjecture?

```
KummerClass[p_Integer] :=
 Round[
    (1 + 2 Sum[ Cos[(2 Pi n^3)/p], {n, (p-1)/2}]) / (2 Sqrt[p])
 ]

KummerHistogram[bound_Integer] := Module[{pmod3, class},

 pmod3 = Select[
   Table[ Prime[n], {n, PrimePi[bound]}],
   Mod[#,3]==1&];

 class = Table[ KummerClass[pmod3[[n]]], {n, Length[pmod3]}];

 Return[Histogram[
    class, Automatic, "Probability",
    PlotRange -> {{-1,2}, {0.0,0.6}}, Axes -> {False,True}]
 ]]
```

Verification of Kummer's Conjecture?

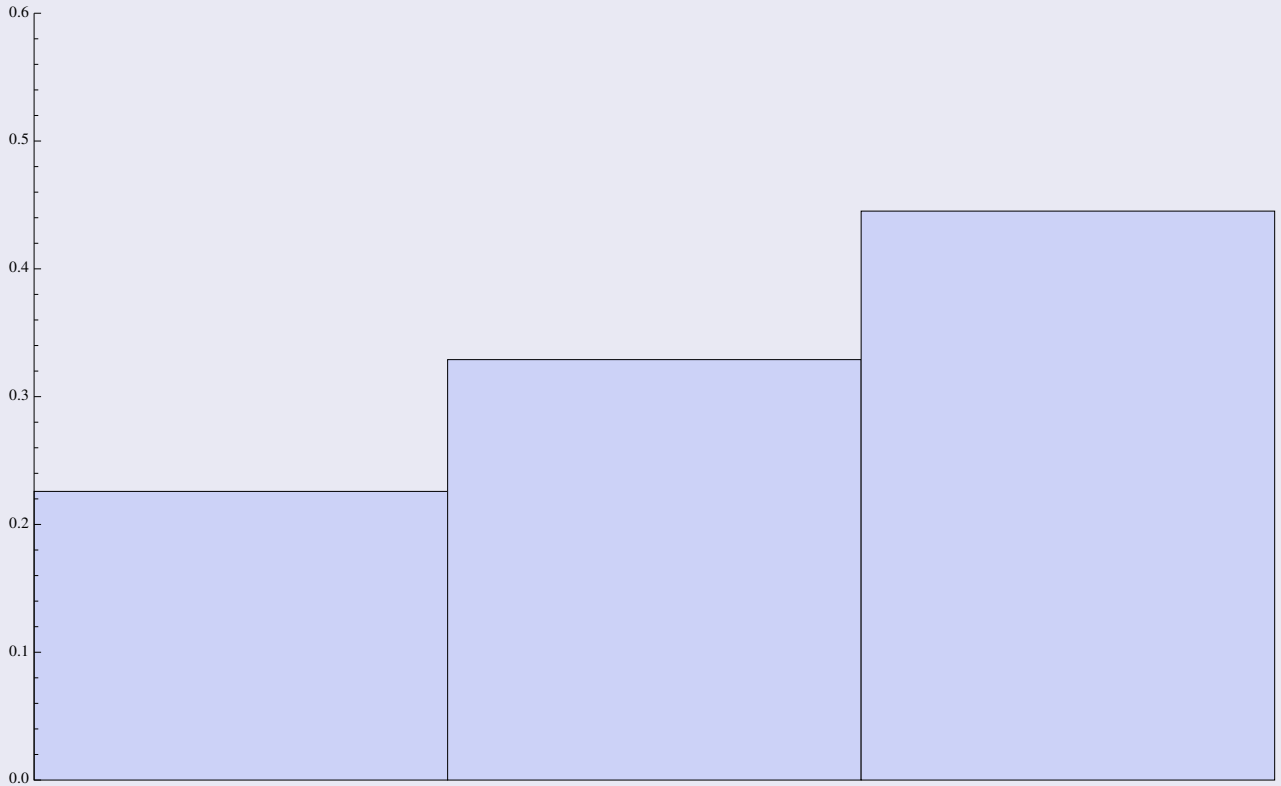
Proposition (Ernst Eduard Kummer, 1846)



45 primes $p \leq 500$ with $(7 : 14 : 24) \approx (1 : 2 : 3)$

Verification of Kummer's Conjecture?

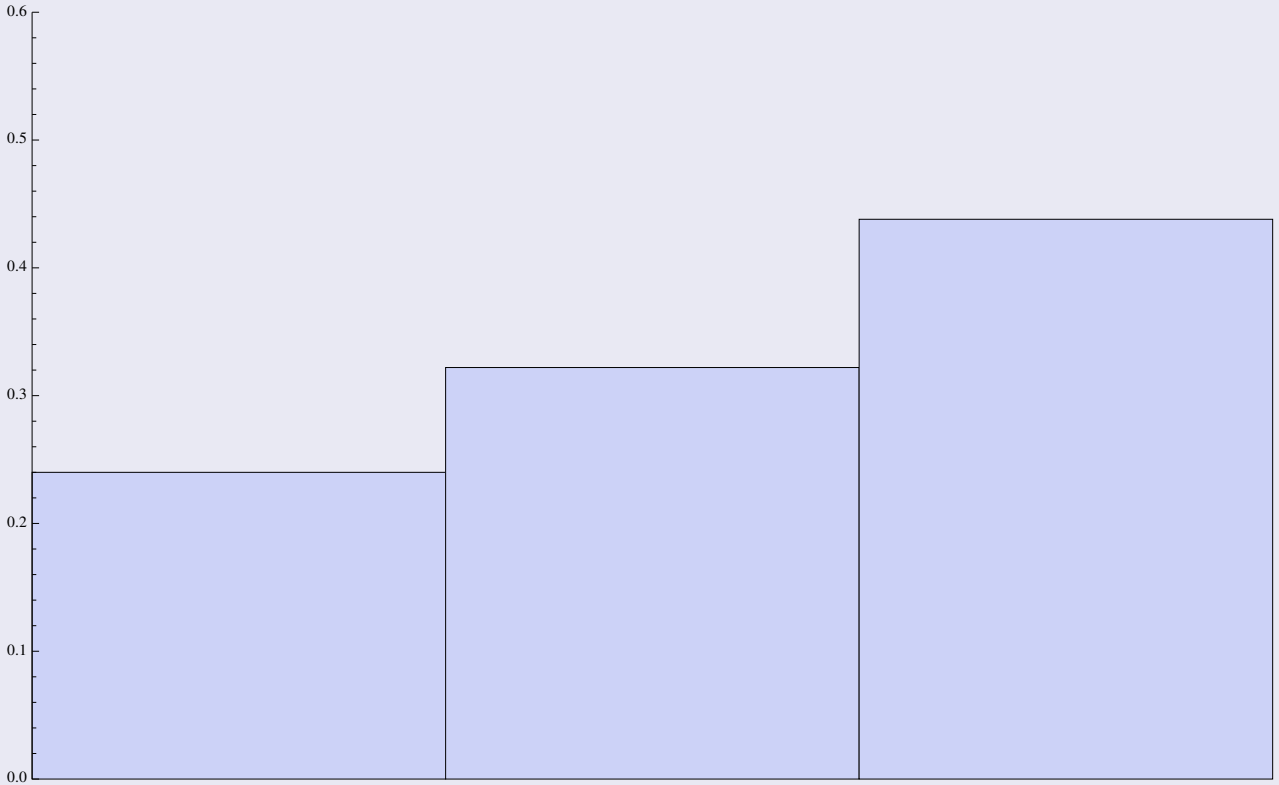
Proposition (John von Neumann and Herman Goldstine, 1953)



611 primes $p \leq 10\,000$ with $(138 : 201 : 272) \approx (2 : 3 : 4)$

Verification of Kummer's Conjecture?

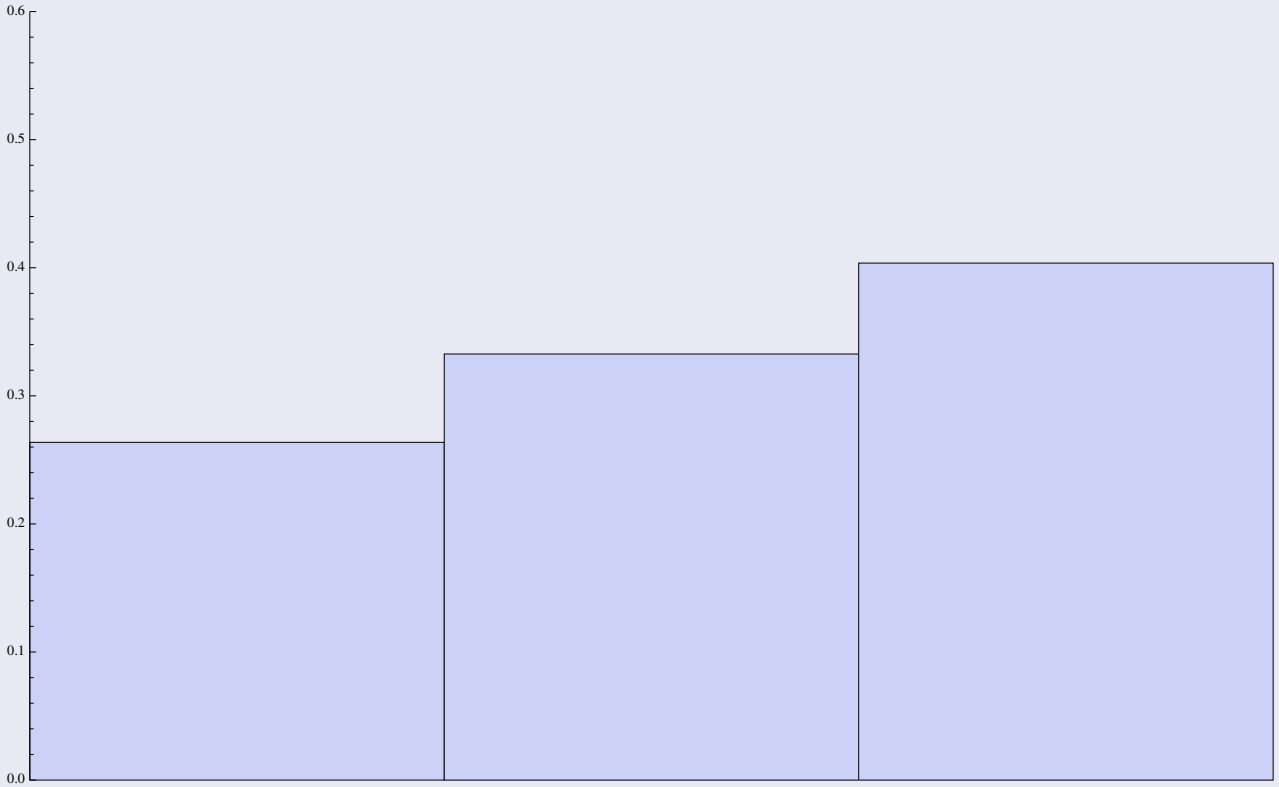
Proposition (Emma Lehmer, 1956)



$1\,000$ primes $p \leq 17\,550$ with $(240 : 322 : 438) \approx (3 : 4 : 5)$

Verification of Kummer's Conjecture?

Proposition (Carl-Erik Fröberg, 1974)



8 988 primes $p \leq 200\,000$ with $(2370 : 2990 : 3628) \approx (4 : 5 : 6)$

Kummer's Conjecture

Conjecture (Ernst Eduard Kummer, 1846)

For each rational prime $p \equiv 1 \pmod 3$, consider the cubic Gauss sum as

$$\tau_p = \sum_{\alpha \in \mathbb{F}_p} \zeta_p{}^{\alpha^3} = \tau(\chi_p) + \tau(\chi_p^2) = -2\sqrt{p}\,\cos\frac{\theta_p}{3}.$$

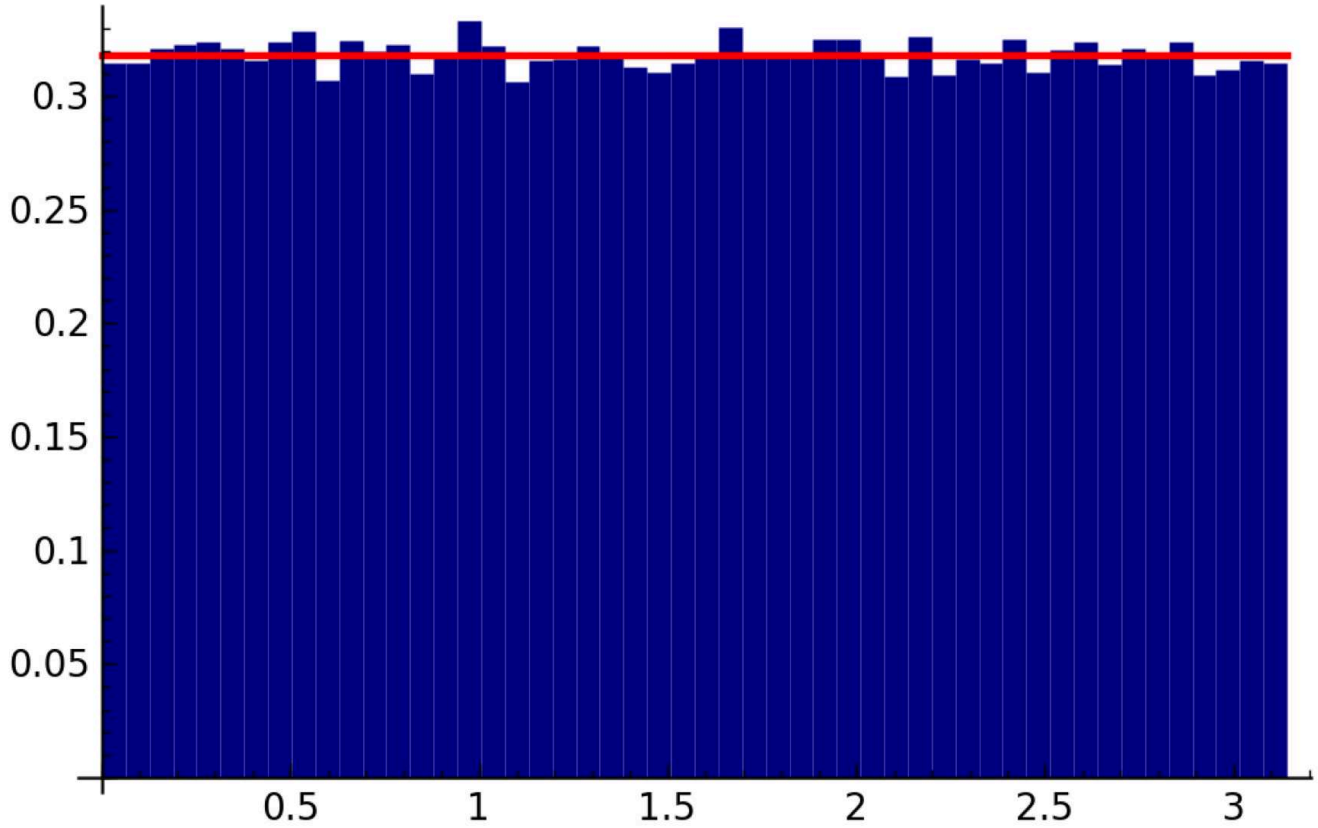
Then $(1:2:3)$ is the proportion of p for which τ_p lies in the intervals

$$\left[-2\sqrt{p},\ -\sqrt{p}\right], \qquad \left[-\sqrt{p},\ \sqrt{p}\right], \qquad \text{and} \qquad \left[\sqrt{p},\ 2\sqrt{p}\right].$$

Theorem (Roger Heath-Brown and Samuel Patterson, 1979)

Kummer's conjecture is false: the angles θ_p defined by $2\cos\theta_p = \dfrac{a_p}{\sqrt{p}}$ are equidistributed in $[0,\pi]$ with respect to the measure $d\mu = \dfrac{1}{\pi}\,d\theta$.

Falsification of Kummer's Conjecture!



Histogram of $\theta_p = \cos^{-1} \dfrac{p + 1 - \#\mathcal{F}_3(\mathbb{F}_p)}{2\sqrt{p}}$ for $p \leq 1\,000\,000$

Can we generalize this?

- Inequality:
$$\left(\sqrt{p}-1\right)^2 \leq \#E(\mathbb{F}_p) \leq \left(\sqrt{p}+1\right)^2.$$
- Angle:
$$\frac{a_p}{\sqrt{p}} = 2\cos\theta_p \qquad \text{in terms of} \qquad a_p = p+1-\#E(\mathbb{F}_p).$$
- "Equidistributed"?

Elliptic Curves

Given a field k, consider the equation

$$E: \qquad y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6.$$

Define the following constants as elements of k:

$$\begin{aligned}
c_4 &= a_1^4 + 8\,a_1^2\,a_2 + 16\,a_2^2 - 24\,a_1\,a_3 - 48\,a_4 \\
c_6 &= -a_1^6 - 12\,a_1^4\,a_2 - 48\,a_1^2\,a_2^2 - 64\,a_2^3 + 36\,a_1^3\,a_3 \\
&\quad + 144\,a_1\,a_2\,a_3 - 216\,a_3^2 + 72\,a_1^2\,a_4 + 288\,a_2\,a_4 - 864\,a_6 \\
\Delta(E) &= -a_1^4\,a_2\,a_3^2 - 8\,a_1^2\,a_2^2\,a_3^2 - 16\,a_2^3\,a_3^2 + a_1^3\,a_3^3 + 36\,a_1\,a_2\,a_3^3 \\
&\quad - 27\,a_3^4 + a_1^5\,a_3\,a_4 + 8\,a_1^3\,a_2\,a_3\,a_4 + 16\,a_1\,a_2^2\,a_3\,a_4 \\
&\quad - 30\,a_1^2\,a_3^2\,a_4 + 72\,a_2\,a_3^2\,a_4 + a_1^4\,a_4^2 + 8\,a_1^2\,a_2\,a_4^2 \\
&\quad + 16\,a_2^2\,a_4^2 - 96\,a_1\,a_3\,a_4^2 - 64\,a_4^3 - a_1^6\,a_6 - 12\,a_1^4\,a_2\,a_6 \\
&\quad - 48\,a_1^2\,a_2^2\,a_6 - 64\,a_2^3\,a_6 + 36\,a_1^3\,a_3\,a_6 + 144\,a_1\,a_2\,a_3\,a_6 \\
&\quad - 216\,a_3^2\,a_6 + 72\,a_1^2\,a_4\,a_6 + 288\,a_2\,a_4\,a_6 - 432\,a_6^2
\end{aligned}$$

Elliptic Curves

Given a field k, consider the equation

$$E: \qquad y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6.$$

If k has characteristic different from 2 and 3, we may write

$$E:\ y^2 = x^3 - \frac{3}{12^2}\,c_4\,x - \frac{2}{12^3}\,c_6 \qquad \text{and} \qquad \Delta(E) = \frac{c_4^3 - c_6^2}{12^3}.$$

We say E is an elliptic curve defined over k if $\Delta(E) \neq 0$. We will focus on the collection of k-rational points

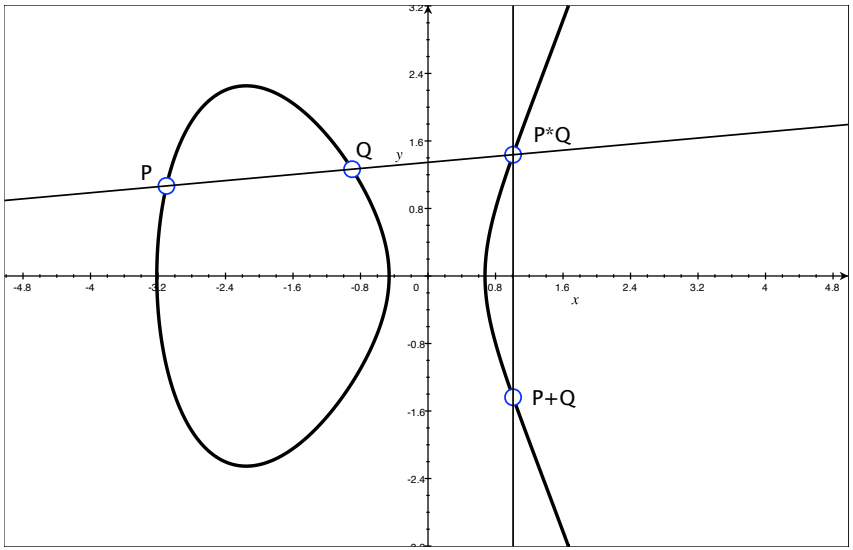
$$E(k) = \left\{ (x_1 : x_2 : x_0) \in \mathbb{P}^2(k) \;\middle|\; \begin{array}{r} x_2^2\,x_0 + a_1\,x_1\,x_2\,x_0 + a_3\,x_2\,x_0^2 \\ = x_1^3 + a_2\,x_1^2\,x_0 + a_4\,x_1\,x_0^2 + a_6\,x_0^3 \end{array} \right\}$$

having a specified base point $\mathcal{O} = (0 : 1 : 0)$. Define the j-invariant as

$$j(E) = \frac{c_4^3}{\Delta(E)} = 12^3\,\frac{c_4^3}{c_4^3 - c_6^2}.$$

Group Law

Let $P, Q \in E(k)$. Denote $P * Q$ as the point of intersection of E and the line through P and Q, and denote $P \oplus Q = (P * Q) * \mathcal{O}$.



Theorem (Henri Poincaré, 1901)

Consider an elliptic curve E defined over a field k. Then $(E(k), \oplus)$ is abelian group with identity $\mathcal{O} = (0 : 1 : 0)$ and inverses $[-1]P = P * \mathcal{O}$.

Properties of Elliptic Curves

Consider an elliptic curve E defined over a field k. Recall the following:

- The ℓ-adic Tate module is the finite dimensional $\mathbb{Q}_\ell$-vector space

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

  in terms of the torsion subgroup $E[m] = \left\{ P \in E(\overline{k}) \,\middle|\, [m]P = \mathcal{O} \right\}$.
- There exist embeddings as $\mathbb{Z}$-algebras

$$\mathbb{Z}\left[\mathrm{Gal}\left(\overline{k}/k\right)\right] \hookrightarrow \mathrm{End}(E) \hookrightarrow \mathrm{End}\left(V_\ell(E)\right).$$

- Viewing $\sigma \in \mathrm{Gal}\left(\overline{k}/k\right) \hookrightarrow GL\left(V_\ell(E)\right)$, define the degree as

$$\deg(\sigma) = \left[k(E) : \sigma^* k(E)\right] = \det(\sigma).$$

- If $\sigma \in \mathrm{End}(E)$ has $\deg(\sigma) = m$, there exists $\widehat{\sigma} \in \mathrm{End}(E)$ such that

$$\sigma \circ \widehat{\sigma} = \widehat{\sigma} \circ \sigma = [m].$$

Hasse Inequality

Theorem (Helmut Hasse, 1934)

Consider an elliptic curve E defined over a field k.

- *The pairing $tr : End(E) \times End(E) \to \mathbb{Z}$ defined by*

$$tr(\sigma, \sigma') = \underbrace{\deg(\sigma + \sigma') - \deg(\sigma) - \deg(\sigma')}_{\text{in } \mathbb{Z}} = \underbrace{\sigma \circ \widehat{\sigma}' + \widehat{\sigma} \circ \sigma'}_{\text{in } \mathbb{Z} \hookrightarrow End(E)}$$

  is a positive definite quadratic form.

- *Assume that $k = \mathbb{F}_p$. The polynomial $Q : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by*

$$Q(x, y) = \deg\left(x - \sigma_p\, y\right) = x^2 - a_p\, x\, y + p\, y^2$$

  in terms of the trace $a_p = p + 1 - \#E(\mathbb{F}_p) = \sigma_p + \widehat{\sigma}_p$ implies

$$\left(\sqrt{p} - 1\right)^2 \leq \#E(\mathbb{F}_p) \leq \left(\sqrt{p} + 1\right)^2.$$

Zeta Function of an Elliptic Curve

Corollary

Consider an elliptic curve E defined over $k = \mathbb{F}_p$.

- *(Rationality) With α_p, $\beta_p = \left(a_p \pm i\sqrt{4\,p - a_p^2}\right)/2$, we have*

$$\begin{aligned} \alpha_p + \beta_p &= a_p \\ \alpha_p \cdot \beta_p &= p \end{aligned} \qquad \text{and} \qquad \#E(\mathbb{F}_{p^n}) = p^n + 1 - \alpha_p^n - \beta_p^n.$$

In particular, we have the identity

$$\zeta_{E/\mathbb{F}_p}(s) = \exp\left[\sum_{n=1}^{\infty} \#E(\mathbb{F}_{p^n})\,\frac{1}{n\,p^{ns}}\right] = \frac{1 - a_p\,p^{-s} + p^{1-2s}}{(1-p^{-s})\,(1-p^{1-s})}.$$

- *(Riemann Hypothesis) If $\zeta_{E/\mathbb{F}_p}(s) = 0$ then $Re(s) = 1/2$.*
- *(Functional Equation) If $\zeta_{E/\mathbb{F}_p}(1-s) = \zeta_{E/\mathbb{F}_p}(s)$.*

ℓ-adic Galois Representation of an Elliptic Curve

Consider an elliptic curve E defined over $k = \mathbb{Q}$. Assume moreover that E is defined over $\mathbb{Z}$, and ℓ is a prime which does not divide $\Delta(E)$.

- By considering the continuous action of the absolute Galois group on the ℓ-adic Tate module, we have a continuous representation

$$\rho_{E,\ell}: \qquad \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to GL_2(\mathbb{Q}_\ell).$$

- For every prime p, we have a short-exact sequence

$$\{1\} \to I_p \to \mathrm{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p\right) \to \mathrm{Gal}\left(\overline{\mathbb{F}}_p/\mathbb{F}_p\right) \to \{1\}.$$

  As long as $p \nmid \ell \cdot \Delta(E)$, the inertia group I_p acts trivially on $V_\ell(E)$.

$$\begin{aligned} \mathrm{tr}\, \rho_{E,\ell}(\sigma_p) &= \alpha_p + \beta_p = a_p \\ \det\, \rho_{E,\ell}(\sigma_p) &= \alpha_p \cdot \beta_p = p \end{aligned}$$

- Using the Hasse Inequality, we can write

$$\begin{aligned} \alpha_p &= e^{+i\theta_p}\sqrt{p} \\ \beta_p &= e^{-i\theta_p}\sqrt{p} \end{aligned} \qquad \Longrightarrow \qquad \frac{a_p}{\sqrt{p}} = 2\cos\theta_p.$$

Unitary Galois Representation of an Elliptic Curve

Theorem

Consider an elliptic curve E defined over $k = \mathbb{Q}$. There exists a normalized continuous complex Galois representation

$$\rho_E^{(2)} : \qquad Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to SU_2(\mathbb{C})$$

in terms of the special unitary group

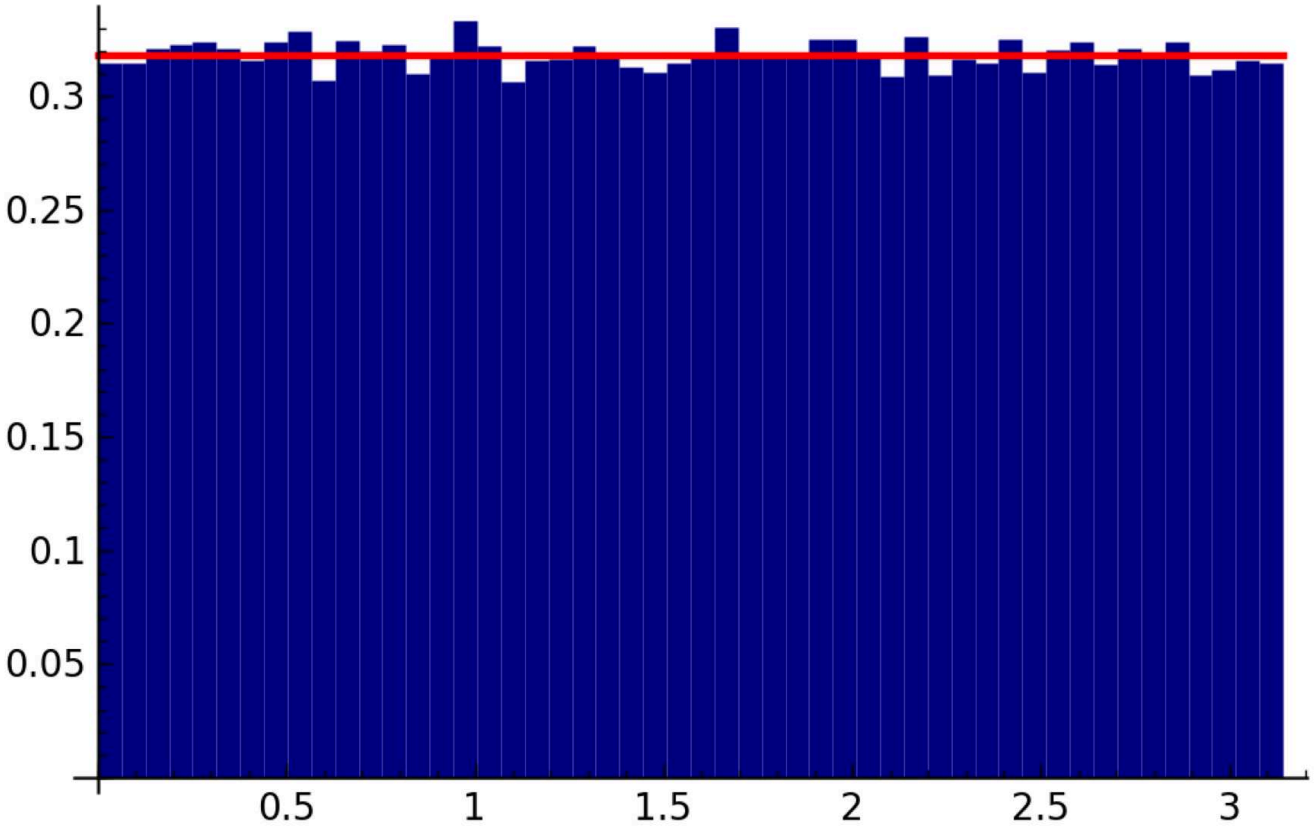
$$SU_2(\mathbb{C}) = \left\{ g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{C}) \middle| \, a\,d - b\,c = 1,\, g^{-1} = \begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} \right\}$$

such that for almost all primes p the image of the Frobenius element is

$$g_p = \frac{1}{\sqrt{p}} \cdot \rho_{E,\ell}(\sigma_p) \sim \begin{bmatrix} e^{+i\theta_p} & 0 \\ 0 & e^{-i\theta_p} \end{bmatrix} \quad \Longrightarrow \quad tr\, g_p = 2\,\cos\theta_p = \frac{a_p}{\sqrt{p}}.$$

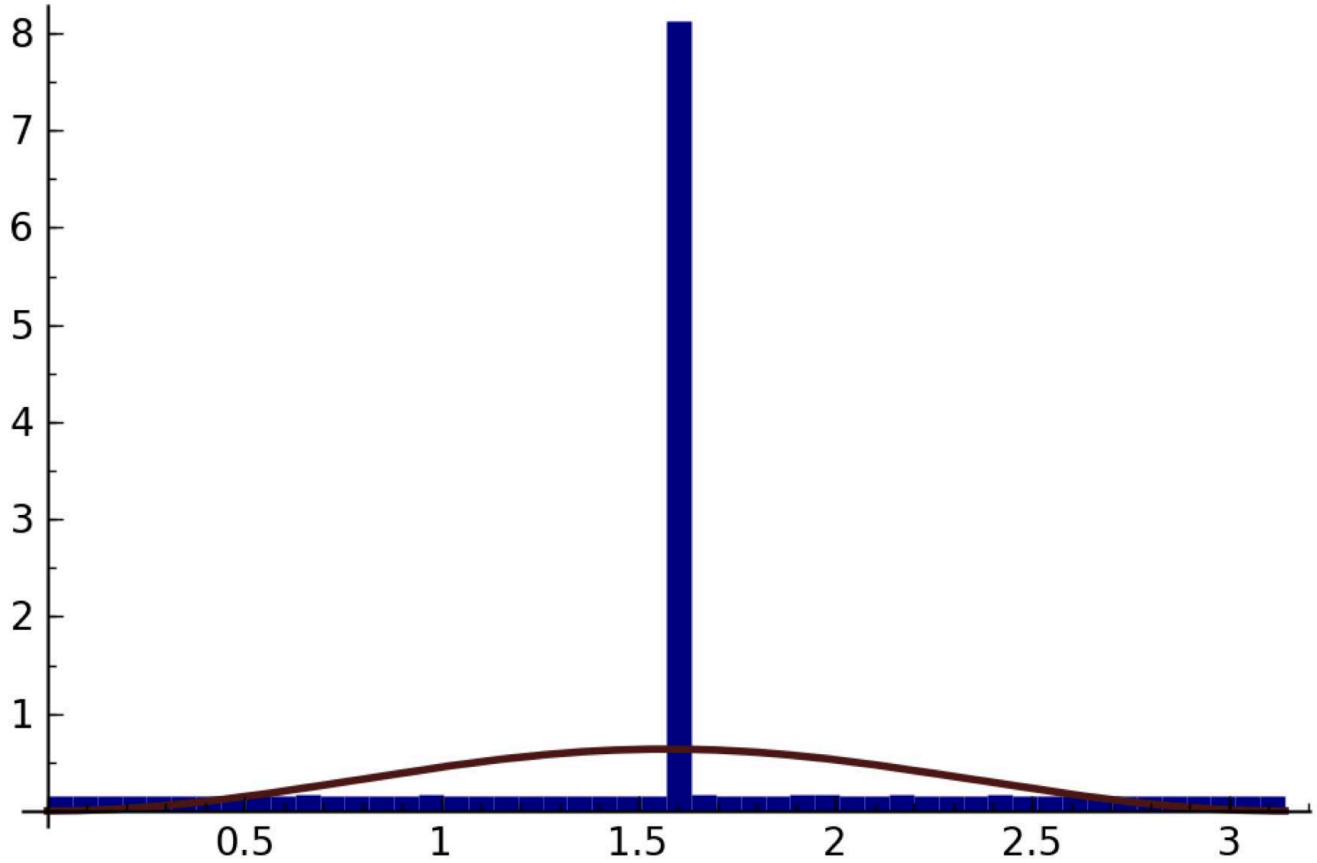
Are the traces "equidistributed"?

$X_0(27): \ y^2 - y = x^3 - 7$



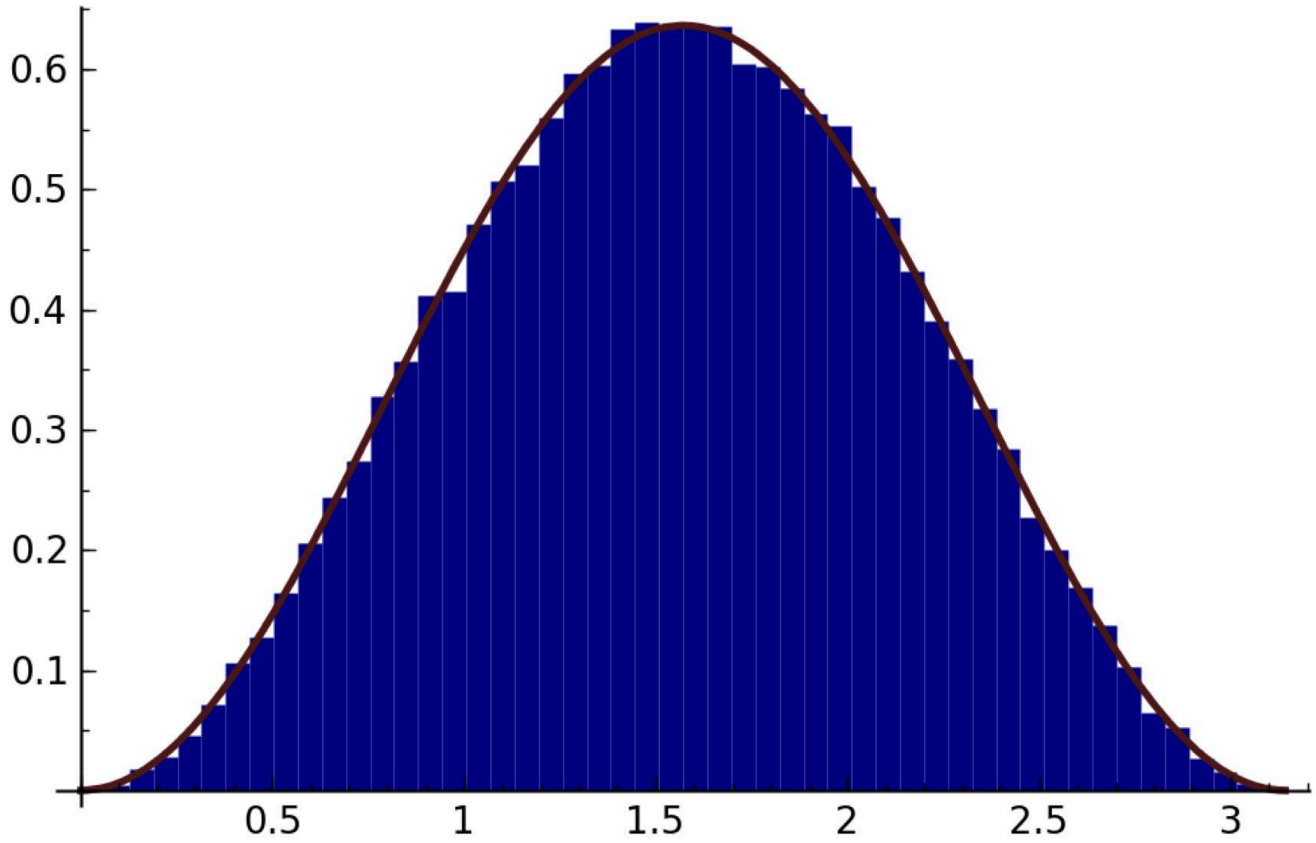
$$\Delta(E) = -3^9 \qquad \text{and} \qquad j(E) = 0$$

$X_0(27): \ y^2 - y = x^3 - 7$



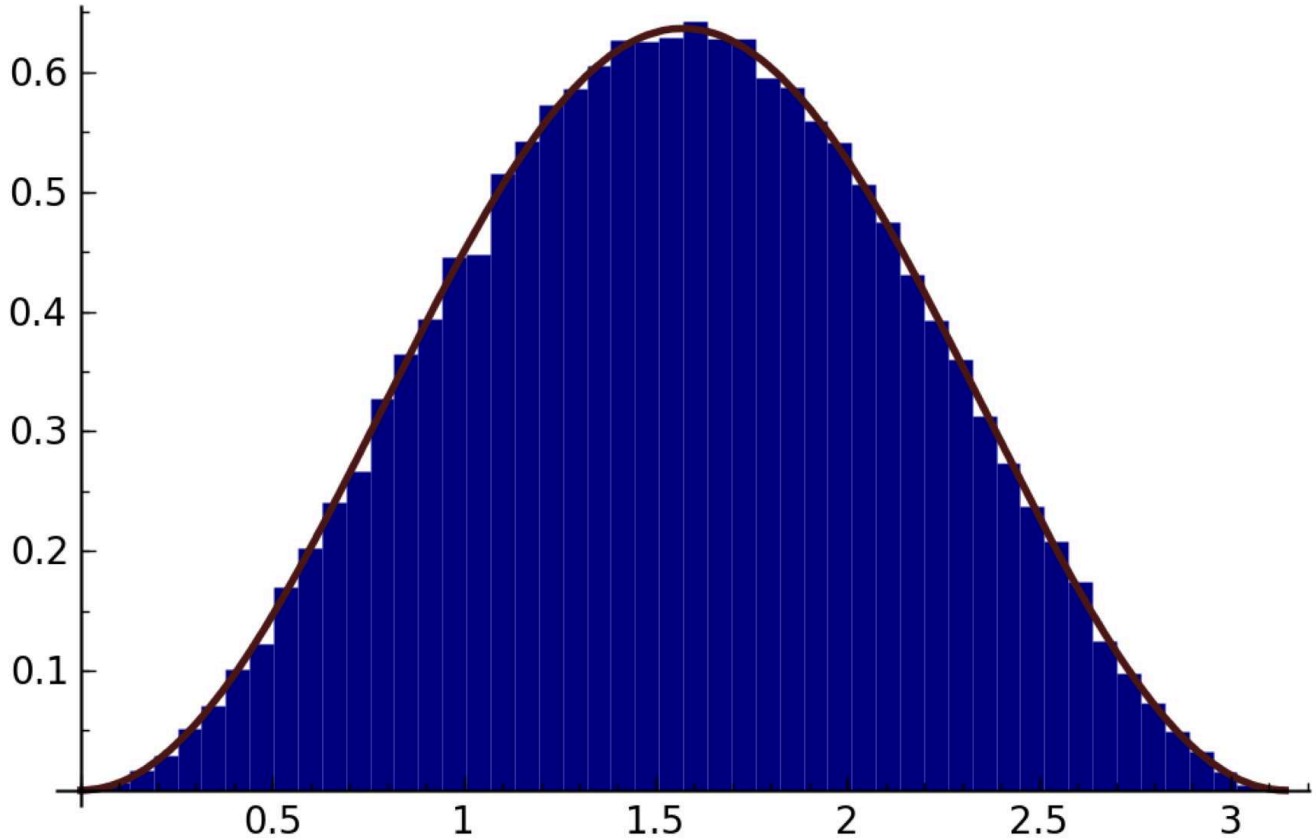
$$\Delta(E) = -3^9 \qquad \text{and} \qquad j(E) = 0$$

$X_0(11): \; y^2 - y = x^3 - x^2 - 10\,x - 20$



$$\Delta(E) = -11^5 \qquad \text{and} \qquad j(E) = -\frac{2^{12} \cdot 31^3}{11^5}$$

$X_0(11)/C: \; y^2 + xy + y = x^2 + x^2 - 305x + 7888$



$$\Delta(E) = -11^{10} \qquad \text{and} \qquad j(E) = -11^2$$

Sato-Tate Conjecture

Conjecture (Mikio Sato and John Tate, 1965)

Consider an elliptic curve E defined over $k = \mathbb{Q}$ without complex multiplication. Then the angles θ_p defined by $2\cos\theta_p = \dfrac{a_p}{\sqrt{p}}$ are equidistributed in $[0, \pi]$ with respect to the measure $d\mu = \dfrac{2}{\pi}\sin^2\theta\, d\theta$.

That is, for any any integrable function $F : [0, \pi] \to \mathbb{C}$, we have the limit

$$\lim_{X\to\infty} \frac{\sum_{p\leq X} F(\theta_p)}{\sum_{p\leq X} 1} = \frac{2}{\pi}\int_0^\pi F(\theta)\sin^2\theta\, d\theta.$$

The Prime Number Theorem asserts that

$$\pi(X) = \sum_{p\leq X} 1 \approx \frac{X}{\log X} \approx \int_2^X \frac{dt}{\log t}.$$

Measures on $SU(2)$

Proposition

Define the special unitary group

$$SU_2(\mathbb{C}) = \left\{ g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C}) \middle| \, a\,d - b\,c = 1,\ g^{-1} = \begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} \right\}.$$

- $SU_2(\mathbb{C}) \simeq U_1(\mathbb{H})$ as groups, and $SU_2(\mathbb{C}) \simeq S^3(\mathbb{R})$ as manifolds.
- There is a normalized measure μ on $SU_2(\mathbb{C})$ such that for any integrable function $G : [-2, 2] \to \mathbb{C}$ we have the integral

$$\int_{SU_2(\mathbb{C})} G\big(\operatorname{tr} g\big)\, d\mu = \frac{2}{\pi} \int_0^{\pi} G(2\cos\theta)\, \sin^2\theta\, d\theta.$$

Sato-Tate Conjecture Revisited

Conjecture

Consider an elliptic curve E defined over $k = \mathbb{Q}$ without complex multiplication, and denote the normalized continuous complex Galois representation $\rho_E^{(2)} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to SU_2(\mathbb{C})$ which sends $\sigma_p \mapsto g_p$.

As $\operatorname{tr} g_p = 2\cos\theta_p$, for any integrable class function

$$\begin{array}{ccccc} & & [0,\,\pi] & & \\ & & \Big\downarrow{\scriptstyle 2\cos} & \searrow^{F} & \\ \chi : \; SU_2(\mathbb{C}) & \xrightarrow{\quad\mathrm{tr}\quad} & [-2,\,2] & \xrightarrow{\quad G\quad} & \mathbb{C} \end{array}$$

we have the limit

$$\lim_{X\to\infty} \frac{\sum_{p\le X} \chi(g_p)}{\sum_{p\le X} 1} = \int_{SU_2(\mathbb{C})} \chi(g)\, d\mu.$$

Proof of Proposition

By the definition of the special unitary group,

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SU_2(\mathbb{C}) \quad \Longleftrightarrow \quad \begin{array}{ll} |a|^2 + |b|^2 = 1 & \overline{a}\,c + \overline{b}\,d = 0 \\ |c|^2 + |d|^2 = 1 & a\,d - b\,c = 1 \end{array}$$

From the latter two identities

$$\begin{array}{l} \overline{a}\,c + \overline{b}\,d = 0 \\ a\,d - b\,c = 1 \end{array} \quad \Longleftrightarrow \quad c = -\frac{\overline{b}}{|a|^2 + |b|^2}, \quad d = \frac{\overline{a}}{|a|^2 + |b|^2}.$$

We have the well-known result

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SU_2(\mathbb{C}) \quad \Longleftrightarrow \quad g = \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} \quad \text{where} \quad |a|^2 + |b|^2 = 1.$$

Proof of Proposition

$$a = \frac{x + i\,y}{2} \qquad b = \frac{z + i\,w}{2} \qquad \Longrightarrow \qquad \begin{aligned} x &= r\,\cos\theta \\ y &= r\,\sin\theta\,\cos\varphi \\ z &= r\,\sin\theta\,\sin\varphi\,\cos\phi \\ w &= r\,\sin\theta\,\sin\varphi\,\sin\phi \end{aligned} \qquad \text{where} \qquad \begin{aligned} 0 &\leq r \\ 0 &\leq \theta \leq \pi \\ 0 &\leq \varphi \leq \pi \\ 0 &\leq \phi \leq 2\,\pi \end{aligned}$$

The Jacobian of this change of variables is

$$dx\,dy\,dz\,dw = \left(r^3\,\sin^2\theta\,\sin\varphi\right)\,dr\,d\theta\,d\varphi\,d\phi$$

so we have a normalized measure on $SU_2(\mathbb{C})$ defined by

$$d\mu = \frac{\sin^2\theta\,\sin\varphi}{2\,\pi^2}\,d\theta\,d\varphi\,d\phi.$$

Noting that $\operatorname{tr} g = x = 2\,\cos\theta$ for $r = 2$, we have the integral

$$\int_{SU_2(\mathbb{C})} G\left(\operatorname{tr} g\right)\,d\mu = \int_{-2}^{2} G(x)\,\frac{\sqrt{4 - x^2}}{2\pi}\,dx = \frac{2}{\pi}\int_0^{\pi} G(2\,\cos\theta)\,\sin^2\theta\,d\theta.$$

Modern Form of the Conjecture

Conjecture

Consider an elliptic curve E defined over $k = \mathbb{Q}$ without complex multiplication, and denote the normalized continuous complex Galois representation

$$\rho_E^{(2)} : \begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \to & SU_2(\mathbb{C}) \\ \sigma_p & \mapsto & g_p = \dfrac{1}{\sqrt{p}} \cdot \rho_{E,\ell}(\sigma_p) \end{array}$$

For any integrable class function $\chi : SU_2(\mathbb{C}) \to \mathbb{C}$ we have the limit

$$\lim_{X\to\infty} \frac{\sum_{p\le X} \chi(g_p)}{\sum_{p\le X} 1} = \int_{SU_2(\mathbb{C})} \chi(g)\, d\mu.$$

How do we prove this?

- Peter-Weyl Theorem:

  Classify all integrable class functions $\chi : SU_2(\mathbb{C}) \to GL(V) \to \mathbb{C}$ *by classifying unitary representations* $\pi : SU_2(\mathbb{C}) \to GL(V)$.

- Wiener-Ikehara Theorem:

  $$\textit{Find an expression for } \lim_{X \to \infty} \frac{\sum_{p \leq X} \chi(g_p) \log p}{X}.$$

- Abel Summation Formula + Prime Number Theorem:

  $$\textit{Find an expression for } \lim_{X \to \infty} \frac{\sum_{p \leq X} \chi(g_p)}{\pi(X)}.$$

Peter-Weyl Theorem

Theorem (Fritz Peter and Hermann Weyl, 1927)

Consider an integrable class function

$$\chi : \qquad SU_2(\mathbb{C}) \xrightarrow{\pi} GL(V) \longrightarrow \mathbb{C}$$

viewed as a matrix coefficient for a complex representation π.

- *The collection of such χ is dense in space of continuous class functions on $SU_2(\mathbb{C})$.*
- *Any unitary representation $\pi : SU_2(\mathbb{C}) \to GL(V)$ is the direct sum of irreducible unitary representations $\pi_n : SU_2(\mathbb{C}) \to GL_n(\mathbb{C})$.*
- *Matrix coefficients χ_n associated to the π_n form an orthonormal basis for the space of (square) integrable class functions.*

Writing $\chi = \sum_n m_n \chi_n$, it suffices to show for nontrivial χ_n that

$$\lim_{X\to\infty} \frac{\sum_{p\leq X} \chi_n(g_p)}{\sum_{p\leq X} 1} = \int_{SU_2(\mathbb{C})} \chi_n(g)\, d\mu = 0.$$

Symmetric Power Representations

Theorem

The only irreducible unitary representations $\pi_n : SU_2(\mathbb{C}) \to GL_n(\mathbb{C})$ are the symmetric powers $\pi_n = Sym^{n-1}$, i.e.,

$$Sym^{n-1} : \quad \begin{bmatrix} \alpha & \\ & \beta \end{bmatrix} \mapsto \begin{bmatrix} \alpha^{n-1} & & & & \\ & \alpha^{n-2}\beta & & & \\ & & \ddots & & \\ & & & \alpha\beta^{n-2} & \\ & & & & \beta^{n-1} \end{bmatrix}.$$

Corollary (Weyl Character Formula)

$$g \sim \begin{bmatrix} \alpha & \\ & \beta \end{bmatrix} \quad \Longrightarrow \quad \chi_n(g) = tr\left(Sym^{n-1} g\right) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Symmetric Power Representations

Sketch of Proof: We consider the following diagram:

$$\underbrace{\begin{bmatrix} +i\,\theta & 0 \\ 0 & -i\,\theta \end{bmatrix} \quad \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 \\ y & 0 \end{bmatrix}}_{\mathfrak{su}_2(\mathbb{C})} \xrightarrow{\Pi_n} \mathfrak{gl}_n(\mathbb{C})$$

$$\downarrow \exp \qquad\qquad \downarrow \exp \qquad\qquad \downarrow \exp$$

$$\underbrace{\begin{bmatrix} e^{+i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix} \quad \begin{bmatrix} 1 & e^{x} \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ e^{y} & 1 \end{bmatrix}}_{SU_2(\mathbb{C})} \xrightarrow{\pi_n} GL_n(\mathbb{C})$$

Any continuous representation π_n of the Lie group $SU_2(\mathbb{C})$ corresponds to a continuous representation Π_n of the Lie algebra $\mathfrak{su}_2(\mathbb{C})$. It suffices to compute properties of the images of the generators.

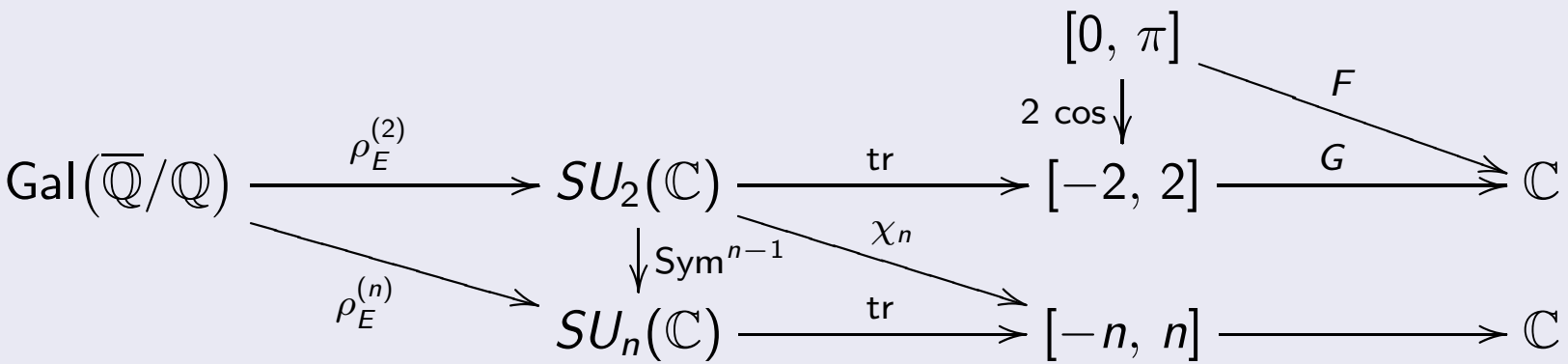
Proof #1: Compute eigenvalues and highest weights.

Proof #2: Use the orthogonality of the sine functions. □

Modern Statement via Symmetric Powers

Conjecture

Consider an elliptic curve E defined over $k = \mathbb{Q}$ without complex multiplication, and denote the continuous Galois representation $\rho_E^{(n)} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to SU_n(\mathbb{C})$ which sends $\sigma_p \mapsto \mathrm{Sym}^{n-1} g_p$.



For all $n \geq 2$, we have the limit

$$\lim_{X \to \infty} \frac{\sum_{p \leq X} \chi_n(g_p)}{\sum_{p \leq X} 1} = 0 \qquad \text{where} \qquad \chi_n(g_p) = \mathrm{tr}\, \rho_E^{(n)}(\sigma_p).$$

Modern Statement via Generating Functions

By the Weyl Character Formula, we know that

$$\chi_n(g_p) = \frac{\alpha_p^n - \beta_p^n}{\alpha_p - \beta_p} \quad \text{for} \quad \det\left[1 - \rho_E^{(2)}(\sigma_p)\, T\right] = \left(1 - \alpha_p T\right)\left(1 - \beta_p T\right).$$

The Sato-Tate Conjecture can be restated as follows:

Conjecture

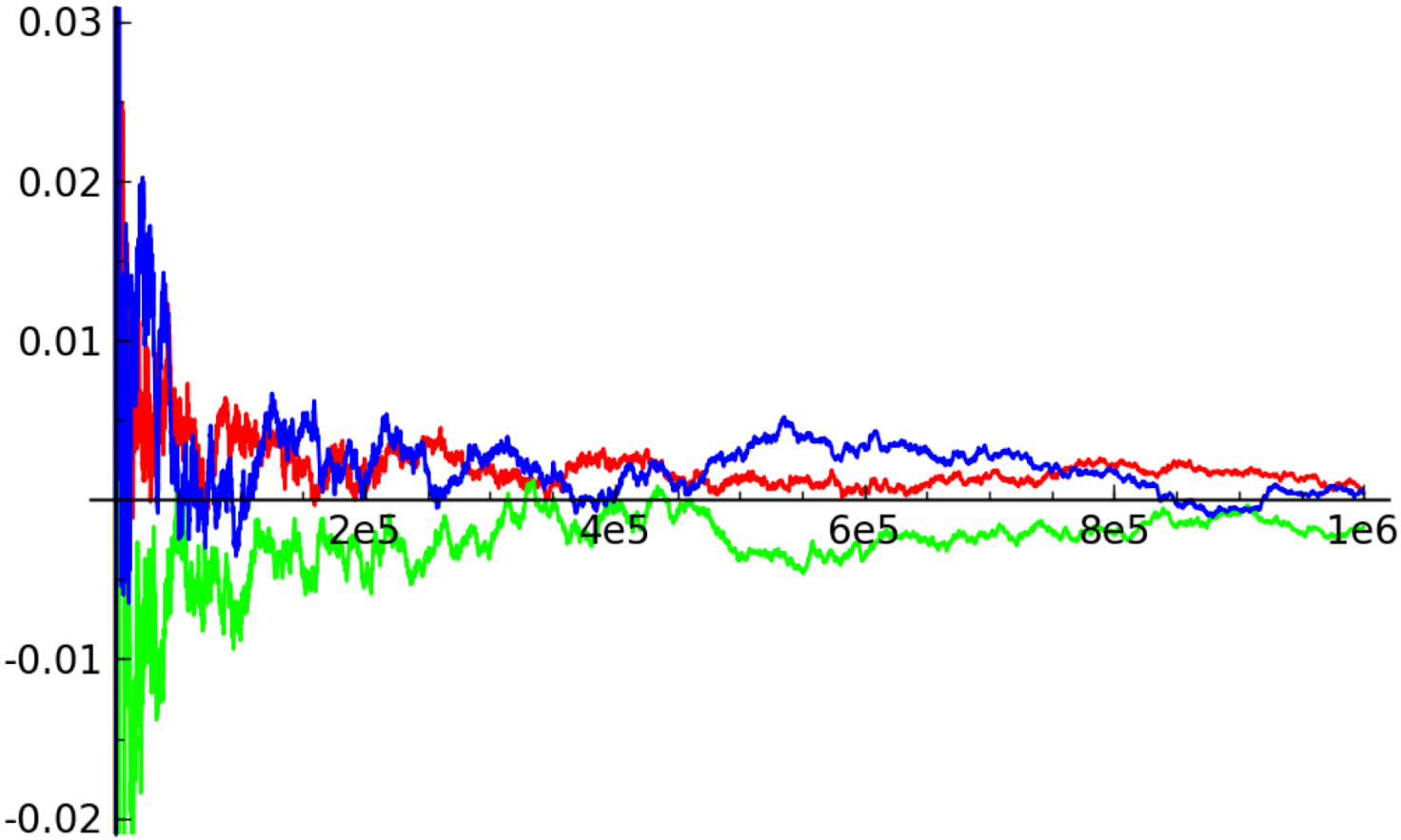
Consider an elliptic curve E defined over $k = \mathbb{Q}$ with or without complex multiplication. For $X > 2$ and $|T| < 1$, define the generating function

$$\rho_E(X, T) = \sum_{n=1}^{\infty} \left[\frac{\sum_{p \le X} \chi_n(g_p)}{\sum_{p \le X} 1}\right] T^{n-1} = \frac{\sum_{p \le X} \det\left[1 - \rho_E^{(2)}(\sigma_p)\, T\right]^{-1}}{\sum_{p \le X} 1}.$$

Then

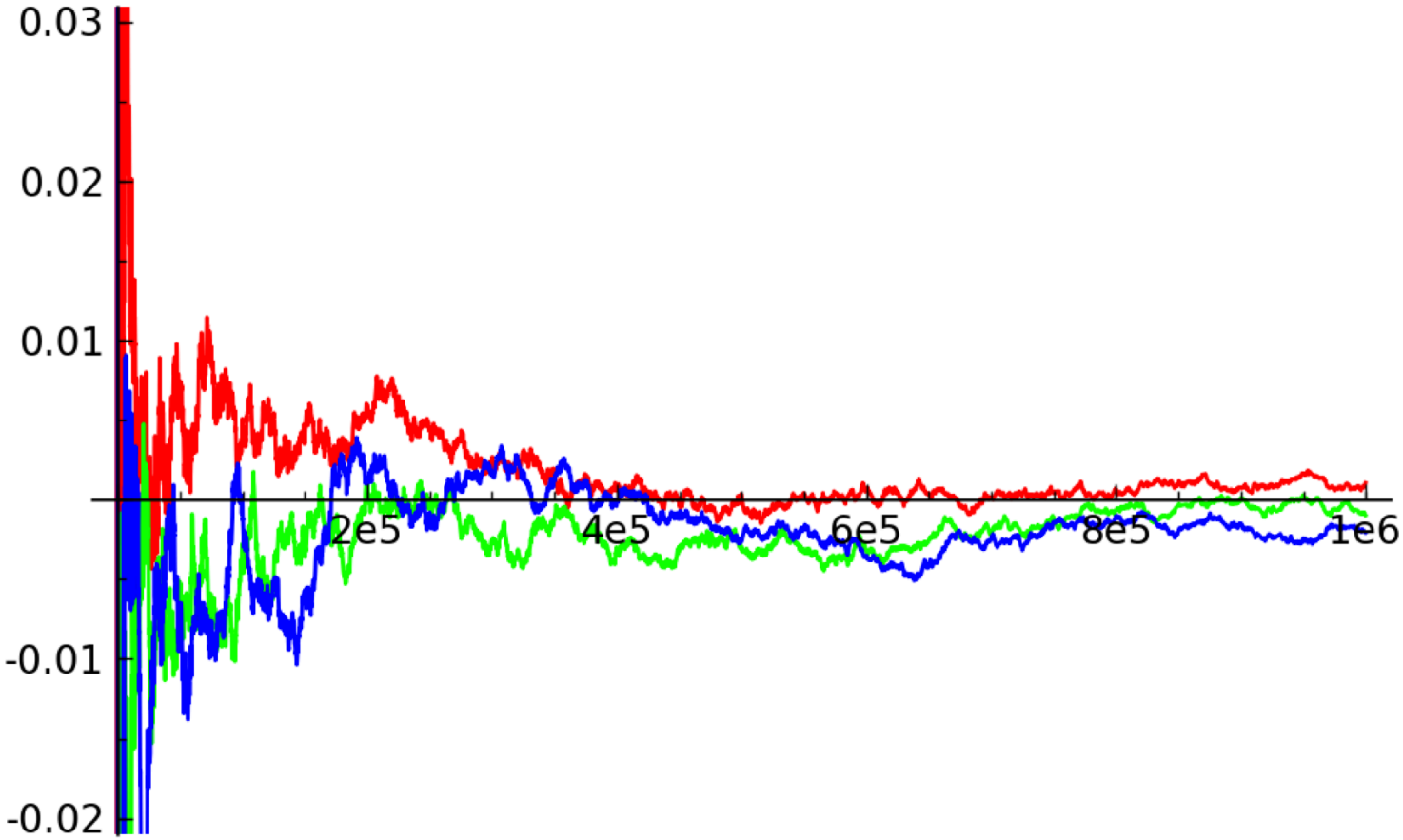
$$\lim_{X \to \infty} \rho_E(X, T) = 1 \qquad \text{uniformly for} \qquad |T| < 1.$$

$X_0(11): \; y^2 - y = x^3 - x^2 - 10\,x - 20$



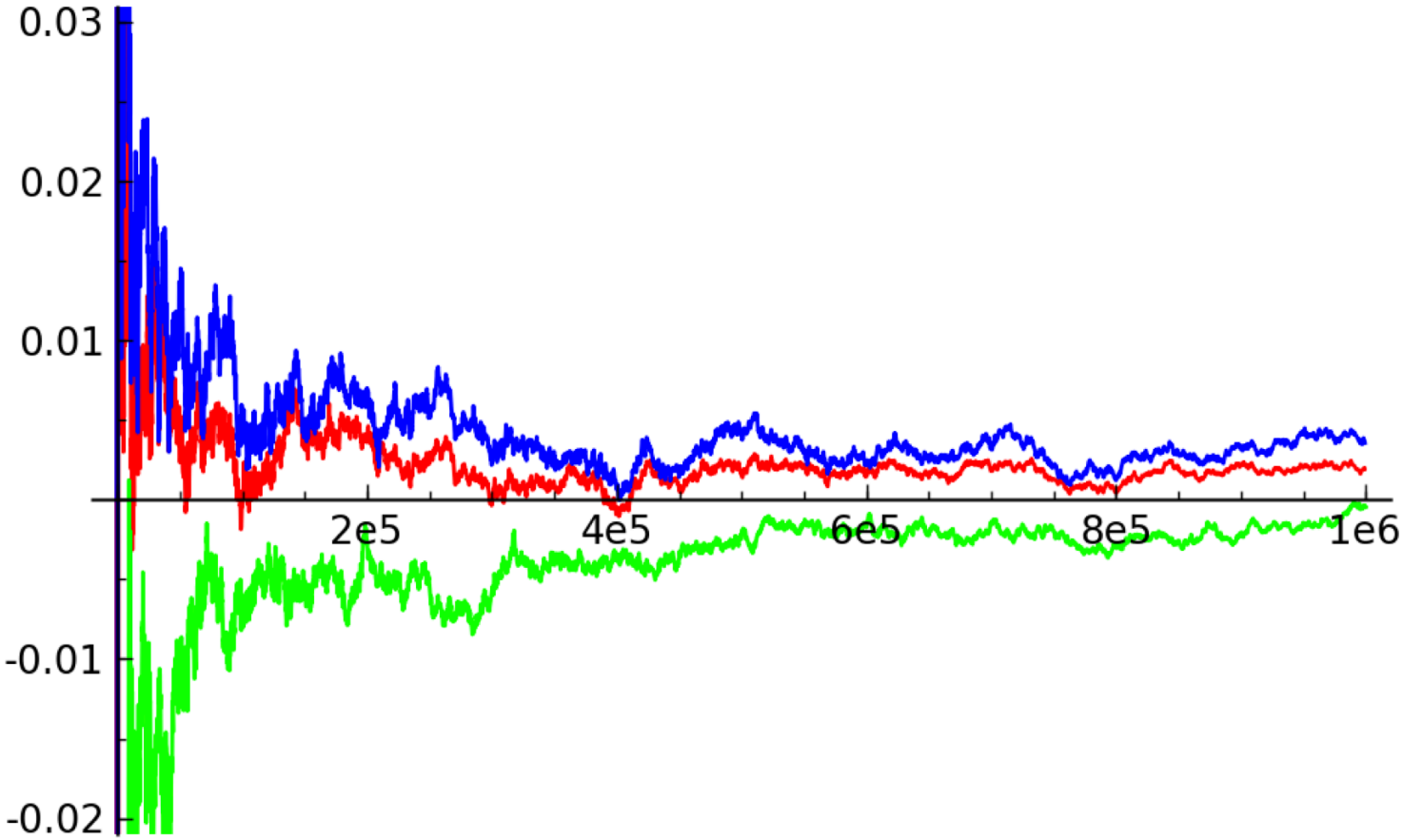
$$\frac{\sum_{p \le X} \chi_n(g_p)}{\sum_{p \le X} 1} \qquad \text{for} \qquad X \le 10^6 \qquad \text{and} \qquad n = 2,\ 3,\ 4$$

$X_0(11)/C: \; y^2 + xy + y = x^2 + x^2 - 305x + 7888$



$$\frac{\sum_{p \leq X} \chi_n(g_p)}{\sum_{p \leq X} 1} \qquad \text{for} \qquad X \leq 10^6 \qquad \text{and} \qquad n = 2, 3, 4$$

$X_0(27): \ y^2 - y = x^3 - 7$



$$\frac{\sum_{p \leq X} \chi_n(g_p)}{\sum_{p \leq X} 1} \qquad \text{for} \qquad X \leq 10^6 \qquad \text{and} \qquad n = 2, 3, 4$$

Is there another way to compute

$$\frac{\sum_{p \leq X} \chi_n(g_p)}{\sum_{p \leq X} 1}?$$

L-Functions

By considering the Taylor series expansion for $\log(1-z)$, we have

$$\log\det\left[1-\frac{\rho_E^{(n)}(\sigma_p)}{p^s}\right]=-\sum_{e=1}^{\infty}\frac{\operatorname{tr}\rho_E^{(n)}(\sigma_p^e)}{e\,p^{es}}=-\sum_{e=1}^{\infty}\frac{\chi_n(g_p^e)}{e\,p^{es}}.$$

For $\operatorname{Re}(s)>1$ we have $L(E,\operatorname{Sym}^{n-1},s)=\prod_p\det\left[1-\rho_E^{(n)}(\sigma_p)\,p^{-s}\right]^{-1}$.
The logarithmic derivative gives the expression

$$-\frac{L'(E,\operatorname{Sym}^{n-1},s)}{L(E,\operatorname{Sym}^{n-1},s)}=\sum_p\sum_{e=1}^{\infty}\frac{\chi_n(g_p^e)\,\log p}{p^{es}}=\left[\sum_p\frac{\chi_n(g_p)\,\log p}{p^s}\right]+R_E(s)$$

in terms of the uniformly bounded error term

$$R_E(s)=\sum_p\sum_{2\leq e}\frac{\chi_n(g_p^e)\,\log p}{p^{es}}\qquad\Longrightarrow\qquad\left|R_E(s)\right|\leq\frac{n}{2}\cdot\zeta\big(\operatorname{Re}(2\,s)\big).$$

Wiener-Ikehara Theorem

Theorem (Shikao Ikehara, 1931; Norbert Wiener, 1932)

Consider a function $f : [0, \infty) \to \mathbb{R}$ such that

- *f is nonnegative and nondecreasing.*
- *The following Laplace transform is convergent for $Re(s) > 1$:*

$$\big(\mathcal{L} f\big)(s) = \int_0^\infty e^{-st} f(t)\, dt.$$

- *The function $\big(\mathcal{L} f\big)(s)$ is holomorphic for $Re(s) \geq 1$ with at most a simple pole at $s = 1$.*

Then we have the limit

$$\lim_{t \to \infty} \frac{f(t)}{e^t} = \lim_{s \to 1} (s-1) \cdot \big(\mathcal{L} f\big)(s).$$

Partial Summation Formula

Corollary

Consider a Dirichlet series $L(s) = \sum_{k \geq 1} a_k \log k / k^s$, holomorphic for $\mathrm{Re}(s) \geq 1$ with at most a simple pole at $s = 1$. Then we have the limit

$$\lim_{X \to \infty} \frac{\sum_{k \leq X} a_k}{X / \log X} = \lim_{X \to \infty} \frac{\sum_{k \leq X} a_k \log k}{X} = \lim_{s \to 1} (s-1) \cdot L(s).$$

Proof: We will use the following result a couple of times.

Lemma (Niels Henrik Abel, 1826)

Let $\{f_k\}$ and $\{g_k\}$ be two sequences of complex numbers, and denote the partial sum $F(X) = \sum_{k \leq X} f_k$. Then for any positive integer N,

$$\sum_{k=1}^{N-1} f_k \, g_k = F(N-1) \, g_N + \sum_{k=1}^{N-1} F(k) \left(g_k - g_{k+1} \right).$$

Proof of Corollary

Denote $f(t) = F(e^t)$ in terms of $f_k = a_k \log k$ and $g_k = 1/k^s$:

$$(\mathcal{L}f)(s) = \int_0^\infty e^{-st} f(t)\,dt = \lim_{N\to\infty}\left[\sum_{k=1}^{N-1} F(k)\int_k^{k+1}\frac{dX}{X^{s+1}}\right]$$

$$= \lim_{N\to\infty}\frac{1}{s}\left[\sum_{k=1}^{N-1} F(k)\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)\right]$$

$$= \lim_{N\to\infty}\frac{1}{s}\left[\sum_{k=1}^{N-1}\frac{f_k}{k^s} - \frac{F(N-1)}{N^s}\right] = \frac{L(s)}{s}.$$

Upon writing $X = e^t$, we have the limits

$$\lim_{X\to\infty}\frac{\sum_{k\le X} f_k}{X} = \lim_{t\to\infty}\frac{f(t)}{e^t} = \lim_{s\to 1}(s-1)\cdot(\mathcal{L}f)(s) = \lim_{s\to 1}(s-1)\cdot L(s).$$

Proof of Corollary

Now denote $f_k = a_k \log k$ and $g_k = 1/\log k$:

$$\sum_{k=2}^{N-1} a_k = \frac{F(N-1)}{\log N} + \sum_{k=2}^{N-1} F(k)\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right)$$

$$\frac{1}{N/\log N}\left[\sum_{k=2}^{N-1} a_k\right] = \frac{F(N-1)}{N} + \frac{1}{N/\log N}\left[\sum_{k=2}^{N-1} F(k)\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right)\right]$$

We have the limits

$$\lim_{X\to\infty} \frac{\sum_{k\leq X} a_k}{X/\log X} = \lim_{X\to\infty} \frac{\sum_{k\leq X} a_k \log k}{X} = \lim_{s\to 1}(s-1)\cdot L(s).$$

Example

Consider an elliptic curve E defined over $k = \mathbb{Q}$. Define the products

$$\left.\begin{aligned} L(E, \mathrm{Sym}^{n-1}, s) &= \prod_p \det\left[1 - \rho_E^{(n)}(\sigma_p)\, p^{-s}\right]^{-1} \\ \zeta(s) &= \prod_p \left[1 - p^{-s}\right]^{-1} \end{aligned}\right\} \quad \text{for} \quad \mathrm{Re}(s) > 1.$$

Define the Dirichlet series as their logarithmic derivatives:

$$\begin{aligned} L_E(s) &= \sum_p \frac{\chi_n(g_p)\,\log p}{p^s} = -\left[\frac{L'(E, \mathrm{Sym}^{n-1}, s)}{L(E, \mathrm{Sym}^{n-1}, s)} + R_E(s)\right] \\ L_{\mathbb{P}^1}(s) &= \sum_p \frac{\log p}{p^s} = -\left[\frac{\zeta'(s)}{\zeta(s)} + R_{\mathbb{P}^1}(s)\right] \end{aligned}$$

Assuming that $\rho_E^{(n)}$ is modular, we have the identity

$$\lim_{X\to\infty} \frac{\sum_{p\le X} \chi_n(g_p)}{\sum_{p\le X} 1} = \lim_{X\to\infty} \left[\frac{\sum_{p\le X} \chi_n(g_p)}{X/\log X}\right] \Big/ \left[\frac{\sum_{p\le X} 1}{X/\log X}\right] = \frac{0}{1}.$$

Modern Statement via L-Functions

Theorem (Jean-Pierre Serre, 1967)

Consider an elliptic curve E defined over $k = \mathbb{Q}$ without complex multiplication, and denote the continuous Galois representation

$$\rho_E^{(n)} : \ Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to SU_n(\mathbb{C}) \qquad \text{which sends} \qquad \sigma_p \mapsto Sym^{n-1} g_p.$$

Assume $\rho_E^{(n)}$ is modular for all $n \geq 2$.

- *The L-series $L(E, Sym^{n-1}, s)$ is holomorphic and nonvanishing in the region $Re(s) \geq 1$.*
- *We have the limit*

$$\lim_{X \to \infty} \frac{\sum_{p \leq X} \chi_n(g_p)}{\sum_{p \leq X} 1} = 0 \qquad \text{where} \qquad \chi_n(g_p) = tr\, \rho_E^{(n)}(\sigma_p).$$

- *In particular, the Sato-Tate conjecture holds for E.*

Modern Statement via L-Functions

Conjecture

Consider an elliptic curve E defined over $k = \mathbb{Q}$ without complex multiplication. Then $\rho_E^{(n)}$ is modular for all $n \geq 2$.

What's known about this conjecture?

- $n = 2$: Equivalent to a Conjecture of Goro Shimura and Yutaka Taniyama from 1955. Partially proved by Andrew Wiles in 1994; and then completely by Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor in 2001.
- $n = 3$: Proved by Steve Gelbart and Hervé Jacquet in 1978.
- $n = 4$: Proved by Henry Kim and Freydoon Shahidi in 2002.
- $n = 5$: Proved by Henry Kim in 2003.
- n even: Proved by Laurent Clozel, Michael Harris, Nicholas Shepherd-Barron and Richard Taylor in 2006. This case suffices to prove the Sato-Tate Conjecture.

Katz-Sarnak Hueristic

Recall that $SU_2(\mathbb{C}) \simeq U_1(\mathbb{H})$.

Conjecture (Nicholas Katz and Peter Sarnak, 1999)

Say that A is an abelian variety of dimension d. Consider a "large" normalized continuous representation

$$\rho_A^{(d)} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to U_d(\mathbb{H}) \quad \text{which sends} \quad \sigma_p \mapsto g_p = \frac{1}{\sqrt{p}} \cdot \rho_{A,\ell}(\sigma_p).$$

The map $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to [-2d, 2d]$ which sends $\sigma_p \mapsto \operatorname{tr} g_p$ is a distribution. That is, there is a normalized measure μ on $U_d(\mathbb{H})$ such that for any any integrable class function $\chi : U_d(\mathbb{H}) \to \mathbb{C}$ we have the limit

$$\lim_{X \to \infty} \frac{\sum_{p \leq X} \chi(g_p)}{\sum_{p \leq X} 1} = \int_{U_d(\mathbb{H})} \chi(g)\, d\mu.$$

Questions?