Elliptic Curves and Convergence: Sato-Tate, GRH, and BSD

William Stein (joint work with Barry Mazur, with input from Andrew Granville,Chris Swierczewski and Tom Boothby)

2007-10-16

Purpose

Find a possible “next question to ask”, now that so much is understood about the Sato-Tate conjecture due to work of Taylor, Haris, et al.

More generally study the general notion of rate of convergence in the context of elliptic curves.

Hecke Eigenvalues

Let E be a **non-CM** elliptic curve over $\mathbb{Q}$, and

$$a_p = p + 1 - \#E(\mathbf{F}_p).$$

Theorem (Hasse): $-1 < \frac{a_p}{2\sqrt{p}} < 1.$

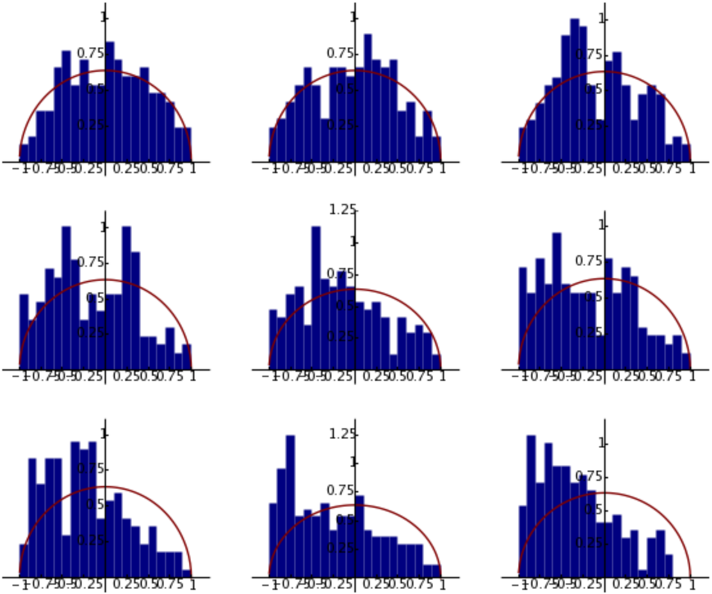
Sato and Tate: How are these numbers distributed? A conjecture...

Convergence to the semicircle distribution

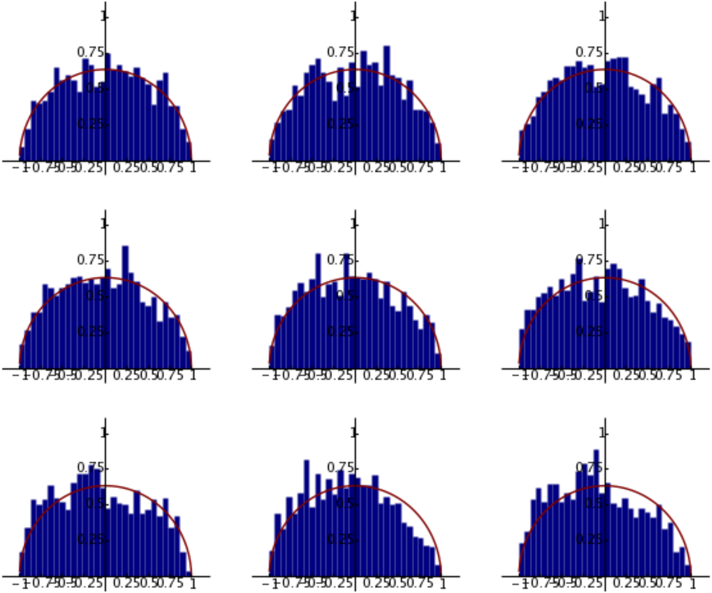
The following slides each contain 8 plots. Each plot displays the distribution of normalized a_p for the lowest conductor elliptic curves of different rank and all a_p for $p < C$, for $C = 10^3, 10^4, 10^5, 10^6$.

Rank 0	Rank 1	Rank 2
Rank 3	Rank 4	Rank 5
Rank 6	Rank 7	Rank 8

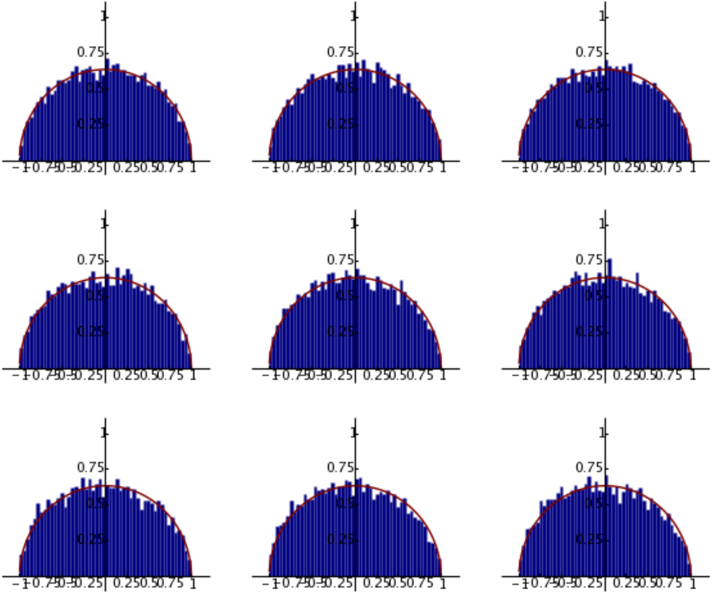
Sato-Tate Frequency Histograms: $C = 10^3$



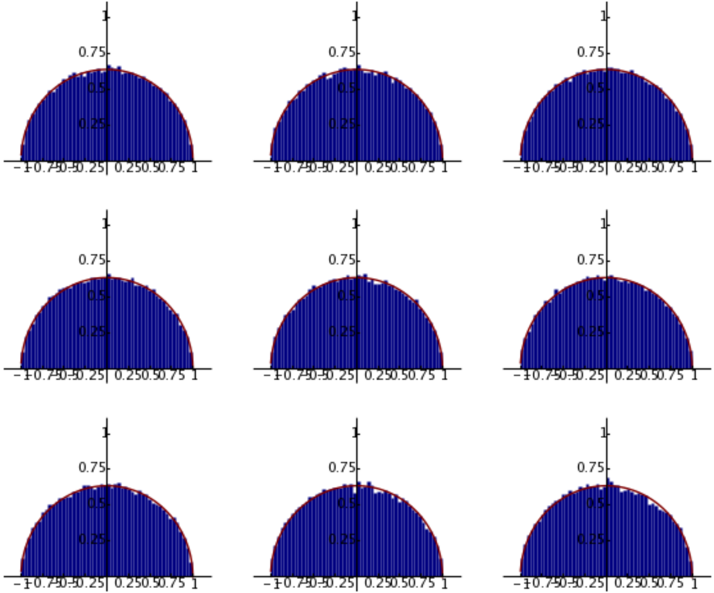
Sato-Tate Frequence Histograms: $C = 10^4$



Sato-Tate Frequence Histograms: $C = 10^5$



Sato-Tate Frequence Histograms: $C = 10^6$



Quantify the convergence?

Barry Mazur: “How can we precisely quantify the convergence of the blue data to the red semicircle theoretical distribution?”

Some Functions (copy on blackboard)

E an elliptic curve; $a_p = p + 1 - \#E(\mathbf{F}_p)$

- $X(T) = \dfrac{\int_{-1}^{T} \sqrt{1-x^2}dx}{\int_{-1}^{1} \sqrt{1-x^2}dx} =$ area under arc of semicircle
- $Y_C(T) = \dfrac{\#\left\{\text{primes } p < C : -1 < \frac{a_p}{2\sqrt{p}} < T\right\}}{\#\left\{\text{primes } p < C\right\}}$.
- $\Delta(C) = \sqrt{\int_{-1}^{1}(X(T) - Y_C(T))^2 dT} =$ the L_2-norm of the difference of $X(T)$ and $Y_C(T)$, and $\Delta(C)_\infty$ the L_∞-norm.

The Sato-Tate Conjecture

Let $\Delta(C)_\infty$ be the max of the difference between the theoretical semicircle distribution and actual data using primes up to C.

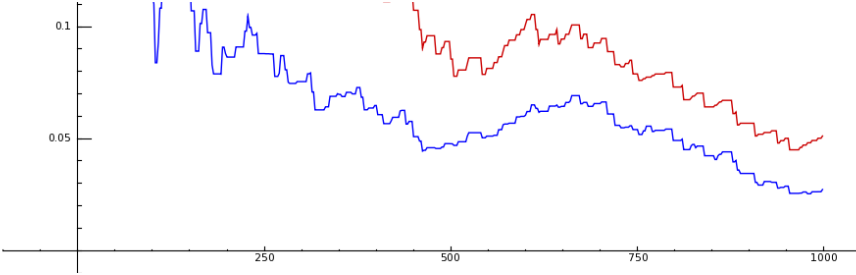
Sato-Tate Conjecture:

$$\lim_{C \to \infty} \Delta(C)_\infty = 0$$

Theorem (Taylor, M. Harris, et al.): If E has multiplicative reduction at some prime, then the Sato-Tate conjecture is true. [Key part of proof is to establish certain analytic properties of symmetric power L-functions.]

Plotting Δ (up to 10^3)

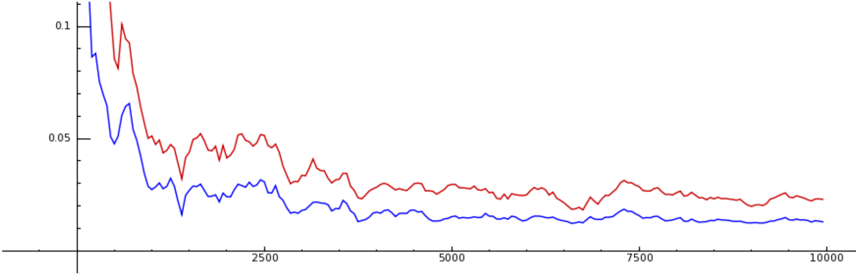
```
sage: e37a = SatoTate(EllipticCurve('37a'), 10^6)
sage: show(e37a.plot_Delta(10^3, plot_points=400,
 max_points=100), ymax=0.1, ymin=0, figsize=[10,3])
```



The red line is $\Delta(C)_\infty$ and the blue line is $\Delta(C)$. By Sato-Tate, they both go to 0 as $C \to \infty$.

Plotting Δ (up to 10^4)

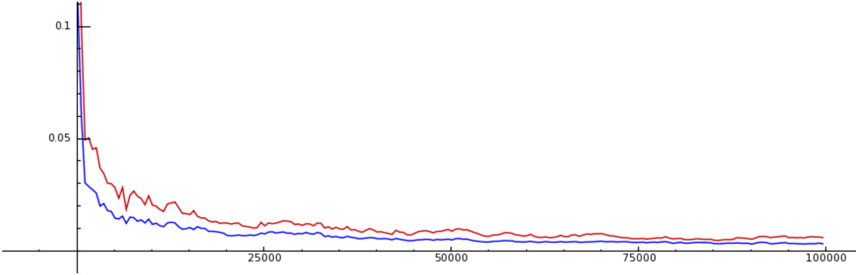
```
sage: e37a = SatoTate(EllipticCurve('37a'), 10^6)
sage: show(e37a.plot_Delta(10^4, plot_points=200,
 max_points=100), ymax=0.1, ymin=0, figsize=[10,3])
```



The red line is $\Delta(C)_\infty$ and the blue line is $\Delta(C)$. By Sato-Tate, they both go to 0 as $C \to \infty$.

Plotting Δ (up to 10^5)

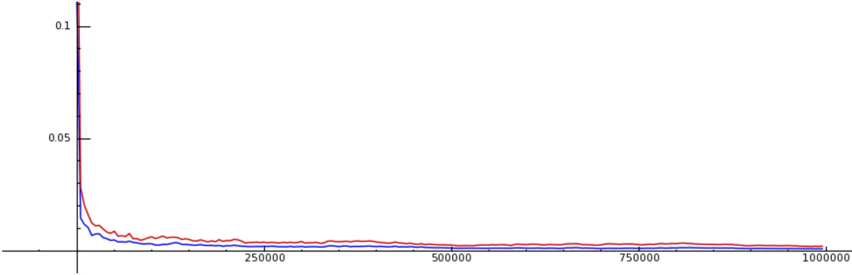
```
sage: e37a = SatoTate(EllipticCurve('37a'), 10^6)
sage: show(e37a.plot_Delta(10^5, plot_points=200,
 max_points=100), ymax=0.1, ymin=0, figsize=[10,3])
```



The red line is $\Delta(C)_\infty$ and the blue line is $\Delta(C)$. By Sato-Tate, they both go to 0 as $C \to \infty$.

Plotting Δ (up to 10^6)

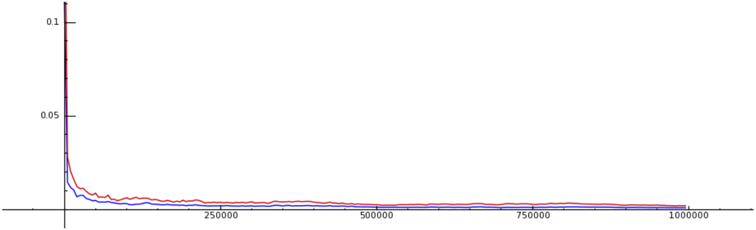
```
sage: e37a = SatoTate(EllipticCurve(’37a’), 10^6)
sage: show(e37a.plot_Delta(10^6, plot_points=200,
 max_points=100), ymax=0.1, ymin=0, figsize=[10,3])
```



The red line is $\Delta(C)_\infty$ and the blue line is $\Delta(C)$. By Sato-Tate, they both go to 0 as $C \to \infty$.

“The next question to ask...”

QUESTION: What about the speed of convergence? I.e., *how* does $\Delta(C)$ or $\Delta(C)_\infty$ converge to 0?



The Akiyama-Tanigawa Conjecture

Conjecture (Akiyama-Tanigawa [Math Comp., 1999]): For every $\epsilon > 0$, for $C \gg 0$ we have

$$\Delta(C)_\infty \leqslant \frac{1}{C^{1/2-\epsilon}}.$$

Theorem (A-T): This conjecture implies the Generalized Riemann Hypothesis for $L(E, s)$.

See Barry Mazur's forthcoming Notices paper for more discussion, references, and pretty pictures.

Converse

Possibly GRH implies the above conjecture:

From: Shigeki Akiyama <akiyama@math.sc.niigata-u.ac.jp>
Date: Sun, 30 Sep 2007 08:17:02 +0900
Dear Professor Mazur

I feel very honored to have your comments on our old experimental paper. I was very pleased to read your expository paper itself, of course including subsections you wrote us. I did not consider the error term problem in this comprehensive manner,

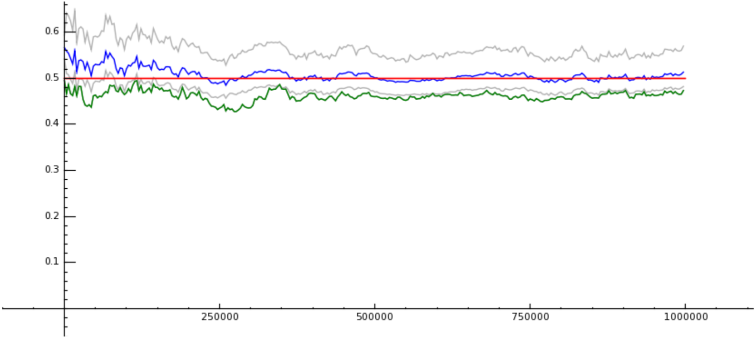
My only comment is that a partial converse is true. If we assume Riemann hypothesis for all symmetric L, then the conjecture is valid for L_{0,1}. This is a claim from H. Nagoshi and basically comes from Erdos-Turan inequility as far as I remember... We did not explore nor publish this observation.

Log Plots

Let's test out Akiyama-Tanigawa, instead of plotting $\Delta(C)$ which just goes to 0 quickly, we instead plot $-\log_C(\Delta(C))$.

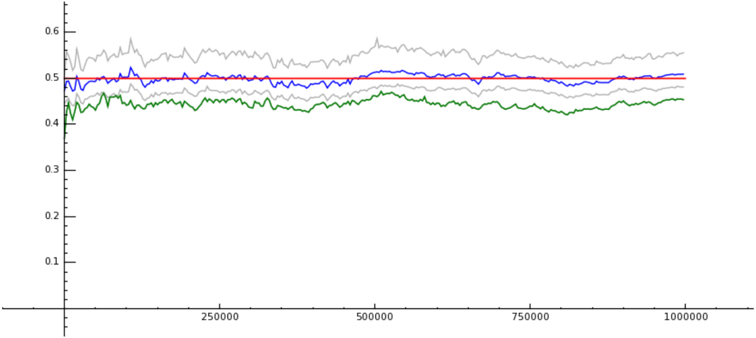
1. How does this function compare to $\dfrac{1}{2}$? I.e., does it eventually get within ϵ of $\frac{1}{2}$.
2. Can we find a simple function that conjecturally nicely approximates $-\log_C(\Delta(C))$?

Rank 0 curve 11a; $p < 10^6$; with 300 sample points



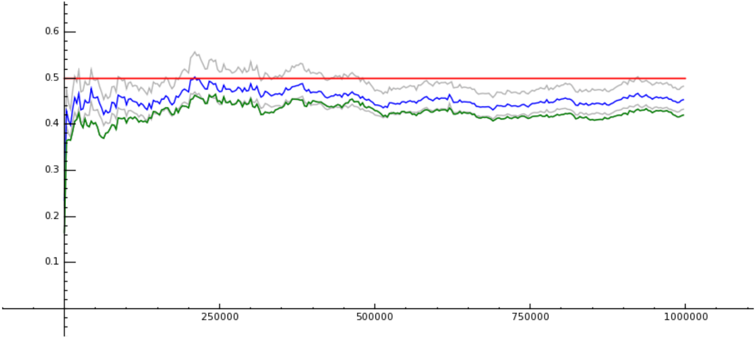
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 1 curve 37a; $p < 10^6$



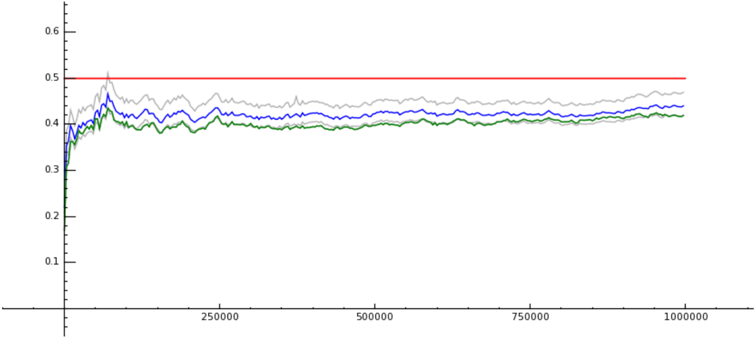
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 2 curve 389a; $p < 10^6$



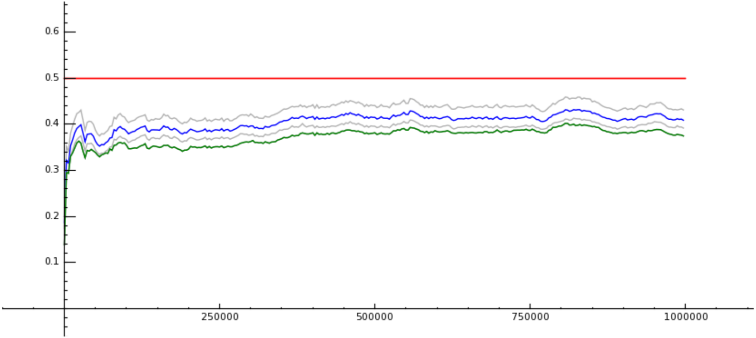
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 3 curve 5077a; $p < 10^6$



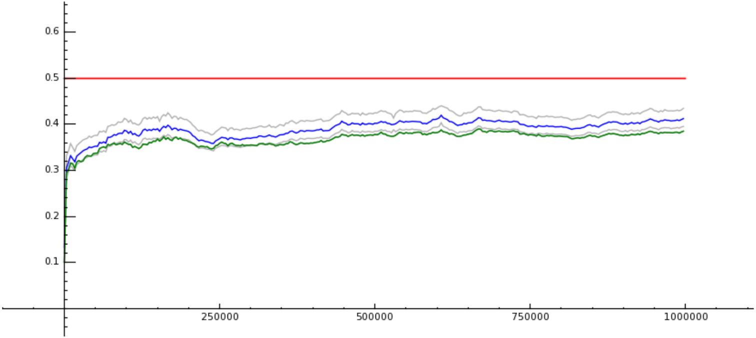
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 4 curve [1,-1,0,-79,289]; $p < 10^6$



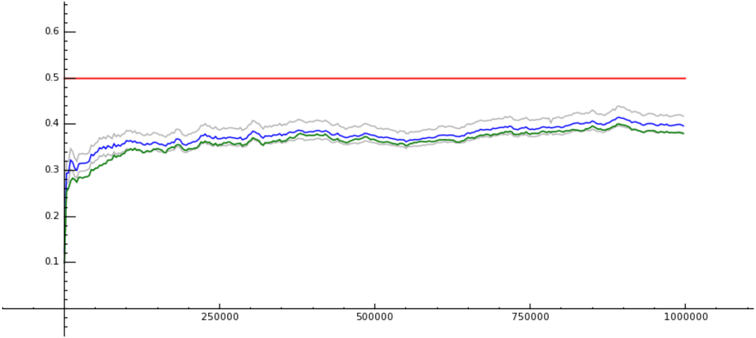
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 5 curve [0, 0, 1, -79, 342]; $p < 10^6$



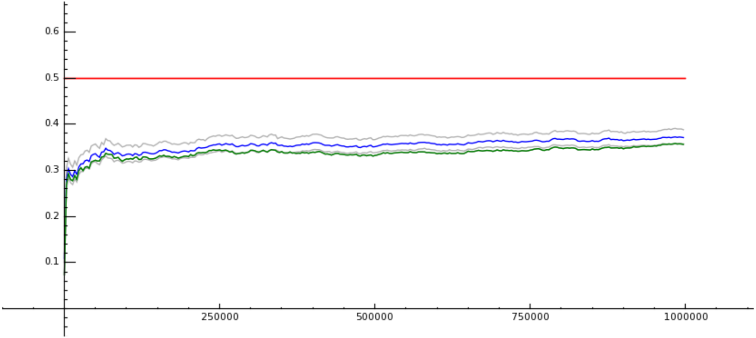
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 6 curve [1, 1, 0, -2582, 48720]; $p < 10^6$



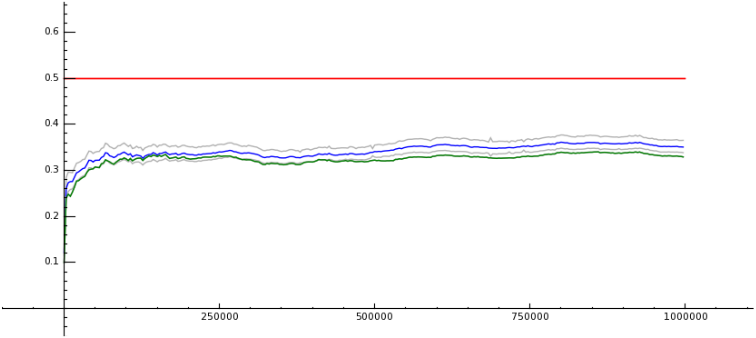
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 7 curve [0, 0, 0, -10012, 346900]; $p < 10^6$



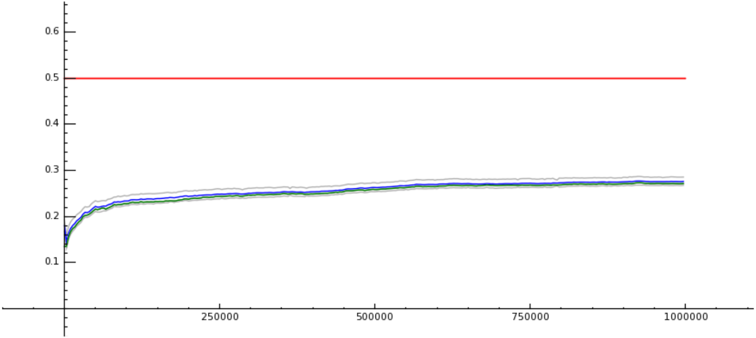
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Rank 8 curve [0, 0, 1, -23737, 960366]; $p < 10^6$



- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

Elkies rank $\geqslant 28$ curve; $p < 10^6$



- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Red line is $1/2$.

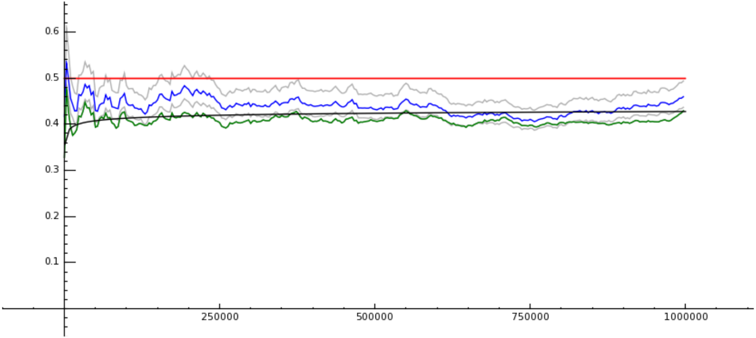
OK, are those lines really going up to $1/2$???

Understanding the Data Better?

Can one predict the asymptotic shape of the curve $\Delta(C)$, say, in terms of either arithmetic invariants of the curve or perhaps in terms of zeros of $L(E, s)$ on the critical strip?

For some curves $\Delta(C)$ is quickly very close to $1/2$, e.g., the curves of rank 0 and 1 above.

Fitting the “random” Rank 0 curve $y^2 = x^3 + 19x + 234$



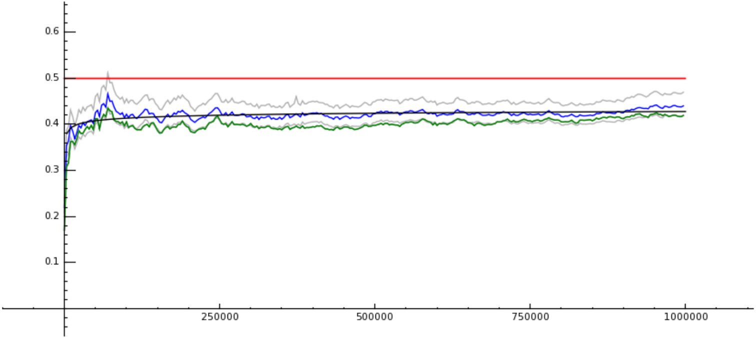
- The black curve is
$$\frac{1}{2} - \frac{1}{\log(X)}.$$
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.
- Conductor = 24093568 $= 2^7 \cdot 41 \cdot 4591$

Low zeros?

```
sage: EllipticCurve('11a').Lseries_zeros(10)
[6.36261389, 8.60353962, 10.0355091,
 11.4512586, 13.5686391, 15.9140726,
 17.0336103, 17.9414336, 19.1857250,
 20.3792605]
```

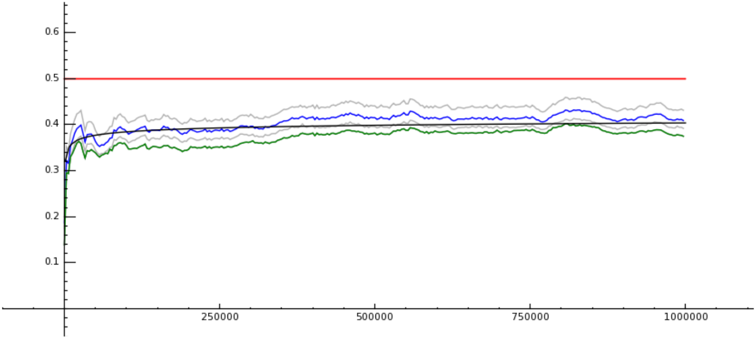
```
sage: EllipticCurve([19,234]).Lseries_zeros(10)
[0.255961213, 0.739839807, 1.03144159,
 1.78804887, 2.11227980, 2.42762599,
 3.11102036, 3.26810134, 3.68155235,
 4.13888170]
```

Fitting the Rank 3 Curve 5077a



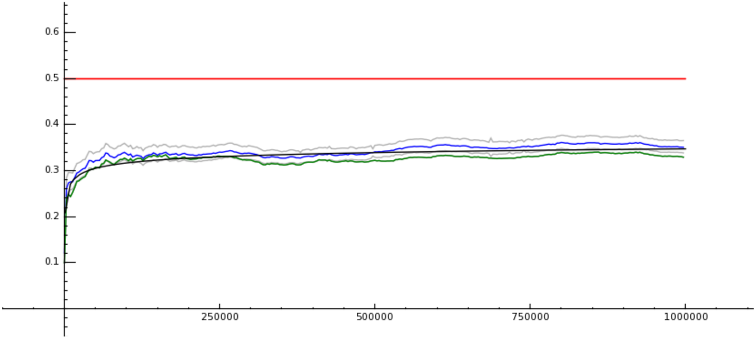
- The black curve is
$$\frac{1}{2} - \frac{3/3}{\log(X)}.$$
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.

Fitting the Rank 4 [1,-1,0,-79,289]; $p < 10^6$



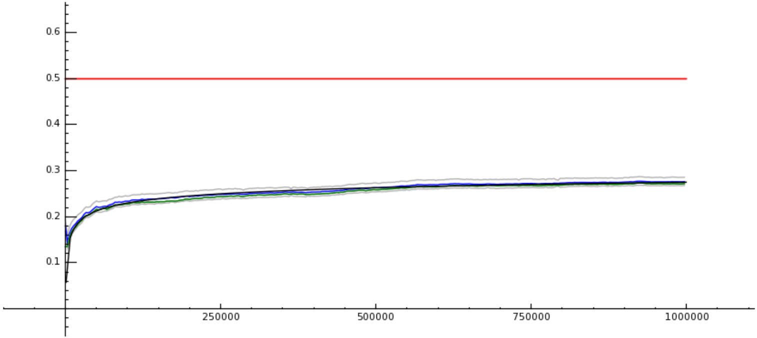
- The black curve is
$$\frac{1}{2} - \frac{4/3}{\log(X)}.$$
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.

Fitting Rank 8 [0, 0, 1, -23737, 960366]; $p < 10^6$



- The black curve is
$$\frac{1}{2} - \frac{19/9}{\log(X)}.$$
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.

Fitting Rank 28 curve; $p < 10^6$



- The black curve is
$$\frac{1}{2} - \frac{28/9}{\log(X)}.$$
- Green line is $-\log_C(\Delta(C)_\infty)$.
- Blue line is $-\log_C(\Delta(C))$, with a grey tubular *numerical integration error bound*.

Conjectural convergence of the measure of convergence

Conjecture (Stein): For any E there is a constant α such that

$$-\log_C(\Delta(C)) \geqslant \frac{1}{2} - \frac{\alpha}{\log(C)}$$

for all C.

For comparison, recall the Akiyama-Tanigawa conjecture asserts that for all $\epsilon > 0$, we have that

$$\Delta(C) \leqslant O\left(\frac{1}{C^{1/2-\epsilon}}\right)$$

Equivalently,

$$-\log_C(\Delta(C)) \gg 1/2 - \epsilon$$

The Sato-Tate convergence parameter

For an elliptic curve E let $\alpha(C)$ be the infimum of all constants that minimizes the L_2 norm of this (i.e. the distance between the black and blue curves above!):

$$-\log_C(\Delta(C)) - \left(\frac{1}{2} - \frac{\alpha(C)}{\log(C)}\right).$$

Thus $\alpha(C)$ is a function of C (and the fixed curve E).

Definition: The *Sate-Tate convergence parameter* of E is

$$\alpha_E = \lim_{C\to\infty} \alpha(C).$$

(I don't know if this exists. replace by limsup and liminf?)

Challenge: Find a conjectural formula for k_E in terms the critical zeros of $L(E,s)$?

Another future direction...

We have

$$X^{1/2-1/\log(X)} = \frac{X^{1/2}}{X^{1/\log(X)}} = e \cdot X^{1/2}.$$

We thus entertain the possibility (following the format of the people who work with random matrices etc.) that the true distribution is well approximated by something like

$$a \cdot (\log X)^b \cdot X^c$$

for appropriate constants a, b, c.
So for the rank 3 example above we might choose

$$a = e, \qquad b = 0, \qquad c = 1/2,$$

but there may be better choices?

More future direction...

1. Restrict to intervals $[a, b] \subset (-1, 1)$. (This seems to have little to know impact.)

2. Push computations much further (next slide).

Pushing Computations Further

1. Drew Sutherland (of MIT) has some amazingly fast *parallel* C code for computing all a_p for $p < C$ quickly (and much much more – over 20,000 lines of new (pure) C code.
2. On sage.math his code computes all a_p for $p < C = 10^7$ in less than 5 seconds!
3. For comparison, $C = 10^7$ takes Sage (via PARI) 94 seconds and Magma (via M Watkins' code) 81.25 seconds (on sage.math, a 16-core opteron 246.).
4. Drew: "My guess then is that on an idle system it would take about 5 minutes to do p to 10^9."

GRH, BSD, and Convergence

A related idea that Barry Mazur and I came up with recently:

1. Let E be an elliptic curve over $\mathbb{Q}$.
2. Construct a step function like $\pi(X)$, but associated to E, so each step is weighted by a_p.
3. Construct an associated step function $\Psi(X)$ with steps at the prime powers. The *distribution* $\Psi'(X)$ has support at (most at) the prime powers.
4. Consider the distribution $\Phi(t) = \Psi'(e^t)/e^{t/2}$.
5. It's Fourier transform is $F(s) = \sum a_{p^n} p^n \log(p) \cos(ns \log(p))$.
6. GRH: The distribution $F(s)$ is discrete with support at the imaginary parts of the nontrivial zeros of $L(E, s)$.
7. In particular, F has a δ function at 0 exactly if E has positive analytic rank, i.e., $r_{E,\mathrm{an}} > 0$.
8. So study the rate of *divergence* of the sum

$$F(0) = \sum \frac{a_{p^n}}{p^n} \log(p).$$

A Numerical Experiment

Let

$$R_E(C) = \sum_{p^n \leqslant C} \frac{a_{p^n}}{p^n} \log(p).$$

Guess: $R_E(C) \sim \alpha \log(C)^{\beta}$, where β depends only on the rank of E and α depends on the arithmetic invariants of E.

Experiment: Compute $\log(R_E(C))/\log(\log(C))$. Does this depend only on rank of E?

Next we give some data. In each case I give several curves with a given rank, along with the value of the above quantity for $C = 10^6$:

```
curve     rank          log(R_E(C)) / log(log(C)) fo
37a1          1            0.622551283326
43a1          1            0.664628966956
53a1          1             0.64056834932
57a1          1            0.743607790253
58a1          1            0.639927175062
61a1          1            0.776549775927
65a1          1            0.717652219993

389a1         2             1.00758391471
433a1         2            0.988605592917
446d1         2              1.0273311084
563a1         2            0.987041109677
571b1         2            0.919099487872
643a1         2            0.889281143176
655a1         2            0.925749865705
664a1         2            0.957156816404
```

curve	rank	log(R_E(C)) / log(log(C)) fo
5077a1	3	1.16071903587
11197a1	3	1.14902783005
11642a1	3	1.16976814614
12279a1	3	1.13108926023
13766a1	3	1.14886584781
16811a1	3	1.04598722161
18097b1	3	1.13427759105
18562c1	3	1.12453834551
234446a1	4	1.20905312451
19047851a1	5	1.29409998755
5187563742a1	6	1.34691224576

Because of the log-log's, etc., I'm probably getting 2 digits correct above usually, from the huge sum. In pictures though, the lines are quickly fairly horizontal (so the true limit is likely close to the above numbers).

The striking thing about the above clumps of numbers (for each rank), is they all lie in disjoint intervals.