Number Theory Seminar
Johns Hopkins University

Random Matrix Theory and Families of Elliptic Curves: Evidence for the Underlying Group Symmetries

Steven J. Miller

The Ohio State University

March 3rd, 2004

http://www.math.ohio-state.edu
/∼sjmiller/math/talks/talks.html

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

Heavy nuclei like Uranium ($200+$ protons / neutrons) even worse!

Info by shooting high-energy neutrons into nucleus.

Fundamental Equation:Quantum Mechanics

$$H\psi_n = E_n\psi_n$$

Similar to stat mech, leads to considering eigenvalues of ensembles of matrices.

Real Symmetric, Complex Hermitian, Classical Compact Groups.

L-Functions

L-functions: $\mathrm{Re}(s) > s_0$:

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s} = \prod_p L_p(p^{-s},f)^{-1}.$$

Functional equation: $s \longleftrightarrow 1-s$.

GRH: All L-functions (after normalization) have their non-trivial zeros on the critical line.

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

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

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 cuspidal 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 $\phi(x) = \prod_i \phi_i(x_i)$, ϕ_i even Schwartz functions, $\widehat{\phi}$ compactly supported.

$$D_{n,f}(\phi) \;=\; \sum_{\substack{j_1,\cdots,jn \\ distinct}} \phi_1\left(L_f\gamma_f^{(j_1)}\right)\cdots\phi_n\left(L_f\gamma_f^{(j_n)}\right)$$

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

$$D_{n,\mathcal{F}}(\phi) \;=\; \frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} D_{n,f}(\phi).$$

Correspondences

Similarities b/w Nuclei and L-Fns:

Zeros $\longleftrightarrow$ Energy Levels

Support $\longleftrightarrow$ Neutron Energy.

Some Number Theory Results

- Orthogonal:

  Iwaniec-Luo-Sarnak: 1-level density for $H_k^{\pm}(N)$, N square-free;

  Dueñez-Miller: 1, 2-level for $\{\phi \times f^2 : f \in H_k(1)\}$, ϕ even Maass;

  Miller: One-parameter families of elliptic curves.

- Symplectic:

  Rubinstein: n-level densities for $L(s, \chi_d)$;

  Dueñez-Miller: 1-level for $\{\phi \times f : f \in H_k(1)\}$, ϕ even Maass.

- Unitary: Miller, Hughes-Rudnick: Families of Primitive Dirichlet Characters.

Main Tools

- Averaging Formulas: Petersson formula, Orthogonality of characters.

- Explicit Formula: Relates sums over zeros to sums over primes.

- Control of conductors: Monotone.

1-Level Densities

Fourier Transforms for 1-level densities:

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

where $\delta_0(u)$ is the Dirac Delta functional and

$$\eta(u) = \begin{cases} 1 & \text{if } |u| < 1 \\ \frac{1}{2} & \text{if } |u| = 1 \\ 0 & \text{if } |u| > 1 \end{cases}$$

Dirichlet Characters: m Prime

$(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic, generator g.

Let $\zeta_{m-1} = e^{2\pi i/(m-1)}$.

Principal character χ_0 is given by

$$\chi_0(k) = \begin{cases} 1 & (k,m) = 1 \\ 0 & (k,m) > 1. \end{cases}$$

Determined by multiplicativity by action on g.

$\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$, $\forall \chi$ $\exists l$ st $\chi(g) = \zeta_{m-1}^l$:

$$\chi_l(k) \;=\; \begin{cases} \zeta_{m-1}^{la} & k \equiv g^a \bmod m \\ 0 & (k,m) > 0 \end{cases}$$

Dirichlet L-Functions

χ a primitive character mod m. Let

$$\tau(m,\chi) = \sum_{k=0}^{m-1} \chi(k) e^{2\pi i k/m}.$$

$\tau(m,\chi)$ is a Gauss sum of modulus $\sqrt{m}$.

$$\begin{aligned} L(s,\chi) &= \prod_p (1-\chi(p)p^{-s})^{-1} \\ \Lambda(s,\chi) &= \pi^{-\frac{1}{2}(s+\epsilon)} \Gamma\left(\frac{s+\epsilon}{2}\right) m^{\frac{1}{2}(s+\epsilon)} L(s,\chi), \end{aligned}$$

where

$$\epsilon = \begin{cases} 0 & \text{if } \chi(-1) = \ \ 1 \\ 1 & \text{if } \chi(-1) = -1 \end{cases}$$

$$\Lambda(s,\chi) = (-i)^{\epsilon} \frac{\tau(m,\chi)}{\sqrt{m}} \Lambda(1-s,\bar{\chi}).$$

Explicit Formula

ϕ even Schwartz, $\widehat{\phi}$ compact support $(-\sigma, \sigma)$.

χ a non-trivial primitive Dirichlet character of conductor m.

$$\begin{aligned}
&\sum \phi\left(\gamma \frac{\log(\frac{m}{\pi})}{2\pi}\right) \\
= &\int_{-\infty}^{\infty} \phi(y)dy \\
&-\sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)[\chi(p)+\bar{\chi}(p)]p^{-\frac{1}{2}} \\
&-\sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\Big(2\frac{\log p}{\log(m/\pi)}\Big)[\chi^2(p)+\bar{\chi}^2(p)]p^{-1} \\
&+O\Big(\frac{1}{\log m}\Big).
\end{aligned}$$

Expansion

$\{\chi_0\} \cup \{\chi_l\}_{l \leq m-2}$ are all the characters mod m.

Consider the family of primitive characters mod a prime m ($m-2$ characters):

$$\begin{aligned}
& \frac{1}{m-2} \sum \phi\left(\gamma \frac{\log(\frac{m}{\pi})}{2\pi}\right) \\
= & \int_{-\infty}^{\infty} \phi(y) dy \\
- & \frac{1}{m-2} \sum_{\chi \neq \chi_0} \sum_{p} \frac{\log p}{\log(m/\pi)} \widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big) [\chi(p) + \bar{\chi}(p)] p^{-\frac{1}{2}} \\
- & \frac{1}{m-2} \sum_{\chi \neq \chi_0} \sum_{p} \frac{\log p}{\log(m/\pi)} \widehat{\phi}\Big(2\frac{\log p}{\log(m/\pi)}\Big) [\chi^2(p) + \bar{\chi}^2(p)] p^{-1} \\
+ & O\Big(\frac{1}{\log m}\Big).
\end{aligned}$$

Note can pass Character Sum through Test Function.

Character Sums

$$\sum_{\chi} \chi(k) = \begin{cases} m-1 & k \equiv 1(m) \\ 0 & \text{otherwise} \end{cases}$$

For any prime $p \neq m$

$$\sum_{\chi \neq \chi_0} \chi(p) \; = \; \begin{cases} m-1-1 & p \equiv 1(m) \\ -1 & \text{otherwise} \end{cases}$$

Substitute into

$$\frac{1}{m-2} \sum_{\chi \neq \chi_0} \sum_{p} \frac{\log p}{\log(m/\pi)} \widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big) [\chi(p) + \bar{\chi}(p)] p^{-\frac{1}{2}}$$

First Sum

$$\begin{aligned}
&\frac{-2}{m-2}\sum_{p}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)p^{-\frac{1}{2}}\\
+\ \ &2\frac{m-1}{m-2}\sum_{p\equiv 1(m)}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)p^{-\frac{1}{2}}\\
\ll\ &\frac{1}{m}\sum_{p}^{m^\sigma}p^{-\frac{1}{2}}\ +\ \sum_{p\equiv 1(m)}^{m^\sigma}p^{-\frac{1}{2}}\\
\ll\ &\frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\ +\ \sum_{\substack{k\equiv 1(m)\\ k\geq m+1}}^{m^\sigma}k^{-\frac{1}{2}}\\
\ll\ &\frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\ +\ \frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\\
\ll\ &\frac{1}{m}m^{\sigma/2}.
\end{aligned}$$

No contribution if $\sigma < 2$.

Results

Theorem [Hughes-Rudnick]

$\mathcal{F}_N$ all primitive characters with prime conductor N.

If $\text{supp}(\widehat{\phi}) < 2$, as $N \to \infty$, agrees with Unitary.

Theorem [Miller]

$\mathcal{F}_N$ all primitive characters with conductor odd square-free integer in $[N, 2N]$.

If $\text{supp}(\widehat{\phi}) < 2$, as $N \to \infty$, agrees with Unitary.

Elliptic Curves

Conductors grow rapidly.

Results are for small support, where Orthogonal densities indistinguishable.

Study 2-Level Density.

2-Level Densities

$$c(\mathcal{G}) = \begin{cases} 0 & \text{if } \mathcal{G} = SO(\text{even}) \\ \frac{1}{2} & \text{if } \mathcal{G} = O \\ 1 & \text{if } \mathcal{G} = SO(\text{odd}) \end{cases}$$

For $\mathcal{G} = SO(\text{even}), O$ or $SO(\text{odd})$:

$$\begin{aligned} & \int\int \widehat{f}_1(u_1)\widehat{f}_2(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 \\ = & \left[\widehat{f}_1(0) + \frac{1}{2}f_1(0)\right]\left[\widehat{f}_2(0) + \frac{1}{2}f_2(0)\right] \\ & + 2\int |u|\widehat{f}_1(u)\widehat{f}_2(u)du \\ & -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) \\ & + c(\mathcal{G})f_1(0)f_2(0). \end{aligned}$$

2-Level Density: Orthogonal Groups

For small support, the difference due to distribution of signs.

Subtract off $j_1 = \pm j_2$ terms.

Let $\rho = 1 + i\gamma_E^{(j)}$ be a zero.

Even functional equation, label the zeros by

$$\cdots \leq \gamma_E^{(-2)} \leq \gamma_E^{(-1)} \leq 0 \leq \gamma_E^{(1)} \leq \gamma_E^{(2)} \leq \cdots, \gamma_E^{(-k)} = -\gamma_E^{(k)},$$

Odd functional equation, label the zeros by

$$\cdots \leq \gamma_E^{(-1)} \leq 0 \leq \gamma_E^{(0)} = 0 \leq \gamma_E^{(1)} \leq \cdots, \gamma_E^{(-k)} = -\gamma_E^{(k)}.$$

Elliptic Curves

$E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6, \;\; a_i \in \mathbb{Q}$

Often can write as $E : y^2 = x^3 + Ax + B$.

Let N_p be the number of solns mod p:

$$N_p = \sum_{x(p)} \left[1 + \left(\frac{x^3 + Ax + B}{p}\right)\right] = p+\sum_{x(p)} \left(\frac{x^3 + Ax + B}{p}\right)$$

Local data: $a_p = p - N_p$. Use to build the L-function.

One-parameter families:

$$y^2 \;=\; x^3 + A(t)x + B(t), \;\; A(t), B(t) \in \mathbb{Z}(t).$$

Elliptic Curves (cont)

$$L(E,s) \;=\; \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s} \;=\; \prod_{p} L_p(E,s).$$

$$\Lambda(s,E) = (2\pi)^{-s} N_E^{s/2} \Gamma\Big(s+\frac{1}{2}\Big) L(s,E) = \epsilon_E \Lambda(1-s,E)$$

By GRH: All zeros on the critical line.

Rational solutions: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus T$.

Birch and Swinnerton-Dyer Conjecture:
Geometric rank equals the analytic rank.

Comments on Previous Results

- explicit formula relating zeros and Fourier coeffs;
- averaging formulas for the family;
- conductors easy to control (constant or monotone)

Elliptic curve E_t: discriminant $\Delta(t)$, conductor $N_{E_t} = C(t)$ is

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

Normalization of Zeros

Local (hard) vs Global (easy).

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} D_{n,E}(f) \;=\; \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{\substack{j_1,\dots,jn\\ j_i\neq\pm j_k}}\prod_i f_i\left(\frac{\log N_E}{2\pi}\gamma_E^{(j_i)}\right)$$

$$\rightarrow \int\cdots\int f(x)W_{n,\mathcal{G}(\mathcal{F})}(x)dx$$

$$\rightarrow \int\cdots\int \widehat{f}(y)\widehat{W}_{n,\mathcal{G}(\mathcal{F})}(y)dy.$$

Conj: Distribution of Low Zeros agrees with Orthogonal Densities.

1-Level Expansion

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

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

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

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

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

Needed Input

For many families

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

Rational Elliptic Surfaces (Silverman and Rosen):

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

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

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

Rational Surfaces Density Theorem CONDITIONS

1-parameter family of Ell Curves, rank r over $\mathbb{Q}(t)$, rational surface. Assume

- GRH;
- $j(t)$ non-constant;
- Sq-Free Sieve if $\Delta(t)$ has irr poly factor of deg ≥ 4.

Pass to positive percent sub-seq where conductors polynomial of degree m.

f_i even Schwartz, support σ_i:

- $\sigma_1 < \min\left(\frac{1}{2}, \frac{2}{3m}\right)$ for 1-level
- $\sigma_1 + \sigma_2 < \frac{1}{3m}$ for 2-level.

Rational Surfaces Density Theorem RESULT

Two pieces.

First equals the contribution from r zeros at the critical point.

The second is

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

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

$N_{\mathcal{F}}(-1)$ *is the percent of curves with odd sign.*

1 and 2-level densities confirm Katz-Sarnak,

B-SD predictions for small support.

Examples

Constant-Sign Families:

1. $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Square-Free: all even.

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

3. $y^2 = x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Square-Free: all odd.

First two rank 0 over $\mathbb{Q}(t)$, third is rank 1.

Without 2-Level Density, couldn't say *which* orthogonal group.

Examples (cont)

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

$$y^2 = x^3 + (2at - B)x^2 + (2bt - C)(t^2 + 2t - A + 1)x \\ +(2ct - D)(t^2 + 2t - A + 1)^2$$

$$\begin{aligned} A &= 8,916,100,448,256,000,000 \\ B &= -811,365,140,824,616,222,208 \\ C &= 26,497,490,347,321,493,520,384 \\ D &= -343,107,594,345,448,813,363,200 \\ a &= 16,660,111,104 \\ b &= -1,603,174,809,600 \\ c &= 2,149,908,480,000 \end{aligned}$$

Need GRH, Sq-Free Sieve to handle sieving.

Sieving

$$\sum_{\substack{t=N \\ D(t) \\ sqfree}}^{2N} S(t) = \sum_{d=1}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t)$$

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

Handle first by progressions.

Handle second by Cauchy-Schwartz: The number of t in the second sum (by Sq-Free Sieve Conj) is $o(N)$:

$$\sum_{t\in\mathcal{T}} S(t) \ll \left(\sum_{t\in\mathcal{T}} S^2(t)\right)^{\frac{1}{2}} \cdot \left(\sum_{t\in\mathcal{T}} 1\right)^{\frac{1}{2}}$$

$$\ll \left(\sum_{t\in[N,2N]} S^2(t)\right)^{\frac{1}{2}} \cdot o\left(\sqrt{N}\right).$$

Sieving (cont)

$$\sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t)$$

$t_i(d)$ roots of $D(t) \equiv 0 \bmod d$.

$$t_i(d), t_i(d) + d^2, \ldots, t_i(d) + \left[\frac{N}{d^2}\right] d^2.$$

If $(d, p_1p_2) = 1$, go through complete set of residue classes $\frac{N/d^2}{p_1p_2}$ times.

Partial Summation

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

Applying Partial Summation

$$S(d,i,r,p) = \sum_{t'=0}^{[N/d^2]} \widetilde{a}^r_{d,i,p}(t') G_{d,i,p}(t')$$

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

First, Second and Third Sums

First Sum: Taylor Expansion. Gives the main term:

$$\frac{S_c(r,P)G_P(N)}{P}.$$

Second Sum: Sum over primes won't contribute for small support. $G_{d,i,P}$ term is $O(1)$, left with

$$\frac{1}{N}\prod_i \sum_{p_i=\log^l N}^{N^\alpha} \frac{1}{p_i} p_i^{1+\frac{r_i}{2}}.$$

Third Sum: Apply Partial Summation again. Taylor Expansion gains a $O\left(\frac{1}{\log N}\right)$, which is sufficient.

$$\begin{aligned} S_3(d,i,r,P) &= \left(G_{d,i,P}(0) - G_{d,i,P}\Big([N/d^2]\Big)\right)\frac{[N/d^2]-1}{P}S_c(r,P) \\ &\quad - \sum_{u=0}^{[N/d^2]-2}\Big(G_{d,i,P}(0) - G_{d,i,P}(u+1)\Big)\frac{1}{P}S_c(r,P). \end{aligned}$$

Difficult Piece: Fourth Sum I

$$\sum_{u=0}^{[N/d^2]-1} O(P^R)\Big(G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big)$$

Taylor $G_{d,i,P}(u) - G_{d,i,P}(u+1)$ gives $P^R \frac{N}{d^2} \frac{1}{P^r \log N}$. $\frac{1}{|\mathcal{F}|} \sum_{i,d}$ gives $O(\frac{P^R}{P^r \log N})$.

Problem is in summing over the primes, as we no longer have $\frac{1}{|\mathcal{F}|}$. We multiply by $\frac{1}{P^r}$.

Consider $r = (1, 0)$. Then $P = p_1 = p$, $R = 1 + \frac{r_1}{2} = \frac{3}{2}$, and $\frac{1}{P^r} = \frac{1}{p}$. We have

$$\sum_{p=\log^l N}^{N^{m\sigma}} \frac{1}{p} \frac{p^{\frac{3}{2}}}{\log N}$$

Fourth Sum: II

If exactly one of the r_j's is non-zero, then

$$\sum_{u=0}^{[N/d^2]-1} \left| G_{d,i,P}(u) - G_{d,i,P}(u+1) \right|$$
$$= \sum_{u=0}^{[N/d^2]-1} \left| g\left(\frac{\log p}{\log C(t_i(d) + ud^2)}\right) - g\left(\frac{\log p}{\log C(t_i(d) + (u+1)d^2)}\right) \right|$$

If the conductors are monotone, for fixed i, d and p, small.

If two of the r_j's are non-zero:

$$\begin{aligned} |a_1a_2 - b_1b_2| &= |a_1a_2 - b_1a_2 + b_1a_2 - b_1b_2| \\ &\leq |a_1a_2 - b_1a_2| + |b_1a_2 - b_1b_2| \\ &= |a_2| \cdot |a_1 - b_1| + |b_1| \cdot |a_2 - b_2| \end{aligned}$$

Handling the Conductors: I

$$y^2+a_1(t)xy+a_3(t)y = x^3+a_2(t)x^2+a_4(t)x+a_6(t)$$

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

$D_1(t)$ = primitive irred. poly. factors $\Delta(t)$ and $c_4(t)$ share

$D_2(t)$ = remaining primitive irred. poly. factors of $\Delta(t)$

$$D(t) = D_1(t)D_2(t)$$

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

Careful: $t(t+1)(t+2)(t+3)$.

Handling the Conductors: II

$$y^2+a_1(t)xy+a_3(t)y \;=\; x^3+a_2(t)x^2+a_4(t)x+a_6(t)$$

Let P be the product of the bad primes.

Tate's Algorithm gives $f_p(t)$, depend only on $a_i(t)$ mod powers of p.

Apply Tate's Algorithm to E_{t_1}. Get $f_p(t_1)$ for $p|P$. For m large, $p|P$,

$$f_p(\tau) = f_p(P^m t + t_1) = f_p(t_1),$$

and order of p dividing $D(P^m t + t_1)$ is independent of t.

Get integers st $C(\tau) = c_{bad}\frac{D_1^2(\tau)}{c_1}\frac{D_2(\tau)}{c_2}$, $D(\tau)$ sq-free.

Excess Rank

One-parameter family, rank r over $\mathbb{Q}(t)$.

RMT $\Longrightarrow$ 50% rank r, r+1.

For many families, observe

Percent with rank r = 32%
Percent with rank r+1 = 18%
Percent with rank r+2 = 48%
Percent with rank r+3 = 2%

Problem: small data sets, sub-families.

Application:
Bounding Excess Rank

$$D_{1,\mathcal{F}}(f_1) = \widehat{f}_1(0) + \frac{1}{2} f_1(0) + r f_1(0).$$

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

$$R f_1(0) P_R \leq \widehat{f}_1(0) + \frac{1}{2} f_1(0), \ R > 1.$$

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

The 2-level density gives ***squares*** of the rank on the left, get a cross term rR.

The disadvantage is our support is smaller.

Once R is large, the 2-level density yields better results.

Excess Rank Calculations
Families with $y^2 = f_t(x)$; $D(t)$ SqFree

Family	t Range	Num t	r	r	$r+1$	$r+2$	$r+3$
$+4(4t+2)$	$[2, 2002]$	1622	$*$	95.44		4.56	
$-4(4t+2)$	$[2, 2002]$	1622	0	70.53		29.35	
$9t+1$	$[2, 247]$	169	0	71.01		28.99	
t^2+9t+1	$[2, 272]$	169	1	71.60		27.81	
$t(t-1)$	$[2, 2002]$	643	0	40.44	48.68	10.26	0.62
$(6t+1)x^2$	$[2, 101]$	93	1	34.41	47.31	17.20	1.08
$(6t+1)x$	$[2, 77]$	66	2	30.30	50.00	16.67	3.03

1. $x^3 + 4(4t+2)x$, $4t+2$ Sq-Free, odd.
2. $x^3 - 4(4t+2)x$, $4t+2$ Sq-Free, even.
3. $x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free, even.
4. $x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free, odd.
5. $x^3 + (t+1)x^2 + tx$, $t(t-1)$ Sq-Free, rank 0.
6. $x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ Sq-Free, rank 1.
7. $x^3 - (6t+1)^2x + (6t+1)^2$, $(6t+1)[4(6t+1)^2 - 27]$ Sq-Free, rank 2.

Excess Rank Calculations
Families with $y^2 = f_t(x)$; All $D(t)$

Family	t Range	Num t	r	r	$r+1$	$r+2$	$r+3$
$+4(4t+2)$	$[2, 2002]$	2001	$*$	6.45	85.76	3.95	3.85
$-4(4t+2)$	$[2, 2002]$	2001	0	63.52	9.90	25.99	.50
$9t+1$	$[2, 247]$	247	0	55.28	23.98	20.73	
t^2+9t+1	$[2, 272]$	271	1	73.80		25.83	
$t(t-1)$	$[2, 2002]$	2001	0	42.03	48.43	9.25	0.30
$(6t+1)x^2$	$[2, 101]$	100	1	32.00	50.00	17.00	1.00
$(6t+1)x$	$[2, 77]$	76	2	32.89	50.00	14.47	2.63

1. $x^3 + 4(4t+2)x$, $4t+2$ Sq-Free, odd.
2. $x^3 - 4(4t+2)x$, $4t+2$ Sq-Free, even.
3. $x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free, even.
4. $x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free, odd.
5. $x^3 + (t+1)x^2 + tx$, $t(t-1)$ Sq-Free, rank 0.
6. $x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ Sq-Free, rank 1.
7. $x^3 - (6t+1)^2x + (6t+1)^2$, $(6t+1)[4(6t+1)^2 - 27]$ Sq-Free, rank 2.

More Data on Excess Rank

$$y^2+a_1xy+a_3y \;=\; x^3+a_2x^2+a_4x+a6$$

Family: $a_1 : 0$ to 10, rest -10 to 10.

Percent with rank 0 = 29.37%
Percent with rank 1 = 48.75%
Percent with rank 2 = 19.81%
Percent with rank 3 = 2.03%
Percent with rank 4 = .04%

14 Hours, 2,136,319 curves (1% repeat).

More Data on Excess Rank

$$y^2 + y = x^3 + tx.$$

Each data set 2000 curves from start.

t-Start	Rk 0	Rk 1	Rk 2	Rk 3	Time (hrs)
-1000	39.4	47.8	12.3	0.6	??
1000	38.4	47.3	13.6	0.6	??
4000	37.4	47.8	13.7	1.1	1
8000	37.3	48.8	12.9	1.0	2.5
24000	35.1	50.1	13.9	0.8	6.8
50000	36.7	48.3	13.8	1.2	51.8

Summary

- Similar behavior in different systems.
- Find correct scale.
- Average over similar elements.
- Need an Explicit Formula.
- Different statistics tell different stories.
- Evidence for B-SD, RMT interpretation of zeros
- Need more data.

Appendices

First two appendices list various standard conjectures. The second provides (at least conjecturally) when a family should have equidistribution of signs of functional equations. Experimental evidence is provided in the third appendix, which is on the distribution of signs of elliptic curves in a one-parameter family. Testing whether or not a generic family is equidistributed in sign. We looked at 1000 consecutive elliptic curves, and calculated the excess of positive over negative. We did this many times, and created a histogram plot. The fluctuations look Gaussian! The final appendix gives the formula to numerically approximate the analytic rank of an elliptic curve. For a curve of conductor N_E, one needs about $\sqrt{N_E}\log N_E$ Fourier coefficients.

Appendix I: Standard Conjectures

Generalized Riemann Hypothesis (for Elliptic Curves) *Let $L(s, E)$ be the (normalized) L-function of the elliptic curve E. Then the non-trivial zeros of $L(s, E)$ satisfy Re$(s) = \frac{1}{2}$.*

Birch and Swinnerton-Dyer Conjecture [BSD1], [BSD2] *Let E be an elliptic curve of geometric rank r over $\mathbb{Q}$ (the Mordell-Weil group is $\mathbb{Z}^r \oplus T$, T is the subset of torsion points). Then the analytic rank (the order of vanishing of the L-function at the critical point) is also r.*

Tate's Conjecture for Elliptic Surfaces [Ta] *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\acute{e}t}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\boldsymbol{C}$ and satisfies $-ord_{s=2}L_2(\mathcal{E}, s) =$ rank $NS(\mathcal{E}/\mathbb{Q})$, where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E}, s)$ does not vanish on the line Re$(s) = 2$.*

Most of the 1-param families we investigate are rational surfaces, where Tate's conjecture is known. See [RSi].

Appendix II: Equidistribution of Signs

ABC Conjecture *Fix $\epsilon > 0$. For co-prime positive integers a, b and c with $c = a + b$ and $N(a, b, c) = \prod_{p|abc} p$, $c \ll_\epsilon N(a, b, c)^{1+\epsilon}$.*

The full strength of ABC is never needed; rather, we need a consequence of ABC, the Square-Free Sieve (see [Gr]):

Square-Free Sieve Conjecture *Fix an irreducible polynomial $f(t)$ of degree at least 4. As $N \to \infty$, the number of $t \in [N, 2N]$ with $f(t)$ divisible by p^2 for some $p > \log N$ is $o(N)$.*

For irreducible polynomials of degree at most 3, the above is known, complete with a better error than $o(N)$ ([Ho], chapter 4).

Restricted Sign Conjecture (for the Family $\mathcal{F}$) *Consider a one-parameter family $\mathcal{F}$ of elliptic curves. As $N \to \infty$, the signs of the curves E_t are equidistributed for $t \in [N, 2N]$.*

The Restricted Sign conjecture often fails. First, there are families with constant $j(E_t)$ where all curves have the same sign. Helfgott [He] has recently related the Restricted Sign conjecture to the Square-Free Sieve conjecture and standard conjectures on sums of Moebius:

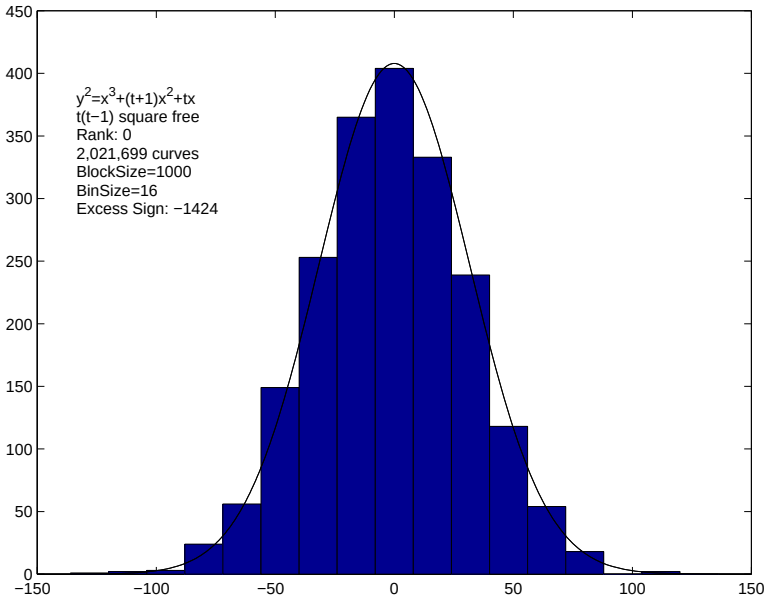
Polynomial Moebius *Let $f(t)$ be a non-constant polynomial such that no fixed square divides $f(t)$ for all t. Then $\sum_{t=N}^{2N} \mu(f(t)) = o(N)$.*

The Polynomial Moebius conjecture is known for linear $f(t)$.

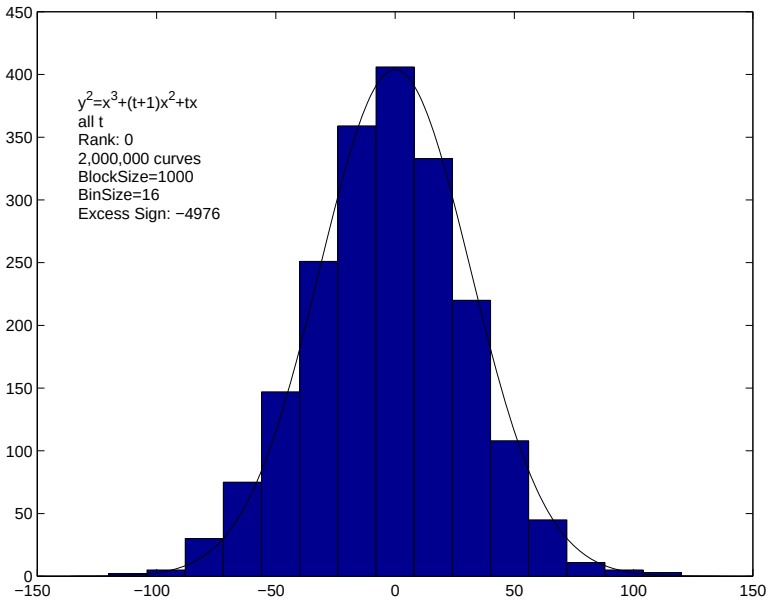
Helfgott shows the Square-Free Sieve and Polynomial Moebius imply the Restricted Sign conjecture for many families. More precisely, let $M(t)$ be the product of the irreducible polynomials dividing $\Delta(t)$ and not $c_4(t)$.

Theorem: Equidistribution of Sign in a Family [He]: *Let $\mathcal{F}$ be a one-parameter family with $a_i(t) \in \mathbb{Z}[t]$. If $j(E_t)$ and $M(t)$ are non-constant, then the signs of E_t, $t \in [N, 2N]$, are equidistributed as $N \to \infty$. Further, if we restrict to good t, $t \in [N, 2N]$ such that $D(t)$ is good (usually square-free), the signs are still equidistributed in the limit.*

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

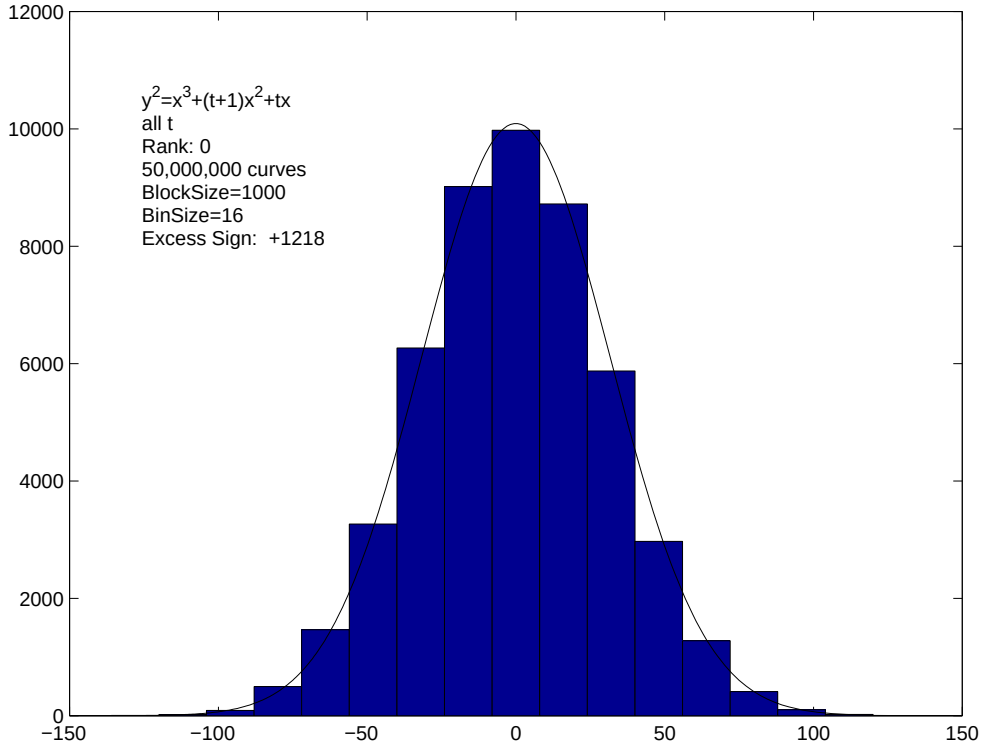


Histogram plot:$D(t)$ sq-free, first $2 \cdot 10^6$ such t.



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 behavior agrees with the predicted behavior. 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

Appendix III: Numerically Approximating Ranks: Preliminaries

Cusp form f, level N, weight 2:

$$\begin{aligned} f(-1/Nz) &= -\epsilon N z^2 f(z) \\ f(i/y\sqrt{N}) &= \epsilon y^2 f(iy/\sqrt{N}). \end{aligned}$$

Define

$$\begin{aligned} L(f,s) &= (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z} \\ \Lambda(f,s) &= (2\pi)^{-s} N^{s/2} \Gamma(s) L(f,s) = \int_0^{\infty} f(iy/\sqrt{N}) y^{s-1} dy. \end{aligned}$$

Get

$$\Lambda(f,s) = \epsilon \Lambda(f, 2-s), \;\; \epsilon = \pm 1.$$

To each E corresponds an f, write $\int_0^\infty = \int_0^1 + \int_1^\infty$ and use transformations.

Algorithm for $L^r(s, E)$: I

$$\begin{aligned}\Lambda(E,s) &= \int_0^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_0^1 f(iy/\sqrt{N})y^{s-1}dy + \int_1^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_1^\infty f(iy/\sqrt{N})(y^{s-1} + \epsilon y^{1-s})dy.\end{aligned}$$

Differentiate k times with respect to s:

$$\Lambda^{(k)}(E,s) = \int_1^\infty f(iy/\sqrt{N})(\log y)^k(y^{s-1} + \epsilon(-1)^k y^{1-s})dy.$$

At $s = 1$,

$$\Lambda^{(k)}(E,1) = (1 + \epsilon(-1)^k)\int_1^\infty f(iy/\sqrt{N})(\log\ y)^k dy.$$

Trivially zero for half of k; let r be analytic rank.

Algorithm for $L^r(s, E)$: II

$$\begin{aligned}\Lambda^{(r)}(E,1) &= 2\int_1^\infty f(iy/\sqrt{N})(\log\ y)^r dy \\ &= 2\sum_{n=1}^\infty a_n \int_1^\infty e^{-2\pi ny/\sqrt{N}}(\log\ y)^r dy.\end{aligned}$$

Integrating by parts

$$\Lambda^{(r)}(E,1) = \frac{\sqrt{N}}{\pi}\sum_{n=1}^\infty \frac{a_n}{n}\int_1^\infty e^{-2\pi ny/\sqrt{N}}(\log\ y)^{r-1}\frac{dy}{y}.$$

We obtain

$$L^{(r)}(E,1) = 2r!\sum_{n=1}^\infty \frac{a_n}{n} G_r\left(\frac{2\pi n}{\sqrt{N}}\right),$$

where

$$G_r(x) = \frac{1}{(r-1)!}\int_1^\infty e^{-xy}(\log y)^{r-1}\frac{dy}{y}.$$

Expansion of $G_r(x)$

$$G_r(x) = P_r\left(\log\frac{1}{x}\right) + \sum_{n=1}^{\infty}\frac{(-1)^{n-r}}{n^r\cdot n!}x^n$$

$P_r(t)$ is a polynomial of degree r, $P_r(t) = Q_r(t-\gamma)$.

$$\begin{aligned}
Q_1(t) &= t;\\
Q_2(t) &= \frac{1}{2}t^2 + \frac{\pi^2}{12};\\
Q_3(t) &= \frac{1}{6}t^3 + \frac{\pi^2}{12}t - \frac{\zeta(3)}{3};\\
Q_4(t) &= \frac{1}{24}t^4 + \frac{\pi^2}{24}t^2 - \frac{\zeta(3)}{3}t + \frac{\pi^4}{160};\\
Q_5(t) &= \frac{1}{120}t^5 + \frac{\pi^2}{72}t^3 - \frac{\zeta(3)}{6}t^2 + \frac{\pi^4}{160}t - \frac{\zeta(5)}{5} - \frac{\zeta(3)\pi^2}{36}.
\end{aligned}$$

For $r = 0$,

$$\Lambda(E,1) = \frac{\sqrt{N}}{\pi}\sum_{n=1}^{\infty}\frac{a_n}{n}\,e^{-2\pi ny/\sqrt{N}}.$$

Need about $\sqrt{N}$ or $\sqrt{N}\log N$ terms.

Bibliography

[BEW] B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. **21**, Wiley-Interscience Publications, John Wiley & Sons, Inc., New York, 1998.

[Bi] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43**, 1968, $57 - 60$.

[BS] B. Birch and N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5**, 1966, $295 - 299$.

[BSD1] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. reine angew. Math. **212**, 1963, $7 - 25$.

[BSD2] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218**, 1965, $79 - 108$.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\boldsymbol{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, no. 4, 2001, $843 - 939$.

[Br] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109**, 1992, $445 - 472$.

[BHB3] A. Brumer and R. Heath-Brown, *The average rank of elliptic curves III*, preprint.

[BHB5] A. Brumer and R. Heath-Brown, *The average rank of elliptic curves V*, preprint.

[BM] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. AMS **23**, 1991, $375 - 382$.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnterton-Dyer*, Invent. Math. **39**, 1977, $43 - 67$.

[Cr] Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

[Di] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144**, 1996, $137 - 166$.

[Fe1] S. Fermigier, *Zéros des fonctions L de courbes elliptiques*, Exper. Math. **1**, 1992, $167 - 173$.

[Fe2] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur $\mathbb{Q}$*, Exper. Math. **5**, 1996, $119 - 130$.

[FP] E. Fouvrey and J. Pomykala, *Rang des courbes elliptiques et sommes d'exponentelles*, Monat. Math. **116**, 1993, $111 - 125$.

[GM] F. Gouvéa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4**, 1991, $45 - 65$.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979), Lecture Notes in Math. **751**, Springer-Verlag, 1979, $108 - 118$.

[Gr] Granville, *ABC Allows Us to Count Squarefrees*, International Mathematics Research Notices **19**, 1998, $991 - 1009$.

[He] H. Helfgott, *On the distribution of root numbers in families of elliptic curves*, preprint.

[Ho] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, Cambridge, 1976.

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. **91**, 2000, $55 - 131$.

[Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, 1992.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36**, 1999, $1 - 26$.

[Ko] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, $429 - 436$.

[Mai] L. Mai, *The analytic rank of a family of elliptic curves*, Canadian Journal of Mathematics **45**, 1993, $847 - 862$.

[Mes1] J. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Mathematica **58**, 1986, $209 - 232$.

[Mes2] J. Mestre, *Courbes elliptiques de rang $\geq$ 11 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, $139 - 142$.

[Mes3] J. Mestre, *Courbes elliptiques de rang $\geq$ 12 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, $171 - 174$.

[Mi] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monat. Math. **120**, 1995, $127 - 136$.

[Mil] S. J. Miller, 1- *and* 2*-Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, P.H.D. Thesis, Princeton University, 2002, http://www.math.princeton.edu/$\sim$sjmiller/thesis/thesis.pdf.

[Mor] Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[Na1] K. Nagao, *On the rank of elliptic curve $y^2 = x^3 - kx$*, Kobe J. Math. **11**, 1994, $205 - 210$.

[Na2] K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11**, 1994, $211 - 219$.

[Na3] K. Nagao, *$\mathbb{Q}(t)$-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**, 1997, $13 - 32$.

[Ri] Rizzo, *Average root numbers for a non-constant family of elliptic curves*, preprint.

[Ro] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87**, 1993, $119 - 151$.

[RSi] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**, 1998, $43 - 67$.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Journal of Math. **81**, 1996, $269 - 322$.

[Sh] T. Shioda, *Construction of elliptic curves with high-rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43**, 1991, $673 - 719$.

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin - New York, 1986.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, Berlin - New York, 1994.

[Si3] J. Silverman, *The average rank of an algebraic family of elliptic curves*, J. reine angew. Math. **504**, 1998, $227 - 236$.

[St1] N. Stephens, *A corollary to a conjecture of Birch and Swinnerton-Dyer*, J. London Math. Soc. **43**, 1968, $146 - 148$.

[St2] N. Stephens, *The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **231**, 1968, $16 - 162$.

[ST] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, Journal of the American Mathematical Society **40**, number 4, 1995.

[Ta] J. Tate, *Algebraic cycles and the pole of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, $93 - 110$.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141**, 1995, $553 - 572$.

[Wa] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48**, number 177, 1987, $371 - 384$.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math **141**, 1995, $443 - 551$.