On the Joint Distribution Of $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_\phi(E'/\mathbb{Q})$ in Quadratic Twist Families

Daniel Kane and Zev Klagsbrun

1. Introduction

Recently, there has a lot of interest in the arithmetic statistics related to the quadratic twist family of a given elliptic curve $E/\mathbb{Q}$. Much progress has been made towards understanding how 2-Selmer ranks are distributed in these families when either $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $E[2]$ has an $\mathcal{S}_3$ Galois action. In both of these cases, there are explicit constants α_r summing to one such that the proportion of twists with 2-Selmer rank r is given by α_r [**Kan10**], [**KMR11**].

Strikingly, this is not true when E has a single rational point of order two. In this case E has a degree two isogeny $\phi : E \to E'$ and an associated Selmer group $\mathrm{Sel}_\phi(E/\mathbb{Q})$. Work of Xiong shows that if E does not have a cyclic 4-isogeny defined over $\mathbb{Q}(E[2])$, then the distribution of the ranks of $\mathrm{Sel}_\phi(E^d/\mathbb{Q})$ as d varies among the squarefree integers less than X tends to the distribution $Max\{0, \mathcal{N}(0, \frac{1}{2}\log\log X)\}$ as $X \to \infty$, where $\mathcal{N}(\mu, \sigma^2)$ is the normal distribution with mean μ and variance σ^2 [**Xio13**]. In this case, $\mathrm{Sel}_\phi(E/\mathbb{Q})$ maps $2-to-1$ into $\mathrm{Sel}_2(E/\mathbb{Q})$, showing that for any fixed r, at least half of the quadratic twists of E have 2-Selmer rank greater than r.

This same result can be deduced by studying how $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E/\mathbb{Q}) - \dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$ varies under quadratic twist, where $\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$ is the Selmer group associated to the dual isogeny $\hat{\phi}$ of ϕ. In [**Kla12**], the second author shows that as d varies among the squarefree integers less than X, the distribution of $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d/\mathbb{Q}) - \dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}(E'^d/\mathbb{Q})$ tends to $\mathcal{N}(0, \frac{1}{2}\log\log X)$ as $X \to \infty$.

This article studies the joint distribution of $\mathrm{Sel}_\phi(E^d/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E'^d/K)$ conditional on a fixed value of $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d/K) - \dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}(E'^d/K)$. In particular, we prove the following:

Theorem 1.1. *Suppose $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over $\mathbb{Q}(E[2])$ and $u \in \mathbb{Z}$. Define*

$$S(X,u) = \{d \text{ squarefree }, |d| \leq X, \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d/\mathbb{Q}) - \dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}(E'^d/\mathbb{Q}) = u\}.$$

Then for any $r \geq Max\{1, u+1\}$,

$$\lim_{X\to\infty} \frac{|\{d \in S(X,u) : (\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d/\mathbb{Q}), \dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}(E'^d/\mathbb{Q})) = (r, r-u)\}|}{|S(X,u)|} = \alpha_{r,u},$$

where

$$\alpha_{r,u} = \frac{2^{-(r-1)(r-u-1)} \prod_{s=1}^{\infty}(1-2^{-s})}{\prod_{s=1}^{r-1}(1-2^{-s}) \prod_{s=1}^{r-u-1}(1-2^{-s})}.$$

Remark 1.2. The constants $\alpha_{r,u}$ appear in Cohen and Lenstra's original paper about the distribution of class groups of quadratic fields and $\alpha_{r,-u}$ is equal to what is described there as the u-probability that a finite abelian 2-group has rank $r-1$. (See Theorem 6.3 in [**CL84**].)

2. ϕ-Descent

We begin by defining the Selmer groups $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$ and then giving an explicit description of the Selmer groups $\mathrm{Sel}_\phi(E^d/\mathbb{Q})$ and $\mathrm{Sel}_{\hat{\phi}}(E'^d/\mathbb{Q})$ associated to the quadratic twist of an elliptic curve by a squarefree integer d.

Let E be an elliptic curve with a single point of order two defined by

$$y^2 = x^3 + Ax^2 + Bx.$$

and set $C = E(\mathbb{Q})[2] = \langle (0,0) \rangle$. There is an isogenous curve E' given by a model

$$y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$$

and an isogeny $\phi : E \to E'$ with kernel C. There is a Kummer map

$$\kappa : E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

via

$$\kappa((x,y)) = \begin{cases} \Delta & \text{if } (x,y) = (0,0) \\ x & \text{if } (x,y) \neq (0,0) \end{cases}$$

where Δ is the discriminant of E. We have similarly defined local maps

$$\kappa_p : E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \to \simeq \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$$

for every completion $\mathbb{Q}_p$ of $\mathbb{Q}$ which give a commutative diagram for every completion $\mathbb{Q}_p$ of $\mathbb{Q}$, where the restriction map Res_p is the natural map $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

$$\begin{array}{ccc} E'(\mathbb{Q})/\phi(E(\mathbb{Q})) & \xrightarrow{\kappa} & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ \downarrow & & \downarrow Res_p \\ E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) & \xrightarrow{\kappa_p} & \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \end{array}$$

The ϕ-Selmer group $\mathrm{Sel}_\phi(E/\mathbb{Q})$ is defined as

$$\mathrm{Sel}_\phi(E/\mathbb{Q}) = \left\{ c \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : Res_p(c) \in \kappa_p(E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p))) \text{ for all places } p \text{ of } \mathbb{Q} \right\}$$

Exchanging the roles of E and ϕ for those of E' and the dual isogeny $\hat{\phi} : E' \to E$ yields a $\hat{\phi}$-Selmer group $\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$ via the same construction.

Standard descent technology tells us that the images of κ_p and κ'_p in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ are dual to each other via the Hilbert symbol pairing. Further, when p is a prime away from 2 where E has good reduction, the images of κ_p and κ'_p are both equal to the unramified subgroup of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ generated by the image of $\mathbb{Z}_p^\times$. This last fact allows us to describe each of $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$ as the intersection of two finite dimensional $\mathbb{F}_2$ subspaces.

Let T be the set of places of $\mathbb{Q}$ dividing $2\Delta\infty$ and define

$$V = \bigoplus_{v\in T} \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2.$$

Define a subspace $U \subset V$ as the image of the T-units $\mathbb{Z}_T^\times$ in V. Next, for each place $p \in T$, define W_p as

$$W_p = \kappa_p(E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)))$$

and

$$W_p' = \kappa_p'(E(\mathbb{Q}_p)/\phi(E'(\mathbb{Q}_p))),$$

and set

$$W = \bigoplus_{v\in T} W_p$$

and

$$W' = \bigoplus_{v\in T} W_p'.$$

It then follows that $\mathrm{Sel}_\phi(E/\mathbb{Q}) \simeq U\cap W$ and $\mathrm{Sel}_{\hat\phi}(E'/\mathbb{Q}) \simeq U\cap W'$. Because the images of κ_p and κ_p' were dual to each other under the Hilbert symbol pairing, it follows that the subspaces W and W' and therefore the Selmer groups $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_{\hat\phi}(E'/\mathbb{Q})$ are orthogonal under the sum of the Hilbert symbol pairings over the places in T.

3. Twisting

Now suppose that d is a squarefree integer relatively prime to 2Δ. Let $T_d = T \cup \{p \mid d\}$ and observe that T_d contains all of the places of $\mathbb{Q}$ above 2∞ and the places at which E^d has bad reduction. We define

$$V = \bigoplus_{v\in T_d} \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$$

and define $U^d \subset V^d$ as the image of $\mathbb{Z}_{T_d}^\times$ in V. For each place in T_d, we define

$$W_p^d = \kappa_p(E'^d(\mathbb{Q}_p)/\phi(E^d(\mathbb{Q}_p)))$$

and

$$W_p'^d = \kappa_p'(E^d(\mathbb{Q}_p)/\phi(E'^d(\mathbb{Q}_p)))$$

and set

$$W = \bigoplus_{v\in T_d} W_p^d$$

and

$$W' = \bigoplus_{v\in T_d} W_p'^d.$$

We then get that $\mathrm{Sel}_\phi(E^d/\mathbb{Q}) \simeq U^d \cap W^d$ and $\mathrm{Sel}_{\hat\phi}(E'^d/\mathbb{Q}) \simeq U^d \cap W'^d$.

Moreover, if $p \mid d$, we can explicitly describe the subsets W_p^d and $W_p'^d$ of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. By Lemma 3.7 in [**Kla11**], the images of κ_p and κ_p' are given by $\kappa_p(E'^d(\mathbb{Q}_p)[2])$ and $\kappa_p'(E^d(\mathbb{Q}_p)[2])$ respectively. Explicitly, we get

$$W_p^d = \begin{cases} \langle\Delta\rangle & \text{if } \left(\frac{\Delta'}{p}\right) = -1 \\ \langle\Delta, d(A+2\sqrt{B})\rangle & \text{if } \left(\frac{\Delta'}{p}\right) = 1 \end{cases}$$

and

$$W_p'^d = \begin{cases} \langle \Delta' \rangle & \text{if } \left(\frac{\Delta}{p}\right) = -1 \\ \langle \Delta', 2d(-A + \sqrt{A^2 - 4B}) \rangle & \text{if } \left(\frac{\Delta}{p}\right) = 1 \end{cases},$$

where Δ' is the discriminant of E'. We note that the sum of the dimensions of W_p^d and $W_p'^d$ will always be equal to two. We also note that up to squares, we have $\Delta = (A^2 - 4B)(\mathbb{Q}^\times)^2$ and $\Delta' = B(\mathbb{Q}^\times)^2$.

4. Tamagawa Numbers and Primes

[Note: Zev, I'm putting this section here because I assume you are going to need some of this discussion]

As seen above the role that an odd prime $p|d$ has in the computation of the $\phi-$Selmer group of E^d depends a lot on the residue symbols $\left(\frac{\Delta}{p}\right)$ and $\left(\frac{\Delta'}{p}\right)$. Since the four possibilities here behave very differently, we will consider them each separately.

Definition 1. *If p is a prime relative prime to $2\Delta\Delta'$*
We say that p is type 1 *if* $\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta'}{p}\right) = 1$.
We say that p is type 2 *if* $\left(\frac{\Delta}{p}\right) = -\left(\frac{\Delta'}{p}\right) = 1$.
We say that p is type 3 *if* $-\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta'}{p}\right) = 1$.
We say thatp is type 4 *if* $-\left(\frac{\Delta}{p}\right) = -\left(\frac{\Delta'}{p}\right) = 1$.

We note that W_p^d is dependent on the type of p. In particular,

$$W_p^d = \begin{cases} \langle d(A + 2\sqrt{B}) \rangle & \text{if } p \text{ is of type 1} \\ 1 & \text{if } p \text{ is of type 2} \\ (\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2) & \text{if } p \text{ is of type 3} \\ (\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2) & \text{if } p \text{ is of type 4} \end{cases}$$

We note that there is a relationship between $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) - \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E'^d)$ and the number of primes of various types.

Lemma 4.1. *For each $L \in (\mathbb{Z}/2\Delta\Delta'\mathbb{Z})^*$ there exists an integer c_L so that for any $d = p_1 \cdots p_n$ where p_i are distinct primes so that the p_i contain n_j primes of type j for $1 \leq j \leq 4$, and so that $d \equiv L \pmod{2\Delta\Delta'}$, then*

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) - \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E'^d) = c_L + n_3 - n_2.$$

Furthermore, for every $u \in \mathbb{Z}$ there exist d relatively prime to $2\Delta\Delta'$ so that $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) - \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E'^d) = u$.

TODO: Zev, can you handle this (assuming I got it right)? □

It should also be noted that if $d = p_1 \cdots p_n$ for p_i are distinct primes relatively prime to $2\Delta\Delta'$ that an element ℓ of U^d can only be in W^d if $p_i \not| \ell$ for p_i of type 2 or 4. Thus if we let U'^d be the span of

$$\{-1, 2\} \cup \{q : q|\Delta\Delta'\} \cup \{p_i : p_i \text{ is of type 1 or 3}\}$$

then $\mathrm{Sel}_\phi(E^d) = U'^d \cap W^d$.

5. A Markov Chain Approach

Based on the above description, it is easy to see that if $d = p_1 \cdots p_n$ for p_i distinct primes relatively prime to $2\Delta\Delta'$ that the rank of $\mathrm{Sel}_\phi(E^d/\mathbb{Q})$ depends only on the values of the p_i modulo $8\Delta\Delta'$, whether or not $A + 2\sqrt{B}$ is a square mod p_i for primes p_i for which $\left(\frac{\Delta}{p_i}\right) = \left(\frac{\Delta'}{p_i}\right) = 1$, and on $\left(\frac{p_i}{p_j}\right)$.

There is a natural probability distribution over possible combinations of such values. Namely, the p_i take random, independent congruence classes in $(\mathbb{Z}/(8\Delta\Delta'\mathbb{Z}))^*$, for p_i with $\left(\frac{\Delta}{p_i}\right) = \left(\frac{\Delta'}{p_i}\right) = 1$, the symbols $\left(\frac{A+2\sqrt{B}}{p_i}\right)$ are randomly $+1$ or -1, and the $\left(\frac{p_i}{p_j}\right)$ are random and independent up to the constraints imposed by quadratic reciprocity. In terms of this probability distribution, there are combinatorial means by which the distribution of Selmer ranks can be analyzed. In particular, we get the following theorem.

Theorem 2. *In terms of the probability distribution above let*

$$\alpha_{r,u}(n) := \mathbb{P}\big(\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) = r | d = p_1 \cdots p_n, \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) - \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E'^d) = u, \text{ there are at least } n/10 \ p_i \text{ of type } i \text{ for all } i\big),$$

then

$$\lim_{n\to\infty} \alpha_{r,u}(n) = \alpha_{r,u}.$$

(as it is clear that the last condition holds with probability approaching 1 as $n \to \infty$).

TODO: Zev, I need to have this in order to get my result to work. □

6. Natural Density

While Theorem 2 proves a limiting result along the lines of [**SD08**], it would be convenient to have a result in terms of natural density such as Theorem 1.1 above. We proceed in a manner analogous to that in [**Kan10**] with a few added complications due to our slightly different context. In particular, we attempt to get at the densities of ranks via moments of the actual sizes of the Selmer groups in question on a large subset. In particular, letting $\omega(n)$ denote the number of distinct primes dividing n, we define:

Definition 3. *Let $S'(X,u)$ be the set of d satisfying the following properties:*

(1) $0 < d \leq X$
(2) d *is squarefree*
(3) d *is relatively prime to* $2\Delta\Delta'$
(4) $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) - \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E'^d) = u$
(5) $|\omega(d) - \log\log(X)| < \log\log(X)^{5/8}$
(6) d *has more than* $\omega(d)/10$ *prime factors of each type (ie. type 1 through type 4).*

Let $S''(X,u)$ be the set of d satisfying only the first four of these properties.

We note that $S(X,u)'$ is a proper subset of $S''(X,u)$, but that the density of one within the other approaches 1 as $X \to \infty$

Lemma 6.1. *For any E and u we have that*

$$\lim_{X\to\infty} \frac{|S'(X,u)|}{|S''(X,u)|} = 1.$$

In order to prove this, we will need the following slight strengthening of [**Kan10**] Proposition 10:

Proposition 6.2. *Let n, N, D be integers with $\log\log N > 1$, and $(\log\log N)/2 < n < 2\log\log N$. Let $G = ((\mathbb{Z}/D\mathbb{Z})^*)^n$. Let $f : G \to \mathbb{C}$ be a function. Let $\bar{f} = \frac{1}{|G|}\sum_{g\in G} f(g)$. Let $|f|_2 = \sqrt{\frac{1}{|G|}\sum_{g\in G}|f(g)|^2}$. Then*

$$\frac{1}{n!}\sum_{\substack{p_1\cdots p_n\leq N\\ p_i \text{ distinct primes}\\ (p_i,D)=1}} f(p_1,\ldots,p_n) = \bar{f}\left(\frac{1}{n!}\sum_{\substack{p_1\cdots p_n\leq N\\ p_i \text{ distinct primes}\\ (p_i,D)=1}} 1\right) + O_D\left(\frac{|f|_2 N\log\log\log N}{\log\log N}\right).$$

Proof. The result follows from the proof of [**Kan10**] Proposition 10. □

There is a particularly, nice version of this result when f is symmetric.

Corollary 4. *Let n, N, D be integers with $\log\log N > 1$, and $(\log\log N)/2 < n < 2\log\log N$. Let $G = ((\mathbb{Z}/D\mathbb{Z})^*)^n$. Let $f : G \to \mathbb{C}$ be a function symmetric in its inputs. For d relatively prime to D with $\omega(d) = n$, let $f(d) = f(p_1,\ldots,p_n)$, where p_i are the prime factors of d. Let $\bar{f} = \frac{1}{|G|}\sum_{g\in G} f(g)$. Let $|f|_2 = \sqrt{\frac{1}{|G|}\sum_{g\in G}|f(g)|^2}$. Then*

$$\sum_{\substack{d\leq N\\ d \text{ squarefree}\\ (d,D)=1}} f(p_1,\ldots,p_n) = \bar{f}\left(\sum_{\substack{d\leq N\\ d \text{ squarefree}\\ (d,D)=1}} 1\right) + O_D\left(\frac{|f|_2 N\log\log\log N}{\log\log N}\right).$$

Proof. This follows immediately from Proposition 6.2 upon noting that each such d can be written as a product $p_1,\ldots,p_n$ in exactly $n!$ ways. □

We can now prove Lemma 6.1.

Proof. We begin by showing that $S''(X,u)$ is reasonably big, in particular, that $|S''(X,u)| = \Omega(X\log\log(X)^{-1/2})$. Pick an L modulo $D = 4\Delta\Delta'$ so that it is possible to have $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) - \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E'^d) = u$ for some $d \equiv L \pmod D$. By Lemma 4.1, this will happen whenever $d \equiv L$ and $n_3 - n_2$ is equal to some particular constant, U. In particular, this implies that $\left(\frac{\Delta\Delta'}{L}\right) = (-1)^U$.

Consider the number $d \leq X$ with d squarefree and $\omega(d) = n$ for some $|n - \log\log X| < \log\log(X)^{5/8}$ with $d \equiv L \pmod D$ and $n_3 - n_2 = U$. Note that whether or not this holds for such a d depends only on the congruence classes of the primes dividing d modulo D. Thus, if we define $f(p_1,\ldots,p_n)$ to be 1 if it holds and 0 otherwise, we may apply Corollary 4.

We note that if the p_i are picked randomly modulo D with probability $\Theta_u(\log\log(X)^{-1/2})$ that $n_3 - n_2 = U$ and that at least one prime is not of type 2 or 3. We note furthermore that upon fixing the values of all of the p_i modulo D except for one of type 1 or 4, there is a unique setting of the last prime modulo D so that $d \equiv L \pmod D$. This setting is of type 1 or 4, since if d' is the product of the other primes dividing d, then $\left(\frac{\Delta\Delta'}{d'}\right) = (-1)^{n_2+n_3} = (-1)^U = \left(\frac{\Delta\Delta'}{L}\right)$, and thus $\left(\frac{\Delta\Delta'}{L/d'}\right) = 1$. Therefore $\bar{f} = \Theta_{D,u}(\log\log(X)^{-1/2})$, and thus $|f|_2 = \Theta_{D,u}(\log\log(X)^{-1/4})$. Hence, applying Corollary 4 for each n with $|n -$

$\log\log(X)| < \log\log(X)^{5/8}$ we find that letting $S(X)$ be the set of d satisfying Properties (1),(2) and (3) above that

$$|S''(X,u)| = \Theta_{D,u}(\log\log(X)^{-1/2})|S(X)| + O_{D,u}\left(\frac{X\log\log\log X}{(\log\log X)^{5/8}}\right).$$

We note that by a slight modification of [**Kan10**] Corollary 8, we can show that the number of $d \leq X$ with $|d - \log\log(X)| > \log\log(X)^{5/8} = \exp(-\Omega(\log\log(X)^{1/4}))$. Thus, $|S(X)| = \Omega_D(X)$, and thus

$$|S''(X,u)| = \Omega_{D,u}(X\log\log(X)^{-1/2}).$$

We have yet to show that $|S''(X,u) - S'(X,u)|$ is small. In particular, by the above, $o(X\log\log(X)^{-1/2})$ of integers less than X fail to satisfy property (5). Of the numbers satisfying the Properties (1),(2),(3) and (5), and $\omega(d) = n$, we can apply Corollary 4 to count the number that fail to satisfy Property (6) since it is clear that this property depends only on the prime factors modulo D. It is also clear that $\bar{f} = e^{-\Omega(n)}$ and that $|f|_2 = \sqrt{\bar{f}}$. Therefore, we have that the number of d failing Property (6) is $O_D(Xe^{-\Omega(n)})$. Summing over all n with $|n - \log\log(X)| < \log\log(X)^{5/8}$ tells us that the number of d satisfying the first five properties but not the sixth is $O_D(X\log(X)^{-\Omega_D(1)})$, which is also much smaller than $|S''(X,u)|$. This completes the proof. □

Having restricted ourselves, to $S'(X,u)$, we may now consider the average moments of twists of E by elements of this set. In particular, the bulk of our work will be to prove the following proposition:

Proposition 6.3. *Let k be a non-negative integer, and u be an integer. Then*

$$\lim_{X\to\infty} \frac{\sum_{d\in S'(X,u)} |\mathrm{Sel}_\phi(E^d)|^k}{|S'(X,u)|} = \sum_{r=0}^{\infty} 2^{kr}\alpha_{r,u}.$$

Note that the limit above is exactly what you would expect if an $\alpha_{r,u}$-fraction of the $d \in S'(X,u)$ had $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) = r$. Before proceeding with the proof, we show how Proposition 6.3 can be used to prove Theorem 1.1.

Proof of Theorem 1.1 assuming Proposition 6.3. From Proposition 6.3 it is not hard to show (along the same lines as [**Kan10**], Section 5) that for any u, r

$$\lim_{X\to\infty} \frac{\#\{d \in S'(X,u) : \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) = r\}}{|S'(X,u)|} = \alpha_{r,u}.$$

[TODO: Should I go into more detail?]

By Lemma 6.1, it immediately follows that

$$\lim_{X\to\infty} \frac{\#\{d \in S''(X,u) : \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^d) = r\}}{|S''(X,u)|} = \alpha_{r,u}.$$

Writing $S''(F,X,u)$ to denote the version of S'' associated to a perhaps different elliptic curve, F, we note that

$$S(X,u) = \bigcup_{m|2\Delta\Delta'} mS''(E^m, X/m, u).$$

Therefore, the set of twists of the form

$$\{E^d : d \in S(X,u)\}$$

can be written as a union

$$\bigcup_{m|2\Delta\Delta'} \{(E^m)^d : d \in S(E^m, X, u)\}.$$

Since an $\alpha_{r,u}$-fraction of the twists in each of these sets have Selmer groups of rank r, the same holds for the union. This completes the proof. □

The rest of this section will be devoted to proving Proposition 6.3. We begin by further partitioning $S'(X,u)$ further. In particular let $S'(X,u,n)$ be the subset of $d \in S'(X,u)$ so that $\omega(d) = n$. We note that (as long as $|n - \log\log(X)| < \log\log(X)^{5/8}$) that each $d \in S'(X,u)$ can be written in exactly $n!$ ways as $d = p_1 \cdots p_n$ where p_i are distinct primes, relatively prime to $2\Delta\Delta'$, so that if n_i of them are of type i, then $n_i > n/10$ and $n_3 - n_2 = U_d := u - c_L$, where c_L is as given in Lemma 4.1 for $d \equiv L \pmod{2\Delta\Delta'}$. Thus we have, letting $D = 8\Delta\Delta'$, that

$$\sum_{d \in S'(X,u,n)} |\mathrm{Sel}_\phi(E^d)|^k = \frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \text{ distinct primes} \\ d=p_1\cdots p_n \le X, (p_i,D)=1 \\ n_i \text{ of type } i, n_3-n_2=U_d \\ n_i > n/10}} |\mathrm{Sel}_\phi(E^d)|^k.$$

We subdivide this sum further by conditioning on the values of each of the p_i modulo D. In particular, we let $C(u,n)$ be the set of elements $(c_1,\ldots,c_n) \in ((\mathbb{Z}/D\mathbb{Z})^*)^n$ so that if there are n_i c's of type i, then $n_i > n/10$ for all i and $n_3 - n_2 = U_d$. It is easy to verify that so long as $n > 10U$ that $|C(u,n)| = \Theta(\phi(D)^n n^{-1/2})$. In any case, we can now rewrite the above equation as

$$\sum_{d \in S'(X,u,n)} |Sel_\phi(E^d)|^k = \sum_{(c_1,\ldots,c_n) \in C(u,n)} \frac{1}{n!} \sum_{\substack{p_1,\ldots,p_n \text{ distinct primes} \\ d=p_1\cdots p_n \le X \\ p_i \equiv c_i \pmod D}} |\mathrm{Sel}_\phi(E^d)|^k. \tag{1}$$

We need to better understand $|\mathrm{Sel}_\phi(E^{p_1\cdots p_n})|$ when $p_i \equiv c_i \pmod D$. If $d = p_1 \cdots p_n$, this is the number of $x \in U'^d$ so that $x \in W^d$. For each i, let $t(i,1),\ldots,t(i,n_i)$ be the distinct indices so $c_{t(i,j)}$ of type i. We note that any such x can be written uniquely as

$$x = y \prod_{i=1}^{n_1} p_{t(1,i)}^{u_i} \prod_{i=1}^{n_3} p_{t(3,i)}^{u_{n_1+i}},$$

where y is squarefree and divides D and $u = (u_1,\ldots,u_{n_1+n_3}) \in \mathbb{F}_2^{n_1+n_3}$. We abbreviate the above as $x = yp^u$.

In order for x to be in W^d it must be the case that $x \in W_q^d$ for $q|D\infty$ and for $q = p_i$ for each i. We note that whether or not $x \in W_q^d$ for $q|D\infty$ depends only on the congruence classes of p_i modulo D. Thus, if $c = (c_1,\ldots,c_n)$, we let $U(c)$ denote the set of pairs (y,u) as above so that yp^u is in W_q^d for all $q|D\infty$. It should also be noted that such x are automatically in $W_{p_i}^d$ for i or type 3 or 4. For p_i of type 1, $x \in W_{p_i}^d$ if and only if the Hilbert symbol $(x, d(A + 2\sqrt{B}))_{p_i}$ equals 1. For p_i of type 2, $x \in W_{p_i}^d$ if and only if the Hilbert symbol $(x,p_i)_{p_i}$ equals 1. Therefore, we have that if $x = yp^u$ for $(y,u) \in U(c)$ then if $p_i \equiv c_i$

$(\mathrm{mod}\ D)$ then

$$\sum_{w\in\mathbb{F}_2^{n_1+n_2}}\prod_{i=1}^{n_1}(x,d(A+2\sqrt{B}))_{p_{t(1,i)}}^{w_i}\prod_{i=1}^{n_2}(x,p_{t(2,i)})_{p_{t(2,i)}}^{w_{n_1+i}}=\begin{cases}2^{n_1+n_2} & \text{if } x\in W^d\\ 0 & \text{else}\end{cases}.$$

Therefore we have that if $d=p_1\cdots p_n$ with $p_i\equiv c_i\ (\mathrm{mod}\ D)$,

$$|\mathrm{Sel}_\phi(E^d)|=\frac{1}{2^{n_1+n_2}}\sum_{\substack{(y,u)\in U(c)\\ w\in\mathbb{F}_2^{n_1+n_2}}}\prod_{i=1}^{n_1}(yp^u,d(A+2\sqrt{B}))_{p_{t(1,i)}}^{w_i}\prod_{i=1}^{n_2}(yp^u,p_{t(2,i)})_{p_{t(2,i)}}^{w_{n_1+i}}.$$

Taking a k^{th} power yields

(2)
$$|\mathrm{Sel}_\phi(E^d)|^k=\frac{1}{2^{k(n_1+n_2)}}\sum_{\substack{(y_\ell,u_\ell)\in U(c)\\ w_\ell\in\mathbb{F}_2^{n_1+n_2}\\ 1\le\ell\le k}}\prod_{\ell=1}^{k}\left(\prod_{i=1}^{n_1}(y_\ell p^{u_\ell},d(A+2\sqrt{B}))_{p_{t(1,i)}}^{w_{i,\ell}}\prod_{i=1}^{n_2}(y_\ell p^{u_\ell},p_{t(2,i)})_{p_{t(2,i)}}^{w_{n_1+i,\ell}}\right).$$

Substituting this in to Equation (1), and interchanging the order of summation, we get that

$$\sum_{d\in S'(X,u,n)}|\mathrm{Sel}_\phi(E^d)|^k=\sum_{(c_1,\ldots,c_n)\in C(u,n)}\frac{1}{2^{k(n_1+n_2)}}\sum_{\substack{(y_\ell,u_\ell)\in U(c)\\ w_\ell\in\mathbb{F}_2^{n_1+n_2}\\ 1\le\ell\le k}}$$

(3)
$$\frac{1}{n!}\sum_{\substack{d=p_1\cdots p_n\le X\\ p_i\text{ distinct primes}\\ p_i\equiv c_i\pmod D}}\prod_{\ell=1}^{k}\left(\prod_{i=1}^{n_1}(y_\ell p^{u_\ell},d(A+2\sqrt{B}))_{p_{t(1,i)}}^{w_{i,\ell}}\prod_{i=1}^{n_2}(y_\ell p^{u_\ell},p_{t(2,i)})_{p_{t(2,i)}}^{w_{n_1+i,\ell}}\right).$$

Define $\lambda(p)$ to be the function on primes p relatively prime to D so that

$$\lambda(p)=\begin{cases}\left(\frac{A+2\sqrt{B}}{p}\right) & \text{if } \left(\frac{\Delta}{p}\right)=\left(\frac{\Delta'}{p}\right)=1\\ 0 & \text{otherwise.}\end{cases}$$

We note that by quadratic reciprocity and our knowledge of the p_i modulo D, we can rewrite the inner summand as

$$z(y_\ell,u_\ell,w_\ell)\prod_{1\le i<j\le n}\left(\frac{p_i}{p_j}\right)^{e_{i,j}(y_\ell,u_\ell,w_\ell)}\prod_{i\in T(y_\ell,u_\ell,w_\ell)}\lambda(p_i).$$

For some $|z(y_\ell,u_\ell,w_\ell)|=1$, $e_{i,j}(y_\ell,u_\ell,w_\ell)=e_{j,i}(y_\ell,u_\ell,w_\ell)\in\mathbb{F}_2$, and $T(y_\ell,u_\ell,w_\ell)\subset\{1,\ldots,n\}$ so that $i\in T(y_\ell,u_\ell,w_\ell)$ only if c_i is of type 1 and $e_{i,j}$ or $e_{j,i}$ is 1 for all j of type 2.

We can now remove the conditioning on the congruence classes of the p_i with an appropriate character sum. Namely, we have that:

$$\sum_{d\in S'(X,u,n)} |\mathrm{Sel}_\phi(E^d)|^k = \frac{1}{\phi(D)^n} \sum_{(c_1,\ldots,c_n)\in C(u,n)} \frac{1}{2^{k(n_1+n_2)}} \sum_{\substack{(y_\ell,u_\ell)\in U(c)\ \chi_i \\ w_\ell\in \mathbb{F}_2^{n_1+n_2}}} \sum_{(\mathrm{mod}\ D)}$$

$$\frac{1}{n!} \sum_{\substack{d=p_1\cdots p_n\leq X \\ p_i \text{ distinct primes}}} z(y_\ell,u_\ell,w_\ell) \prod_{i=1}^n \chi_i(p_i/c_i) \prod_{1\leq i<j\leq n} \left(\frac{p_i}{p_j}\right)^{e_{i,j}(y_\ell,u_\ell,w_\ell)} \prod_{i\in T(y_\ell,u_\ell,w_\ell)} \lambda(p_i). \tag{4}$$

The inner summand is now a constant of norm 1 times a product of $\chi_i(p_i)$ where the χ_i are characters of modulus dividing D, times a product of Legendre symbols $\left(\frac{p_i}{p_j}\right)$ for $i<j$, times a product of terms of the form $\lambda(p_i)\left(\frac{p_i}{p_j}\right)$ where $j=t(2,1)$. Note that this sum is very similar to the sum consider in [**Kan10**] Proposition 9, and can be bounded by similar means. In particular, we have

Lemma 6.4. *Let χ_i, $z=z(y_\ell,u_\ell,w_\ell)$, $e_{i,j}=e_{i,j}(y_\ell,u_\ell,w_\ell)$ and $T=T(y_\ell,u_\ell,w_\ell)$ be as above. Let m be the number of indices $1\leq i\leq n$ so that at least one of the following holds:*

- *$\chi_i\neq 1$*
- *$e_{i,j}=1$ for some $j\neq i$*

Then

$$\left|\frac{1}{n!} \sum_{\substack{d=p_1\cdots p_n\leq X \\ p_i \text{ distinct primes}}} z\prod_{i=1}^n \chi_i(p_i/c_i) \prod_{1\leq i<j\leq n} \left(\frac{p_i}{p_j}\right)^{e_{i,j}} \prod_{i\in T} \lambda(p_i)\right| = O_{c,D}(Xc^m).$$

Proof. We may assume without loss of generality that c_n is of type 2. Thus, we may merge terms to replace the $\lambda(p_i)$ terms with terms of the form $\lambda(p_i)\left(\frac{p_i}{p_n}\right)$. The remainder of the proof is now completely analogous to the proof of Proposition 9 in [**Kan10**] after noting that [**Kan10**] Lemma 15 also implies that

$$\left|\sum_{\substack{A\leq p_1,p_2 \\ p_1p_2\leq X}} a(p_1)b(p_2)\lambda(p_1)\left(\frac{p_1}{p_2}\right)\right| = O(X\log(X)A^{-1/8}).$$

□

For given values of χ_i,y_ℓ,u_ℓ,w_ℓ, let m be as given in Lemma 6.4, and let m' be the number of indices i so that $e_{i,j}=1$ for some $j\neq i$. We would like to show the contribution to the sum in Equation (4) with $m>0$ is negligible. We begin by showing that the sum over terms with $m'>0$ is negligible. In particular, we show that

Lemma 6.5.

$$\frac{1}{\phi(D)^n}\sum_{(c_1,\dots,c_n)\in C(u,n)}\frac{1}{2^{k(n_1+n_2)}}\sum_{\substack{(y_\ell,u_\ell)\in U(c)\ \chi_i\\ w_\ell\in\mathbb{F}_2^{n_1+n_2}\\ m'>0}}\sum_{(\mathrm{mod}\ D)}$$

$$\left|\frac{1}{n!}\sum_{\substack{d=p_1\cdots p_n\le X\\ p_i\ \text{distinct primes}}} z(y_\ell,u_\ell,w_\ell)\prod_{i=1}^n\chi_i(p_i/c_i)\prod_{1\le i<j\le n}\left(\frac{p_i}{p_j}\right)^{e_{i,j}(y_\ell,u_\ell,w_\ell)}\prod_{i\in T(y_\ell,u_\ell,w_\ell)}\lambda(p_i)\right|$$

$$= O_{D,k,U}\left(X\log(X)^{-2^{-k-1}}\right).$$

Furthermore, for fixed c, the number of collections of u_ℓ, v_ℓ so that $m'=0$ is $O_{k,u}(2^{k(n_1+n_2)})$.

Proof. To understand the size of this sum, we must better understand the number of u_ℓ, w_ℓ with a given value of m'. In order to do this, we must better understand the terms $e_{i,j}$. We begin with the following definitions:

- For $1\le i\le n_1$, let $v_{1,i}\in\mathbb{F}_2^{2k}$ be given by $(w_{i,1},\dots,w_{i,\ell},u_{i,1},\dots,u_{i\ell})$.
- For $1\le i\le n_2$, let $v_{2,i}\in\mathbb{F}_2^{k}$ be given by $(w_{n_1+i,1},\dots,w_{n_1+i,\ell})$.
- For $1\le i\le n_3$, let $v_{3,i}\in\mathbb{F}_2^{k}$ be given by $(u_{n_1+i,1},\dots,u_{n_1+i,\ell})$.

It is now easy to verify that:

$$e_{t(2,i),t(3,j)}=\langle v_{2,i},v_{3,j}\rangle,$$

and

$$e_{t(1,i),t(1,j)}=\phi(t(1,i)+t(1,j))$$

where ϕ is the non-degenerate quadratic form $\phi(x_1,\dots,x_k,y_1,\dots,y_k)=\sum_{i=1}^k x_iy_i$.

Call an index, i between 1 and n *active* if $e_{i,j}=1$ for any $j\neq i$. Let $S_1\subset\mathbb{F}_2^{2k}$ be the set of elements of the form $v_{1,i}$ for i so that $t(1,i)$ is not active. Let m_i be the number of active indices of type i. Define $S_2,S_3\subset\mathbb{F}_2^k$ similarly. We make the following claim:

Claim 1.

$$|S_1|\le 2^k,\qquad |S_2||S_3|\le 2^k$$

Furthermore, the first inequality is strict if $m_1>0$ and the second inequality is strict if m_2 or m_3 is bigger than 0. Finally $m_4>0$ only if $m_1>0$.

Proof. The first inequality follows from noting that for any $v_1,v_2\in S_1$ that $\phi(v_1+v_2)=0$, and thus that S_1 is contained in a translation of a Lagrangian subspace of ϕ. If $m_1>0$ then there is some $t(1,i)$ which is active, and thus $v_{1,i}\notin S_1$. On the other hand, by the above reasoning $S_1\cup\{v_{1,i}\}$ is contained in a translate of a Lagrangian subspace for ϕ, implying that the inequality is strict.

The second inequality follows from the observation that S_2 is contained in the orthogonal compliment of the span of S_3. If $e_{t(2,i),t(3,j)}=1$ for some i,j, then S_2 is also orthogonal to $v_{3,j}\notin S_3$, from which we infer that either S_3 is strictly contained in it's span, or that S_2 is strictly contained in the orthogonal complement of S_3, either of which imply that $|S_2||S_3|<2^k$.

Finally, note that $e_{t(4,i),t(4,j)}$ is always 0, and thus if $m_4>0$ then some other m_i must also be positive. □

Note that this claim immediately implies the second part of the Lemma.

We are now ready to prove our Proposition. We write the sum over u_ℓ, w_ℓ in a particular way. First we produce an outer sum over the values of m_1, m_2, m_3, m. Next we sum over possible choices of the sets S_1, S_2, S_3 consistent with the above claim. We note that there are only $O_k(1)$ many possibilities. Then we count the number of choices of u_ℓ, w_ℓ, y_ℓ consistent with these choices. We note that for each choice of u_ℓ, w_ℓ there are $O_{k,D}(1)$ possible valid choices for y_ℓ. We note that making choices of u_ℓ and w_ℓ is equivalent to picking values for the $v_{i,j}$. To do this we first decide which of the indices contribute to m, which can be done in at most $\binom{n}{m}$ many ways. Next, we pick the values of the $v_{i,j}$ consistently with our choices of S_i, which can be done in at most $|S_1|^{n_1}|S_2|^{n_2}|S_3|^{n_3}2^{km'}$ many ways. Finally, we note that By Lemma 6.4, the inner sum is then $O_{k,c,D}(Xc^{m'})$. Finally, we choose the values of χ_i, noting that $\chi_i = 1$ unless i contributes to m. Thus, the χ s can be picked in at most $\phi(D)^m$ ways. Thus the sum in question is at most

$$\begin{aligned}
&\frac{1}{\phi(D)^n}\sum_{c\in C(n,u)}\frac{1}{2^{k(n_1+n_2)}}\sum_{0<m_1+m_2+m_3\leq m} O_{k,D,c}(X(2^k\phi(D)c)^m)\binom{n}{m}|S_1|^{n_1}|S_2|^{n_2}|S_3|^{n_3}\\
\leq&\sum_{0<m_1+m_2+m_3\leq m} O_{k,D,c,U}(X(2^k\phi(D)c)^m)\binom{n}{m}\left(\frac{|S_1|}{2^k}\right)^{n_1}\left(\frac{|S_2||S_3|}{2^k}\right)^{n_2}\\
\leq&(1-2^{-k})^{\min(n_1,n_2)}\sum_m O_{k,D,c,U}(X(c)^m)\binom{n}{m}m^3\\
\leq&(1-2^{-k})^{n/10}O_{c,k,D,U}(X(1+c)^{3n})\\
\leq&(1-2^{-k})^{n/10}O_{k,D,U}(X(1+2^{-k-7})^n)\\
\leq&O_{k,d,U}(X\log(X)^{-2^{-k-5}}).
\end{aligned}$$

This completes our proof. □

Now that we have shown that the contribution from terms with $m' > 0$, we can deal with the sum in question.

Lemma 6.6. *For* $|n - \log\log(X)| < \log\log(X)^{5/8}$,

$$\sum_{d\in S'(X,u,n)}|\mathrm{Sel}_\phi(E^d)|^k = |S'(X,u,n)|\sum_r 2^{kr}\alpha_{r,u}(n) + O_{D,k,U}\left(\frac{X\log\log\log(X)}{\log\log(X)^{5/4}}\right).$$

Furthermore,

$$\sum_r 2^{kr}\alpha_{r,u}(n) = O_{D,k,U}(1).$$

Proof. By Lemma 6.5, we know that we can already safely ignore the terms with $m' > 0$. Also by Lemma 6.5, the number of such terms in the sum over y_ℓ, u_ℓ, v_ℓ is $O_{k,D}(2^{k(n_1+n_2)})$. Thus, up to negligible error the sum in question without the $m > 0$ restriction is

$$\frac{1}{n!}\sum_{\substack{d=p_1\cdots p_n\leq X\\ p_i \text{ distinct primes}}} f(p_1,\ldots,p_n), \tag{5}$$

where $f : ((\mathbb{Z}/D\mathbb{Z})^*)^n \to \mathbb{C}$ is some function with $|f|_\infty \leq O_{k,D}(1)$ and f supported on $C(u,n)$. By Proposition 6.2, this is

$$\left(\frac{1}{\phi(D)^n}\sum_{g\in((\mathbb{Z}/D\mathbb{Z})^*)^n} f(g)\right)\left(\frac{1}{n!}\sum_{\substack{d=p_1\cdots p_n\leq X\\ p_i \text{ distinct primes}}} 1\right)+O_D\left(\frac{X\log\log\log(X)|f|_\infty}{\log\log(X)}\sqrt{\frac{|\mathrm{supp}(f)|}{\phi(D)^n}}\right).$$

The error term here is clearly seen to be

$$O_{D,k,U}\left(\frac{X\log\log\log(X)}{\log\log(X)^{5/4}}\right).$$

First we note that $\sum_r 2^{kr}\alpha_{r,u}(n)$ is the expectation over p_i as described in Theorem 2 of the k^{th} moment of the size of the Selmer group times the indicator function of the event that there are more than $n/10$ primes of each type, given that $n_3 - n_2 = U$. This is the expectation of the k^{th} power of Selmer times the indicator function that all n_i are more than $n/10$ and that $n_3 - n_2 = U$, divided by the probability that $n_3 - n_2 = U$.

The former expectation can be computed via a formula similar to Equation (3) in which the inner sum and the $\frac{1}{n!}$ is replaced by an expectation. In this case, the sum over terms with $m' > 0$ is exactly 0, and thus is equal to an expression analogous to that in Equation (5). Thus, it is easy to see that this sum is exactly

$$\left(\frac{1}{\phi(D)^n}\sum_{g\in((\mathbb{Z}/D\mathbb{Z})^*)^n} f(g)\right).$$

Thus, we have that

$$\sum_r 2^{kr}\alpha_{r,u}(n) = \left(\frac{1}{C'(n,u)}\sum_{g\in((\mathbb{Z}/D\mathbb{Z})^*)^n} f(g)\right)$$

Where $C'(n,u)$ is the set of congruence classes with $n_3 - n_2 = U$. This is clearly $O_{D,k,U}(1)$.

By Proposition 6.2 with f the indicator function of $C(u,n)$, we find that that $|S'(X,u,n)|$ is

$$\#\{d\leq X \text{ squarefree }, (d,D)=1, \omega(d)=n\}\frac{|C(u,n)|}{\phi(D)^n}+O_{D,k,U}\left(\frac{X\log\log\log(X)}{\log\log(X)^{5/4}}\right).$$

Combining these last two lines with Equation (5) yields the desired result. □

We are almost ready to prove Proposition 6.3. First we need one more Lemma.

Lemma 6.7. *For any k, u*

$$\lim_{n\to\infty}\sum_r 2^{kr}\alpha_{r,u}(n) = \sum_r 2^{kr}\alpha_{r,u}.$$

Proof. Applying the second part of Lemma 6.6, with one higher k, we find that

$$\sum_r 2^{kr+r}\alpha_{r,u}(n) = O_{k,D,U}(1)$$

and thus

$$2^{kr}\alpha_{r,u}(n) = O_{D,k,U}(2^{-r}).$$

Theorem 2 tells us that $2^{kr}\alpha_{r,u}(n)$ converge to $2^{kr}\alpha_{r,u}$ pointwise. Our result now follows from the Dominated Convergence Theorem. □

We are now ready to prove Proposition 6.3.

PROOF. By Lemma 6.7, for any $\epsilon > 0$ there is an N so that whenever $n > N$, $|\sum_r 2^{kr}\alpha_{r,u}(n) - \sum_r 2^{kr}\alpha_{r,u}| < \epsilon$. Take X so that $\log\log(X) > 2N$. Then

$$\begin{aligned}
&\sum_{d\in S'(X,u)} |\mathrm{Sel}_\phi(E^d)|^k \\
=&\sum_{|n-\log\log(X)|<\log\log(X)^{5/8}} \sum_{d\in S'(X,u,n)} |\mathrm{Sel}_\phi(E^d)|^k \\
=&\sum_{|n-\log\log(X)|<\log\log(X)^{5/8}} \left(|S'(X,u,n)|\sum_r 2^{kr}\alpha_{r,u}(n) + O_{D,k,U}\left(\frac{X\log\log\log(X)}{\log\log(X)^{5/4}}\right)\right) \\
=&\sum_{|n-\log\log(X)|<\log\log(X)^{5/8}} \left(|S'(X,u,n)|\sum_r 2^{kr}\alpha_{r,u} + O(\epsilon)\right) + O_{D,k,U}\left(\frac{X\log\log\log(X)}{\log\log(X)^{5/8}}\right) \\
=&|S'(X,u)|\sum_r 2^{kr}\alpha_{r,u} + O(\epsilon|S'(X,u)|) + O_{D,k,U}(|S'(X,u)|\log\log(X)^{-1/10}).
\end{aligned}$$

Thus for X sufficiently large,

$$\frac{\sum_{d\in S'(X,u)} |\mathrm{Sel}_\phi(E^d)|^k}{|S'(X,u)|} = O(\epsilon).$$

This completes the proof. □

References

[CL84] H. Cohen and H. Lenstra. Heuristics on class groups of number fields. *Number Theory, Noordwijkerhout 1983*, pages 33–62, 1984.

[Kan10] D.M. Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Preprint available at http://arxiv. org/abs/1009.1365*, 2010.

[Kla11] Z. Klagsbrun. Selmer ranks of quadratic twists of elliptic curves with partial rational two-torsion. *Preprint available at http://arxiv.org/abs/1201.5408*, 2011.

[Kla12] Z. Klagsbrun. On the distribution of 2-Selmer ranks within quadratic twist families of elliptic curves with partial rational two-torsion. *Preprint available at http://arxiv.org/abs/1203.1030*, 2012.

[KMR11] Z. Klagsbrun, B Mazur, and K. Rubin. A markov model for selmer ranks in families of twists. *Preprint available at http://arxiv.org/pdf/1303.6507v1.pdf*, 2011.

[SD08] P. Swinnerton-Dyer. The effect of twisting on the 2-Selmer group. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 145, pages 513–526. Cambridge Univ Press, 2008.

[Xio13] Maosheng Xiong. On Selmer groups of quadratic twists of elliptic curve a two-torsion over $\mathfrak{q}$. *Mathematika*, 2013.