Computers in Undergraduate Education and Zeros of Elliptic Curves

Steven Miller

Princeton University

FoCM: Minneapolis, August 10$^{\text{th}}$, 2002

http://www.princeton.edu/∼sjmiller/math/talks/talks.html
http://www.math.princeton.edu/∼mathlab/index.html

Junior Research Seminar / Undergraduate Math Lab

Problems (2000 – 2001)

1. Random Matrix Theory
2. Ramanujan Graphs
3. Hardy-Littlewood Varieties
4. Prime Spacings
5. Ranks of Elliptic Curves
6. $\{n^2\alpha\}$

Problems (2001 – 2002): Elliptic Curves

1. Analytic / Geometric Ranks in Families
2. Points of Low Height in Families
3. Distribution of Signs in Families
4. First Zero above Critical Point
5. Sato-Tate
6. Cryptography

Random Matrix Theory

Rebecca Lehman & Yi-Kai Liu

Consider $N \times N$ symmetric matrices with entries i.i.d.r.v. chosen from a fixed probability distribution P.

GOE Conjecture: As $N \to \infty$, the probability density of the distance between two consecutive (normalized) eigenvalues approaches the GOE distribution.

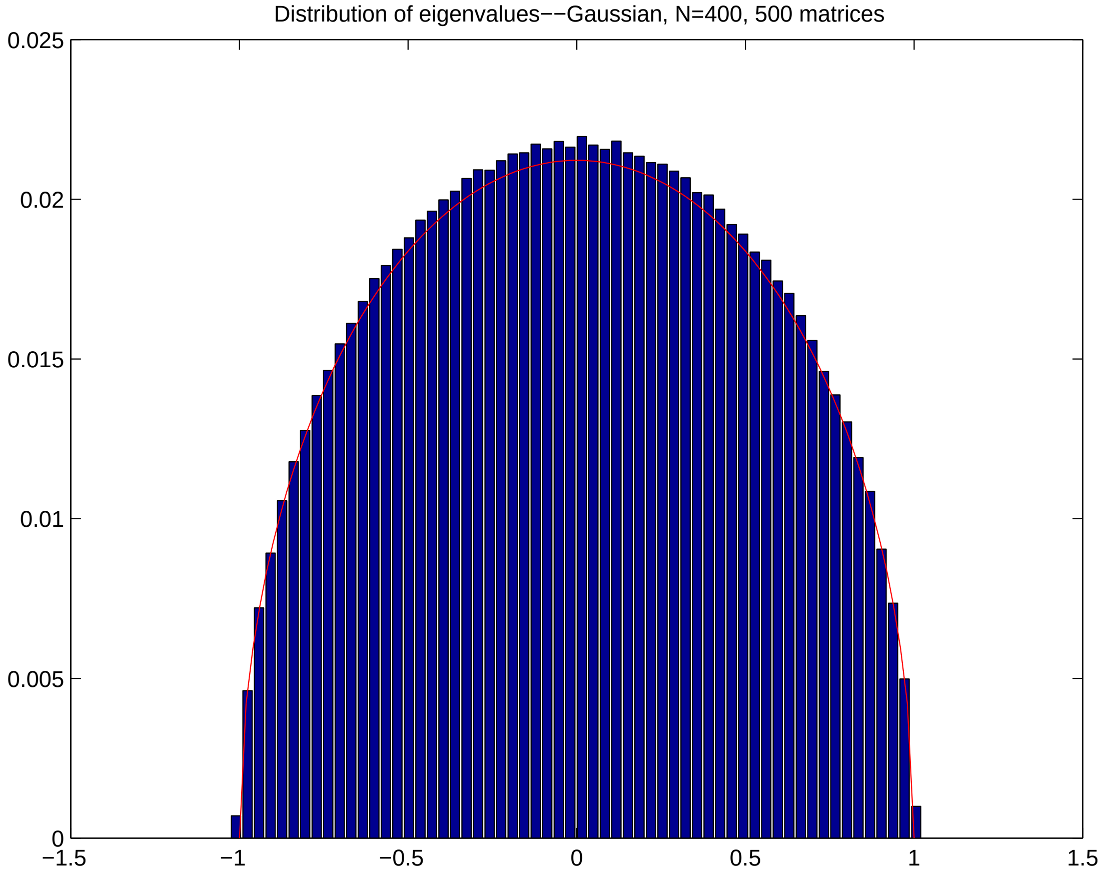
Only known if entries chosen from Gaussian.

Consecutive spacings well approximated by Axe^{-Bx^2}.

Semi-Circle Law: Assume P has mean 0, variance 1, other moments finite, $\frac{\lambda_j}{2\sqrt{N}}$ normalized eigenvectors.

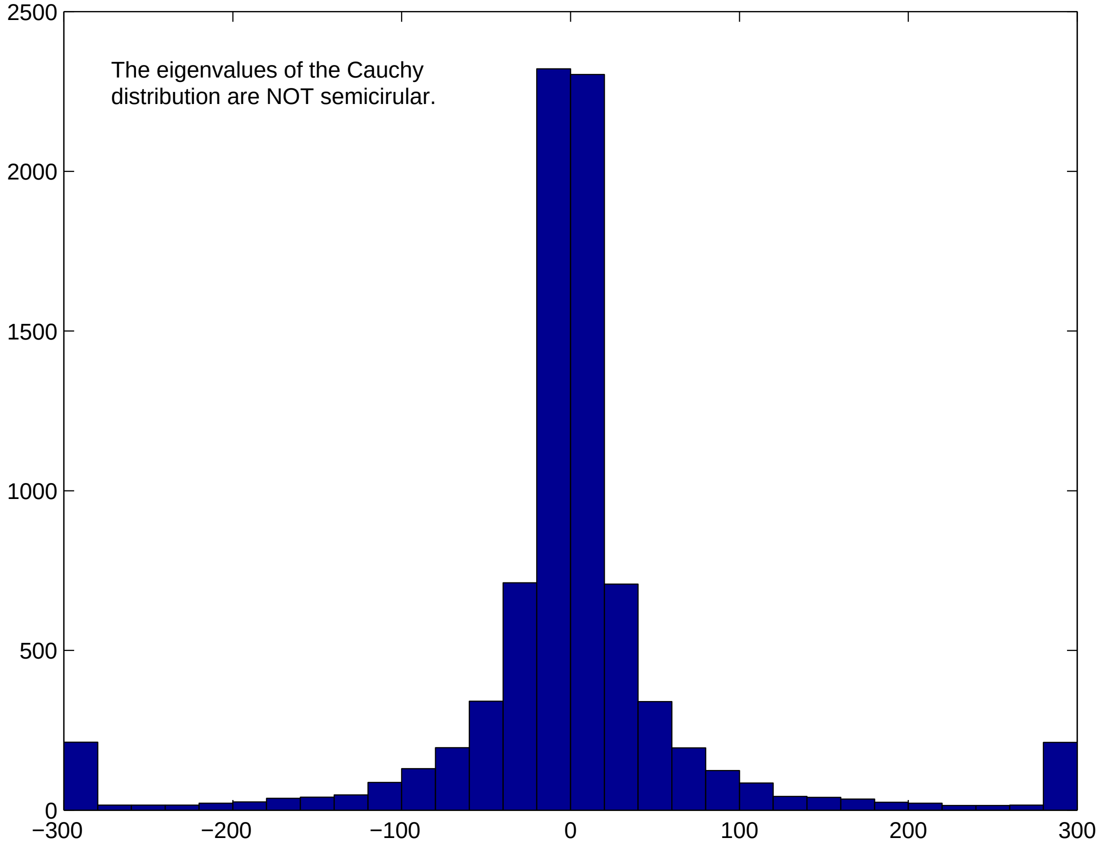
$$\begin{aligned} \mu_{A,N}(x) &= \frac{1}{N} \sum_{j=1}^{N} \delta\Big(x - \frac{\lambda_j}{2\sqrt{N}}\Big) \\ \mu_{A,N}(x) &\to \frac{2}{\pi}\sqrt{1-x^2} \text{ with probability 1} \end{aligned}$$

Random Matrix Theory: Semi-Circle Law



500 Matrices: Gaussian 400 × 400

Random Matrix Theory:
Semi-Circle Law



Cauchy Distr: Not-Semicircular (Infinite Variance)

$$P(t) = \frac{1}{\pi(1+t^2)}$$

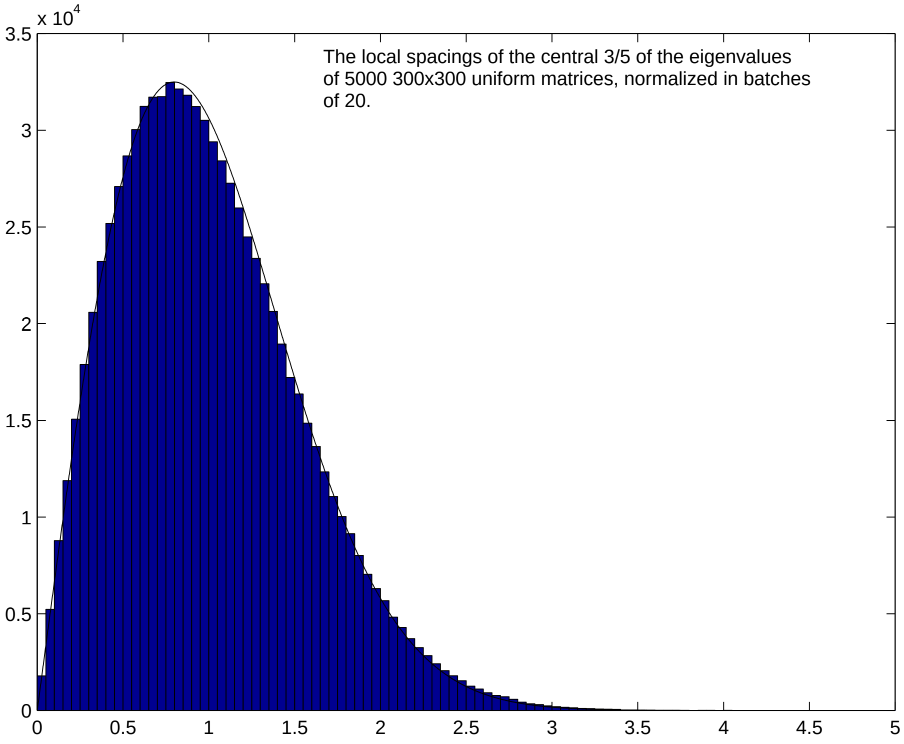
GOE Conjecture

GOE Conjecture: As $N \to \infty$, the probability density of the distance between two consecutive eigenvalues (normalized) approaches $\frac{\pi^2}{4}\frac{d^2\Psi}{dt^2}$ (the GOE distr).

Known if entries chosen from Gaussian.

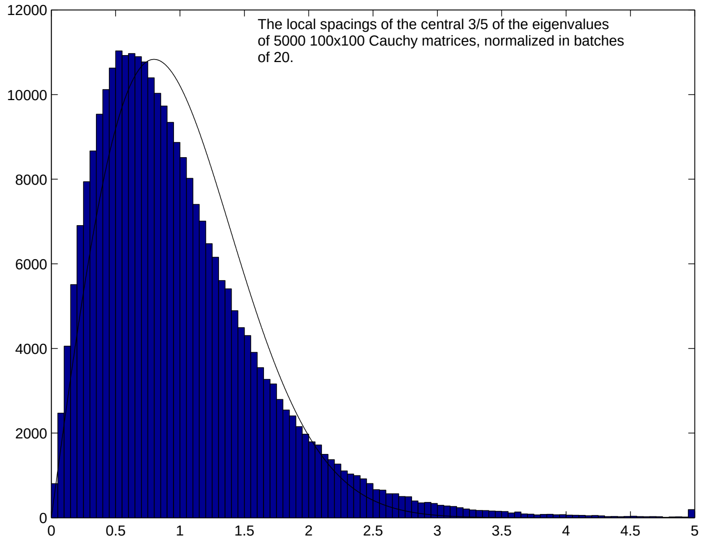
$\Psi(t)$ is (up to constants) the Fredholm determinant of the operator $f \to \int_{-t}^{t} K * f$, kernel $K = \frac{1}{2\pi}\left(\frac{\sin(\xi-\eta)}{\xi-\eta} + \frac{\sin(\xi+\eta)}{\xi+\eta}\right)$.

Consecutive spacings well approximated by Axe^{-Bx^2}.

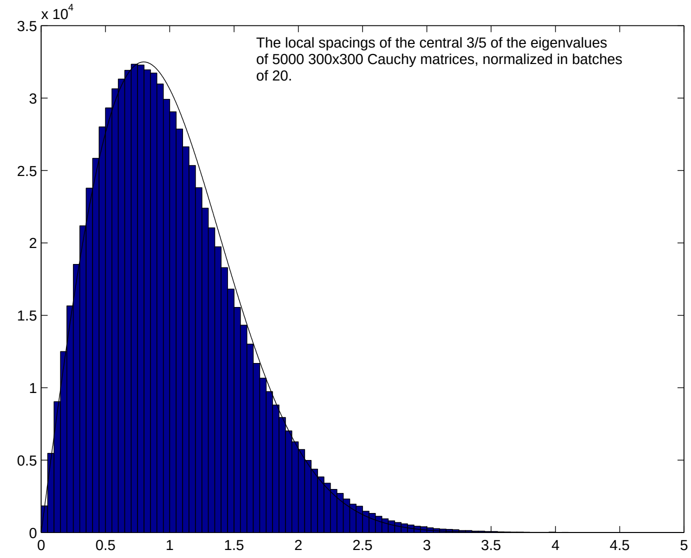


5000: 300×300 uniform on $[-1, 1]$

Cauchy Distr: $P(t) = \frac{1}{\pi(1+t^2)}$

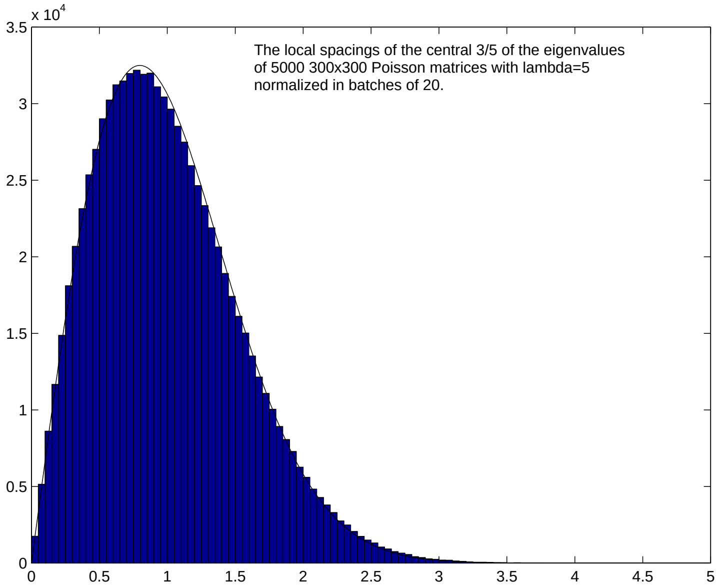


5000: 100 × 100 Cauchy

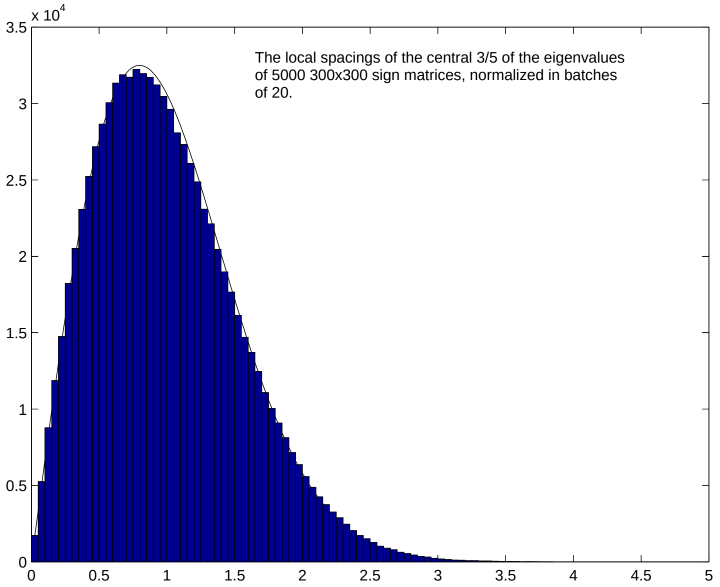


5000: 300 × 300 Cauchy

Poisson Distr: $P(n) = \frac{\lambda^n}{n!} e^{-\lambda}$

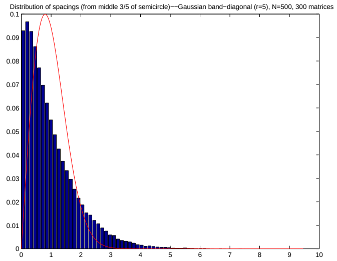


5000: 300×300 Poisson, $\lambda = 5$

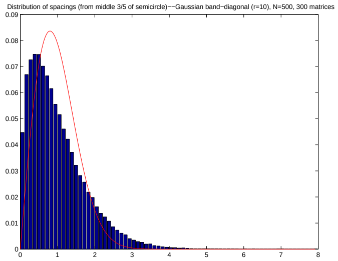


5000: 300×300 Poisson, $\lambda = 20$

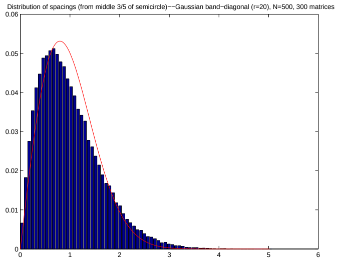
Band Matrices



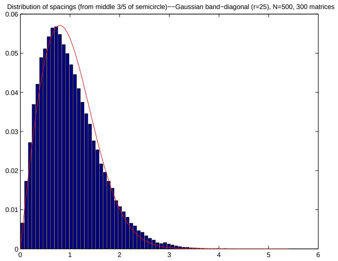
300 Band Matrices, 500×500, $r = 5$



300 Band Matrices, 500×500, $r = 10$

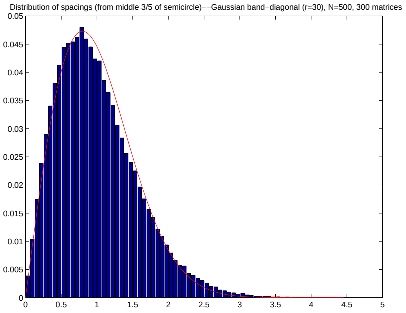


300 Band Matrices, 500×500, $r = 20$

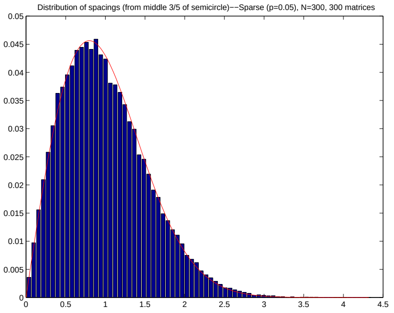


300 Band Matrices, 500×500, $r = 25$

Band and Sparse Matrices

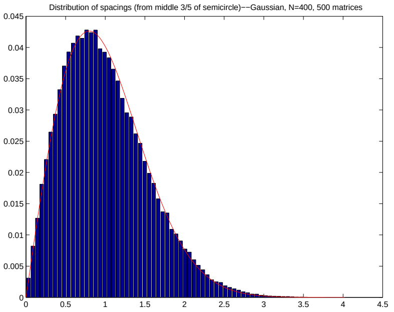


300 Band Matrices, 500×500, $r = 30$



300 Sparse Matrices, 300×300, $p = .05$ for $+1$, $p = .05$ for -1, $p = .90$ for 0

For comparison purposes, below is the distribution of spacings when the entries are chosen from the Gaussian distribution:



400 Gaussian Matrices, 400×400

Ramanujan Graphs

Peter Richter & Kevin Chang

G_n: family of k-reg graphs with n vertices.

1. $\lambda_0(G) = k$ for all $G \in G_n$
2. $\lambda_0(G) > \lambda_1(G)$ iff connected
3. $\liminf_{n\to\infty} \lambda_1(G_n) \geq 2\sqrt{k-1}$

A k-reg graph is Ramanujan if $\lambda_1 \leq 2\sqrt{k-1}$.

Sparse but have small diameters / high connectivity: useful for network building. Known constructions for $p^r + 1$, p prime.

Needed to:

1. Generate large numbers of k-regular bipartite graphs
2. Calculate λ_1 (the second largest eigenvalue)

Ramanujan Graphs: Conjectures

Consider all 3-regular bipartite graphs with n vertices.

Question 1: As $n \to \infty$, what percent of the graphs are Ramanujan?

Question 2: As $n \to \infty$, does each graph have $\lambda_1 \to 2\sqrt{2}$?

IE, is a randomly chosen 3-regular bipartite graph Ramanujan?

Similar questions for 7-regular bipartite graphs. Note 7 is smallest number with no known construction.

Ramanujan Results: $k = 3$

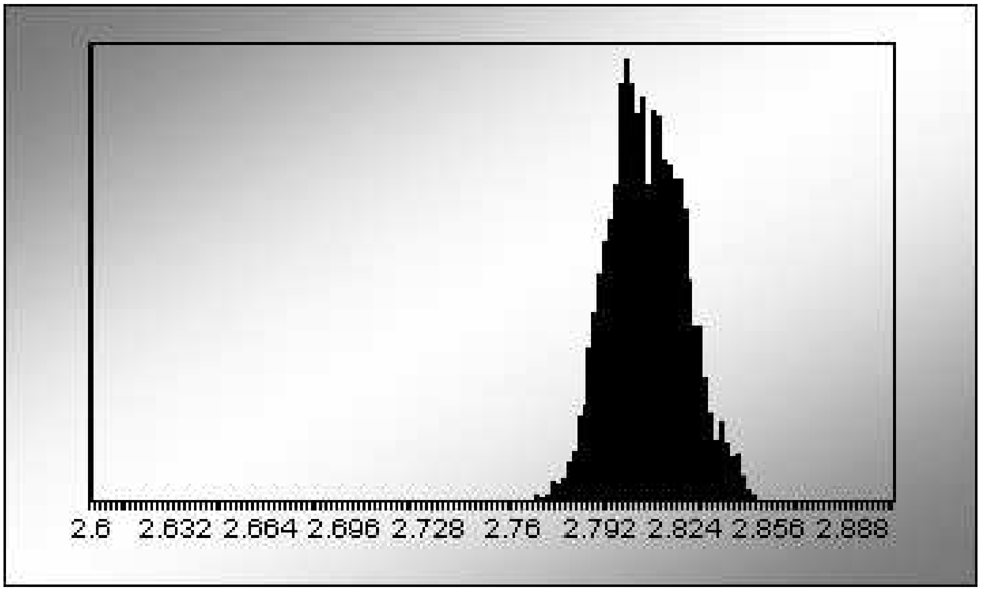
Randomly choosing 5000 3-regular bipartite graphs.

n	λ_1 mean	st dev	% Ram	λ_1 mean	st dev	% Ram
100	2.8076	0.042	76.14	2.777	0.031	95.28
200	2.8160	0.027	76.36	2.800	0.019	93.06
300	2.8187	0.020	77.38	2.808	0.014	92.84
400	2.8210	0.018	75.20	2.813	0.011	91.22
500	2.8216	0.014	76.62	2.815	0.009	91.40
600	2.8225	0.013	77.54	2.817	0.009	90.90
700	2.8226	0.012	78.46	2.818	0.008	91.00
800	2.8231	0.011	79.68	2.819	0.007	90.58
900	2.8233	0.011	80.34	2.820	0.007	91.06
1000	2.8235	0.009	79.86	2.820	0.006	91.12

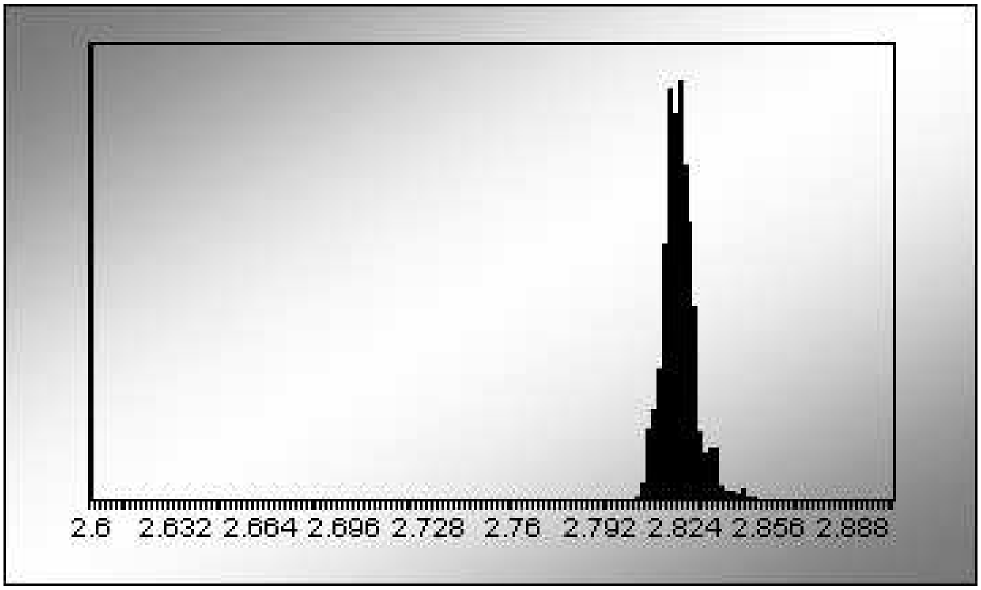
First group allows double and triple bonds; second group simple (single bonds only).

$$2\sqrt{3-1} \ = \ 2\sqrt{2} \ = \ 2.828427.$$

Ram. Results: $k = 3$, $2\sqrt{2} = 2.828$



λ_1: 5000 simple 3-reg graphs, 300 vertices



λ_1: 5000 simple 3-reg graphs, 1000 vertices

Ramanujan Results: $k = 7$

Randomly choosing 5000 7-regular bipartite graphs.

n	λ_1 mean	st dev	% Ram	λ_1 mean	st dev	% Ram
100	4.791	0.113	83.74	4.530	0.100	99.90
200	4.833	0.069	82.68	4.709	0.063	99.70
300	4.849	0.053	83.54	4.767	0.048	99.42
400	4.858	0.043	82.90	4.796	0.040	98.92
500	4.865	0.036	82.92	4.815	0.035	98.77
600	4.869	0.032	83.20	4.828	0.031	98.26
700	4.871	0.028	84.02	4.836	0.028	98.20
800	4.874	0.027	83.18			
900	4.875	0.025	82.84			
1000	4.877	0.022	83.92			

First group allows multipe bonds; second group single bonds only.

$2\sqrt{7-1} = 4.89898.$

Fundamental Problem: Spacing Between Events

General Formulation: Studying some system, observe values at t_1, t_2, t_3, etc. Question: what rules govern the spacings between events?

Often need to normalize by average spacing.

Example 1: Spacings Between Primes / Prime Pairs.

Example 2: Spacings Between Energy Levels of Nuclei.

Example 3: Spacings Between Eigenvalues of Matrices.

Example 4: Spacings Between Zeros of L-Functions.

Elliptic Curves

Consider $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbf{Q}$ and its L-function

$$L(s,E) = \prod_{p|\Delta} (1 - a_p p^{-s})^{-1} \prod_{p\ \dagger\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

By GRH: All non-trivial zeros on the critical line, can talk about spacings between zeros.

Rational solutions form a group:
$E(\mathbf{Q}) = \mathbf{Z}^r \oplus T$, T is the torsion points, r is the geometric rank.

Birch and Swinnerton-Dyer Conjecture: Geometric rank equals the analytic rank, the order of vanishing of $L(s,E)$ at $s = \frac{1}{2}$.

One-parameter families: $a_i = a_i(t) \in \mathbf{Z}[t]$.

Random Matrix Theory

Consider the group of $N \times N$ matrices from one of the classical compact groups: unitary, symplectic, orthogonal.

One assigns probability measures to matrices from various groups. By explicitly calculating properties associated to an individual matrix and integrating over the group, one can often use the group average to make good predictions about the expected behaviour of statistics from a generic, randomly chosen element.

More generally, can consider other spaces: GUE / GOE: Hermitian / Symmetric matrices with Gaussian probabilities for entries.

Measures of Spacings: n-Level Correlations

$\{\alpha_j\}$ be an increasing sequence of numbers, $B \subset \mathbf{R}^{n-1}$ a compact box. Define the n-level correlation by

$$\lim_{N\to\infty} \frac{\#\Big\{(\alpha_{j_1} - \alpha_{j_2}, \dots, \alpha_{j_{n-1}} - \alpha_{j_n}) \in B, j_i \neq j_k\Big\}}{N}$$

Instead of using a box, can use a smooth test function.

Results:

1. Normalized spacings of $\zeta(s)$ starting at 10^{20} (Odlyzko)
2. Pair and triple correlations of $\zeta(s)$ (Montgomery, Hejhal)
3. n-level correlations for all automorphic cupsidal L-functions (Rudnick-Sarnak)
4. n-level correlations for the classical compact groups (Katz-Sarnak)
5. insensitive to any finite set of zeros

Measures of Spacings: n-Level Density and Families

Let $f(x) = \Pi_i\, f_i(x_i)$, f_i even Schwartz functions whose Fourier Transforms are compactly supported.

$$D_{n,E}(f) \;\;=\;\; \sum_{\substack{j_1,\dots,j_n\\ distinct}} f_1(L_E\gamma_E^{(j_1)})\cdots f_n(L_E\gamma_E^{(j_n)})$$

1. individual zeros contribute in limit
2. most of contribution is from low zeros
3. average over similar curves (family)

To any geometric family, Katz-Sarnak predict the n-level density depends only on a symmetry group attached to the family.

Normalization of Zeros

How should we normalize the zeros of the curves in our family?

1. Local Data (hard): using some natural measure from the curve
2. Global Data (easy): using an average from the family

Hope: for f a good even test function with compact support, as $|\mathcal{F}| \to \infty$,

$$\begin{aligned}
\frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} D_{n,E}(f) &= \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} \prod_i f_i\Big(\frac{\log N_E}{2\pi} \gamma_E^{(j_i)}\Big) \\
&\to \int \cdots \int f(x) W_{n,\mathcal{G}(\mathcal{F})}(x) dx \\
&= \int \cdots \int \widehat{f}(u) \widehat{W_{n,\mathcal{G}(\mathcal{F})}}(u) du.
\end{aligned}$$

Much of the work is handling the dependence on the conductors.

1-Level Densities

Katz and Sarnak calculate the n-level densities for the classical compact groups. Unlike the correlations, the densities are different for different groups.

The Fourier Transforms for the 1-level densities are

$$\begin{aligned}
\widehat{W_{1,O^+}}(u) &= \delta_0(u) + \frac{1}{2}\eta(u) \\
\widehat{W_{1,O}}(u) &= \delta_0(u) + \frac{1}{2} \\
\widehat{W_{1,O^-}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) + 1 \\
\widehat{W_{1,Sp}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) \\
\widehat{W_{1,U}}(u) &= \delta_0(u)
\end{aligned}$$

where $\delta_0(u)$ is the Dirac Delta functional and $\eta(u)$ is 1, $\frac{1}{2}$, and 0 for $|u|$ less than 1, 1, and greater than 1.

2-Level Densities

We give the effect of the Fourier Transform of the densities on test functions supported in $\sigma_1 + \sigma_2 < 1$, where σ_i is the support of f_i.

Let $c(\mathcal{G}) = 0$, $\frac{1}{2}$ or 1 for $\mathcal{G} = SO(\text{even})$, O, and $SO(\text{odd})$. For $\mathcal{G}$ one of these three groups we have

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 &= [\widehat{f_1}(0) + \frac{1}{2}f_1(0)][\widehat{f_2}(0) + \frac{1}{2}f_2(0)] \\ &\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0) \\ &\quad -f_1(0)f_2(0) \\ &\quad + c(\mathcal{G})f_1(0)f_2(0).\end{aligned}$$

For $\mathcal{G} = U$ we have

$$\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,U}}(u)du_1du_2 = \widehat{f_1}(0)\widehat{f_2}(0) + \int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - \widehat{f_1f_2}(0),$$

and for $\mathcal{G} = Sp$, we have

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 &= [\widehat{f_1}(0) + \frac{1}{2}f_1(0)][\widehat{f_2}(0) + \frac{1}{2}f_2(0)] \\ &\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0) \\ &\quad - f_1(0)f_2(0) \\ &\quad -f_1(0)\widehat{f_2}(0) - \widehat{f_1}(0)f_2(0) + 2f_1(0)f_2(0).\end{aligned}$$

These densities are all distinguishable for functions with arbitrarily small support.

For the orthogonal groups, the densities (in this range) depend only on the distribution of the signs of the fuctionnal eqs.

Explicit Formula

Relates sums of test functions over zeros to sums over primes of $a_E(p)$ and $a_E^2(p)$.

$$\begin{aligned}\sum_{\gamma_E^{(j)}} G\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\Big) \ &= \ \widehat{G}(0) + G(0) \\ &\quad - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p}\widehat{G}\Big(\frac{\log p}{\log N_E}\Big)a_E(p) \\ &\quad - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{G}\Big(\frac{2\log p}{\log N_E}\Big)a_E^2(p) \\ &\quad + O\Big(\frac{\log\log N_E}{\log N_E}\Big).\end{aligned}$$

Modified Explicit Formula:

$$\begin{aligned}\sum_{\gamma_E^{(j)}} G\Big(\frac{\log X}{2\pi}\gamma_E^{(j)}\Big) \ &= \ \frac{\log N_E}{\log X}\widehat{G}(0) + G(0) \\ &\quad - 2\sum_p \frac{\log p}{\log X}\frac{1}{p}\widehat{G}\Big(\frac{\log p}{\log X}\Big)a_E(p) \\ &\quad - 2\sum_p \frac{\log p}{\log X}\frac{1}{p^2}\widehat{G}\Big(\frac{2\log p}{\log X}\Big)a_E^2(p) \\ &\quad + O\Big(\frac{\log\log X}{\log X}\Big).\end{aligned}$$

Some Previous Results

1. Orthogonal: Iwaniec-Luo-Sarnak: 1-level density for holomorphic even weight k cuspidal newforms of square-free level N (SO(even) and SO(odd) if split by sign)

2. Symplectic: Rubinstein: n-level densities for twists $L(s, \chi_d)$ of the zeta-function.

Main Tools:

1. Averaging Formulas (Petersson formula in ILS, Orthogonality of characters in Rubinstein)

2. Constancy of conductors

Elliptic Curve Conductors:

$$C(t) \ = \ \prod_{p|\Delta(t)} p^{f_p(t)}$$

1-Level Expansion

$$
\begin{aligned}
D_{1,\mathcal{F}}(f) \;=\; & \frac{1}{|\mathcal{F}|} \sum_{E\in\mathcal{F}} \sum_{j} f\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\Big) \\
\\
=\; & \frac{1}{|\mathcal{F}|} \sum_{E\in\mathcal{F}} \widehat{f}(0) + f_i(0) \\
& - \frac{2}{|\mathcal{F}|} \sum_{E\in\mathcal{F}} \sum_{p} \frac{\log p}{\log N_E} \frac{1}{p} \widehat{f}\Big(\frac{\log p}{\log N_E}\Big) a_E(p) \\
& - \frac{2}{|\mathcal{F}|} \sum_{E\in\mathcal{F}} \sum_{p} \frac{\log p}{\log N_E} \frac{1}{p^2} \widehat{f}\Big(2\frac{\log p}{\log N_E}\Big) a_E^2(p) \\
& + O\Big(\frac{\log\log N_E}{\log N_E}\Big)
\end{aligned}
$$

Want to move $\frac{1}{|\mathcal{F}|}\Sigma_{E\in\mathcal{F}}$

Leads us to study

$$A_{r,\mathcal{F}}(p) \;=\; \sum_{t(p)} a_t^r(p), \quad r = 1 \text{ or } 2.$$

2-Level Expansion

Need to evaluate terms like

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\frac{1}{p_i^{r_i}}g_i(\frac{\log p_i}{\log N_E})a_E^{r_i}(p_i).$$

Analogue of Petersson / Orthogonality: If $p_1,\dots,p_n$ are distinct primes

$$\sum_{t(p_1\cdots p_n)} a_{t_1}^{r_1}(p_1)\cdots a_{t_n}^{r_n}(p_n) = A_{r_1,\mathcal{F}}(p_1)\cdots A_{r_n,\mathcal{F}}(p_n).$$

Needed Input

For many families

$$\begin{aligned}(1) : A_{1,\mathcal{F}}(p) &= -rp + O(1)\\ (2) : A_{2,\mathcal{F}}(p) &= p^2 + O(p^{3/2})\end{aligned}$$

Rational Elliptic Surfaces (Silverman and Rosen):

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} -A_{\mathcal{E}}(p) \log p = r$$

Surfaces with $j(t)$ non-constant (Michel):

$$A_{2,\mathcal{F}}(p) = p^2 + O(p^{3/2}).$$

New Results

Rational Surfaces Density Theorem: *Consider a one-parameter family of elliptic curves of rank r over $\boldsymbol{Q}(t)$ that is a rational surface. Assume GRH, $j(t)$ non-constant, and the ABC (or Square-Free Sieve) conjecture if $\Delta(t)$ has an irreducible polynomial factor of degree at least 4. Let $m = deg\, C(t)$ and f_i be an even Schwartz function of small but non-zero support σ_i ($\sigma_1 < \min(\frac{1}{2}, \frac{2}{3m})$ for the 1-level density, $\sigma_1 + \sigma_2 < \frac{1}{3m}$ for the 2-level density). Possibly after passing to a subsequence, we observe two pieces. The first equals the expected contribution from r zeros at the critical point (agreeing with what B-SD suggests). The second is*

$$\begin{aligned} D_{1,\mathcal{F}}^{(r)}(f_1) &= \widehat{f_1}(0) + \frac{1}{2}f_1(0) \\ D_{2,\mathcal{F}}^{(r)}(f) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1 f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1) \end{aligned}$$

where $N(\mathcal{F},-1)$ is the percent of curves with odd sign.

1. 1-level: unconditionally confirms Katz-Sarnak for small support
2. 2-level: conditionally confirms Katz-Sarnak for small support

Examples

Constant-Sign Families:

1. $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free: all even.
2. $y^2 = x^3 \pm 4(4t+2)x$, $4t+2$ Sq-Free: $+$ yields all odd, $-$ yields all even.
3. $y^2 = x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free: all odd.

First two rank 0 over $\mathbf{Q}(t)$; third is rank 1. Only assume GRH for first two; add B-SD to interpret third.

Family of Rank 6 over $\mathbf{Q}(t)$ (modulo reasonable conjs):

$$\begin{aligned} y^2 \ &= \ x^3 + (2at - B)x^2 + (2bt - C)(t^2 + 2t - A + 1)x \\ &\qquad +(2ct - D)(t^2 + 2t - A + 1)^2 \end{aligned}$$

$$\begin{aligned} A &= 8916100448256000000 \\ B &= -811365140824616222208 \\ C &= 26497490347321493520384 \\ D &= -343107594345448813363200 \\ a &= 16660111104 \\ b &= -1603174809600 \\ c &= 2149908480000 \end{aligned} \tag{0.1}$$

Sieving

$$\begin{aligned}\sum_{\substack{t=N\\ D(t)\\ sqfree}}^{2N} S(t) &= \sum_{d=1}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} S(t)\\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} S(t) + \sum_{d\geq \log^l N}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} S(t).\end{aligned}$$

Handle first piece by progressions (need progressions to evaluate sums of $a_t(p)$).

Handle second piece by Cauchy-Schwartz: The number of t in the second sum (by ABC or SqFree Sieve Conj) is $o(N)$. Can show $\sum_{t=N}^{2N} S^2(t) = O(N)$. Then

$$\begin{aligned}\sum_{t\in\mathcal{T}} S(t) &\ll \Big(\sum_{t\in\mathcal{T}} S^2(t)\Big)^{\frac{1}{2}} \cdot \Big(\sum_{t\in\mathcal{T}} 1\Big)^{\frac{1}{2}}\\ &\ll \Big(\sum_{t\in[N,2N]} S^2(t)\Big)^{\frac{1}{2}} \cdot o\Big(\sqrt{N}\Big).\end{aligned}$$

Partial Summation

Notation: $\tilde{a}_{d,i,p}(t') = a_{t(d,i,t')}(p)$, $G_{d,i,P}(u)$ is related to the test functions, d and i from progressions.

Applying Partial Summation

$$\begin{aligned} S(d,i,r,p) &= \sum_{t'=0}^{[N/d^2]} \tilde{a}^r_{d,i,p}(t') G_{d,i,p}(t') \\ &= \Big(\frac{[N/d^2]}{p} A_{r,\mathcal{F}}(p) + O(p^R)\Big) G_{d,i,p}([N/d^2]) \\ &\quad - \sum_{u=0}^{[N/d^2]-1} \Big(\frac{u}{p} A_{r,\mathcal{F}}(p) + O(p^R)\Big) \\ &\quad \cdot \Big(G_{d,i,p}(u) - G_{d,i,p}(u+1)\Big) \end{aligned}$$

$O(p^R)$ is the error from using Hasse to bound the partial sums: $p^R = p^{1+\frac{r}{2}}$.

Difficult Piece

$$\frac{1}{N}\sum_p \frac{1}{p^r}\sum_{d,i}\sum_{u=0}^{[N/d^2]-1} O(p^{1+\frac{r}{2}})\cdot(G_{d,i,p}(u)-G_{d,i,p}(u+1))$$

Taylor Expansion not enough.

Use Bounded Variation: conductors must be monotone.

$$\begin{aligned} &\sum_{u=0}^{[N/d^2]-1}\Big|G_{d,i,p}(u)-G_{d,i,p}(u+1)\Big| \\ = &\sum_{u=0}^{[N/d^2]-1}\Big|g\Big(\frac{\log p}{\log C(t_i(d)+ud^2)}\Big)-g\Big(\frac{\log p}{\log C(t_i(d)+(u+1)d^2)}\Big)\Big|\end{aligned}$$

Handling the Conductors

$$\begin{aligned} C(t) &= \prod_{p|\Delta(t)} p^{f_p(t)} \\ D_1(t) &= \text{primitive irred. poly. factors } \Delta(t) \text{ and } c_4(t) \text{ share} \\ D_2(t) &= \text{remaining primitive irred. poly. factors of } \Delta(t) \\ D(t) &= D_1(t)D_2(t) \end{aligned}$$

$D(t)$ square-free, $C(t)$ like $D_1^2(t)D_2(t)$ except for a finite set of bad primes.

Let P be the product of the bad primes.

By Tate's Algorithm, can determine $f_p(t)$, which depends on the coefficients $a_i(t)$ mod powers of p.

Apply Tate's Algorithm to E_{t_1} to determine $f_p(t_1)$ for the bad primes. m large, $f_p(\tau) = f_p(P^m t + t_1) = f_p(t_1)$ for $p|P$.

m enormous, for bad primes, the order of p dividing $D(P^m t + t_1)$ is independent of t. So can find integers st $C(\tau) = c_{bad}\frac{D_1^2(\tau)}{c_1}\frac{D_2(\tau)}{c_2}$, $D(\tau)$ square-free.

Application: Bounding Excess Rank

$$D_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0).$$

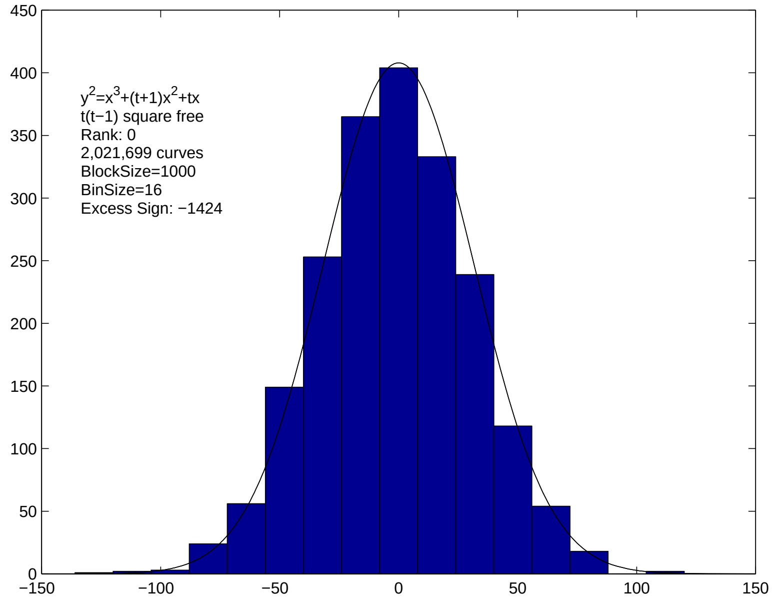
To estimate the percent with rank at least $r + R$, P_R, we get

$$Rf_1(0)P_R \leq \widehat{f_1}(0) + \frac{1}{2}f_1(0), \ R > 1.$$

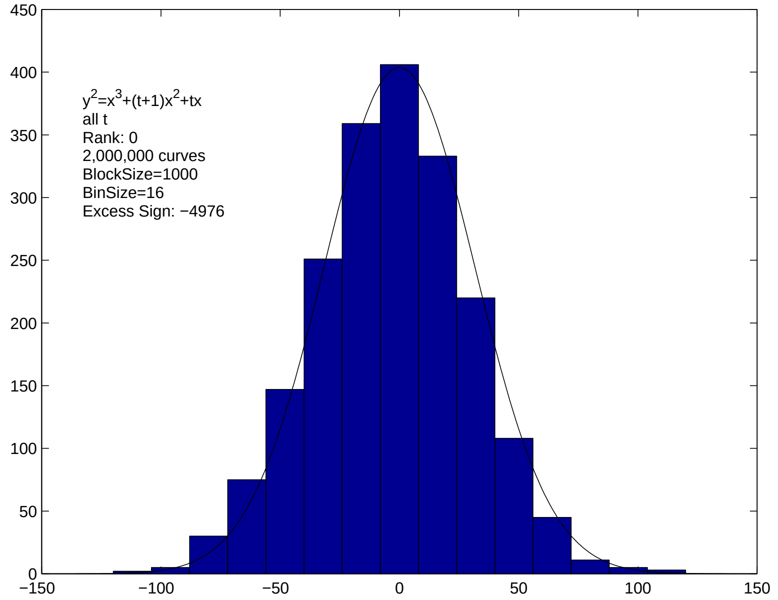
Note the family rank r has been cancelled from both sides.

By using the 2-level density, however, we get *squares* of the rank on the left hand side. The advantage is we get a cross term rR. The disadvantage is our support is smaller. Once R is large, the 2-level density yields better results.

Distribution of Signs: $y^2 = x^3 + (t+1)x^2 + tx$

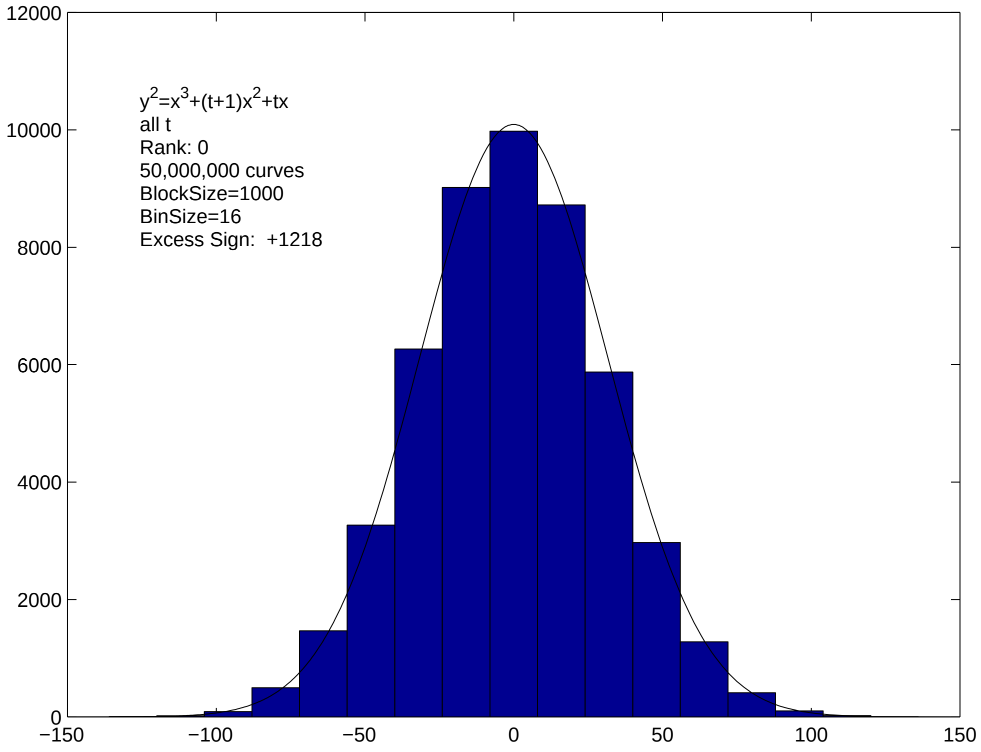


Histogram plot:$D(t)$ sq-free, first $2 \cdot 10^6$ such t.



Histogram plot: All $t \in [2, 2 \cdot 10^6]$.

Distribution of signs: $y^2 = x^3 + (t+1)x^2 + tx$



Histogram plot: All $t \in [2, 5 \cdot 10^7]$

The observed behaviour agrees with the predicted behaviour. Note as the number of curves increase (comparing the plot of $5 \cdot 10^7$ points to $2 \cdot 10^6$ points), the fit to the Gaussian improves.

Graphs by Atul Pokharel