The statistical behavior of modular symbols and arithmetic conjectures

Barry Mazur, Harvard University; Karl Rubin, UC Irvine

Toronto, November 2016

Congratulations Manjul!

The geometry of numbers was initially developed by Hermann Minkowski.

Thanks to Manjul's extraordinary work, and his vision of what one might call a two-tiered geometry of numbers,

we have recently seen so many important breakthroughs in what one might call, broadly, arithmetic statistics.

Statistics for ranks of Mordell-Weil groups

In an appreciation of Manjul's results on ranks of Mordell-Weil groups of elliptic curves over $\mathbb{Q}$ this lecture will be an account of an experimental study

—work in progress with Karl Rubin—

that leads us to make conjectures about ranks of Mordell-Weil groups over a range of 'large' (number) fields.

Growth of ranks in abelian extensions

Fix an abelian variety A over a number field K.

Question

As L runs through abelian extensions of K, how often is $\mathrm{rank}(A(L)) > \mathrm{rank}(A(K))$?

Growth of ranks in abelian extensions

Fix an abelian variety A over a number field K.

Question

As L runs through abelian extensions of K, how often is $\mathrm{rank}(A(L)) > \mathrm{rank}(A(K))$*?*

By considering the action of $\mathrm{Gal}(L/K)$ on $A(L) \otimes \mathbb{Q}$, the representation theory of $\mathbb{Q}[\mathrm{Gal}(L/K)]$ shows that:

Growth of ranks in abelian extensions

Fix an abelian variety A over a number field K.

Question

As L runs through abelian extensions of K, how often is $\mathrm{rank}(A(L)) > \mathrm{rank}(A(K))$?

By considering the action of $\mathrm{Gal}(L/K)$ on $A(L) \otimes \mathbb{Q}$, the representation theory of $\mathbb{Q}[\mathrm{Gal}(L/K)]$ shows that:

- it is enough to consider the case where L/K is cyclic,

Growth of ranks in abelian extensions

Fix an abelian variety A over a number field K.

Question

As L runs through abelian extensions of K, how often is $\mathrm{rank}(A(L)) > \mathrm{rank}(A(K))$*?*

By considering the action of $\mathrm{Gal}(L/K)$ on $A(L) \otimes \mathbb{Q}$, the representation theory of $\mathbb{Q}[\mathrm{Gal}(L/K)]$ shows that:

- it is enough to consider the case where L/K is cyclic,
- if (for example) L/K is cyclic of prime degree p then

$$\mathrm{rank}(A(L)) > \mathrm{rank}(A(K)) \Longrightarrow \mathrm{rank}(A(L)) \geq \mathrm{rank}(A(K)) + (p-1).$$

Birch-Swinnerton-Dyer Conjecturally equivalent: the vanishing of a special value of an L-function

If L/K is cyclic of prime degree p and if $\chi : \mathrm{Gal}(L/K) \hookrightarrow \mathbb{C}^*$ is any faithful character of its Galois group, then

$$\mathrm{rank}(A(L)) > \mathrm{rank}(A(K)) \quad \overset{?}{\Leftrightarrow} \quad L(A_{/K}, \chi; 1) = 0.$$

Growth of ranks in abelian extensions: a recent 'vertical' theorem

Theorem

(Kato, Rohrlich) Let M be any abelian extension of $\mathbb{Q}$ unramified outside a finite set of primes S.
If E is an elliptic curve over $\mathbb{Q}$, the Mordell-Weil group $E(M)$ is finitely generated.

A 'weak' horizontal theorem for abelian varieties of general dimension:

Theorem (M-R)

Let A be a simple abelian variety over K, a number field. Suppose that all endomorphisms of A are defined over K.

Then there is a set $\mathcal{P}$ of primes of positive density, such that for all integers $n \geq 1$ and $p \in \mathcal{P}$, there are infinitely many cyclic extensions L/K of degree p^n such that $A(L) = A(K)$.

Might this also be true for all prime numbers $p \gg_{K,\mathrm{dim(A)}} 0$ and—for each n, for a density 1 collection of cyclic degree p^n extensions L/K?

Growth of ranks in cyclic (Galois) extensions; 'horizontal' conjectures

Let $L/\mathbb{Q}$ be a finite cyclic extension of degree p, and m the absolute value of its conductor. Put:

$$M_p(X) := \#\{L/\mathbb{Q} \text{ cyclic of degree } p;\ m < X\},$$

(Note: $\log M_p(X) \sim \log(X)$.)

Growth of ranks in cyclic (Galois) extensions; 'horizontal' conjectures

Let $L/\mathbb{Q}$ be a finite cyclic extension of degree p, and m the absolute value of its conductor. Put:

$$M_p(X) := \#\{L/\mathbb{Q} \text{ cyclic of degree } p;\ m < X\},$$

(Note: $\log M_p(X) \sim \log(X)$.)

$$N_{E,p}(X) = N_p(X) := \#\{L/\mathbb{Q} \text{ cyclic of degree } p;\ m < X,$$

and

$$E(L) \neq E(\mathbb{Q})\}.$$

Growth of ranks in cyclic extensions; 'horizontal' conjectures

Conjecture (David-Fearnley-Kisilevsky)

1. $\log N_2(X) \sim \log(X)$ *(follows from standard conjectures),*
2. $\log N_3(X) \sim \frac{1}{2}\log(X)$,

Growth of ranks in cyclic extensions; 'horizontal' conjectures

Conjecture (David-Fearnley-Kisilevsky)

1. $\log N_2(X) \sim \log(X)$ *(follows from standard conjectures)*,
2. $\log N_3(X) \sim \frac{1}{2}\log(X)$,

(See the beautiful paper: Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves by Fearnley, Kisilevsky and Kuwata)

Growth of ranks in cyclic extensions; 'horizontal' conjectures

Conjecture (David-Fearnley-Kisilevsky)

1. $\log N_2(X) \sim \log(X)$ *(follows from standard conjectures),*
2. $\log N_3(X) \sim \frac{1}{2}\log(X)$,

   (See the beautiful paper: Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves by Fearnley, Kisilevsky and Kuwata)

3. $\log N_5(X) = o(\log(X))$ *but* $N_5(X)$ *is unbounded,*
4. $N_p(X)$ *is bounded if* p *is a prime,* $p \geq 7$*.*

Mention motivation: random matrix heuristics

Growth of ranks for elliptic curves: the analytic approach

Question

As L runs through cyclic extensions of K, how often is $\mathrm{rank}(E(L)) > \mathrm{rank}(E(K))$*?*

Using the Birch & Swinnerton-Dyer conjecture, this is equivalent to the following:

Question

As χ runs through characters of $\mathrm{Gal}(\bar{K}/K)$, how often is $L(E, \chi, 1) = 0$*?*

When $K = \mathbb{Q}$ (which we assume until further notice), this leads to a study of modular symbols.

Vertical line integrals

Let E be an elliptic curve over $\mathbb{Q}$ and

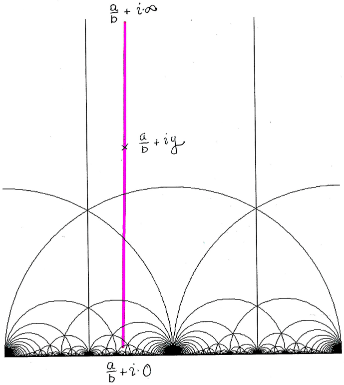
$$f_E(z)dz = \sum_{\nu=1}^{\infty} a_\nu e^{2\pi i \nu z} dz$$

the modular form attached to E, viewed as differential form on the upper-half plane.

For any rational number $r = a/b$, form the integral

$$2\pi i \int_{r+i\cdot 0}^{r+i\cdot\infty} f_E(z)dz.$$

Integrating over vertical lines in the upper half-plane



Raw modular symbols

Symmetrize or anti-symmetrize to define **raw $(\pm)$ modular symbol** attached to the rational number r:

$$\langle r\rangle_E^{\pm} := \pi i\left(\int_{i\infty}^{r} f_E(z)dz \pm \int_{i\infty}^{-r} f_E(z)dz\right)$$

Raw modular symbols

Symmetrize or anti-symmetrize to define **raw** $(\pm)$ **modular symbol** attached to the rational number r:

$$\langle r\rangle_E^{\pm} := \pi i\left(\int_{i\infty}^{r} f_E(z)dz \pm \int_{i\infty}^{-r} f_E(z)dz\right)$$

The raw modular symbols $\langle r\rangle_E^{\pm}$ take values in the discrete subgroup of $\mathbb{R}$ generated by $\frac{1}{D}\Omega_E^{\pm}$ for some positive D.

L-functions and modular symbols

Theorem

For every primitive even Dirichlet character χ of conductor m,

$$\sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\langle a/m \rangle_E^{\pm} = \tau(\chi) L(E, \bar{\chi}, 1).$$

Here $\tau(\chi)$ is the Gauss sum, and the sign in $\langle a/m \rangle_E^{\pm}$ is the sign of the character χ.

Dirichlet characters as Galois characters

For a cyclic extension $L/\mathbb{Q}$ of conductor m we have a canonical surjection

$$\begin{array}{ccccc} (\mathbb{Z}/m\mathbb{Z})^\times & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q}) & \twoheadrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ a & \longmapsto & & & \sigma_a. \end{array}$$

which allows us to think of Dirichlet characters as Galois characters.

Theta-elements

For $g \in \mathrm{Gal}(L/\mathbb{Q})$ define the **Theta-coefficient**

$$c^{\pm}_{E,g} = c^{\pm}_{g} := \sum_{a \,:\, \sigma_a = g} \langle a/m \rangle^{\pm}_{E},$$

Theta-elements

For $g \in \mathrm{Gal}(L/\mathbb{Q})$ define the **Theta-coefficient**

$$c^{\pm}_{E,g} = c^{\pm}_{g} := \sum_{a\,:\,\sigma_a = g} \langle a/m \rangle^{\pm}_{E},$$

and the **Theta-element**

$$\theta^{\pm}_{L} := \sum_{g \in \mathrm{Gal}(L/\mathbb{Q})} c^{\pm}_{g}[g] \in \mathbb{R}[\mathrm{Gal}(L/\mathbb{Q})].$$

Vanishing of the special value of L-functions and 'Theta-elements'

One has:

$$L(E,\chi,1)=0 \iff \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\langle a/m\rangle^{\mathrm{sign}(\chi)} = 0$$

$$\iff \sum_{g\in\mathrm{Gal}(L/\mathbb{Q})} \chi(g) c_g^{\mathrm{sign}(\chi)} = 0$$

$$\iff \chi\left(\theta_L^{\mathrm{sign}(\chi)}\right) = 0$$

Statistics for raw modular symbols, Theta-coefficients, and the vanishing of $L(E, \chi, 1)$

We are interested in the values of

- the raw modular symbols $\langle a/m \rangle_E^{\pm}$,
- the Theta-coefficients $c_g^{\mathrm{sign}(\chi)}$, and use our computational exploration to conjecture how often

$$L(E, \chi, 1) = 0.$$

Statistics for raw modular symbols, Theta-coefficients, and the vanishing of $L(E, \chi, 1)$

The fundamental theorem is by Yiannis Petridis and Morten Risager:

Modular symbols have a normal distribution, Geometric and Functional Analysis (2004) no. 5 1013-1043

which makes use of Eisenstein series twisted by modular symbols, introduced by Dorian Goldfeld.

Our discussion about modular symbol statistics will be a computational addendum to this work.

Relations satisfied by the (raw) modular symbols

Let N be the conductor of E. For every $r \in \mathbb{Q}$, modular symbols satisfy the relations:

Relations satisfied by the (raw) modular symbols

Let N be the conductor of E. For every $r \in \mathbb{Q}$, modular symbols satisfy the relations:

- $\boxed{\langle r \rangle_E^{\pm} = \langle r+1 \rangle_E^{\pm}}$ since $f_E(z) = f_E(z+1)$

Relations satisfied by the (raw) modular symbols

Let N be the conductor of E. For every $r \in \mathbb{Q}$, modular symbols satisfy the relations:

- $\boxed{\langle r \rangle_E^{\pm} = \langle r+1 \rangle_E^{\pm}}$ since $f_E(z) = f_E(z+1)$
- $\boxed{\langle r \rangle_E^{\pm} = \pm\langle -r \rangle_E^{\pm}}$ by definition

Relations satisfied by the (raw) modular symbols

Let N be the conductor of E. For every $r \in \mathbb{Q}$, modular symbols satisfy the relations:

- $\boxed{\langle r \rangle_E^{\pm} = \langle r+1 \rangle_E^{\pm}}$ since $f_E(z) = f_E(z+1)$
- $\boxed{\langle r \rangle_E^{\pm} = \pm \langle -r \rangle_E^{\pm}}$ by definition
- Atkin-Lehner relation: if w_E is the global root number of E, and $aa'N \equiv 1 \pmod{m}$, then $\boxed{\langle a'/m \rangle_E^{\pm} = w_E \cdot \langle a/m \rangle_E^{\pm}}$

Relations satisfied by the (raw) modular symbols

Let N be the conductor of E. For every $r \in \mathbb{Q}$, modular symbols satisfy the relations:

- $\boxed{\langle r\rangle_E^{\pm} = \langle r+1\rangle_E^{\pm}}$ since $f_E(z) = f_E(z+1)$
- $\boxed{\langle r\rangle_E^{\pm} = \pm\langle -r\rangle_E^{\pm}}$ by definition
- Atkin-Lehner relation: if w_E is the global root number of E, and $aa'N \equiv 1 \pmod{m}$, then $\boxed{\langle a'/m\rangle_E^{\pm} = w_E \cdot \langle a/m\rangle_E^{\pm}}$
- Hecke relation: if a prime $\ell \nmid N$ and a_ℓ is the ℓ-th Fourier coefficient of f_E, then $\boxed{a_\ell \cdot \langle r\rangle_E^{\pm} = \langle \ell r\rangle_E^{\pm} + \sum_{i=0}^{\ell-1} \langle (r+i)/\ell\rangle_E^{\pm}}$

Conjectural *regularities* in the modular symbols data

To start, it is worth noting some significant *regularities* in the values of modular symbols.

For example, consider the behavior of contiguous sums of the modular symbol:

Conjectural *regularities* in the modular symbols data

To start, it is worth noting some significant *regularities* in the values of modular symbols.

For example, consider the behavior of contiguous sums of the modular symbol:

For $0 \leq x \leq 1$, let

$$G^{\pm}_{E,m}(x) := \frac{1}{m} \sum_{a=0}^{\lfloor mx \rfloor} \langle \frac{a}{m} \rangle^{\pm}_{E}$$

Conjectural *regularities* in the modular symbols data

And consider these continuous functions for $0 \leq x \leq 1$,

$$g_E^+(x) := \frac{1}{2\pi i} \sum_{\nu=1}^{\infty} \frac{a_\nu}{\nu^2} \sin(\pi \nu x),$$

$$g_E^-(x) := \frac{1}{2\pi i} \sum_{\nu=1}^{\infty} \frac{a_\nu}{\nu^2} \cos(\pi \nu x).$$

Conjectural *regularities* in the modular symbols data

Conjecture

(Karl Rubin, William Stein, me)

$$G_E^{\pm}(x) := \lim_{m\to\infty} G_{E,m}^{\pm}(x) \quad \stackrel{??}{=} \quad g_E^{\pm}(x).$$

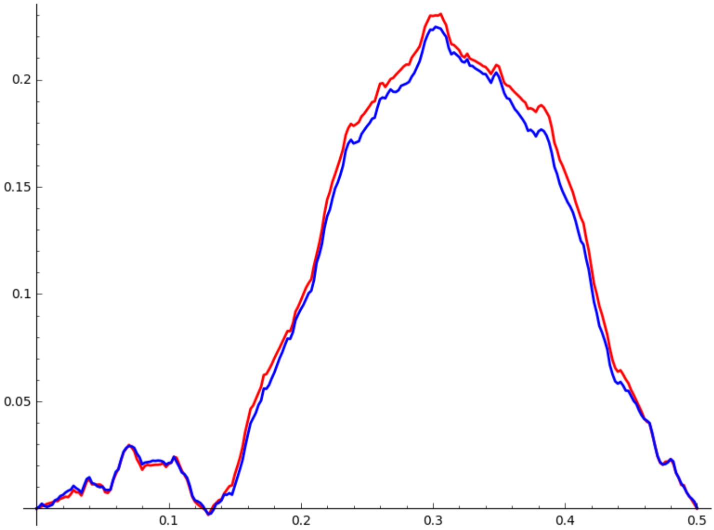
Computational Evidence

For example, for the elliptic curve $E = 11a$, the following three pictures are the graphs of

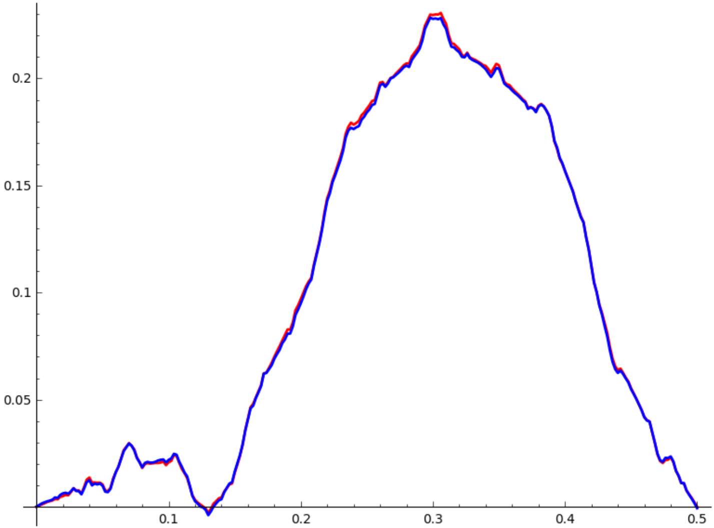
- $G_{E,m}$, in blue, with $m = 1009, 10007$, and 100003 respectively,
- superimposed on the graph of $g_E(x)$, in red.

For the last picture the superposition is so accurate, we don't see the red at all, in the pictures.

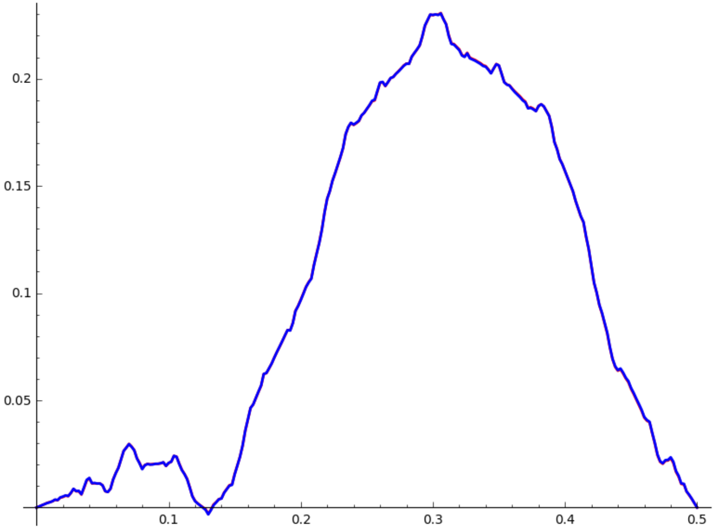
$G_{E,m}$ with $m = 1009$



$G_{E,m}$ with $m = 10007$



$G_{E,m}$ with $m = 100003$



The motivation for this conjecture: a conjectural commutation of two limits

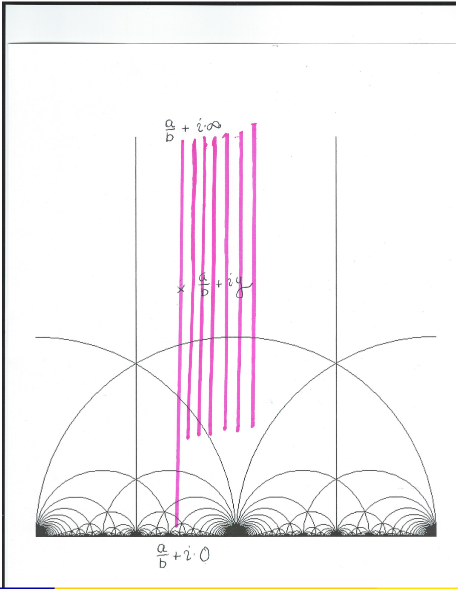
For $\delta > 0$ and any real number r, define the **raw δ-modular symbol**

$$\langle r; \delta\rangle^{\pm} := 2\pi\Big(\int_{r+i\delta}^{r+i\infty} f_E(z)dz \quad \pm \quad \int_{-r+i\delta}^{-r+i\infty} f_E(z)dz\Big) \; \in \; \mathbb{R},$$

and define

$$G^{\pm}_{E,m,\delta}(x) := \frac{1}{m}\sum_{m=0}^{mx}\langle \frac{a}{m}, \delta\rangle^{\pm}_{E}.$$

$G^{\pm}_{E,m,\delta}(x)$ as a Riemann sum



The motivation for this conjecture: a conjectural commutation of two limits

Then:

$$G_E^{\pm}(x) = \lim_{m\to\infty} \lim_{\delta\to 0} G_{E,m,\delta}^{\pm}(x),$$

while

$$g_E^{\pm}(x) = \lim_{\delta\to 0} \lim_{m\to\infty} G_{E,m,\delta}^{\pm}(x).$$

The motivation for this conjecture: a conjectural commutation of two limits

Then:

$$G_E^{\pm}(x) = \lim_{m\to\infty} \lim_{\delta\to 0} G_{E,m,\delta}^{\pm}(x),$$

while

$$g_E^{\pm}(x) = \lim_{\delta\to 0} \lim_{m\to\infty} G_{E,m,\delta}^{\pm}(x).$$

But discuss the issue of the “δ-tails."

(Also: similar phenomena, more generally, in cases where one has the analogues of modular symbols related to higher rank groups?)

Distribution of modular symbols for fixed denominator m

Fix the denominator m and consider the data of $\phi(m)$ real values

$$\{a \mapsto \langle \frac{a}{m} \rangle_E^{\pm}; \ \text{for } a = 1, 2, 3, \ldots, m; \ (a, m) = 1\}.$$

How are these values distributed?

Let $\Sigma_{E,m}^{\pm}(t)$ denote the distribution determined by these $\phi(m)$ values.

I.e., for open subsets $U \subset \mathbb{R}$, the integral $\int_U \Sigma_{E,m}^{\pm}(t)dt$ is $1/\phi(m)$ times the number of values of a (for $a = 1, 2, 3, \ldots, m; \ (a, m) = 1$) such that $\langle \frac{a}{m} \rangle_E^{\pm} \in U$.

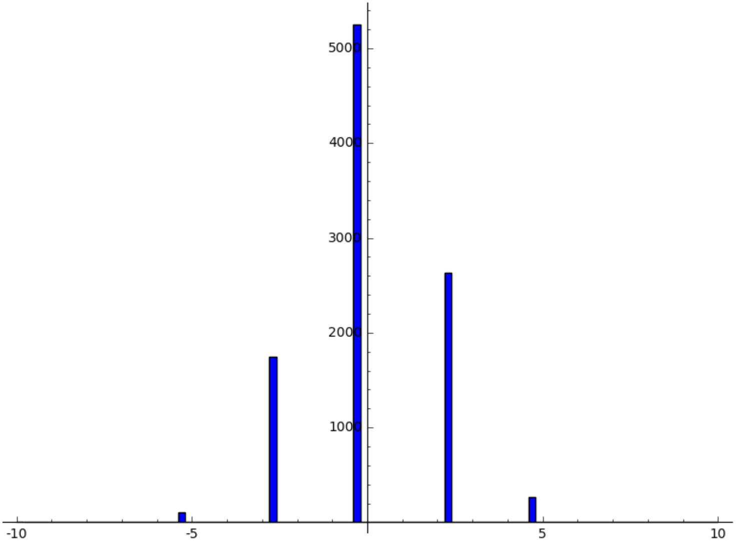
The mean

The mean of $\Sigma^{\pm}_{E,m}(t)$ goes to zero rapidly as m increases:

$$Mean(\Sigma^{\pm}_{E,m}) \ll \log m/\sqrt{m}.$$

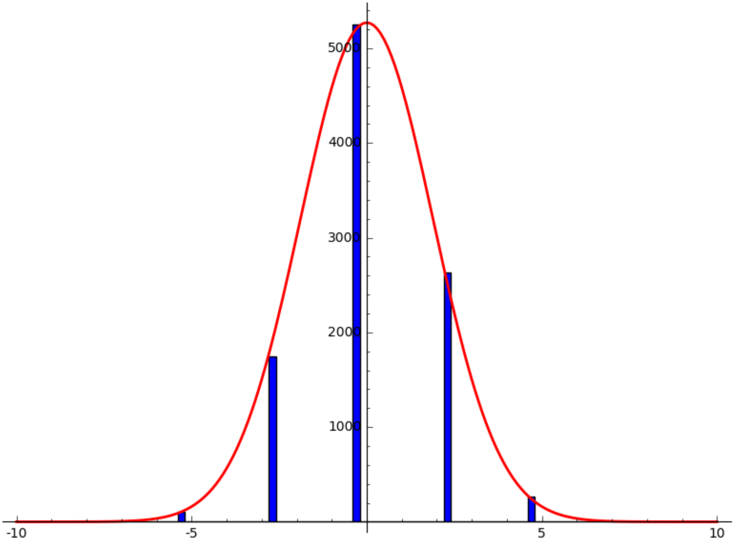
Histograms

Histogram of $\{[a/m]_E^+ : E = 11A1, m = 10,007, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



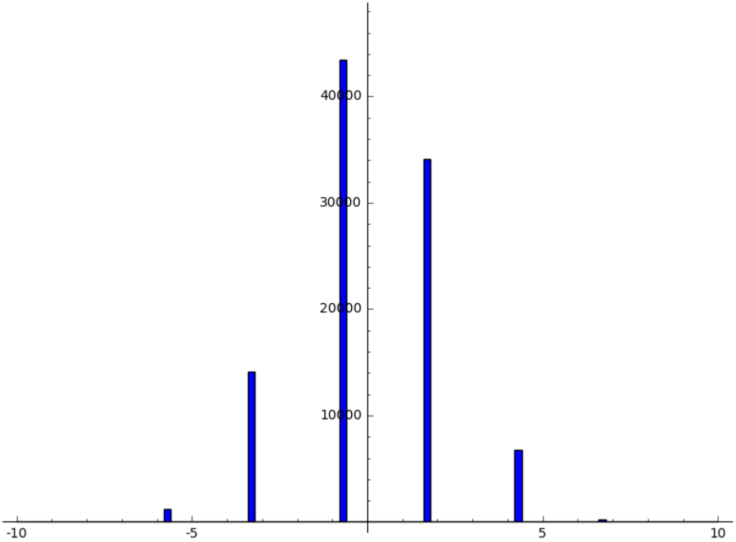
Histograms

Histogram of $\{[a/m]_E^+ : E = 11A1, m = 10,007, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



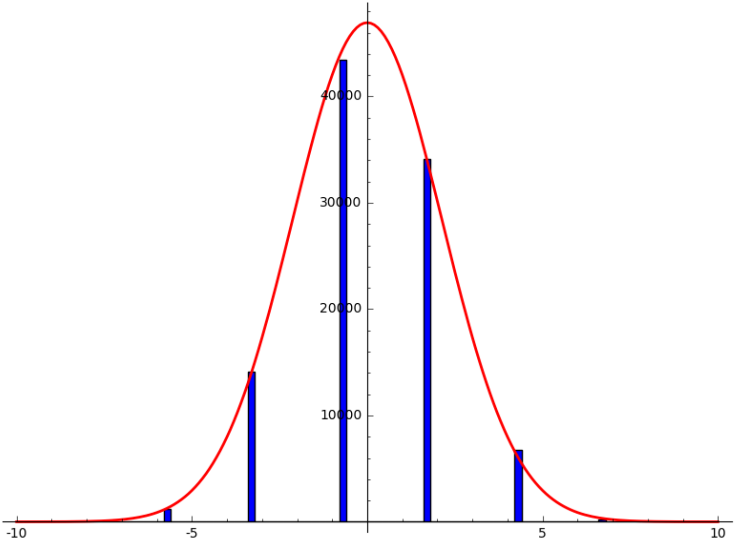
Histograms

Histogram of $\{[a/m]_E^+ : E = 11A1, m = 100,003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



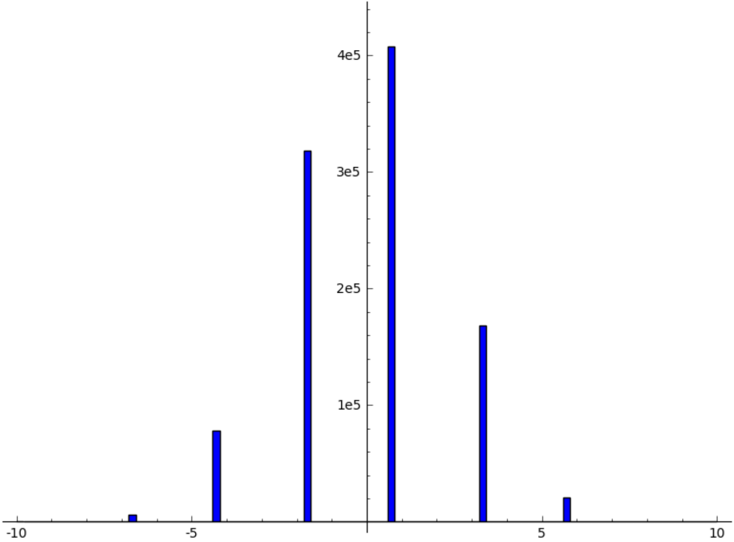
Histograms

Histogram of $\{[a/m]_E^+ : E = 11A1, m = 100,003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



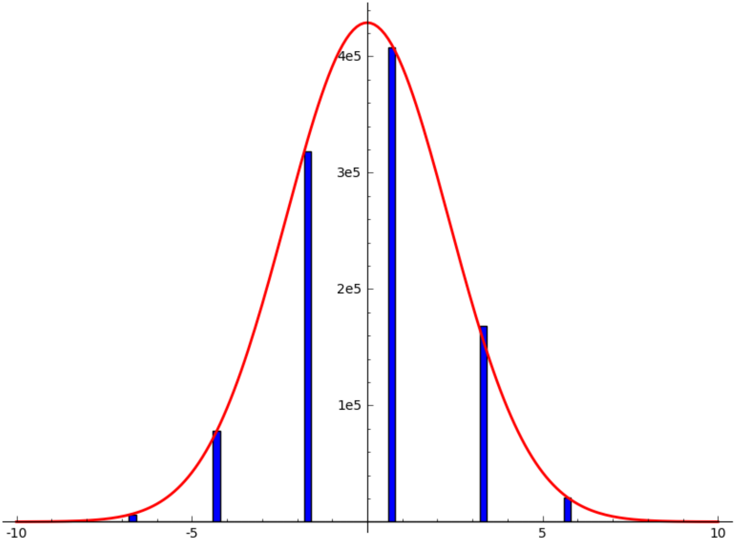
Histograms

Histogram of $\{[a/m]_E^+ : E = 11A1, m = 1,000,003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



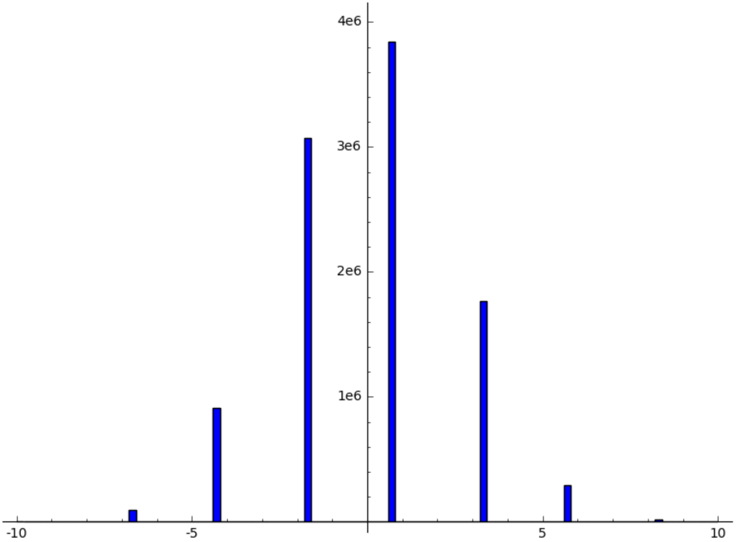
Histograms

Histogram of $\{[a/m]^+_E : E = 11A1, m = 1,000,003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



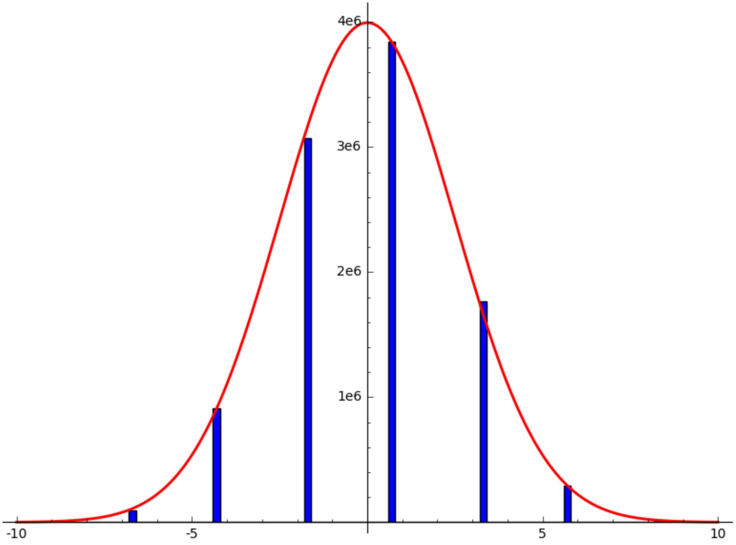
Histograms

Histogram of $\{[a/m]^+_E : E = 11A1, m = 10,000,019, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



Histograms

Histogram of $\{[a/m]_E^+ : E = 11A1, m = 10,000,019, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



Distribution of modular symbols

How does the variance depend on m?

Petridis and Risager have a beautiful formula for this, and what follows is a guess at a slight refinement of it.

Definition

Let $\mu_k(E, m)^{\pm}$ denote the k-th moment of $\Sigma^{\pm}_{E,m}$ centered at the mean.

So,

$$\mu_2(E, m)^{\pm} = Var(E, m)^{\pm}$$

is the variance of $\Sigma^{\pm}_{E,m}$.

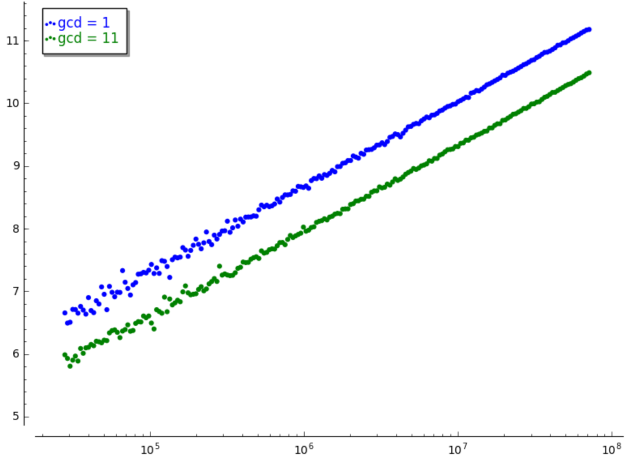
The variance

Let E be an elliptic curve of conductor N. Let κ be a divisor of N.

What follows are graphs of the variances $Var(E,m)^{\pm}$ for m growing subject to the condition: $gcd(N,m) = \kappa$.

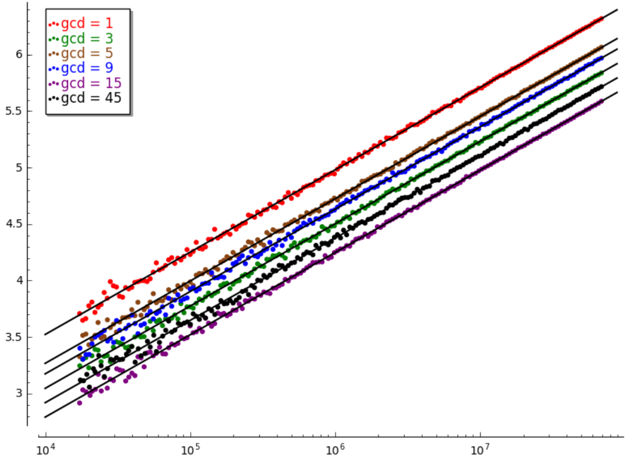
The variance

Here is a picture for the elliptic curve of conductor 11, the horizontal axis being on a log-scale. The dots give the data for $\kappa = 1$ and $\kappa = 11$ (in descending order).



The variance

Here is a picture for the elliptic curve of conductor 45. The six parallel lines correspond to the six positive numbers κ that divide 45.



The ‘Variance slope’ and ‘Variance shift’

Conjecture

There exist real-valued constants $C_E, D_{E,\kappa}$ *such that*

$$\lim_{m\to\infty \ | \ gcd(m,N)=\kappa} Var(E,m)^{\pm} \quad - \quad C_E \cdot \log m \quad = \quad D_{E,\kappa}$$

The 'Variance slope' and 'Variance shift'

Conjecture

There exist real-valued constants $C_E, D_{E,\kappa}$ such that

$$\lim_{m\to\infty \ | \ gcd(m,N)=\kappa} Var(E,m)^{\pm} \quad - \quad C_E \cdot \log m \quad = \quad D_{E,\kappa}$$

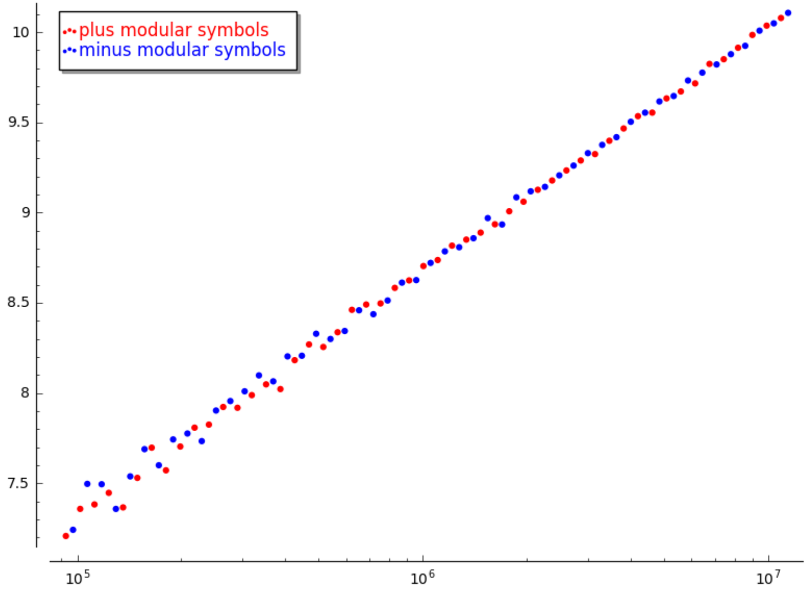
Call the conjectured C_E the **variance-slope** of E and the conjectured $D_{E,\kappa}$ the **variance-shift** of E.

The 'Variance slope' and 'Variance shift'

The above conjecture implies, for example, that

$$\lim_{m \to \infty} Var(E, m)^{+} - Var(E, m)^{-} \quad = \quad 0.$$

Plus versus minus variances



The Variance slope

Fix E a semistable elliptic curve over $\mathbb{Q}$ of conductor N uniformized by the modular newform

$$\omega_E = \sum_{\nu=0}^{\infty} a_\nu q^\nu dq/q.$$

Let $L(sym^2(\omega_E), s)$ denote the L-function of the symmetric square of the automorphic form ω_E.

The Variance slope

Conjecture

The variance slope C_E (exists, and)—following Petridis and Risager—is equal to

$$\mathcal{C}_E := \frac{6}{\pi^2} \cdot \prod_{p \mid N} \frac{p}{p+1} \cdot L(sym^2(\omega_E), 2).$$

.

Some Data

E	$\mathcal{C}_E$	$D_{E,1}$
11a1	0.589364640046590	0.5246
14a1	0.417980893000416	0.3763
15a1	0.355822978842096	0.4879
17a1	0.450713790373816	0.3872
19a1	0.535892587242072	0.4429
20a1	0.340755807914852	0.4900
21a1	0.411611414031698	0.6450
24a1	0.289291723879085	0.4562

Distribution of modular symbols

Theorem

(Petridis-Risager)The distribution determined by the data

$$a/m \quad \mapsto \frac{\langle a/m\rangle_E^{\pm}}{\sqrt{\mathcal{C}_E \log(m) + D_{E,\kappa}}}$$

(for all $a, m = 0, 1, 2, \ldots,$ and $(a, m) = 1$)

is normal with variance 1.

For example:

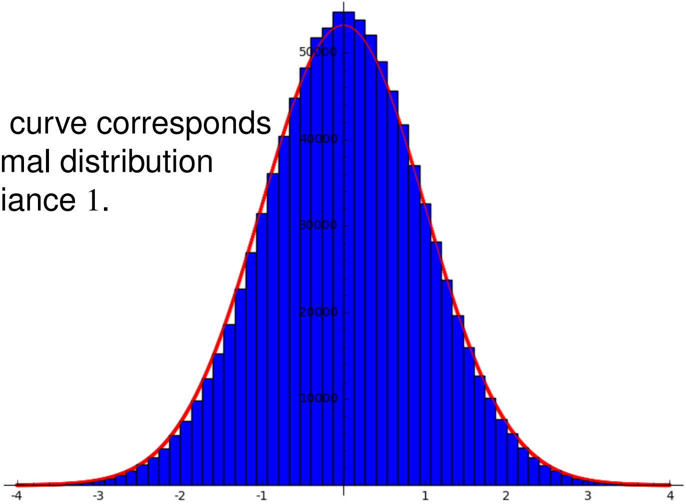
Consider the histogram of

$$\frac{\langle a/m\rangle_E^+}{\sqrt{\mathcal{C}_E \log(m) + D_{E,\kappa}}}$$

for the elliptic curve $E = 11a1$ and $\kappa = 1$; taken for 10^6 random values of a/m with m prime to 11 and $0 < m < 10^{16}$:

$E = 11a1$

The red curve corresponds to a normal distribution with variance 1.



Recall θ-coefficients and θ-elements

Suppose $L/\mathbb{Q}$ has conductor m.

$$c_g := \sum_{a\,:\,\sigma_a = g} \langle a/m \rangle \quad \text{for } g \in \mathrm{Gal}(L/\mathbb{Q}),$$

$$\theta_L := \sum_{g \in \mathrm{Gal}(L/\mathbb{Q})} c_g [g] \in \mathbb{R}[\mathrm{Gal}(L/\mathbb{Q})].$$

Then for all faithful $\chi : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathbb{C}^\times$,

$$\chi(\theta_L) = \tau(\chi) L(E, \bar{\chi}, 1).$$

We want to know how often this vanishes.

Distribution of θ-coefficients

Let E be an elliptic curve with conductor N. Let $[L : \mathbb{Q}]$ be cyclic of (say, odd) degree d and conductor m prime to N. Then each θ-coefficient $c_{E,g} = c_g$ is a sum of $\varphi(m)/d$ modular symbols.

Distribution of θ-coefficients

Let E be an elliptic curve with conductor N. Let $[L:\mathbb{Q}]$ be cyclic of (say, odd) degree d and conductor m prime to N. Then each θ-coefficient $c_{E,g} = c_g$ is a sum of $\varphi(m)/d$ modular symbols.

The Atkin-Lehner duality induces an 'involution' $g \to g'$ such that

$$c_{g'} = w_E \cdot c_g.$$

The θ-coefficient c_{g_o} attached to the fixed point of this involution we'll call the **sensitive θ-coefficient**.

Since we have an idea how the modular symbols behave, we conjecture:

The curious distribution of θ-coefficients for fixed d

Fix d. Let $\Lambda_{E,d}(t)$ be the distribution determined by the data

$$(g, m) \mapsto \frac{c_{E,g}}{\sqrt{\mathcal{C}_E \log(m) \cdot \varphi(m)/d}}$$

where (g, m) runs through all triples such that:

The curious distribution of θ-coefficients for fixed d

- $\varphi(m)$ is a multiple of d,
- g is an element of $\mathrm{Gal}(L/\mathbb{Q})$ for $L/\mathbb{Q}$ a cyclic extension of $\mathbb{Q}$ in $\mathbb{C}$ of degree d and conductor m. But g is not the *sensitive element*.

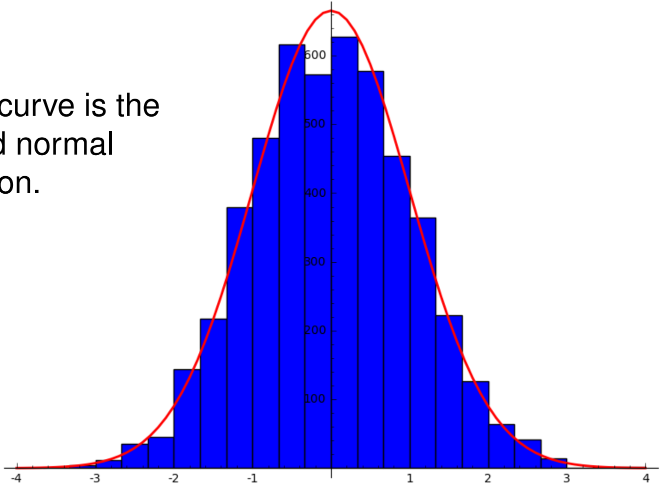
Conjecture

- *If $d > 2$ the distribution $\Lambda_{E,d}(t)$ is a bounded function.*
- *The limiting distribution as $d \to \infty$ is the normal distribution of variance 1.*

$\Lambda_{E,d}(t)$, large d

$E = 11A1$, $m = 25035013$, L is the field of degree $d = 5003$ in $\mathbb{Q}(\boldsymbol{\mu}_m)$:

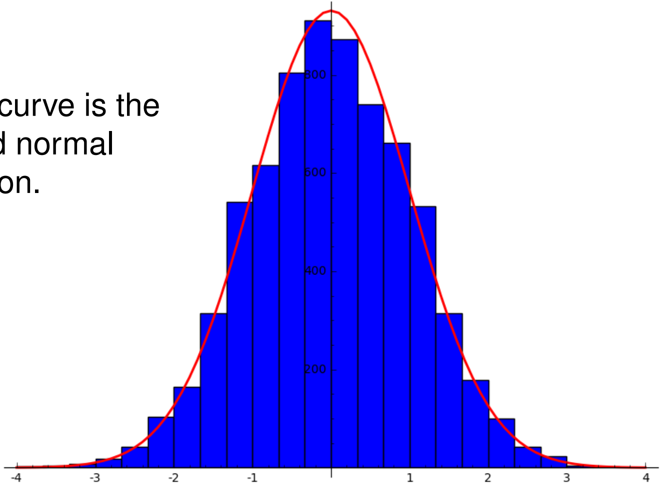
The red curve is the expected normal distribution.



$\Lambda_{E,d}(t)$, large d

$E = 11A1$, $m = 49063009$, L is the field of degree $d = 7001$ in $\mathbb{Q}(\boldsymbol{\mu}_m)$:

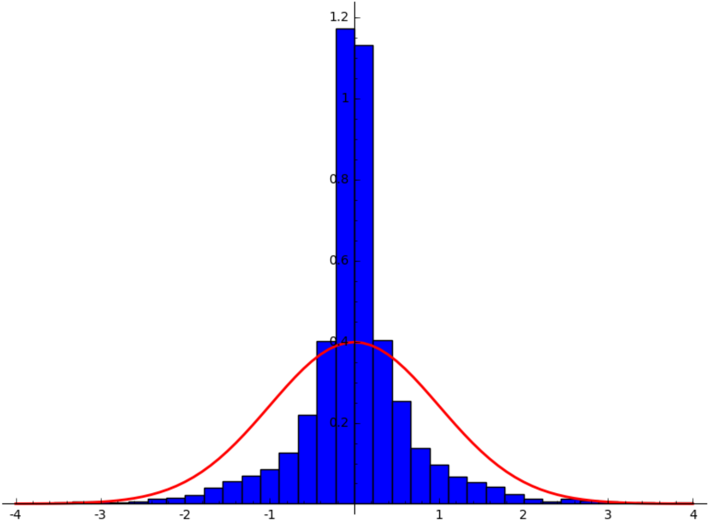
The red curve is the expected normal distribution.



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

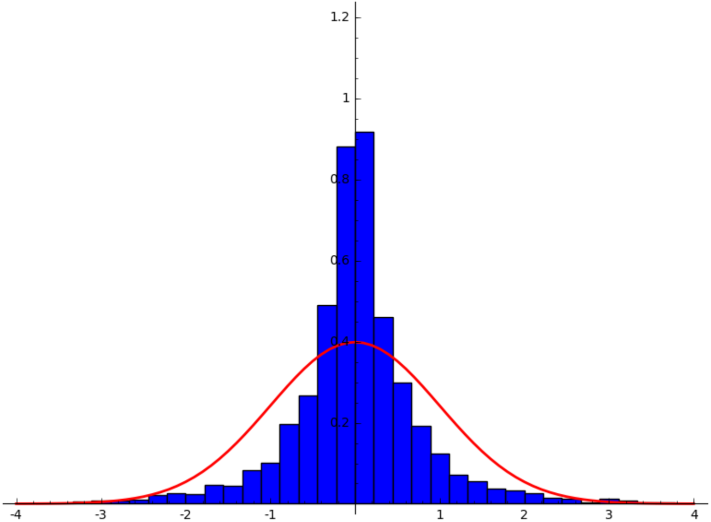
$d = 3$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L:\mathbb{Q}] = d$,

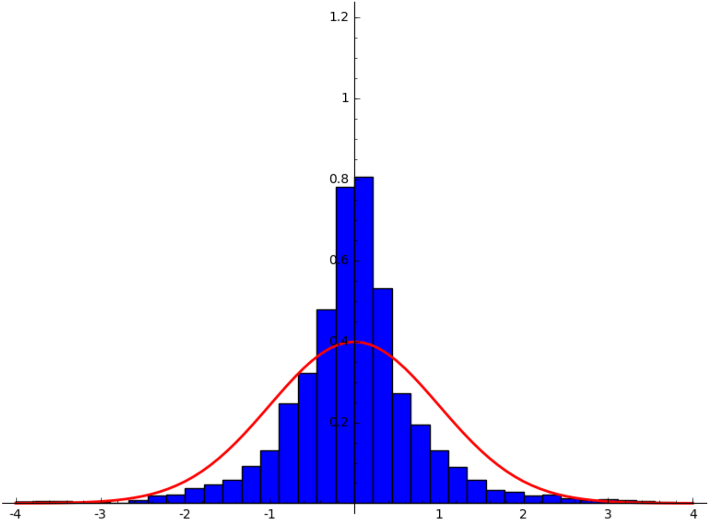
$d = 5$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

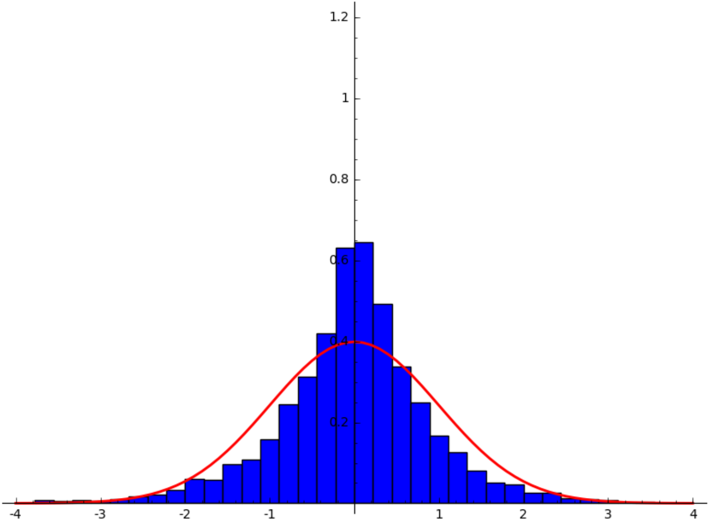
$d = 7$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L:\mathbb{Q}] = d$,

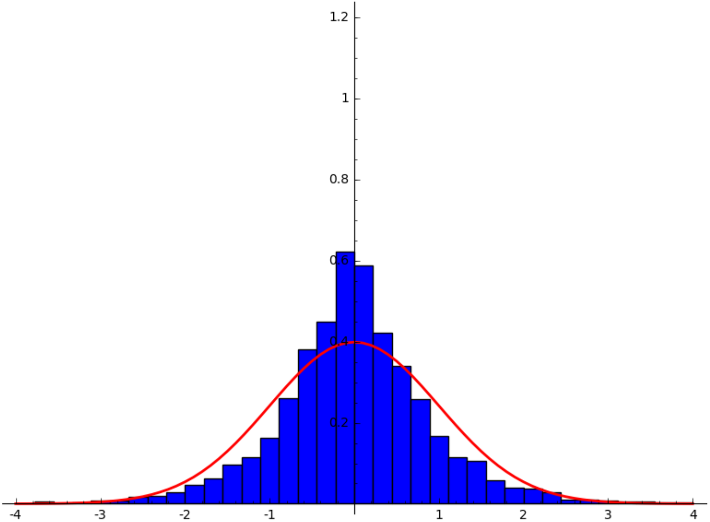
$d = 11$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

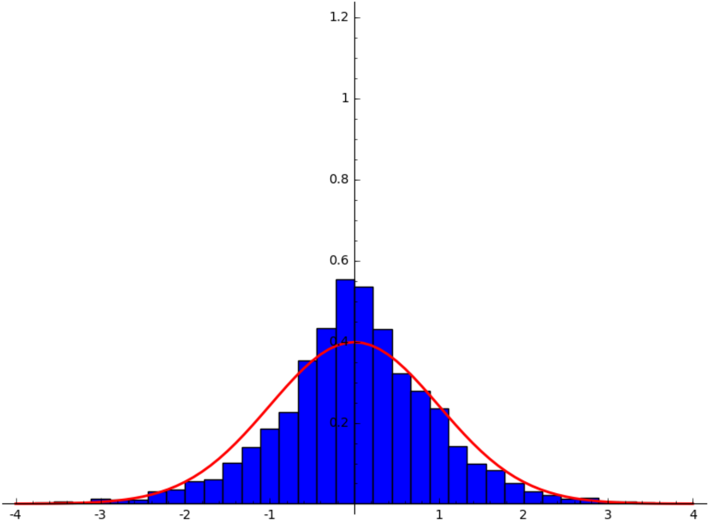
$d = 13$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

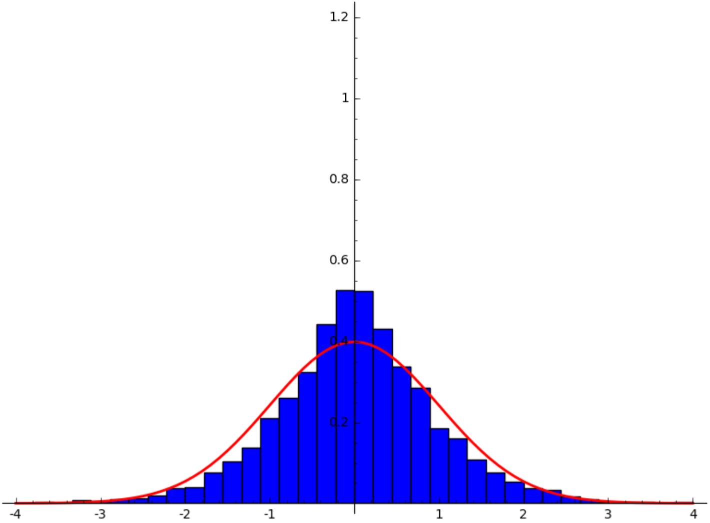
$d = 17$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

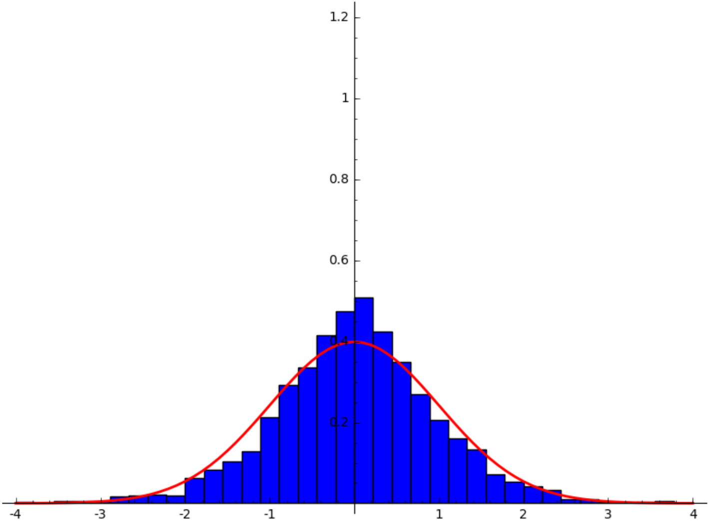
$d = 23$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

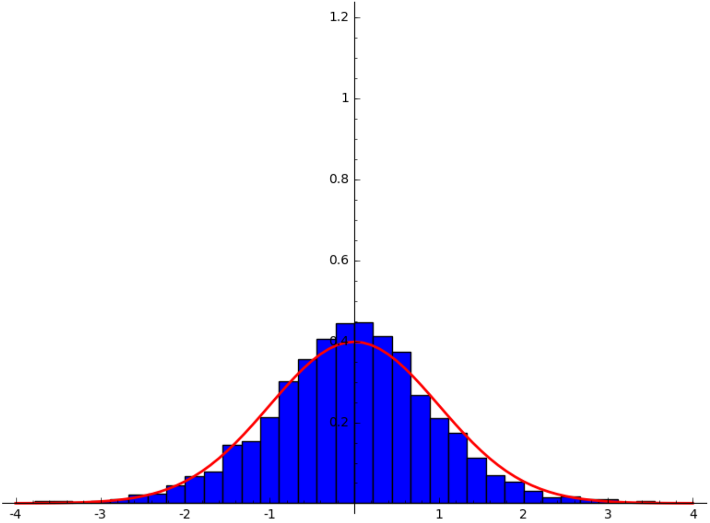
$d = 31$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod d$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L:\mathbb{Q}] = d$,

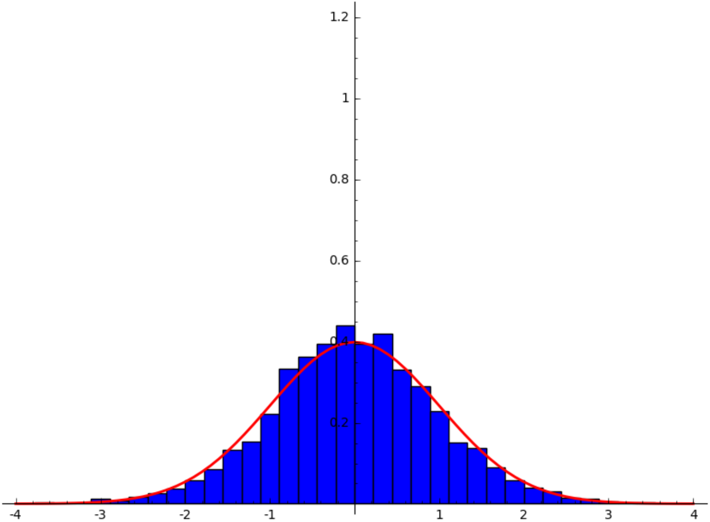
$d = 41$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L:\mathbb{Q}] = d$,

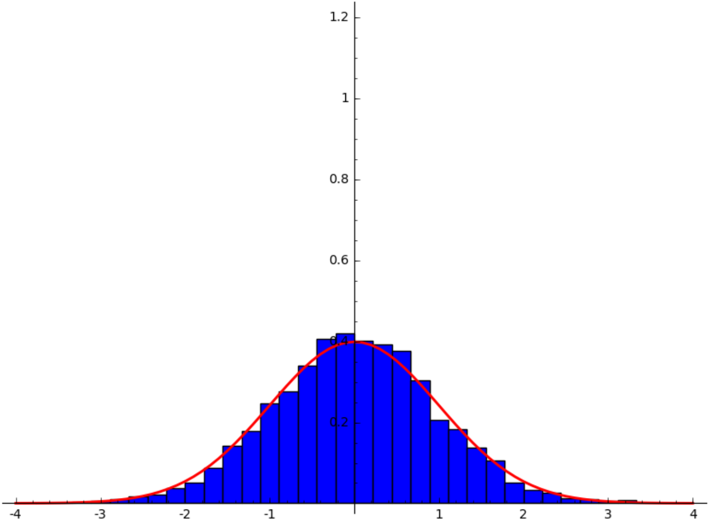
$d = 53$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L : \mathbb{Q}] = d$,

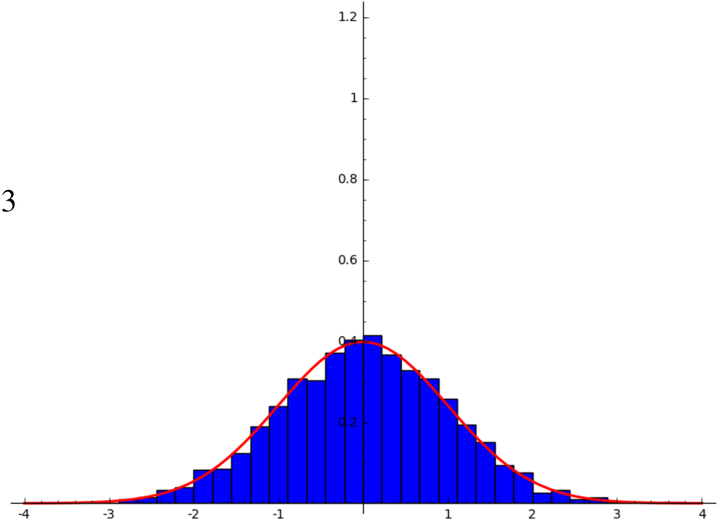
$d = 97$



$\Lambda_{E,d}(t)$, small d

$E = 11A1$, $m \equiv 1 \pmod{d}$, $L \subset \mathbb{Q}(\boldsymbol{\mu}_m)$, $[L:\mathbb{Q}] = d$,

$d = 293$



"Expectation" of L-function vanishing

Heuristic

There is a constant γ_E, depending only on E, such that

$$\text{“Exp}[L(E,\chi,1)=0]\text{”} \leq \left(\frac{d}{\varphi(m)}\cdot\frac{\gamma_E}{\log(m)}\right)^{\varphi(d)/4}$$

where d is the order of χ and m its conductor.

This should hold for all χ of order greater than 2.

Consequences of the heuristic; $d = 3$

Heuristic

$$\text{“Exp}[L(E,\chi,1) = 0]\text{”} \leq \left(\frac{d}{\varphi(m)} \cdot \frac{\gamma_E}{\log(m)}\right)^{\varphi(d)/4}.$$

Example ($d = 3$)

$$\sum_{\chi \text{ order } 3, \text{ conductor } < X} \text{“Exp}[L(E,\chi,1) = 0]\text{”} \ll \sum_{m=2}^{X} \frac{1}{(\log(m)\varphi(m))^{1/2}} \ll \sqrt{X}.$$

Consequences of the heuristic; $d = 5$

Example ($d = 5$)

$$\sum_{\chi \text{ order } 5,\ \text{conductor} < X} \text{“Exp}[L(E,\chi,1) = 0]\text{”} \ll \sum_{m=2}^{X} \frac{1}{\log(m)\varphi(m)} \ll \log X.$$

These are consistent with the prediction of David-Fearnley-Kisilevsky.

Consequences of the heuristic: $d = 7$

Example ($d = 7$)

$$\sum_{\chi \text{ of order } 7} \text{“Exp}[L(E,\chi,1) = 0]\text{”} \ll \sum_{m=2}^{\infty} \frac{1}{(\log(m)\varphi(m))^{3/2}} < \infty.$$

This is consistent with the prediction of David-Fearnley-Kisilevsky.

Consequences of the heuristic: all large d

Heuristic

$$\text{“Exp}[L(E,\chi,1)=0]\text{”} \leq \left(\frac{d}{\varphi(m)}\cdot\frac{\gamma_E}{\log(m)}\right)^{\varphi(d)/4}.$$

Let $f(d,m)$ denote the number of characters of order d of conductor m

Proposition

Suppose $t:\mathbb{Z}_{>0}\to\mathbb{R}_{\geq 0}$ *is a function, and* $t(d)\gg\log(d)$. *Then*

$$\sum_{d\,:\,t(d)>1, m>d} f(d,m)\left(\frac{d}{\varphi(m)}\cdot\frac{\gamma_E}{\log(m)}\right)^{t(d)} \quad \textit{converges.}$$

When $\varphi(d) > 4$

Applying this with $t(d) = \varphi(d)/4$ shows

Heuristic

$$\sum_{d\,:\,\varphi(d)>4} \ \sum_{\chi \text{ order } d} \text{“}\mathrm{Exp}[L(E,\chi,1) = 0]\text{”} \quad \textit{converges.}$$

Consequences of the heuristic

This leads to:

Conjecture

Suppose $L/\mathbb{Q}$ is an abelian extension with only finitely many subfields of degree 2, 3, or 5 over $\mathbb{Q}$.

Then for every elliptic curve $E/\mathbb{Q}$, we expect that $E(L)$ is finitely generated.

Consequences of the heuristic

This leads to:

Conjecture

Suppose $L/\mathbb{Q}$ is an abelian extension with only finitely many subfields of degree 2, 3, or 5 over $\mathbb{Q}$.

Then for every elliptic curve $E/\mathbb{Q}$, we expect that $E(L)$ is finitely generated.

For example, these conditions hold when L is:

- the $\hat{\mathbb{Z}}$-extension of $\mathbb{Q}$,
- the maximal abelian ℓ-extension of $\mathbb{Q}$, for $\ell \geq 7$,
- the compositum of all of the above.