A Statistical Analysis of 2-Selmer Groups for Elliptic Curves with Prescribed Torsion

A. Rollick[1] J. Weigandt[2]

[1]Department of Mathematics
John Carroll University

[2]Department of Mathematics
Purdue University

Summer Undergraduate Mathematical Sciences Research Institute 2007

Outline

- Family of Elliptic Curves with $E(\mathbb{Q})_{tors} \simeq Z_2 \times Z_8$
  - The 2-Selmer Group
- Computations
  - `mwrank`
  - Algorithm
- Distribution of 2-Selmer Ranks
  - Poisson Distribution?
  - Generating Functions

Introduction

- We are attempting to find Mordell-Weil rank r of elliptic curves
- An upper bound for the rank is s, the rank of the 2-Selmer group of the elliptic curve
- $E(\mathbb{Q})$ may be infinite group
- Instead consider $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}$, which is a finite group

Connecting Homomorphism

Let E be a curve such that:

- is defined by $Y^2 = X^3 + A\,X + B$ where A and $B \in \mathbb{Z}$
- $X^3 + A\,X + B$ has three distinct rational roots: $e_1,\ e_2,\ e_3$

Then we have the "connecting homomorphism":

$$\delta_E : \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \qquad P = (X, Y) \mapsto (X - e_1, X - e_2)$$

δ_E is injective and its image lies in a finite group

$$G = \left\{ (d_1,\ d_2) \;\middle|\; \begin{array}{c} d_i = \pm \ell_1^{a_{i1}} \cdots \ell_r^{a_{ir}}, \text{ where} \\ \ell_j \text{ divides } -16(4\,A^3 + 27\,B^2) \end{array} \right\}$$

Counting Rational Points

For $(d_1, d_2) \in G$ consider the curve

$$C_d : \quad d_1 u^2 - d_2 v^2 = e_2 - e_1, \quad d_1 u^2 - d_1 d_2 w^2 = e_3 - e_1.$$

Then the connecting homomorphism implies the isomorphism

$$\frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq \left\{ d \in G \,\middle|\, C_d(\mathbb{Q}) \neq \emptyset \right\} \simeq {Z_2}^{r+2}.$$

That is, if $(u, v, w) \in C_d(\mathbb{Q})$ then $(d_1\, u^2 + e_1,\ d_1\, d_2\, u\, v\, w)$ in $E(\mathbb{Q})$. Conversely, if $P \in E(\mathbb{Q})$ then there is a point in $C_d(\mathbb{Q})$ for $d = \delta_E(P)$.

To compute the rank r we count $d \in G$ such that $C_d(\mathbb{Q}) \neq \emptyset$.

Motivation

- Identify points in $\dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})}$ with homogeneous spaces.
- Need to find rational points on C_d for $d \in G$.
- How do we do this?

2-Selmer and Shafarevich-Tate Groups

$$\frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \xrightarrow{\delta_E} \mathrm{Sel}^{(2)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[2]$$

where we define the 2-Selmer and Shafarevich-Tate groups

$$\mathrm{Sel}^{(2)}(E/\mathbb{Q}) = \left\{ d \in G \;\middle|\; \begin{array}{c} C_d(\mathbb{R}) \neq \emptyset \text{ and} \\ C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p \end{array} \right\}$$

$$Ш(E/\mathbb{Q})[2] = \left\{ d \in G \;\middle|\; \begin{array}{c} C_d(\mathbb{R}) \neq \emptyset \text{ and} \\ C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p \\ \text{but } C_d(\mathbb{Q}) = \emptyset \end{array} \right\}$$

2-Selmer and Shafarevich-Tate Groups

- $\left|\dfrac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right| = 2^{r+2}$
- $\left|\mathrm{Sel}^{(2)}(E/\mathbb{Q})\right| = 2^{s+2}$
- $\left|Ш(E/\mathbb{Q})[2]\right| = 2^{s-r}$

- 2-Selmer group is easy to compute, Shafarevich-Tate group is hard to compute
- Hopefully $r = s$, i.e., the Shafarevich-Tate group is trivial
- We use `mwrank`

mwrank

John Cremona

http://www.maths.nott.ac.uk/personal/jec/mwrank/index.html

Searching For a Curve with Rank $r \geq 3$

To search for an elliptic curve defined over $\mathbb{Q}$ with torsion subgroup $Z_2 \times Z_8$ and rank $r \geq 3$, we use the following algorithm:

#1. Generate a list of candidate curves

#2. Compute the ranks of the 2-Selmer groups of these curves.

#3. Compute the Mordell-Weil ranks of the curves with 2-Selmer ranks $s \geq 3$.

Classification of Curves with Torsion $Z_2 \times Z_8$

E is an elliptic curve with torsion subgroup $Z_2 \times Z_8$ if and only if there exist integers a and b such that E is birationally equivalent to

$$y^2 = (1 - x^2)(1 - k^2 x^2), \quad \text{where} \quad k = \frac{a^4 - 6a^2b^2 + b^4}{(a^2 + b^2)^2}.$$

Using the maps $(a, b) \mapsto (-a, b)$ and $(a, b) \mapsto (a - b, a + b)$, we may choose a and b such that $0 < (1 + \sqrt{2})a < b$.

Generating Candidate Curves

#1. INPUT: Bound N

#2. For integers a and b satisfying $0 < (1+\sqrt{2})a < b \leq N$

a. Define

$$p = a^4 - 6a^2b^2 + b^4 \qquad A = -27(p^4 + 14p^2q^2 + q^4)$$
$$q = (a^2 + b^2)^2 \qquad B = -54(p^6 - 33p^4q^2 - 33p^2q^4 + q^6)$$

b. Record the elliptic curve $Y^2 = X^3 + AX + B$ to a list.

#3. OUTPUT: List of elliptic curves

- $N = 5\,000$ took 10 minutes to generate 3 148 208 curves
- Divide into 256 files (12 300 curves per file) for parallel processing

Algorithm

Redhawk at Miami University

Bound N	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%)

Computation of Mordell-Weil Ranks

- Data for $N = 1\,000$ and $s = 3$
- $16\,933$ curves in this list
- 12 of these curves are known to have $r = 3$
- Can we find more?

New Curves we found

Parameter t	Rank r
$\frac{19}{84}$	3
$\frac{101}{299}$	3
$\frac{86}{333}$	3
$\frac{12}{65}$	$2 \leq r \leq 3$
$\frac{21}{92}$	$2 \leq r \leq 3$
$\frac{9}{296}$	$2 \leq r \leq 3$
$\frac{65}{337}$	$2 \leq r \leq 3$

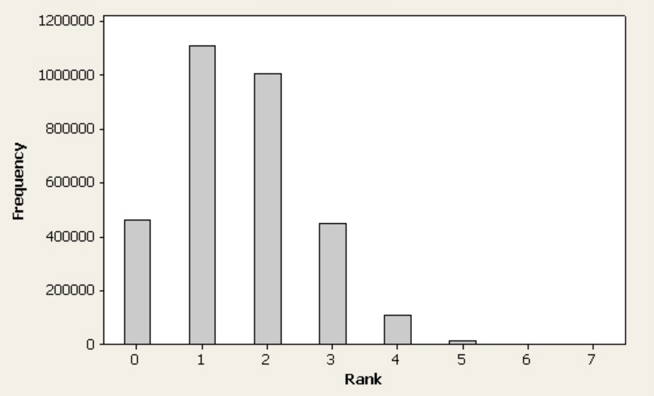
Algorithm

Radon at Purdue University

Q: What do we do while `mwrank` is running?

A: Consider 2-Selmer ranks, of course!

Poisson Distribution?



Histogram of Ranks of 2-Selmer Groups for $N = 5\,000$

Is this Poisson?

Poisson Distributions

- Observed: $O(s)$ with average $\bar{s} = \dfrac{\sum_{s=0}^{m(N)} s \cdot O(s)}{\sum_{s=0}^{m(N)} O(s)}$
- Expected: $E(s) = \left[\displaystyle\sum_{m=0}^{m(N)} O(m)\right] \cdot \dfrac{\lambda^s}{s!} e^{-\lambda}$ with $\lambda = \bar{s}$
- Chi-square distribution: $\chi^2 = \displaystyle\sum_{s=0}^{m(N)} \frac{[O(s) - E(s)]^2}{E(s)}$
- Compare with value of $\chi^2_{\alpha,\text{df}}$ where $\alpha = 5\%$ and $\text{df} = m(N) - 1$. If $\chi^2 \leq \chi^2_{\alpha,\text{df}}$, accept hypothesis.

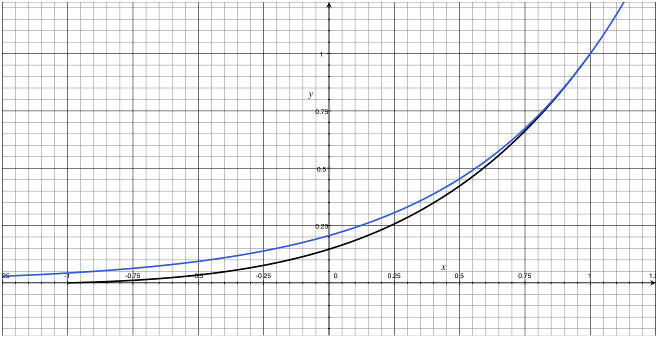
Chi-Square Distribution of 2-Selmer Ranks

Bound N	$m(N)$	$\bar{s}$	χ^2	$\chi^2_{\alpha,\,\mathrm{df}}$
1 000	6	1.529456	7 700.072	11.070
2 000	7	1.558704	29 761.771	12.592
3 000	7	1.569643	65 653.675	12.592
4 000	7	1.575738	115 008.433	12.592
5 000	7	1.579246	177 788.496	12.592

Poisson Distribution?

Bound N	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%)

Generating Functions



$$f_{\text{sel}}(z) \approx 0.146 + 0.353\,z + 0.319\,z^2 + 0.143\,z^3 + \cdots$$

Acknowledgments and References

- SUMSRI and Miami University
- Residential Computing at Miami University
- Rosen Center for Advanced Computing at Purdue
- Dr. Goins and Maria Salcedo
- Dr. Waikar and Ashley Swandby
- NSF and NSA

References

1. Edray Goins. SUMSRI Number Theory Notes. In preparation, 2007.
2. John Cremona. `mwrank` and related programs for elliptic curves over $\mathbb{Q}$. `http://www.maths.nott.ac.uk/personal/jec/mwrank/`.
3. Joseph H. Silverman. *The Arithmetic of Elliptic Curves, Springer-Verlag, New York-Berlin, 1986.*