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

Edray Herber Goins

Department of Mathematics
Purdue University

January 24, 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 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 $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$
   - 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

Mordell-Weil Group

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 $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$.

Theorem (Barry Mazur, 1977)

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

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} Z_n & \text{for } 1 \leq n \leq 10 \text{ or } n = 12; \\ Z_2 \times Z_{2n} & \text{for } 1 \leq n \leq 4. \end{cases}$$

$E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_4$ or $Z_2 \times Z_8$

Theorem (G, 2005)

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

$$E: \qquad y^2 = \left(1 - x^2\right)\left(1 - k^2\, x^2\right).$$

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

$$Y^2 = X^3 + A\,X + B, \qquad \begin{aligned} A &= -27\left(p^4 + 14\,p^2\,q^2 + q^4\right) \\ B &= -54\left(p^6 - 33\,p^4\,q^2 - 33\,p^2\,q^4 + q^6\right) \end{aligned}$$

2. *E is an elliptic curve with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_4$ or $Z_2 \times Z_8$.*

3. *Any elliptic curve over $\mathbb{Q}$ with torsion subgroup $Z_2 \times Z_4$ or $Z_2 \times Z_8$ is birationally equivalent to E for some rational k. In the latter case, $k = \dfrac{t^4 - 6\,t^2 + 1}{(t^2+1)^2}$ 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 $\Delta(E) = -16\left(4\,A^3 + 27\,B^2\right) \neq 0$.
- The roots of the cubic in X are rational. That is,

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

Remark: $E[2] \subseteq E(\mathbb{Q})$, so Mazur's Theorem implies $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2n}$.

In the case of the quartic curve

$$E : \qquad y^2 = \left(1 - x^2\right)\left(1 - k^2\,x^2\right)$$

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

$$\begin{aligned} e_1 &= -3\left(p^2 + 6\,p\,q + q^2\right) \\ e_2 &= -3\left(p^2 - 6\,p\,q + q^2\right) \\ e_3 &= 6\left(p^2 + q^2\right) \end{aligned} \quad \text{for} \quad \begin{aligned} A &= -27\left(p^4 + 14\,p^2\,q^2 + q^4\right) \\ B &= -54\left(p^6 - 33\,p^4\,q^2 - 33\,p^2\,q^4 + q^6\right) \end{aligned}$$

Computing the Mordell-Weil Rank

Last time, we showed that the connecting homomorphism implies

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

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

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

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

$$\text{Sel}^{(2)}(E/\mathbb{Q}) = \left\{ (d_1, d_2) \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \,\middle|\, \begin{array}{c} C_{(d_1,d_2)}(\mathbb{Q}_\ell) \neq \emptyset \\ \text{for all primes } \ell \end{array} \right\}$$

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 $E(\mathbb{Q})_{\text{tors}} \simeq T$ 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 $E(\mathbb{Q})_{\text{tors}} \simeq T$ and Mordell-Weil rank $r(E) \geq r_0$.

For each torsion group T, define the quantity

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

Question: Is $B(T)$ unbounded?

Records for Prescribed Torsion and Rank

$E(\mathbb{Q})_{\text{tors}}$	Highest Rank r	Found By	Year Discovered
Trivial	28	Elkies	2006
Z_2	18	Elkies	2006
Z_3	13	Eroshkin	2007, 2008
Z_4	12	Elkies	2006
Z_5	6	Dujella, Lecacheux	2001
Z_6	7	Dujella Eroshkin	2001, 2006 2007
Z_7	5	Dujella, Kulesz Elkies	2001 2006
Z_8	6	Elkies	2006
Z_9	4	Dujella MacLeod Eroshkin Dujella, Eroshkin	2001 2004 2006 2007
Z_{10}	4	Dujella Elkies	2005 2006
Z_{12}	3	Dujella Rathbun	2001, 2005, 2006 2005, 2006
$Z_2 \times Z_2$	14	Elkies	2005
$Z_2 \times Z_4$	8	Elkies	2005
$Z_2 \times Z_6$	6	Elkies	2006
$Z_2 \times Z_8$	3	Connell Dujella Campbell, Goins Rathbun Flores, Jones, Rollick, Weigandt	2000 2000, 2001, 2006 2003 2003, 2006 2007

http://web.math.hr/~duje/tors/tors.html

Rank Records for Curves with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$

For rational numbers $t \neq -1, 0, 1$, consider the elliptic curve

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

with Mordell-Weil group $E_t(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$ for some $r = r(t)$. Recall that all elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ are in this form.

There are thirteen known elliptic curves E over $\mathbb{Q}$ with Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$, all corresponding to

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

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

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

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

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

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

Example (Quadratic Twists)

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

Example (Family with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$)

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

$$\begin{aligned} A(t) &= -27\, \big(k^4 + 14\, k^2 + 1\big) \\ B(t) &= -54\, \big(k^6 - 33\, k^4 - 33\, k^2 + 1\big) \end{aligned} \qquad \text{for} \quad k = \frac{t^4 - 6\, t^2 + 1}{(t^2 + 1)^2}.$$

Upper Bound for 2-Selmer Ranks

Consider an elliptic surface $\mathcal{E}$ over a curve V. For each fiber E_t, define

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

Theorem

Let $\mathcal{E}$ be the elliptic surface which classifies elliptic curves E over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. 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

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

which is a finite group of order $\left(2^{|S|+1}\right)^2$. □

Remark (Barry Mazur): One should be able to replace $2\,|S|$ by just $|S|$.

Example

Consider the elliptic curve corresponding to $t = 5/29$.

$$E: \quad Y^2 + X\,Y = X^3 - 1574593253082908 9880\,X + 24028219957095969426339278400$$

- This curve has Mordell-Weil rank $r = 3$:

$$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3 \qquad \Longrightarrow \qquad \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq {Z_2}^5.$$

- It also has 2-Selmer rank $s = 3$:

$$\mathrm{Sel}^{(2)}(E/\mathbb{Q}) \simeq {Z_2}^5 \qquad \Longrightarrow \qquad Ш(E/\mathbb{Q})[2] = \{0\}.$$

- Those primes which divide the discriminant $\Delta(E)$ are

$$S = \{2,\, 3,\, 5,\, 7,\, 17,\, 29,\, 79,\, 263,\, 433\} \qquad \Longrightarrow \qquad 2\,|S| = 18.$$

Histograms and Distributions

Consider an elliptic surface $\mathcal{E}$ over a curve V. Given $f : V \to \mathbb{Z}$, define

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

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

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

Problem

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

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

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

where $\text{Avg}(f) = \Phi_f'(1)$ and $\text{Var}(f) = \Phi_f''(1) + \Phi_f'(1) - \Phi_f'(1)^2$.

$E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$

Let $\mathcal{E}$ be the elliptic surface defined over the curve

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

which classifies elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$.
Denoting $t = a/b$, we have an action on isomorphism classes $\{E_t\}$ by

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

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

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

Theorem (G, 2005-08)

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

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

$E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$

For a given bound T, the number isomorphism classes $\{E_t\}$ is the ratio

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

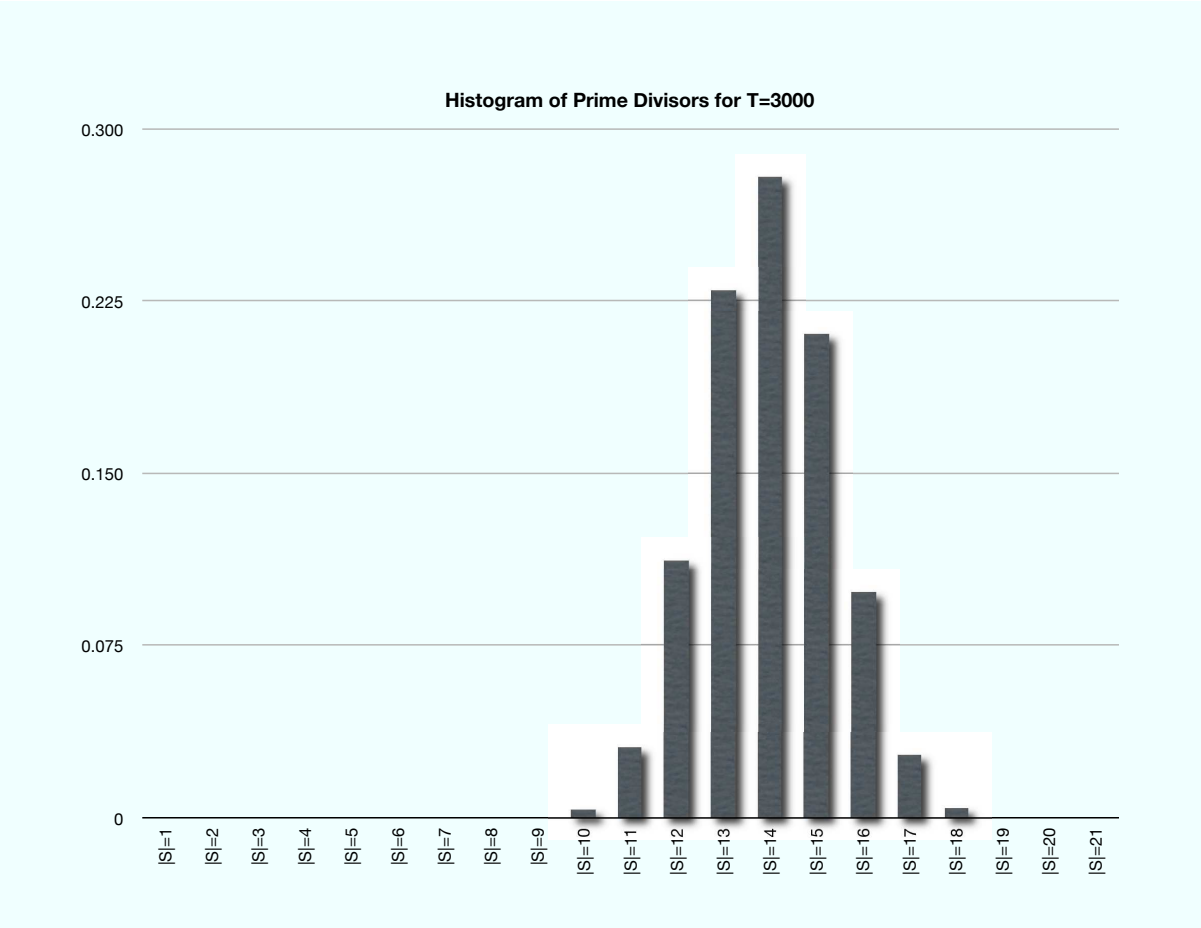
Bound T	1 000	2 000	3 000	4 000	5 000
$\frac{\lvert W_T\rvert}{\lvert D_8\rvert}$	126 003	503 923	1 133 364	2 014 563	3 148 208

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



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

Questions?