On the Ranks of the 2-Selmer Groups of Twists of a Given Elliptic Curve

Daniel M. Kane

September 8, 2010

1 Introduction

Let c_1, c_2, c_3 be distinct rational numbers. Let Γ be the elliptic curve defined by the equation

$$y^2 = (x - c_1)(x - c_2)(x - c_3).$$

We makes the additional technical assumption that none of the $(c_i - c_j)(c_i - c_k)$ are squares. This is equivalent to saying that Γ is an elliptic curve over $\mathbb{Q}$ with complete 2-torsion and no cyclic subgroup of order 4 defined over $\mathbb{Q}$. For b a square-free number, let Γ_b be the twist defined by the equation

$$y^2 = (x - bc_1)(x - bc_2)(x - bc_3).$$

Let S be a finite set of places of $\mathbb{Q}$ including $2, \infty$ and all of the places at which Γ has bad reduction. Let D be a positive integer divisible by 8 and by the primes in S. Let $S_2(\Gamma_b)$ denote the 2-Selmer group of the curve Γ_b. We will be interested in how the rank varies with b and in particular in the asymptotic density of b's so that $S_2(\Gamma_b)$ has a given rank.

The parity of $\dim(S_2(\Gamma_b))$ depends only on the class of b in $\prod_{\nu \in S} \mathbb{Q}_\nu^*/(\mathbb{Q}_\nu^*)^2$. We claim that for exactly half of these values this dimension is odd and exactly half of the time it is even.

Lemma 1. *For exactly half of the classes c in $(\mathbb{Z}/D)^*/((\mathbb{Z}/D)^*)^2$, if we pick b a positive representative of the class c then $\dim(S_2(\Gamma_b))$ is even.*

Let $b = p_1 p_2 \ldots p_n$ where p_i are distinct primes relatively prime to D. The rank of $S_2(\Gamma_b)$ is easily seen to depend only on the images of the p_i in $(\mathbb{Z}/D)^*/2(\mathbb{Z}/D)^*$ and upon which p_i are quadratic residues modulo which p_j. There are $2^{n|S| + \binom{n}{2}}$ possible sets of values for these. Let $\pi_d(n)$ be the fraction of this set of possibilities that cause $S_2(\Gamma_b)$ to have rank exactly d. Then the main Theorem of [4] together with Lemma 1 implies that:

Theorem 2.

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

where $\alpha_0 = \alpha_1 = 0$ and $\alpha_{n+2} = \frac{2^n}{\prod_{j=1}^{n}(2^j - 1) \prod_{j=0}^{\infty}(1 + 2^{-j})}$.

This tells us information about the asymptotic density of twists of Γ whose 2-Selmer group has a particular rank. Unfortunately, this asymptotic density is taken in a somewhat awkward way by letting the number of primes dividing b go to infinity. In this paper we prove the following more natural version of Theorem 2:

Theorem 3.

$$\lim_{N\to\infty} \frac{\#\{b \leq N : b \text{ square-free, } (b,D)=1 \text{ and } \dim(S_2(\Gamma_b))=d\}}{\#\{b\leq N : b \text{ square-free and } (b,D)=1\}} = \alpha_d.$$

Applying this to twists of Γ by divisors of D and noting that twists by squares do not affect the Selmer rank we have that

Corollary 4.

$$\lim_{N\to\infty} \frac{\#\{b\leq N : \dim(S_2(\Gamma_b))=d\}}{N} = \alpha_d.$$

and

Corollary 5.

$$\lim_{N\to\infty} \frac{\#\{-N\leq b\leq N : \dim(S_2(\Gamma_b))=d\}}{2N} = \alpha_d.$$

Our technique is fairly straightforward. Our goal will be to prove that the average moments of the size of the Selmer groups will be as expected. As it turns out, this will be enough to determine the probability of seeing a given rank. In order to analyze the Selmer groups we follow the method described in [4]. Here the 2-Selmer group of Γ_b can be expressed as the intersection of two Lagrangian subspaces, U and W, of a particular symplectic space, V, over $\mathbb{F}_2$. Although U, V and W all depend on b, once the number of primes dividing b has been fixed along with its congruence class modulo D, these spaces can all be written conveniently in terms of the primes, p_i, dividing b, which we think of as formal variables. Using the formula $|U\cap W| = \frac{1}{\sqrt{|V|}}\sum_{u\in U, w\in W}(-1)^{u\cdot w}$, we reduce our problem to bounding the size of the "characters" $(-1)^{u\cdot w}$ when averaged over b. These "characters" turn out to be products of Dirichlet characters of the p_i and Legendre symbols of pairs of the p_i. The bulk of our analytic work is in proving these bounds.

In Section 2 we introduce some basic concepts that will be used throughout. In Section 3 we will prove the necessary character bounds. We use these bounds in Section 4 to establish the average moments of the size of the Selmer groups. Finally in Section 5 we explain how these results can be used to prove our main Theorem.

2 Preliminaries

For an integer m, let $\omega(m)$ be the number of prime divisors of m. Recall that among numbers $m \leq N$ that $\omega(m)$ is concentrated around $\log\log N$. In particular the fraction of such numbers that have $|\omega(m)-\log\log N| \leq (\log\log N)^{3/4}$

goes to 1 as $N \to \infty$. We will make use of this fact throughout noting that we only need to deal with b with $\omega(b)$ roughly $\log\log N$.

3 Character Bounds

Our main purpose in this section will be to prove the following Propositions:

Proposition 6. *Fix positive integers D, n, N with $4|D$, $n = \Theta(\log\log N)$, $D = O(1)$. Let $c > 0$ be a constant. Let $d_{i,j}, e_{i,j} \in \mathbb{Z}/2$ for $i, j = 1, \ldots, n$ with $e_{i,j} = e_{j,i}, d_{i,j} = d_{j,i}, e_{i,i} = d_{i,i} = 0$ for all i, j. Let χ_i be a quadratic character with modulus dividing D for $i = 1, \ldots, n$. Let m be the number of indices i so that at least one of the following hold:*

- *$e_{i,j} = 1$ for some j or*
- *χ_i has modulus not dividing 4 or*
- *χ_i has modulus exactly 4 and $d_{i,j} = 0$ for all j.*

Let $\epsilon(p) = (p-1)/2$. Then if $m > 0$

$$\left| \frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \\ \text{distinct primes} \\ (D,p_i)=1 \\ \prod_i p_i \leq N}} \prod_i \chi_i(p_i) \prod_{i<j} (-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}} \prod_{i<j} \left(\frac{p_i}{p_j}\right)^{e_{i,j}} \right| = O\left(Nc^m\right). \quad (1)$$

Note that m is the number of indices i so that no matter how we fix the values of p_j for the $j \neq i$ that the summand on the left hand side of Equation 1 still depends on p_i.

Essentially we are summing over all $b = \prod_i p_i$ with $\omega(b) = n$ and $b \leq N$, where the summand is a "character" defined by the $\chi_i, d_{i,j}$ and $e_{i,j}$. The $\frac{1}{n!}$ accounts for the different possible reorderings of the p_i.

Proposition 7. *Let n, N, D be positive integers with $D = O(1)$, $n = \Theta(\log\log N)$. Let $G = ((\mathbb{Z}/D)^*/2(\mathbb{Z}/D)^*)^n$. Let $f : G \to \mathbb{C}$ be a function with $|f|_\infty \leq 1$. Then*

$$\frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \\ \text{distinct primes} \\ (D,p_i)=1 \\ \prod_i p_i \leq N}} f(p_1, \ldots, p_n) \quad (2)$$

$$= \left(\frac{1}{|G|} \sum_{g \in G} f(g) \right) \left(\frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \\ \text{distinct primes} \\ (D,p_i)=1 \\ \prod_i p_i \leq N}} 1 \right) + O\left(\frac{N (\log\log\log N)^2}{\log\log N} \right).$$

Note that again, the sum can be thought of as a sum over all $b = \prod_i p_i$ with $b \leq N$ and $\omega(b) = n$.

We begin with a Proposition that gives a more precise form of Proposition 6 in the case when the $e_{i,j}$ are all 0.

Proposition 8. *Let D, n, N be integers with $4|D$. Let $C > 0$ be a constant. Let $d_{i,j} \in \mathbb{Z}/2$ for $i, j = 1, \ldots, n$ with $d_{i,j} = d_{j,i}, d_{i,i} = 0$. Let χ_i be a quadratic character of modulus dividing D for $i = 1, \ldots, n$. Suppose that no Dirichlet character of modulus dividing D has an associated Siegel zero larger than $1-\beta^{-1}$. Let $B = \max(e^{3C\beta \log\log N}, e^{(\log D)^2(\log\log N)^4})$. Suppose that $B^n < \sqrt{N}$. Let m be the number of indices i so that either:*

- *χ_i does not have modulus dividing 4 or*
- *χ_i has modulus exactly 4 and $d_{i,j} = 0$ for all j.*

Then

$$\left| \frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \\ \text{distinct primes} \\ (D,p_i)=1 \\ \prod_i p_i \leq N}} \prod_i \chi_i(p_i) \prod_{i<j} (-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}} \right| = N\left(O\left(\frac{\log\log B}{n}\right)^m + O(\log N)^{-C} \right). \tag{3}$$

Note once again that m is the number of i so that if the values of p_j for $j \neq i$ are all fixed, the resulting summand will still depend on p_i.

Proof. We proceed by induction on n. If $m = 0$, we can bound the left hand side of Equation 3 by N. This is because there are at most N possible values of $p_1 \cdots p_n$, each such product shows up $n!$ times and thus contributes at most 1 to the left hand side.

For $m > 0$ we proceed as follows. We pick a p_i that is contributing to the value of m. In other words, we pick a p_i so that either χ_i does not have modulus dividing 4 or so that the modulus of χ_i is exactly 4 and $d_{i,j} = 0$ for all j.

We break the sum into parts based on whether p_i is larger than B. For $p_i > B$ we will argue based on standard results about sums of characters. For $p_i < B$ this will not be sufficient since the range of possible values of p_i is too small. Instead we note that that only a $O\left(\frac{\log\log B}{\log\log N}\right)$ proportion of terms have p_i in this range, and that after fixing a value of p_i we are left with a similar sum only with n and m reduced.

First we handle the case where $p_i > B$. We begin by partitioning $(B, N]$ into intervals I_ℓ of the form $(A, A(1 + \Theta(\log(M)^{-C}))]$. We begin by throwing away all terms in our summation in which if p_i were replaced by the largest prime in its interval the resulting value of $p_1 \cdots p_n$ would exceed N. We note that for such terms it must be the case that $p_1 \cdots p_n \geq N(1 - O(\log N)^{-C})$.

Since there are at most $NO(\log N)^{-C}$ such products the sum over such terms is at most $NO(\log N)^{-C}$. To bound the remaining terms, we fix p_j for all $j \neq i$ and fix the interval in which p_i lies. We are left with a sum over all primes $p \in I$ (with possibly n exceptions coming from the p_j) of $\chi(p)$, where $\chi(p) = \chi_i(p) \prod_{j \neq i} (-1)^{\epsilon(p)\epsilon(p_j)d_{i,j}}$. It should be noted that χ is a non-trivial Dirichlet character of modulus dividing D. [2] Theorem 5.27 implies that for any X that

$$\sum_{n \leq X} \chi(n)\Lambda(n) = XO\left(X^{-\beta^{-1}} + \exp\left(\frac{-c\sqrt{\log(X)}}{\log D}\right)(\log D)^4\right)$$

for some absolute constant c. Using standard techniques this implies that our sum over p_i is

$$AO\left(A^{-\beta^{-1}} + \exp\left(\frac{-c\sqrt{\log(A)}}{\log D}\right)(\log D)^4\right).$$

Using the fact that $A \geq B \geq e^{3C\beta \log\log N}, e^{(\log D)^2(\log\log N)^4}$, this is

$$AO\left(e^{-3C\log\log N} + e^{-c(\log\log N)^2}(\log D)^4 + \frac{\log N}{B}\right).$$

Note that unless $\log D = O(\log N)$ that $B > e^{(\log D)^2} > N$ and this case is trivial. Hence the above quantity is at most

$$AO((\log N)^{-3C}).$$

Notice that for each of these terms there are at most $\frac{N}{A}$ possible values for $\prod_{j \neq i} p_j$. Each of these products is represented $(n-1)!$ times. Hence after fixing the interval in which p_i lies our sum is at most

$$\left(\frac{1}{n!}\right)\left(\frac{N(n-1)!}{A}\right) AO\left((\log N)^{-3C}\right) \leq NO((\log N)^{-3C}).$$

Noticing that there are $O((\log N)^{C+1})$ intervals to deal with we find that the sum of these terms is $NO((\log N)^{-C})$.

Next we consider the contribution from terms where $p_i \leq B$. We notice that after fixing p_i we are left with a sum similar to the one with started with with a few exceptions. Namely:

- N is now smaller by a factor of p.
- n is smaller by 1.
- There is an additional factor of $\frac{1}{n}$ in front of the summation.
- $\chi_j(p)$ is replaced by $\chi_j(p)(-1)^{d_{i,j}\epsilon(p_i)\epsilon(p)}$.

- m may change, but is at least its old value minus 1.

Having fixed this p_i, we now have a bound of

$$\frac{N}{np_i}E$$

where E is

$$O\left(\frac{\log\log B}{n}\right)^{m-1} + O((\log N)^{-C}).$$

Summing over p_i prime less than B we get

$$\frac{NO(\log\log B)}{n}E = N\left(O\left(\frac{\log\log B}{\log\log N}\right)^{m} + O((\log N)^{-C})\right).$$

Unfortunately we need to be a little more careful since when we fix p_i the remaining values of n, N, B are no longer the same. On the other hand, the value of B only decreases and the value of N never shrinks below $NB^{-n} > \sqrt{N}$. Hence we may think of all of our $O(\log N)^{-C}$ and $O(\log\log B)$ terms as using the original N and B. Then a straightforward computation of our errors produces a bound of N times

$$\begin{aligned}
O(\log N)^{-C}&\sum_{k=0}^{m-1}\frac{O(\log\log B)^k}{n(n-1)\cdots(n-k+1)} + \frac{O(\log\log B)^m}{n(n-1)\cdots(n-m+1)}\\
&\le O(\log N)^{-C}\sum_{k=0}^{m} O\left(\frac{\log\log B}{n}\right)^{k} + O\left(\frac{\log\log B}{n}\right)^{m}\\
&\le nO(\log N)^{-C} + nO(\log N)^{-C}O\left(\frac{\log\log B}{n}\right)^{m} + O\left(\frac{\log\log B}{n}\right)^{m}.
\end{aligned}$$

Noting that the assumption $B^n < \sqrt{N}$ implies that $n = O(\log N)$ and replacing C by $C+1$, we get the desired bound.

Note that this argument can be made into a rigorous induction by introducing a new variable, M, equal to the "original" value on N. We then set $B = \max(e^{3C\beta\log\log M}, e^{(\log D)^2(\log\log M)^4})$ and require that $N \le M \le (B^{-n}N)^2$. We allow for a set, S (of size at most $O(\log M)$) of disallowed primes corresponding to primes that have already been fixed, allow m to be an integer smaller than the value we specify and prove a bound of the form:

$$N\left(O(\log M)^{-C}\sum_{k=0}^{m-1}\frac{O(\log\log B)^k}{n(n-1)\cdots(n-k+1)} + \frac{O(\log\log B)^m}{n(n-1)\cdots(n-m+1)}\right).$$

□

We are now prepared to prove Proposition 7

Proof. First note that we can assume that $4|D$. This is because if that is not the case, we can split our sum up into two cases, one where none of the p_i are 2, and one where one of the p_i is 2. In either case we get a sum of the same form but now can assume that D is divisible by 4. We assume this so that we can use Proposition 8.

It is clear that the error in Equation 2 is

$$\frac{1}{|G|}\left(\sum_{\chi\in\widehat{G}\setminus\{1\}}\left(\frac{1}{n!}\sum_{\substack{p_1,\ldots,p_n\\ \text{distinct primes}\\ (D,p_i)=1\\ \prod_i p_i\le N}}\chi(p_1,\ldots,p_n)\right)\left(\sum_{g\in G}f(g)\chi(g)\right)\right).$$

Using Cauchy-Schwartz we find that this is at most

$$\frac{1}{|G|}\sqrt{|G|}|f|_2\sum_{\chi\in\widehat{G}\setminus\{1\}}\left|\frac{1}{n!}\sum_{\substack{p_1,\ldots,p_n\\ \text{distinct primes}\\ (D,p_i)=1\\ \prod_i p_i\le N}}\chi(p_1,\ldots,p_n)\right|^2.$$

We note that $|f|_2\le\sqrt{|G|}$ and hence that $\frac{1}{|G|}\sqrt{|G|}|f|_2\le 1$. Bounding the character sum using Proposition 8 we get

$$\sum_{\chi\in\widehat{G}\setminus\{1\}}O\left(\frac{\log\log\log N}{\log\log N}\right)^{2\cdot\langle\text{Number of components on which }\chi\text{ is non-trivial}\rangle}.$$

Since each component of χ can either be trivial or have one of finitely many non-trivial values (which gives a contribution of $O((\log\log\log N)^2/(\log\log N)^2))$ and this can be chosen independently for each component we get that this is

$$\begin{aligned}\left(1+O\left(\frac{\log\log\log N}{\log\log N}\right)^2\right)^n-1&=\exp\left(O\left(\frac{(\log\log\log N)^2}{\log\log N}\right)\right)-1\\&=O\left(\frac{(\log\log\log N)^2}{\log\log N}\right).\end{aligned}$$

□

In order to prove Proposition 6 we will need the following Lemma:

Lemma 9. *Let Q and N be positive integers with $Q^2\ge N$. Let $a:\{1,2,\ldots,N\}\to\mathbb{C}$ be a function supported on square-free numbers. Then we have that*

$$\sum_{\substack{\chi\text{ quadratic character}\\ \text{of modulus }\le Q}}\left|\sum_{n=1}^N a_n\chi(n)\right|^2=O\left(Q\sqrt{N}|a|^2\right)$$

where $|a|^2 = \sum_{n=1}^N |a_n|^2$ *is the squared* L^2 *norm.*

Proof. Let M be a positive integer so that $Q^2 \leq NM^2 \leq 4Q^2$. Let $b : \{1,2,\ldots,M^2\} \to \mathbb{C}$ be the function $b_{n^2} = \frac{1}{M}$ and $b = 0$ on non-squares. Let $c = a*b$ be the multiplicative convolution of a and b. Note that since a is supported on square-free numbers and b supported on squares that $|c|^2 = |a|^2|b|^2 = |a|^2/M$. Applying the multiplicative large sieve inequality (see [2] Theorem 7.13) to c we have that

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \left| \sum_n c_n \chi(n) \right|^2 \leq (Q^2 + NM^2 - 1)|c|^2. \tag{4}$$

Now the right hand side is easily seen to be $O(Q^2)|a|^2/M = O(Q^2|a|^2/(\sqrt{Q^2/N})) = O(Q\sqrt{N}|a|^2)$. For the left hand side we may note that it only becomes smaller if we remove the $\frac{q}{\phi(q)}$ or ignore the characters that are not quadratic. For quadratic characters χ note that

$$\sum_n c_n \chi(n) = \left(\sum_n a_n \chi(n) \right) \left(\sum_n b_n \chi(n) \right) = \sum_n a_n \chi(n).$$

Where the last equality above follows from the fact that χ is 1 on squares. Hence the left hand side of Equation 4 is at least

$$\sum_{\substack{\chi \text{ quadratic character} \\ \text{of modulus } \leq Q}} \left| \sum_{n=1}^N a_n \chi(n) \right|^2.$$

This completes our proof. ∎

We are now prepared to prove Proposition 6

Proof. Our proof will be similar to the proof of Proposition 8. Again we will use induction on n, this time using Proposition 8as our base case. Unfortunately, for this application to work, we will need to pay closer attention to the possibility of Siegel zeroes. First pick a C so that $c^n \ll (\log N)^{-C}$ (we can do this since $n = O(\log\log N)$). Let Q be the modulus of the quadratic character of modulus between $\log^C N$ and $e^{(\log\log N)^4}$, (which is bigger than $De^{n(\log\log N)^2}$) with the largest Siegel zero among such characters (if any exist). Notice that the sum over terms where $Q|D\prod_i p_i$ is $O(N/Q) = O(N\log^{-C}(N))$ and can thus be ignored. Notice that by [2] Theorem 5.28 that any other quadratic character of modulus less than $De^{n(\log\log N)^2}$ does not have any Siegel zero larger than $1-\Omega((\log N)^{-\epsilon})$, for any $\epsilon > 0$, where the implied constant in the Ω depends on C and ϵ but not N. We now throw out all terms in the sum in which $Q|D\prod_i p_i$.

We proceed by induction on n. If $e_{i,j} = 0$ for all i,j we use Proposition 8. Otherwise we pick an i,j so that $e_{i,j} = 1$. As in the proof of Proposition 8 we break our sum into cases based on whether or not p_i and p_j are greater than

$B = e^{(\log\log N)^2}$. As before, if either p_i is small, we fix the value of p_i and are left with a similar looking sum over the remaining primes. This time though if both p_i and p_j are large, we use Lemma 9 to provide our bound.

We first deal with the case where both p_i and p_j are greater than B. We partition $(B, N]$ into intervals of the form $(A, A(1+\Theta(\log M)^{-C}))]$. We break our sum up by conditioning which of these intervals p_i and p_j land in. Suppose that p_i lands in I_i and p_j lands in I_j. Next we throw away all terms in our sum where replacing p_i and p_j with the largest primes in I_i and I_j respectively would cause $\prod_k p_k > N$. This only happens when the current value of $\prod_k p_k$ is at least $N(1-\Theta(\log(N))^{-C})$ and hence the sum of these terms contributes a total of $O(N(\log N)^{-C})$ and may be ignored. If we are not in this case, fixing all of the p_k for $k \neq i, j$ we are left with a sum over all pairs of primes (p_i, p_j) in $I_i \times I_j$ except for those where

- p_i or p_j equals one of the other p_k,
- p_i or p_j is the remaining prime factor in Q not in $D\prod_{k\neq i,j} p_k$ or
- $p_i p_j$ is exactly the pair of prime factors of Q missing from $D\prod_{k\neq i,j} p_k$.

Assuming without loss of generality that either $i < j$, the summand is

$$\chi_i(p_i)\chi_j(p_j)(-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}}\left(\frac{p_i}{p_j}\right).$$

Notice that the first two of the excluded cases rule out $O(\log\log N)$ possible values for p_i and p_j. The last only excludes a single term and can thus be ignored. Suppose that I_i starts at A_i and I_j starts at A_j. Let S_i be the set of primes in I_i not excluded by the above and S_j the set of primes in I_j not excluded by the above. We wish to bound:

$$\sum_{p_i\in S_i, p_j\in S_j} \chi_i(p_i)\chi_j(p_j)(-1)^{\epsilon(p_i)\epsilon(p_j)d_{i,j}}\left(\frac{p_i}{p_j}\right). \tag{5}$$

Suppose without loss of generality that $A_j \geq A_i$ (otherwise we can switch i and j using quadratic reciprocity). Let a be the function supported on S_i defined by $a(p_i) = \chi_i(p_i)$. Let b be the function sending quadratic characters to complex numbers so that if χ is the character $\chi(n) = (-1)^{\epsilon(n)\epsilon(p_j)d_{i,j}}\left(\frac{n}{p_j}\right)$ for some $p_j \in S_j$ then $b(\chi) = \chi_j(p_j)$, and $b(\chi) = 0$ if χ is not of that form. Then the expression in Equation 5 equals

$$\sum_\chi b(\chi)\sum_n a_n\chi(n).$$

Noting that b is supported on characters of modulus at most $5A_j$, by Cauchy-Schwartz this is at most

$$\left(\sum_\chi |b(\chi)|^2\right)^{1/2}\left(\sum_{\substack{\chi \text{ quadratic character} \\ \text{of modulus at most } 5A_j}}\left|\sum_n a_n\chi(n)\right|^2\right)^{1/2}.$$

Applying Lemma 9 to the second sum we get that this is at most

$$O\left(|S_j|A_j\sqrt{A_i}|S_i|\right)^{1/2} = O(A_jA_i^{3/4}).$$

After fixing I_i and I_j the number of possible products $\prod_{k\neq i,j} p_k$ is at most $\frac{N}{A_iA_j}$. Hence the number of ways of picking those terms is at most $\frac{(n-2)!N}{A_iA_j}$. Therefore the value of $\frac{1}{n!}$ times our sum in these cases is at most

$$\frac{N}{A_iA_j}O(A_jA_i^{3/4}) = O(NA_i^{-1/4}) = O(N(\log N)^{-5C}).$$

The number of intervals in our partition is $O((\log N)^{C+1})$, hence summing over all pairs of these the contribution from these terms is $O(N(\log N)^{-C})$.

Next we bound the terms in the sum where $p_i \leq B$. We note that after fixing this p_i we are left with a sum similar to the one we started with but with the following modifications:

- N is reduced by a factor of p_i
- The values of the χ_j are changed.
- D is increased by a factor of p_i
- n is decreased by 1
- m is changed but is at least its old value minus 1
- We have an additional factor of $\frac{1}{n}$ out front

We suspect that after fixing p_i the remaining sum gives a contribution of at most $O\left(\frac{Nc^{m-1}}{np_i}\right)$. Summing over $p_i \leq B$ we get $O\left(\frac{Nc^{m-1}(\log\log\log N)}{n}\right)$. We get a similar bound for the sum of terms with $p_j \leq B$, and for the sum of terms with both p_i and p_j at most B we get the bound $O\left(\frac{Nc^{m-2}(\log\log\log N)^2}{n^2}\right)$. Hence by inclusion-exclusion the sum of the terms where either p_i or p_j is less than B should be at most

$$O\left(\frac{Nc^{m-1}\log\log\log N}{n}\right).$$

So as long as we have at least one non-zero value of $e_{i,j}$ we can relate our sum to similar ones with smaller n. We get $NO((\log N)^{-C})$ plus $O\left(\frac{\log\log\log N}{n}\right)$ times an appropriate average of simpler sums. As in the proof of Proposition 8 we need to be careful since our values of N, B and D change at each iteration. Note that N gets smaller at each step but will never shrink by a factor of more than $B^n = \exp(O(\log\log N)^3)$. D will always increase, but will not increase by more than a similar factor.

At some point we will find ourselves reduced to a case where all of the $e_{i,j}$ are 0. At this point we obtain a bound using Proposition 8. Since we have arranged things so that no character with modulus dividing D has a Siegel 0 more than $1-\Omega(\log N)^{-\epsilon}$, we may apply Proposition 8 with $\log B = O(\max(3C(\log N)^{\epsilon}\log\log N, (\log\log N)^{10}))$. Hence $\log\log B = o(\log\log N)$. This gives us a final bound of N times

$$\begin{aligned}
O((\log N)^{-C}) \sum_{k=0}^{n} \frac{O(\log\log\log N)^k}{n(n-1)\cdots(n-k+1)} &+ \sum_{k=0}^{m} \frac{o(\log\log N)^{m-k} O(\log\log\log N)^k}{n(n-1)\cdots(n-m+1)} \\
&\leq O((\log N)^{-C}) + \left(\frac{o(\log\log N)}{n}\right)^m \\
&\leq c^m.
\end{aligned}$$

In order to make the above into a rigorous induction, we need to do a few things. We first throw away all terms in our sum where $Q|D\prod_i p_i$. Next we need a new variable M to represent our "original" value of N. We want that $N \leq M \leq ND^n e^{n^2(\log\log M)^2}$. We relax our bound on D subject still to the equation in the last sentence. We allow for m to be any positive integer as long as it is at most the one specified, and require that $n-m = \Omega(\log\log M)$. We change where we split our cases so that now we split the sum based on which of p_i and p_j are more than $e^{(\log\log M)^2}$. Lastly we prove a bound of the form

$$N\left(O((\log M)^{-C}) \sum_{k=0}^{n} \frac{O(\log\log\log M)^k}{n(n-1)\cdots(n-k+1)} + \sum_{k=0}^{m} \frac{o(\log\log M)^{m-k} O(\log\log\log M)^k}{n(n-1)\cdots(n-m+1)}\right)$$

instead of the old bound. But this is largely a more complicated recasting of the argument above to make it fit the mold of a formal induction. $\square$

4 Average Sizes of Selmer Groups

Here we use the results from the previous section to prove the following Proposition:

Proposition 10. *Let Γ be an elliptic curve as described above. Let S be a finite set of places containing $2, \infty$ and all of the places where Γ has bad reduction. Let x be either -1 or a power of 2. Let $\omega(m)$ denote the number of prime factors of m. Say that $(m,S)=1$ if m is an integer not divisible by any of the finite places in S. Then*

$$\lim_{N\to\infty} \frac{\sum_{\substack{b\leq N \text{ square-free} \\ |\omega(b)-\log\log N|<(\log\log N)^{3/4} \\ (b,S)=1}} x^{\dim(S_2(\Gamma_b))}}{\sum_{\substack{b\leq N \text{ square-free} \\ |\omega(b)-\log\log N|<(\log\log N)^{3/4} \\ (b,S)=1}} 1} = \sum_n x^n \alpha_n.$$

This says that the k^{th} moment of $S_2(\Gamma_b)$ averaged over $b \leq N$ with $|\omega(b) - \log\log N| \leq (\log\log N)^{3/4}$ is what you would expect it to be by Theorem 3, and that averaged over the same b's that the rank of the Selmer group is odd half of the time. The latter part of the Proposition follows from Lemma 1, which we prove now:

proof of Lemma 1. First we replace Γ by a twist so that $c_i - c_j$ are pairwise relatively prime integers. It is now the case that Γ has everywhere good or multiplicative reduction, and we are now concerned with $\dim(S_2(\Gamma_{db}))$ for some constant $d|D$. By [1] Theorem 2.3, and [3] Corollary 1 we have that $\dim(S_2(\Gamma_{bd})) \equiv \dim(S_2(\Gamma)) \pmod 2$ if and only if $(-1)^x \chi_{bd}(-N) = 1$ where x is the number of primes dividing d, N is the product of the primes not dividing d at which Γ has bad reduction, and χ_{bd} is the quadratic character corresponding to the extension $\mathbb{Q}(\sqrt{bd})$. From this the Lemma follows immediately. $\square$

In order to prove the rest of Proposition 10 we will need to come up with a way to talk about the Selmer groups of twists of Γ. We follow the treatment given in [4]. Let $b = p_1 \cdots p_n$ where p_i are distinct primes relatively prime to S (we leave which primes unspecified for now). Let $B = S \cup \{p_1, \ldots, p_n\}$. For $\nu \in B$ let V_ν be the subspace of $(u_1, u_2, u_3) \in (\mathbb{Q}_\nu^*/(\mathbb{Q}_\nu^*)^2)^3$ so that $u_1u_2u_3 = 1$. Note that V_ν has a symplectic form given by $(u_1, u_2, u_3) \cdot (v_1, v_2, v_3) = \prod_{i=1}^3 (u_i, v_i)_\nu$, where $(u_i, v_i)_\nu$ is the Hilbert Symbol. Let $V = \prod_{\nu \in B} V_\nu$ be a symplectic $\mathbb{F}_2$-vector space of dimension $2M$.

There are two important Lagrangian subspaces of V. The first, which we call U, is the image in V of $(\mathfrak{o}_B^*/(\mathfrak{o}_B^*)^2)^3$. The other, which we call W, is given as the product of W_ν over $\nu \in B$, where W_ν consists of points of the form $(x - bc_1, x - bc_2, x - bc_3)$ for $(x, y) \in \Gamma_b$. Note that we can write $W = W_S \times W_b$ where $W_S = \prod_{\nu \in S} W_\nu$ and $W_b = \prod_{\nu | b} W_\nu$. The the Selmer group is given by

$$S_2(\Gamma_b) = U \cap W.$$

Let U' be the $\mathbb{F}_2$-vector space generated by the symbols ν, ν' for $\nu \in S$ and p_i, p_i' for $1 \leq i \leq n$. There is an isomorphism $f : U' \to U$ given by $f(\infty) = (-1, -1, 1), f(\infty') = (1, -1, -1), f(p) = (p, p, 1), f(p') = (1, p, p)$.

Note also that W_{p_i} is generated by $((c_1 - c_2)(c_1 - c_3), b(c_1 - c_2), b(c_1 - c_3))$ and $(b(c_3 - c_1), b(c_3 - c_2), (c_3 - c_1)(c_3 - c_2))$. If we define W' to be the $\mathbb{F}_2$-vector space generated by the symbols p_i, p_i' for $1 \leq i \leq n$, then there is an isomorphism $g : W' \to W_b$ given by $g(p_i) = ((c_1 - c_2)(c_1 - c_3), b(c_1 - c_2), b(c_1 - c_3)) \in W_{p_i}$ and $g(p_i') = (b(c_3 - c_1), b(c_3 - c_2), (c_3 - c_1)(c_3 - c_2)) \in W_{p_i}$.

Let $G = \prod_{\nu \in S \setminus \infty} \mathfrak{o}_\nu^*/(\mathfrak{o}_\nu^*)^2$. Note that if b is positive W_S is determined by the restriction of b to G. So for $c \in G$ let $W_{S,c}$ be W_S for such b. Let $W_c' = W_{S,c} \times W'$. Then we have a natural map $g_c : W_c' \to V$ that is an isomorphism between W_c' and W if b restricts to c.

We are now ready to prove Proposition 10.

Proof. For $x = -1$ this Proposition just says that the parity is odd half of the time, which follows from Lemma 1. For $x = 2^k$ this says something about the expected value of $|S_2(\Gamma_b)|^k$. For $x = 2^k$ we will show that for each $n \in (\log\log N - (\log\log N)^{3/4}, \log\log N + (\log\log N)^{3/4})$ that

$$\sum_{\substack{b \le N \\ b \text{ square-free} \\ \omega(b)=n \\ (b,S)=1}} |S_2(\Gamma_b)|^k = \left(\sum_{\substack{b \le N \\ b \text{ square-free} \\ \omega(b)=n \\ (b,S)=1}} 1 \right) \left(\sum_m \alpha_m (2^k)^m + \delta(n,N)\right) + O\left(\frac{N(\log\log\log N)^2}{\log\log N} \right).$$

Where $\delta(n,N)$ is some function so that $\lim_{N\to\infty} \delta(n,N) = 0$. Summing over n and noting that there are $\Omega(N)$ values of $b \le N$ square-free with $|\omega(b) - \log\log N| < (\log\log N)^{3/4}$, and $(b,S) = 1$ gives us our desired result.

In order to do this we need to better understand $|S_2(\Gamma_b)| = |U \cap W|$. For $v \in V$ we have since U is Lagrangian of size 2^M,

$$\begin{aligned} \frac{1}{2^M} \sum_{u \in U} (-1)^{u \cdot v} &= \begin{cases} 1 \text{ if } v \in U^\perp \\ 0 \text{ else} \end{cases} \\ &= \begin{cases} 1 \text{ if } v \in U \\ 0 \text{ else} \end{cases} . \end{aligned}$$

Hence

$$\begin{aligned} |S_2(\Gamma_b)| &= |U \cap W| \\ &= \#\{w \in W : w \in U\} \\ &= \sum_{w \in W} \frac{1}{2^M} \sum_{u \in U} (-1)^{u \cdot w} \\ &= \frac{1}{2^M} \sum_{u \in U, w \in W} (-1)^{u \cdot w} \\ &= \frac{1}{2^M} \sum_{u \in U', w \in W'_b} (-1)^{f(u) \cdot g_b(w)} \\ &= \frac{1}{2^M} \sum_{c \in G} \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(bc) \sum_{u \in U', w \in W'_c} (-1)^{f(u) \cdot g_c(w)} \\ &= \frac{1}{2^M |G|} \sum_{\substack{c \in G, \chi \in \widehat{G} \\ u \in U', w \in W'_c}} \chi(bc) (-1)^{f(u) \cdot g_c(w)}. \end{aligned}$$

If we extend f and g_c to $f^k : (U')^k \to U^k$, $g_c^k : (W'_c)^k \to V^k$, and extend the inner product on V to an inner product on V^k, we have that

$$|S_2(\Gamma_b)|^k = \frac{1}{2^{kM} |G|^k} \sum_{\substack{c \in G, \chi \in \widehat{G} \\ u \in (U')^k, w \in (W'_c)^k}} \chi(bc) (-1)^{f^k(u) \cdot g_c^k(w)}. \tag{6}$$

Notice that once we fix values of c, χ, u, w in Equation 6 the summand (when treated as a function of $p_1, \ldots, p_n$) is of the same form as the "characters" studied in Section 3.

We want to take the sum over all $b \leq N$ square-free, $\omega(b) = n$, $(b, S) = 1$, of $|S_2(\Gamma_b)|^k$. If we let D be 8 times the product of the finite odd primes in S, we note that each such b can be expressed exactly $n!$ ways as a product $p_1, \ldots, p_n$ with p_i distinct, $(p_i, D) = 1$. Therefore this sum equals

$$\frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \\ \text{distinct primes} \\ (D,p_i)=1 \\ \prod_i p_i \leq N}} \frac{1}{2^{kM}|G|^k} \sum_{\substack{c\in G,\chi\in\widehat{G} \\ u\in(U')^k, w\in(W_c')^k}} \prod_i \chi(p_i)\chi(c)(-1)^{f^k(u)\cdot g_c^k(w)}.$$

Interchanging the order of summation gives us

$$\frac{1}{2^{kM}|G|^k} \sum_{\substack{c\in G,\chi\in\widehat{G} \\ u\in(U')^k, w\in(W_c')^k}} \frac{\chi(c)}{n!} \sum_{\substack{p_1,\ldots,p_n \\ \text{distinct primes} \\ (D,p_i)=1 \\ \prod_i p_i \leq N}} \left(\prod_i \chi(p_i)\right)(-1)^{f^k(u)\cdot g_c^k(w)}.$$

Now the inner sum is exactly of the form studied in Proposition 6.

We first wish to bound the contribution from terms where this inner sum has terms of the form $\left(\frac{p_i}{p_j}\right)$, or in the terminology of Proposition 6 for which not all of the $e_{i,j}$ are 0. In order to do this we will need to determine how many of these terms there are and how large their values of m are. Notice that terms of the form $\left(\frac{p_i}{p_j}\right)$ show up here when we are evaluating the Hilbert symbols of the form $(p, b(c_a - c_b))_p, (p, b(c_a - c_b))_q, (q, b(c_a - c_b))_p, (q, b(c_a - c_b))_q$ and in no other places.

Let $U_i \subset U'$ be the subspace generated by p_i and p_i'. For $u \in U'$ let u_i be its component in U_i in the obvious way. Let $W_i \subset W'$ be W_{p_i}. For $w \in W_c'$ let w_i be its component in W_i. Let U_0 be the $\mathbb{F}_2$-vector space with formal generators p and p'. We have a natural isomorphism between U_0 and U_i sending p to p_i and p' to p_i'. We will hence often think of u_i as an element of U_0. Similarly let W_0 be the $\mathbb{F}_2$-vector space with formal generators $((c_1-c_2)(c_1-c_3), b(c_1-c_2), b(c_1-c_3))$ and $(b(c_3-c_1), b(c_3-c_2), (c_3-c_1)(c_3-c_2))$. We similarly have natural isomorphisms between W_i and W_0 and will often consider w_i as an element of W_0 instead of W_i.

Additionally, we have a bilinear form $U_0 \times W_0 \to \mathbb{F}_2$ defined by:

$$\begin{aligned} &p\cdot((c_1 - c_2)(c_1 - c_3), b(c_1 - c_2), b(c_1 - c_3)) \\ &\quad = p' \cdot ((c_1 - c_2)(c_1 - c_3), b(c_1 - c_2), b(c_1 - c_3)) \\ &\quad = p \cdot (b(c_3 - c_1), b(c_3 - c_2), (c_3 - c_1)(c_3 - c_2)) \\ &\quad = p' \cdot (b(c_3 - c_1), b(c_3 - c_2), (c_3 - c_1)(c_3 - c_2)) \\ &\quad = 1. \end{aligned}$$

We notice that if $u \in U'$ and $w \in W'_c$, then the exponent of $\left(\frac{p_i}{p_j}\right)$ that appears in $(-1)^{f(u)\cdot g_c(w)}$ is $(u_i+u_j)\cdot(w_i+w_j)$. Similarly if $u \in (U')^k, w \in (W'_c)^k$, the exponent of $\left(\frac{p_i}{p_j}\right)$ that appears in $(-1)^{f^k(u)\cdot g_c^k(w)}$ is $(u_i+u_j)\cdot(w_i+w_j)$, where u_*, w_* are thought of as elements of U_0^k and W_0^k.

We define a symplectic form on $T = U_0^k \times W_0^k$ by $(u,w)\cdot(u',w') = u\cdot w' + u'\cdot w$. Also define a quadratic form q on T by $q(u,w) = u\cdot w$. We claim that given some set of $t_i = (u_i, w_i)_{i\in I} \in T$ that $(u_i+u_j)\cdot(w_i+w_j) = 0$ for all pairs $i,j \in I$ only if all of the (u_i,w_i) lie in a translate of a Lagrangian subspace of T. First note that for $t=(u,w), t'=(u',w')$ that $(u+u')\cdot(w+w') = t\cdot t' + q(t) + q(t')$. We need to show that for all $i,j,k \in I$ that $(t_i+t_j)\cdot(t_i+t_k) = 0$. This is true because

$$
\begin{aligned}
&(t_i+t_j)\cdot(t_i+t_k)\\
&\qquad = t_i\cdot t_i + t_i\cdot t_k + t_j\cdot t_i + t_j\cdot t_k\\
&\qquad = t_i\cdot t_k + t_j\cdot t_i + t_j\cdot t_k\\
&\qquad = t_i\cdot t_k + t_j\cdot t_i + t_j\cdot t_k + 2q(t_i) + 2q(t_j) + 2q(t_k)\\
&\qquad = (t_i\cdot t_j + q(t_i) + q(t_j)) + (t_i\cdot t_k + q(t_i) + q(t_k)) + (t_k\cdot t_j + q(t_k) + q(t_j))\\
&\qquad = 0.
\end{aligned}
$$

So suppose that we have some $u \in \prod_{i=1}^n U_i^k$ and $w \in \prod_{i=1}^n W_i^k$, and suppose that we have a set of ℓ indices in $\{1,2,\ldots,n\}$, which we call *active* indices, so that $(-1)^{f^k(u)\cdot g^k(w)}$ has terms of the form $\left(\frac{p_i}{p_j}\right)$ only for i,j both are active, and suppose furthermore that each active index shows up as either i or j in at least one such term. Let $t_i = (u_i,w_i) \in T$. We claim that t_i takes fewer than 2^k different values on non-active indices, i.

Since $t_i\cdot t_j + q(t_i) + q(t_j) = 0$ for any two non-active indices t_i and t_j, all of these must lie in a translate of some Lagrangian subspace of T. Therefore t_i can take at most 2^k values on non-active indices. Suppose for sake of contradiction that all of these values are actually assumed by some non-active index. Then consider t_j for j an active index. The t_i for i either non-active or equal to j must similarly lie in a translate of a Lagrangian subspace. Since such a space is already determined by the non-active indices and since all elements of this affine subspace are already occupied, t_j must equal t_i for some non-active i. But this means that every t_j is assumed by some non-active index which implies that no terms of the form $\left(\frac{p_i}{p_j}\right)$ survive, yielding a contradiction.

Now consider the number of such u,w so that there are at most ℓ active indices and so that at least one of these terms survive. Once we fix the values t_i that are allowed to be taken by the non-active indices (which can only be done in finitely many ways), there are $\binom{n}{\ell}$ ways to choose the active indices, at most 2^k-1 ways to pick t_i for each non-active index, and at most 2^{2k} ways for each active index. Hence the total number of such u,w with exactly ℓ active indices is

$$
O\left(\binom{n}{\ell}\left(2^k-1\right)^{n-\ell}\left(2^{2k}\right)^{\ell}\right).
$$

By Proposition 6, the value of the inner sum for such a (u, w) is at most $O\left(N(2^{-2k-1})^\ell\right)$. Hence summing over all $\ell > 0$ and recalling the 2^{-Mk} out front we get a contribution of at most

$$
\begin{aligned}
N2^{-nk}O\left(\sum_\ell \binom{n}{\ell}\left(2^k-1\right)^{n-\ell}\left(\frac{1}{2}\right)^\ell\right) &= N2^{-nk}O\left((2^k-1/2)^n\right) \\
&= NO\left((1-2^{-k-1})^n\right) \\
&= NO\left((\log N)^{-2^{-k-2}}\right).
\end{aligned}
$$

Therefore we may safely ignore all of the terms in which a $\left(\frac{p_i}{p_j}\right)$ shows up. Notice also by the above analysis, that the number of remaining terms must be $O(2^{Mk})$. Additionally, for these terms we may apply Proposition 7. Therefore because of the 2^{-Mk} factor out front we have that up to an error of $O\left(\frac{(\log\log\log N)^2}{\log\log N}\right)$ that the sum over $b = p_1 \cdots p_n$, square free, at most N, relatively prime to D, of $|S_2(\Gamma_b)|^k$ is the number of such b times the average over all possible values of $p_i \in G$, $\left(\frac{p_i}{p_j}\right)$, of $|S_2(\Gamma_b)|^k$. Furthermore our work shows that this average is bounded in terms of k independently on n.

On the other hand, recalling the notation from Theorem 2, this average is just

$$\sum_d \pi_d(n) 2^{kd}.$$

Using the fact that this is bounded for $k+1$ independently of n, we find that $\pi_d(n) = O(2^{-(k+1)d})$ where the implied constant depends on k but not d or n. In order to complete the proof of our Proposition we need to show that

$$\lim_{n\to\infty} \sum_d (\pi_d(n) - \alpha_d) 2^{kd} = 0.$$

But this follows from the fact that

$$\sum_{d>X} (\pi_d(n) - \alpha_d) 2^{kd} = O\left(\sum_{d>X} 2^{-d}\right) = O(2^{-X})$$

independently of n, and that $\pi_d(n) \to \alpha_d$ for all d by Theorem 2.

□

5 From Sizes to Ranks

In this section we turn Proposition 10 into a proof of Theorem 3, but first we must do some computations with the α_i.

Note that

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

Now $\prod_{j=1}^n (1-2^{-j})^{-1}$ is the sum over partitions, P, into parts of size at most n of $2^{-|P|}$. Equivalently we could sum over partitions P of at most n parts. Multiplying by $2^{-\binom{n}{2}}$ we get the sum over partitions P with n distinct parts (possibly a part of size 0) of $2^{-|P|}$. Therefore we have that

$$F(x) = \sum_{n=0}^{\infty} \alpha_n x^n = \frac{x^2 \prod_{j=0}^{\infty}(1+2^{-j}x)}{\prod_{j=0}^{\infty}(1+2^{-j})}.$$

This implies in particular that $\sum_{n=0}^{\infty} \alpha_n$ equals 1 as it should.

Let $C_d(N)$ equal

$$\frac{\#\{b \leq N \text{ square-free, } (b,D)=1, |\omega(b) - \log\log N| < (\log\log N)^{3/4}, \dim(S_2(\Gamma_b)) = d\}}{\#\{b \leq N \text{ square-free, } (b,D)=1, |\omega(b) - \log\log N| < (\log\log N)^{3/4}\}}.$$

Let $C(N) = (C_0(N), C_1(N), \ldots) \in [0,1]^{\omega}$. Theorem 3 is equivalent to showing that

$$\lim_{N\to\infty} C(N) = (\alpha_0, \alpha_1, \ldots).$$

Lemma 11. *Suppose that some subsequence of the $C(N)$ converges to $(\beta_0, \beta_1, \ldots) \in [0,1]^{\omega}$. Let $G(x) = \sum_n \beta_n x^n$. Then $G(x)$ has infinite radius of convergence and $F(x) = G(x)$ for $x = -1$ or x equals a power of 2. Also $\beta_0 = \beta_1 = 0$.*

This Lemma says that if the $C(N)$ have some limit that the naive attempt to compute moments of the Selmer groups from this limit would succeed.

Proof. The last claim follows from the fact that since Γ_b has full 2-torsion, its 2-Selmer group always has rank at least 2. Notice that $\sum_d C_d(N)x^d$ is equal to the average size of $x^{\dim(S_2(\Gamma_b))}$ over $b \leq N$ square-free, relatively prime to D with $|\omega(b) - \log\log N| < (\log\log N)^{3/4}$. This has limit $F(x)$ as $N \to \infty$ by Proposition 10 if x is -1 or a power of 2. In particular it is bounded. Therefore there exists an R_k so that

$$\sum_d C_d(N) 2^{kd} \leq R_k$$

for all N. Therefore $C_d(N) \leq R_k 2^{-kd}$ for all d, N. Therefore $\beta_d \leq R_k 2^{-kd}$. Therefore G has infinite radius of convergence.

Furthermore if we pick a subsequence, $N_i \to \infty$ so that $C_d(N_i) \to \beta_d$ for all d, we have that

$$\begin{aligned}
F(2^k) &= \lim_{i\to\infty} \sum_d C_d(N_i) 2^{dk} \\
&= \lim_{i\to\infty} \sum_{d \leq X} C_d(N_i) 2^{dk} + O\left(\sum_{d > X} R_{k+1} 2^{-d}\right) \\
&= \lim_{i\to\infty} \sum_{d \leq X} C_d(N_i) 2^{dk} + O(R_{k+1} 2^{-X}) \\
&= \sum_{d \leq X} \beta_d 2^{dk} + O(R_{k+1} 2^{-X}).
\end{aligned}$$

So

$$\lim_{X\to\infty}\sum_{d\le X}\beta_d 2^{dk} = F(2^k).$$

Thus $G(2^k)=F(2^k)$. For $x=-1$ the argument is similar but comes from the equidistribution of parity rather than expectation of size. $\square$

Lemma 12. *Suppose that $G(x)=\sum_n \beta_n x^n$ is a Taylor series with infinite radius of convergence. Suppose also that $\beta_n\in[0,1]$ for all n and that $G(x)=F(x)$ for x equal to -1 or a power of 2. Suppose also that $\beta_0=\beta_1=0$. Then $\beta_n=\alpha_n$ for all n.*

Proof. First we wish to prove a bound on the size of the coefficients of G. Note that

$$F(2^k)=\frac{2^{2k}(1+2^k)(1+2^{k-1})\cdots}{(1+2^0)(1+2^{-1})\cdots}=2^{2k}\prod_{j=1}^{k}(1+2^k)=O\left(2^{2k+k(k+1)/2}\right).$$

Now

$$2^{nk}\beta_n\le G(2^k)=F(2^k)=O\left(2^{2k+k(k+1)/2}\right).$$

Therefore

$$\beta_n=O\left(2^{2k+k(k+1)/2-kn}\right).$$

Setting $k=n$ we find that

$$\beta_n=O\left(2^{-n^2/2+5n/2}\right)=O\left(2^{-\binom{n-2}{2}}\right).$$

The same can be said for F. Now consider $F-G$. This is an entire function whose x^n coefficient is bounded by $O\left(2^{-\binom{n-2}{2}}\right)$. Furthermore $F-G$ vanishes to order at least 2 at 0, and order at least 1 at -1 and at powers of 2. The bounds on coefficients imply that

$$|F(x)-G(x)|\le O\left(\sum_n 2^{-\binom{n-2}{2}}|x|^n\right).$$

The terms in the above sum clearly decay rapidly for n on either side of $\log_2(|x|)$. Hence

$$|F(x)-G(x)|=O\left(2^{(-\log_2(|x|)^2+5\log_2(|x|))/2+\log_2(|x|)^2}\right)=O\left(2^{(\log_2(|x|)^2+5\log_2(|x|))/2}\right).$$

In particular $F-G$ is a function of order less than 1. Hence it must equal

$$Cx^2\prod_\rho(1-x/\rho).$$

Where the product is over non-zero roots ρ of $F-G$. On the other hand, this tells us that if $C\neq 0$ the average value of $\log_2(|F-G|)$ on a circle of radius R is

$$\log_2|C|+2\log_2 R+\sum_{|\rho<R|}\log_2(R/|\rho|).$$

Setting $R = 2^k$ and noting the contributions from $\rho = -1$ and $\rho = 2^j$ for $j < k$ we have

$$O(1) + 3k + \sum_{j<k}(k-j) = O(1) + 3k + \binom{k+1}{2} = O(1) + \frac{k^2+7k}{2} > \frac{k^2+5k}{2}$$

which is the largest that $|F - G|$ can be at this radius. This provides a contradiction. $\square$

We now prove Theorem 3.

Proof. Suppose that $C(N)$ does not have limit $(\alpha_0, \alpha_1, \ldots)$. Then there is some subsequence N_i so that $C(N_i)$ avoid some neighborhood of $(\alpha_0, \alpha_1, \ldots)$. By compactness, $C(N_i)$ must have some subsequence with a limit $(\beta_0, \beta_1, \ldots)$. By Lemmas 11 and 12, $(\alpha_0, \alpha_1, \ldots) = (\beta_0, \beta_1, \ldots)$. This is a contradiction.

Therefore $\lim_{N\to\infty} C(N) = (\alpha_0, \alpha_1, \ldots)$. Hence $\lim_{N\to\infty} C_d(N) = \alpha_d$ for all d. The Theorem follows immediately from this and the fact the fraction of $b \leq N$ square-free with $(b, D) = 1$ that have $|\omega(b) - \log\log N| < (\log\log N)^{3/4}$ approaches 1 as $N \to \infty$. $\square$

It should be noted that our bounds on the rate of convergence in Theorem 3 are non-effective in two places. One is our treatment in this last Section. We assume that we do not have an appropriate limit and proceed to find a contradiction. We believe that this is not a serious non-effectivity and that a more careful analysis could make this part of the Theorem effective. The more serious problem comes in our proof of Proposition 6 where we make use of non-effective bounds on the size of Siegel zeroes. This latter problem may well be fundamental to our approach.

References

[1] B. Mazur and K. Rubin *Ranks of Twists of Elliptic Curves and Hilbert's* 10^{th} *problem*, manuscript found at

\protect\vrule width0pt\protect\href{http://arxiv.org/PS_cache/arxiv/pdf/0904/0904.3709

[2] Henryk Iwaniec adn Emmanuel Kowalski *Analytic Number Theory*, American Mathematical Society, 2004.

[3] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Transactions Amer. Math. Soc. 264 (1981) 121135.

[4] Peter Swinnerton-Dyer *The effect of twisting on the 2-Selmer group*, Mathematical Proceedings of the Cambridge Philosophical Society, Vol 145 part 3, pp 513-526.