On the ϕ-Selmer groups of the elliptic curves $y^2 = x^3 - Dx$

Daniel M. Kane* and Jack A. Thorne†

June 23, 2013

Contents

1 Introduction

Consider the family of elliptic curves with 2-isogeny

$$E_D : y^2 = x^3 - Dx,$$

for $D \in \mathbb{Q}^\times$. The 2-isogeny in question is the morphism $\phi : E_D \to E_{-4D}$ given by the formula

$$\phi(x, y) = (y^2/x^2, y(-D - x^2)/x^2).$$

These are the elliptic curves with j-invariant 1728. (The curves E_D, $E_{D'}$ are isomorphic over $\mathbb{Q}$ if and only if $D/D' \in (\mathbb{Q}^\times)^4$.)

Associated to each curve E_D is its *ϕ-Selmer group*, the definition of which we recall in §2 below. It fits into an exact sequence

$$0 \longrightarrow E_{-4D}(\mathbb{Q})/\phi E_D(\mathbb{Q}) \longrightarrow \mathrm{Sel}_\phi(E_D) \longrightarrow Ш(E_D)[\phi] \longrightarrow 0,$$

and can be easily calculated. Computing the groups $\mathrm{Sel}_\phi(E_D)$ and $\mathrm{Sel}_\phi(E_{-4D})$[1] is thus an efficient way to give an upper bound for the rank of the finitely generated abelian group $E_D(\mathbb{Q})$.

*During the period this research was conducted, this author was supported by an NSF postdoctoral research fellowship.
†During the period this research was conducted, the author served as a Clay Research Fellow.

[1] We are saved here from an abuse of notation by the observation that the dual isogeny $\widehat{\phi} : E_{-4D} \to E_D$ is naturally identified with the isogeny $\phi : E_{-4D} \to E_{16D}$ defined above.

In this note we study the behaviour of the groups $\mathrm{Sel}_\phi(E_D)$ as D varies. In order to do this, we organize the curves E_D according to their relative Tamagawa numbers

$$T_D = \#\,\mathrm{Sel}_\phi(E_D)/\#\,\mathrm{Sel}_\phi(E_{-4D}) = 2^{-t_D}.$$

As was first observed by Cassels, T_D may be expressed as a product of local factors, and the integer $t_D \in \mathbb{Z}$ can take on any value. If $t \in \mathbb{Z}_{\geq 0}$, then we define a probability distribution $(\pi_i(t))_{i=0}^{\infty}$ on $\{0, 1, 2, \dots\}$ by the formula

$$\pi_i(t) = \frac{2^i \prod_{k=1}^{\infty}(1 - 2^{-(k+t)})}{\prod_{k=1}^{i}(2^k - 1)(2^{k+t} - 1)}.$$

If $t \in \mathbb{Z}_{\leq 0}$, then we define a probability distribution $(\pi_i(t))_{i=-t}^{\infty}$ on $\{0, 1, 2, \dots\}$ by the formula $\pi_i(t) = \pi_{i+t}(-t)$ if $i + t \geq 0$, and $\pi_i(t) = 0$ otherwise. (See Table 3.3 below for some numerical values.) We can now state our first main result.

Theorem 1.1 (Theorem 5.3)**.** *Let $t \in \mathbb{Z}$, and for each $X > 0$ let $\mathcal{S}_t(X)$ denote the set of fourth-power free integers D such that $t_D = t$ and $-X < D < X$. Then for each $k \geq 1$, the limit*

$$\lim_{X \to \infty} \frac{\#\{D \in \mathcal{S}_t(X) \mid \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k\}}{\#\mathcal{S}_t(X)}$$

exists, and is equal to $\pi_{k-1}(t)$.

The above result is derived from another, which is in a sense more precise. Fix a non-zero integer F, and let S_0 denote the set of primes dividing F, together with the prime 2. Fix a class $\mathcal{C} \in \prod_{p \in S_0} \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^4$.

Theorem 1.2 (Theorem 5.1)**.** *If $X > 0$, let $\mathcal{S}_{F,\mathcal{C}}(X)$ denote the set of integers $-X < D < X$ of the form $D = Fp_1 \dots p_N$, where $p_1, \dots, p_N$ are pairwise distinct primes, coprime to S_0, such that the image of the product $p_1 \dots p_N$ in $\prod_{p \in S_0} \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^4$ is equal to $\mathcal{C}$. Then:*

1. *The relative Tamagawa number $T_D = 2^{-t_D}$ is independent of the choice of $D \in \mathcal{S}_{F,\mathcal{C}}(X)$.*
2. *For each integer $k \geq 1$,*

$$\lim_{X \to \infty} \frac{\#\{D \in \mathcal{S}_{F,\mathcal{C}}(X) \mid \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k\}}{\#\mathcal{S}_{F,\mathcal{C}}(X)}$$

exists and is equal to $\pi_{k-1}(t_D)$.

The proof of Theorem 1.2 follows similar lines to that of [Kan, Theorem 3]. We first prove a result (Theorem 4.1) modeled after the main theorem of [SD08]. Given an integer $D = Fp_1 \dots p_N \in \mathcal{S}_{F,\mathcal{C}}(X)$, the ϕ-Selmer group can be represented as the kernel of a $(\#S_0 + N + t_D) \times (\#S_0 + N)$ matrix $A = A_D$ with $\mathbb{F}_2$-coefficients, whose entries can be written down explicitly in terms of Legendre symbols involving the primes of $S_0 \cup \{p_1, \dots, p_N\}$. Supposing these entries to be independently and uniformly distributed, subject only to the constraints coming from quadratic reciprocity, gives a probability distribution on the quantity $\dim_{\mathbb{F}_2} \ker(A)$. We first show that for each $k \geq 1$, the limit

$$\lim_{N \to \infty} \mathbb{P}(\dim_{\mathbb{F}_2} \ker(A) = k)$$

exists and is equal to $\pi_{k-1}(t_D)$. This is done by showing that, as more rows and columns are added to the matrix A, the quantity $\dim_{\mathbb{F}_2} \ker(A)$ evolves, with high probability, according to a Markov process. As N tends to infinity, the probability of being in any given state converges to the invariant distribution of this Markov process, which is exactly $(\pi_i(t_D))_{i=0}^{\infty}$.

To upgrade this to a result about natural densities, we argue as in [Kan]. The moments of $\#\,\mathrm{Sel}_\phi(E_D)$ are closely related to the average values taken by Dirichlet characters at product of primes. We first establish the following result concerning these moments.

Theorem 1.3 (Proposition 5.2)**.** *Let $m \geq 0$ be an integer. Let $S'_{F,\mathcal{C}}(X)$ be the set of D in $S_{F,\mathcal{C}}(X)$ so that $\omega(D)$, the number of distinct prime divisors of D satisfies $|\omega(D) - \log\log(X)| < \log\log(X)^{3/4}$. Then the limit*

$$\lim_{X\to\infty} \frac{\sum_{D\in S'_{F,\mathcal{C}}(X)} (\#\operatorname{Sel}_\phi(E_D))^m}{\#S'_{F,\mathcal{C}}(X)}$$

exists, and equals

$$\sum_{k=1}^{\infty} 2^{mk}\pi_{k-1}(t) = 2\left(1 + \sum_{n=1}^{m} 2^{-nt} \begin{bmatrix} m \\ n \end{bmatrix}_2\right).$$

(Here we write $\begin{bmatrix} m \\ n \end{bmatrix}_q$ for the usual q-binomial coefficient; see Proposition 3.2 below.) It should be noted that as $X \to \infty$, the density of $S'_{F,\mathcal{C}}(X)$ within $S_{F,\mathcal{C}}(X)$, goes to 1. We expect that this result should hold with $S'_{F,\mathcal{C}}(X)$ replaced by $S_{F,\mathcal{C}}(X)$, but are unable to prove this for technical reasons. We can then deduce the statement of Theorem 1.2 above. Taking $m = 1$ in Theorem 1.3, we obtain:

Corollary 1.4. *The limit*

$$\lim_{X\to\infty} \frac{\sum_{D\in S'_{F,\mathcal{C}}(X)} (\#\operatorname{Sel}_\phi(E_D) - 2)/T_D}{\#S'_{F,\mathcal{C}}(X)}$$

exists, and is equal to 2. In particular, it does not depend on the choice of F or $\mathcal{C}$.

The consideration of this weighted average is natural from the perspective of the calculations appearing in the work of Bhargava and his collaborators; compare, for example, the proof of [BS, Proposition 5.12]. One can interpret the number $\#\operatorname{Sel}_\phi(E_D) - 2$ as the number of 'non-trivial' elements of the ϕ-Selmer group, the 'trivial' ones being represented by the identity and the image of the 2-torsion point $(0, 0)$ (which is almost always non-zero.)

We now describe the organization of this paper. In §2 below, we recall some basic facts about the arithmetic of the curves E_D. In particular, we give the definition of the group $\operatorname{Sel}_\phi(E_D)$, and a formula for the relative Tamagawa number T_D as a product of local factors. In §3, we study the basic properties of the distributions $(\pi_i(t))_{i=0}^{\infty}$, and their interpretation in terms of certain Markov chains. Inspired by the work of Poonen and Rains [PR12], we also give a heuristic interpretation of these distributions in terms of linear algebra; in this optic, the quantity $\dim_{\mathbb{F}_2} \operatorname{Sel}_\phi(E_D)$ is distributed as if the ϕ-Selmer group (modulo the image of the 2-torsion point $(0, 0)$) were the kernel of a random homomorphism $\mathbb{F}_2^s \to \mathbb{F}_2^{s+t_D}$, for some indeterminate s. This model also explains the origins of the Markov chains in the description of the evolution of the ϕ-Selmer group.

In §4, we prove our first approximation to Theorem 1.2. Finally in §5, we prove Theorem 1.2 and Theorem 1.3, and deduce Theorem 1.1 as a consequence.

1.1 Acknowledgements

The second author would like to thank Manjul Bhargava and Arul Shankar for useful conversations. This collaboration was begun at the 'Arithmetic of abelian varieties in families' workshop at EPFL in November 2012, and we thank the organizers for the stimulating environment.

2 Background

We consider again the curves

$$E_D : y^2 = x^3 - Dx,$$

now assuming for simplicity that D is a fourth-power free integer. The point $(0, 0) \in E_D(\mathbb{Q})$ is a 2-torsion point, and generates the kernel of the isogeny $\phi : E_D \to E_{-4D}$ of the introduction. For more information about the objects under consideration here, we refer the reader to [Sil09, Ch. X].

Proposition 2.1. 1. *The curve E_D has good reduction at all primes $p \nmid 2D$.*

2. *Suppose that $D \neq -4$ and D is not a square. Then $E_D(\mathbb{Q})_{tors}$ is generated by $(0,0)$.*

The ϕ-Selmer group $\mathrm{Sel}_\phi(E_D)$ is defined as the kernel of the natural map of Galois cohomology groups:

$$H^1(\mathbb{Q}, E_D[\phi]) \to \prod_v H^1(\mathbb{Q}_v, E_D),$$

the product running over all places v of $\mathbb{Q}$. The reason for studying this group is the existence of the 'Kummer' exact sequence associated to ϕ:

$$0 \to E_D[\phi] \to E_D \to E_{-4D} \to 0.$$

Thus there is an injection $E_{-4D}(\mathbb{Q})/\phi E_D(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E_D[\phi])$, with image contained in the (finite) subgroup $\mathrm{Sel}_\phi(E_D)$. Writing $W_{D,v} \subset H^1(\mathbb{Q}, E_D[\phi])$ for the image of the group of local points $E_{-4D}(\mathbb{Q}_v)/\phi E_D(\mathbb{Q}_v)$, we can define equivalently

$$\mathrm{Sel}_\phi(E_D) = \ker\left[H^1(\mathbb{Q}, E_D[\phi]) \to \prod_v H^1(\mathbb{Q}_v, E_D[\phi])/W_{D,v}\right].$$

The following observation is basic to what follows.

Proposition 2.2. 1. *There is a canonical isomorphism of finite group schemes $E_D[\phi] \cong \mu_2$, and hence for any extension $k/\mathbb{Q}$ a canonical identification $H^1(k, E_D[\phi]) \cong k^\times/(k^\times)^2$.*

2. *Suppose that $v = \infty$. If $D < 0$, then $W_{D,v} = \langle \pm 1 \rangle \subset \mathbb{R}^\times/(\mathbb{R}^\times)^2$. If $D > 0$, then $W_{D,v}$ is trivial.*

3. *Suppose that v is the place corresponding to an odd prime p, and let p^a be the largest power of p dividing D. Then we have*

$$W_{D,v} = \begin{cases} \langle \mathbb{Z}_p^\times \rangle & a = 0 \text{ or } a = 2,\ p \equiv 1 \bmod 4 \text{ and } D \notin (\mathbb{Q}_p^\times)^2 \\ \langle D \rangle & a = 1 \text{ or } 3 \\ \langle \pm\sqrt{D} \rangle & a = 2 \text{ and } D \in (\mathbb{Q}_p^\times)^2 \\ \langle 1 \rangle & a = 2,\ p \equiv 3 \bmod 4 \text{ and } D \notin (\mathbb{Q}_p^\times)^2. \end{cases}$$

4. *Suppose that v is the place corresponding to the prime 2. Then we have*

$$W_{D,v} = \begin{cases} \langle 2, 5 \rangle & D \equiv 1 \bmod 16 \\ \langle -1, 5 \rangle & D \equiv 3, 11 \bmod 16 \\ \langle 5 \rangle & D \equiv 5, 9 \bmod 16 \\ \langle -1, 2, 5 \rangle & D \equiv 7, 15 \bmod 16 \\ \langle -2, 5 \rangle & D \equiv 13 \bmod 16 \\ \langle D \rangle & D \text{ is even.} \end{cases}$$

Proof. The first part is immediate. The rest is contained in [Got01, §3]. □

The variation of the Selmer groups $\mathrm{Sel}_\phi(E_D)$ and $\mathrm{Sel}_\phi(E_{-4D})$ is subject to one major constraint. We define the relative Tamagawa number of ϕ as the quotient

$$T_D = \#\mathrm{Sel}_\phi(E_D)/\#\mathrm{Sel}_\phi(E_{-4D}) = 2^{-t_D}.$$

A theorem of Cassels [Cas65] implies that this is a purely local quantity:

$$T_D = \prod_v |W_{D,v}|/2,$$

where $W_{D,v} \subset H^1(\mathbb{Q}_v, E_D[\phi])$ is the subspace of local conditions. Comparing with Proposition 2.2, see that the factor $|W_{D,v}|/2$ can be non-trivial only if $v = \infty, 2$, or p, where $p \equiv 3 \bmod 4$ and $p^2 || D$. We make two further remarks. First, the parity of t_D is the same as that of the root number of E_D:

$$(-1)^{t_D} = w(E_D).$$

For the curves E_D, this is a theorem of Birch-Stephens [BS66]. Second, as long as $|D|$ is not a square, the torsion point $(0,0)$ has non-trivial image in $\mathrm{Sel}_\phi(E_D)$ and $\mathrm{Sel}_\phi(E_{-4D})$. If one further assumes that $t_D < 0$, we obtain the inequality $\#\mathrm{Sel}_\phi(E_D) \geq 2^{1-t_D}$. (This is the reason that the probability distributions of the introduction are supported in $\{-t_D, 1-t_D, 2-t_D, \dots\}$ when $t_D < 0$.)

3 Probabilities

In this section we define and study the probability distributions introduced in §1. We then introduce some related Markov chains, and realize the distributions as the invariant distributions of the Markov chains. Finally, we give an interpretation of all of these objects in terms of linear algebra.

3.1 A probability distribution

We begin by recalling some remarkable identities.

Lemma 3.1. *We have the following equalities of formal power series:*

$$\prod_{i=1}^{\infty}\left(1-\frac{1}{q^i z}\right)^{-1} = 1+\sum_{n=1}^{\infty}\frac{q^n}{\prod_{j=1}^{n}(q^j-1)(q^j z-1)} \tag{3.1}$$

and

$$\beta\left(1+\sum_{n=1}^{\infty}\frac{q^n x^n}{\prod_{j=1}^{n}(q^j-1)(q^j z-1)}\right) = 1+\sum_{n=1}^{\infty}\frac{(x-1)(x-q)\dots(x-q^{n-1})}{z^n(q^n-1)(q^n-q)\dots(q^n-q^{n-1})}, \tag{3.2}$$

where

$$\beta = \prod_{i=1}^{\infty}\left(1-\frac{1}{q^i z}\right).$$

Proof. The first of these identities is [Jac29, §64, (1)]. We leave the second as an exercise for the reader. □

We fix for this section an integer t. (Later, the parameter t will play the role of the exponent of the relative Tamagawa number $T_D = 2^{-t}$.) Let us first suppose that $t \geq 0$. Let $q = 2$ and $z = 2^t$ in the above identities. Then taking $x = 1$ in equation 3.2 gives

$$\beta\left(1+\sum_{n=1}^{\infty}\frac{2^n}{\prod_{j=1}^{n}(2^j-1)(2^{j+t}-1)}\right) = 1,$$

where now by definition $\beta = \prod_{i=1}^{\infty}(1-2^{-i-t})$. Define $\pi_0(t) = \beta$ and for each $i \geq 1$,

$$\pi_i(t) = \frac{2^i\beta}{\prod_{j=1}^{i}(2^j-1)(2^{j+t}-1)}.$$

Then $\sum_{i=0}^{\infty}\pi_i(t) = 1$, and this does indeed define a probability distribution.

If $t \leq 0$, when we define $\pi_i(t) = \pi_{i+t}(-t)$. Then again $(\pi_i(t))_{i=0}^{\infty}$ defines a probability distribution on $\{0, 1, 2, \dots\}$, and we have $\pi_i(t) > 0$ if and only if $i \geq t$. Here is a table showing the value of $\pi_i(t)$ for some small values of i and t:[2]

t	$\pi_0(t)$	$\pi_1(t)$	$\pi_2(t)$	$\pi_3(t)$	$\pi_4(t)$
0	0.288788	0.577576	0.128350	0.005239	0.000047
1	0.577576	0.385051	0.036672	0.000699	0.000003
2	0.770102	0.220029	0.009779	0.000090	0.000000
3	0.880116	0.117349	0.002524	0.000011	0.000000
4	0.938791	0.060567	0.000641	0.000001	0.000000
5	0.969074	0.030764	0.000161	0.000000	0.000000

(3.3)

Proposition 3.2. *Define a random variable X valued in $\{0, 1, 2, 3, \dots\}$ by $\mathbb{P}(X = i) = \pi_i(t)$. Then the m^{th}-moment of 2^X exists and is equal to*

$$\mathbb{E}(2^{mX}) = 1+\sum_{n=1}^{m}2^{-nt}\begin{bmatrix}m\\n\end{bmatrix}_2.$$

[2] Values are shown here to 6 decimal places.

In particular, $\mathbb{E}(2^X)$ exists and is equal to $1 + 2^{-t}$. (Here we write $\begin{bmatrix} m \\ n \end{bmatrix}_q = \prod_{i=1}^{n} \frac{(q^m - q^{i-1})}{(q^n - q^{i-1})}$ for the usual q-binomial coefficient.)

Proof. Apply equation 3.2 with $x = 2^m$. □

3.2 A Markov chain

If $t \in \mathbb{Z}_{\geq 0}$, we define a Markov chain $(X_n(t))_{n \geq 0}$ with state space $\mathbb{N} = \{0, 1, 2, \dots\}$, and transition probabilities given by:

$$\mathbb{P}(X_{n+1} = j \mid X_n = i) = \begin{cases} 2^{-(2k+t+1)} & j = i+1 \\ (1 - 2^{-k})(1 - 2^{(k+t)}) & j = i-1 \\ (1 + 2^{-t} + 2^{-(t+i+1)}) & j = i. \end{cases} \tag{3.4}$$

If $t = -s \in \mathbb{Z}_{\leq 0}$, then we define a Markov chain $(X_n(t))_{n \geq 0}$ with state space $\{s, s+1, s+2, \dots\}$, and transition probabilities given by the same formulae. We observe that in this case $X_\bullet(t)$ is a Markov chain of type $s + X_\bullet(-t)$. (We refer the reader unfamiliar with Markov chains to [Nor98].)

The object of this section is to prove the following result.

Theorem 3.3. 1. *The distribution $\pi_i(t)$ of the previous section is an invariant distribution for the Markov chain $(X_n(t))_{n \geq 0}$.*

2. *Let $\mu = (\mu_m)_{m \geq 0}$ be an initial probability distribution for $(X_n(t))_{n \geq 0}$. Then there exist constants $c_0, c_1 > 0$ depending only on t such that*

$$|\mathbb{P}_\mu(X_n(t) = i) - \pi_i| \leq c_0/n + c_1/n \cdot \sum_{m \geq 0} m\mu_m.$$

Corollary 3.4. *Let $\mu = (\mu_m)_{m \geq 0}$ be an initial probability distribution for $(X_n(t))_{n \geq 0}$ which is supported in the range $0 \leq m \leq \alpha$, for some $\alpha \geq 1$. Then*

$$|\mathbb{P}_\mu(X_n(t) = i) - \pi_i| = O(\alpha/n),$$

where the implied constant depends only on t.

The rest of this section is devoted to the proof of Theorem 3.3. By symmetry, we can assume that $t \geq 0$. For simplicity, let us in fact assume that $t = 0$, since this is the 'least recurrent' Markov chain in the family. We now write $\pi_i = \pi_i(0)$ and $X_n = X_n(0)$.

Lemma 3.5. *$(\pi_i)_{i=0}^{\infty}$ is the invariant distribution of the Markov chain $(X_n)_{n \geq 0}$. The chain is positive recurrent.*

Proof. It is easy to check that $(\pi_i)_{i=0}^{\infty}$ satisfies the detailed balance equations, which implies that it must be a invariant distribution. The existence of the invariant distribution implies that $(X_n)_{n \geq 0}$ is indeed positive recurrent. □

Now introduce a Markov process $(X_n, Y_n)_{n \geq 0}$ on $\mathbb{N} \times \mathbb{N}$, where X_n, Y_n are independent Markov chains with the same transition matrices. We assume that the initial distributions of X_n and Y_n are μ and π, respectively, and define a random variable

$$T_0 = \inf\{n \geq 0 \mid X_n = Y_n = 0\}.$$

Since $(X_n)_{n \geq 0}$ is positive recurrent, the same is true for this joint chain, and $\mathbb{E}_0(T_0) < \infty$. (For this and the proof of the next lemma, compare [Nor98, §1.8].)

Lemma 3.6. *With notation as above, we have*

$$|\mathbb{P}_\mu(X_n = i) - \pi_i| \leq \mathbb{E}_\mu(T_0)/(n-1).$$

Proof. Let $Z_n = X_n$ if $n < T_0$, and $Z_n = Y_n$ if $n \geq T_0$. Then $(Z_n)_{n\geq 0}$ is a Markov chain with the same transition probabilities as $(X_n)_{n\geq 0}$ and initial distribution μ. We then have

$$|\mathbb{P}_\mu(X_n = i) - \pi_i| = |\mathbb{P}_\mu(Z_n = i) - \mathbb{P}_\mu(Y_n = i)|$$

$$= |(\mathbb{P}_\mu(X_n = i, n < T_0) + \mathbb{P}_\mu(Y_n = i, n \geq T_0)) - (\mathbb{P}_\mu(Y_n = i, n < T_0) + \mathbb{P}_\mu(Y_n = i, n \geq T_0))|$$

$$= |\mathbb{P}_\mu(X_n = i, n < T_0) - \mathbb{P}_\mu(Y_n = i, n < T_0)| \leq \mathbb{P}_\mu(n < T_0) \leq \mathbb{E}_\mu(T_0)/(n-1),$$

by Markov's inequality. □

Corollary 3.7. *Let δ_m denote the Dirac distribution centered at m: $\mathbb{P}_{\delta_m}(X_0 = i) = \delta_{im}$. Let $\sigma_m = \mathbb{E}_{\delta_m}(T_0)$. Then*

$$|\mathbb{P}_\mu(X_n = i) - \pi_i| \leq \left(\sum_{m\geq 0} \mu_m \sigma_m\right)/(n-1).$$

To prove Theorem 3.3, it therefore suffices to show that there exist constants $C, D > 0$ such that $\sigma_m \leq C + mD$ (and in particular, $\sigma_m < \infty$). We now show this by calculating σ_m explicitly. We first introduce the auxiliary variable $S_0 = \inf\{n \geq 0 \mid X_n = 0\}$, and define $\tau_m = \mathbb{E}_{\delta_m}(S_0)$, the expected first passage time from m to 0. As is well-known, the expected return time $\mathbb{E}_{\delta_0}(S_0)$ equals $1/\pi_0$.

A well-known calculation for birth-death processes shows that

$$\tau_1 = 4 + \sum_{k=2}^{\infty} \left(\frac{\prod_{i=1}^{k-1} 2^{-2i+1}}{\prod_{i=1}^{k}(1-2^{-i})^2}\right) < 5 < \infty,$$

while for $m \geq 1$

$$\tau_{m+1} = \tau_m + \sum_{k=m+1}^{\infty} \left(\frac{\prod_{i=m+1}^{k-1} 2^{-2i+1}}{\prod_{i=m+1}^{k}(1-2^{-i})^2}\right) \leq \tau_m + 2.$$

On the other hand, conditional expectation and the strong Markov property show that

$$\sigma_m = \sum_{k=1}^{\infty} (\tau_m + (k-1)/\pi_0)(1-\pi_0)^{k-1}\pi_0 = \tau_m \sum_{k=1}^{\infty} (1-\pi_0)^{k-1}\pi_0 + \sum_{k=1}^{\infty} (k-1)(1-\pi_0)^{k-1}.$$

It is now clear that $\sigma_m < \infty$, and satisfies a bound of the desired type.

3.3 Interpretation in terms of linear algebra

Let D be a fourth-power free integer, and let S denote the set of places of $\mathbb{Q}$ dividing D, together with 2 and ∞. The group $\mathrm{Sel}_\phi(E_D)$ is, by definition, the kernel of the natural map

$$\mathbb{Q}(S,2) \to \prod_{v\in S} V_v/W_{D,v},$$

where $\mathbb{Q}(S,2) \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is the subgroup of elements which are unramified outside S, $V_v = \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$, and $W_{D,v} \subset V_v$ is the subspace of local conditions at v, as described in §2. Now, $\mathbb{Q}(S,2)$ is an $\mathbb{F}_2$-vector space of dimension $\#S$, while $\prod_{v\in S} V_v/W_{D,v}$ is an $\mathbb{F}_2$-vector space of dimension $\#S + t_D$, by the expression for $T_D = 2^{-t_D}$ as a product of local factors. It therefore makes sense to ask if the quantity $\dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D)$ behaves as if $\mathrm{Sel}_\phi(E_D)$ were the kernel of a random homomorphism $\mathbb{F}_2^s \to \mathbb{F}_2^{s+t_D}$, for some $s \geq 0$.

Given the theorems of the introduction, we can rephrase this by asking if the distributions $(\pi_i(t))_{i=0}^\infty$ admit such an interpretation. We now show that this is indeed the case. By symmetry, we can assume that $t \geq 0$. Given an integer $n \geq 1$, let $\Omega(n)$ denote the set of $(n+t)\times n$ matrices A with $\mathbb{F}_2$-coefficients. We endow $\Omega(n)$ with the uniform probability measure. If $k \geq 0$ is an integer, we let $p_{k,n}(t) = \mathbb{P}_\Omega(\dim_{\mathbb{F}_2} \ker(A) = k)$.

Proposition 3.8. *The limit*

$$\lim_{n\to\infty} p_{k,n}(t)$$

exists and is equal to $\pi_k(t)$.

For each $1 \le m \le n$, let A_m denote the upper-left $(m+t) \times m$ submatrix of A. We define random variables $Z_m : \Omega(n) \to \mathbb{Z}_{\ge 0}$ by the formula $Z_m = \dim_{\mathbb{F}_2} \ker(A_m)$.

Lemma 3.9. *The sequence of random variables* $(Z_m)_{m=1}^n$ *is a Markov chain of type* $X_\bullet(t)$.

Proof. Let $Z_m = \dim_{\mathbb{F}_2} \ker(A_m) = k$. We write

$$A_{m+1} = \begin{pmatrix} A_m & w \\ {}^t v & x \end{pmatrix},$$

where $v \in \mathbb{F}_2^m$, $w \in \mathbb{F}_2^{m+t}$, and $x \in \mathbb{F}_2$. A calculation shows that we have the following possibilities for $Z_{m+1} = \dim_{\mathbb{F}_2} \ker(A_{m+1})$:

1. $w \in \mathrm{im}(A_m)$, $v \in \ker(A_m)^\perp$. Then $\dim_{\mathbb{F}_2} \ker(A_{m+1}) = k+1$ if $x \in v \cdot A_m^{-1}(w)$, and $\dim_{\mathbb{F}_2} \ker(A_{m+1}) = k$ otherwise.
2. $w \in \mathrm{im}(A_m)$, $v \notin \ker(A_m)^\perp$. Then $\dim_{\mathbb{F}_2} \ker(A_{m+1}) = k$.
3. $w \notin \mathrm{im}(A_m)$, $v \in \ker(A_m)^\perp$. Then $\dim_{\mathbb{F}_2} \ker(A_{m+1}) = k$.
4. $w \notin \mathrm{im}(A_m)$, $v \notin \ker(A_m)^\perp$. Then $\dim_{\mathbb{F}_2} \ker(A_{m+1}) = k-1$.

We have $\mathbb{P}_\Omega(w \in \mathrm{im}(A_m)) = 2^{-k+t}$ and $\mathbb{P}_\Omega(v \in \ker(A_m)^\perp) = 2^{-k}$. It is now easy to see that the sequence $Z_\bullet$ satisfies the Markov property, with transition probabilities given by equation 3.4. □

Proposition 3.8 now follows from the lemma. Indeed, in the notation of §3.2 we have $p_{k,n}(t) = \mathbb{P}_{\delta_0}(X_n(t) = k)$. This quantity tends to $\pi_k(t)$ as $n \to \infty$, by Corollary 3.4.

4 Markov density

We now come to our first main theorem. We fix a non-zero integer F, and set $S_0 = \{2, \infty\} \cup \{p | F\} = \{2, \infty, q_1, \dots, q_s\}$, say. Fix a class $\mathcal{C}$ in the group

$$\prod_{v \in S_0 \setminus \{\infty\}} \mathbb{Z}_v^\times / (\mathbb{Z}_v^\times)^4.$$

We write $\mathcal{S}(\mathcal{C}, N)$ for the set of integers of the form $Fp_1 \dots p_N$, where the p_i are distinct prime numbers, coprime to S_0, and the product $p_1 \dots p_N$ is of class $\mathcal{C}$. We will study the ϕ-Selmer groups $\mathrm{Sel}_\phi(E_D)$ for $D \in \mathcal{S}(\mathcal{C}, N)$, as $\mathcal{C}$ is fixed and the integer N is allowed to vary. (In what follows, we will view the Legendre symbols $\left(\frac{a}{p}\right)$ as taking values in the $\mathbb{F}_2$, this group being identified with $\{\pm 1\}$ in the natural way.)

Theorem 4.1. 1. *The quantity* $\dim \mathrm{Sel}_\phi(E_D)$, $D \in \mathcal{S}(\mathcal{C}, N)$ *depends only on the following data:*

   (a) *The Legendre symbols* $\left(\frac{-1}{p_i}\right)$ *and* $\left(\frac{2}{p_i}\right)$, $1 \le i \le N$.

   (b) *The Legendre symbols* $\left(\frac{p_i}{q_j}\right)$, $1 \le j \le s$, $1 \le i \le N$.

   (c) *The Legendre symbols* $\left(\frac{p_i}{p_j}\right)$, $1 \le i < j \le N$.

   Moreover, for any choice of assignment of these values, subject to the constraint that $p_1 \dots p_N$ *be of class* $\mathcal{C}$, *there exists* $D \in \mathcal{S}(\mathcal{C}, N)$ *realizing them.*

2. *Let* $k \ge 0$ *be an integer, and let* $p_k(N)$ *denote the probability that* $\dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k$, *the above Legendre symbols being distributed according to the uniform probability measure. Then* $\lim_{N\to\infty} p_k(N)$ *exists and equals* $\pi_{k-1}(t)$, *where* $(\pi_i(t))_{i=0}^\infty$ *is the probability distribution constructed in §3, with parameter* $t = -\log_2 T_D$. *Here* T_D *is the relative Tamagawa number of the isogeny* $\phi : E_D \to E_{-4D}$, *which depends only on* F *and* $\mathcal{C}$.

The rest of this section is devoted to the proof of the above theorem. We first note that, replacing F by $-4F$, we can assume that $F > 0$. We now write the quantity $\mathrm{Sel}_\phi(E_D)$ in terms of a morphism of $\mathbb{F}_2$-vector spaces. Let $S = S_0 \cup \{p_1, \ldots, p_N\}$, and let $X_S = \oplus_{v \in S \setminus \{\infty\}} V_v/W_v$, where $V_v = \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$ and $W_v = W_{D,v}$ is the subspace of local conditions. The $\mathbb{F}_2$-vector space $U_S = \{\lambda \in \mathbb{Q}(S,2) \mid \lambda > 0\}$ has a basis consisting of the elements $2, q_1, \ldots, q_s, p_1, \ldots p_N$. We choose for each $v \in S_0$ a basis of the quotient V_v/W_v. For each $i = 1, \ldots, N$, we take the basis element of V_{p_i}/W_{p_i} corresponding to a non-square in $\mathbb{Z}_{p_i}^\times$.

Lemma 4.2. 1. *The space* $\mathrm{Sel}_\phi(E_D) \subset U_S$ *may be identified with the kernel of the following* $(s+1+t+N) \times (s+1+N)$ *matrix* A_0*:*

$$\begin{pmatrix} & & M & & \mathbf{b}_1 & & \mathbf{b}_N \\ \left(\frac{2}{p_1}\right) & \left(\frac{q_1}{p_1}\right) & \cdots & \left(\frac{q_s}{p_1}\right) & \left(\frac{D/p_1}{p_1}\right) & \cdots & \left(\frac{p_N}{p_1}\right) \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ \left(\frac{2}{p_i}\right) & \left(\frac{q_1}{p_i}\right) & \cdots & \left(\frac{q_s}{p_i}\right) & \left(\frac{p_1}{p_i}\right) & \cdots \left(\frac{D/p_i}{p_i}\right) \cdots & \left(\frac{p_N}{p_i}\right) \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ \left(\frac{2}{p_N}\right) & \left(\frac{q_1}{p_N}\right) & \cdots & \left(\frac{q_s}{p_N}\right) & \left(\frac{p_1}{p_N}\right) & \cdots & \left(\frac{D/p_N}{p_N}\right) \end{pmatrix}.$$

Here M *is an* $(s+1+t) \times (s+1)$ *matrix which depends only on* F *and* $\mathcal{C}$ *and not on* $p_1, \ldots, p_N$*, and the* $\mathbf{b}_i$ *are column vectors of length* $s+1+t$*.*

2. *There exist matrices* S*,* T *and a vector* $\mathbf{v}$ *depending only on* F *and* $\mathcal{C}$ *such that*

$$\mathbf{b}_i = T^t\left(\left(\frac{2}{p_i}\right), \left(\frac{q_1}{p_i}\right), \ldots, \left(\frac{q_s}{p_i}\right)\right)$$

if $p_i \equiv 1 \bmod 4$ *and*

$$\mathbf{b}_i = \mathbf{v} + S^t\left(\left(\frac{2}{p_i}\right), \left(\frac{q_1}{p_i}\right), \ldots, \left(\frac{q_s}{p_i}\right)\right)$$

if $p_i \equiv 3 \bmod 4$*. Moreover, viewing* M *and* T *as homomorphisms* $\mathbb{F}_2^{s+1} \to \mathbb{F}_2^{s+1+t}$*, we have* $\mathrm{im}(M) + \mathrm{im}(T) + \langle \mathbf{b}_i \rangle = \mathbb{F}_2^{s+1+t}$*, for any* i *such that* $p_i \equiv 3 \bmod 4$*.*

Proof. 1. The given matrix represents the homomorphism $U_S \to X_S$, where U_S and X_S are given the above bases.

2. The existence of the matrices S, T and $\mathbf{v}$ follows from quadratic reciprocity. For the spanning statement, it is enough to observe that for any $p \in S_0 \setminus \{\infty\}$, the space V_p is spanned by the images of D, p_i, and the images of all primes p' which are congruent to 1 mod 4.

□

It is apparent from Lemma 4.2 that, the integer F and class $\mathcal{C}$ having been fixed, the quantity $\dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D)$ depends only on the Legendre symbols $\left(\frac{-1}{p_i}\right)$, $\left(\frac{2}{p_i}\right)$, $\left(\frac{q_j}{p_i}\right)$ and $\left(\frac{p_i}{p_j}\right)$. In particular, this proves the first part of Theorem 4.1. We now write

$$\Omega(N) \subset \left[(\mathbb{Z}/8\mathbb{Z})^\times\right]^N \times \left[\prod_{i=1}^{s} \mathbb{F}_{q_i}^\times/(\mathbb{F}_{q_i}^\times)^2\right]^N \times \prod_{i=1}^{N} \prod_{j=i+1}^{N} \mathbb{F}_{p_j}^\times/(\mathbb{F}_{p_j}^\times)^2$$

for the subset of elements such that the product of the first N elements is the equal to the image of the class $\mathcal{C}$. There is an obvious surjective map $\mathcal{S}(\mathcal{C}, N) \to \Omega(N)$, and the map $D \mapsto \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D)$ factors through this one.

In particular, it makes sense to endow $\Omega(N)$ with the uniform probability measure and ask for the distribution of the random variable $X = \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D)$, viewed as a function $\Omega(N) \to \mathbb{Z}_{\geq 0}$. This distribution is given by the quantities $p_k(N)$ described in the second part of Theorem 4.1.

Lemma 4.3. *Let A denote the submatrix of A_0 obtained by deleting the last column and row, and let $n = N - 1$. Then:*

1. *Let $Y = \dim_{\mathbb{F}_2} \ker A$. Then for all $k \in \mathbb{Z}$, we have $\mathbb{P}_\Omega(X = k) = \mathbb{P}_\Omega(Y = k - 1)$.*
2. *Let $\mathcal{S}$ denote the set of functions $\Omega(N) \to \mathbb{F}_2$ consisting of the Legendre symbols $\left(\frac{2}{p_i}\right)$, $1 \leq i \leq n$, $\left(\frac{q_j}{p_i}\right)$, $1 \leq i \leq n$, $1 \leq j \leq s$, $\left(\frac{p_i}{p_j}\right)$, $1 \leq i < j \leq n$, and $\left(\frac{D/p_i}{p_i}\right)$, $1 \leq i \leq n$. Then the elements of $\mathcal{S}$ are mutually independent, identically distributed random variables, each taking the value 0 or 1 with equal probability $1/2$.*

Proof. 1. We show that $X = Y + 1$. The element $D \in \mathrm{Sel}_\phi(E_D)$ gives an element of $\ker(A_0)$ with last entry non-zero. It suffices, therefore, to show that $j \ker(A) \subset \ker(A_0)$, where $j : \mathbb{F}_2^{s+N} \to \mathbb{F}_2^{s+1+N}$ is the natural inclusion with image consisting of elements with last entry zero. Equivalently, we must show that if $u \in U_S$ maps to W_v for all $v \in S \setminus p_N$, then it also maps to W_{p_N}. This follows from the product formula for the Hilbert symbol (here a sum formula, since we write Legendre and Hilbert symbols additively). Indeed, we have

$$\left(\frac{u}{p_N}\right) = (u, p_N)_{p_N} = (u, -D)_{p_N} = \sum_{v \in S \setminus p_N} (u, -D)_v.$$

Since $-D$ annihilates the subspace $W_v \subset V_v = \mathbb{Q}_v^\times / (\mathbb{Q}_v^\times)^2$ of local conditions under the Hilbert symbol, each individual term in the above sum is equal to 0. This gives the result.

2. We must show the independence of the quantities ($1 \leq i \leq n$):

$$\left(\frac{D/p_i}{p_i}\right) = \left(\frac{F}{p_i}\right) + \sum_{\substack{j=1 \\ j \neq i}}^{N} \left(\frac{p_j}{p_i}\right).$$

This follows as $\left(\frac{p_N}{p_i}\right)$ is independent of all other Legendre symbols and takes the values 0 and 1 with equal probability.

□

In studying the behavior of $Y = \dim_{\mathbb{F}_2} \ker A$, we may assume without loss of generality that the primes $p_1, \ldots, p_{n_1}$ are congruent to 3 mod 4, and the primes $p_{n_1+1}, \ldots, p_{n_1+n_2}$, $n_1 + n_2 = n$, are congruent to 1 mod 4. This choice having been fixed, the entries of the matrix A are uniformly random subject to the constraint imposed by quadratic reciprocity, namely that $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_i}\right)$ unless $i, j \leq n_1$, in which case $\left(\frac{p_i}{p_j}\right) = 1 + \left(\frac{p_j}{p_i}\right)$.

Let us therefore introduce the finite set $\omega(n_1, n_2)$ of such $(s + 1 + t + n_1 + n_2) \times (s + 1 + n_1 + n_2)$ matrices, endowed with the uniform probability measure.

Lemma 4.4. *Let $A \in \omega(n_1, n_2)$, and let $1 \leq m \leq n$. Let C denote the upper-left $(s+1+t+m) \times (s+1+m)$ submatrix of A, and let $v \in \mathbb{F}_2^{s+1+m} \setminus \{0\}$. Then $\mathbb{P}_\omega(Cv = 0) \leq 2^{-m}$.*

Proof. Let $\overline{C}$ denote the submatrix of C obtained by deleting the first $s+1+t$ rows. We bound $\mathbb{P}_\omega(Cv = 0)$ by $\mathbb{P}_\omega(\overline{C}v = 0)$. Let us assume, for simplicity, that the last entry v_m of v is non-zero.

Let $\overline{D}$ denote the submatrix of $\overline{C}$ obtained by deleting the last row and column. Conditioning on the choice of $\overline{D}$, it is clear that amongst the 2^{m+s+1} possible choices for $\overline{C}$, each occurring with equal probability, there are 2^{s+1} that give $\overline{C}v = 0$. Thus $\mathbb{P}_\omega(\overline{C}v = 0) = 2^{-m}$. □

If $1 \leq m \leq n$, we write T_m for the $(s + 1 + t + m) \times (s + 1 + m)$ matrix given as follows:

$$T_m = \begin{pmatrix} T & 0 \\ 0 & 1_m \end{pmatrix}.$$

Lemma 4.5. *Let $A \in \omega(n_1, n_2)$, and let $n_1 \leq m \leq n$. Let C denote the upper-left $(s+1+t+m)\times(s+1+m)$ submatrix of A. Then $\mathbb{P}_\omega(\left[T_m^{-1}\operatorname{im}(C)\right] + \ker(C)^\perp \neq \mathbb{F}_2^{s+1+m}) \leq 2^{s+2+t-n_1}$.*

Proof. Let $S_m = \left[T_m^{-1}\operatorname{im}(C)\right]^\perp \cap \ker(C) \setminus \{0\}$. By Markov's inequality, we have

$$\mathbb{P}_\omega(\left[T_m^{-1}\operatorname{im}(C)\right] + \ker(M_0)^\perp \neq \mathbb{F}_2^{s+1+m}) = \mathbb{P}_\omega(S_m \neq \emptyset) \leq \mathbb{E}_\omega(\#S_m).$$

On the other hand, we have $\left[T_m^{-1}\operatorname{im}(C)\right]^\perp = {}^tT_m \ker({}^tC)$, hence $S_m \subset {}^tT_m \ker(C\,{}^tT_m + T_m\,{}^tC) \setminus \{0\}$. The matrix $C\,{}^tT_m + T_m\,{}^tC$ has rank at least $n_1 - 1$ (consider the lower-right $m \times m$ submatrix). We then have

$$\mathbb{E}_\omega(\#S_m) \leq 2^{s+1+t+m-(n_1-1)} \cdot 2^{-m} = 2^{s+2+t-n_1},$$

by Lemma 4.4. This completes the proof. □

Lemma 4.6.
1. *Let C denote the upper-left $(s+1+t+n_1)\times(s+1+n_1)$ submatrix of A. Let $k \in \mathbb{Z}_{\geq 0}$. Then $\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(C) \geq k) \leq 2^{s+1-k}$.*
2. *Let $n_1 \leq m \leq n$, and let C denote the upper-left $(s+1+t+m)\times(s+1+m)$ submatrix of A. Suppose that $n_1 > 0$. Then $\operatorname{im}(C) + \operatorname{im}(T_m) = \mathbb{F}_2^{s+1+t+m}$.*

Proof.
1. By Markov's inequality and Lemma 4.4,

$$\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(C) \geq k) \leq \mathbb{E}_\omega(\#\ker(C))/2^k \leq 2^{s+2+n_1} \cdot 2^{-n_1} \cdot 2^{-k} = 2^{s+2-k}.$$

2. This follows immediately from the second part of Lemma 4.2.

□

We now fix an integer $n_1 \leq m \leq n-1$ and a choice of upper-left $(s+1+t+m)\times(s+1+m)$ submatrix C of A, and find the distribution of the upper-left $(s+1+t+m+1)\times(s+1+m+1)$ submatrix C' of A, conditioned on this choice of C. We can write

$$C' = \begin{pmatrix} C & T_m v \\ {}^tv & x \end{pmatrix},$$

where $v \in \mathbb{F}_2^m$ and $x \in \mathbb{F}_2$. The choice of C being fixed, there are $2^{s+1+m+1}$ choices of pair (v, x), each occurring with equal probability.

Lemma 4.7. *Suppose that $\left[T_m^{-1}\operatorname{im}(C)\right] + \ker(C)^\perp = \mathbb{F}_2^{s+1+m}$. Let $k = \dim_{\mathbb{F}_2}\ker(C)$. Then we have*

$$\mathbb{P}_\omega(\dim\ker(C') = s \mid C) = \begin{cases} 2^{-(2k+t+1)} & s = k+1 \\ 2^{-(2k+1)} + 2(2^{-k} - 2^{-2k}) & s = k \\ (1-2^{-k})(1-2^{-(k+t)}) & s = k-1 \end{cases}$$

Proof. A calculation shows that we have the following possibilities:
1. $T_m v \in \operatorname{im}(C')$, $v \in \ker(C')^\perp$. Then $\dim\ker(C) = k+1$ if $x \in v \cdot C'^{-1}(T_m v)$, and k otherwise.
2. $T_m v \in \operatorname{im}(C')$, $v \notin \ker(C')^\perp$. Then $\dim\ker(C) = k$.
3. $T_m v \notin \operatorname{im}(C')$, $v \in \ker(C')^\perp$. Then $\dim\ker(C) = k$.
4. $T_m v \notin \operatorname{im}(C')$, $v \notin \ker(C')^\perp$. Then $\dim\ker(C) = k-1$.

We have $\mathbb{P}_\omega(v \in \ker(C)^\perp \mid C) = 2^{-k}$. Using that $\operatorname{im}(C) + \operatorname{im}(T_m) = \mathbb{F}_2^{s+1+t+m}$, we have $\mathbb{P}_\omega(T_m v \in \operatorname{im}(C) \mid C) = 2^{-(k+t)}$. Under the assumption $\left[T_m^{-1}\operatorname{im}(C)\right] + \ker(C)^\perp = \mathbb{F}_2^{s+1+m}$, these two events are independent, leading to the probabilities described in the statement of the lemma. □

Theorem 4.8. . *We have for all integers $k \geq 0$:*

$$\mathbb{P}_\Omega(\dim_{\mathbb{F}_2}\ker(A) = k) \to \pi_k(t) \text{ as } N \to \infty.$$

Proof. The quantity $|\mathbb{P}_\Omega(\dim_{\mathbb{F}_2}\ker(A)=k)-\pi_k(t)|$ is bounded above by the expression

$$\mathbb{P}_\Omega(|n_1-n/2|\geq n/6)+\sum_{\substack{n_1+n_2=n\\ n_1/2\leq n_2\leq 2n_1}}\mathbb{P}_\Omega(n_1+n_2=n)|\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(A)=k)-\pi_k|.$$

The first term here tends to zero as $n\to\infty$, by Chebyshev's inequality; for the second term, we have for any $\alpha>0$:

$$|\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(A)=k)-\pi_k(t)|\leq\mathbb{P}_\omega(d_{n_1}\geq\alpha)+|\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(A)=k\mid d_{n_1}\leq\alpha)-\pi_k|.$$

Here d_{n_1} is, by definition, the dimension of the kernel of the upper-left $(s+1+t+n_1)\times(s+1+n_1)$-submatrix of A. By Lemma 4.6, we have $\mathbb{P}_\omega(d_{n_1}\geq\alpha)\leq 2^{s+2-\alpha}$. On the other hand, we have by Corollary 3.4:

$$|\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(A)=k\mid d_{n_1}\leq\alpha)-\pi_k(t)|\leq\mathbb{P}_\omega(\mathcal{E})+O(\alpha/n_2)\leq\mathbb{P}_\omega(\mathcal{E})+O(\alpha/n),$$

where $\mathcal{E}$ is the event that $\left[T_m^{-1}\operatorname{im}(C)\right]+\ker(C)^\perp\neq\mathbb{F}_2^{s+1+m}$, C the upper left $(s+1+t+m)\times(s+1+m)$ submatrix of A, for some $n_1\leq m\leq n-1$. Lemma 4.7 shows that conditional on $\omega(n_1,n_2)\setminus\mathcal{E}$, the quantity $\dim_{\mathbb{F}_2}\ker(C)$ evolves according to the Markov chain $(X_n(t))_{n\geq 0}$ described in §3.2.

On the other hand, we have $\mathbb{P}_\omega(\mathcal{E})\leq n_2 2^{s+2+t-n_1}\leq 3n\cdot 2^{s+2+t-n/3}$, by Lemma 4.5. We therefore have

$$\sum_{\substack{n_1+n_2=n\\ n_1/2\leq n_2\leq 2n_1}}\mathbb{P}_\Omega(n_1+n_2=n)|\mathbb{P}_\omega(\dim_{\mathbb{F}_2}\ker(A)=k)-\pi_k(t)|=O(2^{-\alpha}+n2^{-n/3}+\alpha/n),$$

the implied constant depending only on s and t. Choosing $\alpha=\sqrt{n}$ and letting $n\to\infty$ gives the result. □

Theorem 4.1 now follows immediately from Theorem 4.8.

5 Natural Density

For F and $\mathcal{C}$ as in Theorem 4.1, let $S(\mathcal{C})=\bigcup_{N=0}^\infty S(\mathcal{C},N)$. Theorem 4.1 tells us about the limiting distribution of ranks of $\mathrm{Sel}_\phi(E_D)$ for $D\in S(\mathcal{C})$, in roughly the same sense that [SD08] tells us about the densities of ranks of 2-Selmer groups of twists of a given elliptic curve with full 2-torsion. In the same way that [Kan] improved the latter result to talk about the natural density of such twists, we will be able to obtain our results in terms of the natural density as well. In particular, we will show:

Theorem 5.1. *For any fixed $k,F,\mathcal{C}$,*

$$\lim_{N\to\infty}\frac{\#\{|D|\leq N:D\in S(\mathcal{C}),\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E_D)=d\}}{\#\{|D|\leq N:D\in S(\mathcal{C})\}}=\pi_{d-1}(t).$$

The proof of Theorem 5.1 will be analogous to the proof of the main theorem of [Kan]. In particular, our approach will be to prove that the average moments of the size of the Selmer group are correct. In particular, we will restrict our attention to the case when $H=D/F$ has exactly n prime divisors for $n\approx\log\log N$. For convenience of notation, let $\omega(n)$ be the number of distinct prime factors of n. Also, let $\pi_{d,\mathcal{C}}(n)$ be $p_d(n)$ in the notation of Theorem 4.1.

Throughout the rest of this section, we consider F and $\mathcal{C}$ to be fixed.

Proposition 5.2. *For any integer $k\geq 0$,*

$$\lim_{N\to\infty}\frac{\sum_{\substack{|D|\leq N|F|:D\in S(\mathcal{C})\\ |\omega(D/F)-\log\log(N)|\leq\log\log(N)^{3/4}}}|\mathrm{Sel}_\phi(E_D)|^k}{\#\{|D|\leq N|F|:D\in S(\mathcal{C}),|\omega(D/F)-\log\log(N)|\leq\log\log(N)^{3/4}\}}=\sum_{d=0}^\infty 2^{kd}\pi_{d,\mathcal{C}}.$$

Proof. For distinct primes $p_1, \dots, p_n$ let $A_{p_1,\dots,p_n}$ be the matrix given in Lemma 4.2 for $D = Fp_1 \cdots p_n$. Letting $D = Fp_1p_2 \cdots p_n$, we have that

$$\begin{aligned}
|\operatorname{Sel}_\phi(E_D)| &= |\ker(A_{p_i})| \\
&= \sum_{v \in \mathbb{F}_2^{s+1+t+n}} \begin{cases} 1 & \text{if } A_{p_i} v = 0 \\ 0 & \text{else} \end{cases} \\
&= \sum_{v \in \mathbb{F}_2^{s+1+t+n}} \frac{1}{2^{s+1+n}} \sum_{w \in \mathbb{F}_2^{s+1+n}} (-1)^{\langle A_{p_i} v, w \rangle} \\
&= \frac{1}{2^{s+1+n}} \sum_{v \in \mathbb{F}_2^{s+1+t+n}, w \in \mathbb{F}_2^{s+1+n}} (-1)^{\langle A_{p_i} v, w \rangle}.
\end{aligned}$$

Therefore we have that

$$|\operatorname{Sel}_\phi(E_D)|^k = \frac{1}{2^{k(s+1+n)}} \sum_{v^j \in \mathbb{F}_2^{s+1+t+n}, w^j \in \mathbb{F}_2^{s+1+n}} (-1)^{\sum_{j=1}^k \langle A_{p_i} v^j, w^j \rangle}.$$

For fixed $n \approx \log\log(N)$ we wish to compute

$$\begin{aligned}
&\sum_{\substack{|D| \le N|F| \\ D \in S(\mathcal{C}) \\ \omega(D/F) = n}} |\operatorname{Sel}_\phi(E_D)|^k \\
&= \frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1 \cdots p_n \le N \\ p_1 \cdots p_n \in \mathcal{C}}} |\operatorname{Sel}_\phi(E_{Fp_1 \cdots p_n})|^k \\
&= \frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1 \cdots p_n \le N \\ p_1 \cdots p_n \in \mathcal{C}}} \frac{1}{2^{k(s+1+n)}} \sum_{\substack{v^j \in \mathbb{F}_2^{s+1+t+n} \\ w^j \in \mathbb{F}_2^{s+1+n}}} (-1)^{\sum_{j=1}^k \langle A_{p_i} v^j, w^j \rangle} \\
&= \frac{1}{2^{k(s+1+n)}} \sum_{\substack{v^j \in \mathbb{F}_2^{s+1+t+n} \\ w^j \in \mathbb{F}_2^{s+1+n}}} \frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1 \cdots p_n \le N \\ p_1 \cdots p_n \in \mathcal{C}}} (-1)^{\sum_{j=1}^k \langle A_{p_i} v^j, w^j \rangle} \\
&= \frac{1}{2^{k(s+1+n)}} \sum_{\substack{v^j \in \mathbb{F}_2^{s+1+t+n} \\ w^j \in \mathbb{F}_2^{s+1+n}}} \frac{1}{|(\mathbb{Z}/F)^*/((\mathbb{Z}/F)^*)^4|} \sum_{\substack{\chi \pmod{|F|} \\ \chi^4 = 1}} \bar{\chi}(\mathcal{C}) \\
&\qquad \frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1 \cdots p_n \le N}} \chi(p_1 \cdots p_n) (-1)^{\sum_{j=1}^k \langle A_{p_i} v^j, w^j \rangle}.
\end{aligned}$$

The thing to note here is that once the values of v^j and w^j and the values of the p_i have been fixed modulo 4, the inner summand can be written as a product of terms of the form $\left(\frac{p_i}{p_\ell}\right)$ and $(-1)^{\epsilon(p_i)\epsilon(p_\ell)}$ (where here $\epsilon(p) = (p-1)/2$), and $\chi_i(p_i)$ for quadratic characters χ_i with modulus dividing $|F|$. Sums of this form were dealt with extensively in Propositions 9 and 10 of [Kan].

In order to deal with the dependence modulo 4, let $A^{\epsilon_1,\dots,\epsilon_n}_{p_1,\dots,p_n}$ be the matrix

$$\begin{pmatrix} \left(\frac{D/p_1}{p_1}\right) & \cdots & \left(\frac{p_N}{p_1}\right) & \left(\frac{2}{p_1}\right) & \left(\frac{q_1}{p_1}\right) & \cdots & \left(\frac{q_s}{p_1}\right) \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \left(\frac{p_1}{p_i}\right) & \cdots \left(\frac{D/p_i}{p_i}\right) \cdots & \left(\frac{p_N}{p_i}\right) & \left(\frac{2}{p_i}\right) & \left(\frac{q_1}{p_i}\right) & \cdots & \left(\frac{q_s}{p_i}\right) \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \left(\frac{p_1}{p_N}\right) & \cdots & \left(\frac{D/p_N}{p_N}\right) & \left(\frac{2}{p_N}\right) & \left(\frac{q_1}{p_N}\right) & \cdots & \left(\frac{q_s}{p_N}\right) \\ \mathbf{b}_1 & \cdots & \mathbf{b}_N & & & M & \end{pmatrix}.$$

Where M is as in Lemma 4.2, and $\mathbf{b}_i$ is

$$T^t\left(\left(\frac{2}{p_i}\right),\dots\left(\frac{q_s}{p_i}\right)\right)$$

if $\epsilon_i \equiv 1 \bmod 4$ and

$$\mathbf{v} + S^t\left(\left(\frac{2}{p_i}\right),\dots\left(\frac{q_s}{p_i}\right)\right)$$

if $\epsilon_i \equiv 3 \bmod 4$. Note that if $p_i \equiv \epsilon_i \pmod 4$, this matrix is obtained from A_{p_i} by rearranging the rows and columns. Thus we have that

$$\begin{aligned}
&\sum_{\substack{|D|\le N|F| \\ D\in S(\mathcal{C}) \\ \omega(D/F)=n}} |\operatorname{Sel}_\phi(E_D)|^k \\
=&\frac{1}{2^{k(s+1+n)}} \sum_{\substack{v^j\in\mathbb{F}_2^{s+1+t+n} \\ w^j\in\mathbb{F}_2^{s+1+n}}} \frac{1}{|(\mathbb{Z}/F)^*/((\mathbb{Z}/F)^*)^4|} \sum_{\substack{\chi \pmod{|F|} \\ \chi^4=1}} \bar\chi(\mathcal{C}) \\
&\qquad \frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1\cdots p_n\le N}} \chi(p_1\cdots p_n)(-1)^{\sum_{j=1}^k \langle A_{p_i} v^j, w^j\rangle} \\
=&\frac{1}{2^{k(s+1+n)}} \sum_{\substack{v^j\in\mathbb{F}_2^{s+1+t+n} \\ w^j\in\mathbb{F}_2^{s+1+n}}} \frac{1}{|(\mathbb{Z}/F)^*/((\mathbb{Z}/F)^*)^4|} \sum_{\substack{\chi \pmod{|F|} \\ \chi^4=1}} \bar\chi(\mathcal{C}) \frac{1}{2^n} \sum_{\psi_i \pmod 4} \sum_{\epsilon_i \pmod 4} \\
&\prod_{i=1}^n \psi_i(\epsilon_i) \frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1\cdots p_n\le N}} \prod_{i=1}^n \chi(p_i)\psi_i(p_i)(-1)^{\sum_{j=1}^k \langle A^{\epsilon_i}_{p_i} v^j, w^j\rangle}. \qquad (5.1)
\end{aligned}$$

For fixed $v^j, w^j, \chi, \psi_i, \epsilon_i$, the innermost sum is now exactly of the form described in Proposition 9 of [Kan]. In particular, we call $1 \le i \le n$, *active* if for some ℓ, the term $\left(\frac{p_i}{p_\ell}\right)$ appears in the summand without being canceled by a $\left(\frac{p_\ell}{p_i}\right)$. Let m be the number of active indices. By Proposition 9 of [Kan], we have that if $(\log\log N)/2 < n < 2\log\log N$ that, for any $c > 0$,

$$\frac{1}{n!} \sum_{\substack{p_1,\dots,p_n \text{ distinct odd primes} \\ p_1\cdots p_n\le N}} \prod_{i=1}^n \chi(p_i)\psi_i(p_i)(-1)^{\sum_{j=1}^k \langle A^{\epsilon_i}_{p_i} v^j, w^j\rangle} = O_{c,\mathcal{C}}(Nc^m). \qquad (5.2)$$

We would like to show that the contribution from terms with $m > 0$ is negligible. In order to show this, we will need to bound the number of v^j, w^j with a small number of active indices. To do this, we note

that the exponent of $\left(\frac{p_i}{p_\ell}\right)$ appearing in $(-1)^{\langle A_p v,w\rangle}$ is $(v_i+v_\ell)(w_i+w_\ell)$ modulo 2. Given, $v^j, w^j \in \mathbb{F}_2^n$ let $u_i \in \mathbb{F}_2^{2k}$ for $1 \le i \le n$ be given by

$$u_i = (v_i^1, w_i^1, v_i^2, w_i^2, \ldots, v_i^k, w_i^k).$$

Let $\phi : \mathbb{F}_2^{2k} \to \mathbb{F}_2$ be the quadratic form

$$\phi((x_1, y_1, \ldots, x_k, y_k)) = \sum_{i=1}^{k} x_i y_i.$$

Then the power of $\left(\frac{p_i}{p_\ell}\right)$ appearing in $(-1)^{\sum_{j=1}^k \langle A_{p_i} v^j, w^j\rangle}$ is $\phi(u_i+u_\ell)$.

Claim 1. *The set S of values obtained by u_i for inactive indices i is contained in a translate of a Lagrangian subspace for ϕ. Furthermore, if $m > 0$, they lie in a proper subset of this translate of a Lagrangian subspace. In particular, $|S| \le 2^k$ with strict inequality if $m > 0$.*

Proof. The first claim comes from noting that if S is translated by u_i for some inactive index i, then it is Lagrangian because $\phi(u_i + u_j) = 0$ for i and j inactive. The second statement follows by noting that if S' is the set of values obtain by the u_i for i either inactive or some single particle active index j, then $\phi(u+u') = 0$ for any $u, u' \in S$, and thus once again S' is contained in a translate of a Lagrangian subspace. On the other hand $u_j \notin S$, or else j would also be inactive. Thus $S \subsetneq S'$. This completes the proof. □

Claim 2. *If $(\log\log N)/2 < n < 2\log\log N$, then the sum in Equation (5.1) over terms with $m > 0$ is at most*

$$O_{k,\mathcal{C}}(N(\log(N))^{-2^{-k-1}}).$$

Proof. We begin by bounding the number of tuples v^j, w^j with a given value of m. We note that picking a sequence of $v^j \in \mathbb{F}_2^{s+t+1+n}, w^j \in \mathbb{F}_2^{s+1+n}$ is equivalent to picking $u_1, \ldots, u_n \in \mathbb{F}_2^{2k}$, along with $k(2s+2+t+2n) = O_{k,\mathcal{C}}(1)$ other coordinates. We bound the number of ways to do this for a given value of m. There are $O_k(1)$ ways to pick the set S of values attained by inactive indices. By the previous claim, $|S| \le 2^k - 1$. There are $\binom{n}{m}$ ways to pick which m indices are inactive. There are then at most $|S|^{n-m}2^{2km}$ ways to pick the values of the u_i, and $O_{k,\mathcal{C}}(1)$ ways to pick the values of the other coordinates of the v^j and w^j. By Equation (5.2), once the u_i are picked, the summand is $O_{c,\mathcal{C}}(Nc^m)$ for any $c > 0$. Also note that there are only $O_{k,\mathcal{C}}(1)$ choices for χ, ϵ_i, ψ_i. Therefore, the sum over terms in Equation (5.1) with $m > 0$ is at most

$$\begin{aligned}
\frac{1}{2^{kn}} \sum_{m=0}^{n} O_{k,\mathcal{C}}(1)\binom{n}{m}(2^k-1)^{n-m}4^{km}O_c(N)c^m &= \frac{O_{c,k}(N)}{2^{kn}} \sum_{m=0}^{n} \binom{n}{m}(2^k-1)^{n-m}(c4^k)^m \\
&= \frac{O_{c,k,\mathcal{C}}(N)}{2^{kn}}(2^k - 1 + c4^k)^n \\
&= \frac{O_{k,\mathcal{C}}(N)}{2^{kn}}(2^k - 1/2)^n \\
&= O_{k,\mathcal{C}}(N)(1-2^{-k-1})^n \\
&= O_{k,\mathcal{C}}(N(\log(N))^{-2^{-k-1}}).
\end{aligned}$$

□

We will also need some absolute bound on the sum of terms with $m = 0$:

Claim 3. *The number of ways to choose v^j, w^j in Equation (5.1) so that $m = 0$ is $O_{k,\mathcal{C}}(2^{kn})$. Furthermore, the sum in Equation (5.1) over terms with $m = 0$ is at most*

$$O_k(\#\{|D| \le N|F|, D \in S(\mathcal{C}, n)\}).$$

Proof. The number of ways of picking v^j, w^j with $m = 0$ is at most the number of ways of picking S, times the number of ways of picking $u_i \in S$, times $O_{k,\mathcal{C}}(1)$. This is at most $O_{k,\mathcal{C}}(2^{nk})$. For each such choice, the inner sum is at most

$$\#\{|D| \leq N|F|, D \in S(\mathcal{C}, n)\}$$

Thus the total sum over terms with $m = 0$ is

$$\frac{O_{k,\mathcal{C}}(2^{kn}\#\{|D| \leq N|F|, D \in S(\mathcal{C}, n)\})}{2^{kn}} = O_{k,\mathcal{C}}(\#\{|D| \leq N|F|, D \in S(\mathcal{C}, n)\}).$$

□

Note that if $m = 0$, then the inner summand of Equation (5.1) is a product of $(-1)^{\epsilon(p_i)\epsilon(p_j)}$ terms of the form $\chi_i(p_i)$ where χ_i is a quadratic character of modulus dividing $|F|$, and thus depends only on the values of $p_i \pmod{|F|}$. Note that by Proposition 10 of [Kan], that v^j, w^j are chosen so that $m = 0$ and if $(\log\log N)/2 < n < 2\log\log N$ then

$$\begin{aligned}
&\frac{1}{n!}\sum_{\substack{p_1,\ldots,p_n \text{ distinct odd primes} \\ p_1\cdots p_n \leq N}} \prod_{i=1}^{n} \chi(p_i)\psi_i(p_i)(-1)^{\sum_{j=1}^{k}\langle A_{p_i}^{\epsilon_i} v^j, w^j\rangle} \\
&= \#\{H \leq N \text{ odd, squarefree} : (H, F) = 1, \omega(D) = n\}\times \\
&\quad \mathbb{E}_{p_i \pmod F}\left[\prod_{i=1}^{n} \chi(p_i)\psi_i(p_i)(-1)^{\sum_{j=1}^{k}\langle A_{p_i}^{\epsilon_i} v^j, w^j\rangle}\right] + O_{\mathcal{C}}\left(\frac{N\log\log\log(N)}{\log\log(N)}\right).
\end{aligned}$$

Therefore, combining this with Claim 2, we find that when $(\log\log N)/2 < n < 2\log\log N$ the expression is Equation (5.1) is

$$\begin{aligned}
&\#\{H \leq N \text{ odd, squarefree} : (H, F) = 1, \omega(D) = n\}\times \\
&\left[\frac{1}{2^{k(s+1+n)}}\sum_{\substack{v^j \in \mathbb{F}_2^{s+1+t+n} \\ w^j \in \mathbb{F}_2^{s+1+n}}} \frac{1}{|(\mathbb{Z}/F)^*/((\mathbb{Z}/F)^*)^4|}\sum_{\substack{\chi \pmod{|F|} \\ \chi^4 = 1}} \bar{\chi}(\mathcal{C})\frac{1}{2^n}\sum_{\substack{\psi_i \pmod 4 \\ \epsilon_i \pmod 4}}\right. \\
&\left.\prod_{i=1}^{n}\psi_i(\epsilon_i)\mathbb{E}_{p_i \pmod F}\left[\prod_{i=1}^{n} \chi(p_i)\psi_i(p_i)(-1)^{\sum_{j=1}^{k}\langle A_{p_i}^{\epsilon_i} v^j, w^j\rangle}\right]\right] + O_{k,\mathcal{C}}\left(\frac{N\log\log\log(N)}{\log\log(N)}\right).
\end{aligned}$$

Where the expectation above is over primes p_i so that the Legendre symbols of p_i on p_ℓ are independent and uniformly distributed for $i < \ell$ as are the values of $p_i \in (\mathbb{Z}/|F|)^*$. On the other hand, this is:

$$\begin{aligned}
&\#\{H \leq N \text{ odd, squarefree} : (H, F) = 1, \omega(D) = n\}\mathbb{E}_{p_i}\left[\mathbf{1}_{\prod p_i \in \mathcal{C}}|\ker(A_{p_i})|^k\right] + O_{k,\mathcal{C}}\left(\frac{N\log\log\log(N)}{\log\log(N)}\right) \\
&= \frac{\#\{H \leq N \text{ odd, squarefree} : (H, F) = 1, \omega(D) = n\}}{|(\mathbb{Z}/F)^*/((\mathbb{Z}/F)^*)^4|}\sum_{d=0}^{\infty} 2^{kd}\pi_{d,\mathcal{C}}(n) + O_{k,\mathcal{C}}\left(\frac{N\log\log\log(N)}{\log\log(N)}\right). \qquad (5.3)
\end{aligned}$$

Furthermore by Claim 3 this is

$$O_{k,\mathcal{C}}(\#\{H \leq N \text{ odd, squarefree} : (H, F) = 1, \omega(D) = n\}) + O_{k,\mathcal{C}}\left(\frac{N\log\log\log(N)}{\log\log(N)}\right).$$

Applying this result for $k = 0$ implies that

$$\#\{|D| \leq N|F|, D \in S(\mathcal{C}, n)\}$$

equals

$$\frac{\#\{H \leq N \text{ odd, squarefree} : (H, F) = 1, \omega(D) = n\}}{|(\mathbb{Z}/F)^*/((\mathbb{Z}/F)^*)^4|} + O_{k,\mathcal{C}}\left(\frac{N\log\log\log(N)}{\log\log(N)}\right).$$

Thus, the expression in Equation (**??**) simplifies to

$$\#\{|D| \leq N|F|, D \in S(\mathcal{C}, n)\} \sum_{d=0}^{\infty} 2^{kd} \pi_{d,\mathcal{C}}(n) + O_{k,\mathcal{C}}\left(\frac{N \log\log\log(N)}{\log\log(N)}\right) \tag{5.4}$$

We know that $\lim_{n\to\infty} \pi_{d,\mathcal{C}}(n) \to \pi_d(t)$ pointwise, and would like to be able to say that

$$\lim_{n\to\infty} \sum_{d=0}^{\infty} 2^{kd} \pi_{d,\mathcal{C}}(n) = \sum_{d=0}^{\infty} 2^{kd} \pi_d(t). \tag{5.5}$$

To do this, we note by the above (for $n \approx \log\log(N)$) that

$$\sum_{d=0}^{\infty} 2^{kd} \pi_{d,\mathcal{C}}(n) = O_{k,\mathcal{C}}(1).$$

Applying this result for larger k, we find that

$$\sum_{d=0}^{\infty} 2^{(k+1)d} \pi_{d,\mathcal{C}}(n) = O_{k,\mathcal{C}}(1).$$

Thus,

$$\pi_{d,\mathcal{C}}(n) = O_{k,\mathcal{C}}(2^{-(k+1)d})$$

for all d, n. Therefore,

$$\sum_{d=0}^{\infty} \sup_n 2^{kd} \pi_{d,\mathcal{C}}(n) = \sum_{d=0}^{\infty} O_{k,\mathcal{C}}(2^{-d}) = O_{k,\mathcal{C}}(1).$$

Thus Equation (5.6) follows by dominated convergence.

Summing Equation (5.5) over all n with $|n - \log\log(N)| < \log\log(N)^{3/4}$, and noting that almost all $H \leq N$ have a number of divisors in this range, we find that

$$\begin{aligned}
&\frac{\sum_{\substack{|D|\leq N|F|: D\in S(\mathcal{C}) \\ |\omega(D/F)-\log\log(N)|<\log\log(N)^{3/4}}} |\operatorname{Sel}_\phi(E_D)|^k}{\#\{|D| \leq N|F|, D \in S(\mathcal{C}), |\omega(D/F) - \log\log(N)| < \log\log(N)^{3/4}\}} \\
=&\sum_{d=0}^{\infty} 2^{kd} \pi_d(n) + \delta_N + O_k\left(\frac{\log\log\log(N)}{\log\log(N)^{1/4}}\right),
\end{aligned}$$

where $\lim_{N\to\infty} \delta_N = 0$. This completes our proof. □

Theorem 5.1 now follows in a straightforward manner from Proposition 5.2 after noting that density 1 of numbers less than N have $\log\log(N) \pm \log\log(N)^{3/4}$ distinct prime factors.

5.1 Complements

We now deduce from Theorem 5.1 the one remaining theorem of the introduction.

Theorem 5.3. *Let $t \in \mathbb{Z}$, and for each $X > 0$ let $\mathcal{S}_t(X)$ denote the set of fourth-power free integers D such that $t_D = t$ and $-X < D < X$. Then for each $k \geq 1$, the limit*

$$\lim_{X\to\infty} \frac{\#\{D \in \mathcal{S}_t(X) \mid \dim_{\mathbb{F}_2} \operatorname{Sel}_\phi(E_D) = k\}}{\#\mathcal{S}_t(X)}$$

exists, and is equal to $\pi_{k-1}(t)$.

Proof. Let $\mathcal{T}(t)$ be the set of pairs $(F, \mathcal{C})$ that have associated Tamagawa number $t_D = t$ so that whenever $p|F$ for $p > 2$, we have that $p^2|F$. Let $S(\mathcal{C}, X)$ be the elements of $S(\mathcal{C})$ of absolute value less than X. We have that

$$\mathcal{S}_t(X) = \bigcup_{\mathcal{C} \in \mathcal{T}(t)} S(\mathcal{C}, X).$$

It should also be noted that each of these terms is of comparable size. In particular,

$$|\mathcal{S}_t(X)| = O(X),$$

and

$$|S(\mathcal{C}, X)| = d_{\mathcal{C}} X + o(X)$$

for some constant $d_{\mathcal{C}} > 0$. Combining these, we find that

$$|\mathcal{S}_t(X)| = \Omega_t(X).$$

Thus, in order to prove our Theorem, it suffices to show that

$$\#\{D \in \mathcal{S}_t(X) \mid \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k\} = \pi_{k-1}(t) \#\mathcal{S}_t(X) + o_t(X).$$

Our basic approach will be to approximate $\mathcal{S}_t(X)$ by a union of finitely many of the $S(\mathcal{C}, X)$. In particular, let $\mathcal{T}(t, n)$ be the elements of $\mathcal{T}(t)$ for which F is not divisible by the square of any number more than n. It is easily seen that this is a finite set. On the other hand, we have

$$\begin{aligned}
&\#\left(\mathcal{S}_t(X) - \cup_{\mathcal{C} \in \mathcal{T}(t,n)} \mathcal{C}\right) \\
&\leq \#\{m \in \mathbb{Z} : |m| < X, m \text{ is divisible by the square of a number more than } n\} \\
&\leq \sum_{d=n}^{X} O\left(\frac{X}{d^2}\right) = O(X/n).
\end{aligned}$$

Thus by Theorem 5.1, the quantity $\#\{D \in \mathcal{S}_t(X) \mid \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k\}$ is equal to

$$\begin{aligned}
&\sum_{\mathcal{C} \in \mathcal{T}(t)} \#\{D \in S(\mathcal{C}, X) \mid \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k\} \\
&= \sum_{\mathcal{C} \in \mathcal{T}(t,n)} \#\{D \in S(\mathcal{C}, X) \mid \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E_D) = k\} + O(X/n) \\
&= \sum_{\mathcal{C} \in \mathcal{T}(t,n)} (|S(\mathcal{C}, X)| \pi_{k-1}(t) + o_{n,t}(X)) + O(X/n) \\
&= \sum_{\mathcal{C} \in \mathcal{T}(t,n)} (|S(\mathcal{C}, X)|) \, \pi_{k-1}(t) + o_{n,t}(X) + O(X/n) \\
&= (|\mathcal{S}_t(X)| + O(X/n)) \, \pi_{k-1}(t) + o_{n,t}(X) + O(X/n) \\
&= |\mathcal{S}_t(X)| \pi_{k-1}(t) + o_{n,t}(X) + O(X/n) \\
&= |\mathcal{S}_t(X)| \pi_{k-1}(t) + o_t(X),
\end{aligned}$$

as desired. This completes our proof. □

References

[BS] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. Preprint.

[BS66] B. J. Birch and N. M. Stephens. The parity of the rank of the Mordell-Weil group. *Topology*, 5:295–299, 1966.

[Cas65] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[Got01] Takeshi Goto. A note on the Selmer group of the elliptic curve $y^2 = x^3 + Dx$. *Proc. Japan Acad. Ser. A Math. Sci.*, 77(7):122–125, 2001.

[Jac29] K. G. J. Jacobi. *Fundamenta nova theoriae functionum ellipticarum*. Königsberg, 1829.

[Kan] Daniel M. Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. To appear in Algebra and Number Theory.

[Nor98] J. R. Norris. *Markov chains*, volume 2 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, 1998. Reprint of 1997 original.

[PR12] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.

[SD08] Peter Swinnerton-Dyer. The effect of twisting on the 2-Selmer group. *Math. Proc. Cambridge Philos. Soc.*, 145(3):513–526, 2008.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.