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

A. Rollick\textsuperscript{1}  J. Weigandt\textsuperscript{2}

\textsuperscript{1}Department of Mathematics
John Carroll University

\textsuperscript{2}Department of Mathematics
Purdue University

Summer Undergraduate Mathematical Sciences Research Institute 2007
Outline

Family of Elliptic Curves with $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$

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

Then we have the “connecting homomorphism”:

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

$\delta_E$ is injective and its image lies in a finite group

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

\[ \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \left\{ d \in G \mid C_d(\mathbb{Q}) \neq \emptyset \right\} \cong \mathbb{Z}_2^{r+2}. \]

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 \(C_d(\mathbb{Q}) \neq \emptyset\).
The 2-Selmer Group

**Motivation**

- Identify points in $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}$ 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

\[
\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \xrightarrow{\delta_E} \text{Sel}^{(2)}(E/\mathbb{Q}) \xrightarrow{\Phi} \text{III}(E/\mathbb{Q})[2]
\]

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

\[
\text{Sel}^{(2)}(E/\mathbb{Q}) = \left\{ d \in G \mid C_d(\mathbb{R}) \neq \emptyset \text{ and } C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p \right\}
\]

\[
\text{III}(E/\mathbb{Q})[2] = \left\{ d \in G \mid C_d(\mathbb{R}) \neq \emptyset \text{ and } C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p \text{ but } C_d(\mathbb{Q}) = \emptyset \right\}
\]
2-Selmer and Shafarevich-Tate Groups

- \( \frac{|E(\mathbb{Q})|}{|2E(\mathbb{Q})|} = 2^{r+2} \)
- \( |\text{Sel}^{(2)}(E/\mathbb{Q})| = 2^{s+2} \)
- \( |\text{III}(E/\mathbb{Q})[2]| = 2^{s-r} \)

- 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 \texttt{mwrank}
Family of Elliptic Curves with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$

Computations

Distribution of 2-Selmer Ranks

mwrack

Rollick, Weigandt

SUMSRI, Miami University

2-Selmer Ranks

---

John Cremona

http://www.maths.nott.ac.uk/personal/jec/mwrack/index.html
Searching For a Curve with Rank \( r \geq 3 \)

To search for an elliptic curve defined over \( \mathbb{Q} \) with torsion subgroup \( \mathbb{Z}_2 \times \mathbb{Z}_8 \) 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 $\mathbb{Z}_2 \times \mathbb{Z}_8$

$E$ is an elliptic curve with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$ if and only if there exist integers $a$ and $b$ such that $E$ is birationally equivalent to

$$y^2 = (1 - x^2)(1 - k^2 x^2),$$

where

$$k = \frac{a^4 - 6a^2 b^2 + b^4}{(a^2 + b^2)^2}.$$ 

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

Rollick, Weigandt

SUMSRI, Miami University
Family of Elliptic Curves with $E(Q)_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$

Computations

Distribution of 2-Selmer Ranks

Algorithm

Generating Candidate Curves

#1. INPUT: Bound $N$

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

   a. Define

   \[
   p = a^4 - 6a^2b^2 + b^4 \quad A = -27(p^4 + 14p^2q^2 + q^4)
   \]

   \[
   q = (a^2 + b^2)^2 \quad B = -54(p^6 - 33p^4q^2 - 33p^2q^4 + q^6)
   \]

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

#3. OUTPUT: List of elliptic curves

- $N = 5000$ took 10 minutes to generate 3148208 curves
- Divide into 256 files (12300 curves per file) for parallel processing

Rollick, Weigandt

SUMSRI, Miami University

2-Selmer Ranks
Family of Elliptic Curves with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$

Algorithm

Computations

Distribution of 2-Selmer Ranks

Redhawk at Miami University

Rollick, Weigandt

2-Selmer Ranks

SUMSRI, Miami University
Family of Elliptic Curves with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$

## Computations

### Distribution of 2-Selmer Ranks

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

- Data for $N = 1000$ 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

<table>
<thead>
<tr>
<th>Parameter $t$</th>
<th>Rank $r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{19}{84}$</td>
<td>3</td>
</tr>
<tr>
<td>$\frac{101}{299}$</td>
<td>3</td>
</tr>
<tr>
<td>$\frac{86}{333}$</td>
<td>3</td>
</tr>
<tr>
<td>$\frac{12}{65}$</td>
<td>$2 \leq r \leq 3$</td>
</tr>
<tr>
<td>$\frac{21}{92}$</td>
<td>$2 \leq r \leq 3$</td>
</tr>
<tr>
<td>$\frac{9}{296}$</td>
<td>$2 \leq r \leq 3$</td>
</tr>
<tr>
<td>$\frac{65}{337}$</td>
<td>$2 \leq r \leq 3$</td>
</tr>
</tbody>
</table>
Family of Elliptic Curves with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$

Algorithm

Computations

Distribution of 2-Selmer Ranks

Radon at Purdue University

Rollick, Weigandt

SUMSRI, Miami University

2-Selmer Ranks
Q: What do we do while $\text{mwrank}$ is running?

A: Consider 2-Selmer ranks, of course!
Family of Elliptic Curves with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$

Computations

Distribution of 2-Selmer Ranks

Poisson Distribution?

Histogram of Ranks of 2-Selmer Groups for $N = 5000$

Rollick, Weigandt

SUMSRI, Miami University

2-Selmer Ranks
Is this Poisson?
Poisson Distributions

- Observed: \( O(s) \) with average \( \bar{s} = \frac{\sum_{s=0}^{m(N)} s \cdot O(s)}{\sum_{s=0}^{m(N)} O(s)} \)

- Expected: \( E(s) = \left[ \sum_{m=0}^{m(N)} O(m) \right] \cdot \frac{\lambda^s}{s!} e^{-\lambda} \) with \( \lambda = \bar{s} \)

- Chi-square distribution: \( \chi^2 = \sum_{s=0}^{m(N)} \frac{[O(s) - E(s)]^2}{E(s)} \)

- Compare with value of \( \chi^2_{\alpha, df} \) where \( \alpha = 5\% \) and \( df = m(N) - 1 \). If \( \chi^2 \leq \chi^2_{\alpha, df} \), accept hypothesis.
### Chi-Square Distribution of 2-Selmer Ranks

<table>
<thead>
<tr>
<th>Bound $N$</th>
<th>$m(N)$</th>
<th>$\bar{s}$</th>
<th>$\chi^2$</th>
<th>$\chi^2_{\alpha, df}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 000</td>
<td>6</td>
<td>1.529456</td>
<td>7 700.072</td>
<td>11.070</td>
</tr>
<tr>
<td>2 000</td>
<td>7</td>
<td>1.558704</td>
<td>29 761.771</td>
<td>12.592</td>
</tr>
<tr>
<td>3 000</td>
<td>7</td>
<td>1.569643</td>
<td>65 653.675</td>
<td>12.592</td>
</tr>
<tr>
<td>4 000</td>
<td>7</td>
<td>1.575738</td>
<td>115 008.433</td>
<td>12.592</td>
</tr>
<tr>
<td>5 000</td>
<td>7</td>
<td>1.579246</td>
<td>177 788.496</td>
<td>12.592</td>
</tr>
</tbody>
</table>
### Poisson Distribution?

<table>
<thead>
<tr>
<th>Bound N</th>
<th>1000</th>
<th>2000</th>
<th>3000</th>
<th>4000</th>
<th>5000</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s = 0$</td>
<td>19,309</td>
<td>75,384</td>
<td>167,581</td>
<td>296,135</td>
<td>461,127</td>
</tr>
<tr>
<td></td>
<td>(15.32%)</td>
<td>(14.96%)</td>
<td>(14.79%)</td>
<td>(14.70%)</td>
<td>(14.65%)</td>
</tr>
<tr>
<td>$s = 1$</td>
<td>45,807</td>
<td>179,361</td>
<td>401,351</td>
<td>711,392</td>
<td>1,110,462</td>
</tr>
<tr>
<td></td>
<td>(36.35%)</td>
<td>(35.59%)</td>
<td>(35.41%)</td>
<td>(35.31%)</td>
<td>(35.27%)</td>
</tr>
<tr>
<td>$s = 2$</td>
<td>40,044</td>
<td>161,031</td>
<td>362,152</td>
<td>643,340</td>
<td>1,004,658</td>
</tr>
<tr>
<td></td>
<td>(31.75%)</td>
<td>(31.96%)</td>
<td>(31.95%)</td>
<td>(31.93%)</td>
<td>(31.91%)</td>
</tr>
<tr>
<td>$s = 3$</td>
<td>16,933</td>
<td>70,481</td>
<td>160,695</td>
<td>287,682</td>
<td>450,939</td>
</tr>
<tr>
<td></td>
<td>(13.44%)</td>
<td>(13.99%)</td>
<td>(14.18%)</td>
<td>(14.28%)</td>
<td>(14.32%)</td>
</tr>
<tr>
<td>$s = 4$</td>
<td>3,550</td>
<td>15,845</td>
<td>36,956</td>
<td>67,289</td>
<td>106,791</td>
</tr>
<tr>
<td></td>
<td>(2.82%)</td>
<td>(3.14%)</td>
<td>(3.26%)</td>
<td>(3.34%)</td>
<td>(3.39%)</td>
</tr>
<tr>
<td>$s = 5$</td>
<td>338</td>
<td>1,707</td>
<td>4,370</td>
<td>8,208</td>
<td>13,371</td>
</tr>
<tr>
<td></td>
<td>(0.27%)</td>
<td>(0.34%)</td>
<td>(0.39%)</td>
<td>(0.41%)</td>
<td>(0.42%)</td>
</tr>
<tr>
<td>$s = 6$</td>
<td>22</td>
<td>112</td>
<td>256</td>
<td>509</td>
<td>839</td>
</tr>
<tr>
<td></td>
<td>(0.02%)</td>
<td>(0.02%)</td>
<td>(0.02%)</td>
<td>(0.03%)</td>
<td>(0.03%)</td>
</tr>
<tr>
<td>$s = 7$</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>(0.00%)</td>
<td>(0.00%)</td>
<td>(0.00%)</td>
<td>(0.00%)</td>
<td>(0.00%)</td>
</tr>
</tbody>
</table>
Family of Elliptic Curves with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$

Computations

Distribution of 2-Selmer Ranks

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

