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

Edray Herber Goins

Department of Mathematics
Purdue University

January 24, 2008
Abstract

Consider the family of all elliptic curves $E$ defined over $\mathbb{Q}$ such that the kernel of the multiplication-by-2-map $[2] : E \rightarrow E$ is rational. Galois cohomology asserts that the finite quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ 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 $\text{Sel}^{(2)}(E/\mathbb{Q})$, 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 second of three talks, we discuss techniques for finding elliptic curves with large Mordell-Weil rank. We discuss how the Mordell-Weil and 2-Selmer ranks are related by considering the number of primes which divide the discriminant. We assume basic working knowledge of algebraic varieties, since most of the language will be in terms of elliptic surfaces.
Outline of Talk

1. Review
   - Classification of Curves with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$
   - Complete 2-Descent

2. Bounds for Ranks of Elliptic Curves
   - Records of Mordell-Weil Ranks
   - Mordell-Weil Ranks
   - 2-Selmer Ranks

3. Introduction to Distributions
   - Basic Definitions
   - Counting Classes of Fibers on Elliptic Surfaces
   - Distribution of Primes which Divide the Discriminant
Conjecture (Henri Poincaré, 1901)

Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $(E(\mathbb{Q}), \oplus)$ is a finitely generated abelian group.

Theorem (Louis Mordell, 1922)

Let $E$ be an elliptic curve over $\mathbb{Q}$. There exists a finite group $E(\mathbb{Q})_{\text{tors}}$ and a nonnegative integer $r$ such that $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$.

Theorem (Barry Mazur, 1977)

Let $E$ be an elliptic curve over $\mathbb{Q}$. Its torsion subgroup is one of 15 types:

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}_n & \text{for } 1 \leq n \leq 10 \text{ or } n = 12; \\ \mathbb{Z}_2 \times \mathbb{Z}_{2n} & \text{for } 1 \leq n \leq 4. \end{cases}$$
Theorem (G, 2005)

Fix a rational number $k \neq -1, 0, 1$ and consider the quartic curve

$$E : \quad y^2 = (1 - x^2) (1 - k^2 x^2).$$

Writing $k = p/q$, this curve is birationally equivalent to

$$Y^2 = X^3 + AX + B,$$

where

$$A = -27 \left( p^4 + 14 p^2 q^2 + q^4 \right),$$
$$B = -54 \left( p^6 - 33 p^4 q^2 - 33 p^2 q^4 + q^6 \right).$$

E is an elliptic curve with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_8$.

Any elliptic curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_8$ is birationally equivalent to $E$ for some rational $k$. In the latter case, $k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}$ for some rational number $t \neq -1, 0, 1$. 
Assumptions Revisited

Last week, we assumed that $E : Y^2 = X^3 + A X + B$ is a curve satisfying

- $A$ and $B$ are integers such that $\Delta(E) = -16 (4 A^3 + 27 B^2) \neq 0$.
- The roots of the cubic in $X$ are rational. That is,

$$X^3 + A X + B = (X - e_1)(X - e_2)(X - e_3), \quad e_1, e_2, e_3 \in \mathbb{Z}.$$  

Remark: $E[2] \subseteq E(\mathbb{Q})$, so Mazur’s Theorem implies $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$.

In the case of the quartic curve

$$E : \quad y^2 = (1 - x^2) (1 - k^2 x^2)$$

we set $k = p/q$. Then have $\Delta(E) = -2^4 3^{12} p^2 q^2 (p^2 - q^2)^4$ and roots

$$e_1 = -3 (p^2 + 6 pq + q^2) \quad e_2 = -3 (p^2 - 6 pq + q^2) \quad e_3 = 6 (p^2 + q^2)$$

and

$$A = -27 (p^4 + 14 p^2 q^2 + q^4)$$

$$B = -54 (p^6 - 33 p^4 q^2 - 33 p^2 q^4 + q^6)$$
Computing the Mordell-Weil Rank

Last time, we showed that the connecting homomorphism implies

$$\delta_E : \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \sim \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \mid C_{(d_1, d_2)}(\mathbb{Q}) \neq \emptyset \right\}$$

as a finite group of order $2^{r+2}$. In order to determine the rank $r$,

1. Consider pairs $(d_1, d_2)$ of square-free integers which divide $\Delta(E)$.
2. Determine which homogeneous spaces have a (global) rational point

$$C_{(d_1, d_2)} : \begin{align*}
    d_1 u^2 - d_2 v^2 &= (e_2 - e_1) t^2 \\
    d_1 u^2 - d_1 d_2 w^2 &= (e_3 - e_1) t^2
\end{align*}$$

We will use the 2-Selmer group, which has order $2^{s+2}$:

$$\text{Sel}^{(2)}(E/\mathbb{Q}) = \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \mid C_{(d_1, d_2)}(\mathbb{Q}_\ell) \neq \emptyset \right\}$$

for all primes $\ell$. 
Prescribed Torsion and Rank

Conjecture

Let $T$ be one of the fifteen torsion groups in Mazur’s Theorem. For any given nonnegative integer $r_0$, there exists an elliptic curve $E$ over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \cong T$ and Mordell-Weil rank $r(E) \geq r_0$.

Open Problem

Given $T$ and $r_0$, find an elliptic curve $E$ over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \cong T$ and Mordell-Weil rank $r(E) \geq r_0$.

For each torsion group $T$, define the quantity

$$B(T) = \sup \left\{ r \in \mathbb{Z} \mid \text{there exists a curve } E \text{ with } E(\mathbb{Q}) \cong T \times \mathbb{Z}^r \right\}.$$

Question: Is $B(T)$ unbounded?
# Records for Prescribed Torsion and Rank

<table>
<thead>
<tr>
<th>$E(\mathbb{Q})_{\text{tors}}$</th>
<th>Highest Rank $r$</th>
<th>Found By</th>
<th>Year Discovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trivial</td>
<td>28</td>
<td>Elkies</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_2$</td>
<td>18</td>
<td>Elkies</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_3$</td>
<td>13</td>
<td>Eroshkin</td>
<td>2007, 2008</td>
</tr>
<tr>
<td>$\mathbb{Z}_4$</td>
<td>12</td>
<td>Elkies</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_5$</td>
<td>6</td>
<td>Dujella, Lecacheux</td>
<td>2001</td>
</tr>
<tr>
<td>$\mathbb{Z}_6$</td>
<td>7</td>
<td>Dujella</td>
<td>2001, 2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_6$</td>
<td>7</td>
<td>Eroshkin</td>
<td>2007</td>
</tr>
<tr>
<td>$\mathbb{Z}_7$</td>
<td>5</td>
<td>Dujella, Kulesz</td>
<td>2001</td>
</tr>
<tr>
<td>$\mathbb{Z}_8$</td>
<td>6</td>
<td>Elkies</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_9$</td>
<td>4</td>
<td>Dujella</td>
<td>2001</td>
</tr>
<tr>
<td>$\mathbb{Z}_9$</td>
<td>4</td>
<td>MacLeod</td>
<td>2004</td>
</tr>
<tr>
<td>$\mathbb{Z}_9$</td>
<td>4</td>
<td>Eroshkin</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_9$</td>
<td>4</td>
<td>Dujella, Eroshkin</td>
<td>2007</td>
</tr>
<tr>
<td>$\mathbb{Z}_{10}$</td>
<td>4</td>
<td>Dujella</td>
<td>2005</td>
</tr>
<tr>
<td>$\mathbb{Z}_{10}$</td>
<td>4</td>
<td>Elkies</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_{12}$</td>
<td>3</td>
<td>Dujella</td>
<td>2001, 2005, 2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_{12}$</td>
<td>3</td>
<td>Rathbun</td>
<td>2005, 2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>14</td>
<td>Elkies</td>
<td>2005</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_4$</td>
<td>8</td>
<td>Elkies</td>
<td>2005</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_6$</td>
<td>6</td>
<td>Elkies</td>
<td>2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_8$</td>
<td>3</td>
<td>Connell</td>
<td>2000</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_8$</td>
<td>3</td>
<td>Dujella</td>
<td>2000, 2001, 2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_8$</td>
<td>3</td>
<td>Campbell, Goins</td>
<td>2003</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_8$</td>
<td>3</td>
<td>Rathbun</td>
<td>2003, 2006</td>
</tr>
<tr>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_8$</td>
<td>3</td>
<td>Flores, Jones, Rollick, Weigandt</td>
<td>2007</td>
</tr>
</tbody>
</table>

http://web.math.hr/~duje/tors/tors.html
For rational numbers $t \neq -1, 0, 1$, consider the elliptic curve

$$E_t : \quad y^2 = (1 - x^2) (1 - k^2 x^2) \quad \text{where} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}$$

with Mordell-Weil group $E_t(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_r$ for some $r = r(t)$. Recall that all elliptic curves $E$ over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$ are in this form.

There are thirteen known elliptic curves $E$ over $\mathbb{Q}$ with Mordell-Weil group $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3$, all corresponding to

$$t \in \left\{ \begin{array}{c} \frac{5}{29}, \frac{18}{47}, \frac{15}{76}, \frac{74}{207}, \frac{47}{219}, \frac{19}{220}, \frac{87}{407}, \\ \frac{143}{419}, \frac{17}{439}, \frac{145}{444}, \frac{159}{569}, \frac{230}{923}, \frac{223}{1012} \end{array} \right\}.$$

Question: Can we find a rational $t \neq -1, 0, 1$ such that $r(t) \geq 4$?
Upper Bound for Mordell-Weil Ranks

Recall that the connecting homomorphism gives the exact diagram

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q}) & \longrightarrow & \frac{2E(\mathbb{Q})}{E(\mathbb{Q})} & \overset{\delta_E}{\longrightarrow} & \text{Sel}^{(2)}(E/\mathbb{Q}) & \longrightarrow & \text{III}(E/\mathbb{Q})[2] & \longrightarrow & 0 \\
& & \downarrow{\cong} & & \downarrow{\cong} & & \downarrow{\cong} & & \downarrow{\cong} & & \\
1 & \longrightarrow & \mathbb{Z}_2^{r+2} & \longrightarrow & \mathbb{Z}_2^{s+2} & \longrightarrow & \mathbb{Z}_2^{s-r} & \longrightarrow & 1 \\
\end{array}
\]

Hence the Mordell-Weil rank \( r \) is bounded above by the 2-Selmer rank \( s \).

Observation (Noam Elkies, 2005)

Compute the 2-Selmer ranks \( s \) first as a way to filter out those elliptic curves \( E \) with low Mordell-Weil rank \( r \).

Remark: The finiteness conjecture of the Shafarevich-Tate group implies

\[ r \equiv s \pmod{2}. \]

Since \( r \leq s \), we have \( r = s \) when this group has no 2-torsion.
Classification via Elliptic Surfaces

Choose a curve $V$ over $\mathbb{Q}$. For rational functions $A, B \in \mathbb{Q}(V)$, define

$$
\mathcal{E} = \left\{ \left( (X_1 : X_2 : X_0), \ t \right) \in \mathbb{P}^2 \times V \bigg| X_2^2 X_0 = X_1^3 + A(t) X_1 X_0^2 + B(t) X_0^3 \right\}
$$

$E_t$, the fiber of $\mathcal{E} \to V$ defined by $\left( (X_1 : X_2 : X_0), \ t \right) \mapsto t$, has a rational point $O_t = ((0 : 1 : 0), \ t)$. Hence they are elliptic curves defined over $\mathbb{Q}$.

Example (Quadratic Twists)

Choose $V = \text{Spec} \mathbb{Z}[w, t]/ (w t - 1)$ with $A(t) = t^2 A_1$ and $B(t) = t^3 B_1$.

Example (Family with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$)

Choose $V = \text{Spec} \mathbb{Z}[w, t]/ (w t (t^4 - 1)(t^4 - 6 t^2 + 1) - 1)$ with

$$
A(t) = -27 \left( k^4 + 14 k^2 + 1 \right)
\quad \text{for} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}.
$$

$$
B(t) = -54 \left( k^6 - 33 k^4 - 33 k^2 + 1 \right)
\quad \text{for} \quad k = \frac{t^4 - 6 t^2 + 1}{(t^2 + 1)^2}.
$$
Consider an elliptic surface $E$ over a curve $V$. For each fiber $E_t$, define

$$S(t) = \left\{ \ell \in \text{Spec } \mathbb{Z} \left| \ell \text{ occurs in the factorization of } \Delta(E_t) = -16 \left( 4 A(t)^3 + 27 B(t)^2 \right) \right. \right\}.$$

**Theorem**

Let $E$ be the elliptic surface which classifies elliptic curves $E$ over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_8$. For each fiber $E_t$,

$$r(t) \leq s(t) \leq 2 |S(t)|.$$

**Proof:** Both $E(\mathbb{Q})/2 E(\mathbb{Q})$ and $\text{Sel}^{(2)}(E/\mathbb{Q})$ are contained in

$$\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) = \left\{ (d_1, d_2) \in \left( \mathbb{Q}^\times / \mathbb{Q}^\times \right)^2 \times \left( \mathbb{Q}^\times / \mathbb{Q}^\times \right)^2 \left| d_i = \pm \prod_{\ell \in S} \ell^{e_i(\ell)} \right. \right\},$$

which is a finite group of order $(2|S|+1)^2$. \(\square\)

**Remark (Barry Mazur):** One should be able to replace $2 |S|$ by just $|S|$. 
Consider the elliptic curve corresponding to $t = 5/29$.

$$E : \quad Y^2 + X Y = X^3 - 15745932530829089880 X + 24028219957095969426339278400$$

- This curve has Mordell-Weil rank $r = 3$:
  $$E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \quad \implies \quad \frac{E(\mathbb{Q})}{2 E(\mathbb{Q})} \cong \mathbb{Z}_2^5.$$  

- It also has 2-Selmer rank $s = 3$:
  $$\text{Sel}^{(2)}(E/\mathbb{Q}) \cong \mathbb{Z}_2^5 \quad \implies \quad \text{III}(E/\mathbb{Q})[2] = \{0\}.$$  

- Those primes which divide the discriminant $\Delta(E)$ are
  $$S = \{2, 3, 5, 7, 17, 29, 79, 263, 433\} \quad \implies \quad 2 |S| = 18.$$
Consider an elliptic surface $\mathcal{E}$ over a curve $V$. Given $f : V \to \mathbb{Z}$, define

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

for $W \subseteq V$ with $\dim W = 0$. Similarly, define the probability distribution

$$
\text{Probability}_f(W \mid \alpha \leq f \leq \beta) = \sum_{\alpha \leq x \leq \beta} \frac{|f^{-1}(x) \cap W|}{|W|}.
$$

**Problem**

Compute the probability distributions for $r = r(t)$ and $s = s(t)$.

**Remark:** With convergence, we may also use a generating function.

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

where $\text{Avg}(f) = \Phi'_f(1)$ and $\text{Var}(f) = \Phi''_f(1) + \Phi'_f(1) - \Phi'_f(1)^2$. 
Let $E$ be the elliptic surface defined over the curve

$$V = \left\{ (a : b) \in \mathbb{P}^1 \mid a \ b (a^4 - b^4) \ (a^4 - 6 \ a^2 \ b^2 + b^4) \neq 0 \right\}$$

which classifies elliptic curves $E$ over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$. Denoting $t = a/b$, we have an action on isomorphism classes $\{E_t\}$ by

$$\sigma : (a : b) \mapsto (a - b : a + b) \quad \text{and} \quad \tau : (a : b) \mapsto (-a : b)$$

which generate the dihedral group $D_8$. We choose the $D_8$-conjugate

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

**Theorem (G, 2005-08)**

$W_T \subseteq V$ and $\dim W_T = 0$ for each $T$. In fact, $W_T \rightarrow V$ as $T \rightarrow \infty$, and

$$\lim_{T \rightarrow \infty} \frac{|W_T|}{T^2} = \frac{4}{1 + \sqrt{2}} \cdot \frac{6}{\pi^2} = 1.0072 \ldots$$
For a given bound $T$, the number isomorphism classes $\{E_t\}$ is the ratio

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

<table>
<thead>
<tr>
<th>Bound $T$</th>
<th>1000</th>
<th>2000</th>
<th>3000</th>
<th>4000</th>
<th>5000</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{</td>
<td>W_T</td>
<td>}{</td>
<td>D_8</td>
<td>}$</td>
<td>126 003</td>
</tr>
</tbody>
</table>

Question: We have the inequalities

$$r(t) \leq s(t) \leq 2|S(t)|.$$

What can we say about the distributions of these three functions?
Number of Bad Primes Data

Histogram of Prime Divisors for $T = 3000$

$|S(t)|$ for $T = 3000$ over 1,133,364 Curves
Questions?