A heuristic for abelian points on elliptic curves

Barry Mazur, Harvard University
Karl Rubin, UC Irvine

MIT, August 2018

Growth of ranks in cyclic extensions

Fix an elliptic curve E over a number field K.

Question

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

By considering the action of $\mathrm{Gal}(F/K)$ on $E(F) \otimes \mathbb{Q}$, the representation theory of $\mathbb{Q}[\mathrm{Gal}(F/K)]$ shows that it is enough to consider the case where F/K is cyclic.

General philosophy: it's hard to find $P \in E(K^{\mathrm{ab}})$ with $K(P)/K$ cyclic of large degree.

Growth of ranks: analytic approach

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:

Question

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

Modular symbols

Fix $E/\mathbb{Q}$ once and for all, and suppress it from the notation.

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

Fix $E/\mathbb{Q}$ once and for all, and suppress it from the notation.

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.

Theorem

For every primitive even Dirichlet character χ of conductor m,

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

theta elements

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.

theta elements

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.

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

- $\sigma_{a,m} \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})$ the automorphism $\zeta_m \mapsto \zeta_m^a$,
- $\theta_m := \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} [a/m]\sigma_{a,m} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})]$,
- $\theta_F := \theta_m|_F \in \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})]$.

theta elements

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.

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

- $\sigma_{a,m} \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})$ the automorphism $\zeta_m \mapsto \zeta_m^a$,
- $\theta_m := \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} [a/m]\sigma_{a,m} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})]$,
- $\theta_F := \theta_m|_F \in \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})]$.

If χ is an even character of $\mathrm{Gal}(F/\mathbb{Q})$, then

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

theta coefficients

We have

$$\theta_F = \sum_{\gamma \in \mathrm{Gal}(F/\mathbb{Q})} c_{F,\gamma}\gamma$$

where

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

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

theta coefficients

We have

$$\theta_F = \sum_{\gamma \in \mathrm{Gal}(F/\mathbb{Q})} c_{F,\gamma}\gamma$$

where

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

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*

$$\chi(\theta_F) = 0 \iff c_{F,\gamma} = c_{F,\gamma'}\ \forall \gamma, \gamma' \in \mathrm{Gal}(F/\mathbb{Q}).$$

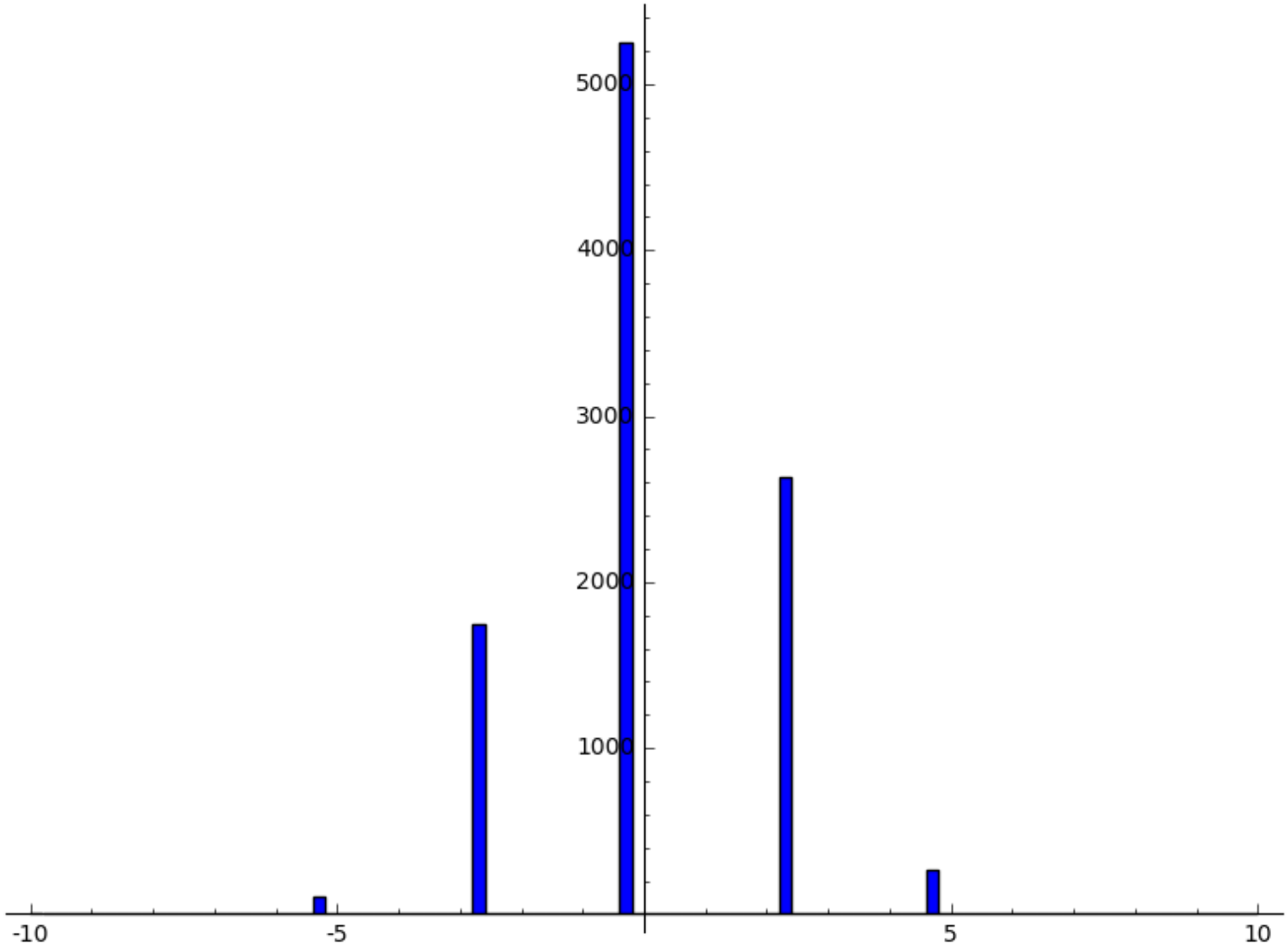
Modular symbols

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

- There is a $\delta \in \mathbb{Z}$ independent of r such that $\delta[r] \in \mathbb{Z}$
- $\boxed{[r] = [r+1]}$ since $f_E(z) = f_E(z+1)$
- $\boxed{[r] = [-r]}$ by definition
- 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 $\boxed{a_\ell[r] = [\ell r] + \sum_{i=0}^{\ell-1}[(r+i)/\ell]}$

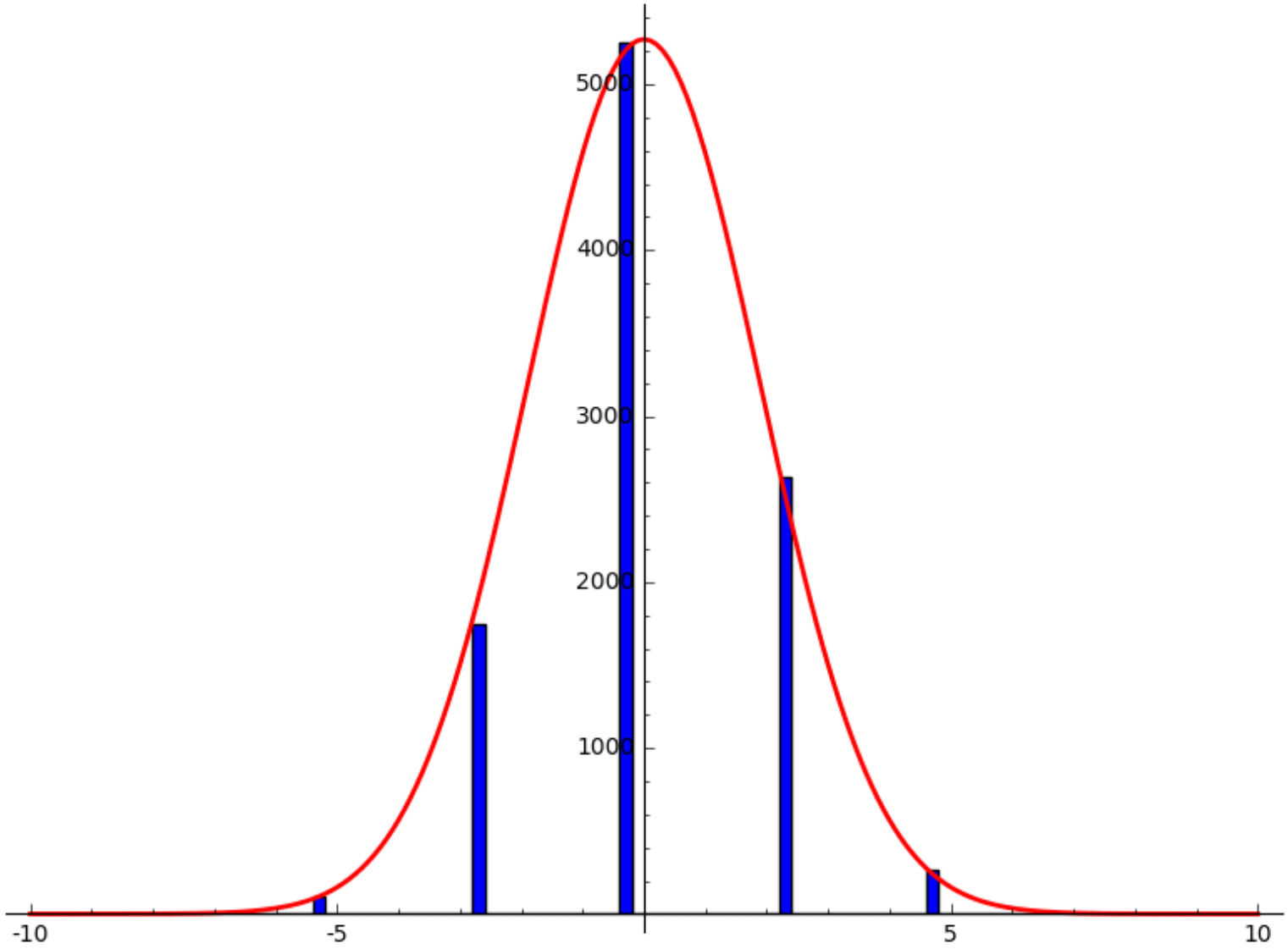
Distribution of modular symbols

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



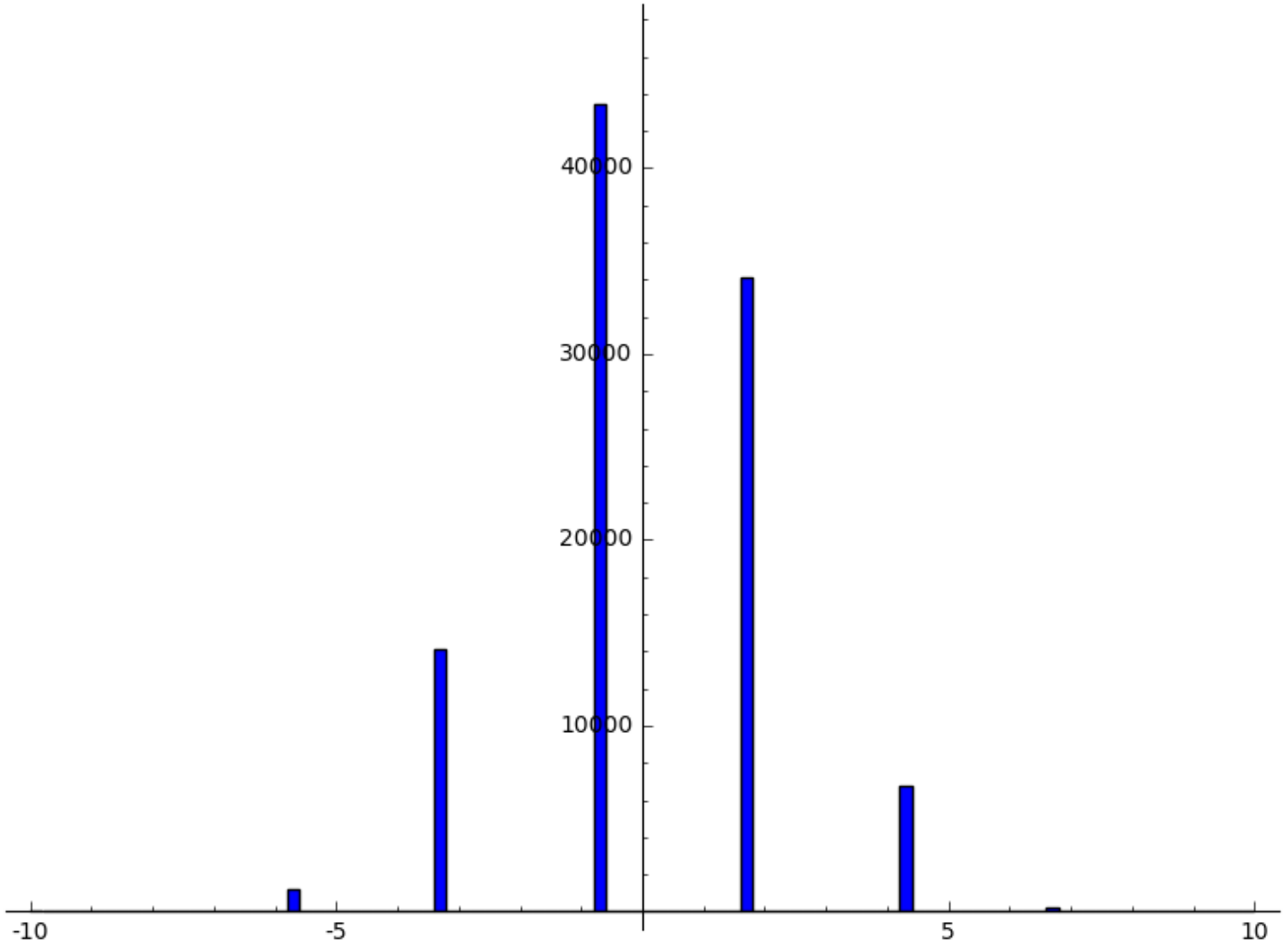
Distribution of modular symbols

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



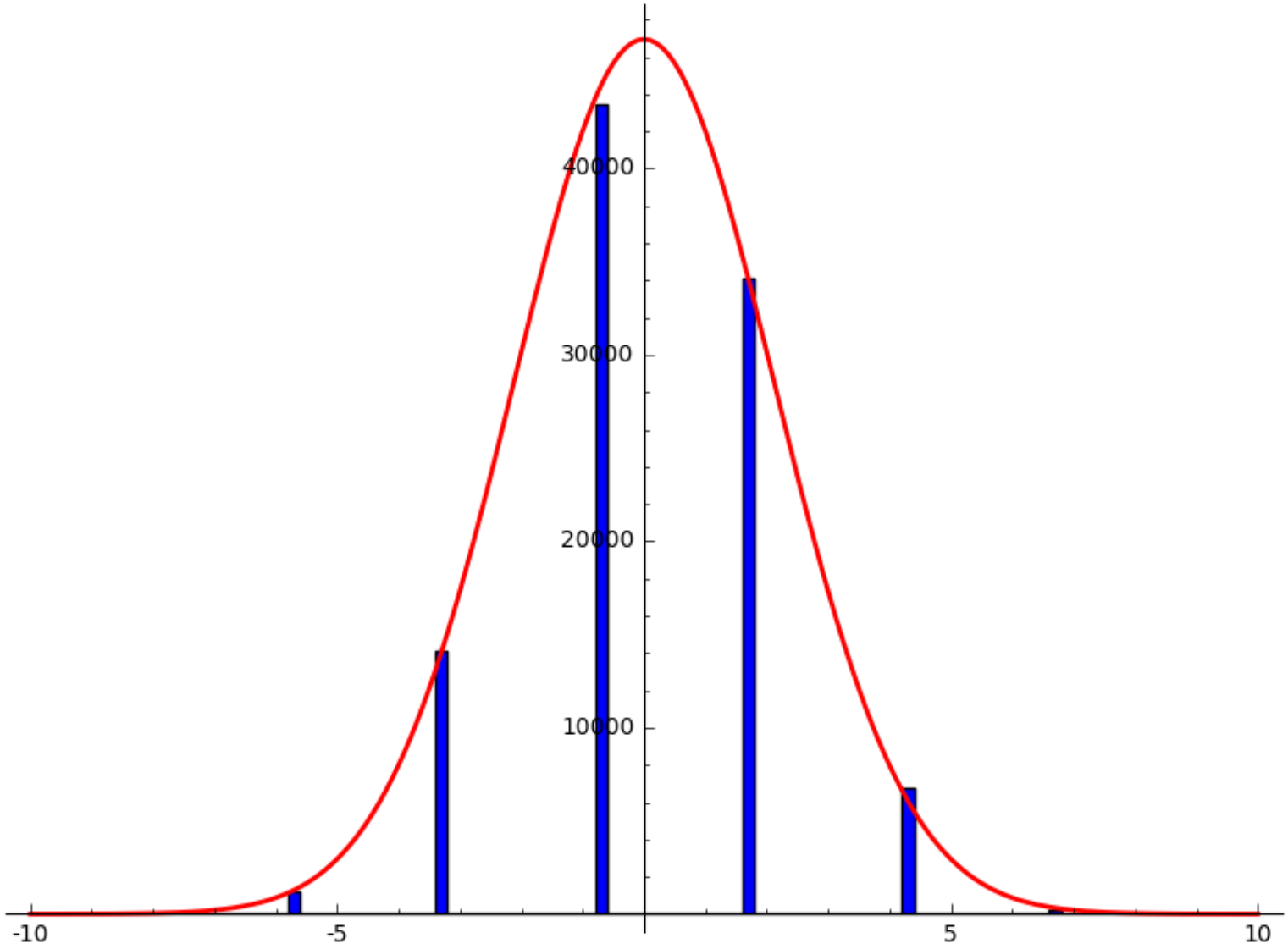
Distribution of modular symbols

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



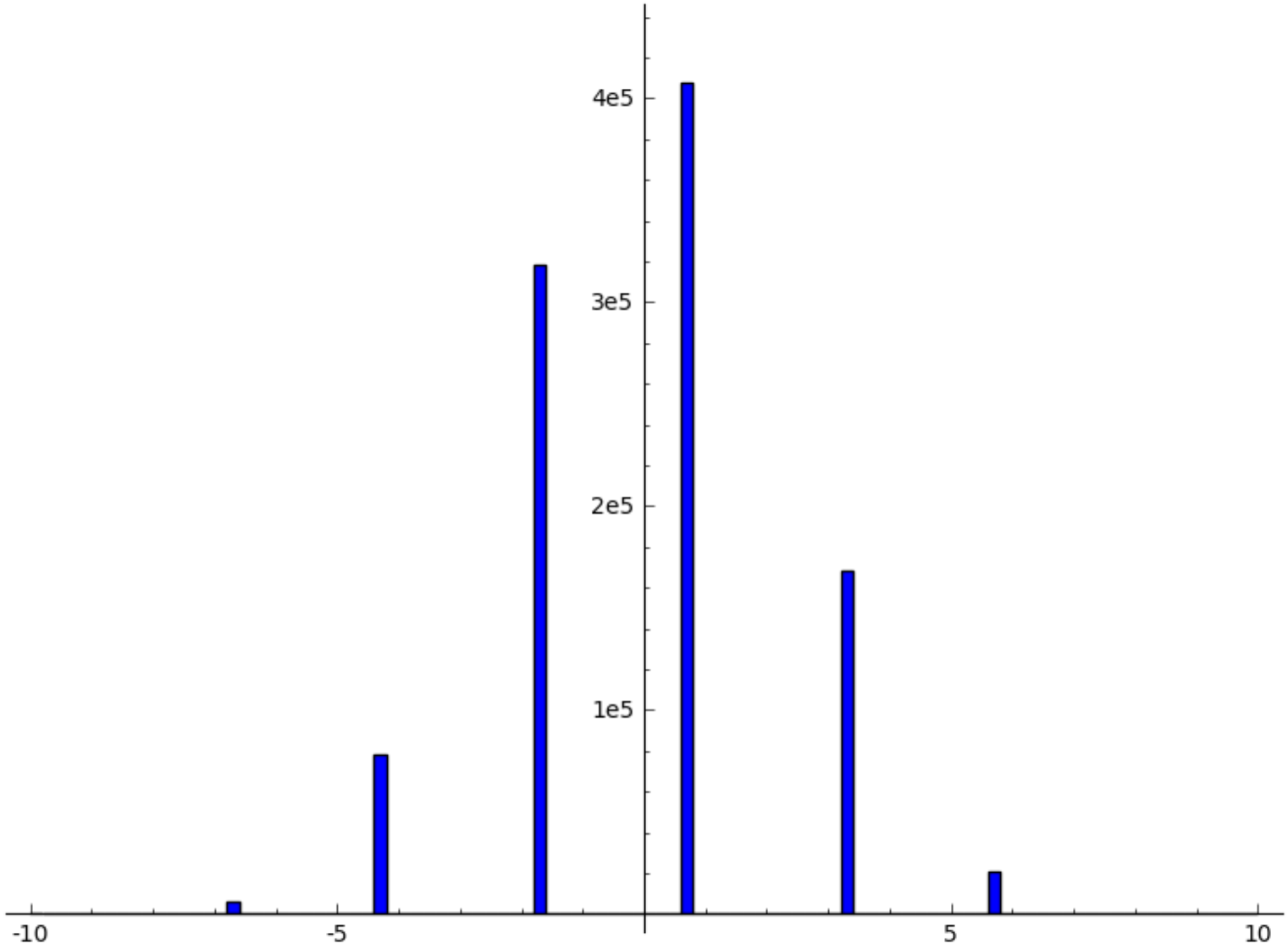
Distribution of modular symbols

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



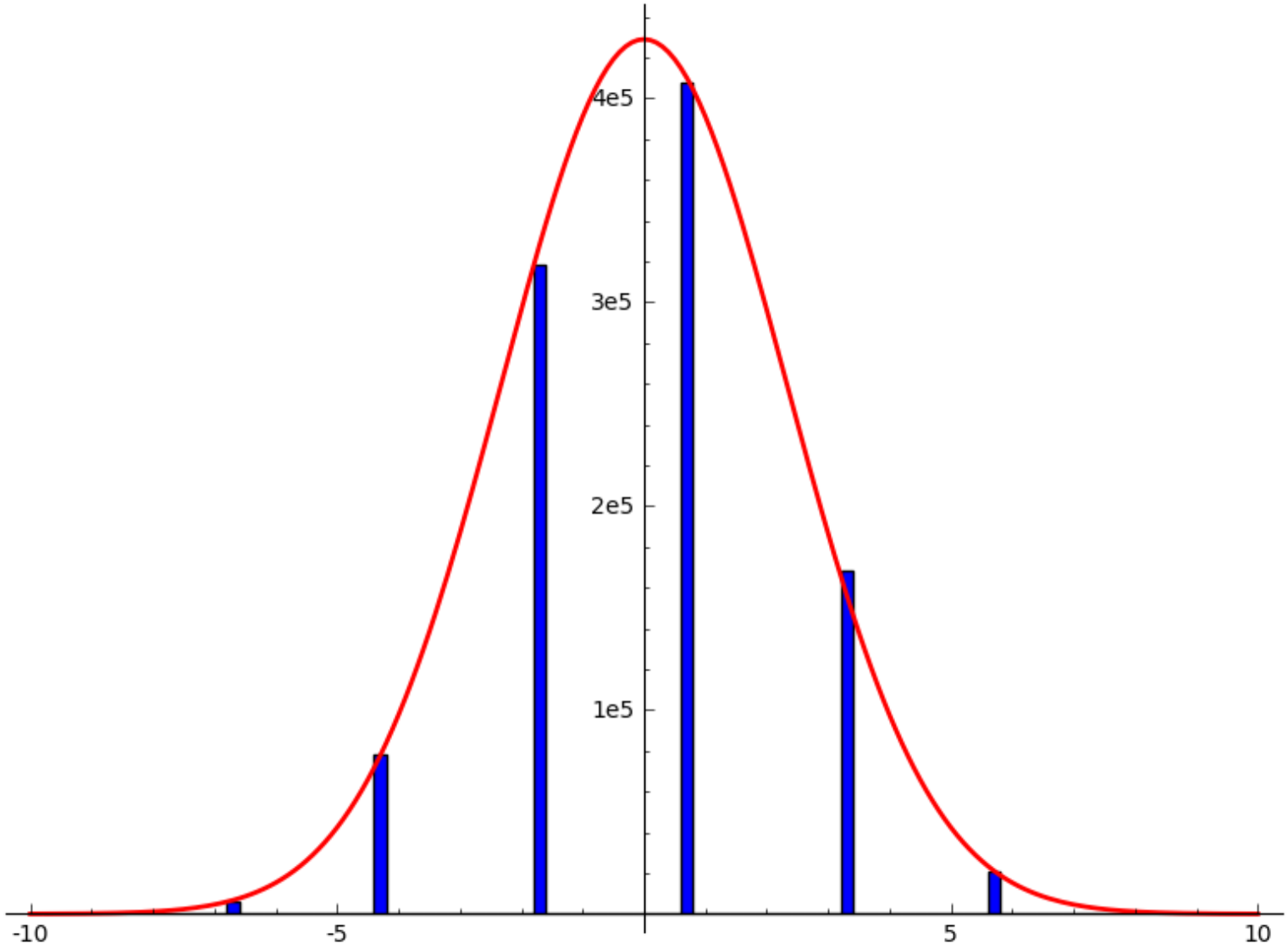
Distribution of modular symbols

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



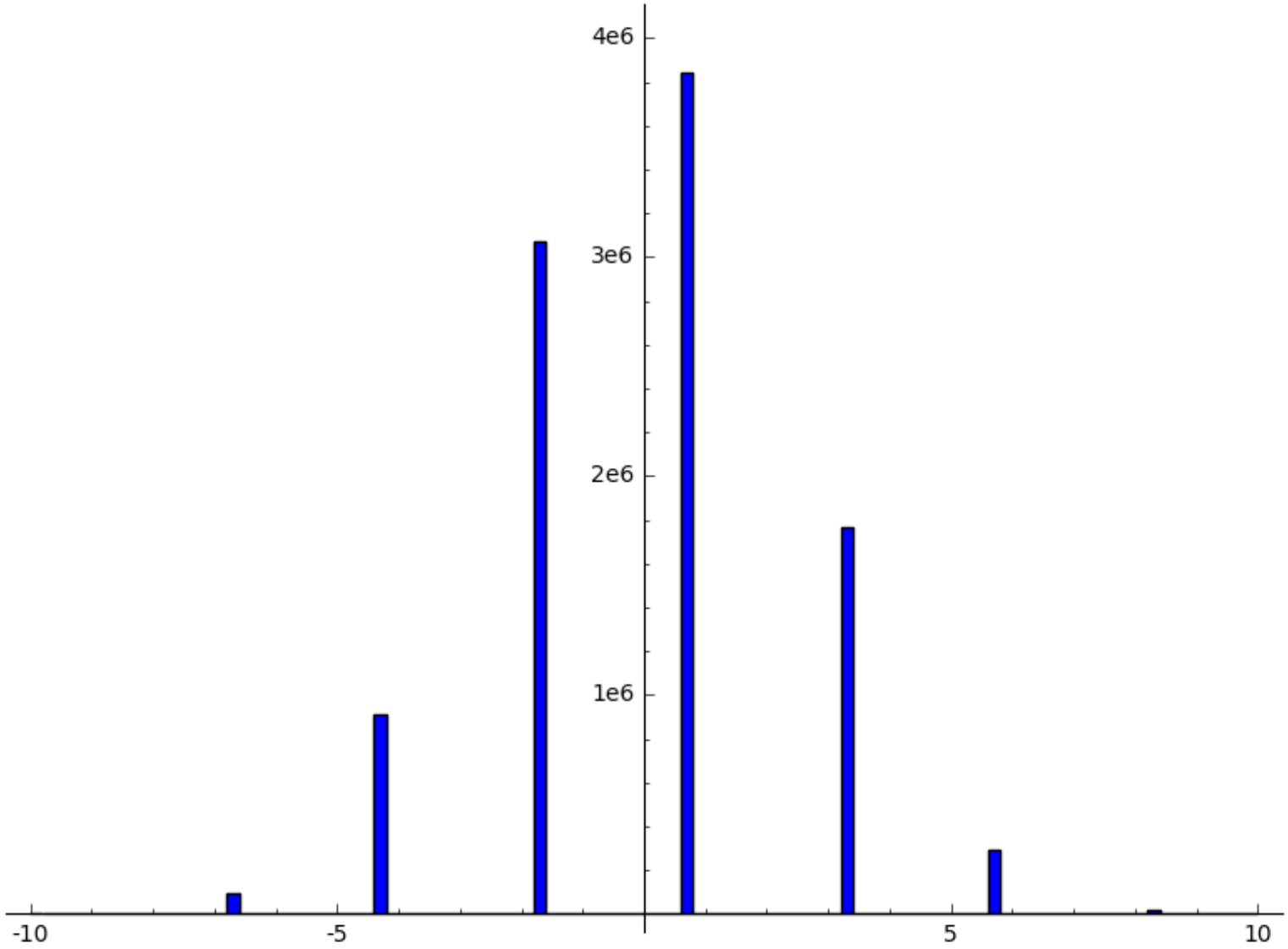
Distribution of modular symbols

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



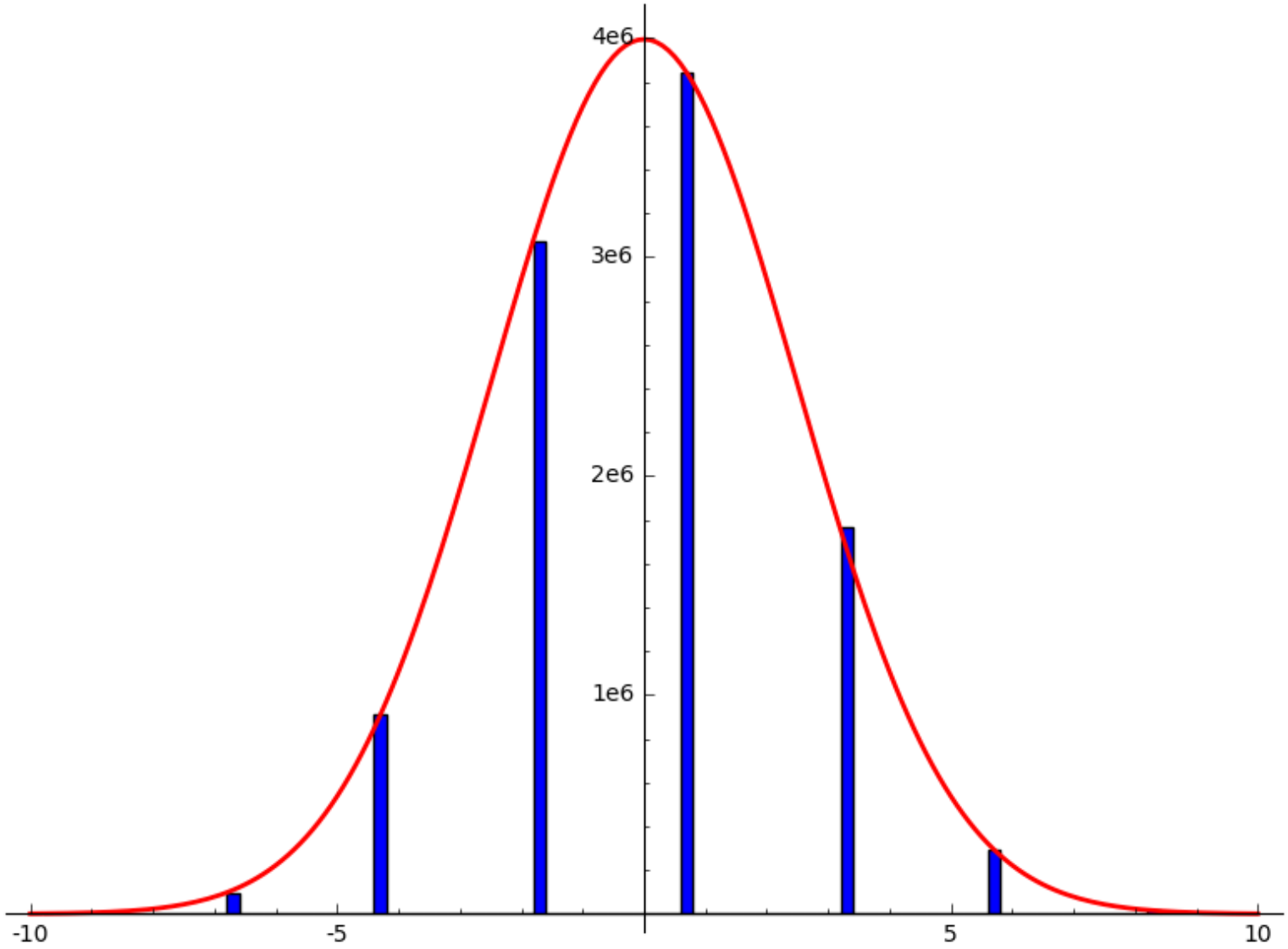
Distribution of modular symbols

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.

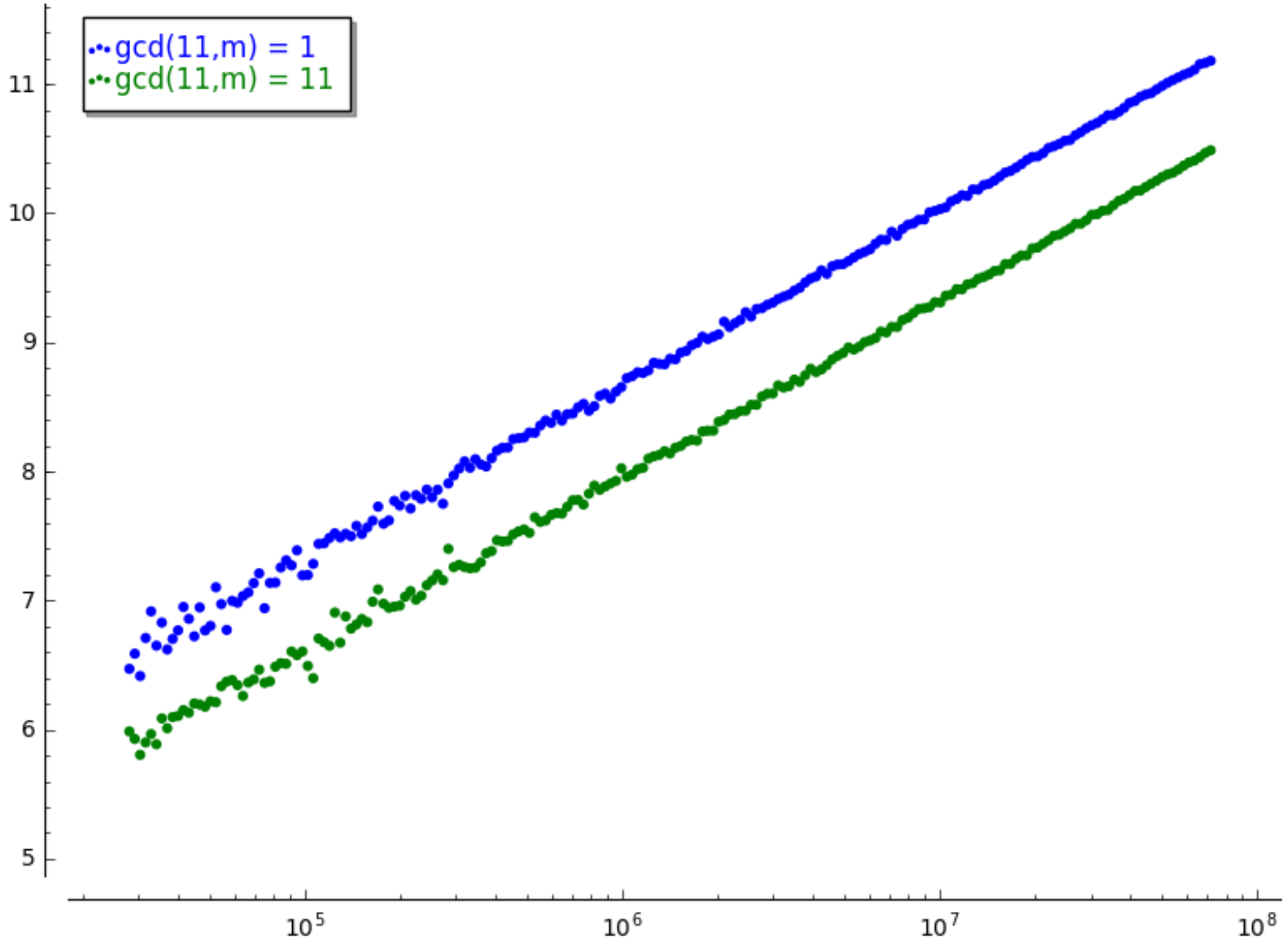
Distribution of modular symbols

This looks like a normal distribution.

How does the variance depend on m?

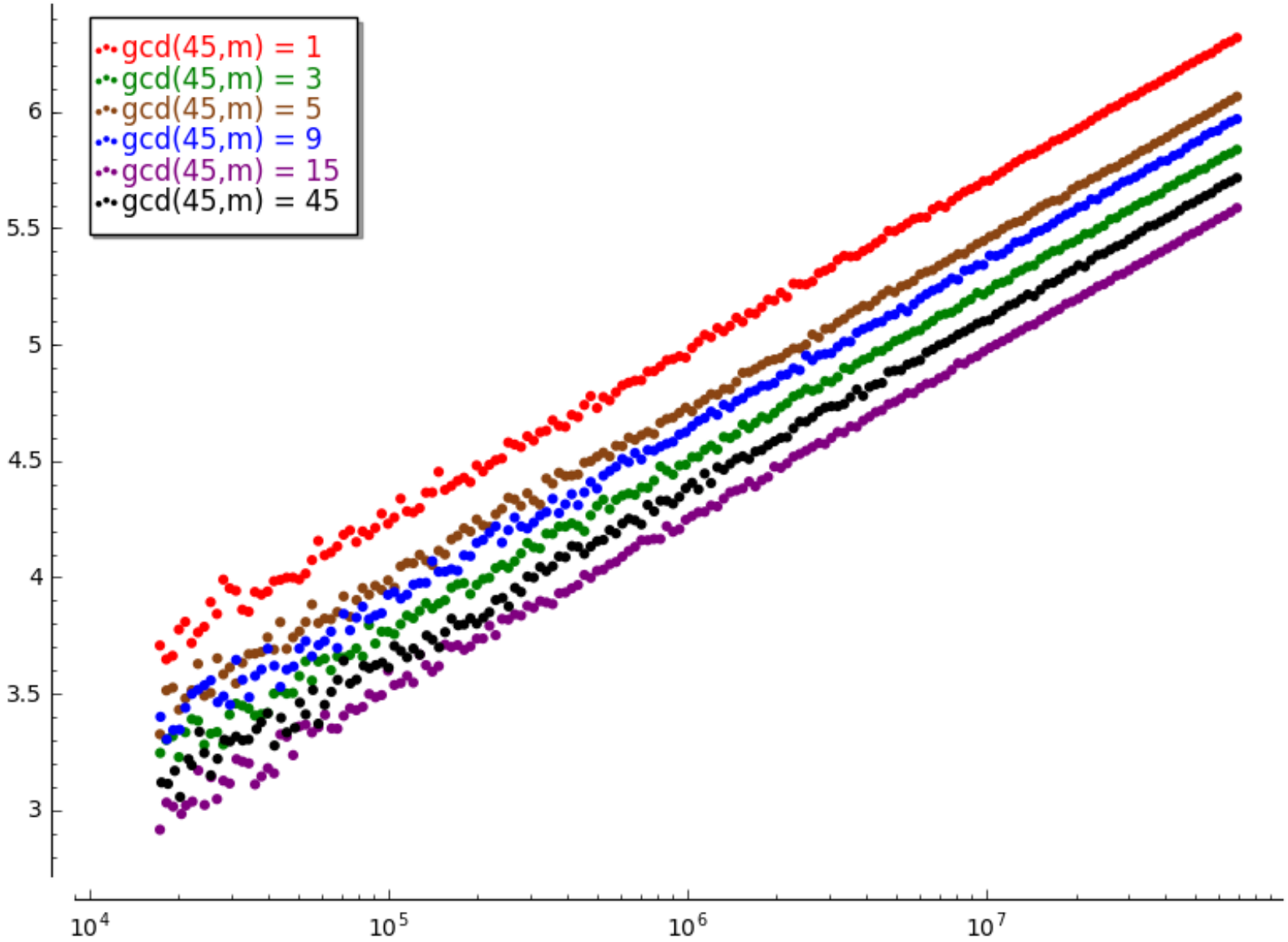
Distribution of modular symbols

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



Distribution of modular symbols

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



Distribution of modular symbols

For $m \geq 1$ let S_m denote the data $S_m = \{[a/m] : a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$.

Conjecture

There is an explicit constant V_E such that

1. *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 V_E.*
2. *for every divisor κ of N, $\lim_{\substack{m\to\infty \\ (m,N)=\kappa}} \mathrm{Variance}(S_m) - V_E \log(m)$ exists and is finite.*

Distribution of modular symbols

For $m \geq 1$ let S_m denote the data $S_m = \{[a/m] : a \in (\mathbb{Z}/m\mathbb{Z})^\times\}$.

Conjecture

There is an explicit constant V_E such that

1. *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 V_E.*
2. *for every divisor κ of N, $\lim_{\substack{m\to\infty \\ (m,N)=\kappa}} \mathrm{Variance}(S_m) - V_E \log(m)$ exists and is finite.*

Theorem (Petridis-Risager)

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

The variance V_E is essentially $L(\mathrm{Sym}^2(E), 1)$, and Petridis & Risager compute the limit in 2 in terms of $L(\mathrm{Sym}^2(E), 1)$ and $L'(\mathrm{Sym}^2(E), 1)$.

Distribution of theta coefficients

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

If $[F:\mathbb{Q}] = d$, then 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

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

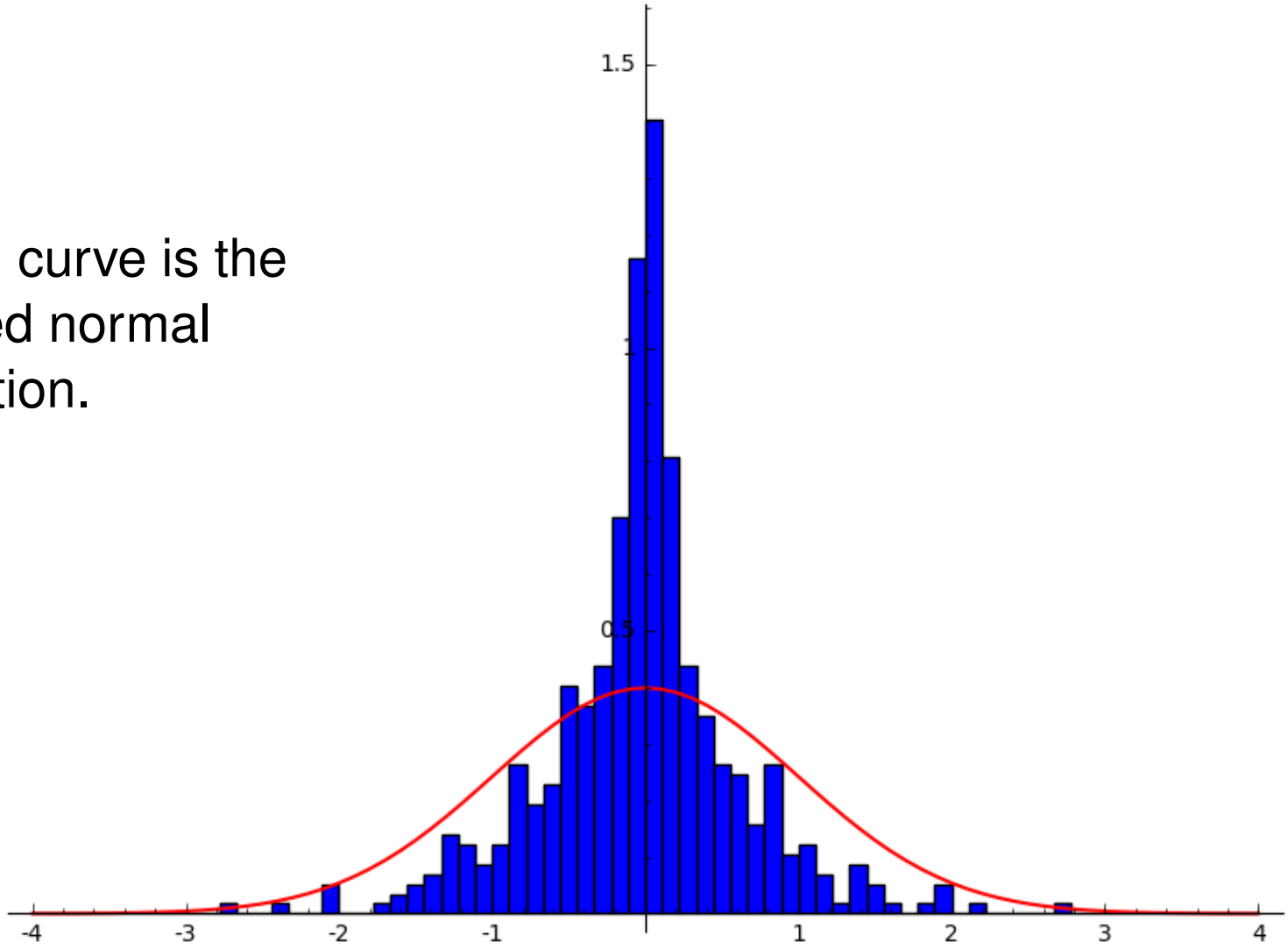
should satisfy a normal distribution with variance 1.

Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$10000 < m < 20000$:

The red curve is the expected normal distribution.

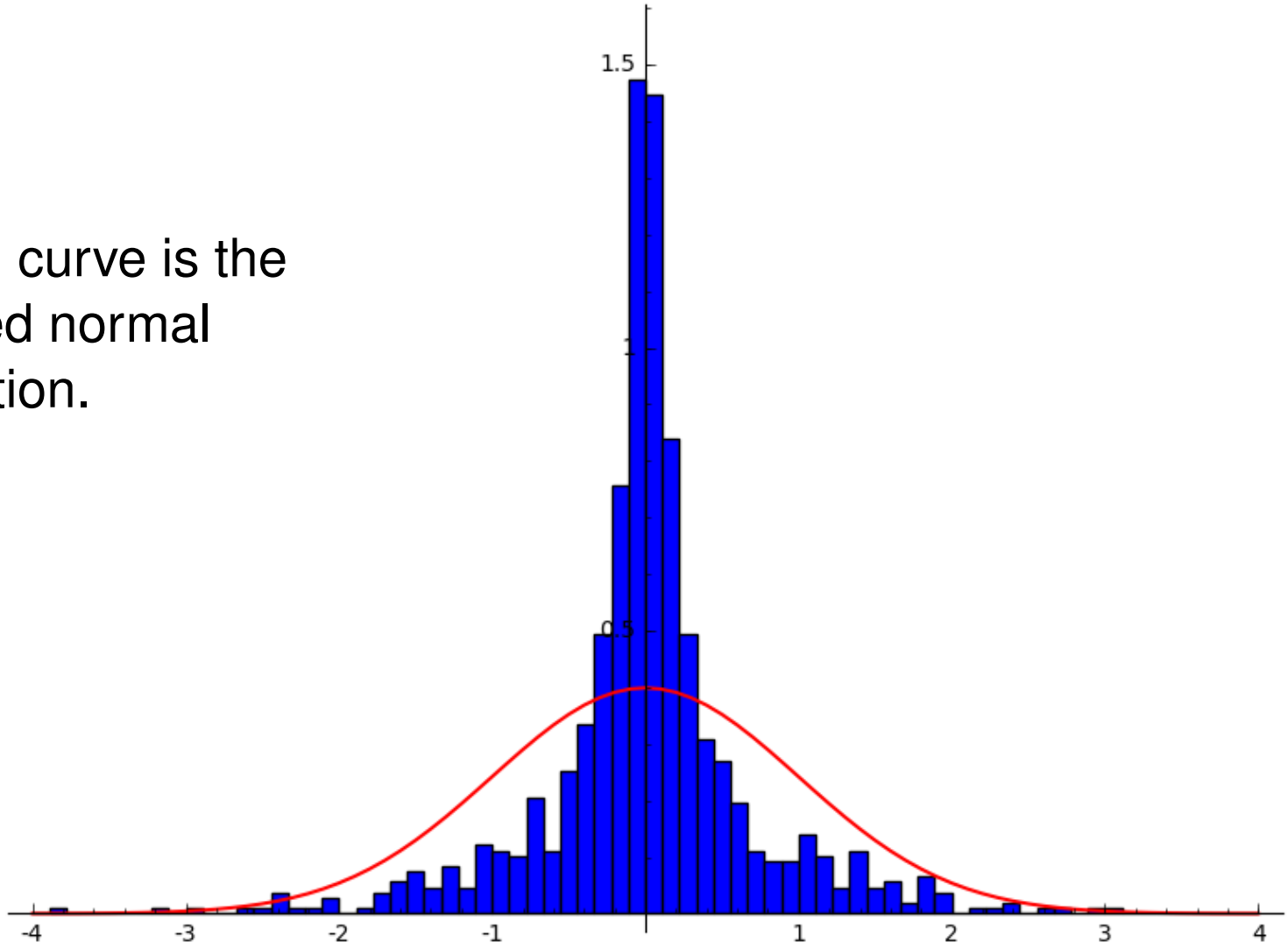


Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$20000 < m < 40000$:

The red curve is the expected normal distribution.

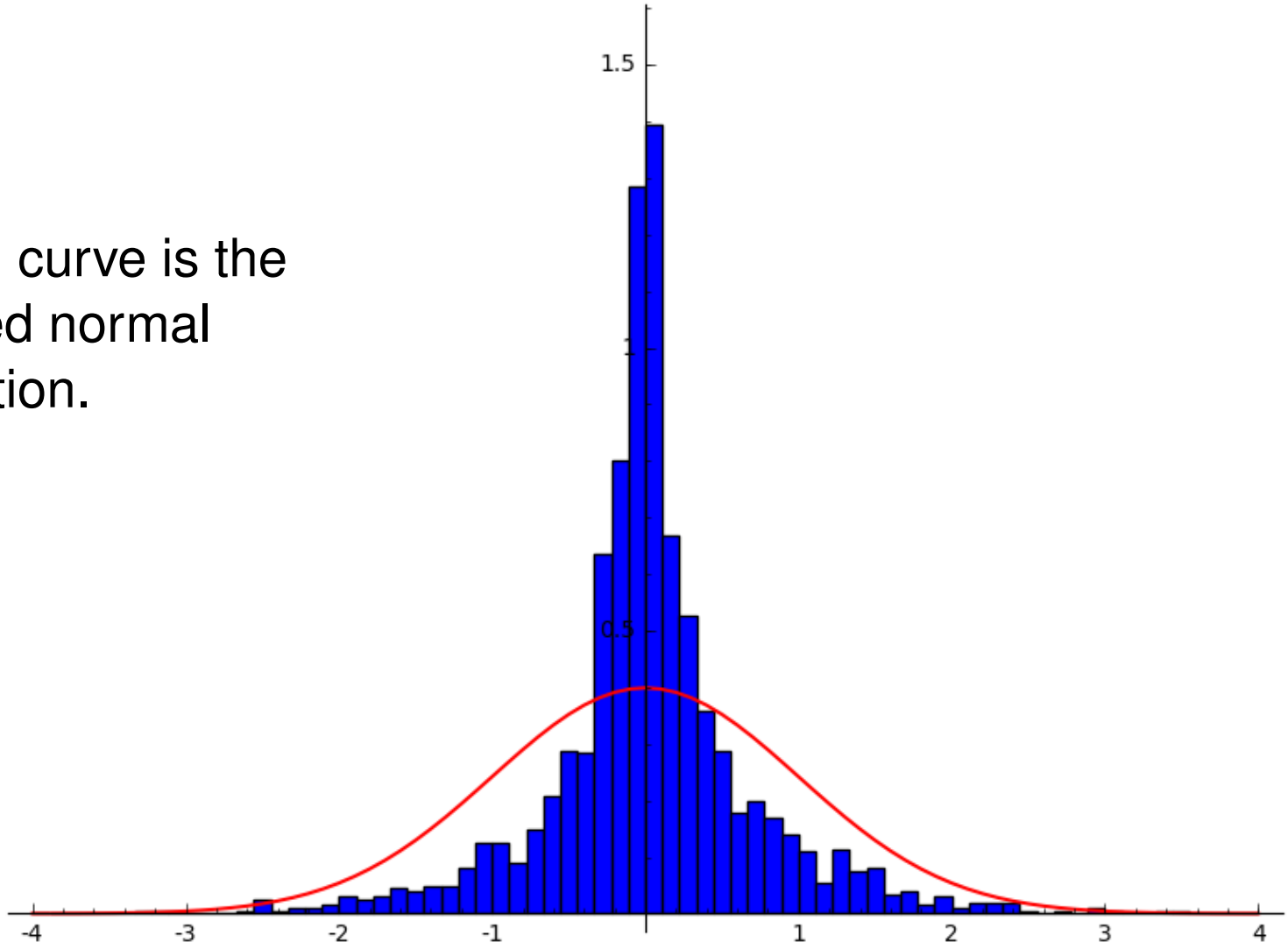


Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$40000 < m < 80000$:

The red curve is the expected normal distribution.

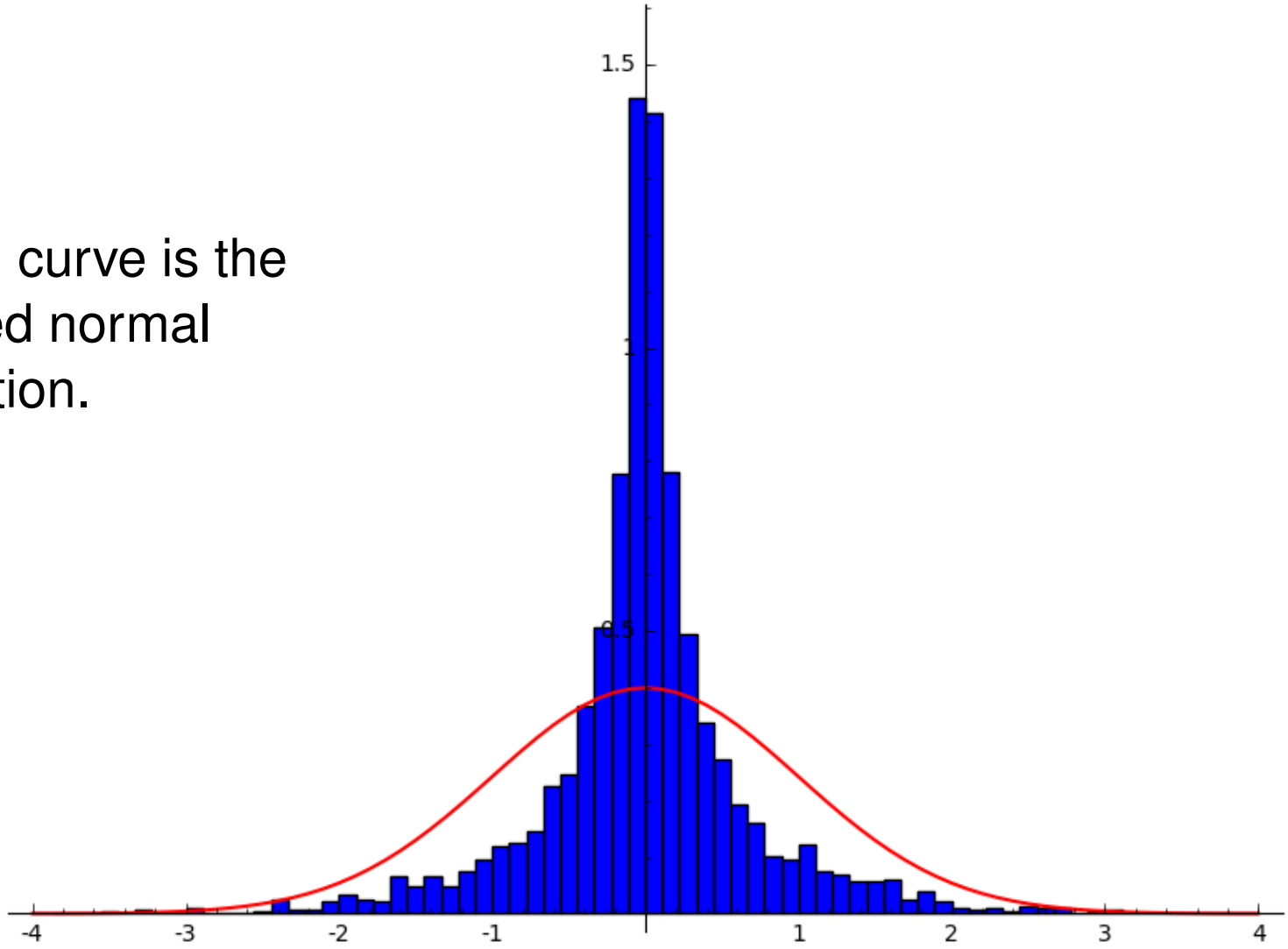


Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$80000 < m < 160000$:

The red curve is the expected normal distribution.

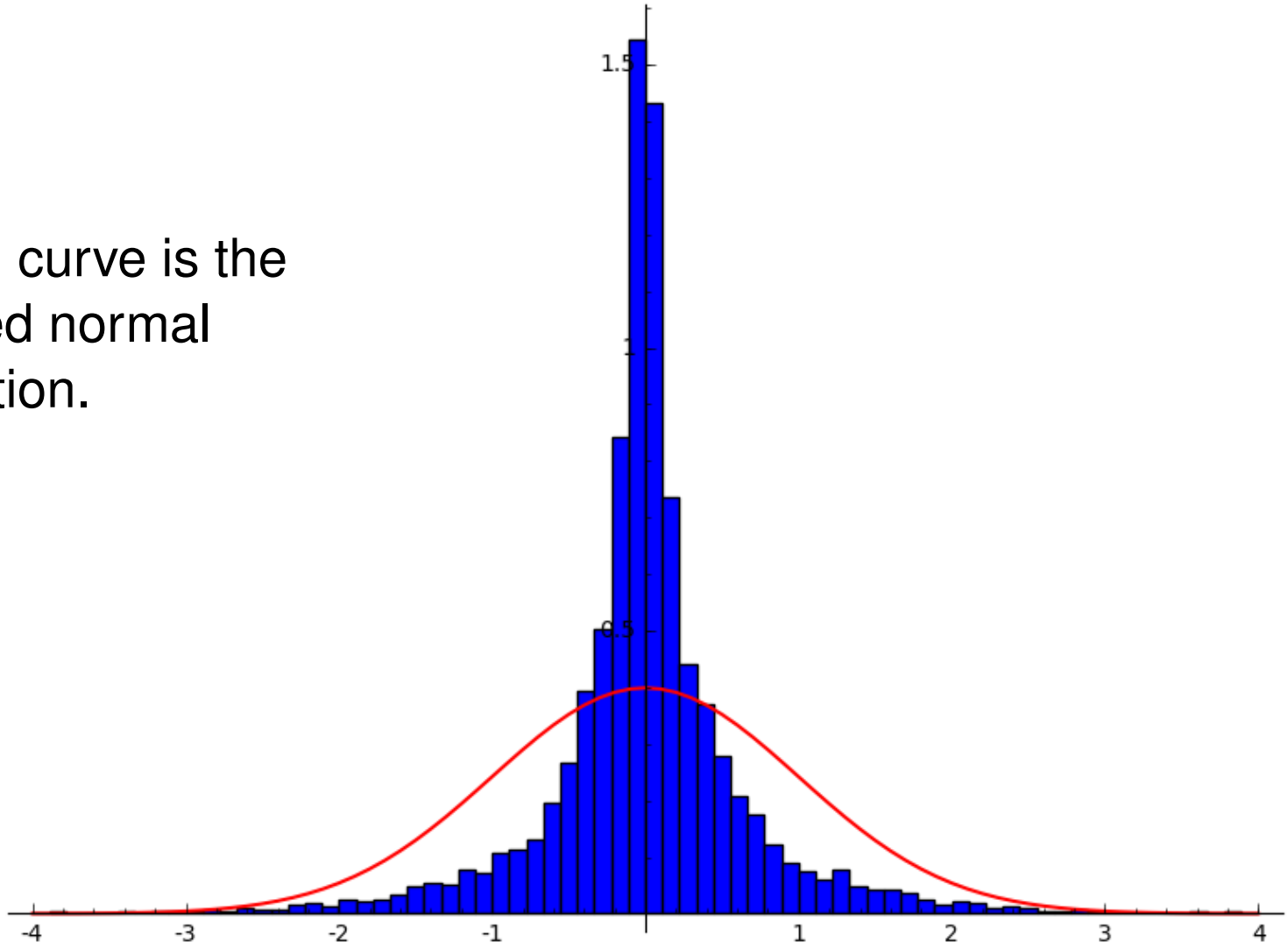


Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$160000 < m < 320000$:

The red curve is the expected normal distribution.

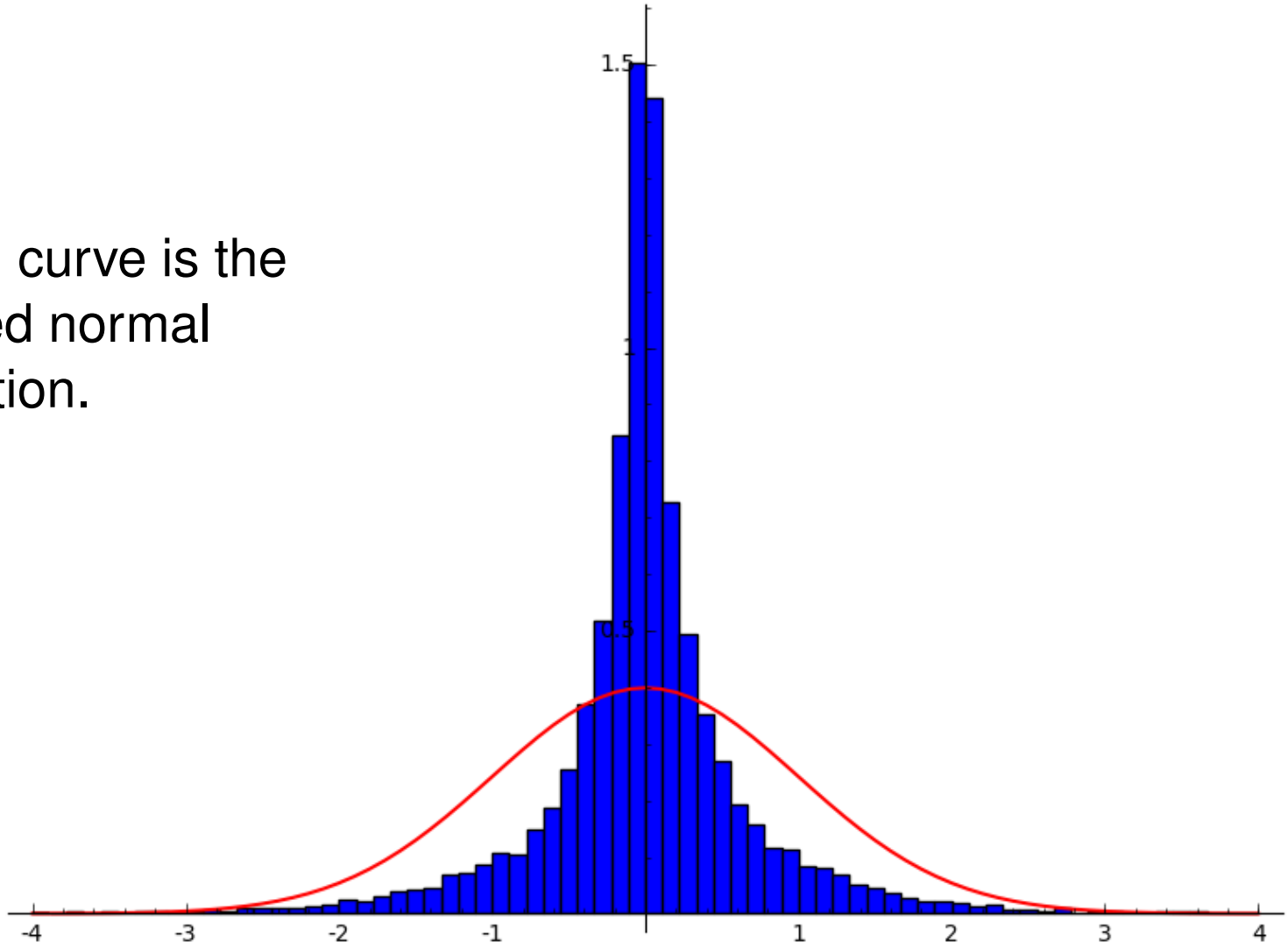


Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$320000 < m < 640000$:

The red curve is the expected normal distribution.

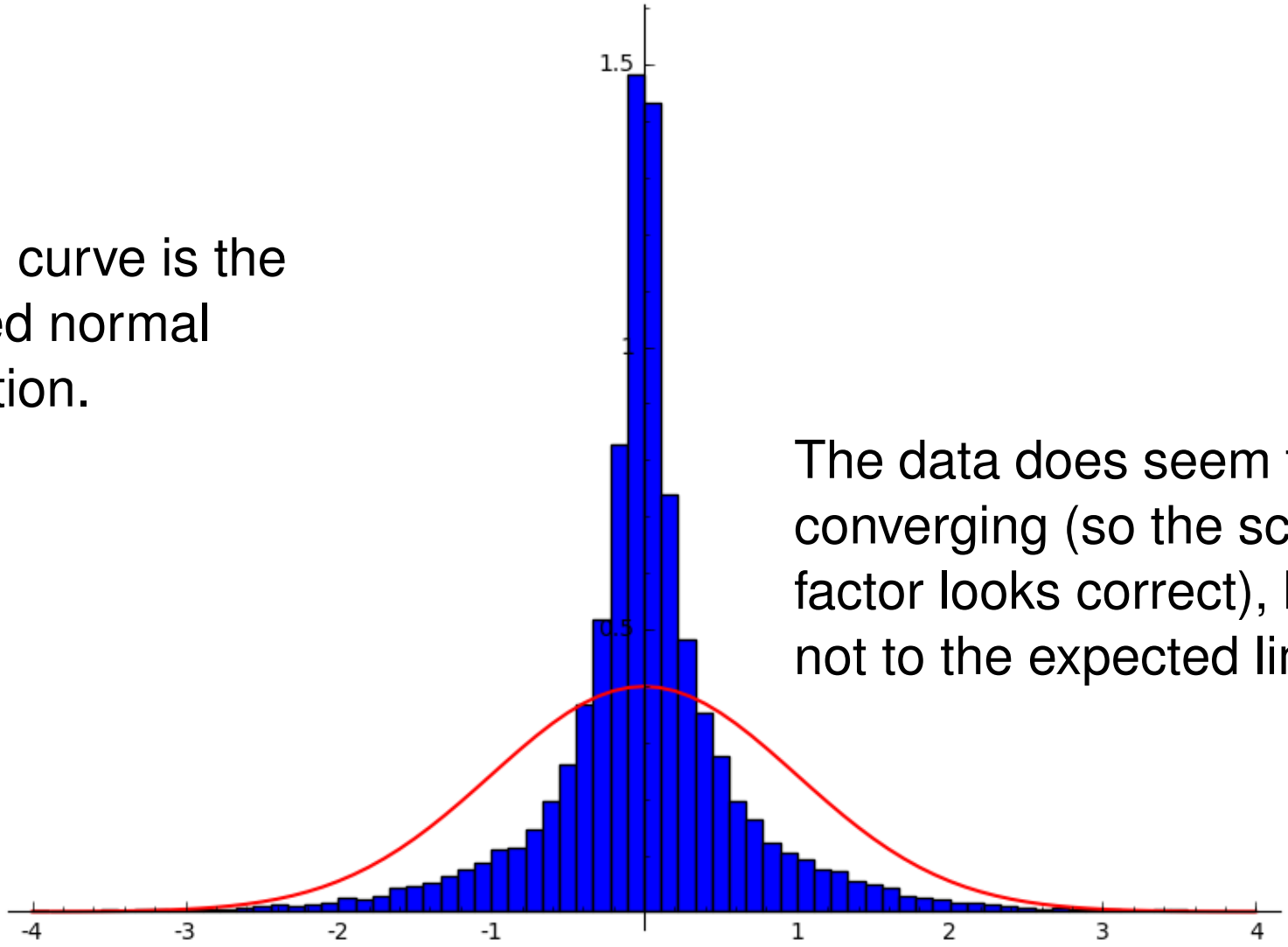


Distribution of normalized theta coefficients, $d = 3$

$E = 11A1$, primes $m \equiv 1 \pmod 3$, $L \subset \mathbb{Q}(\mu_m)$, $[L : \mathbb{Q}] = 3$,

$10000 < m < 640000$:

The red curve is the expected normal distribution.

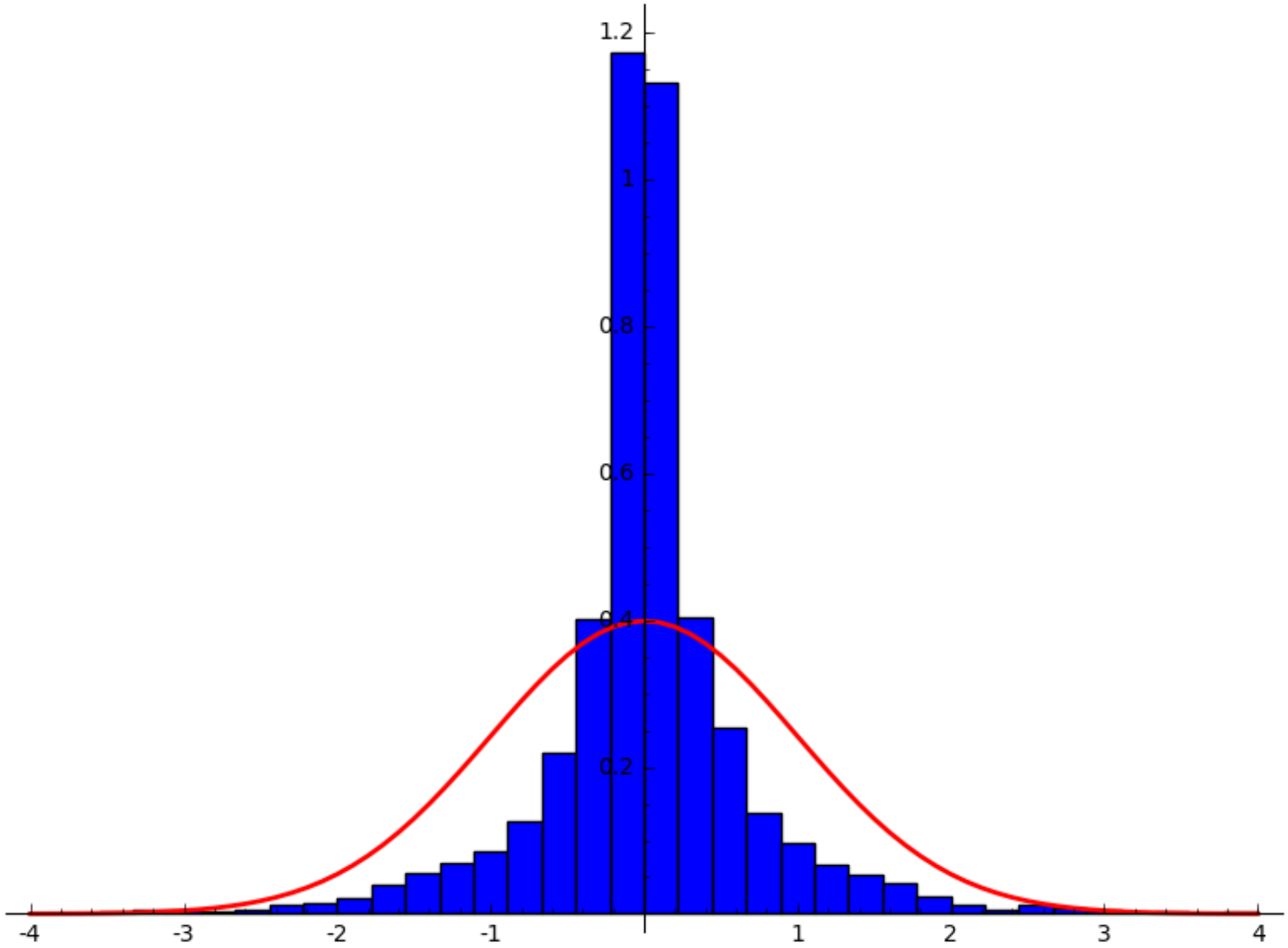


The data does seem to be converging (so the scaling factor looks correct), but not to the expected limit.

Distribution of theta coefficients, small d

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

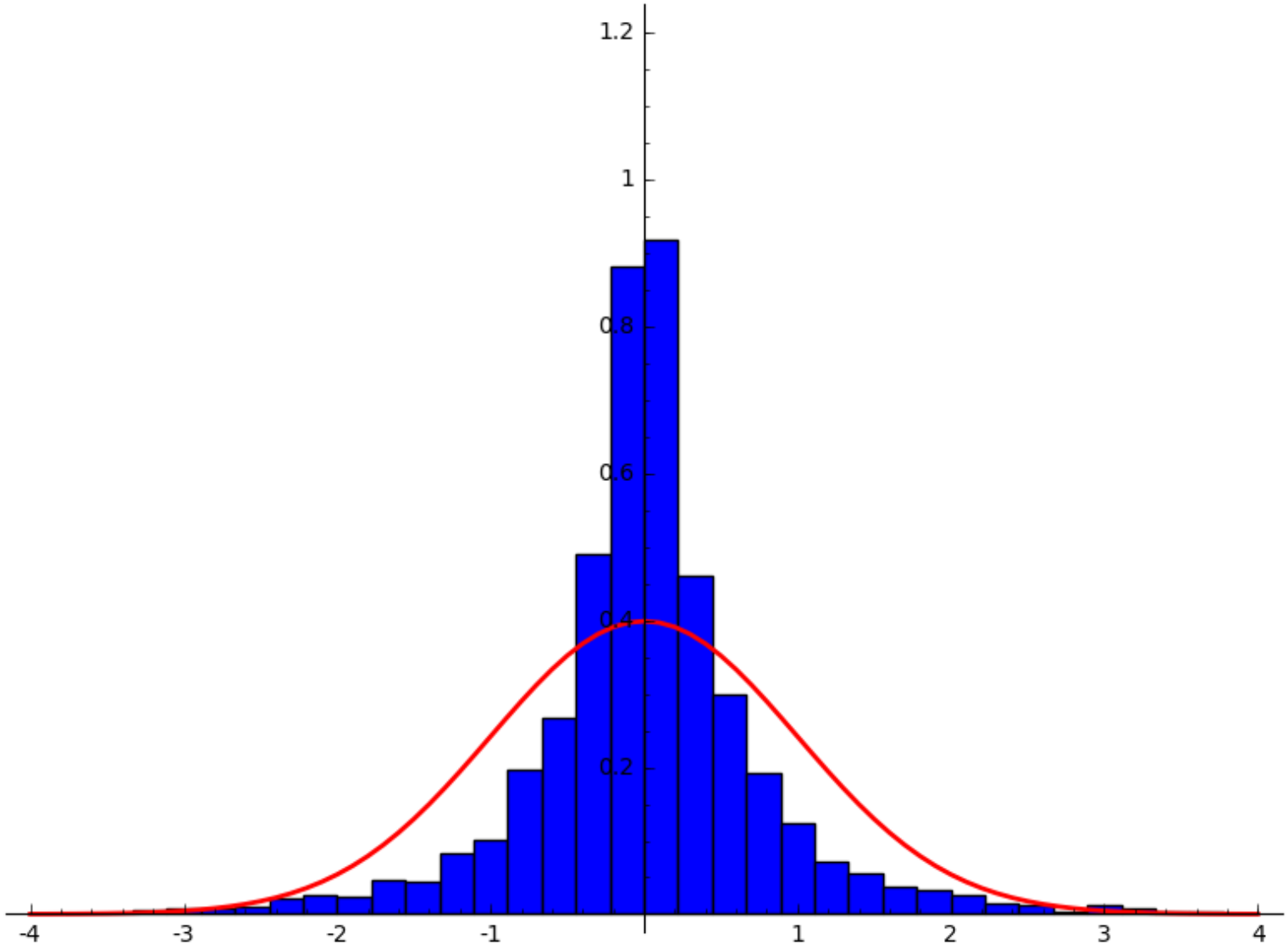
$d = 3$



Distribution of theta coefficients, small d

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

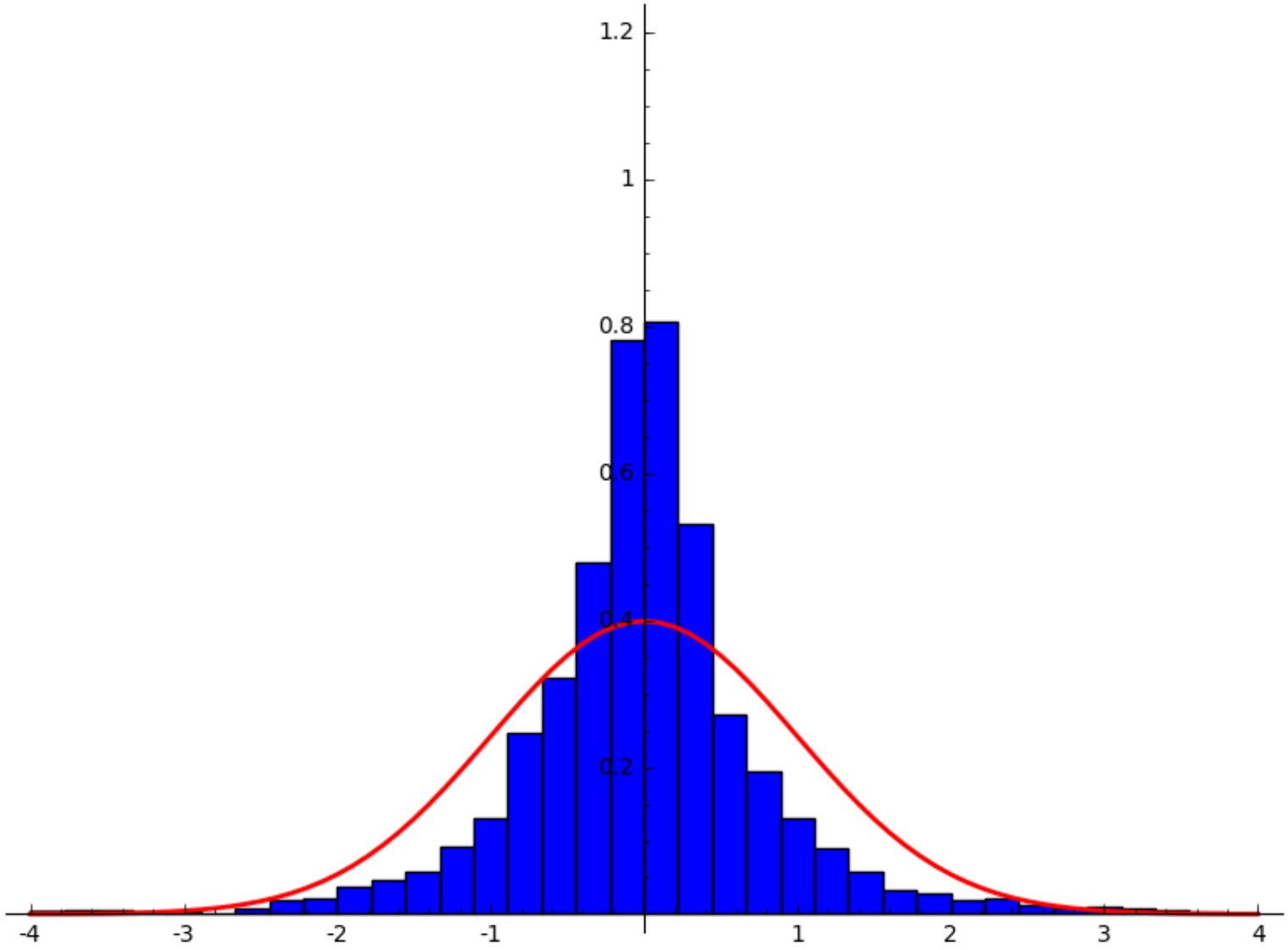
$d = 5$



Distribution of theta coefficients, small d

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

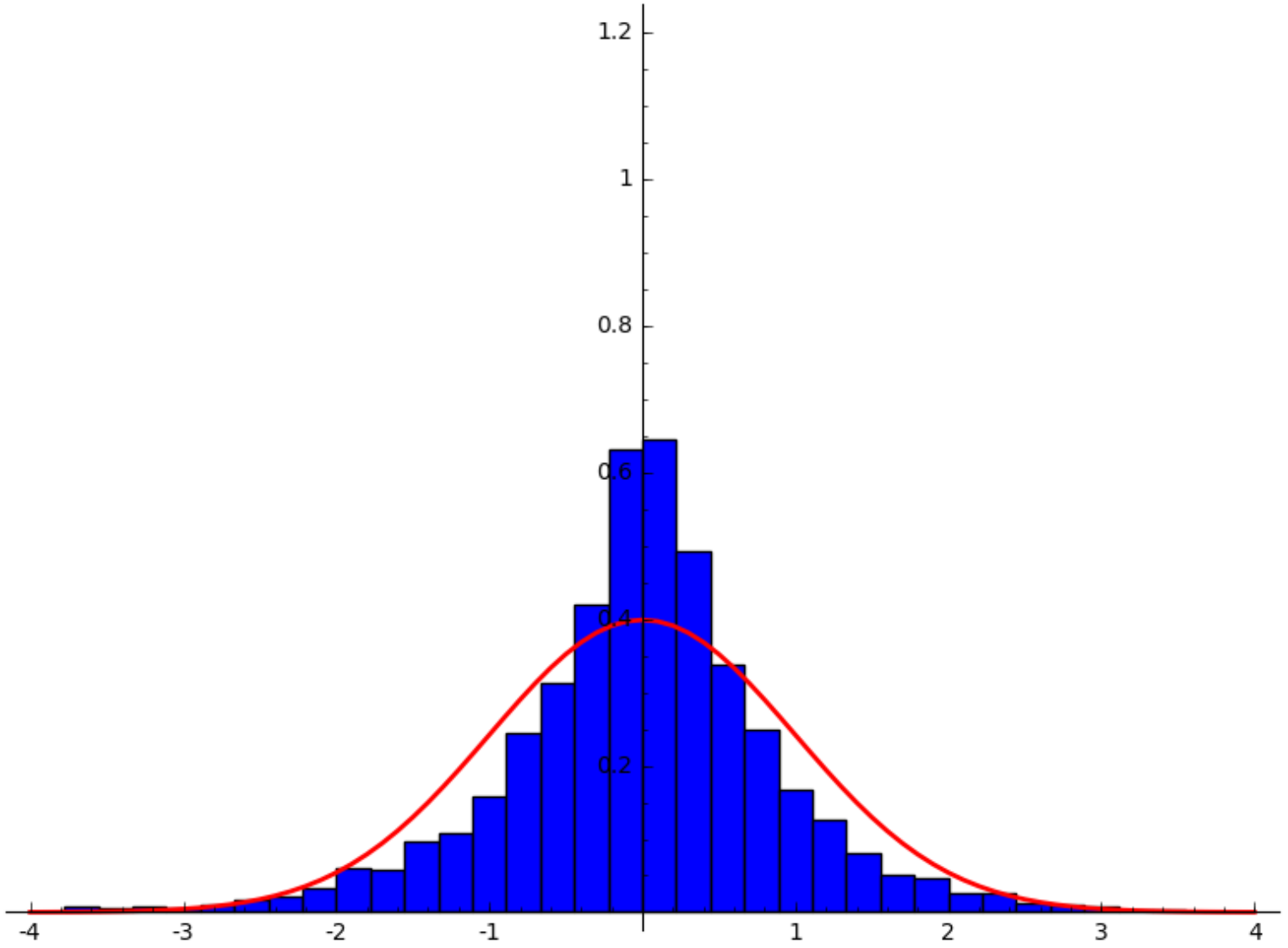
$d = 7$



Distribution of theta coefficients, small d

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

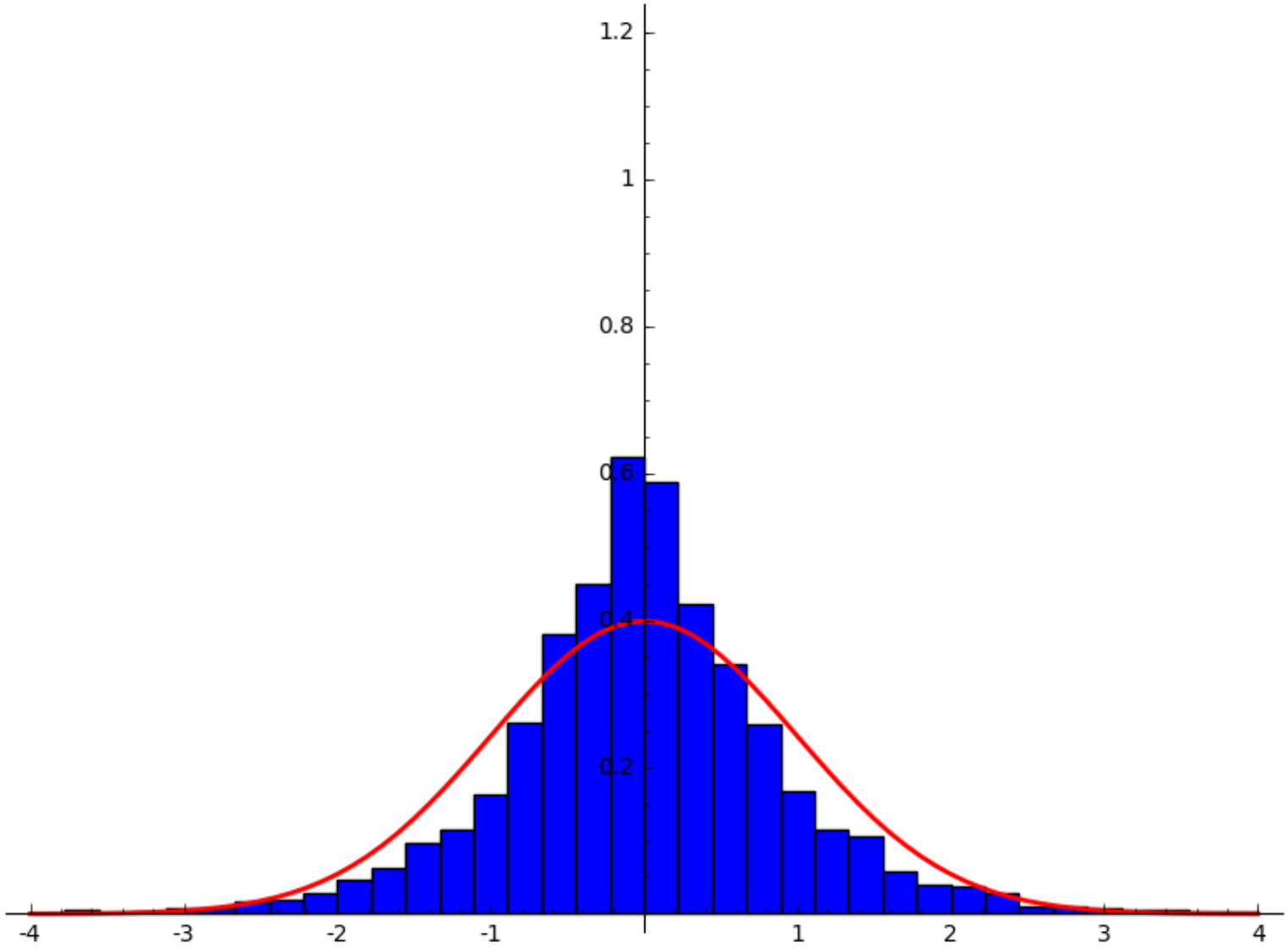
$d = 11$



Distribution of theta coefficients, small d

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

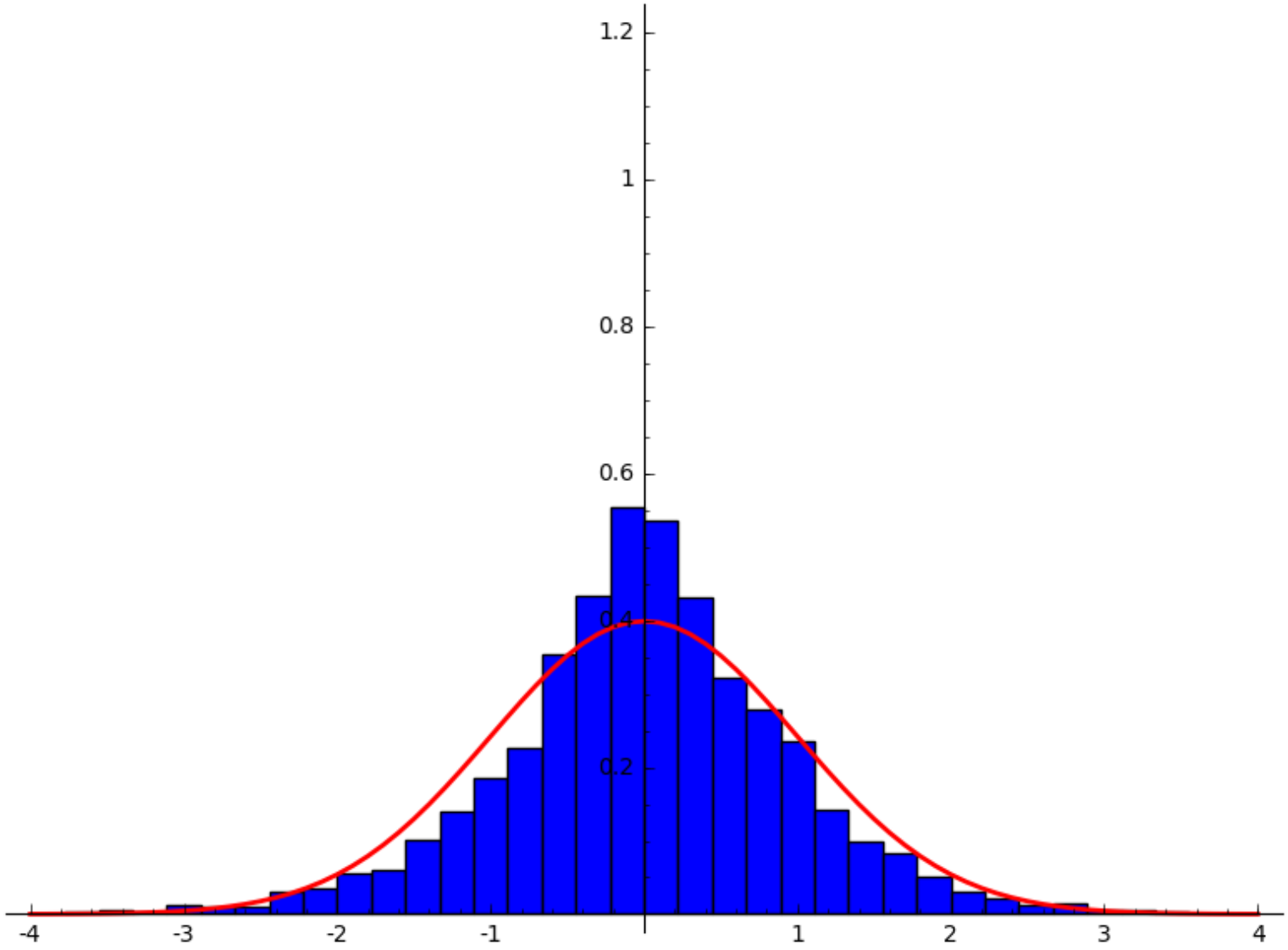
$d = 13$



Distribution of theta coefficients, small d

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

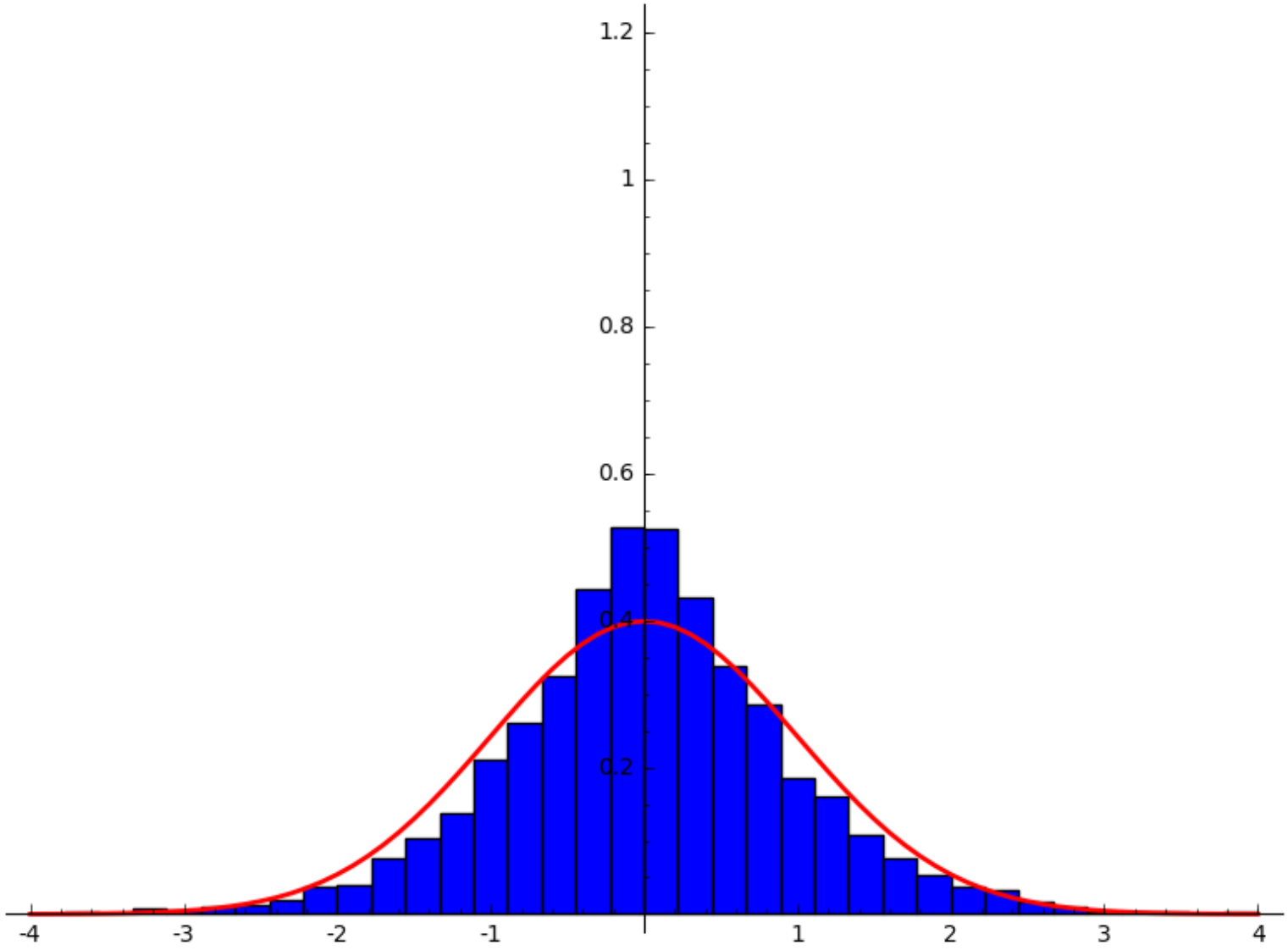
$d = 17$



Distribution of theta coefficients, small d

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

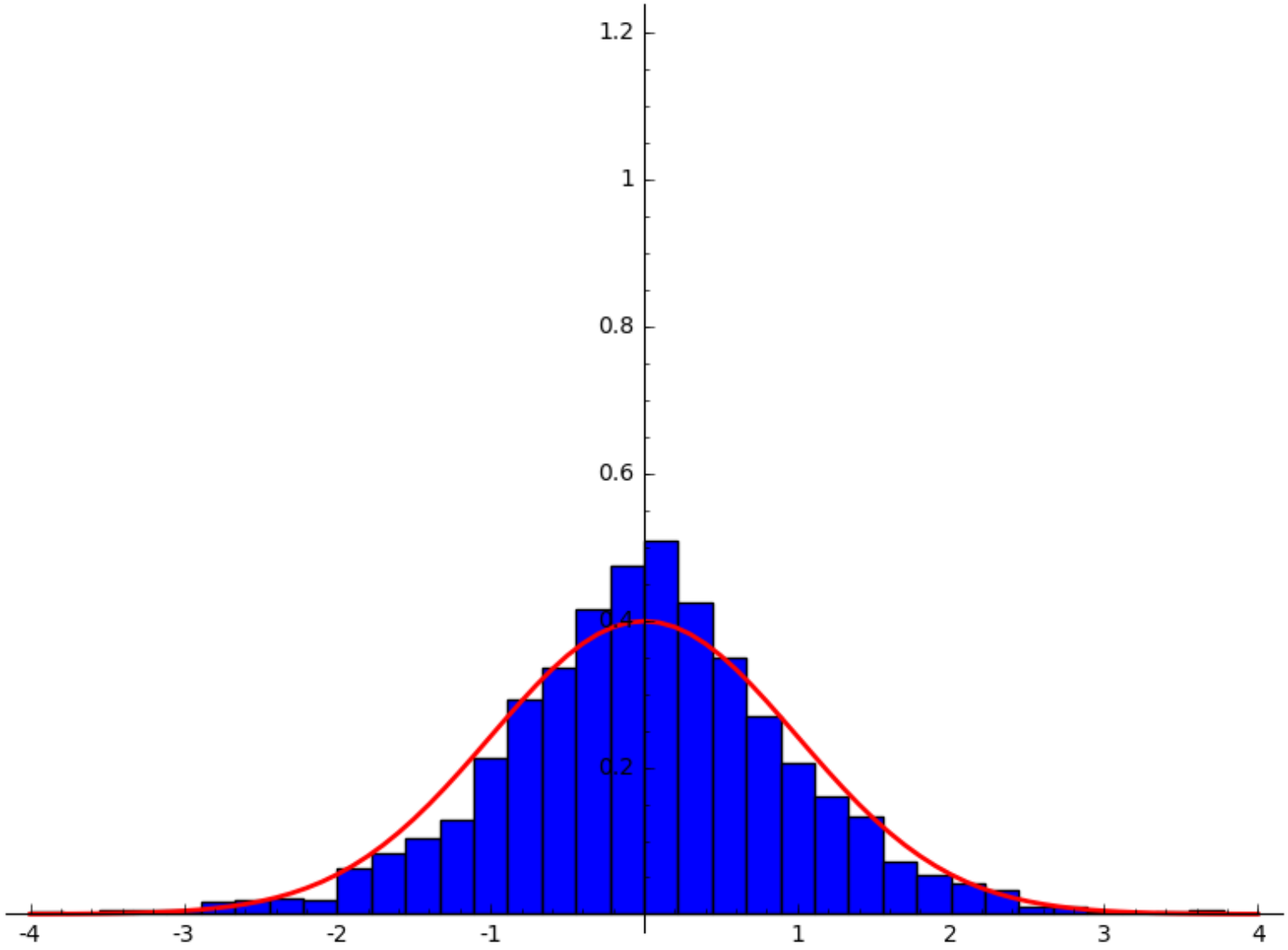
$d = 23$



Distribution of theta coefficients, small d

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

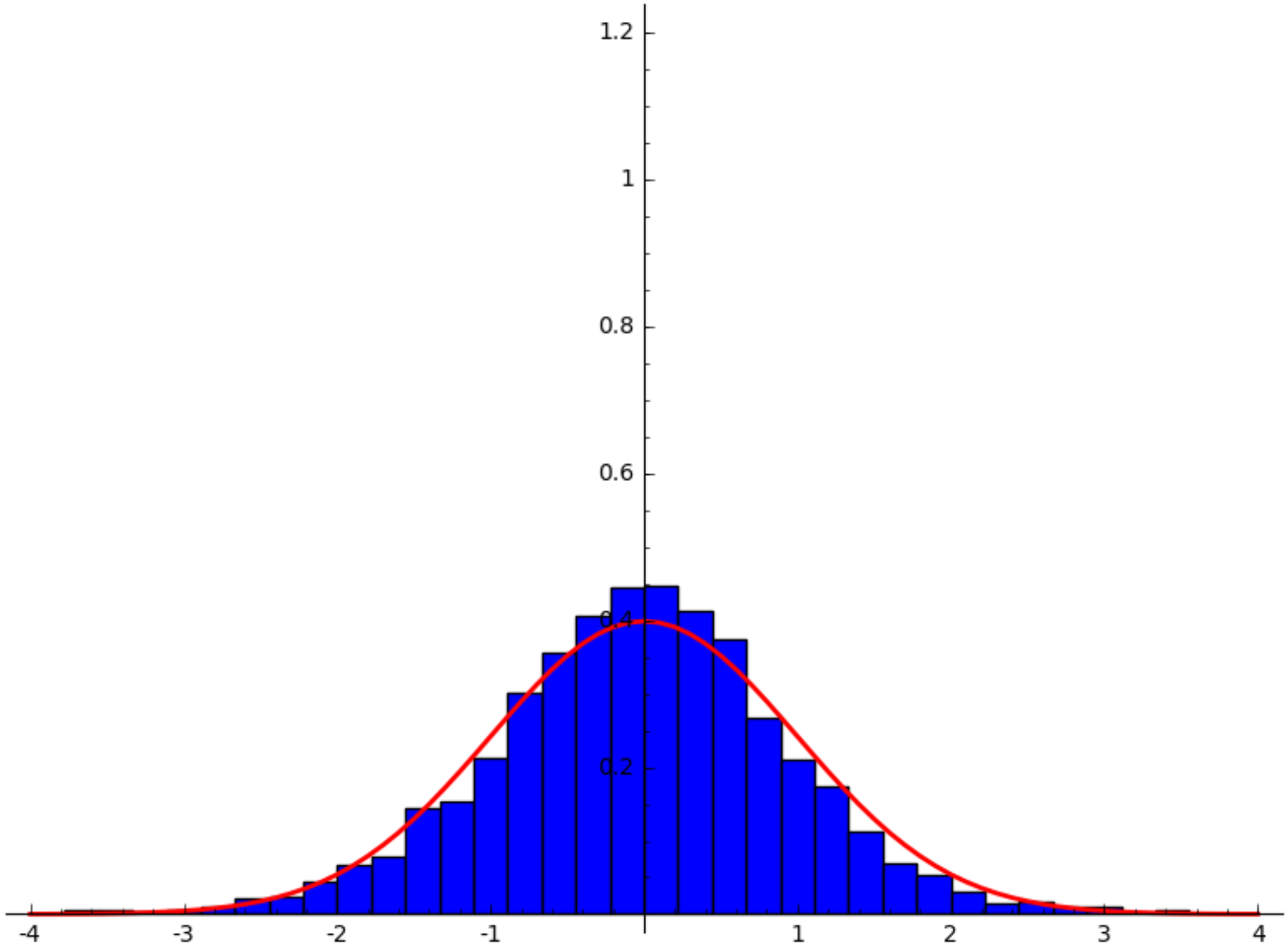
$d = 31$



Distribution of theta coefficients, small d

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

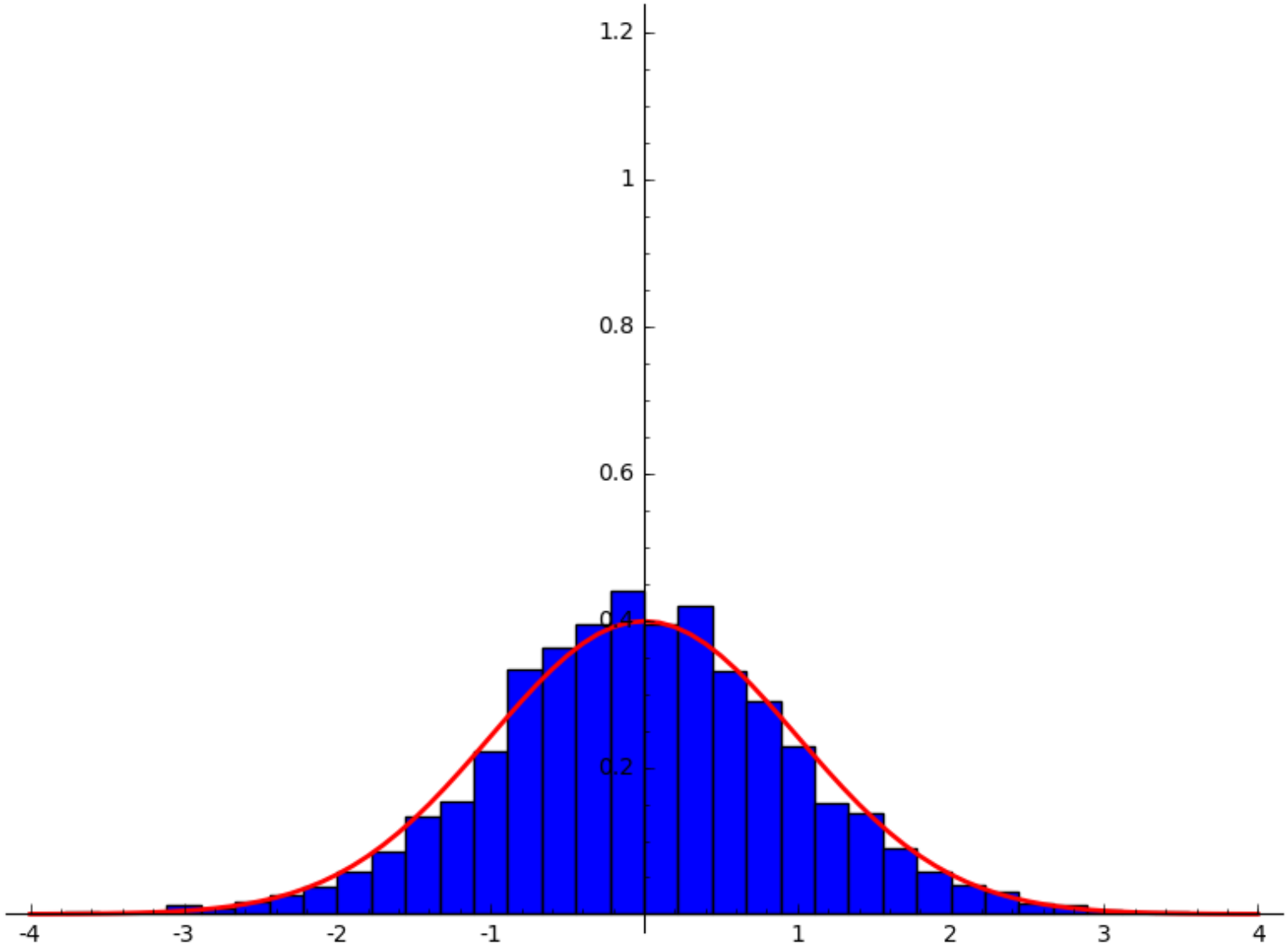
$d = 41$



Distribution of theta coefficients, small d

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

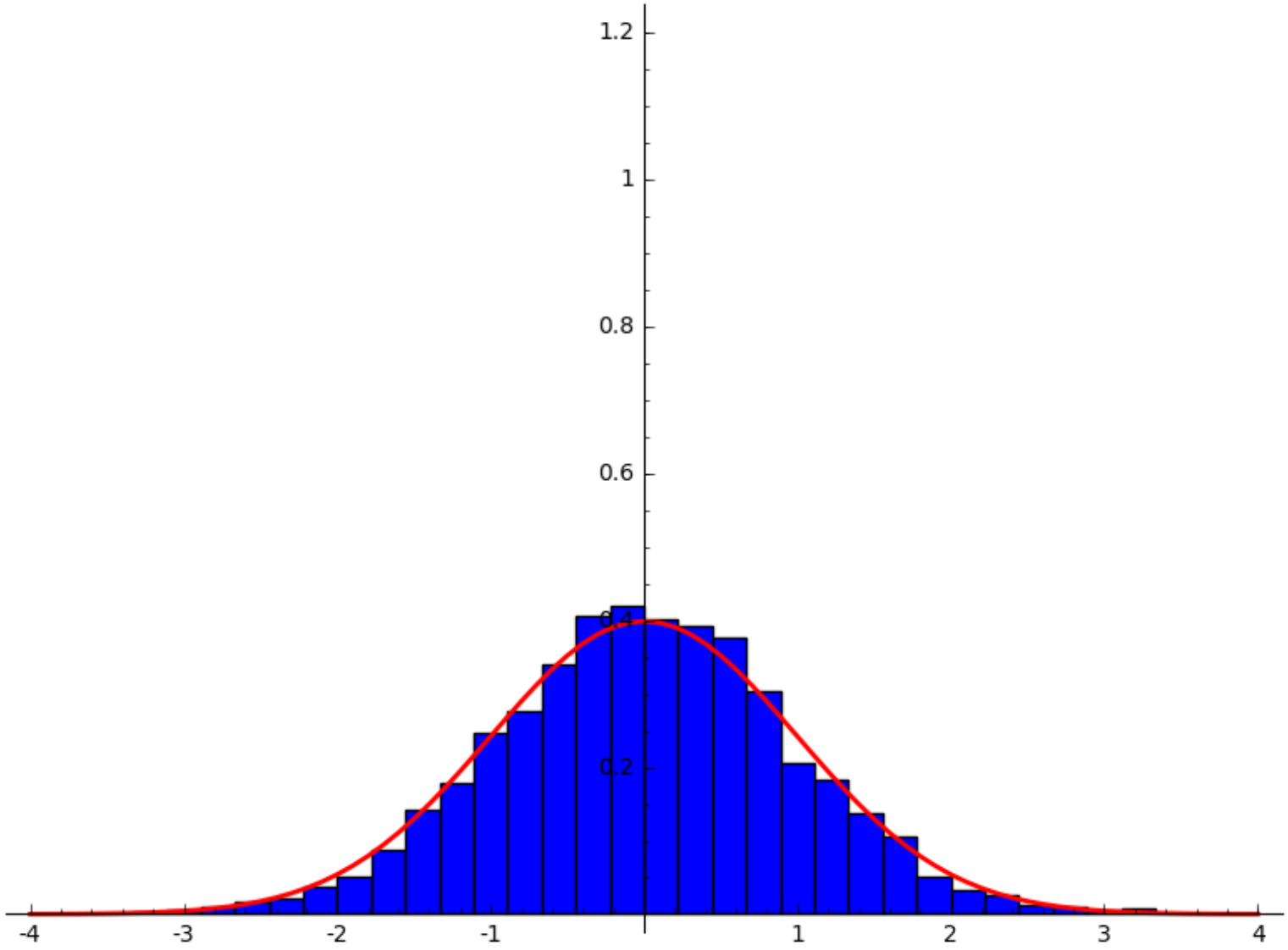
$d = 53$



Distribution of theta coefficients, small d

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

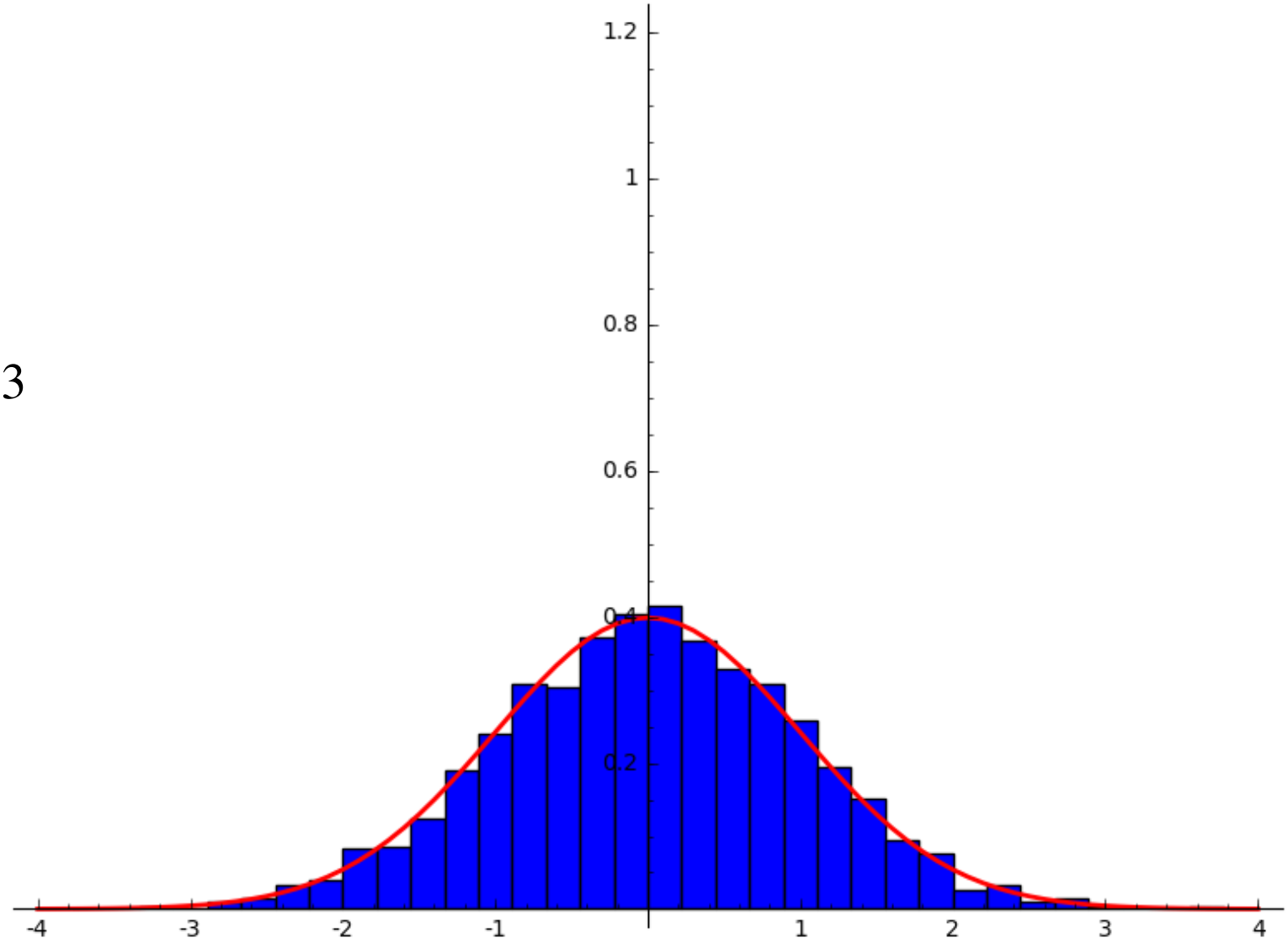
$d = 97$



Distribution of theta coefficients, small d

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

$d = 293$



Oversimplified picture

Suppose $F/\mathbb{Q}$ is a cyclic extension of degree d and conductor m.

Very roughly, θ_F lies in a cube of side $\sqrt{V_E \log(m)\varphi(m)/d}$ in the d-dimensional lattice $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$.

Suppose $\chi : \mathrm{Gal}(F/\mathbb{Q}) \xrightarrow{\sim} \boldsymbol{\mu}_d$ is a faithful character. Then

$$L(E,\chi,1) = 0 \iff \theta_F \in \ker(\chi : \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})] \to \mathbb{C}).$$

That kernel is a sublattice of codimension $\varphi(d)$, so we might expect the "probability" that $L(E,\chi,1) = 0$ should be about

$$\left(\frac{C_E}{\sqrt{\log(m)\varphi(m)/d}}\right)^{\varphi(d)}$$

for some constant C_E.

This goes to zero **very** fast as d and m grow.

Oversimplified picture

This isn't quite right:

- The previous argument ignores the Atkin-Lehner relation, which "pairs up" the coefficients and forces θ_F into a sublattice of $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ with rank approximately $d/2$. Taking this into account changes the expectation to

$$\left(\frac{C_E\, d}{\log(m)\varphi(m)}\right)^{\varphi(d)/4}.$$

Oversimplified picture

This isn't quite right:

- The previous argument ignores the Atkin-Lehner relation, which "pairs up" the coefficients and forces θ_F into a sublattice of $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ with rank approximately $d/2$. Taking this into account changes the expectation to

$$\left(\frac{C_E\, d}{\log(m)\varphi(m)}\right)^{\varphi(d)/4}.$$

- The distribution of the (normalized) θ_L is not uniform in a box, and we don't fully understand what the correct distribution is. Fortunately, for applications, it doesn't seem to matter very much what the distribution is, only that there is one and it's bounded independent of d.

The heuristic

This all leads to the folowing heuristic estimate:

Heuristic

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

$$\mathrm{Prob}[L(E,\chi,1)=0] \le \left(\frac{C_E\, d}{\log(m)\varphi(m)}\right)^{\varphi(d)/4}$$

where $d>2$ is the order of χ and m its conductor.

The exponent $\varphi(d)/4$ comes from the assumption that the theta coefficients are independent (except for the Atkin-Lehner relation).

Consequences of the heuristic

Heuristic

$$\mathrm{Prob}[L(E,\chi,1)=0] \le \left(\frac{C_E\, d}{\log(m)\varphi(m)}\right)^{\varphi(d)/4}.$$

Random matrix theory prediction:

RMT prediction (David, Fearnley, Kisilevsky)

For fixed prime d,

$$\mathrm{Prob}[L(E,\chi,1)=0] \approx C_{E,d}\left(\frac{\sqrt{\log(m)}}{m}\right)^{\varphi(d)/4}.$$

These agree up to power of log.

Consequences of the heuristic

Heuristic

$$\mathrm{Prob}[L(E,\chi,1)=0] \le \left(\frac{C_E\, d}{\log(m)\varphi(m)}\right)^{\varphi(d)/4}.$$

Proposition

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

$$\sum_{d\,:\,t(d)>1} \sum_{\chi \text{ order } d} \left(\frac{C_E\, d}{\log(m)\varphi(m)}\right)^{t(d)} \quad \textit{converges.}$$

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

Heuristic

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

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.

Consequences of the heuristic

Alternatively:

Conjecture

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

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

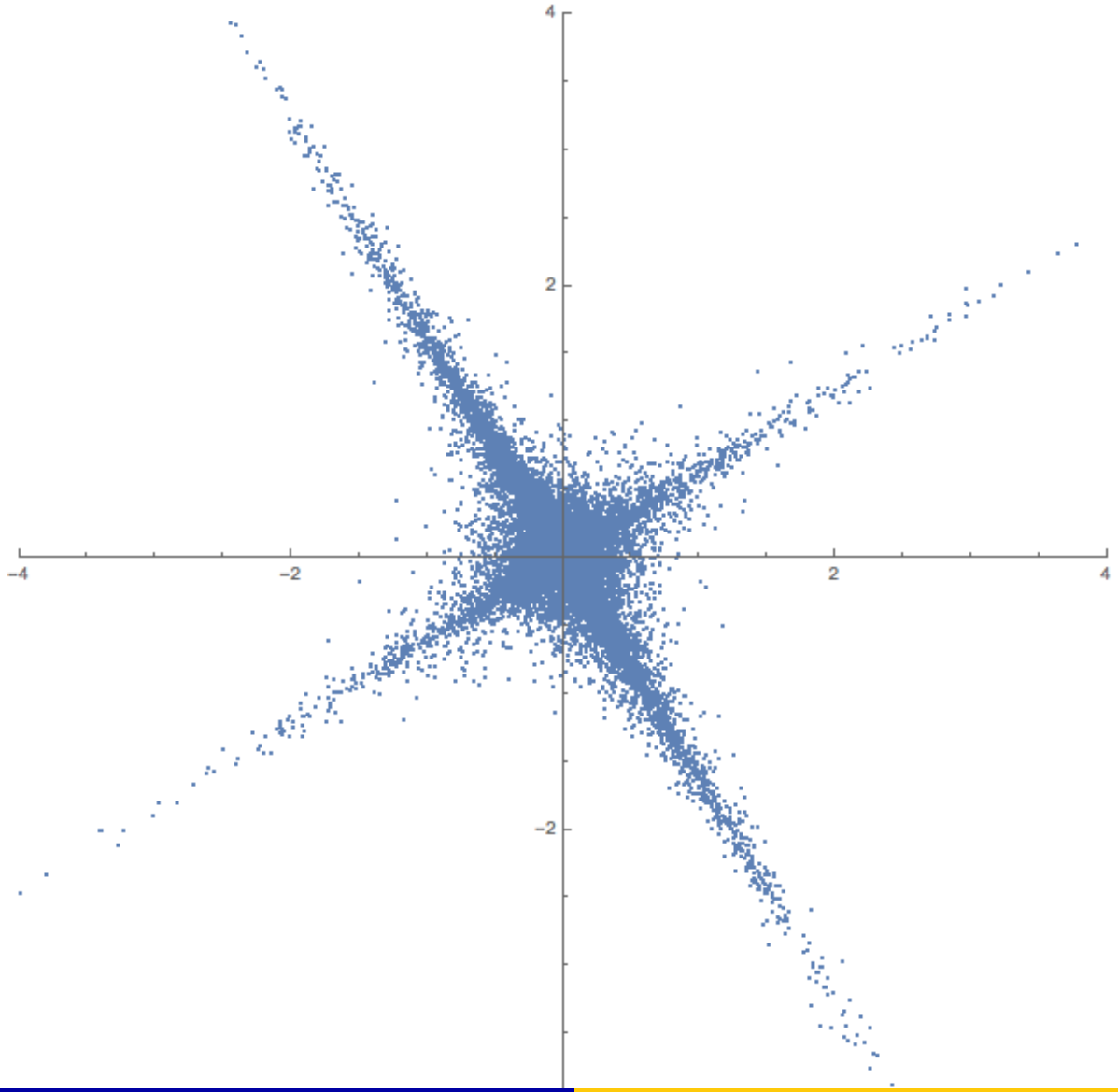
(In)dependence: star-like structure

Suppose d is an odd prime. Consider $F/\mathbb{Q}$ cyclic of degree d and E with global root number -1. Then the Atkin-Lehner relation tells us that one of the d theta coefficients is zero, and the others come in $(d-1)/2$ pairs $(c, -c)$.

If $d = 5$ or 7 we can plot the $(d-1)/2$-tuples of (normalized) theta coefficients. If they are indeed independent, we should get a cloud of data points concentrated near the origin without much other structure.

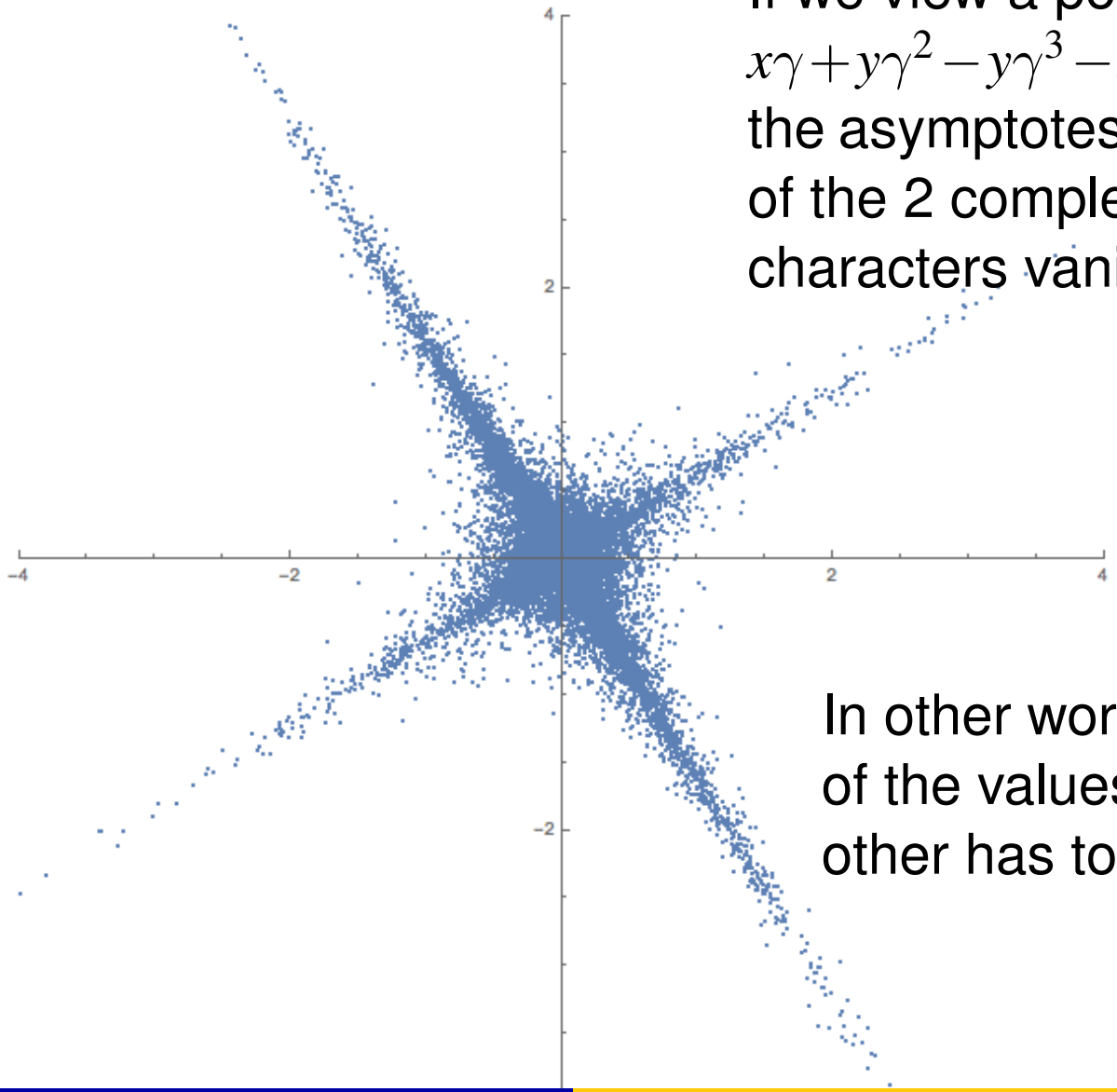
(In)dependence: star-like structure

Example: $E = 37A1$, $d = 5$



(In)dependence: star-like structure

Example: $E = 37A1$, $d = 5$



If we view a point (x, y) as an element $x\gamma + y\gamma^2 - y\gamma^3 - x\gamma^4 \in \mathbb{R}[\mathrm{Gal}(F/\mathbb{Q})]$, then the asymptotes are the lines where one of the 2 complex conjugate pairs of characters vanishes.

In other words, this says that if one of the values $\chi(\theta_F)$ is large, the other has to be small.

(In)dependence: star-like structure

Example: $E = 37A1$, $d = 7$

[3-dimensional Mathematica graphic]

(In)dependence: star-like structure

Example: $E = 37A1$, $d = 7$

[3-dimensional Mathematica graphic]

In this example the asymptote lines are the lines where **all except one** of the $(d-1)/2$ pairs of characters vanish.

In other words, if one of the values $\chi(\theta_F)$ is large, all the others seem to be (relatively) small.

(In)dependence: star-like structure

When $d = 5$ and the root number is $+1$, then there are 3 (potentially) independent theta coefficients. However, the Hecke relation on the modular symbols says that

$$\sum_{\gamma} c_{F,\gamma} = \left(\prod_{\ell | m} (a_\ell - 2) \right) [0] \ll \sqrt{m}$$

Since the $c_{F,\gamma}$ have size roughly $\sqrt{m \log(m)}$, this says that the sum of all the theta coefficients is essentially zero for large m.

Example: $E = 11A1$, $d = 5$

[3-dimensional Mathematica graphic]

(In)dependence: star-like structure

Another way to try to measure this phenomenon: Consider the monic polynomial

$$f_F(x) = x^{(p-1)/2} + c_1 x^{(p-3)/2} + \cdots + c_{(p-1)/2}$$

whose roots are the $(p-1)/2$ positive real numbers

$$\frac{|\chi(\theta_F)|^2}{m_\chi \log(m_\chi)}$$

for nontrivial χ (note that the $|\chi(\theta_F)|^2$ are positive, real, conjugate cyclotomic integers).

(In)dependence: star-like structure

Another way to try to measure this phenomenon: Consider the monic polynomial

$$f_F(x) = x^{(p-1)/2} + c_1 x^{(p-3)/2} + \cdots + c_{(p-1)/2}$$

whose roots are the $(p-1)/2$ positive real numbers

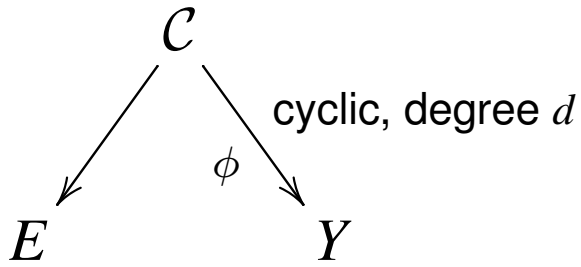
$$\frac{|\chi(\theta_F)|^2}{m_\chi \log(m_\chi)}$$

for nontrivial χ (note that the $|\chi(\theta_F)|^2$ are positive, real, conjugate cyclotomic integers).

The assertion that at most one $|\chi(\theta_F)|^2$ is 'large' is similar to asking that in the set $\{c_n^{1/n} : 1 \le n \le (p-1)/2\}$, only c_1 can be 'large'.

Constructing abelian points

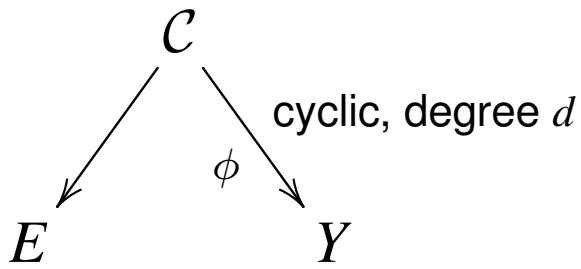
Suppose we have a diagram of curves



If $P \in Y(\mathbb{Q})$, then the points in the fiber $\phi^{-1}(P)$ are defined over a cyclic extension $L/\mathbb{Q}$ of degree (dividing) d. These project to points in $E(L)$.

Constructing abelian points

Suppose we have a diagram of curves

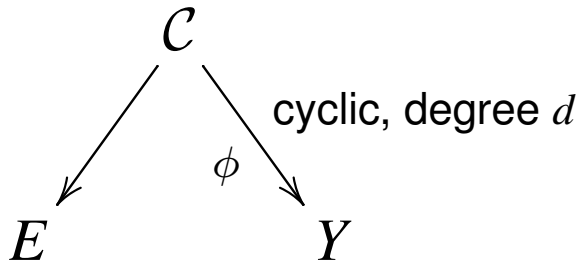


If $P \in Y(\mathbb{Q})$, then the points in the fiber $\phi^{-1}(P)$ are defined over a cyclic extension $L/\mathbb{Q}$ of degree (dividing) d. These project to points in $E(L)$.

If $Y = \mathbf{P}^1$, and d is prime, this produces $\sim X^\alpha$ cyclic extensions $L/\mathbb{Q}$ of degree d with $\operatorname{rank} E(L) > \operatorname{rank} E(\mathbb{Q})$ and $\operatorname{disc}(L) < X$, where α depends on $\deg(\phi)$.

Constructing abelian points

Suppose we have a diagram of curves



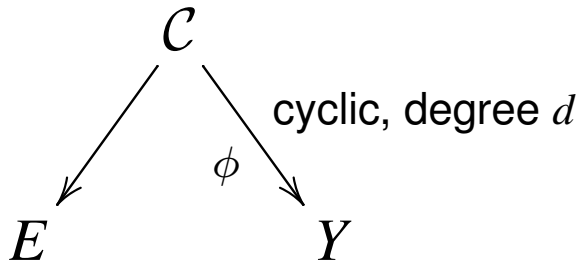
If $P \in Y(\mathbb{Q})$, then the points in the fiber $\phi^{-1}(P)$ are defined over a cyclic extension $L/\mathbb{Q}$ of degree (dividing) d. These project to points in $E(L)$.

If $Y = \mathbf{P}^1$, and d is prime, this produces $\sim X^\alpha$ cyclic extensions $L/\mathbb{Q}$ of degree d with $\operatorname{rank} E(L) > \operatorname{rank} E(\mathbb{Q})$ and $\operatorname{disc}(L) < X$, where α depends on $\deg(\phi)$.

- If $d = 3$, then for many elliptic curves E with a 3-isogeny, we can construct such a diagram with $Y = \mathbf{P}^1$.

Constructing abelian points

Suppose we have a diagram of curves



If $P \in Y(\mathbb{Q})$, then the points in the fiber $\phi^{-1}(P)$ are defined over a cyclic extension $L/\mathbb{Q}$ of degree (dividing) d. These project to points in $E(L)$.

If $Y = \mathbf{P}^1$, and d is prime, this produces $\sim X^\alpha$ cyclic extensions $L/\mathbb{Q}$ of degree d with $\operatorname{rank} E(L) > \operatorname{rank} E(\mathbb{Q})$ and $\operatorname{disc}(L) < X$, where α depends on $\deg(\phi)$.

- If $d = 5$ we know *one* example of such a diagram ($\mathcal{C}$ =“Bring’s curve”, of genus 4) with E in the isogeny class 50A and with Y of genus zero but $Y(\mathbb{Q}) = \emptyset$. For many imaginary quadratic fields K this gives many cyclic degree 5 extensions L/K with $\operatorname{rank} E(L) > \operatorname{rank} E(K)$.

Extensions and generalizations

Extension to other base fields: Suppose now that K is a number field and E is an elliptic curve over K. In this case there can be characters χ of $\mathrm{Gal}(\bar{K}/K)$ such that $L(E,\chi,1)$ vanishes because of root number considerations.

For all *other* χ we can ask whether

$$\mathrm{Prob}[L(E,\chi,1)=0] \ll \left(\frac{C_E d_\chi}{\log(m_\chi)\varphi(m_\chi)}\right)^{\varphi(d_\chi)/4} \qquad (*)$$

where d_χ is the order of χ and m_χ is the norm of its conductor.

Extensions and generalizations

Extension to other base fields: Suppose now that K is a number field and E is an elliptic curve over K. In this case there can be characters χ of $\mathrm{Gal}(\bar{K}/K)$ such that $L(E,\chi,1)$ vanishes because of root number considerations.

For all *other* χ we can ask whether

$$\mathrm{Prob}[L(E,\chi,1)=0] \ll \left(\frac{C_E d_\chi}{\log(m_\chi)\varphi(m_\chi)}\right)^{\varphi(d_\chi)/4} \qquad (*)$$

where d_χ is the order of χ and m_χ is the norm of its conductor.

(The motivation for (*) depends on the distribution of theta coefficients for abelian extensions F/K. Maarten Derickx and Alex Best are currently working to compute these general theta coefficients.)

Extensions and generalizations

Conjecture

Suppose L/K is an abelian extension with only finitely many subfields of degree 2, 3, or 5.

Then for every elliptic curve E/K, if we exclude those characters that vanish for root number considerations, then we expect $L(E, \chi, 1) = 0$ for only finitely many other characters χ of $\mathrm{Gal}(L/K)$.

Extensions and generalizations

Conjecture

Suppose L/K is an abelian extension with only finitely many subfields of degree 2, 3, or 5.

Then for every elliptic curve E/K, if we exclude those characters that vanish for root number considerations, then we expect $L(E, \chi, 1) = 0$ for only finitely many other characters χ of $\mathrm{Gal}(L/K)$.

Conjecture

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

Then for every elliptic curve E/L, we expect that $E(L)$ is finitely generated.

Extensions and generalizations

Studying p-Selmer: Instead of asking how often $L(E, \chi, 1) = 0$, we can ask how often $L(E, \chi, 1)/\Omega_E$ is divisible by (some prime above) p. By the Birch & Swinnerton-Dyer conjecture, this should tell us about the p-Selmer group $\mathrm{Sel}_p(E/L)$.

It seems reasonable to expect that if the θ-coefficents $c_{L,\chi,g}$ are not all the same (mod p), then they are equidistributed (mod p).

Extensions and generalizations

Studying p-Selmer: Instead of asking how often $L(E,\chi,1)=0$, we can ask how often $L(E,\chi,1)/\Omega_E$ is divisible by (some prime above) p. By the Birch & Swinnerton-Dyer conjecture, this should tell us about the p-Selmer group $\mathrm{Sel}_p(E/L)$.

It seems reasonable to expect that if the θ-coefficents $c_{L,\chi,g}$ are not all the same (mod p), then they are equidistributed (mod p).

For example, this leads to the following:

Conjecture

Let S be a finite set of rational primes, not containing p. Let L be the compositum of the cyclotomic $\mathbb{Z}_\ell$-extensions of $\mathbb{Q}$ for $\ell \in S$. If E is an elliptic curve over $\mathbb{Q}$ whose mod p representation is irreducible, then $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/L)$ is finite.

The heuristic does *not* predict finite p-Selmer rank when S is infinite.