Arithmetic conjectures suggested by the statistical behavior of modular symbols

Barry Mazur, Harvard University
Karl Rubin, UC Irvine

HINT, March 2019

Diophantine Stability

Fix a variety V over a number field K. Say that a field extension M/K of algebraic numbers is **Diophantine Stable for** V, if the variety V acquires no new rational points when the base is extended from K to M. That is, if

$$\boxed{V(M) = V(K).}$$

Diophantine Stability

Fix a variety V over a number field K. Say that a field extension M/K of algebraic numbers is **Diophantine Stable for** V, if the variety V acquires no new rational points when the base is extended from K to M. That is, if

$$\boxed{V(M) = V(K).}$$

If $V = \mathbf{P}^1$ is the projective line over K, for example, then no nontrivial extension M/K is Diophantine Stable for V.

Diophantine Stability

Fix a variety V over a number field K. Say that a field extension M/K of algebraic numbers is **Diophantine Stable for** V, if the variety V acquires no new rational points when the base is extended from K to M. That is, if

$$\boxed{V(M) = V(K).}$$

If $V = \mathbf{P}^1$ is the projective line over K, for example, then no nontrivial extension M/K is Diophantine Stable for V.

If $V = A$ is an abelian variety, for example, and If M/K is 'Diophantine stable' for A, we would have an equality of Mordell-Weil ranks:

$$\mathrm{rank}(A(M)) = \mathrm{rank}(A(K)).$$

Lots of Diophantine Stability

Karl Rubin and I showed some years ago that there are uncountably many field extensions of algebraic numbers M/K that are **Diophantine Stable** for any given elliptic curve E over K (of course, most of these fields would have infinite degree).

Ranks in abelian extensions (of infinite degree over $\mathbb{Q}$)

One of the great results in the subject is due to Kato, Ribet, Rohrlich:

Theorem

Let S be a finite set of primes, and $M_S/\mathbb{Q}$ the maximal abelian extension of $\mathbb{Q}$ unramified outside S.

For any elliptic curve $E/\mathbb{Q}$ its group of M_S-rational points is finitely generated.

What else might one hope in terms of finite generation of Mordell-Weil for abelian extensions of $\mathbb{Q}$ of infinite degree?

Comment about Hilbert's Tenth Problem

Note: **Every** *elliptic curve has infinite Mordell-Weil rank over the maximal abelian extension of* $\mathbb{Q}$.

Growth of ranks in abelian extensions that contain finitely many subfields of degree ≤ 5

Inspired by the work of David-Fearnley-Kisilevsky, and bolstered by what I'll be calling a *naive heuristic*, Karl Rubin and I conjecture:

Growth of ranks in abelian extensions that contain finitely many subfields of degree ≤ 5

Inspired by the work of David-Fearnley-Kisilevsky, and bolstered by what I'll be calling a *naive heuristic*, Karl Rubin and I conjecture:

Conjecture

For E any elliptic curve over $\mathbb{Q}$, and $M/\mathbb{Q}$ any abelian extension (of algebraic numbers) that contains only finitely many subfields of degree ≤ 5, the Mordell-Weil group $E(M)$ 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.

Statistics of the growth of ranks in abelian extensions

Question

As F runs through abelian extensions of K of finite degree, "how often" is $\mathrm{rank}(E(F)) > \mathrm{rank}(E(K))$*?*

Statistics of the growth of ranks in abelian extensions

Question

As F runs through abelian extensions of K of finite degree, "how often" is $\mathrm{rank}(E(F)) > \mathrm{rank}(E(K))$?

Consider the representation of $\mathrm{Gal}(F/K)$ on $E(F) \otimes \mathbb{Q}$.

Since $\mathrm{Gal}(F/K)$ is abelian, it is enough to consider the case where F/K is cyclic.

Statistics of growth of ranks in cyclic extensions

Fix an elliptic curve E over a number field K.

Question

As F runs through cyclic abelian extensions of K, how often is

$$\mathrm{rank}(E(F)) > \mathrm{rank}(E(K))?$$

Statistics of growth of ranks in cyclic extensions

Fix an elliptic curve E over a number field K.

Question

As F runs through cyclic abelian extensions of K, how often is

$$\mathrm{rank}(E(F)) > \mathrm{rank}(E(K))?$$

not often! when F/K is cyclic of large degree.

General philosophy:

David-Fearnley-Kisilevsky show that “Random Matrix Heuristics," (which is in accord with the classical Hilbert-Polya scenario) suggest the following conjecture:

Conjecture

(David-Fearnley-Kisilevsky) Let E be an elliptic curve over $\mathbb{Q}$ and $p \geq 7$ a prime number. there are only finitely many cyclic extensions $L/\mathbb{Q}$ of degree p that are Diophantine unstable for E.

General philosophy:

We will consider these questions from the viewpoint of a somewhat more naive heuristic regarding the statistics of numerical invariants attached to an elliptic curve E defined over $\mathbb{Q}$ and cyclic extensions $L/\mathbb{Q}$ of degree d.

Our heuristic depends on **growth bounds** of certain distributions denoted

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

The distributions $\Lambda_{E,d}(t)$ are built on modular symbols,

Our heuristic depends on **growth bounds** of certain distributions denoted

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

The distributions $\Lambda_{E,d}(t)$ are built on modular symbols,

(Although modular symbol values are normally distributed, these distributions are not.)

General philosophy:

These (conjectured) distributions $\Lambda_{E,d}(t)$ are, we think, interesting in themselves, and we only use bounds much weaker than the conjectured Growth bounds for these distributions to obtain heuristic support for our conjectures.

Growth of ranks: analytic approach (conditional on BSD)

Question

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

Growth of ranks: analytic approach (conditional on BSD)

Question

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

Using BSD and the factorization

$$L(E/F, s) = \prod_{\chi:\mathrm{Gal}(F/K)\to\mathbb{C}^\times} L(E, \chi, s)$$

this is equivalent to:

Vanishing of special values of L-functions

Question

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

Vertical line integrals

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

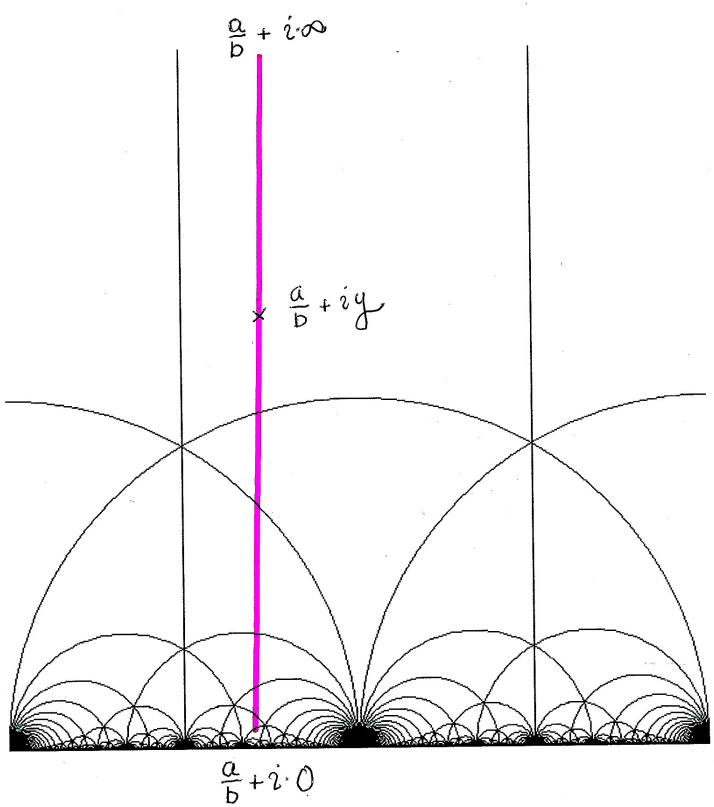
$$f_E(z)dz = \sum_{\nu=1}^{\infty} a_\nu e^{2\pi i \nu z} dz$$

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 $\frac{1}{\delta}\Omega_E^{\pm}$ for some positive integer δ.

Modular symbols

Fix $E/\mathbb{Q}$ once and for all, and suppress it from the notation. We normalize to get rational values by dividing by the period:

Definition

For $r \in \mathbb{Q}$, define the (plus) modular symbol $[r] = [r]_E$ by

$$[r] := \frac{1}{2}\left(\frac{2\pi i}{\Omega}\int_{i\infty}^{r} f_E(z)dz + \frac{2\pi i}{\Omega}\int_{i\infty}^{-r} f_E(z)dz\right) \in \mathbb{Q}$$

where f_E is 'the' modular form attached to E, and Ω is the real period.

Modular symbols and special values of L-functions

Theorem

For every primitive even Dirichlet character χ of conductor m,

$$\sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)[a/m] = \frac{\tau(\chi) L(E, \bar{\chi}, 1)}{\Omega}.$$

I.e., the χ-weighted sum of modular symbols with denominator m is equal (after normalization) to the special L-value for E twisted by χ of interest to us.

Vanishing of the special value of our L-function

In particular

$$L(E,\chi,1)=0 \iff \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)[a/m]=0.$$

We want to use statistical properties of modular symbols to predict how often this happens.

The combinatorics of Modular Symbols

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

- $\boxed{[\infty] = 0}$ by definition
- There is a $\delta \in \mathbb{Z}_{>0}$ independent of r such that $\delta \cdot [r] \in \mathbb{Z}$

The combinatorics of Modular Symbols

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

- $\boxed{[\infty] = 0}$ by definition
- There is a $\delta \in \mathbb{Z}_{>0}$ independent of r such that $\delta \cdot [r] \in \mathbb{Z}$
- $\boxed{[r] = [r+1]}$ since $f_E(z) = f_E(z+1)$

The combinatorics of Modular Symbols

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

- $\boxed{[\infty] = 0}$ by definition
- There is a $\delta \in \mathbb{Z}_{>0}$ independent of r such that $\delta \cdot [r] \in \mathbb{Z}$
- $\boxed{[r] = [r+1]}$ since $f_E(z) = f_E(z+1)$
- $\boxed{[r] = [-r]}$ by definition

and

Invariance under the action of $\Gamma_0(N)$

If

$$T := \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N) \subset \mathrm{SL})2(\mathbb{Z}),$$

so that for $r \in \mathbb{Q} \sqcup \{\infty\}$,

$$T(r) = \frac{ar + b}{cNr + d} \in \mathbb{Q} \sqcup \{\infty\},$$

we have the following relation in modular symbols:

$$\boxed{[r] = [T(r)] - [T(\infty)].}$$

The Atkin-Lehner and Hecke relations

- **Atkin-Lehner relation:** if w is the global root number of E, and $aa'N \equiv 1 \pmod{m}$, then

$$\boxed{[a'/m] = w[a/m]}$$

The Atkin-Lehner and Hecke relations

- **Atkin-Lehner relation:** if w is the global root number of E, and $aa'N \equiv 1 \pmod{m}$, then

$$\boxed{[a'/m] = w[a/m]}$$

- **Hecke relation:** if a prime $\ell \nmid N$ and a_ℓ is the ℓ-th Fourier coefficient of f_E, then

$$\boxed{a_\ell[r] = [\ell r] + \sum_{i=0}^{\ell-1}[(r+i)/\ell]}$$

Theta elements

If $m \geq 1$, and $F/\mathbb{Q}$ is cyclic of conductor m, let

$G_m := \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})$, the Galois group of the m-cyclotomic field, and

- $\sigma_a \in G_m$ the automorphism

$$\zeta_m \mapsto \zeta_m^a,$$

Theta elements

Define:

- (The m-cyclotomic **theta element**):

$$\boxed{\theta_m := \quad \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} [a/m]\sigma_a \quad \in \quad \mathbb{Q}[G_m],}$$

Theta elements

Define:

- (The m-cyclotomic **theta element**):

$$\boxed{\theta_m := \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} [a/m]\sigma_a \in \mathbb{Q}[G_m],}$$

and

- (The **theta element** for $F/\mathbb{Q}$):

$$\boxed{\theta_F := \theta_m|_F \in \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})].}$$

The theta elements determine the vanishing of special L-values

If

$$\chi : \mathrm{Gal}(F/\mathbb{Q}) \hookrightarrow \mathbb{C}^*$$

is an even character 'cutting out' $F/\mathbb{Q}$, we have:

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

theta coefficients

Write:

$$\theta_F = \sum_{\gamma \in \mathrm{Gal}(F/\mathbb{Q})} c_{F,\gamma}\gamma \quad \in \quad \frac{1}{\delta}\mathbb{Z}[Gal(F/\mathbb{Q})]$$

where each of its coefficients (the "theta coefficients") is given as an explicit sum of modular symbols:

$$\boxed{c_{F,\gamma} = \sum_{\sigma_a|_F = \gamma} [a/m].}$$

'Atkin-Lehner' relations (alias: 'functional equation')

Assuming that N the conductor of E is prime to $m :=$ the conductor of F, The *Atkin-Lehner Relations* for modular symbols,

$$\boxed{[a'/m] = w \cdot [a/m]}$$

implies an analogous relation:

$$\boxed{c_{F,\gamma'} = w \cdot c_{F,\gamma}}$$

where if $\mathbb{Z}/m\mathbb{Z})^* \to Gal(F/\mathbb{Q})$ is the natural map, and $\gamma_N \in Gal(F/\mathbb{Q})$ is the image of N, then $\gamma' = (\gamma\gamma_N)^{-1}$.

'Atkin-Lehner' relations (alias: 'functional equation')

Assuming that N the conductor of E is prime to $m :=$ the conductor of F, The *Atkin-Lehner Relations* for modular symbols,

$$\boxed{[a'/m] = w \cdot [a/m]}$$

implies an analogous relation:

$$\boxed{c_{F,\gamma'} = w \cdot c_{F,\gamma}}$$

where if $\mathbb{Z}/m\mathbb{Z})^* \to Gal(F/\mathbb{Q})$ is the natural map, and $\gamma_N \in Gal(F/\mathbb{Q})$ is the image of N, then $\gamma' = (\gamma\gamma_N)^{-1}$.

Say that $c_{F,\gamma}$ is a **generic** theta-coefficient if $\gamma' \neq \gamma$

Discuss

The 'average value' of the theta coefficients

If $m = cond(F)$ is square-free we have:

$$\boxed{\frac{1}{\phi(d)} \sum_{\gamma \in \mathrm{Gal}(F/\mathbb{Q})} c_{F,\gamma} = \frac{\prod_{\ell | m} (a_\ell - 2)[0]}{\phi(d)} \ll \frac{\sqrt{m}}{\phi(d)}}$$

The cyclotomic algebraic numbers $\chi(\theta_F)$

For a character χ cutting out $\mathrm{Gal}(F/\mathbb{Q})$ we get the cyclotomic algebraic number

$$\theta_F \xrightarrow{\chi} \chi(\theta_F) \in \frac{1}{\delta}\mathbb{Z}[e^{2\pi i/d}]$$

where $d = [F : \mathbb{Q}]$.

How likely is it that $\chi(\theta_F) = 0$?

Example

Suppose $[F : \mathbb{Q}] = p$ is prime, and $\chi : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^\times$ is nontrivial.

The only nontrivial $\mathbb{Q}$-linear relation among the p-th roots of unity is that their sum is zero, so:

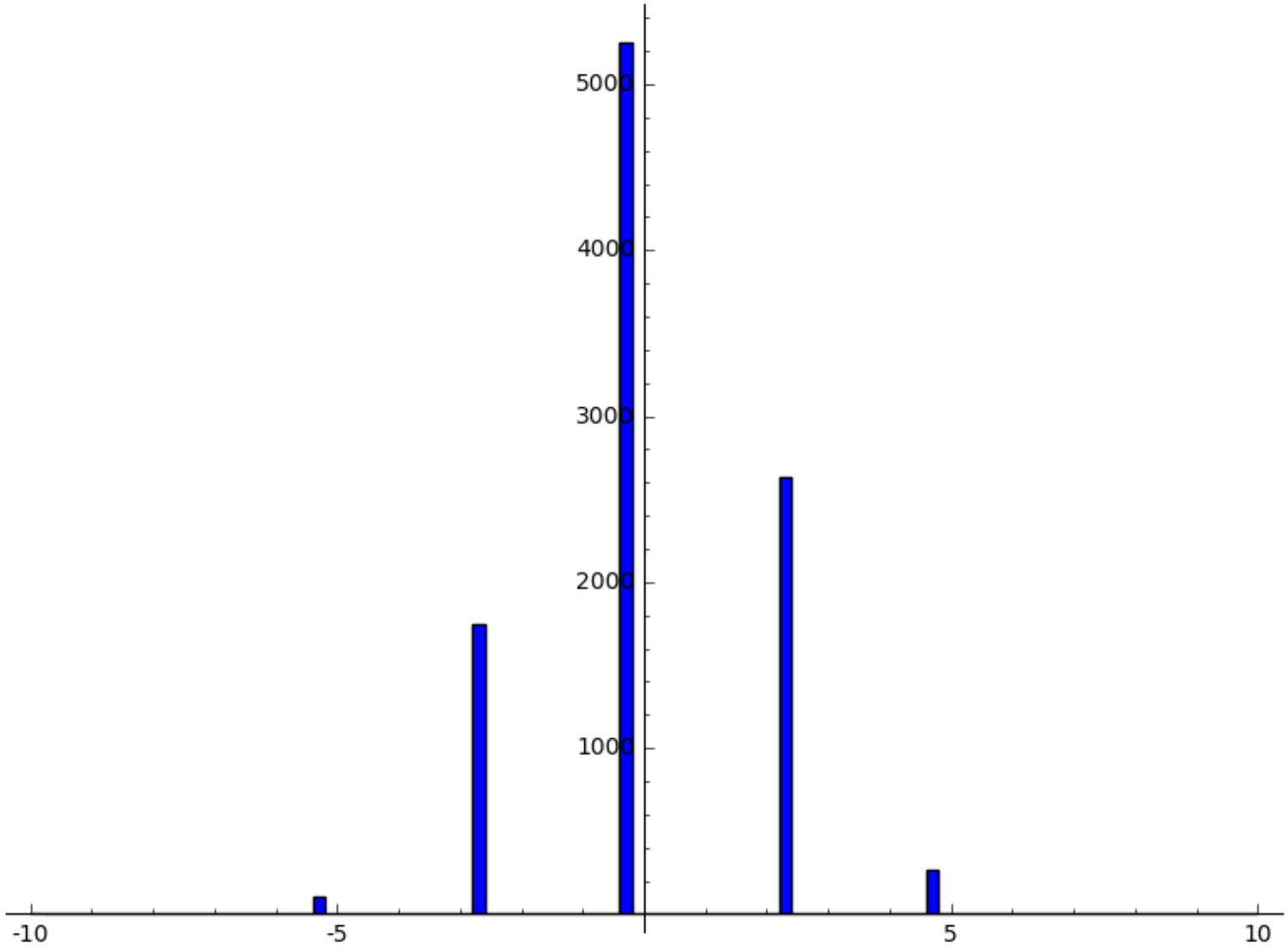
How likely is it that $\chi(\theta_F) = 0$?

$$\chi(\theta_F) = 0 \quad \Longleftrightarrow \quad c_{F,\gamma_0} = c_{F,\gamma_1} \quad \forall \gamma_0, \gamma_1 \in \mathrm{Gal}(F/\mathbb{Q}).$$

That is, all the theta coefficients must be equal in order for $L(E, \chi, 1)$ to vanish.

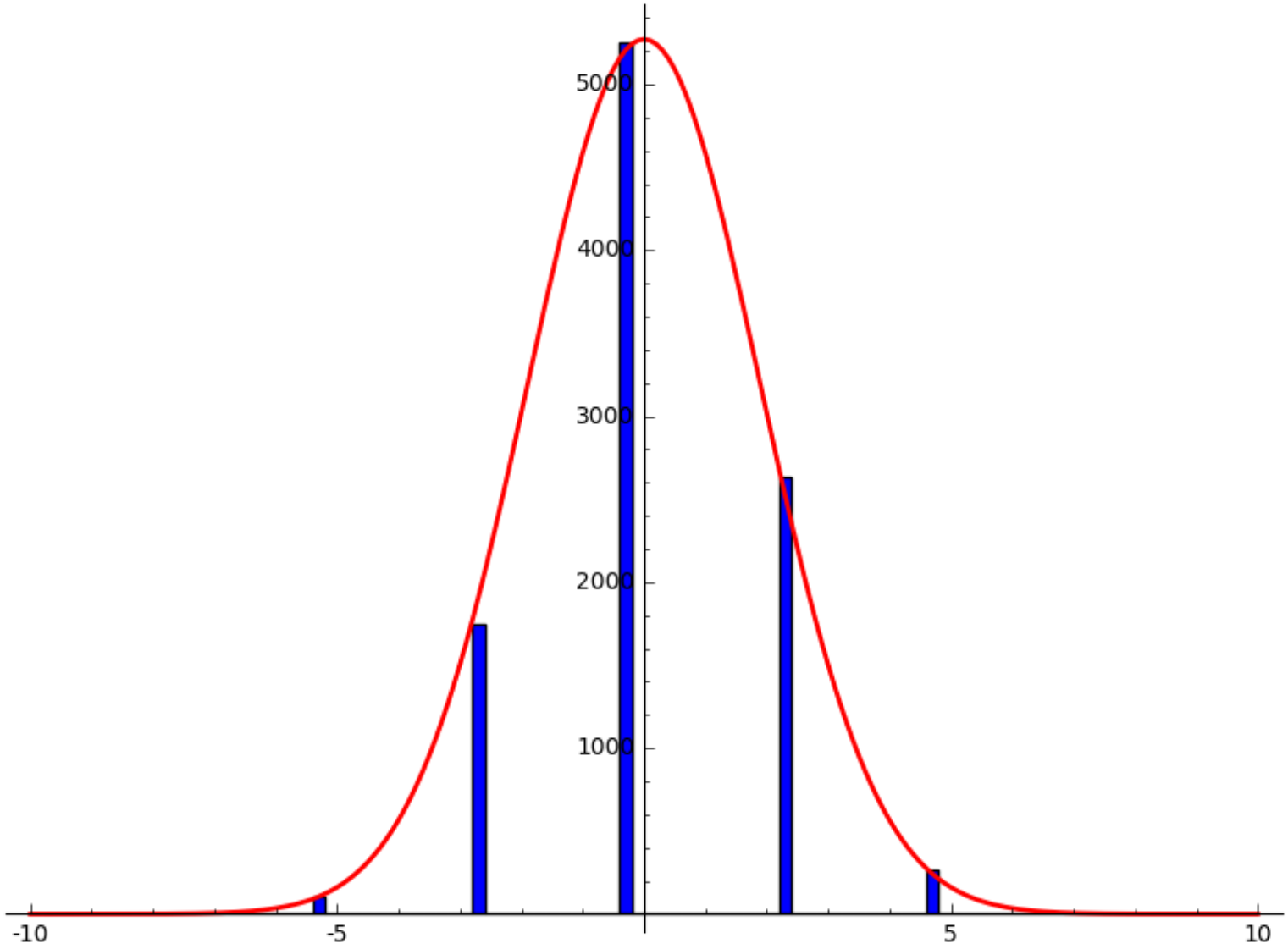
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 10007, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



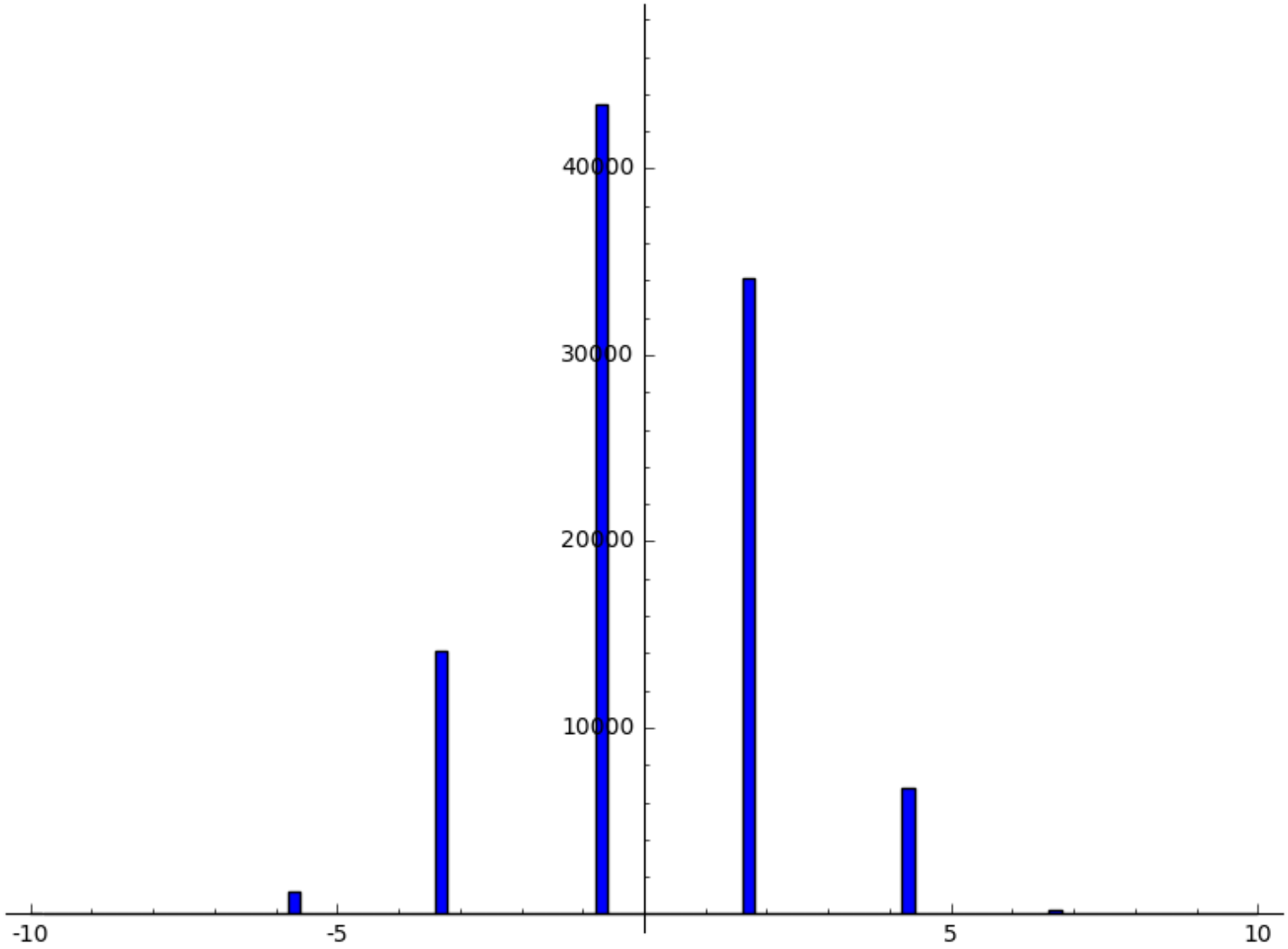
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 10007, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



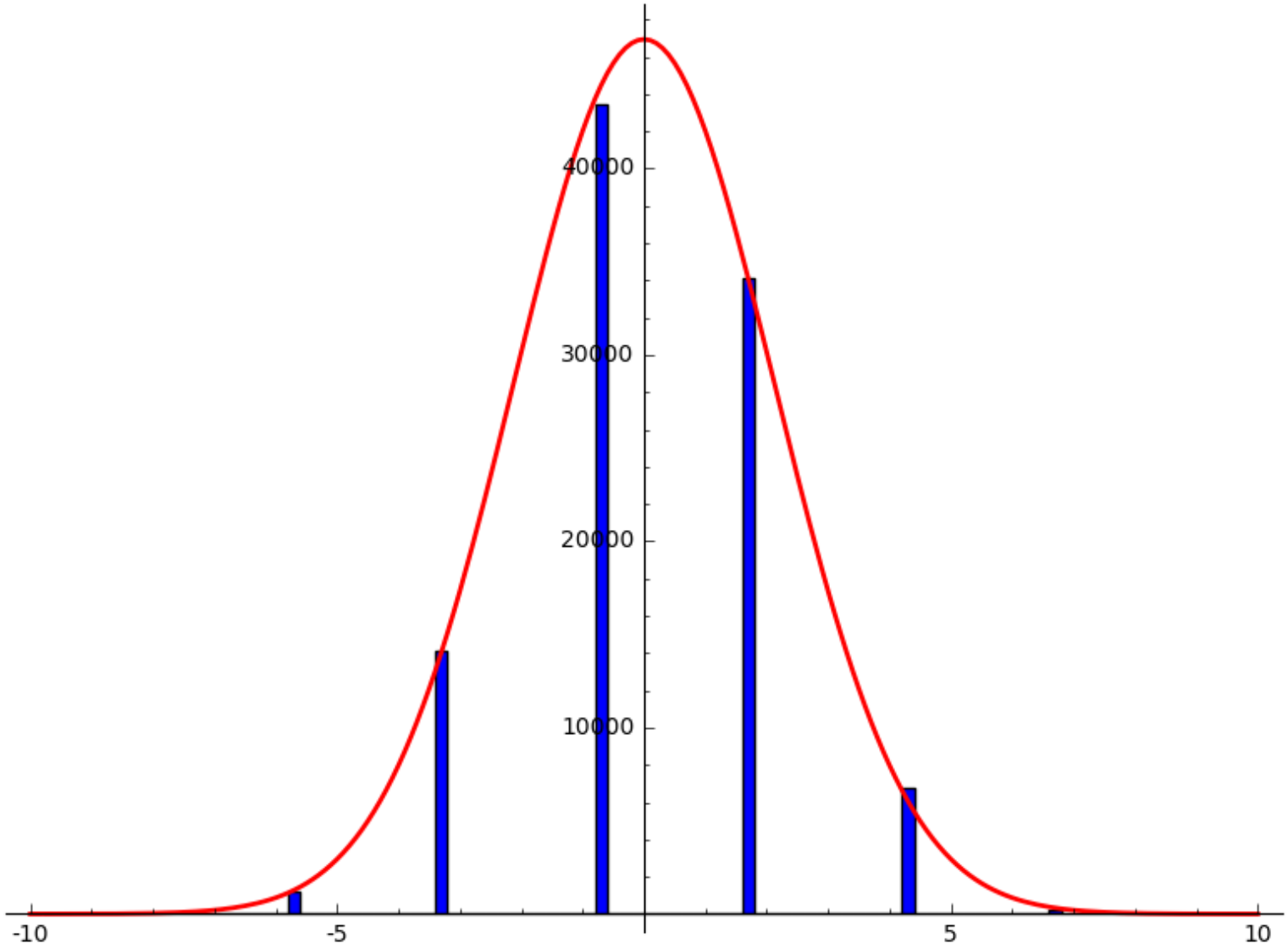
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 100003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



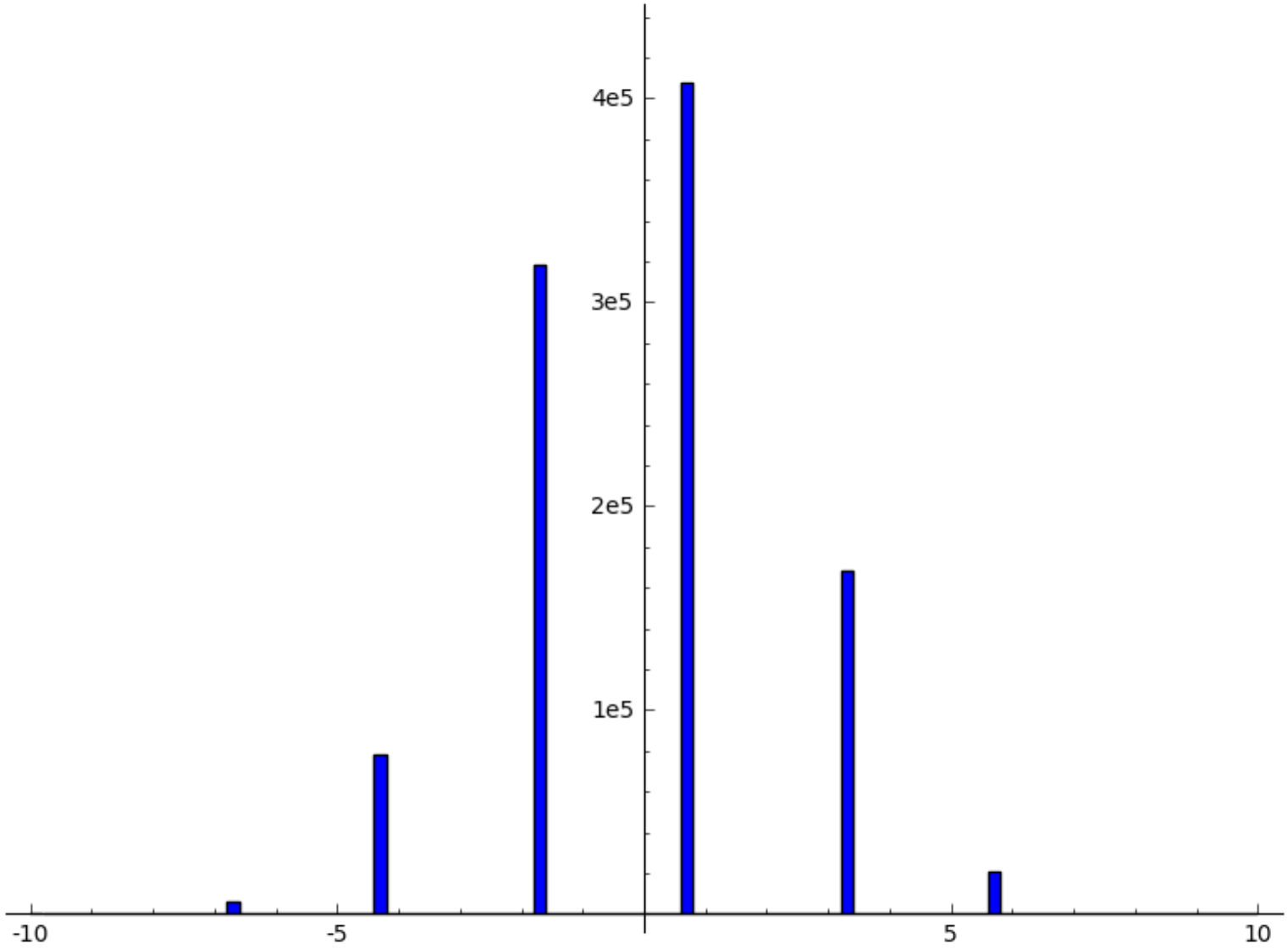
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 100003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



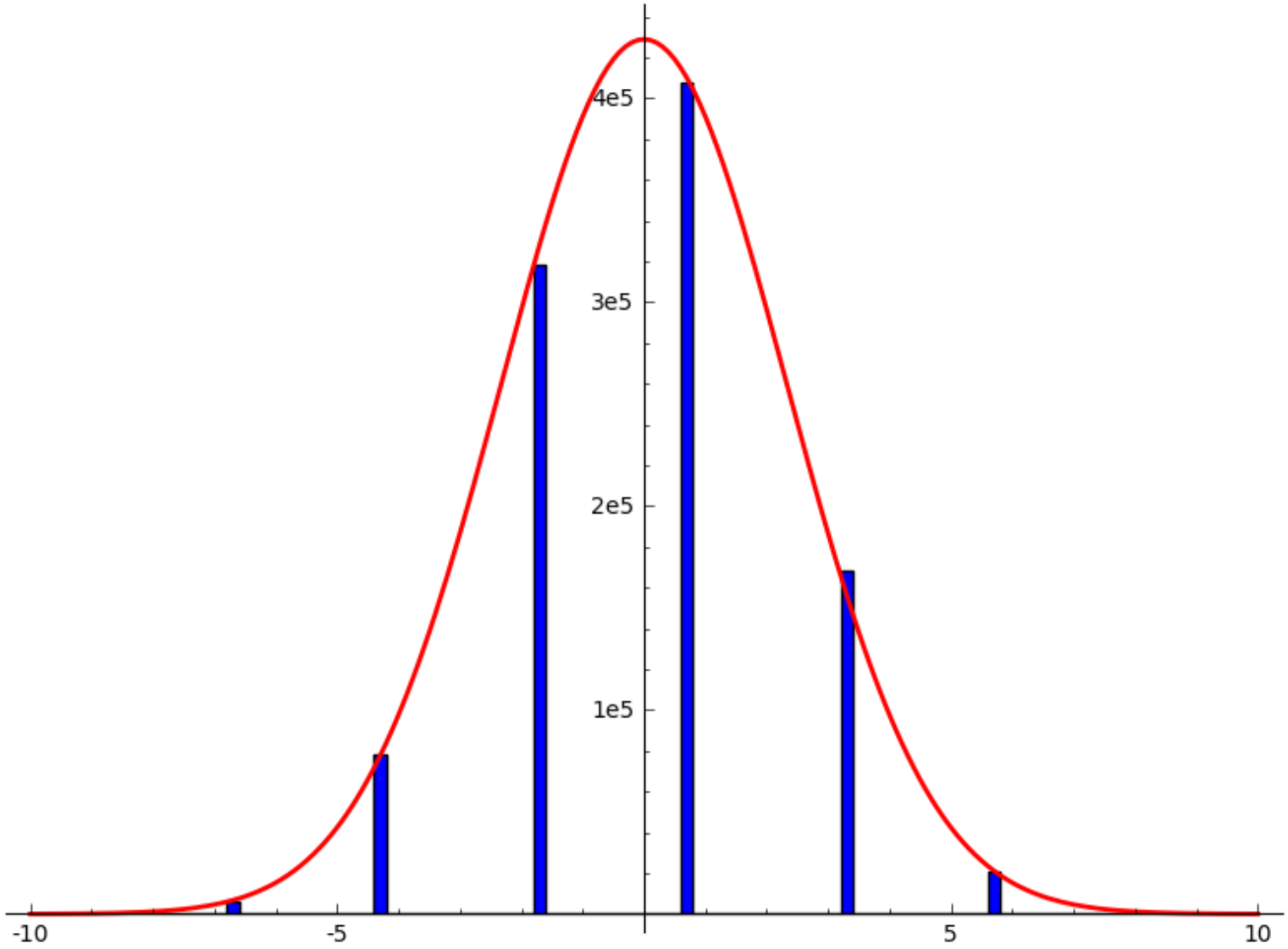
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 1000003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



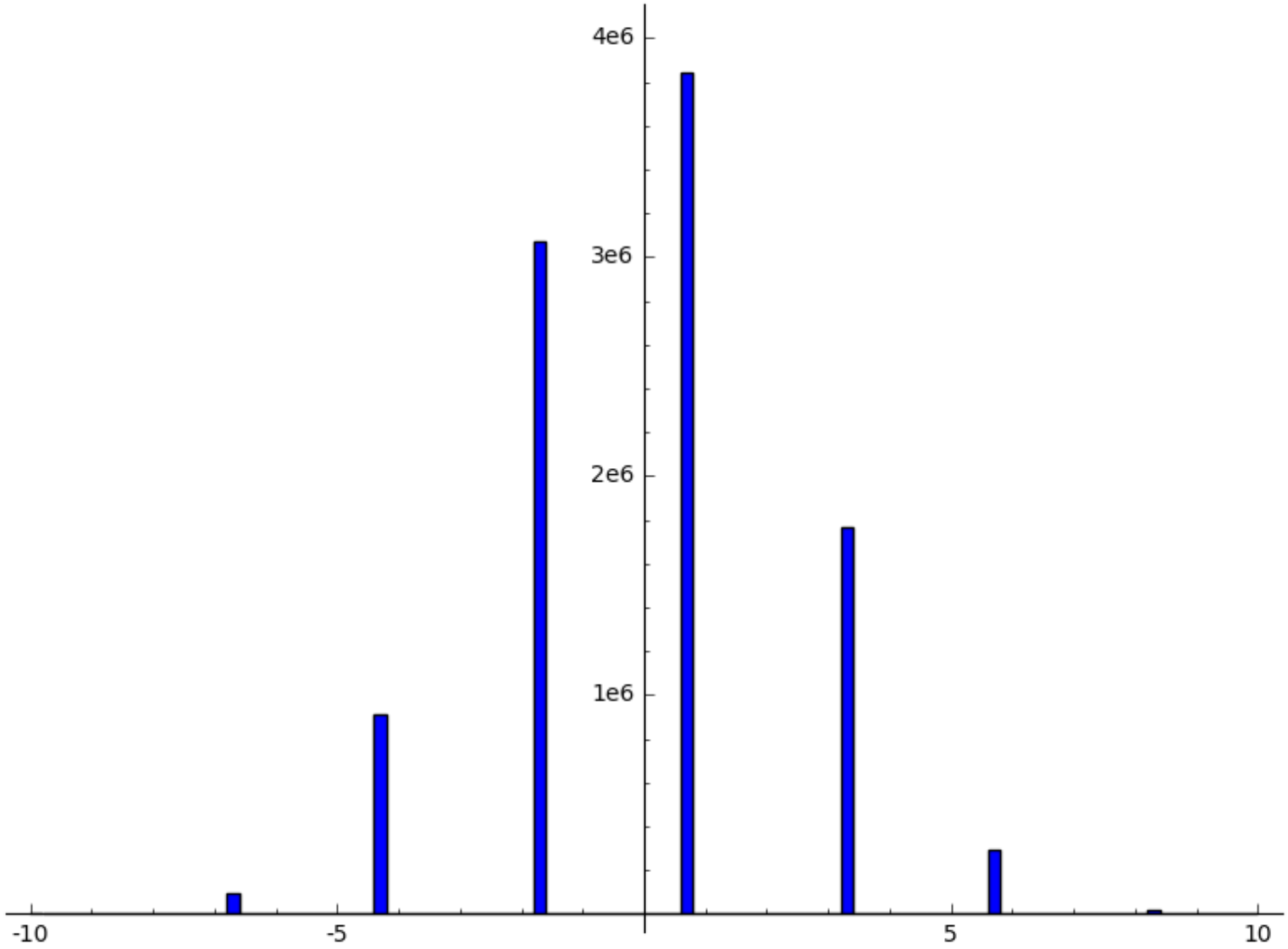
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 1000003, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



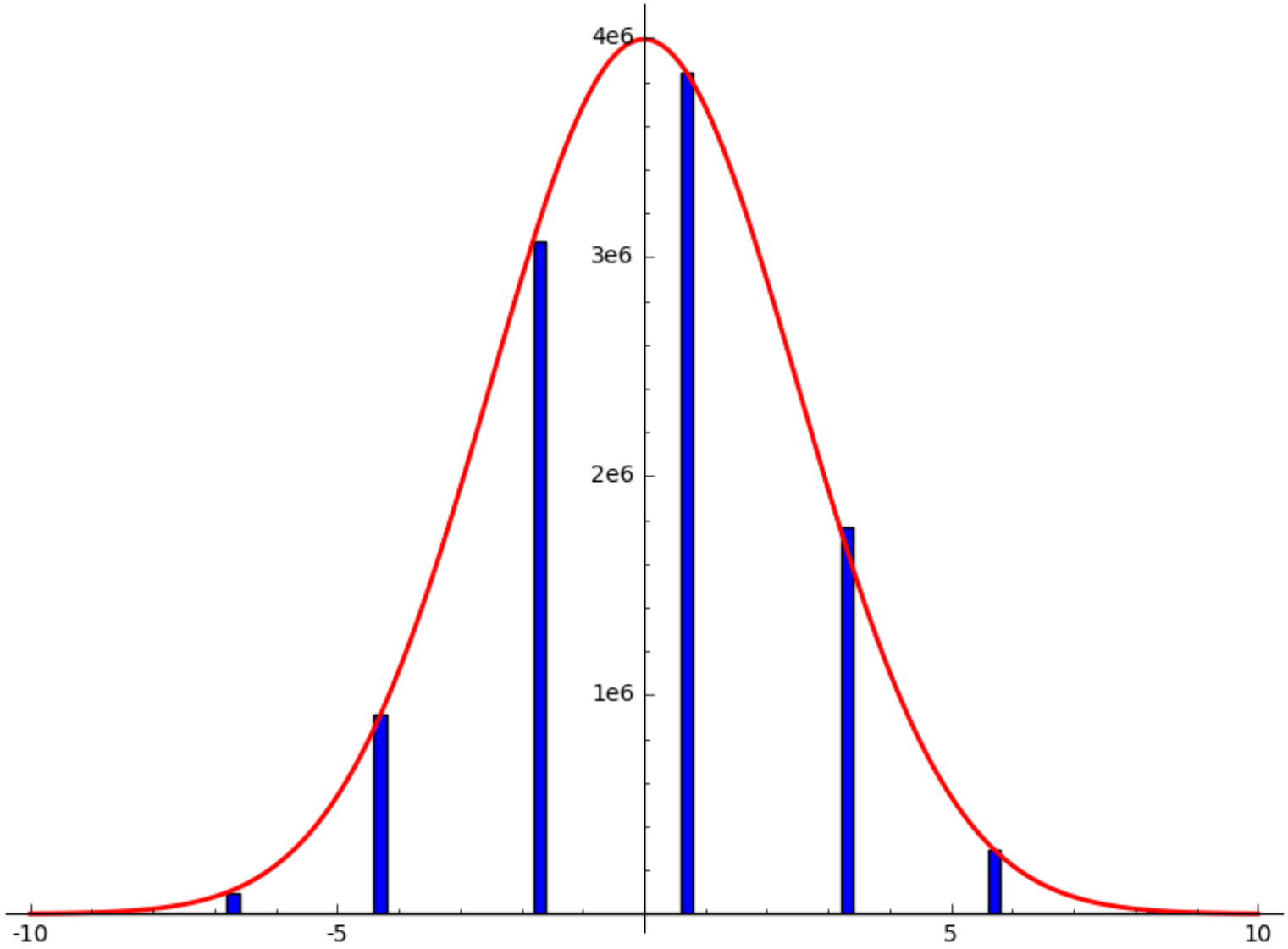
Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 10000019, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



Distribution of modular symbols

Histogram of $\{[a/m] : E = 11A1, m = 10000019, a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$



Distribution of modular symbols

This looks like a normal distribution.

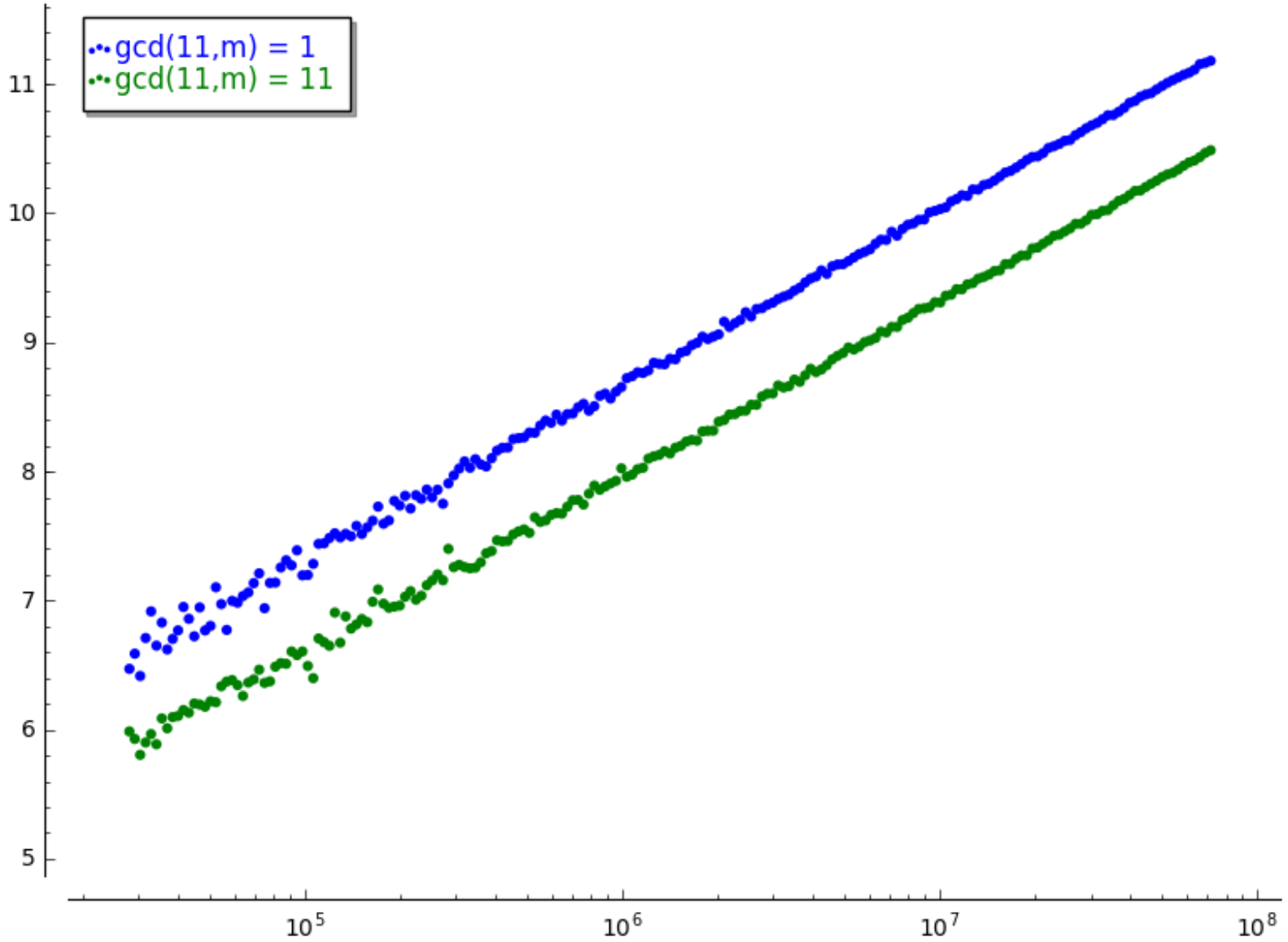
Distribution of modular symbols

This looks like a normal distribution.

How does the variance depend on m?

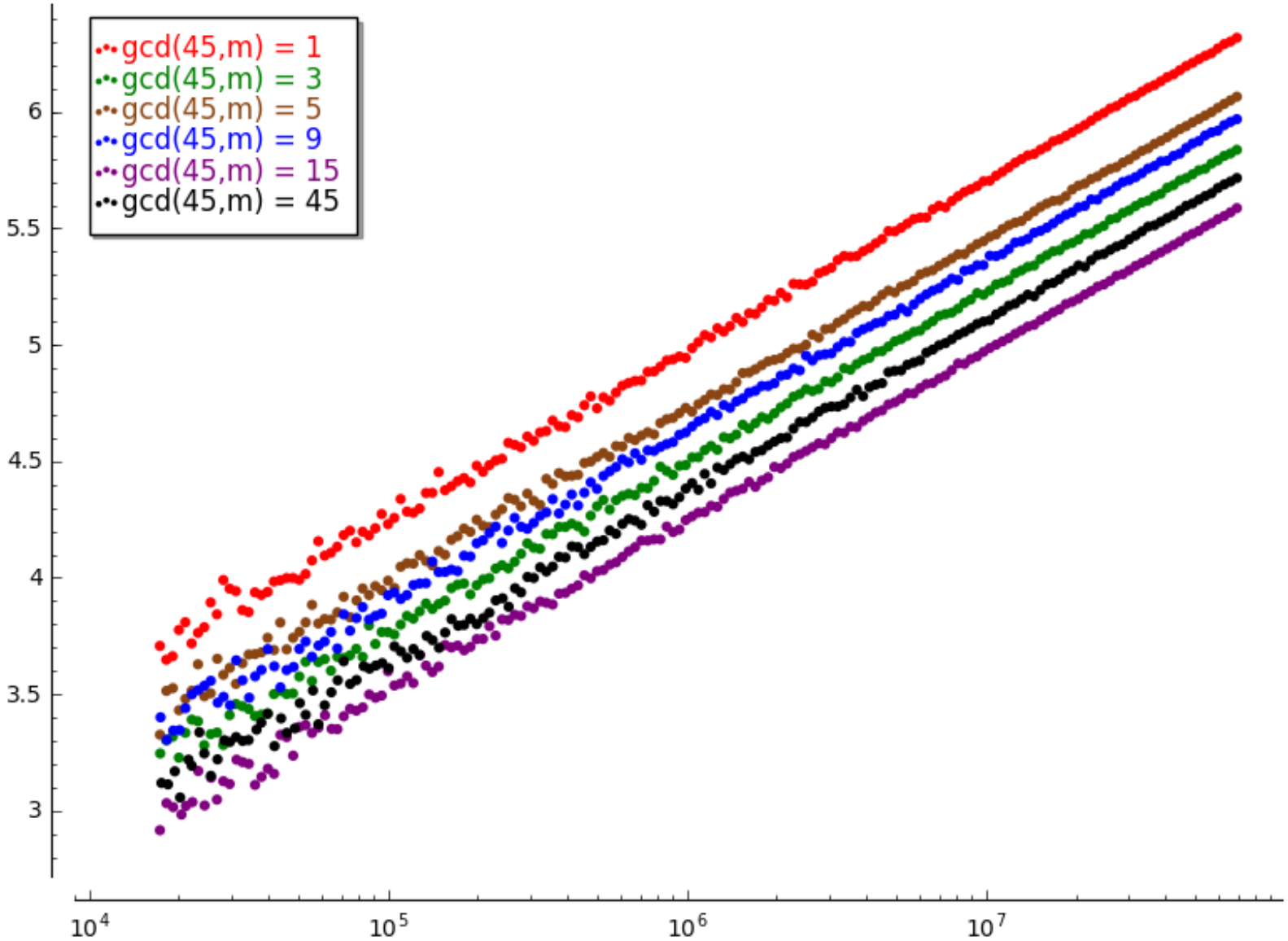
Distribution of variance of modular symbols

Plot of variance vs. m, for $E = 11A1$:



Distribution of variance of modular symbols

Plot of variance vs. m, for $E = 45A1$:



Distribution of modular symbols

For $m \geq 1$ let S_m consider the data:

$$S_m = \{[a/m] : a \in (\mathbb{Z}/m\mathbb{Z})^\times\}.$$

Distribution of modular symbols

Conjecture

There is an explicit constant C_E such that

- *as $m \to \infty$, the distribution of the*

$$\frac{1}{\sqrt{\log(m)}} S_m$$

converge to a normal distribution with mean zero and variance C_E.

Distribution of variance of modular symbols

Conjecture

- *for every divisor κ of N, there is an explicit constant $\mathcal{D}_{E,\kappa}$ such that*

$$\lim_{\substack{m\to\infty \\ (m,N)=\kappa}} \text{Variance}(S_m) - \mathcal{C}_E \log(m) = \mathcal{D}_{E,\kappa}.$$

Distribution of variance of modular symbols

Theorem (Petridis-Risager)

The conjecture above holds if N is squarefree and we average over m.

The variance $\mathcal{C}_E$ is essentially

$$L(\mathrm{Sym}^2(E), 1),$$

and Petridis & Risager compute $\mathcal{D}_{E,\kappa}$ in terms of

$$L(\mathrm{Sym}^2(E), 1) \text{ and } L'(\mathrm{Sym}^2(E), 1).$$

P&R deal with non-holomorphic Eisenstein series twisted by the moments of modular symbols.

Distribution of modular symbols studied via the dynamics of continued fractions

H. Lee and H.S. Sun more recently have proven the same result (for arbtrary N, averaged over m, but without explicit determination of the constants $\mathcal{C}_E$ and $\mathcal{D}_{E,\kappa}$) by considering dynamics of continued fractions.

Distribution of modular symbols studied via the dynamics of continued fractions

H. Lee and H.S. Sun more recently have proven the same result (for arbtrary N, averaged over m, but without explicit determination of the constants $\mathcal{C}_E$ and $\mathcal{D}_{E,\kappa}$) by considering dynamics of continued fractions.

(See also: “Limit laws for rational continued fractions and value distribution of quantum modular forms" by S. Bettin and S. Drappeau).

What does this tell us about the distribution of the theta coefficients?

Fix $d > 1$ and consider cyclic fields such that $[F : \mathbb{Q}] = d$.

Each theta coefficient $c_{F,\gamma}$ is a sum of $\varphi(m)/d$ modular symbols. We (think we) know how the modular symbols are distributed, but are they independent? If so, then the following data

$$\left\{ \frac{c_{F,\gamma}}{\sqrt{C_E \log(m)(\varphi(m)/d)}} \right\}$$

What does this tell us about the distribution of the theta coefficients?

for $F/\mathbb{Q}$ ranging through cyclic extensions of fixed degree d and where, for each such F, $c_{F,\gamma}$ ranges through the corresponding *generic* coefficients. . .

What does this tell us about the distribution of the theta coefficients?

for $F/\mathbb{Q}$ ranging through cyclic extensions of fixed degree d and where, for each such F, $c_{F,\gamma}$ ranges through the corresponding *generic* coefficients. . .

. . . should converge to a normal distribution. . . but it doesn't.

The distributions related to E for cyclic extensions of fixed degree d

Conjecture

Fix E an elliptic curve over $\mathbb{Q}$.

1. *For any positive integer $d > 1$, the data*

$$(F, \gamma) \quad \mapsto \quad \frac{c_{F,\gamma}}{\sqrt{c_E \log(m)(\varphi(m)/d)}}$$

converges to a distribution—which we denote:

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

Growth

Conjecture

1. *The distributions $\Lambda_{E,d}(t)$ are continuous away from $t = 0$ and decrease as t moves away from 0.*

The distributions $\Lambda_{E,d}(t)$ as $d \to \infty$

Conjecture

1. *The distributions $\Lambda_{E,d}(t)$ converge to a normal distribution with variance 1 as d tends to ∞.*

Pictures of $\Lambda_{E,d}(t)$

The collection

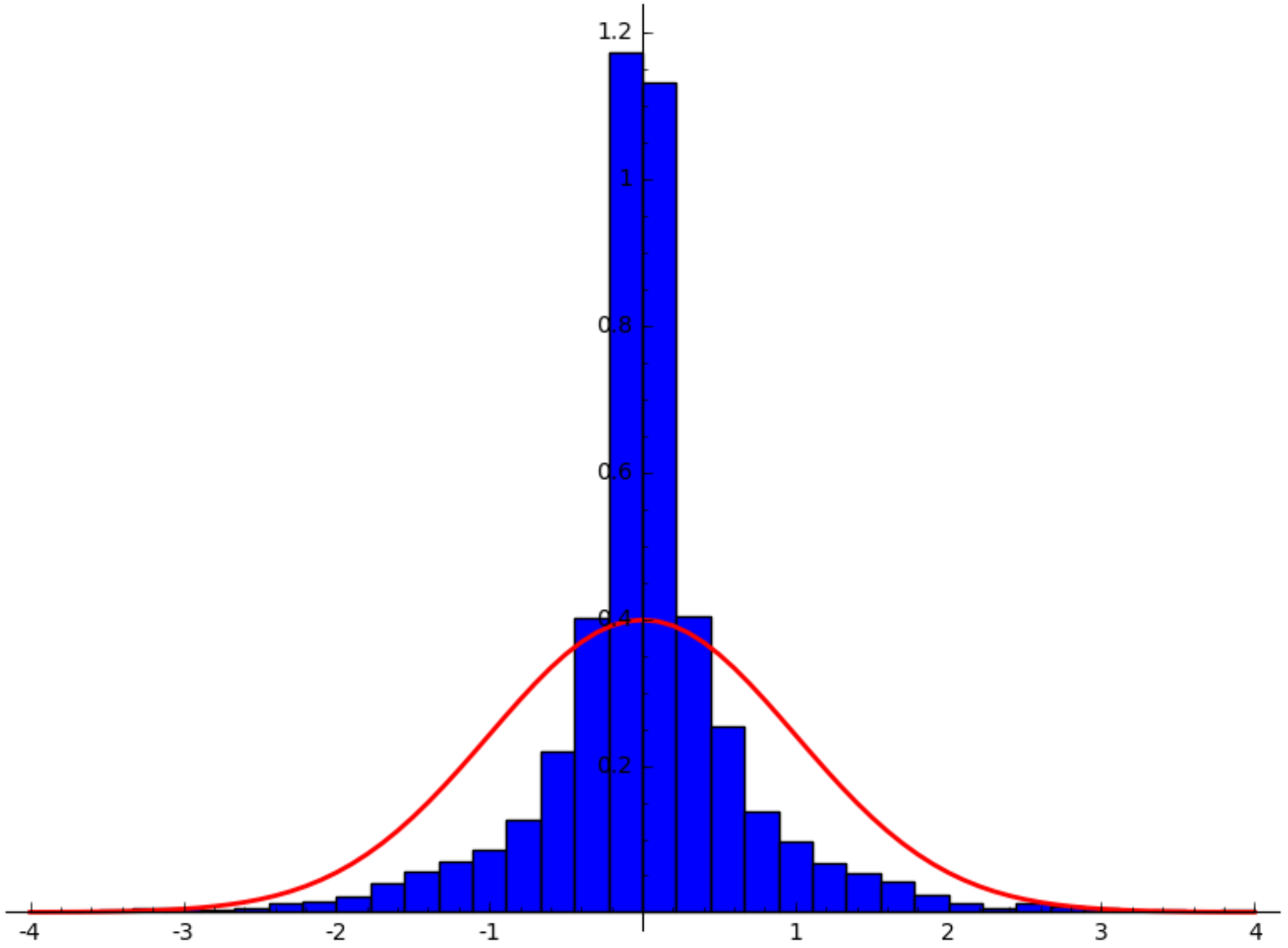
$$\{\Lambda_{E,d}(t) \text{ for } d = 2, 3, 4, \dots\}$$

packages important information about the arithmetic of E. . . . but we don't yet even have conjectures relating their moments to the automorphic form attached to E . . .

Pictures of $\Lambda_{E,d}(t)$

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

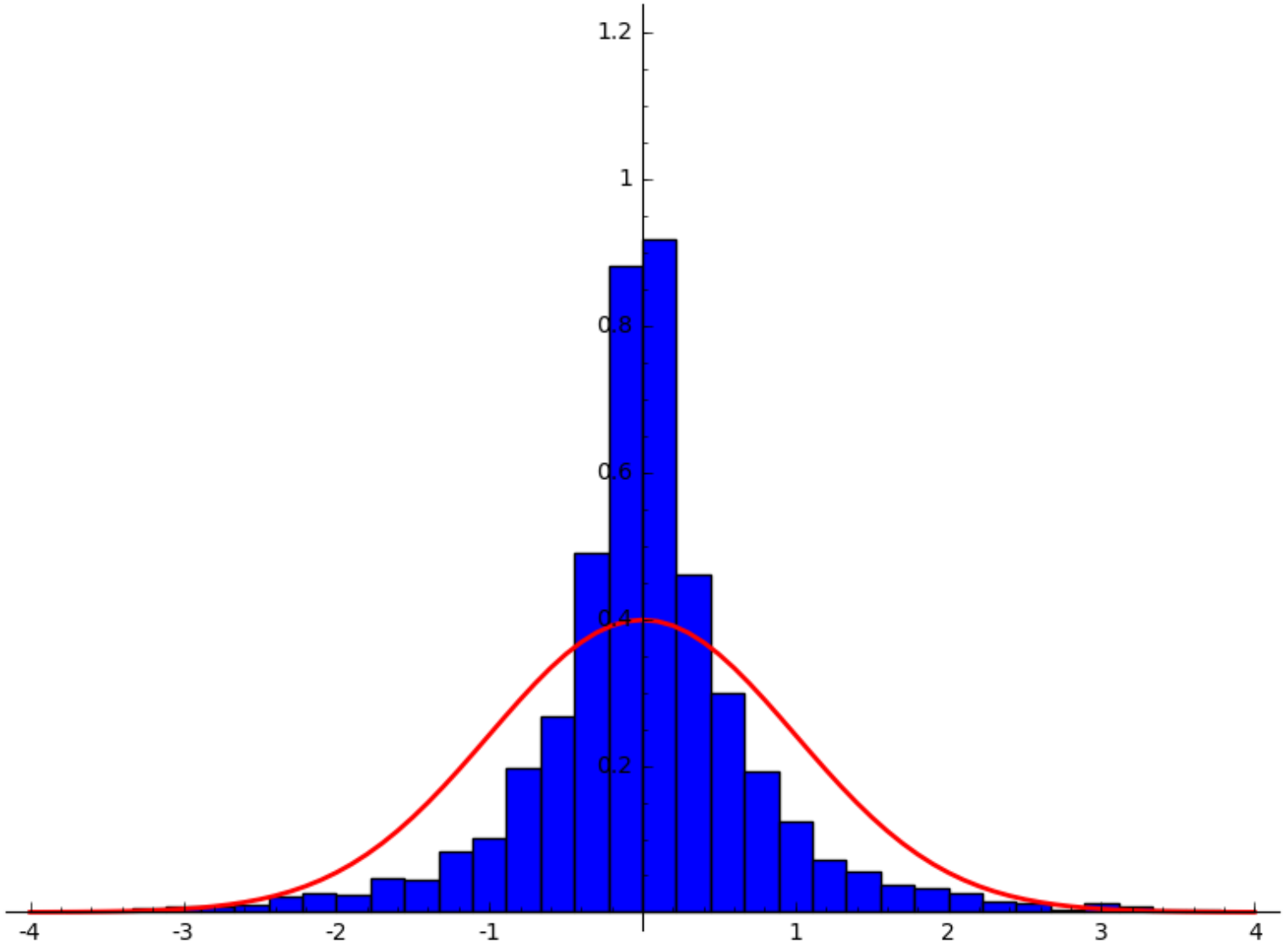
$d = 3$



Pictures of $\Lambda_{E,d}(t)$

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

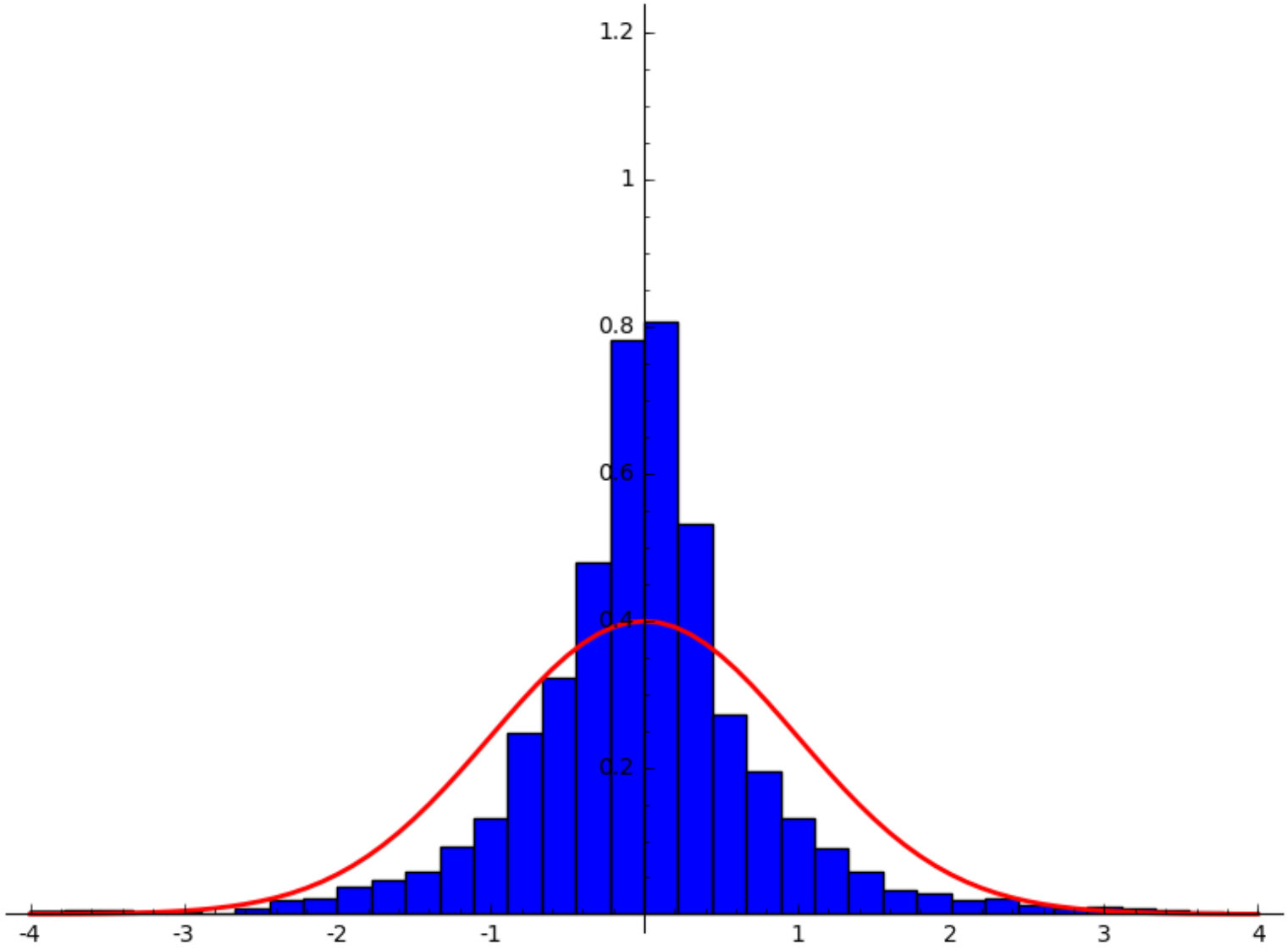
$d = 5$



Pictures of $\Lambda_{E,d}(t)$

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

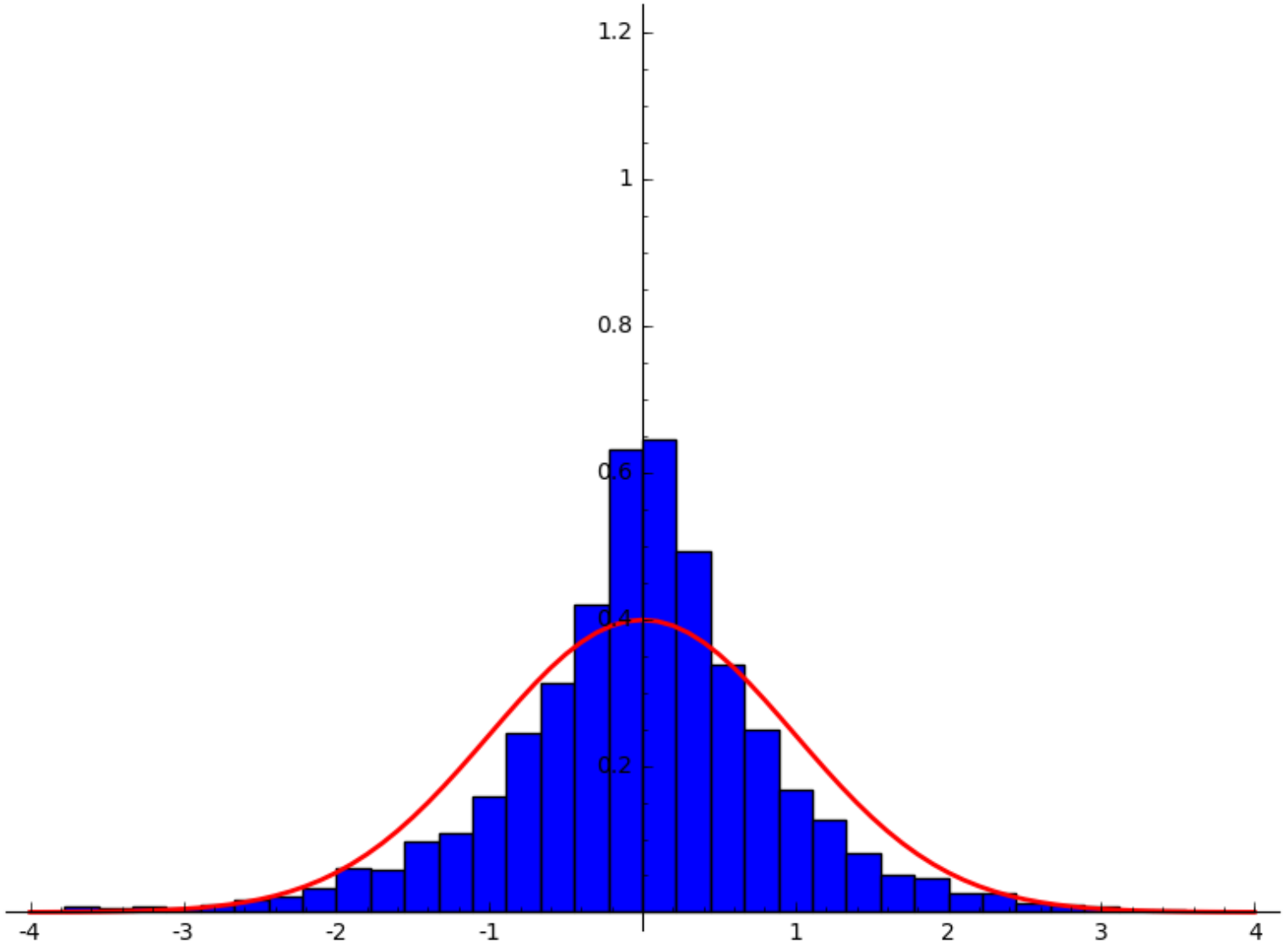
$d = 7$



Pictures of $\Lambda_{E,d}(t)$

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

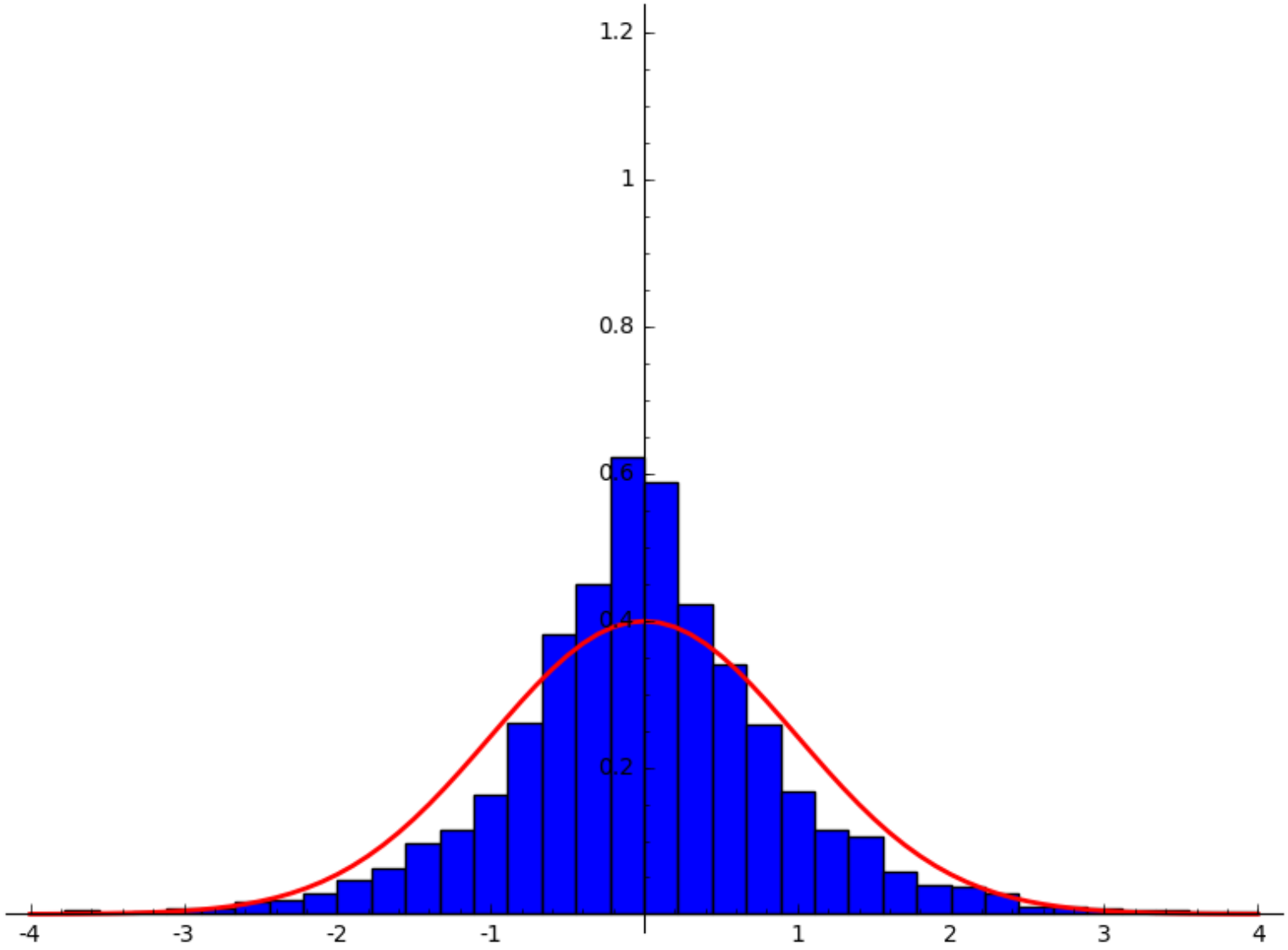
$d = 11$



Pictures of $\Lambda_{E,d}(t)$

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

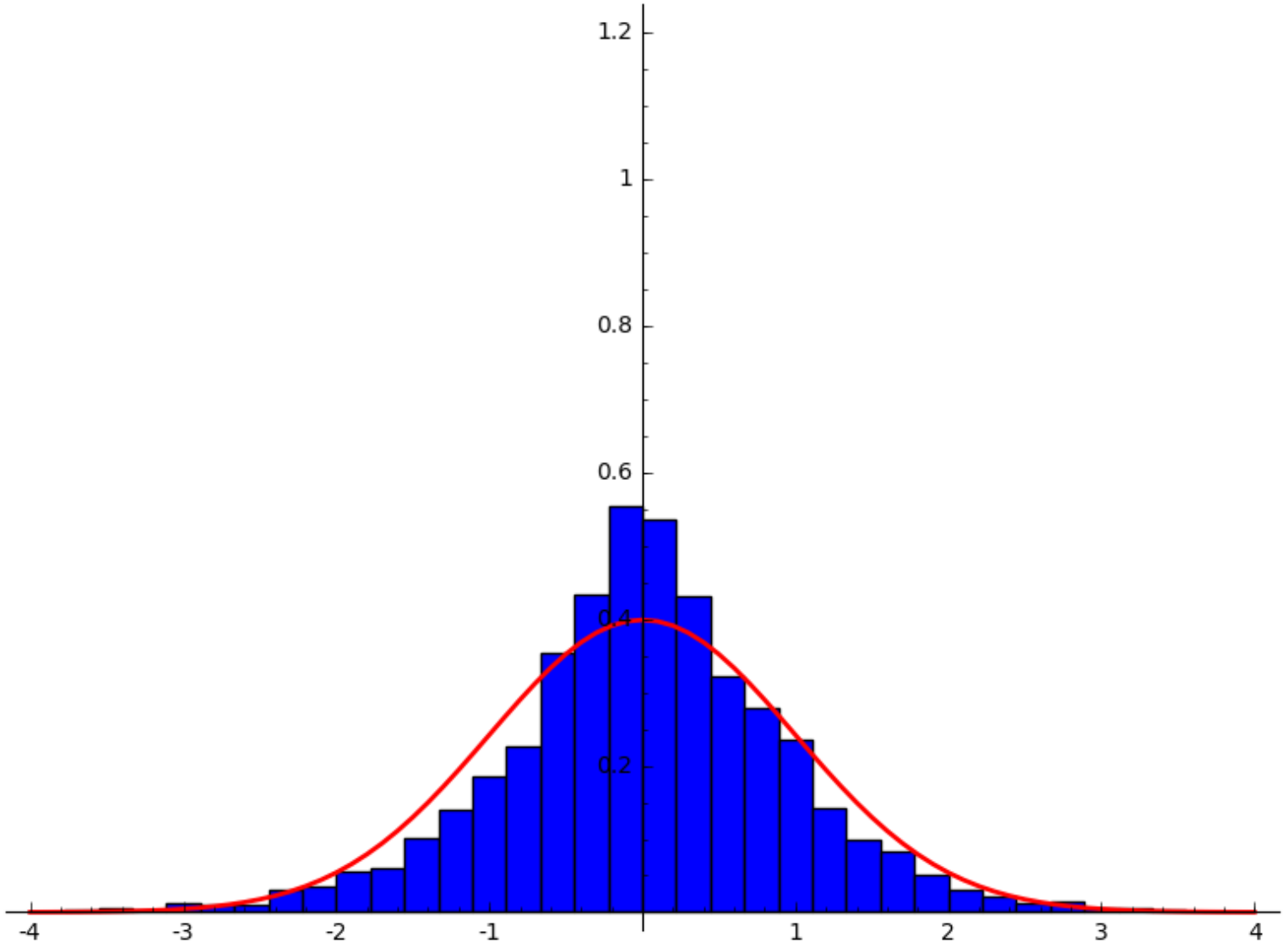
$d = 13$



Pictures of $\Lambda_{E,d}(t)$

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

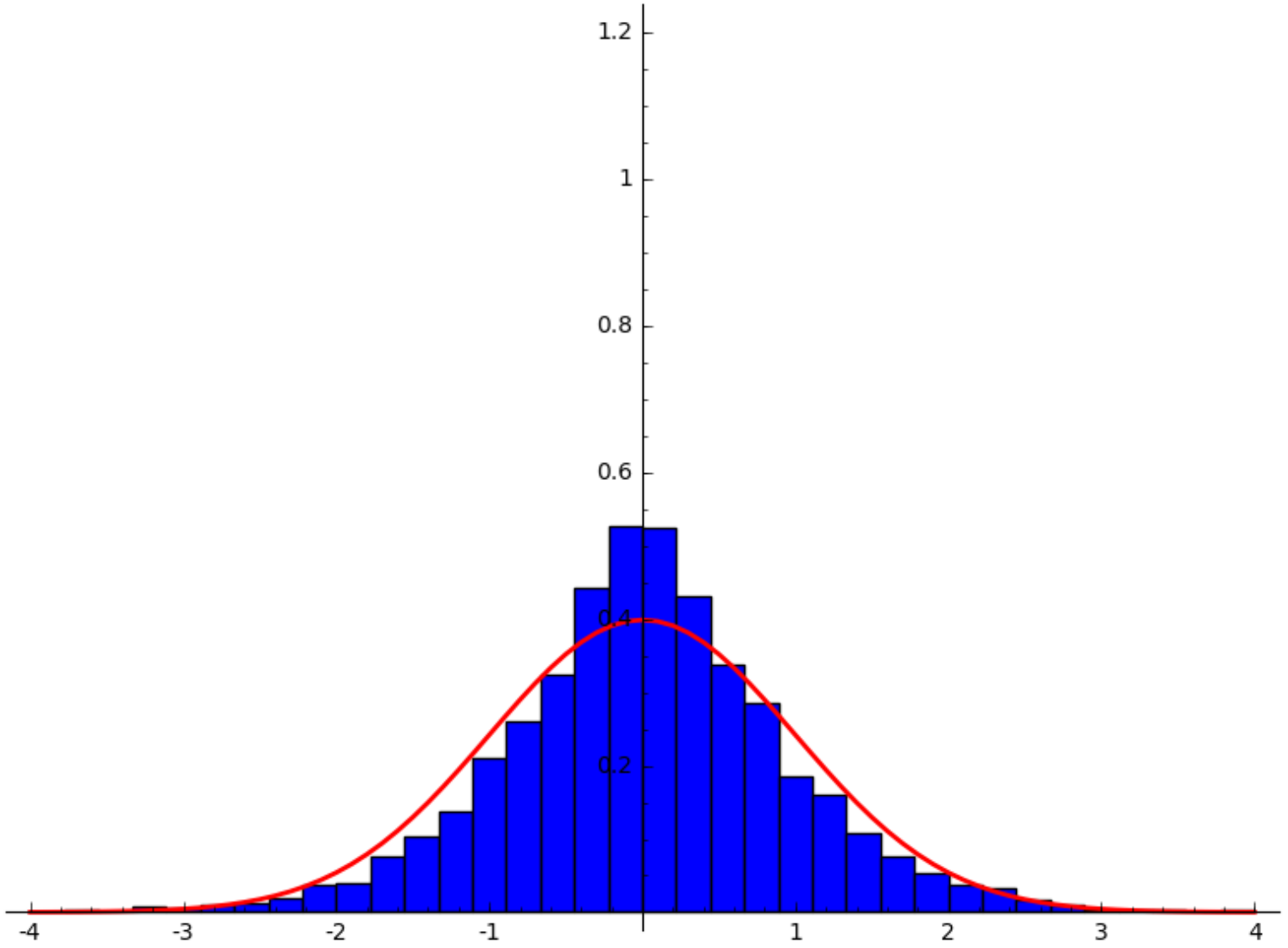
$d = 17$



Pictures of $\Lambda_{E,d}(t)$

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

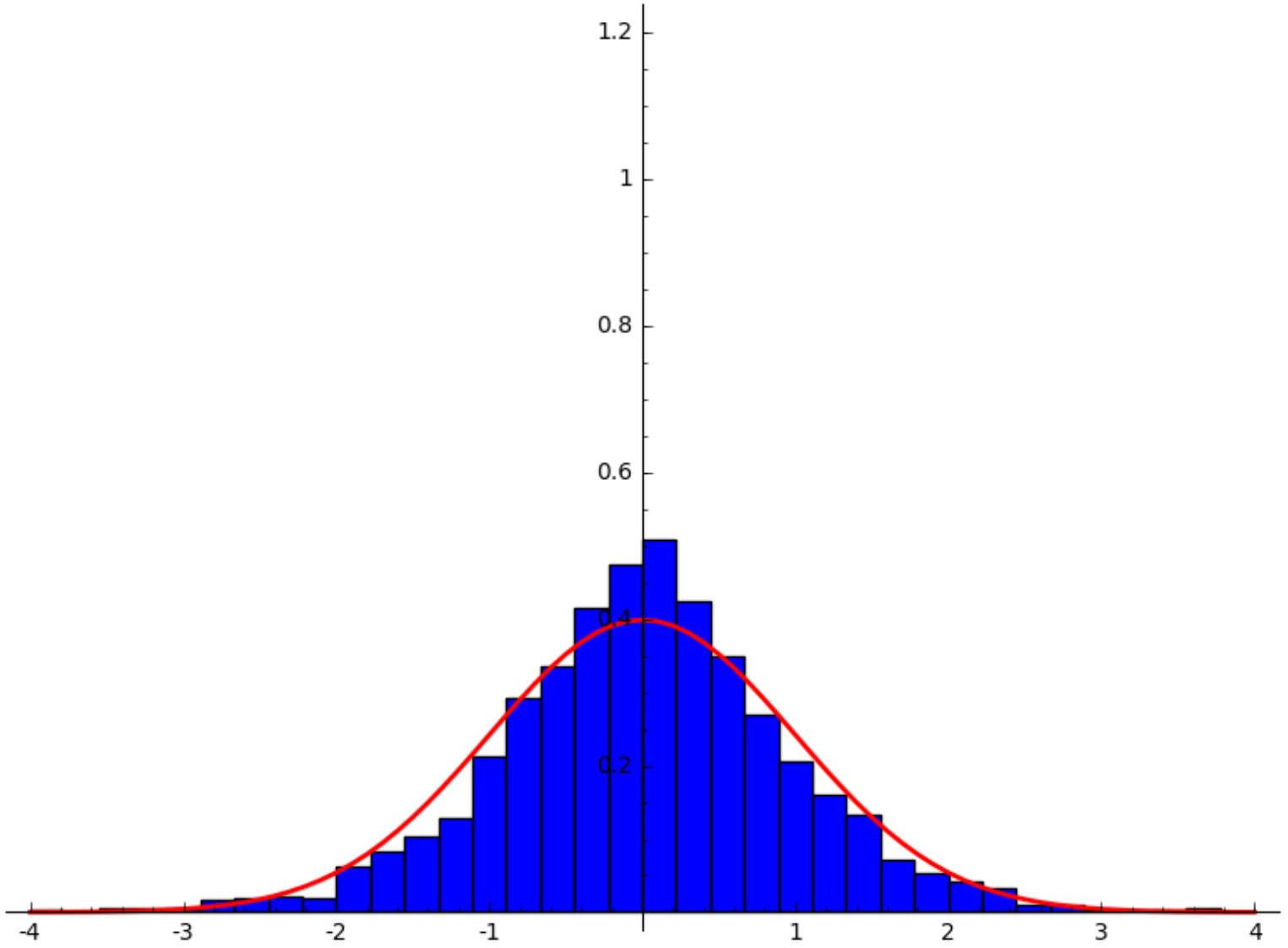
$d = 23$



Pictures of $\Lambda_{E,d}(t)$

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

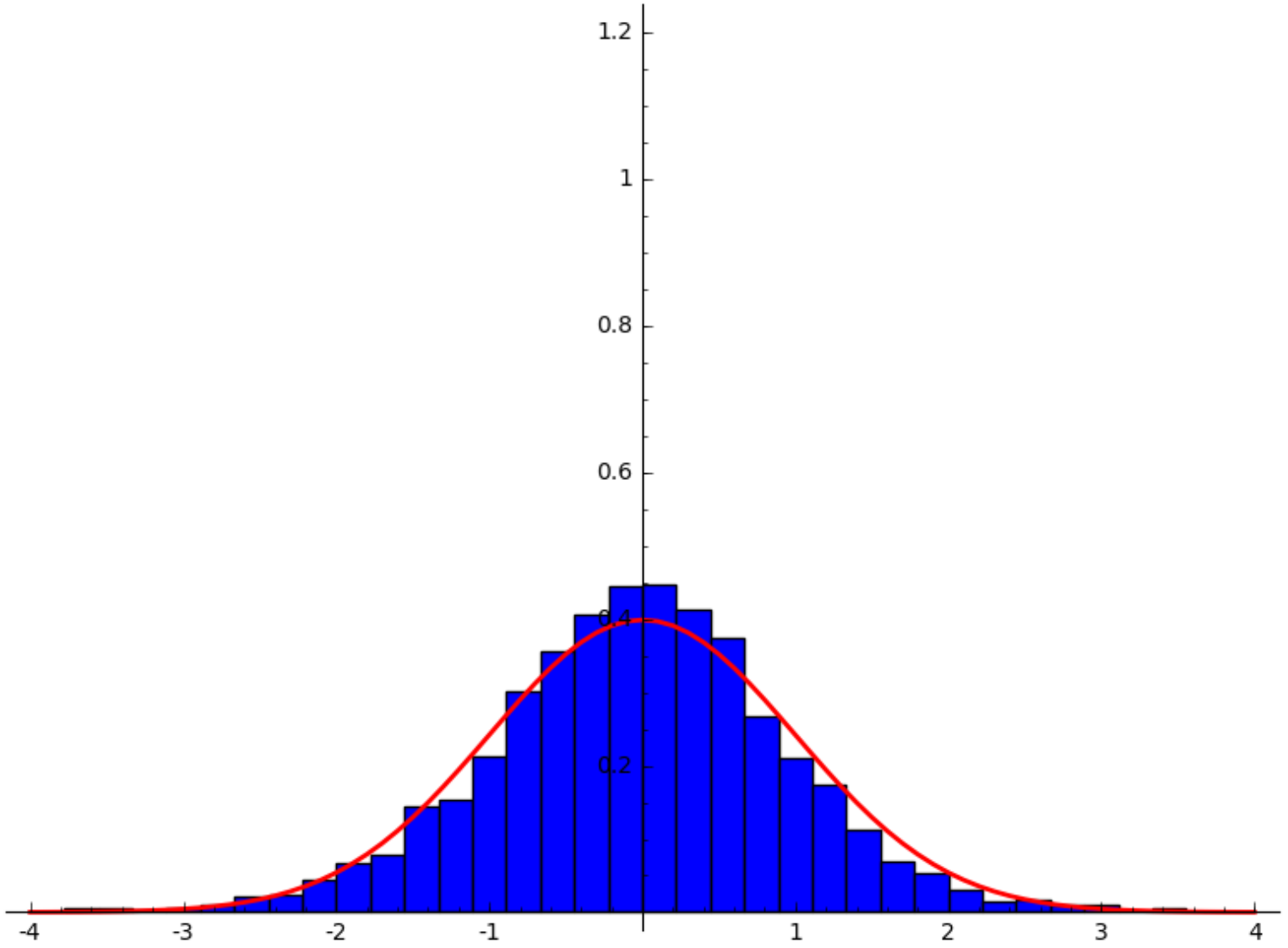
$d = 31$



Pictures of $\Lambda_{E,d}(t)$

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

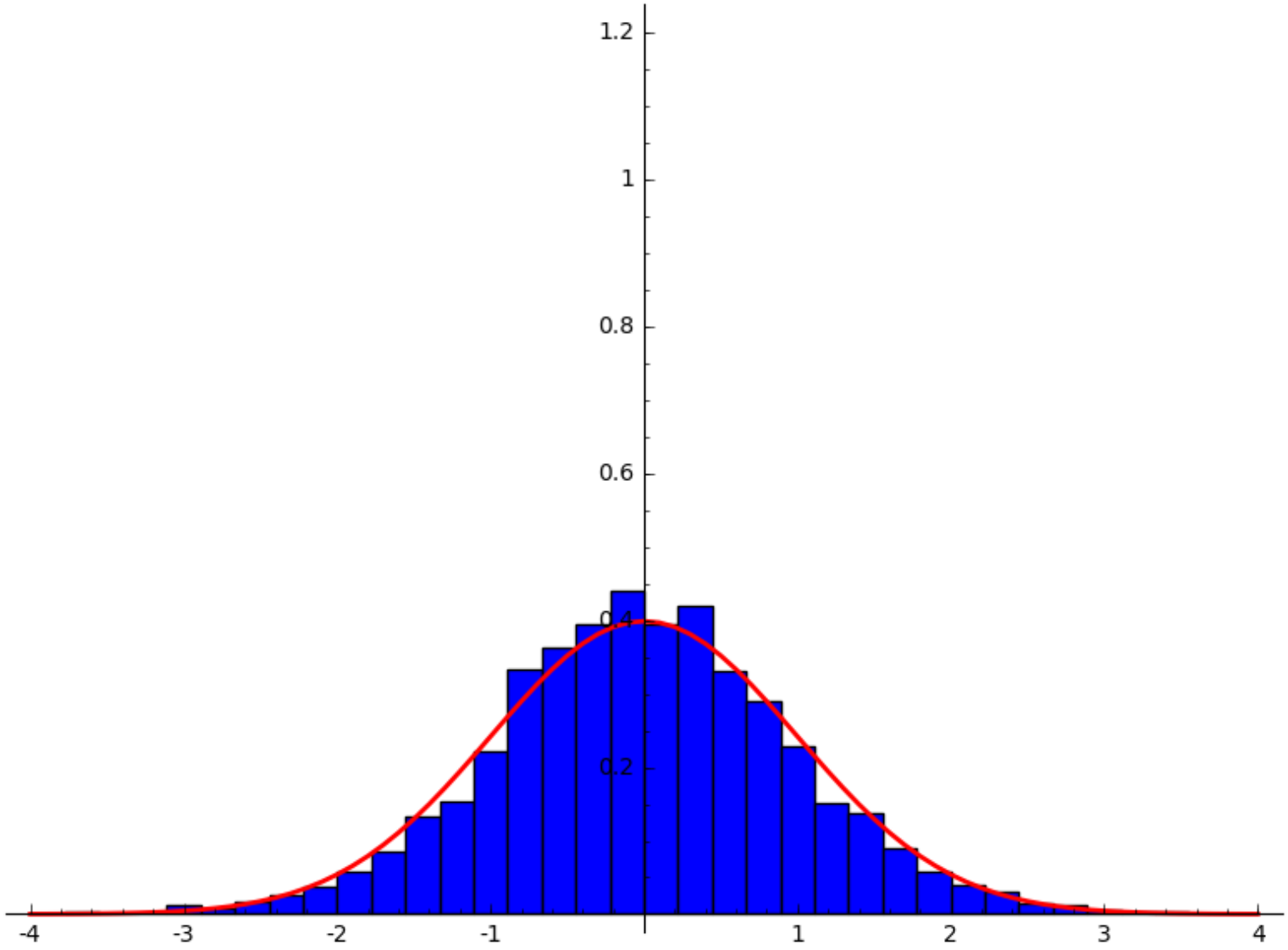
$d = 41$



Pictures of $\Lambda_{E,d}(t)$

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

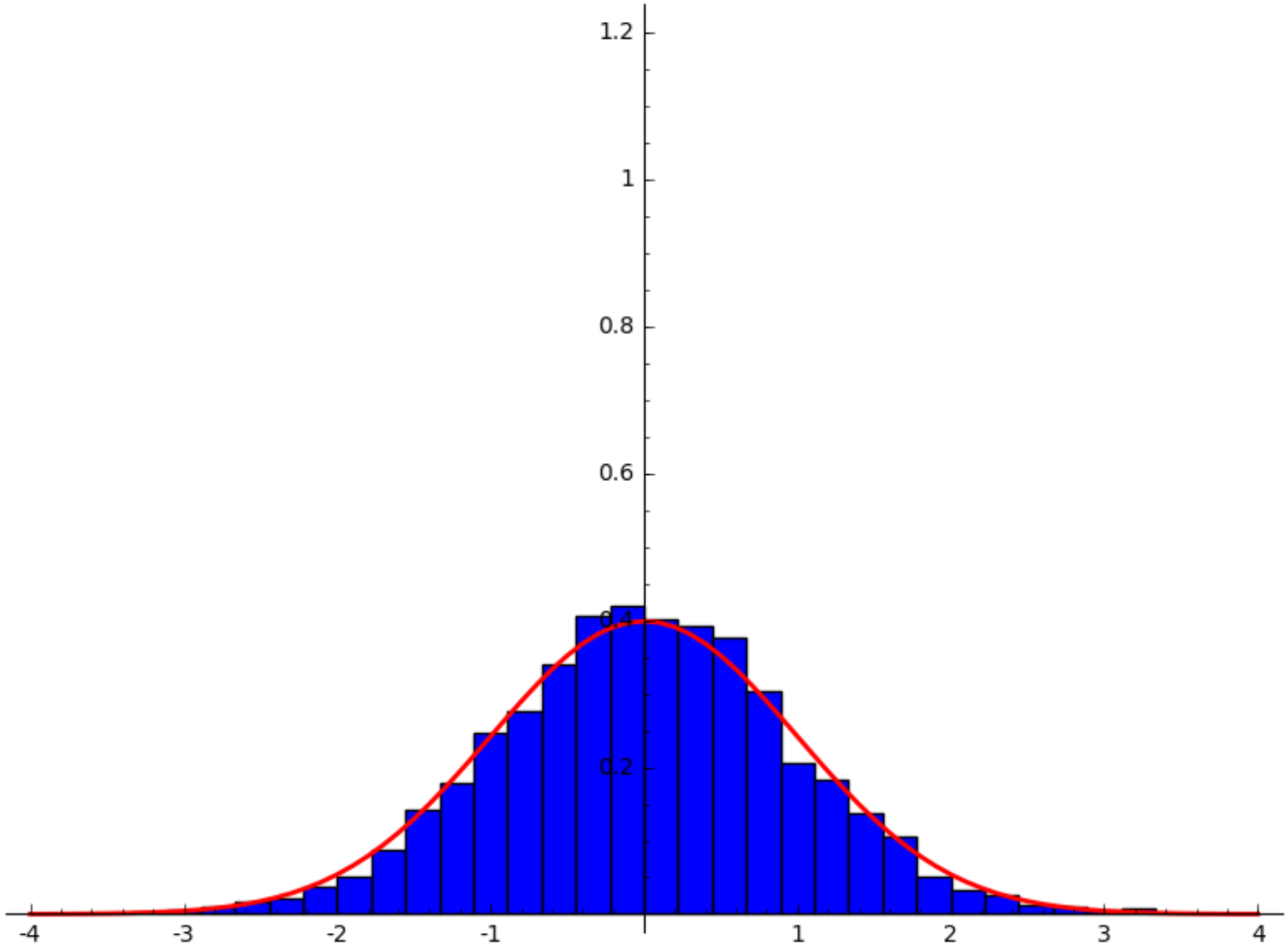
$d = 53$



Pictures of $\Lambda_{E,d}(t)$

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

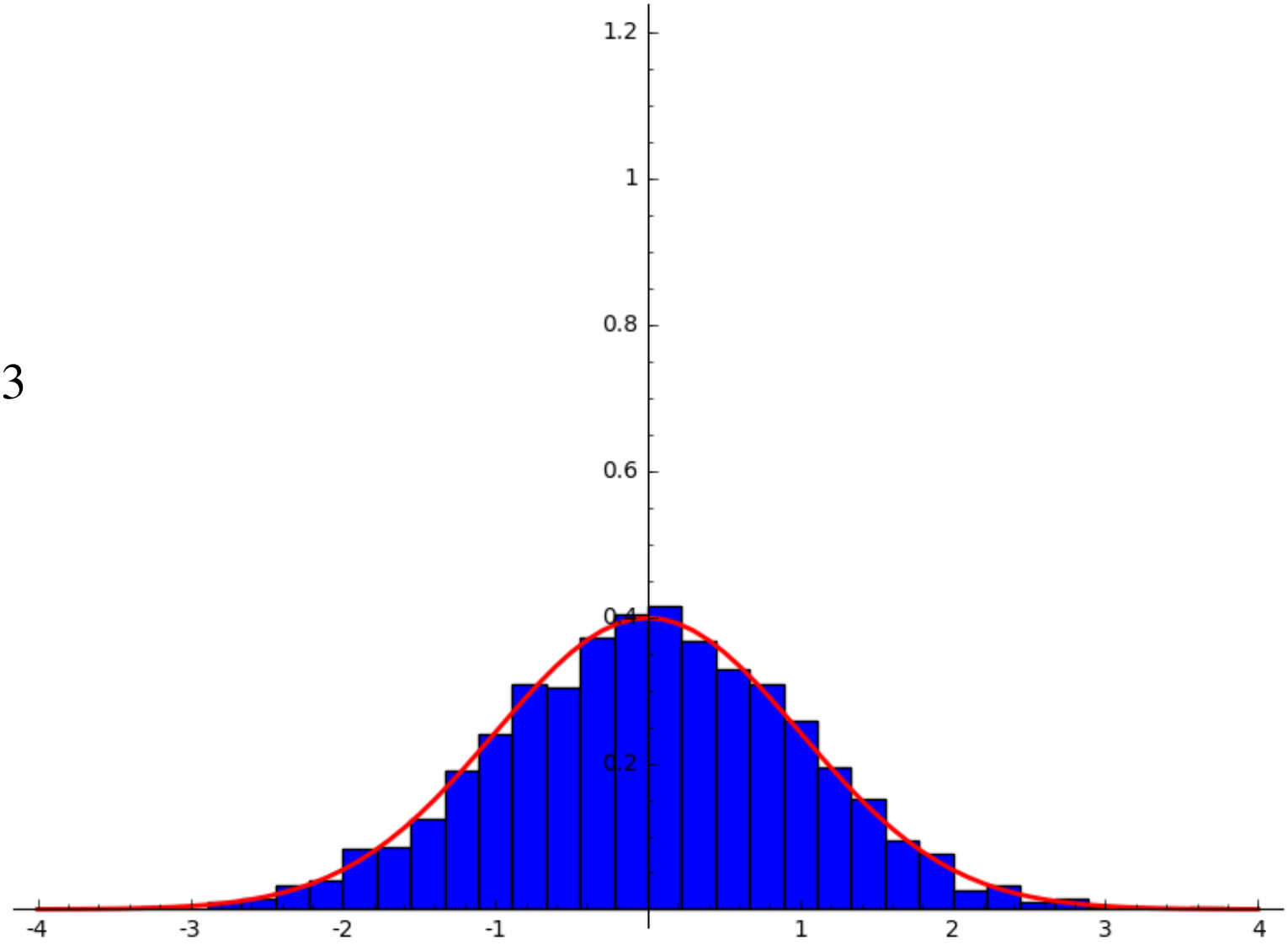
$d = 97$



Pictures of $\Lambda_{E,d}(t)$

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

$d = 293$



A basic invariant: the **growth** of $\Lambda_{E,d}(t)$ (near 0)

Define:

$$f(\epsilon) = f_{E,d}(\epsilon) := \quad \frac{1}{\epsilon}\int_{-\epsilon/2}^{t+\epsilon/2} \Lambda_{E,d}(t))$$

for $0 < \epsilon \leq 2/3$.

Our heuristic (only) depends on:

- some growth bounds for $\Lambda_{E,d}(t)$,
- some statistical independence of different theta coefficients of the same theta element.

Growth bounds for $\Lambda_{E,d}(t)$

Numerical experiments seem to offer support for the following conjecture.

Conjecture

There is a constant M depending only on E, and a sequence of real numbers β_d converging to zero as $d \to \infty$ such that

Growth bounds for $\Lambda_{E,d}(t)$

Conjecture

- $$f_{E,d}(\epsilon) \leq M\epsilon^{-1/2}|\log(\epsilon)|^{\beta_2}$$

  for $d = 2$ *and*

- $$f_{E,d}(\epsilon) \leq M|\log(\epsilon)|^{\beta_d}$$

  for $d \geq 3$.

but the only thing we really need for our heuristic to get going is. . .

Weaker Conjecture

Fix an elliptic curve E over $\mathbb{Q}$ and $d > 2$. There is a constant M and a sequence of real numbers $\alpha_d \leq 2/3$ converging to zero as $d \to \infty$ such that:

$$f_{E,d}(\epsilon) \leq M\epsilon^{-\alpha_d}$$

for $d \geq 3$.

The “Probability" that two theta coefficients are equal

Let $F/\mathbb{Q}$ be cyclic of degree d. What is the probability that

$$\frac{c_{F,\gamma_0}}{\sqrt{\mathcal{C}_E \log(m)\varphi(m)/d}} = \frac{c_{F,\gamma_1}}{\sqrt{\mathcal{C}_E \log(m)\varphi(m)/d}}$$

for two different elements $\gamma_0, \gamma_1 \in \mathrm{Gal}(F/\mathbb{Q})$?

The “Probability" that two theta coefficients are equal

Considering that

$$\tau := \frac{1}{\sqrt{C_E \log(m)\varphi(m)/d}}$$

is the *‘mesh’* of our normalization, we take that probability to be measured by $\tau f_{E,d}(\tau)$.

Computations suggest the conjecture that:

. . . the $c_{F,\gamma}$ are relatively uncorrelated beyond being subject to the Atkin-Lehner relation.

E.g., if d is prime, as χ ranges through all Dirichlet characters of order d, thinking of

$$\text{“Prob}[L(E,\chi,1)=0]\text{”}$$

as the probability that for a given $F/\mathbb{Q}$ cyclic of degree d the theta coefficients $c_{F,\gamma}$ are all equal we might expect that:

Heuristic

"Prob$[L(E,\chi,1)=0]$" is given by $\left(\tau f_{E,d}(\tau)\right)^{m(d)}$.

Heuristic

$$\text{“Prob}[L(E,\chi,1)=0]\text{” is given by } \left(\tau f_{E,d}(\tau)\right)^{m(d)}.$$

with $m(d) =$

the number of ‘independent’ theta-coefficients; i.e.:

$$m(d) = \frac{\phi(d)}{2}.$$

Consequences of the Heuristic

But even assuming far less correlation:

$$m(d) \gg \log(d),$$

our heuristic gives us:

Heuristic

$$\sum_{d\,:\,\phi(d) > \frac{4}{1-\alpha_d}} \quad \sum_{\chi \text{ order } d} \text{“Prob}[L(E,\chi,1) = 0]\text{”} \quad \textit{converges.}$$

Consequences of the heuristic

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

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.

Alternatively:

Conjecture

Suppose E is an elliptic curve over $\mathbb{Q}$, and let M denote the compositum of all abelian fields of degrees ≤ 5 and 8.

Then $E(\mathbb{Q}^{\mathrm{ab}})/E(M)$ is finitely generated.

Abelian varieties? and over more general number fields?

At present it seems difficult to collect substantial amounts of numerical data to give us any sense of what to expect regarding the following question:

Questions

Is there a finite bound $p(g)$ such that for A any abelian variety over $\mathbb{Q}$ of dimension g, and any prime $p \geq p(g)$ there are only finitely many cyclic extensions $L/\mathbb{Q}$ of degree p that are Diophantine **un-***stable for A?*

Thoughts about the starlike structure of the theta-coefficients of the same theta-elements