Equidistribution, discrepancy, and the analytic properties of Dirichlet series

Daniel Miller

27 November 2016

Cornell University

Outline

Background

The Sato–Tate conjecture

Breaking the Akiyama–Tanigawa converse

Generalizations

Background

Elliptic curves

Equation of the form $E : y^2 = x^3 + ax + b$.

Elliptic curves

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Elliptic curves

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Elliptic curves

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Count points modulo p:

$$\#E(\mathbf{F}_p) = \#\{(x, y) \in (\mathbf{F}_p)^2 : x^2 = y^3 + ax + b\} + 1.$$

Elliptic curves

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Count points modulo p:

$$\#E(\mathbf{F}_p) = \#\{(x, y) \in (\mathbf{F}_p)^2 : x^2 = y^3 + ax + b\} + 1.$$

$+1 =$ "point at infinity."

Elliptic curves

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

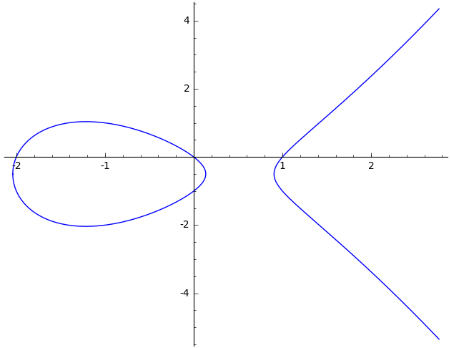
Count points modulo p:

$$\#E(\mathbf{F}_p) = \#\{(x, y) \in (\mathbf{F}_p)^2 : x^2 = y^3 + ax + b\} + 1.$$

$+1 =$ "point at infinity."

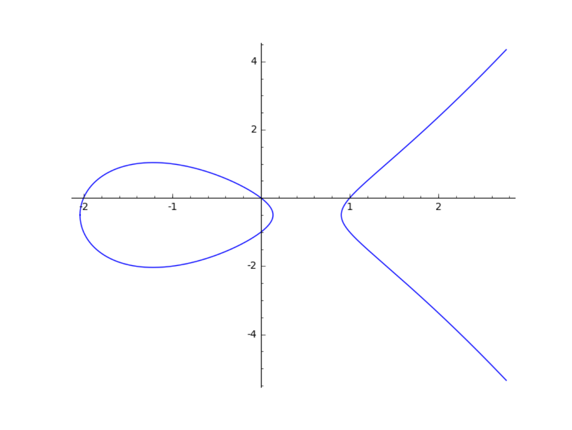
Geometric structure of $E(\mathbf{C})$

Our example



$$E : y^2 = x^3 - 3024x + 46224$$

Our example



$$E : y^2 = x^3 - 3024x + 46224$$

Where is ∞?

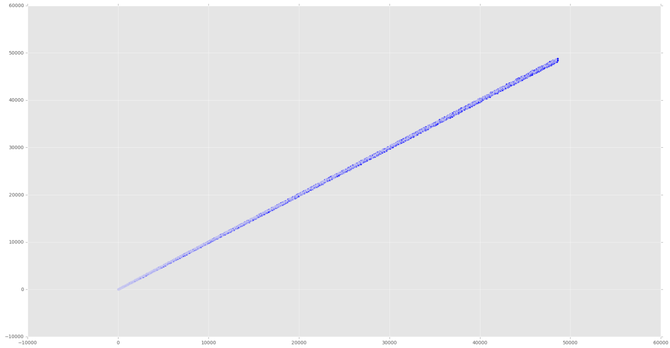
Initial data

p	2	3	5	7	11	13	...	999999929	999999937
$\#E(\mathbf{F}_p)$	1	2	3	3	8	11	...	999950222	1000031072

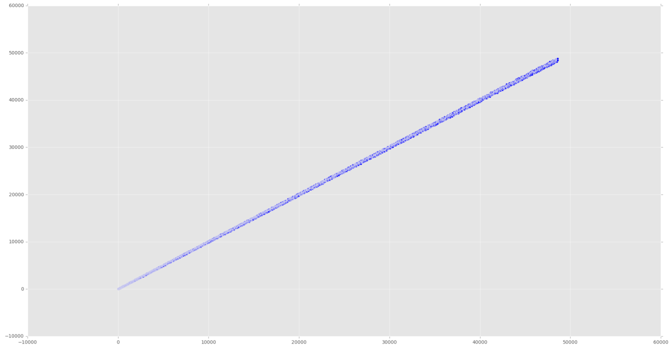
Initial data

p	2	3	5	7	11	13	$\dots$	999999929	999999937
$\#E(\mathbf{F}_p)$	1	2	3	3	8	11	$\dots$	999950222	1000031072

Look at more data...



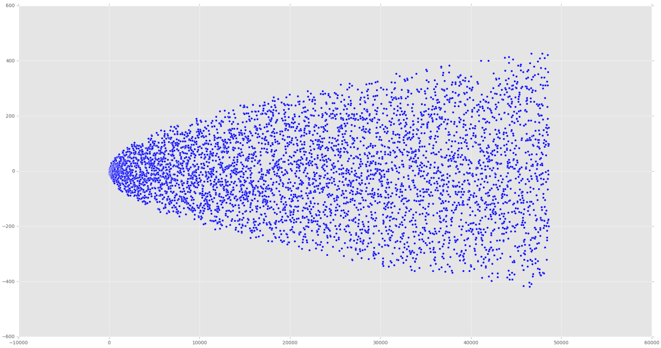
$\#E(\mathbf{F}_p)$ as a function of p.



$\#E(\mathbf{F}_p)$ as a function of p.

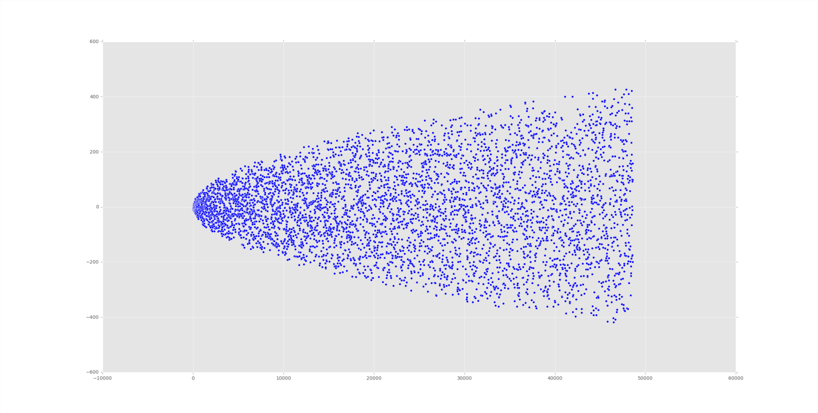
How does the error term behave?

Hasse bound



$a_p(E) := p + 1 - \#E(\mathbf{F}_p)$ as a function of p.

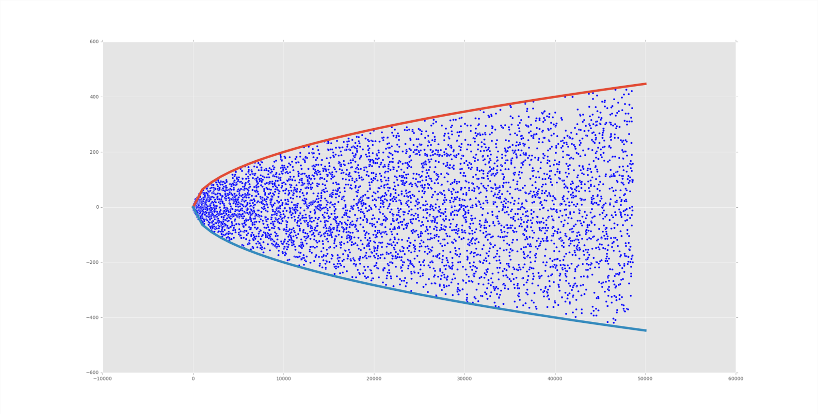
Hasse bound



$$a_p(E) := p + 1 - \#E(\mathbf{F}_p) \text{ as a function of } p.$$

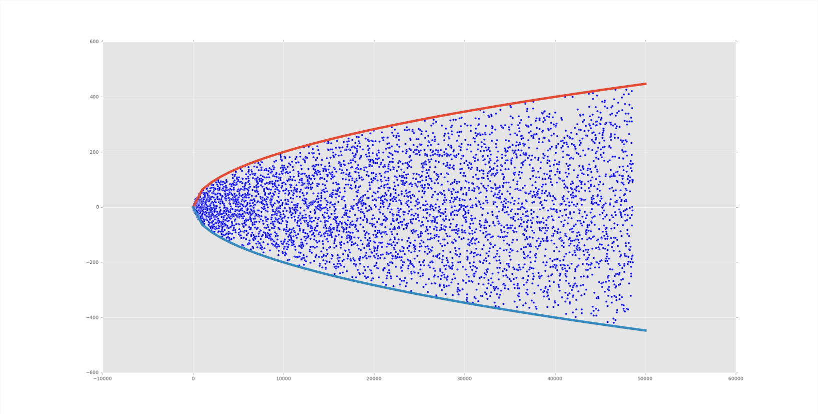
Intuition: why is a_p small? (and how small is it?)

Hasse bound



$a_p(E)$ vs. $\pm 2\sqrt{p}$.

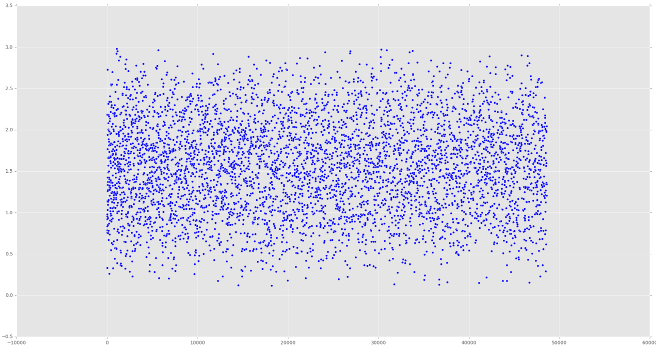
Hasse bound



$a_p(E)$ vs. $\pm 2\sqrt{p}$.

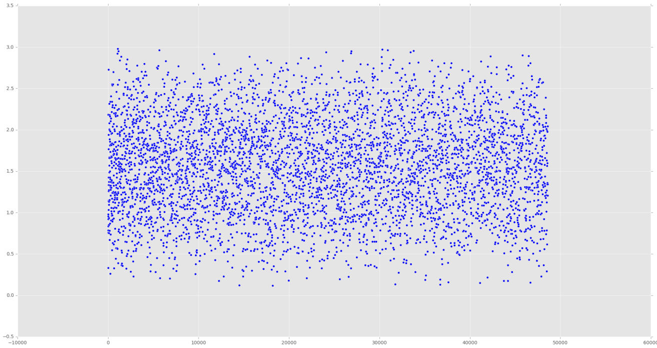
Perhaps we should normalize?

Satake parameters



$\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right)$ as a function of p.

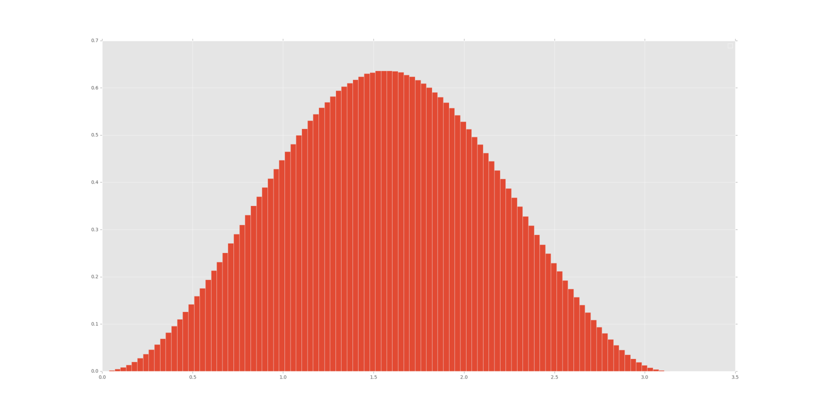
Satake parameters



$$\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right) \text{ as a function of } p.$$

Look at the statistics of $\{\theta_p\}$.

Their statistics



Histogram of $\{\theta_p\}_{p \leqslant 10^9}$.

Their statistics

Histogram with graph of $\mathrm{ST}(\theta) = \frac{2}{\pi}\sin^2(\theta)$.

Their statistics

Histogram with graph of $\mathrm{ST}(\theta) = \frac{2}{\pi}\sin^2(\theta)$.

Some kind of convergence happening. . .

The Sato–Tate conjecture

Some definitions

Two cumulative distribution functions:

$$\mathsf{cdf}_N(x) = \frac{\#\{p \leqslant N : \theta_p \leqslant x\}}{\#\{p \leqslant N\}}$$

$$\mathsf{cdf}_{\mathsf{ST}}(x) = \int_0^x \mathsf{ST}(x)\,\mathrm{d}x = \frac{x - \sin(x)\cos(x)}{\pi}$$

Some definitions

Two cumulative distribution functions:

$$\mathrm{cdf}_N(x) = \frac{\#\{p \leqslant N : \theta_p \leqslant x\}}{\#\{p \leqslant N\}}$$

$$\mathrm{cdf}_{\mathrm{ST}}(x) = \int_0^x \mathrm{ST}(x)\,\mathrm{d}x = \frac{x - \sin(x)\cos(x)}{\pi}$$

Discrepancy

$$\mathrm{disc}_E(N) = \sup_{0 \leqslant x \leqslant \pi} |\,\mathrm{cdf}_N(x) - \mathrm{cdf}_{\mathrm{ST}}(x)|.$$

Some definitions

Two cumulative distribution functions:

$$\mathrm{cdf}_N(x) = \frac{\#\{p \leqslant N : \theta_p \leqslant x\}}{\#\{p \leqslant N\}}$$

$$\mathrm{cdf}_{\mathrm{ST}}(x) = \int_0^x \mathrm{ST}(x)\,\mathrm{d}x = \frac{x - \sin(x)\cos(x)}{\pi}$$

Discrepancy

$$\mathrm{disc}_E(N) = \sup_{0 \leqslant x \leqslant \pi} |\,\mathrm{cdf}_N(x) - \mathrm{cdf}_{\mathrm{ST}}(x)|.$$

Other ways to measure distabce between distributions?

A deep theorem

Theorem (Sato–Tate)
For any elliptic curve E, $\mathrm{disc}_E(N) \to 0$ as $N \to \infty$.

A deep theorem

Theorem (Sato–Tate)

For any elliptic curve E, $\mathrm{disc}_E(N) \to 0$ *as* $N \to \infty$.

Conjecture (Akiyama–Tanigawa)

For any elliptic curve E, $\mathrm{disc}_E(N) = O_E(N^{-\frac{1}{2}+\epsilon})$.

A deep theorem

Theorem (Sato–Tate)

For any elliptic curve E, $\mathrm{disc}_E(N) \to 0$ as $N \to \infty$.

Conjecture (Akiyama–Tanigawa)

For any elliptic curve E, $\mathrm{disc}_E(N) = O_E(N^{-\frac{1}{2}+\epsilon})$.

Theorem

The Akiyama–Tanigawa conjecture implies the Riemann Hypothesis (for the elliptic curve).

A deep theorem

Theorem (Sato–Tate)

For any elliptic curve E, $\mathrm{disc}_E(N) \to 0$ as $N \to \infty$.

Conjecture (Akiyama–Tanigawa)

For any elliptic curve E, $\mathrm{disc}_E(N) = O_E(N^{-\frac{1}{2}+\epsilon})$.

Theorem

The Akiyama–Tanigawa conjecture implies the Riemann Hypothesis (for the elliptic curve).

Key idea: Koksma–Hlawka inequality.

Some L-functions

Definition (Riemann zeta function)

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \sum_{n\geqslant 1} \frac{1}{n^s}$$

Some L-functions

Definition (Riemann zeta function)

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}} = \sum_{n \geqslant 1} \frac{1}{n^s}$$

Definition (L-function of elliptic curve)

$$L(E, s) = \prod_p \frac{1}{(1 - e^{i\theta_p} p^{-s})(1 - e^{-i\theta_p} p^{-s})}$$

Some L-functions

Definition (Riemann zeta function)

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \sum_{n \geqslant 1} \frac{1}{n^s}$$

Definition (L-function of elliptic curve)

$$L(E,s) = \prod_p \frac{1}{(1-e^{i\theta_p}p^{-s})(1-e^{-i\theta_p}p^{-s})}$$

Definition (strange Dirichlet series)

$$L_f(E,s) = \prod_p \frac{1}{1-f(\theta_p)p^{-s}}$$

Some L-functions

Definition (Riemann zeta function)

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}} = \sum_{n \geqslant 1} \frac{1}{n^s}$$

Definition (L-function of elliptic curve)

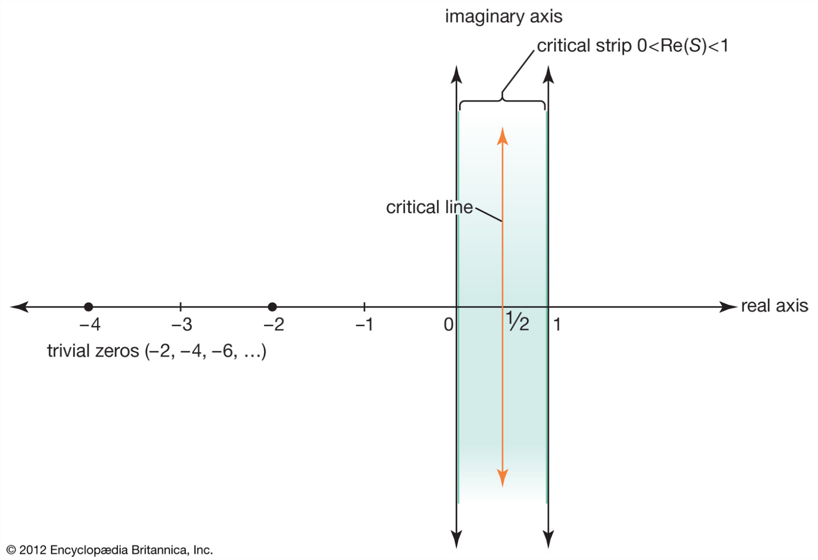
$$L(E, s) = \prod_p \frac{1}{(1 - e^{i\theta_p} p^{-s})(1 - e^{-i\theta_p} p^{-s})}$$

Definition (strange Dirichlet series)

$$L_f(E, s) = \prod_p \frac{1}{1 - f(\theta_p) p^{-s}}$$

(Standing assumption: $\int f \cdot \mathrm{ST} = 0$.)

L-functions on the complex plane



Intuition for Akiyama–Tanigawa conjecture

A–T for Riemann zeta function:

$$\left|\#\{p \leqslant N\} - \int_0^x \frac{t}{\log t}\,\mathrm{d}t\right| = O(\sqrt{N})$$

Intuition for Akiyama–Tanigawa conjecture

A–T for Riemann zeta function:

$$\left|\#\{p \leqslant N\} - \int_0^x \frac{t}{\log t}\,\mathrm{d}t\right| = O(\sqrt{N})$$

(Equivalent to Riemann Hypothesis.)

Intuition for Akiyama–Tanigawa conjecture

A–T for Riemann zeta function:

$$\left| \#\{p \leqslant N\} - \int_0^x \frac{t}{\log t}\,\mathrm{d}t \right| = O(\sqrt{N})$$

(Equivalent to Riemann Hypothesis.)

A–T for elliptic curves implies:

$$\left| \sum_{p \leqslant N} f(\theta_p) \right| = O_f(N^{\frac{1}{2}})$$

Intuition for Akiyama–Tanigawa conjecture

A–T for Riemann zeta function:

$$\left|\#\{p \leqslant N\} - \int_0^x \frac{t}{\log t}\,\mathrm{d}t\right| = O(\sqrt{N})$$

(Equivalent to Riemann Hypothesis.)

A–T for elliptic curves implies:

$$\left|\sum_{p \leqslant N} f(\theta_p)\right| = O_f(N^{\frac{1}{2}})$$

A–T $\Rightarrow$ RH.

Intuition for Akiyama–Tanigawa conjecture

A–T for Riemann zeta function:

$$\left|\#\{p \leqslant N\} - \int_0^x \frac{t}{\log t}\,\mathrm{d}t\right| = O(\sqrt{N})$$

(Equivalent to Riemann Hypothesis.)

A–T for elliptic curves implies:

$$\left|\sum_{p \leqslant N} f(\theta_p)\right| = O_f(N^{\frac{1}{2}})$$

A–T $\Rightarrow$ RH. Is the converse true?

Intuition for Akiyama–Tanigawa conjecture

A–T for Riemann zeta function:

$$\left|\#\{p \leqslant N\} - \int_0^x \frac{t}{\log t}\,\mathrm{d}t\right| = O(\sqrt{N})$$

(Equivalent to Riemann Hypothesis.)

A–T for elliptic curves implies:

$$\left|\sum_{p \leqslant N} f(\theta_p)\right| = O_f(N^{\frac{1}{2}})$$

A–T $\Rightarrow$ RH. Is the converse true? No!

Breaking the Akiyama–Tanigawa converse

What is needed?

Construct a sequence $\{\theta_p\}$ such that

1. Sums of the form $\sum_{p \leqslant N} f(\theta_p)$ have "good bounds" like $O(\sqrt{N})$.

What is needed?

Construct a sequence $\{\theta_p\}$ such that

1. Sums of the form $\sum_{p \leqslant N} f(\theta_p)$ have "good bounds" like $O(\sqrt{N})$.
2. The discrepancy $\mathrm{disc}_{\{\theta_p\}}(N)$ is *not* $O(N^{-\frac{1}{2}})$.

Key idea

Choose an angle θ, and let let $\theta_n = n\theta \mod \pi$. Then

$$\left|\sum_{n\leqslant N} e^{2\pi i m\theta_n}\right| = O\left(\frac{1}{|e^{2\pi i\theta} - 1|}\right)$$

Key idea

Choose an angle θ, and let let $\theta_n = n\theta \mod \pi$. Then

$$\left|\sum_{n\leqslant N} e^{2\pi i m\theta_n}\right| = O\left(\frac{1}{|e^{2\pi i\theta} - 1|}\right)$$

Right-hand-side doesn't depend on N.

Key idea

Choose an angle θ, and let let $\theta_n = n\theta \mod \pi$. Then

$$\left|\sum_{n \leqslant N} e^{2\pi i m \theta_n}\right| = O\left(\frac{1}{|e^{2\pi i\theta} - 1|}\right)$$

Right-hand-side doesn't depend on N.

Corollary

If f is a smooth function, then

$$\left|\sum_{n \leqslant N} f(\theta_n)\right| = O_f(1).$$

Two degrees of freedom

If $\theta_{p_n} = n\theta$, then

$$L_f(s) = \prod_p \frac{1}{1 - f(\theta_p)p^{-s}}$$

satisfies Riemann Hypothesis.

Two degrees of freedom

If $\theta_{p_n} = n\theta$, then

$$L_f(s) = \prod_p \frac{1}{1 - f(\theta_p)p^{-s}}$$

satisfies Riemann Hypothesis.

Also, we can control the discrepancy of the sequence $\{\theta_p\}$ via an *irrationality exponent*.

Diophantine approximation

Definition

The *irrationality exponent* of x is the largest η such that

$$\left| x - \frac{p}{q} \right| < q^{-\eta}$$

for infinitely many p/q.

Diophantine approximation

Definition

The *irrationality exponent* of x is the largest η such that

$$\left| x - \frac{p}{q} \right| < q^{-\eta}$$

for infinitely many p/q.

Theorem (Thue–Siegel–Roth)

If x is algebraic but not rational (e.g. $\sqrt{2}$), then it has irrationality exponent 2.

Diophantine approximation

Definition

The *irrationality exponent* of x is the largest η such that

$$\left| x - \frac{p}{q} \right| < q^{-\eta}$$

for infinitely many p/q.

Theorem (Thue–Siegel–Roth)

If x is algebraic but not rational (e.g. $\sqrt{2}$), then it has irrationality exponent 2.

Theorem

There are x with arbitrary irrationality exponent > 2.

Putting things together

Theorem

For any $\eta \in (-1/2, 0)$, *there exists a sequence* $\{\theta_p\}$ *such that*

$$L(\{\theta_p\}, s) = \prod_p \frac{1}{(1 - e^{i\theta_p} p^{-s})(1 - e^{-i\theta_p} p^{-s})}$$

satisfies the Riemann Hypothesis, but for which

$$\mathrm{disc}_{\{\theta_p\}}(N) \neq O(N^\eta).$$

Putting things together

Theorem

For any $\eta \in (-1/2, 0)$, there exists a sequence $\{\theta_p\}$ such that

$$L(\{\theta_p\}, s) = \prod_p \frac{1}{(1 - e^{i\theta_p} p^{-s})(1 - e^{-i\theta_p} p^{-s})}$$

satisfies the Riemann Hypothesis, but for which

$$\mathrm{disc}_{\{\theta_p\}}(N) \neq O(N^\eta).$$

Problem: this sequence $\{\theta_p\}$ is uniformly distributed, not ST-distributed.

Inverse inverse sampling transform

If $\tilde{\theta}_p = \mathrm{cdf}_{\mathrm{ST}}^{-1}(\theta_p)$, then $\{\tilde{\theta}_p\}$ is ST-distributed.

Inverse inverse sampling transform

If $\tilde{\theta}_p = \mathrm{cdf}_{\mathrm{ST}}^{-1}(\theta_p)$, then $\{\tilde{\theta}_p\}$ is ST-distributed.

Also $\mathrm{cdf}_{\mathrm{ST}}^{-1}$ preserves discrepancy of sequences.

Inverse inverse sampling transform

If $\tilde{\theta}_p = \mathrm{cdf}_{\mathrm{ST}}^{-1}(\theta_p)$, then $\{\tilde{\theta}_p\}$ is ST-distributed.

Also $\mathrm{cdf}_{\mathrm{ST}}^{-1}$ preserves discrepancy of sequences.

Tricky part: show that Riemann Hypothesis holds for $\{\tilde{\theta}_p\}$.

Inverse inverse sampling transform

If $\tilde{\theta}_p = \mathrm{cdf}_{\mathsf{ST}}^{-1}(\theta_p)$, then $\{\tilde{\theta}_p\}$ is ST-distributed.

Also $\mathrm{cdf}_{\mathsf{ST}}^{-1}$ preserves discrepancy of sequences.

Tricky part: show that Riemann Hypothesis holds for $\{\tilde{\theta}_p\}$.

Problem: the $\tilde{\theta}_p$ don't come from integral a_p.

Inverse inverse sampling transform

If $\tilde{\theta}_p = \mathrm{cdf}_{\mathrm{ST}}^{-1}(\theta_p)$, then $\{\tilde{\theta}_p\}$ is ST-distributed.

Also $\mathrm{cdf}_{\mathrm{ST}}^{-1}$ preserves discrepancy of sequences.

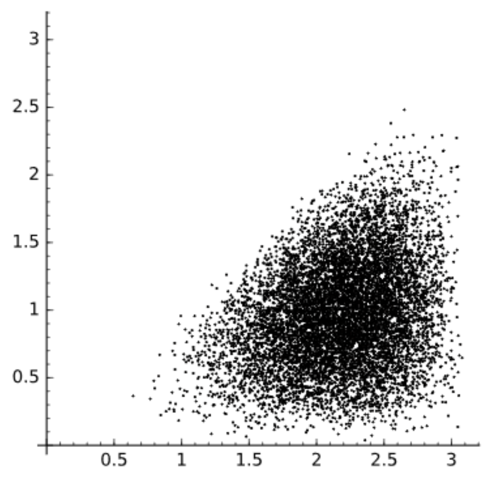
Tricky part: show that Riemann Hypothesis holds for $\{\tilde{\theta}_p\}$.

Problem: the $\tilde{\theta}_p$ don't come from integral a_p.

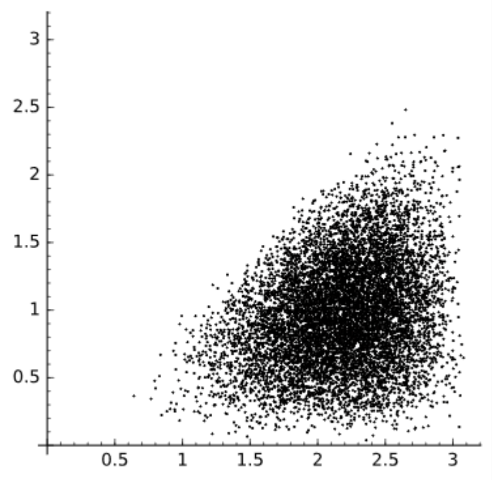
Solution: tweak them so they do, then prove everything still works.

Generalizations

From $y^2 = x^3 + ax + b$ to $y^2 = x^5 - 1$:



From $y^2 = x^3 + ax + b$ to $y^2 = x^5 - 1$:



Higher-dimensional counterexamples, Galois representations.

Questions?

Further reading

S. Akiyama and Y. Tanigawa. Calculation of values of L-functions associated to elliptic curves. *Math. Comp.*, 68(227):1201–1231, 1999.

Y. Bugeaud. Diophantine approximation and Cantor sets. *Math. Ann.*, 341(3):677–684, 2008.

L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience, 1974.

M. Laurent. On transfer inequalities in Diophantine approximation. In *Analytic number theory*, pages 306–314. Cambridge Univ. Press, 2009.

B. Polyak. Convexity of nonlinear image of a small ball with applications to optimization. *Set-Valued Anal.*, 9(1–2):159–168, 2001.