Ranks of 2-Selmer Groups of Twists of an Elliptic Curve

Daniel M. Kane

Department of Mathematics
Stanford University
aladkeenin@gmail.com

December, 2nd 2013
Selmer Groups

- $E$ and elliptic curve over $\mathbb{Q}$.
- Want to understand group of rational points $E(\mathbb{Q})$.
- Difficult to do directly.
- Consider $\text{Sel}_2(E)$ instead:
  - Easily computable
  - Finite 2-torsion group
  - $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \text{Sel}_2(E)$
Twists

- Elliptic curve $E : y^2 = f(x)$
- Twist $E_b : by^2 = f(x)$
  - Isomorphic over $\mathbb{C}$
  - Non-isomorphic over $\mathbb{Q}$ unless $b$ is a square

Main goal: Understand the distribution of $\text{rank}(\text{Sel}_2(E_b))$ as $b$ varies.
Early Work

Theorem (Heath-Brown)

Let $E$ be the curve

$$y^2 = x^3 - x,$$

then

$$\lim_{N \to \infty} \frac{\# \{ b \leq N : \dim(Sel_2(E_b)) = d \}}{N} = \alpha_d$$

where $\alpha_0 = \alpha_1 = 0$ and

$$\alpha_{n+2} = \frac{2^n}{\prod_{j=1}^{n}(2j - 1) \prod_{j=0}^{\infty}(1 + 2^{-j})}.$$

Unfortunately, this result depends on some specific formulas for the Selmer groups of twists of this particular curve, and doesn’t generalize well.
Full 2-Torsion Case

For the rest of the talk we will consider the case where $E$ has full 2-torsion.

- $E$ given by $y^2 = (x - a_1)(x - a_2)(x - a_3)$
- $E_b$ given by $y^2 = (x - ba_1)(x - ba_2)(x - ba_3)$
- If $b = p_1p_2\cdots p_n$ for distinct primes $p_i$, $\dim(Sel_2(E_b))$ depends only on:
  - $p_i$ modulo $4\Delta(E)$
  - $\left(\frac{p_i}{p_j}\right)$
- Let $\pi_d(n)$ be the fraction of elements of $((\mathbb{Z}/4\Delta(E)\mathbb{Z})^*\right)^n \times \{\pm 1\}^{n\choose 2}$ so that the appropriate twist has 2-Selmer rank $d$
Theorem (Swinnerton-Dyer)

If $E$ is an elliptic curve over $\mathbb{Q}$ with full 2-torsion over $\mathbb{Q}$ and no cyclic 4-isogeny defined over $\mathbb{Q}$, then

$$\lim_{n \to \infty} \pi_d(n) = \alpha_d$$

for all $d$.

The proof is essentially algebraic/combinatorial, making it much easier to deal with complicated curves. It gives the asymptotic density of twists with a given Selmer rank as the number of primes dividing the twist parameter goes to infinity.
Our Goal

**Goal:** Show that an $\alpha_d$-fraction of twists have 2-Selmer rank $d$ using the natural notion of density.

**Outline:**

- Find a concrete way of writing Selmer groups
- Express *moments* of Selmer groups in terms of certain sums of “characters”
- Show that each of these “characters” has average value approximately equal to its average value in the Swinnerton-Dyer sense
- Bound total error, show that the average moments are the same in the natural and Swinnerton-Dyer notions of density
- Use moment computations to get a handle on ranks
Let $E$ be the curve given by $y^2 = (x - a_1)(x - a_2)(x - a_3)$. To a point $(x, y) \in E(\mathbb{Q})$ we associate an invariant as follows:

- Each $(x - a_i) \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, have product 1.
- $(x - a_1, x - a_2, x - a_3) \in (\mathbb{Q}^*/(\mathbb{Q}^*)^2)_1^3$.
- Map to $\mathcal{V} := \prod_\nu (\mathbb{Q}_\nu^*/(\mathbb{Q}_\nu^*)^2)_1^3$.
- Image lies in:
  - $U := \text{Im}((\mathbb{Q}^*/(\mathbb{Q}^*)^2)_1^3))$
  - $W := \prod_\nu W_\nu$
    - $W_\nu$ are elements coming from points of $E(\mathbb{Q}_\nu)$
- $\text{Sel}_2(E) := U \cap W$
Finite Version

To turn the above into a finite computation:

- Let $S = \{2, \infty\} \cup \{\text{bad places of } E\}$
- For $\nu \not\in S$, $W_\nu = \{\text{unramified elements}\}$
- Elements of $U \cap W$ must come from $(\mathbb{Z}_S^*/(\mathbb{Z}_S^*)^2)_1^3$
- Let:
  - $U := (\mathbb{Z}_S^*/(\mathbb{Z}_S^*)^2)_1^3$
  - $V := \prod_{\nu \in S} (\mathbb{Q}_\nu^*/(\mathbb{Q}_\nu^*)^2)_1^3$
  - $W := \prod_{\nu \in S} W_\nu$
- Then $\text{Sel}_2(E) = U \cap W$
There is a symplectic form on $V$ given by:

$$(-1)^\langle(x_\nu, i), (y_\nu, i)\rangle = \prod_{\nu, i} (x_\nu, i, y_\nu, i)_\nu.$$ 

$U$ and $W$ Lagrangian subspaces.
Moment Formula

\[ |U \cap W| = \frac{1}{|U|} \sum_{u \in U, w \in W} (-1)^{\langle u, w \rangle}. \]

\[ |U \cap W|^k = \frac{1}{|U|^k} \sum_{u_i \in U^k, w_i \in W^k} (-1)^{\sum \langle u_i, w_i \rangle}. \]

Want to approximate

\[ \sum_{b=1}^{N} |\text{Sel}_2(E_b)|^k. \]
Consider for fixed number of prime divisors of $b$. Take $n \approx \log \log(N)$:

- Let $S_{N,n}$ be the set of $n$-tuples of primes $p_1, \ldots, p_n$ so that:
  - $p_i$ distinct
  - $(p_i, \Delta(E)) = 1$
  - $b := p_1 \cdots p_n \leq N$

- Note: Each $b$ can be written $n!$ ways.

- Approximate:

\[
\frac{1}{n!} \sum_{S_{N,n}} \left| \text{Sel}_2(E_b) \right|^k = \frac{1}{n!} \sum_{S_{N,n}} \frac{1}{|U|^k} \sum_{u_i \in U^k, w_i \in W^k} (-1)^{\sum \langle u_i, w_i \rangle}.
\]
Approximate:

\[
\frac{1}{n!} \sum_{S_{N,n}} |\text{Sel}_2(E_b)|^k = \frac{1}{n!} \sum_{S_{N,n}} \frac{1}{|U|^k} \sum_{u_i \in U^k, w_i \in W^k} (-1)^{\sum \langle u_i, w_i \rangle}.
\]

- **Idea**: Interchange order of summation.
- **Problem**: The spaces \( U \) and \( W \) in the inner sum depend on \( b \).
- **Solution**: Write \( U, V, W \) in terms of formal generators that do not depend on \( b \).
Formal Generators

- \( b = p_1 \cdots p_n \)
- \( S = \{2, \infty\} \cup \{\text{bad primes } q_i \text{ of } E\} \cup \{p_i\} \)
- \( V := \prod_{\nu \in S} (\mathbb{Q}_\nu^*/(\mathbb{Q}_\nu^*)^2)_1^3 \)
  - For \( \nu = p_i \), \( \mathbb{Q}_\nu^*/(\mathbb{Q}_\nu^*)^2 = \langle p_i, r_i \rangle \)
- \( U := (\mathbb{Z}_S^*/(\mathbb{Z}_S^*)^2)_1^3 \)
  - \( \mathbb{Z}_S^*/(\mathbb{Z}_S^*)^2 = \langle -1, 2, q_i, p_i \rangle \)
- \( W := \prod_{\nu \in S} W_\nu \)
  - \( W_\infty \) depends only on the sign of \( b \)
  - For \( \nu = 2, q_i \), \( W_\nu \) depends on a congruence class of \( b \)
  - For \( \nu = p_i \), \( W_\nu \) is generated by:

\[
((a_1 - a_2)(a_1 - a_3), b(a_1 - a_2), b(a_1 - a_3)), \text{ and }
(b(a_2 - a_1), (a_2 - a_1)(a_2 - a_3), b(a_2 - a_3))
\]

- Write \( U, V, W \) formally in terms of \( p_i \)
New Sum

- Outer sum over $k$-tuples of $u_i \in U, w_i \in W$ written formally in terms of $p_i$
- Inner sum over $S_{N,n}$
- Summand $(-1)\sum \langle u_i, w_i \rangle$
- For fixed $u_i, w_i$ get product of:
  - $\chi_i(p_i)$ for characters $\chi$ of modulus dividing $4\Delta(E)$
  - Legendre symbols $\left(\frac{p_i}{p_j}\right)$
  - $(-1)^\epsilon(p_i)\epsilon(p_j)$ with $\epsilon(p) = (p - 1)/2$
- Approximate inner sum
Inner Sum

Consider:

\[
\frac{1}{n!} \sum_{S_{N,n}} \prod_{i=1}^{n} \chi_i(p_i) \prod_{1 \leq i < j \leq n} \left( \frac{p_i}{p_j} \right)^{e_{i,j}} \prod_{1 \leq i < j \leq n} (-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}}
\]

- Expect lots of cancellation
- Some \( i \) so that however you fix \( p_j \) for \( j \neq i \) have a non-trivial character of \( p_i \)
- Let \( m \) be the number of such \( i \). Namely, the number of \( i \) so that one of:
  - \( e_{i,j} = 1 \) for some \( j \)
  - Modulus of \( \chi_i \) is more than 4
  - Modulus of \( \chi_i \) is 4 and \( d_{i,j} = 0 \) for all \( j \)
- Want to show: \( \text{Sum} \ll N \) if \( m \) is large
- Note: If \( m > 0 \) then average is 0 in the Swinnerton-Dyer sense
Warmup

Bound:

\[ \frac{1}{n!} \sum_{S_{N,n}} \prod_{i=1}^{n} \chi_i(p_i) \prod_{1 \leq i < j \leq n} (-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}} \]

- Induct on \( m \)
- Let \( Q(n, m) \) be the max of \( \left( \frac{1}{n!} \sum_{S_{N,n}} \text{character} \right) / N \)
- \( Q(n, 0) \leq \frac{|S_{N,n}|}{N \cdot n!} \leq O \left( \frac{1}{\sqrt{\log \log N}} \right) \)
- For \( m > 0 \), have some \( i \) so that summand depends non-trivially on \( p_i \) no matter what \( p_j \). Cases:
  - If \( p_i \) large, use standard character bounds
  - If \( p_i \) small, fix its value and bound recursively
Let $D$ be 4 times the largest modulus
Let worst Siegel zero be no worse than $1 - \beta^{-1}$
For any $C > 0$ and $K$ sufficiently large, let

$$B := \max \left( e^{(C+2)\beta \log \log(N)}, e^{K((C+2) \log(D) \log \log(DN))^2}, n \log^{C+2}(N) \right)$$

Standard bounds on character sums imply that the sum over terms with $p_i \geq B$ is at most $O(N \log^{-C}(N))$. 
For $p_i < B$ sum with $p_i = p$ is

$$\pm \frac{1}{n!} \sum_{S_{N/p,n-1}} \text{Stuff} \leq \frac{N}{p} \left( \frac{Q(n-1, m-1)}{n} \right)$$

Sum over such $p_i$ is at most

$$\frac{Q(n-1, m-1)}{n} \sum_{p<B} \frac{N}{p} = NO \left( \frac{\log \log(B)}{n} \right) Q(n-1, m-1)$$
Recursive Bound

\[ Q(n, 0) = O\left( \frac{1}{\sqrt{\log \log(N)}} \right) \]

\[ Q(n, m) \leq O(\log^{-c}(N)) + O\left( \frac{\log \log(B)}{n} \right) Q(n - 1, m - 1) \]

\[ Q(n, m) = \left( \frac{1}{\sqrt{\log \log(N)}} \right) \left( O\left( \frac{\log \log(B)}{n} \right)^m + O(\log^{-c}(N)) \right) \]
Full Sum

\[ \frac{1}{n!} \sum_{S_{N,n}} \prod_{i=1}^{n} \chi_i(p_i) \prod_{1 \leq i < j \leq n} \left( \frac{p_i}{p_j} \right)^{e_{i,j}} \prod_{1 \leq i < j \leq n} (-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}} \]

- Same idea as before
- \( Q(n, m, D) \) biggest possible value when characters have modulus at most \( D \) divided by \( N \)
- Use previous result as a base case if all \( e_{i,j} = 0 \)
- Otherwise if \( e_{i,j} = 1 \)
  - If \( p_i, p_j \) both large, bound directly (large sieve type result)
  - If one is small, fix and bound recursively
Details

- If $p_i, p_j > A$, sum at most $O(N \log(N) A^{-1/8})$
- Take $A = \log^{8C+8}(N)$
- If $p_i < A$ (similarly if $p_j < A$ or both less than $A$) have

$$\frac{1}{n} \sum_{p < A} \frac{NQ(n-1, m-1, pD)}{p} \leq O \left( \frac{\log \log(A)}{n} \right) NQ(n-1, m-1, pD)$$

- Problem: We may introduce new Siegel zeroes that mess up our base case
- Solution: Can only have one really bad Siegel zero, deal with it separately
Let $q$ be the modulus of the worst Siegel zero between $X = \log^C(N)$ and $Y = DA^n$.

Sum of terms with $q|4Db$ is at most $O(N/q) = O(N\log^{-C}(N))$.

For other terms, worst Siegel zero we need to deal with is either the worst Siegel zero with modulus less than $X$ or the second worst with modulus less than $Y$.

$$\beta \leq \max(O_\epsilon(X^\epsilon), O(\log(Y)))$$

$$\log \log(B) = o(\log \log(N))$$
Putting it Together

Let $Q'(n, m)$ be the worst possible sum over terms in $S_{N,n}$ so that $q \not| 4Dq$

\[
Q'(n, m) \leq O \left( \log^{-C}(N) \right) + O \left( \frac{\log \log(A)}{n} \right) Q'(n-1, m-1) + o(1)^m
\]

Since $m \leq n = O(\log \log(N))$, $\log^{-C}(N) < c^m$ if $C$ is sufficiently large

\[
Q'(n, m) \leq o(1)^m
\]
Remaining Terms

- When $m = 0$ don’t necessarily have cancellation.
- Have product of $(-1)^{\epsilon(p_i)\epsilon(p_j)}$ and $(-1)^{\epsilon(p_i)}$.
- Expect average to be the same as in the Swinnerton-Dyer sense.

**Lemma**

Let $f : ((\mathbb{Z}/4\mathbb{Z})^*)^n \to \mathbb{C}$ with $|f|_\infty \leq 1$. Then

$$\frac{1}{n!} \sum_{S_{N,n}} f(p_1, \ldots, p_n) = \frac{|S_{N,n}|}{n!} \bar{f} + O \left( \frac{N \log \log \log(N)}{\log \log(N)} \right).$$

**Proof idea.**

Write $f$ in the Fourier basis. Constant term gives main term in answer. Other terms bounded by previous results.
Summary

- We have

\[
\text{Average}(|\text{Sel}_2(E_b)|^k) = \frac{1}{|U|^k} \sum_{u_i \in U, w_i \in W} \text{Average(“character”).}
\]

- Holds for both Swinnerton-Dyer average and average over $S_{N,n}$

- Each individual character has approximately the same average in each context

- Need to show that the errors are not too large

- Bound the number of terms with small $m$
Legendre Symbols

- Trying to bound the number of terms with $m$ small
- Bound the number of terms with few Legendre symbols
- Where do Legendre symbols come from?
- $U$ has generators $(p_i, p_i, 1), (1, p_i, p_i)$
- $W$ has generators $((a_1 - a_2)(a_1 - a_3), b(a_1 - a_2), b(a_1 - a_3))_{p_i}$ and $(b(a_2 - a_1), (a_2 - a_1)(a_2 - a_3), b(a_2 - a_3))_{p_i}$
- Legendre symbol $\left(\frac{p_i}{p_j}\right)$ comes from dot products:
  - $(p_i, p_i, 1)$ or $(p_j, p_j, 1)$ with $((a_1 - a_2)(a_1 - a_3), b(a_1 - a_2), b(a_1 - a_3))_{p_i/p_j}$ OR
  - $(1, p_i, p_i)$ or $(1, p_j, p_j)$ with $(b(a_2 - a_1), (a_2 - a_1)(a_2 - a_3), b(a_2 - a_3))_{p_i/p_j}$
Split $U$ and $W$ into parts corresponding to each $p_i$:
- $U_i = \langle (p_i, p_i, 1), (1, p_i, p_i) \rangle$
- $W_i = W_{p_i}$

Each $U_i$ and each $W_i$ the same:
- $U_i \sim U_0 := \langle (p, p, 1), (1, p, p) \rangle$
- $W_i \sim W_0 := \langle ((a_1 - a_2)(a_1 - a_3), b(a_1 - a_2), b(a_1 - a_3)), (b(a_2 - a_1), (a_2 - a_1)(a_2 - a_3), b(a_2 - a_3)) \rangle$

Using this notation write
- $u \in U$ write as $(u_*, u_1, \ldots, u_n) \in U_* \times U_0^n$
- $w \in W$ write as $(w_*, w_1, \ldots, w_n) \in W_* \times W_0^n$

The power of $\left(\begin{array}{c} p_i \\ p_j \end{array}\right)$ appearing in $(-1)^{\langle u, w \rangle}$ is $\{u_i + u_j, w_i + w_j\}$, where $\{,\}$ is a perfect pairing on $U_0 \times W_0$. 
Legendre Symbols

- For out $k$-tuples $(u_i), (w_i) \in U^k \times W^k$, write as

  $$(u_i), (w_i) = (z_*, z_1, z_2, \ldots, z_n)$$

  $$\in (U_* \times W_*)^k \times ((U_0 \times W_0)^k)^n.$$ 

- Power of $\left( \frac{p_i}{p_j} \right)$ in $(-1)^{\sum \langle u_i, w_i \rangle}$ is $\phi(z_i + z_j)$, where $\phi$ is a non-degenerate quadratic form on $(U_0 \times W_0)^k$. 
Number of Legendre Symbols

Given $u_i, w_i$, call an index $i$ inactive if $p_i$ does not show up in any Legendre Symbols.

For $i, j$ inactive, $\phi(z_i + z_j) = 0$.

Let $T = \{ z_i : i \text{ inactive} \}$

$T$ must be contained in a translate of a Lagrangian subspace of $\phi$. So $|T| \leq 4^k$.

Must also hold for $T \cup \{ z_j \}$ for any $j$, so if there are some active indices, then $|T| < 4^k$. 
Contribution from Terms with Legendre Symbols

- Consider the contribution from terms with $\ell > 0$ active indices
- Each term contributes $o(1)^\ell N$ to inner sum
- Count the number of $(u_i), (w_i)$ for given $\ell$
  - Constant number of ways to choose $T, z_*$
  - $\binom{n}{\ell}$ ways to choose which $i$ active
  - $|T|^{n-\ell}$ ways to choose inactive $z_i$
  - $16^{k\ell}$ ways to choose active $z_i$

Total at most

$$O(1) \sum_{m} \binom{n}{\ell} (4^k - 1)^{n-\ell} 16^{k\ell} o(1)^\ell N$$

$$= O(N) \sum_{\ell} \binom{n}{\ell} (1 - 4^{-k})^{n-\ell} o(1)^\ell$$

$$= O(N)(1 - 4^{-k} + o(1))^n$$

$$= O(N)(1 - 4^{-k}/2)^n$$

$$= O(N \log^{-4^{-k}-1}(N))$$
For terms with no active indices:

- Finite outer sum over $T$ and $z_*$
- At most $4^{kn}$ ways to choose the $z_i$
- Have:

$$\sum_{U} \sum_{O_k} k^n \sum_{S_{N,n}} \frac{1}{n!} \text{character} = O_k \left( \frac{|S_{N,n}|}{n!} \right)$$

Furthermore, each character has the same average as it does in the Swinnerton-Dyer sense up to an error of $O \left( \frac{N \log \log \log(N)}{\log \log(N)} \right)$.

Thus,

$$\frac{1}{n!} \sum_{S_{N,n}} |\text{Sel}_2(E_b)|^k = \left( \sum_d \pi_d(n)2^{kd} \right) \frac{|S_{N,n}|}{n!} + O \left( \frac{N \log \log \log(N)}{\log \log(N)} \right).$$
Convergence Issues

- Have average of $|\text{Sel}_2(E_b)|^k$ over $S_{N,n}$ is roughly $\sum_d \pi_d(n)2^{kd}$.
- Want average to be $\sum_d \alpha_d 2^{kd}$
- Have $\pi_d(n) \to \alpha_d$
- Also have $\sum_d \pi_d(n)2^{(k+1)d} \leq C_k$
- Thus, $\sup_n (\pi_d(n)2^{kd}) \leq C_k 2^{-d}$
- By Dominated Convergence $\sum_d \pi_d(n)2^{kd} \to \sum_d \alpha_d 2^{kd}$
- Hence

$$\frac{1}{n!} \sum_{S_{N,n}} |\text{Sel}_2(E_b)|^k$$

$$= \left( \sum_d \alpha_d 2^{kd} + o(1) \right) \frac{|S_{N,n}|}{n!} + O \left( \frac{N \log \log \log(N)}{\log \log(N)} \right).$$
Moments

- Let $S_N$ be the set of $b \leq N$ so that:
  - $b$ squarefree
  - $(b, \Delta(E)) = 1$
  - The number of prime factors of $b$ is $\log \log(N) \pm \log \log^{3/4}(N)$ (almost all $b$ satisfy this)

- By summing the old results over all $n = \log \log(N) \pm \log \log^{3/4}(N)$,

\[
\sum_{S_N} |\text{Sel}_2(E_b)|^k = |S_N| \left( \sum_d \alpha_d 2^{kd} + o(1) \right) + O \left( \frac{N \log \log \log(N)}{\log \log^{1/4}(N)} \right).
\]

or,

\[
\lim_{N \to \infty} \frac{\sum_{S_N} |\text{Sel}_2(E_b)|^k}{|S_N|} = \sum_d \alpha_d 2^{kd}.
\]
Moments alone are not enough to determine densities

Enough if you also know:

- Never rank 0 or 1
  - Follows from the fact that we have full 2-torsion
- Equal densities of even and odd ranks
  - Is true because the parity of \( \text{rank}(\text{Sel}_2(E_b)) \) is determined by some non-trivial character of \( b \)
Conclusions

- We have proven results on the asymptotic density of twists of a curve with full 2-torsion and no cyclic 4-isogeny that have 2-Selmer groups of given rank.
- We have developed techniques for converting results about Swinnerton-Dyer-type densities into results about honest densities.
- A number of other recent results have talked about the ranks of 2-Selmer or 2-isogeny-Selmer of various families of curves using Swinnerton-Dyer type densities. Our techniques can hopefully be generalized to enhance these results to cover natural densities.
