Distributions of 2-Selmer Ranks for Elliptic Curves: Part 3 of 3

Edray Herber Goins

Department of Mathematics
Purdue University

January 31, 2008

PURDUE
UNIVERSITY

Abstract

Consider the family of all elliptic curves E defined over $\mathbb{Q}$ such that the kernel of the multiplication-by-2-map $[2] : E \to E$ is rational. Galois cohomology asserts that the finite quotient $E(\mathbb{Q})/2\,E(\mathbb{Q})$ may be embedded in the infinite group $H^1(G_{\mathbb{Q}},\ E[2])$ in a canonical way. The latter contains is a "nice" finite subgroup, the 2-Selmer group $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$, which in turn contains the former. Fortunately, there are efficient algorithms to compute the size of this group – even though none really exist to compute the size of the aforementioned quotient.

In this the third of three talks, we discuss specific data compiled from a large number of examples. We focus on the idea that the sizes of the 2-Selmer groups may satisfy a distribution, and give computational evidence that the growth of these groups may not be a rapid as once expected.

Outline of Talk

Mordell-Weil and 2-Selmer Ranks

Recall that we wish to consider elliptic curves in the form

$$E_t: \qquad y^2 = \left(1 - x^2\right)\left(1 - k^2\, x^2\right) \qquad \text{where} \qquad k = \frac{t^2 - 6\, t^2 + 1}{\left(t^2 + 1\right)^2}.$$

Every elliptic curve E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ is in this form for some t. We think of E_t as fibers of an elliptic surface $\mathcal{E}$ defined over

$$V = \left\{ t = \frac{a}{b} \in \mathbb{P}^1 \;\middle|\; a\, b \left(a^4 - b^4\right)\left(a^4 - 6\, a^2\, b^2 + b^4\right) \neq 0 \right\}.$$

Using the connecting homomorphism δ_E, the Mordell-Weil rank $r = r(t)$ and the 2-Selmer rank $s = s(t)$ are defined using the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} & \xrightarrow{\delta_E} & \text{Sel}^{(2)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[2] & \longrightarrow & 0 \\
 & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq & & \\
1 & \longrightarrow & {Z_2}^{r+2} & \longrightarrow & {Z_2}^{s+2} & \longrightarrow & {Z_2}^{s-r} & \longrightarrow & 1
\end{array}$$

Histograms and Generating Functions

Let $\mathcal{E}$ be the elliptic surface which classifies elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. For each fiber E_t, define

$$S(t) = \left\{ p \in \text{Spec } \mathbb{Z} \;\middle|\; p \text{ divides } a\,b\,(a^4 - b^4)\,(a^4 - 6\,a^2\,b^2 + b^4) \right\}$$

as the collection of primes of bad reduction. Recall $r(t) \leq s(t) \leq 2\,|S(t)|$.

Given $f : V \to \mathbb{Z}$, define

$$\text{Histogram}_f(W) = \left\{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \;\middle|\; y = \left| f^{-1}(x) \cap W \right| \right\}$$

for $W \subseteq V$ with $\dim W = 0$. If these histograms converge, we will find it useful to define the generating function

$$\Phi_f(z) = \sum_{x \in \mathbb{Z}} \left[\lim_{W \to V} \frac{\left| f^{-1}(x) \cap W \right|}{|W|} \right] z^x.$$

Question: What can we say about the distributions of r, s, and $|S|$?

Number of Candidate Curves

Let $\mathcal{E}$ be the elliptic surface which classifies elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. For a bound T, we choose the D_8-conjugate

$$W_T = D_8 \cdot \left\{ (a : b) \in \mathbb{P}^1 \;\middle|\; 0 < \left(1 + \sqrt{2}\right) a < b \leq T \text{ and } \gcd(a, b) = 1 \right\}$$

as a finite subset of V. Recall that

$$\lim_{T \to \infty} W_T = V \qquad \text{and} \qquad \lim_{T \to \infty} \frac{|W_T|}{|T^2|} = \frac{4}{1 + \sqrt{2}} \cdot \frac{6}{\pi^2} = 1.0072\ldots$$

Hence the number isomorphism classes $\{E_t\}$ of fibers is the ratio

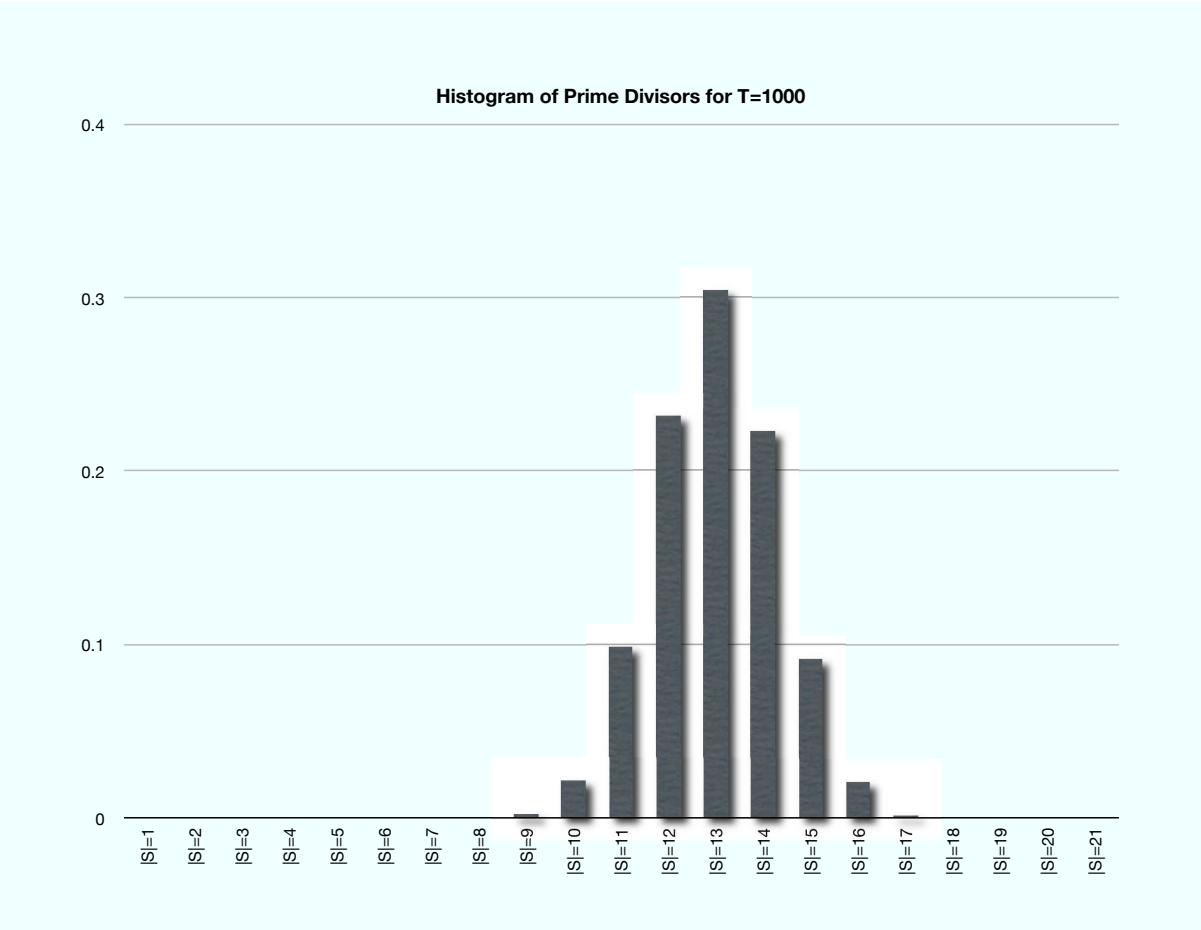
$$\frac{|W_T|}{|D_8|} \approx \frac{T^2}{8}$$

Bound T	1 000	2 000	3 000	4 000	5 000
$\frac{\lvert W_T \rvert}{\lvert D_8 \rvert}$	126 003	503 923	1 133 364	2 014 563	3 148 208

Data on Number of Prime Divisors

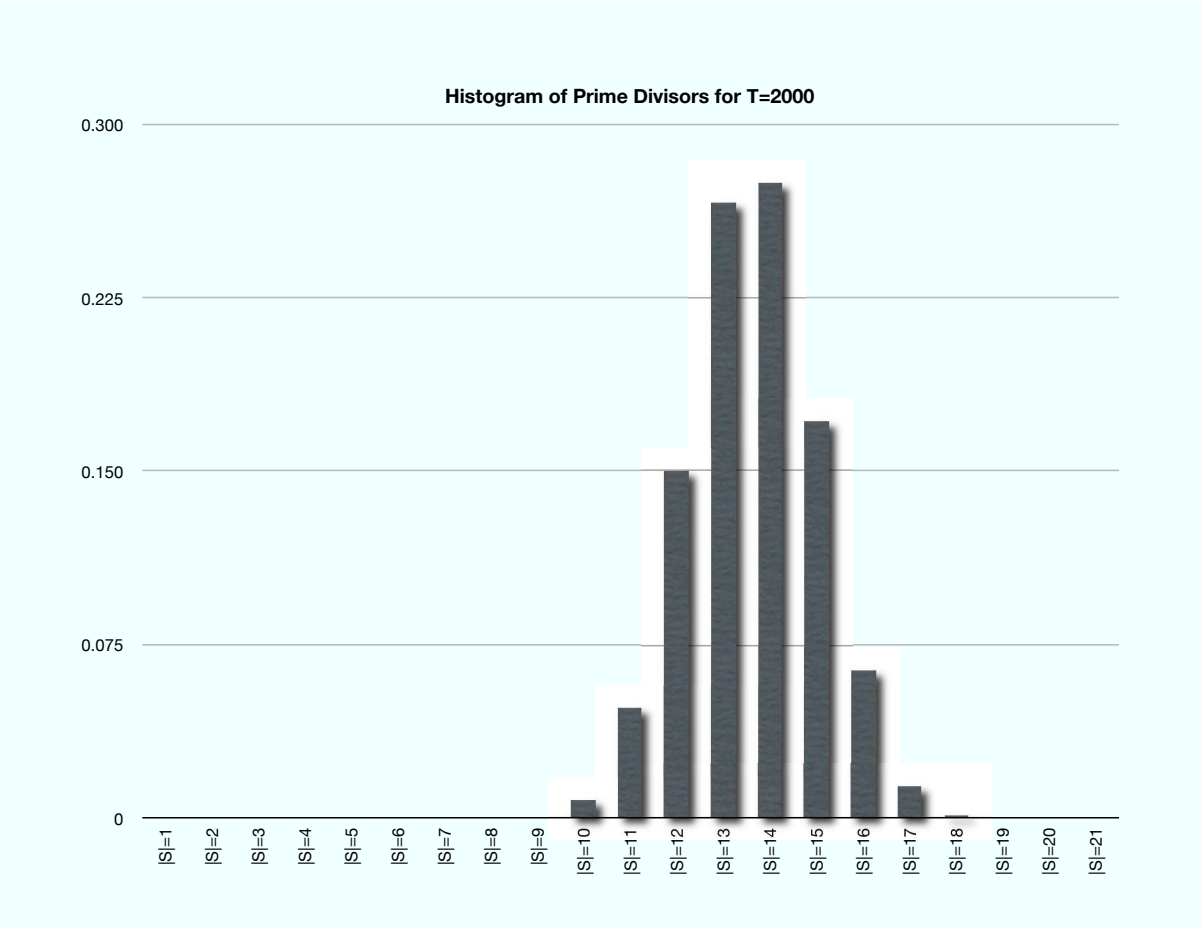
Bound T	1 000	2 000	3 000	4 000	5 000
$\lvert S\rvert = 5$	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
$\lvert S\rvert = 6$	5 (0.00%)	5 (0.00%)	5 (0.00%)	5 (0.00%)	5 (0.00%)
$\lvert S\rvert = 7$	10 (0.00%)	10 (0.00%)	10 (0.00%)	10 (0.00%)	10 (0.00%)
$\lvert S\rvert = 8$	50 (0.03%)	51 (0.00%)	51 (0.00%)	51 (0.00%)	51 (0.00%)
$\lvert S\rvert = 9$	350 (0.28%)	376 (0.07%)	387 (0.00%)	395 (0.00%)	402 (0.00%)
$\lvert S\rvert = 10$	2 785 (2.21%)	3 911 (0.78%)	4 711 (0.42%)	5 347 (0.27%)	5 936 (0.19%)
$\lvert S\rvert = 11$	12 516 (9.93%)	24 245 (4.81%)	34 988 (3.09%)	45 210 (2.24%)	55 080 (1.75%)
$\lvert S\rvert = 12$	29 273 (23.23%)	75 626 (15.01%)	127 228 (11.23%)	181 405 (9.00%)	238 278 (7.57%)
$\lvert S\rvert = 13$	38 331 (30.42%)	134 256 (26.64%)	260 702 (23.00%)	409 212 (20.31%)	575 506 (18.28%)
$\lvert S\rvert = 14$	28 128 (22.32%)	138 557 (27.50%)	316 659 (27.94%)	550 677 (27.33%)	833 793 (26.48%)
$\lvert S\rvert = 15$	11 614 (9.22%)	86 628 (17.19%)	239 260 (21.11%)	468 043 (23.23%)	768 019 (24.40%)
$\lvert S\rvert = 16$	2 669 (2.11%)	32 350 (6.42%)	111 905 (9.87%)	250 788 (12.45%)	453 719 (14.41%)
$\lvert S\rvert = 17$	261 (0.21%)	7 077 (1.40%)	31 754 (2.80%)	84 151 (4.18%)	171 012 (5.43%)
$\lvert S\rvert = 18$	9 (0.01%)	795 (0.16%)	5 236 (0.46%)	17 106 (0.85%)	40 222 (1.28%)
$\lvert S\rvert = 19$	1 (0.00%)	35 (0.01%)	457 (0.04%)	2 048 (0.04%)	5 768 (0.18%)
$\lvert S\rvert = 20$	0 (0.00%)	0 (0.00%)	10 (0.00%)	110 (0.01%)	389 (0.01%)

Data for Number of Bad Primes



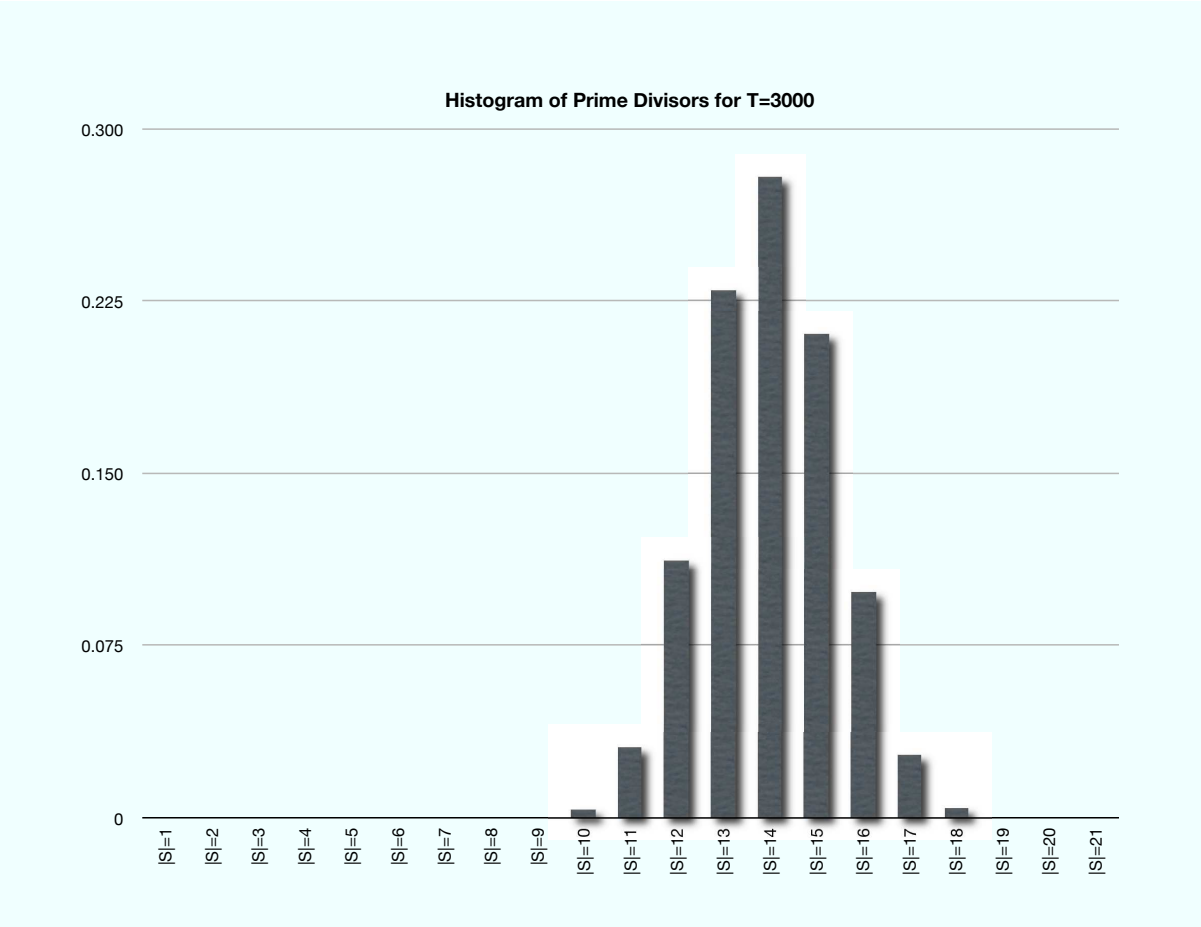
$|S(t)|$ for $T = 1\,000$ over $126\,003$ Curves

Data for Number of Bad Primes



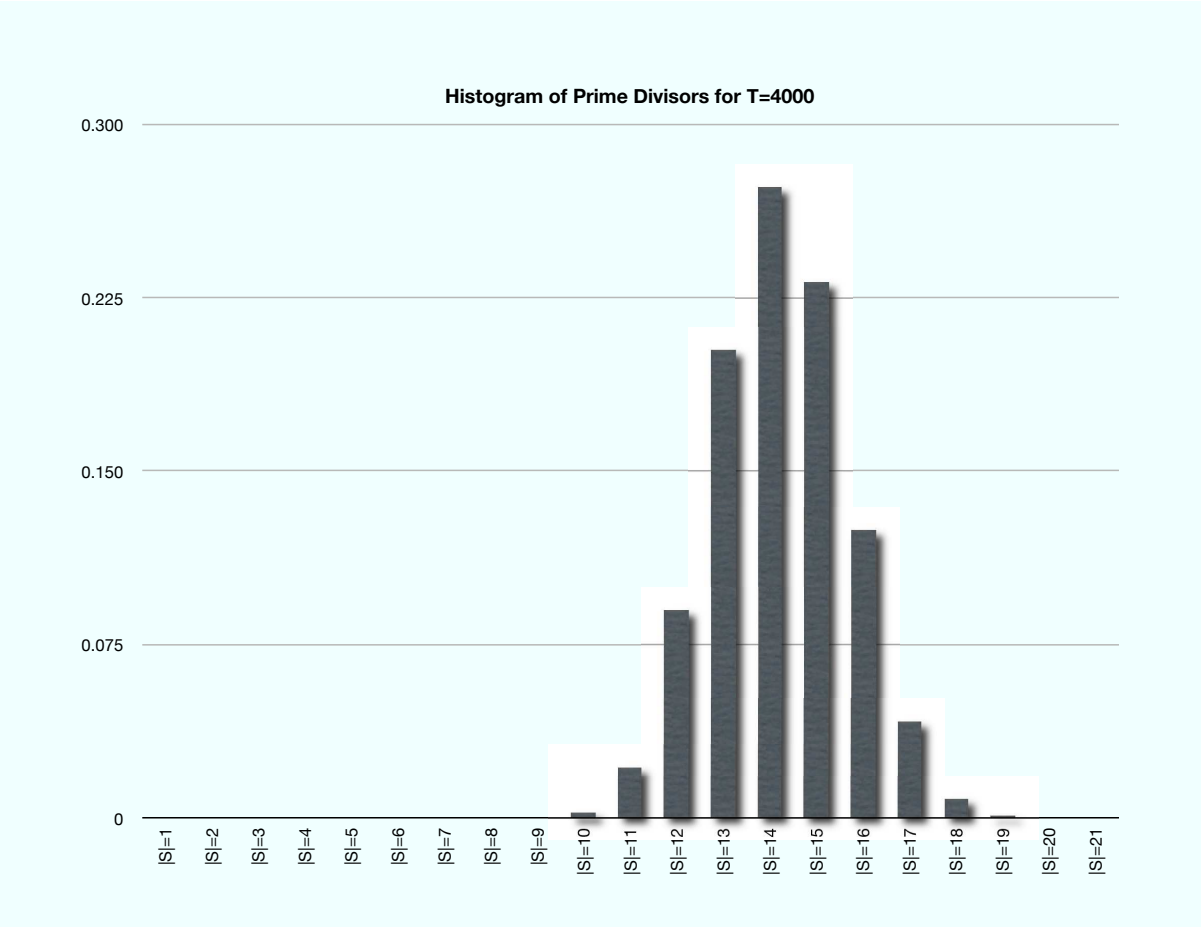
$|S(t)|$ for $T = 2\,000$ over $503\,923$ Curves

Data for Number of Bad Primes



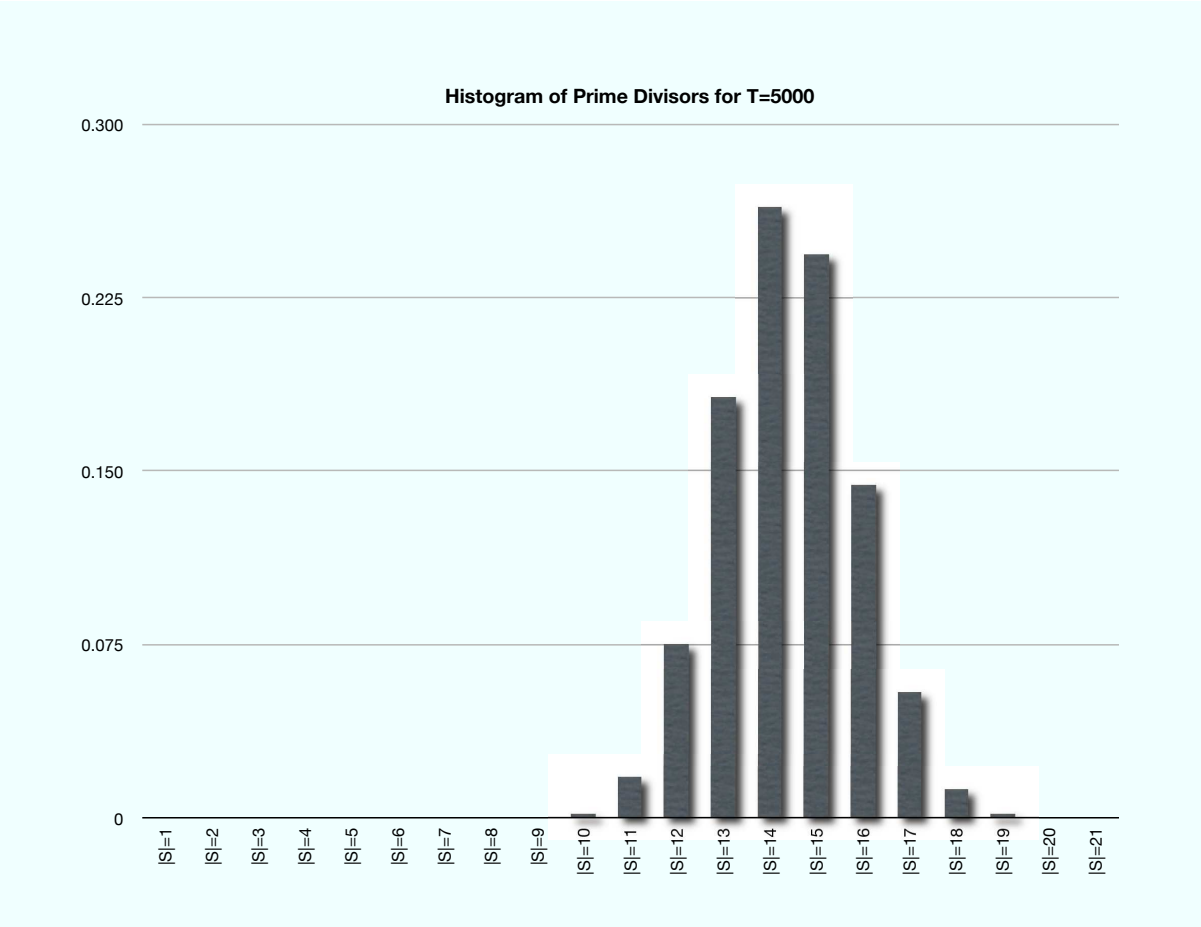
$|S(t)|$ for $T = 3\,000$ over $1\,133\,364$ Curves

Data for Number of Bad Primes



$|S(t)|$ for $T = 4\,000$ over $2\,014\,563$ Curves

Data for Number of Bad Primes



$|S(t)|$ for $T = 5\,000$ over $3\,148\,208$ Curves

Erdös-Kac for Elliptic Surfaces

Conjecture

Let $\mathcal{E}$ be that elliptic surface which classifies elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. The function $|S| : V \to \mathbb{Z}$ which counts the number of primes p occurring in the factorization of the discriminant $\Delta(E_t)$ of each fiber E_t is normally distributed.

To be more precise, upon defining the probability distribution

$$p_{\mathcal{E}}(T \,|\, \alpha, \beta) = \frac{1}{|W_T|} \left| \left\{ t \in W_T \;\middle|\; \alpha \leq \frac{|S(t)| - \log\log T}{\sqrt{\log\log T}} \leq \beta \right\} \right|$$

in terms of W_T defined above, we have the limit

$$\lim_{T \to \infty} \; p_{\mathcal{E}}(T \,|\, \alpha, \beta) = \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-z^2/2} \, dz.$$

Erdös-Kac for Elliptic Surfaces

Heuristic Proof: $S = S(t)$ is the number of primes which divide

$$N(a,b) = \left| a\,b\,(a^4 - b^4)\,(a^4 - 6\,a^2\,b^2 + b^4) \right|$$

This is bounded by $C_{\mathcal{E}}\,T^{10}$ on W_T.

Theorem (Paul Erdös and Mark Kac, 1940)

Let $\omega(N)$ denote the number of primes which divide N. Upon defining

$$p_{\mathbb{Z}}(T \,|\, \alpha,\, \beta) = \frac{1}{T} \left| \left\{ N \in \mathbb{Z} \;\middle|\; 0 < N \leq T,\ \alpha \leq \frac{\omega(N) - \log\log T}{\sqrt{\log\log T}} \leq \beta \right\} \right|$$

in terms of a positive $T \in \mathbb{Z}$, we have the limit

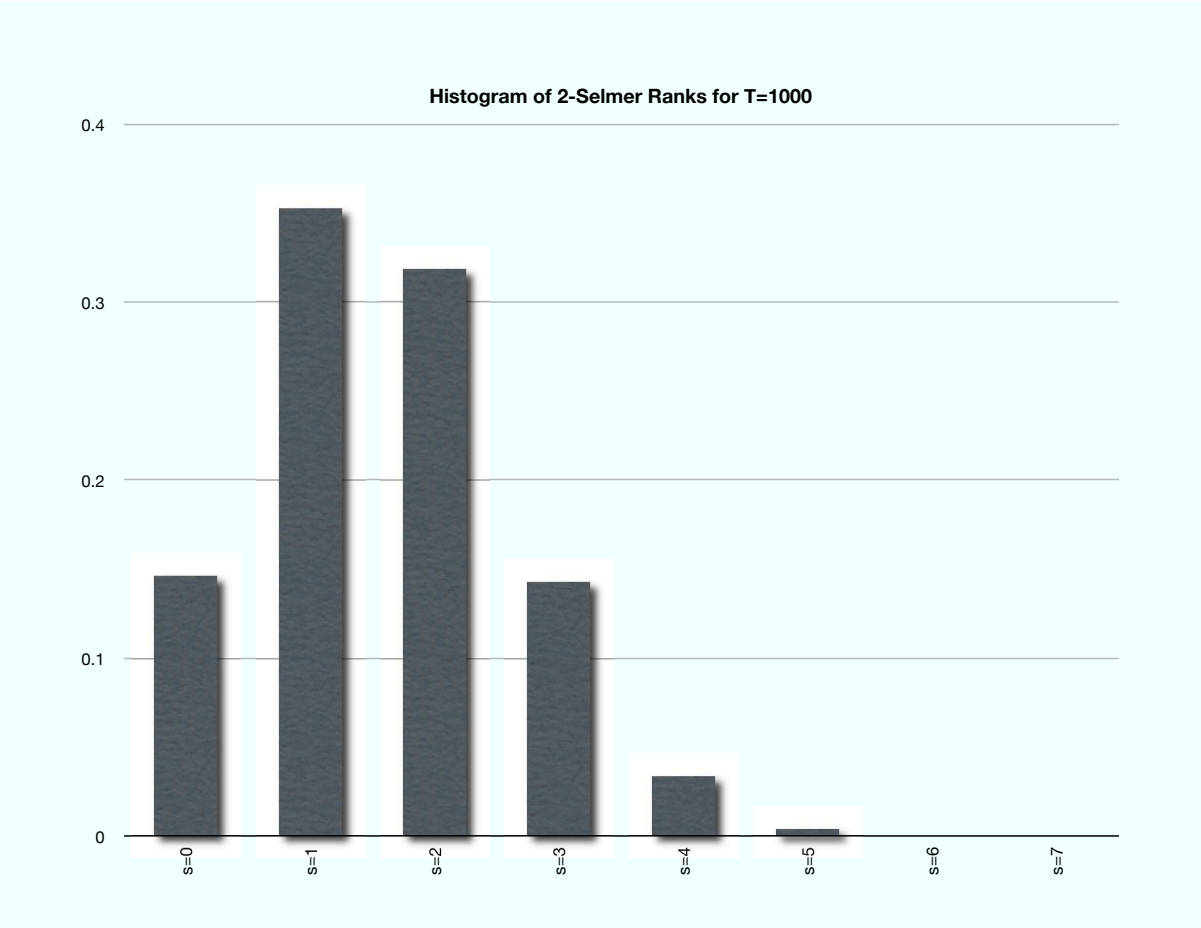
$$\lim_{T \to \infty} p_{\mathbb{Z}}(T \,|\, \alpha,\, \beta) = \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-z^2/2}\, dz.$$

$\omega(N) = |S(t)|$ when $N = N(a,b)$. One should be able to piece together the remainder of the details. □

2-Selmer Rank Data

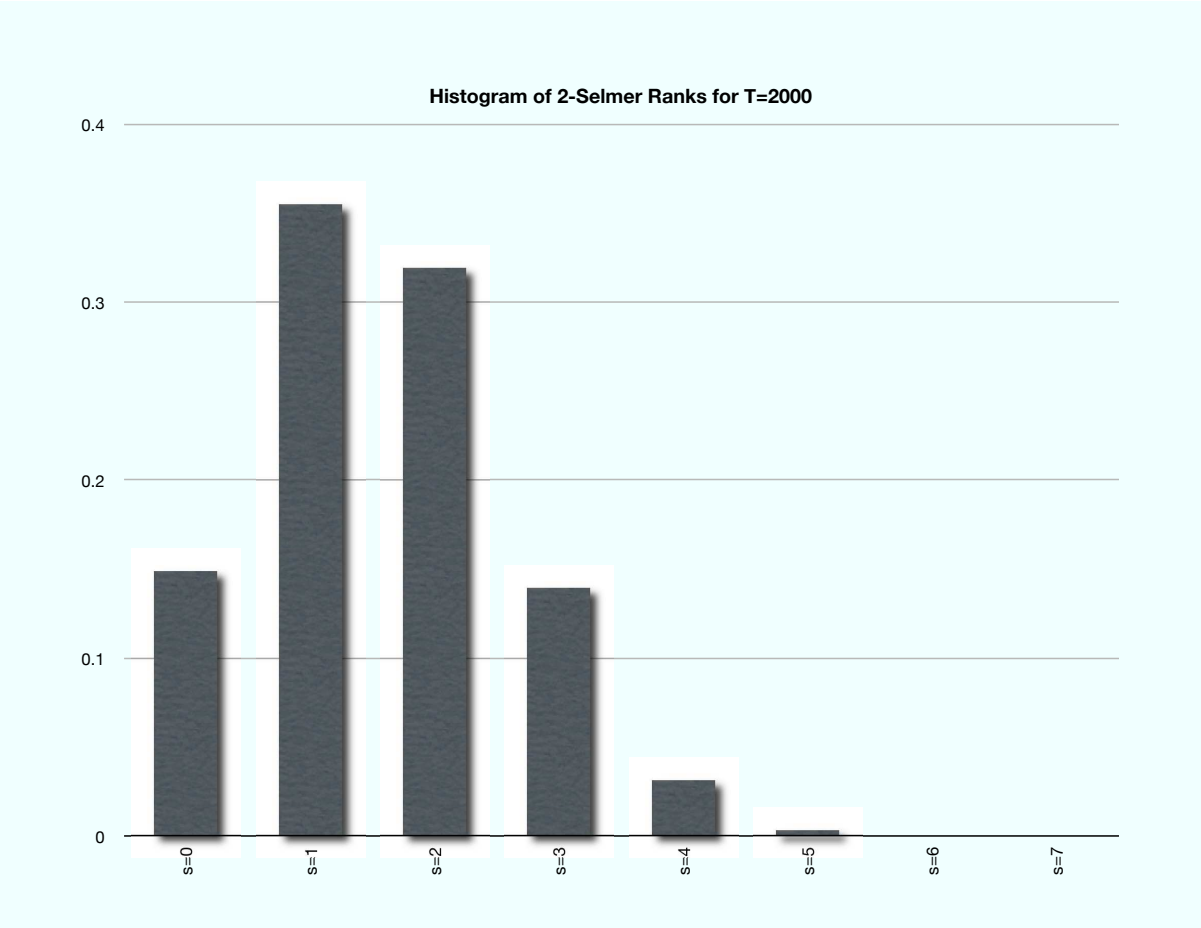
Bound T	1 000	2 000	3 000	4 000	5 000
$s = 0$	19 309 (15.32%)	75 384 (14.96%)	167 581 (14.79%)	296 135 (14.70%)	461 127 (14.65%)
$s = 1$	45 807 (36.35%)	179 361 (35.59%)	401 351 (35.41%)	711 392 (35.31%)	1 110 462 (35.27%)
$s = 2$	40 044 (31.75%)	161 031 (31.96%)	362 152 (31.95%)	643 340 (31.93%)	1 004 658 (31.91%)
$s = 3$	16 933 (13.44%)	70 481 (13.99%)	160 695 (14.18%)	287 682 (14.28%)	450 939 (14.32%)
$s = 4$	3 550 (2.82%)	15 845 (3.14%)	36 956 (3.26%)	67 289 (3.34%)	106 791 (3.39%)
$s = 5$	338 (0.27%)	1 707 (0.34%)	4 370 (0.39%)	8 208 (0.41%)	13 371 (0.42%)
$s = 6$	22 (0.02%)	112 (0.02%)	256 (0.02%)	509 (0.03%)	839 (0.03%)
$s = 7$	0 (0.00%)	2 (0.00%)	4 (0.00%)	8 (0.00%)	21 (0.00%)

Data for 2-Selmer Ranks



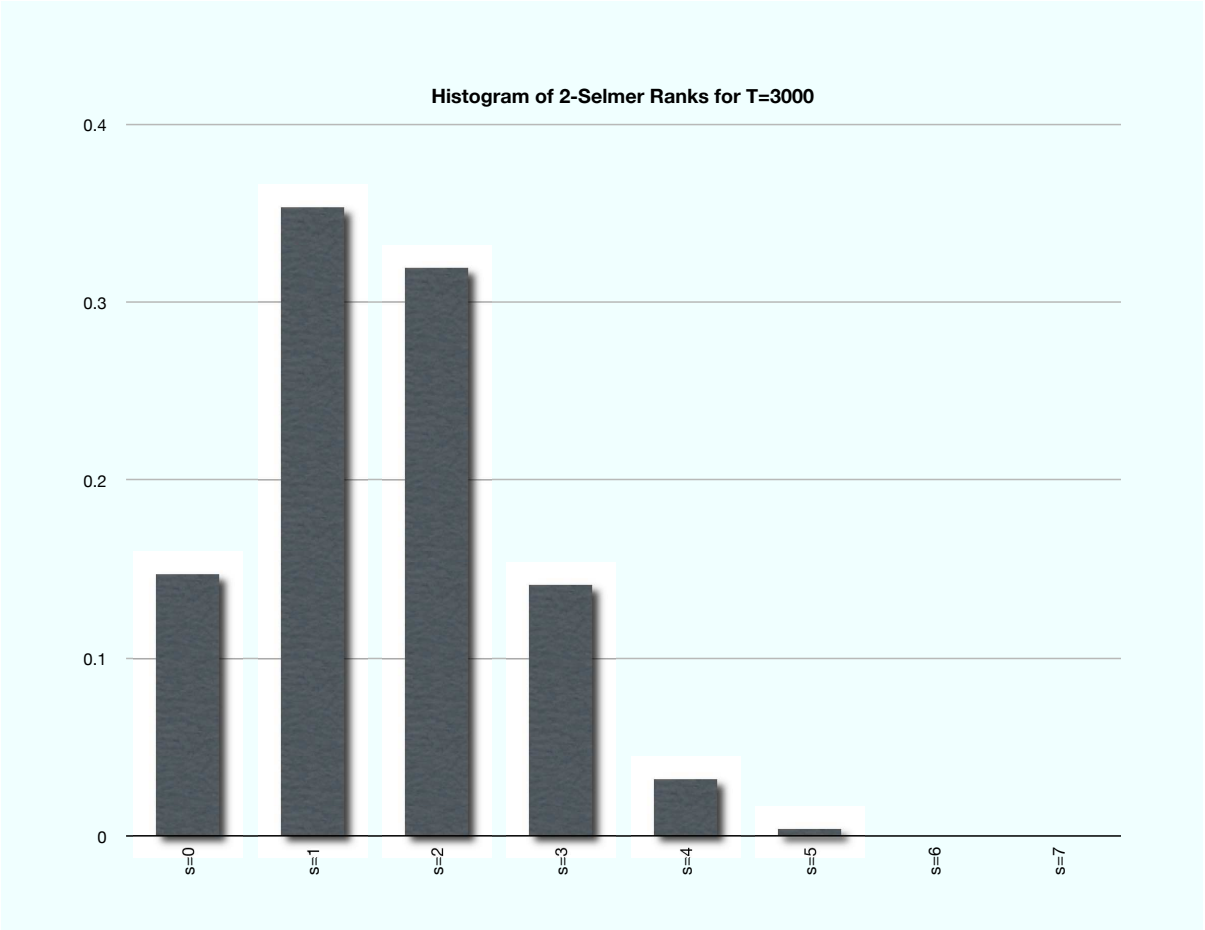
Ranks of 2-Selmer Groups for $T = 1\,000$ over $126\,003$ Curves

Data for 2-Selmer Ranks



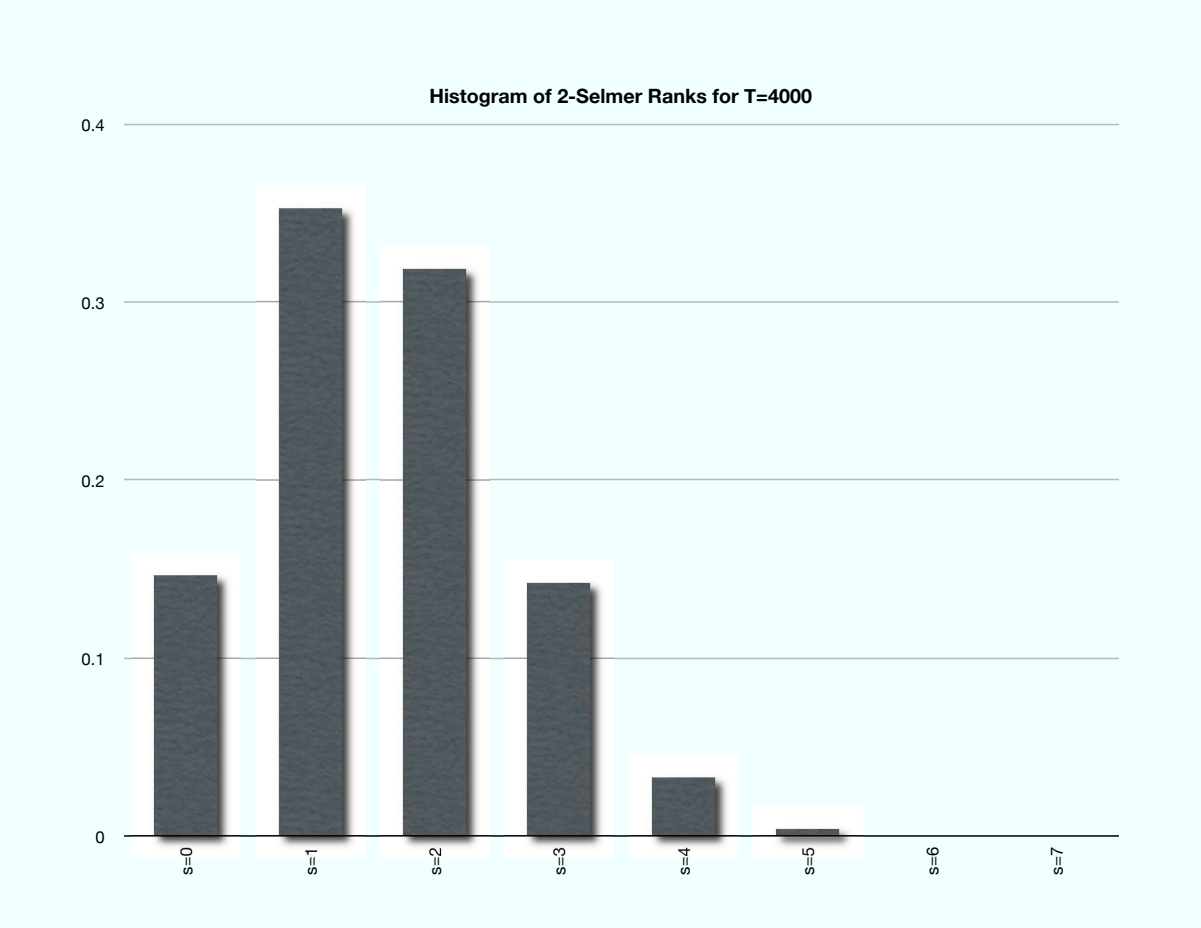
Ranks of 2-Selmer Groups for $T = 2\,000$ over $503\,923$ Curves

Data for 2-Selmer Ranks



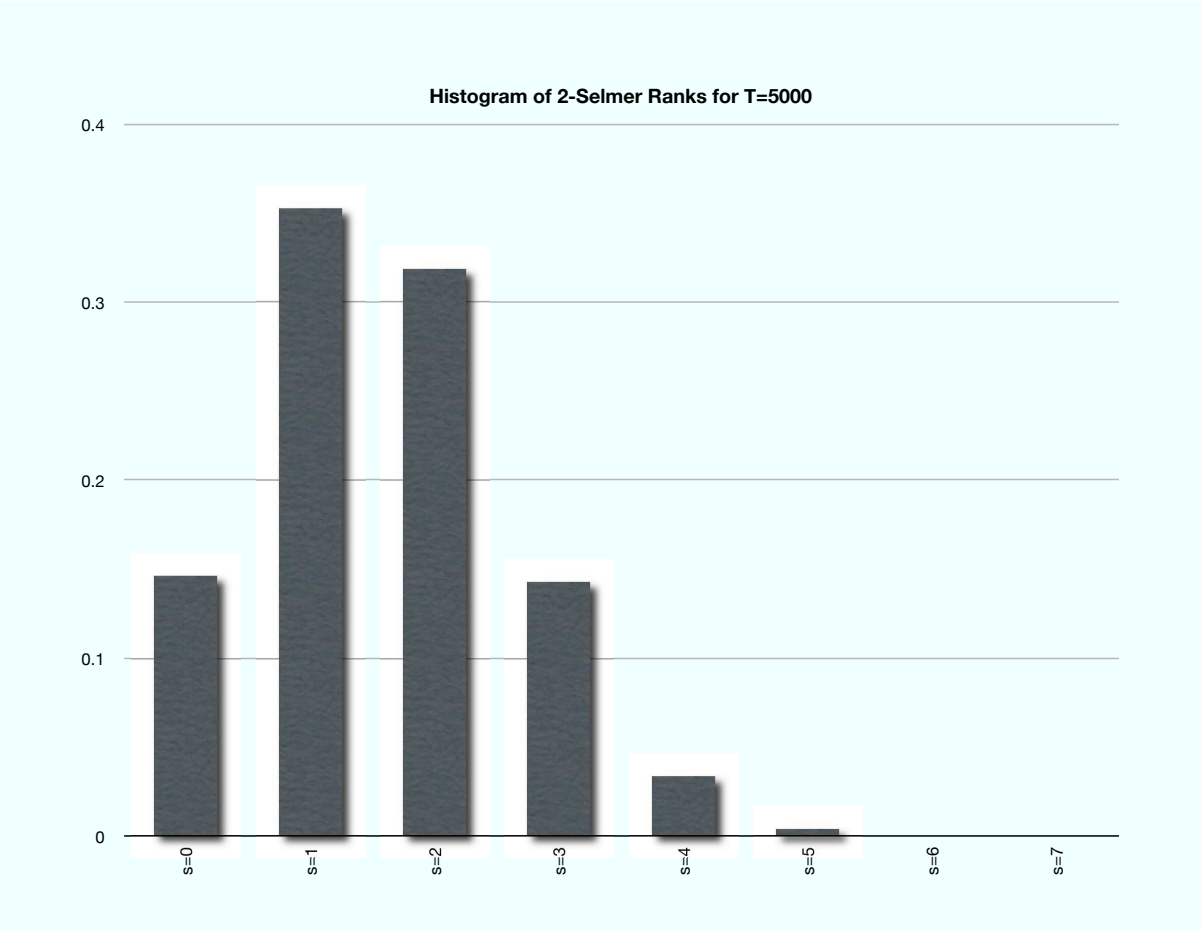
Ranks of 2-Selmer Groups for $T = 3\,000$ over $1\,133\,364$ Curves

Data for 2-Selmer Ranks



Ranks of 2-Selmer Groups for $T = 4\,000$ over $2\,014\,563$ Curves

Data for 2-Selmer Ranks



Ranks of 2-Selmer Groups for $T = 5\,000$ over $3\,148\,208$ Curves

Poisson Distributed?

The histograms appear to converge to a limit!

Conjecture

Let $\mathcal{E}$ be that elliptic surface which classifies elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. The function $s : V \to \mathbb{Z}$ which computes the 2-Selmer rank of each fiber E_t is not Poisson distrbuted.

To be more precise, there does not exist λ such that

$$\lim_{T\to\infty} \frac{\left|s^{-1}(x) \cap W_T\right|}{|W_T|} = e^{-\lambda}\frac{\lambda^x}{x!} \qquad \text{for each } x \in \mathbb{Z}.$$

Heuristic Proof: Consider the following generating function:

$$\Phi_s(z) = \sum_{x=0}^{\infty}\left[\lim_{T\to\infty} \frac{\left|s^{-1}(x) \cap W_T\right|}{|W_T|}\right] z^x, \qquad |z| \leq 1.$$

If s is Poisson, then $\Phi_s(z) = e^{\lambda(z-1)}$ for some λ. Hence $\Phi_s(-1) \neq 0$.

Poisson Distributed?

The expression $[\Phi_s(1) + (-1)^{\varepsilon}\Phi_s(-1)]/2$ corresponds to the probability that we find even (odd) 2-Selmer ranks by setting $\varepsilon = 0$ (1, respectively):

$$\sum_{x \equiv \varepsilon \pmod 2} \left[\lim_{T \to \infty} \frac{\left| s^{-1}(x) \cap W_T \right|}{|W_T|} \right] = \left\{ \begin{array}{c} \text{Probability that} \\ E_t \text{ has 2-Selmer rank} \\ s(t) \equiv \varepsilon \pmod 2 \end{array} \right\}.$$

Assuming $Ш(E/\mathbb{Q})$ is finite, we have $r \equiv s \pmod 2$:

$$\left\{ \begin{array}{c} \text{Probability that} \\ E_t \text{ has 2-Selmer rank} \\ s(t) \equiv \varepsilon \pmod 2 \end{array} \right\} = \left\{ \begin{array}{c} \text{Probability that} \\ E_t \text{ has Mordell-Weil rank} \\ r(t) \equiv \varepsilon \pmod 2 \end{array} \right\}.$$

Assuming the Birch and Swinnerton-Dyer Conjecture is true, the sign of the functional equation predicts the parity of the Mordell-Weil rank:

$$\left\{ \begin{array}{c} \text{Probability that} \\ E_t \text{ has Mordell-Weil rank} \\ r(t) \equiv \varepsilon \pmod 2 \end{array} \right\} = \left\{ \begin{array}{c} \text{Probability that} \\ E_t \text{ has root number} \\ W(E_t/\mathbb{Q}) = (-1)^{\varepsilon} \end{array} \right\}.$$

If this probability is $1/2$, we find the contradiction $\Phi_s(-1) = 0$. □

Global Minimal Model

Theorem (G, 2008)

Let $\mathcal{E}$ be that elliptic surface which classifies elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. Then each fiber E_t is a semistable elliptic curve having split multiplicative reduction at $\ell = 2$ and 3.

Proof: For $t = a/b$, denote the integers

$$p = \left(a^4 - 6\,a^2\,b^2 + b^4\right)/d \qquad A = -27\left(p^4 + 14\,p^2\,q^2 + q^4\right)$$

$$q = \left(a^2 + b^2\right)^2/d \qquad B = -54\left(p^6 - 33\,p^4\,q^2 - 33\,p^2\,q^4 + q^6\right)$$

with $d = 4^{\varepsilon}\gcd(a,b)^4$ chosen to make $p^2 \equiv q^2 \equiv 1 \pmod{48}$. Denote

$$X = 12^2\left(u + \frac{1}{12}\right) \qquad Y = 12^3\left(v + \frac{1}{2}\,u\right)$$

and

$$a_4 = \frac{A + 432}{12^4} \qquad a_6 = \frac{B + 12\,A + 1728}{12^6}$$

Then $E_t:\ Y^2 = X^3 + A\,X + B$ is equivalent to $v^2 + u\,v = u^3 + a_4\,u + a_6$.

Global Minimal Model

This curve has multiplicative reduction at all "bad" primes p.

$\ell = 2$: Both $a_4 \equiv a_6 \equiv 0 \pmod 2$, so E_t reduces to $v^2 + u\,v = u^3$ over $\mathbb{F}_2$. Hence E_t has split multiplicative reduction at this prime.

$\ell = 3$: Make the substitution

$$\begin{aligned} u &= \mu + \alpha \\ v &= \mu + \nu + \alpha \end{aligned} \qquad \text{in terms of} \qquad \alpha = \frac{1-p^2}{48} + \frac{1-q^2}{48}.$$

We have $a_4 \equiv \alpha \pmod 3$ and $a_6 \equiv \alpha^2 - \alpha^3 \pmod 3$, so E_t reduces to $\nu^2 = \mu^3 + \mu^2$ over $\mathbb{F}_3$. Hence E_t has split multiplicative reduction. □

Root Numbers

Theorem (David Rohrlich, 1996)

Let E be a semistable elliptic curve defined over $\mathbb{Q}$. Define root number $W(E/\mathbb{Q})$ as sign of the functional equation associated to E.

1. *The global root number can be expressed as a product of local root numbers:*
$$W(E/\mathbb{Q}) = \prod_{\ell} W(E/\mathbb{Q}_\ell).$$
2. *The local root numbers can be computed as follows:*
$$W(E/\mathbb{Q}_\ell) = \begin{cases} -1 & \text{if } \ell \text{ is a prime of split multiplicative reduction;} \\ +1 & \text{otherwise.} \end{cases}$$

Question: How is $W(E_t/\mathbb{Q})$ related to$(-1)^{|S(t)|}$?

New Curves of Rank 3

While we did not find any desired curves with Mordell-Weil rank $r = 4$, we did find three new elliptic curves E over $\mathbb{Q}$ with Mordell-Weil group

$$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$$

$$t = \frac{19}{84}: \quad Y^2 + XY = X^3 - 799729857585105059057812561 80\,X + 86224769524747474237043540868256843645764 00$$

$$t = \frac{101}{299}: \quad Y^2 + XY = X^3 - 977867541351362912053252014560183 00\,X + 619261854407125870378759391947293497741496443889 0000$$

$$t = \frac{86}{333}: \quad Y^2 + XY = X^3 - 250878395393474545316759183209311840250\,X + 1479979592022167493224960512910755689574299477808903560932$$

Questions?