THE DISTRIBUTION OF 2-SELMER RANKS OF QUADRATIC TWISTS OF ELLIPTIC CURVES WITH PARTIAL TWO-TORSION

ZEV KLAGSBRUN AND ROBERT J. LEMKE OLIVER

ABSTRACT. This paper presents a new result concerning the distribution of 2-Selmer ranks in the quadratic twist family of an elliptic curve over an arbitrary number field K with a single point of order two that does not have a cyclic 4-isogeny defined over its two-division field. We prove that at least half of all the quadratic twists of such an elliptic curve have arbitrarily large 2-Selmer rank, showing that the distribution of 2-Selmer ranks in the quadratic twist family of such an elliptic curve differs from the distribution of 2-Selmer ranks in the quadratic twist family of an elliptic curve having either no rational two-torsion or full rational two-torsion.

1. INTRODUCTION

1.1. **Distributions of Selmer Ranks.** Let E be an elliptic curve defined over a number field K and let $\mathrm{Sel}_2(E/K)$ be its 2-Selmer group (see Section 2 for its definition). We define the **2-Selmer rank of** E/K, denoted $d_2(E/K)$, by

$$d_2(E/K) = \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2}E(K)[2].$$

In 1994, Heath-Brown [4] proved that the 2-Selmer ranks of all of the quadratic twists of the congruent number curve $E/\mathbb{Q}$ given by $y^2 = x^3 - x$ had a particularly nice distribution. In particular, he showed that there are explicits constants $\alpha_0, \alpha_1, \alpha_2, \ldots$ summing to one such that

$$\lim_{X\to\infty} \frac{|\{d \text{ squarefree } |d| < X : d_2(E^d/\mathbb{Q}) = r\}|}{|\{d \text{ squarefree } |d| < X\}|} = \alpha_r$$

for every $r \in \mathbb{Z}^{\geq 0}$, where E^d is the quadratic twist of E by d. This result was extended by Swinnerton-Dyer [10] and Kane [5] to all elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that do not have a cyclic 4-isogeny defined over K.

A similar result was obtained by Klagsbrun, Mazur, and Rubin [7] for elliptic curves E over a general number field K with $\mathrm{Gal}(K(E[2])/K) \simeq \mathcal{S}_3$, where squarefree d are replaced by quadratic characters of K and a suitable ordering of all such characters is taken.

In this work we show that this type of result does not hold when $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. In particular, we prove the following:

Theorem 1.1. *For $d \in \mathcal{O}_K$, let χ_d be the quadratic character of K that cuts out the extension $K(\sqrt{d})$ and define*

$$C(K, X) := \{\chi_d : |\mathbf{N}_{K/\mathbb{Q}}d| < X\}.$$

Let E be an elliptic curve defined over K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $K(E[2])$. Then for any fixed r,

$$\liminf_{X\to\infty} \frac{|\{\chi \in C(K, X) : d_2(E^\chi/K) \geq r\}|}{|C(K, X)|} \geq \frac{1}{2}$$

where E^χ is the quadratic twist of E by any $d \in \mathcal{O}_K$ with $\chi_d = \chi$.

In particular, this shows that there is not a distribution function on 2-Selmer ranks within the quadratic twist family of E.

Theorem 1.1 is an easy consequence of the following result.

Theorem 1.2. *Let E be an elliptic curve defined over K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $K(E[2])$. Then the normalized distribution*

$$\frac{P_r(\mathcal{T}(E/E'), X)}{\sqrt{\frac{1}{2}\log\log X}}$$

converges weakly to the Gaussian distribution

$$G(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{\frac{-w^2}{2}}\, \mathrm{d}w,$$

where

$$P_r(\mathcal{T}(E/E'), X) = \frac{|\{\chi \in C(K, X) : \mathrm{ord}_2 \mathcal{T}(E^\chi/E'^\chi) \leq r\}|}{|C(K, X)|}$$

for $X \in \mathbb{R}^+$, $r \in \mathbb{Z}^{\geq 0}$, and $\mathcal{T}(E^\chi/E'^\chi)$ as defined in Section 2.

In turn, Theorem 1.2 follows from a variant of the Erdős-Kac theorem for quadratic characters of number fields. Let $C(K)$ denote the set of all quadratic characters of K. For any $\chi \in C(K)$, we can associate a unique squarefree ideal D_χ to χ by taking D_χ to be the squarefree part of the ideal $\langle d \rangle$, where d is any element of $\mathcal{O}_K$ such that $\chi_d = \chi$. We say that a function f on the ideals of $\mathcal{O}_K$ is **additive** if $f(\mathfrak{a}\mathfrak{a}') = f(\mathfrak{a}) + f(\mathfrak{a}')$ whenever the ideals $\mathfrak{a}$ and $\mathfrak{a}'$ are relatively prime; we define $f(\chi)$ for $\chi \in C(K)$ to be $f(D_\chi)$.

To an additive function f, we attach quantities $\mu_f(X)$ and $\sigma_f(X)$, defined to be

$$\mu_f(X) := \sum_{\mathbf{N}\mathfrak{p} < X} \frac{f(\mathfrak{p})}{\mathbf{N}\mathfrak{p}}, \quad \sigma_f(X) := \left(\sum_{\mathbf{N}\mathfrak{p} < X} \frac{f(\mathfrak{p})^2}{\mathbf{N}\mathfrak{p}} \right)^{1/2},$$

and we prove the following.

Theorem 1.3. *Suppose that f is an additive function such that $0 \leq f(\mathfrak{p}) \leq 1$ for every prime $\mathfrak{p}$. If $\sigma_f(X) \to \infty$ as $X \to \infty$, then*

$$\lim_{X \to \infty} \frac{|\{\chi \in C(K, X) : f(\chi) - \mu_f(X) \leq z \cdot \sigma_f(X)\}|}{|C(K, X)|} = G(z),$$

In the special case where $K = \mathbb{Q}$, Theorem 1.1 follows from results recently obtained by Xiong about the distribution of $\dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E/\mathbb{Q})$ in quadratic twist families [11]. We are able to obtain results over general number fields by applying different methods to the coarser question about the distribution of $\mathrm{ord}_2 T(E/E')$ in twist families (see Theorem 1.2).

Remark 1.4. The methods in the paper can easily be adapted to studying cubic twists of the j-invariant 0 curve $y^2 = x^3 + k$ for any number field K with $K(\sqrt{k}, \sqrt{-3})/K$ biquadratic. In that case, Theorem 1.1 holds with 2-Selmer rank replaced by 3-Selmer rank and quadratic characters replaced by cubic characters.

Remark 1.5. This work is the first of a series of papers which develop techniques for using additive functions to study questions relating to the distribution of 2-Selmer ranks of elliptic curves. The next paper in this series will use these techniques to prove variants of Theorems

1.1 and 1.2 for the set of all elliptic curves with a rational point of order two [8]. The third and final paper in this series will address a number of questions relating to the joint distribution of 2-Selmer ranks within quadratic twist families [9].

1.2. **Layout.** We begin in Section 2 by recalling the definitions of the 2-Selmer group and the Selmer groups associated with a 2-isogeny ϕ and presenting some of the connections between them. In Section 3, we examine the behavior of the local conditions for the ϕ-Selmer group under quadratic twist and show how that quantity $\mathcal{T}(E^\chi/E'^\chi)$ can be related to the value $f(\chi)$ of an additive function f on $C(K)$. Theorem 1.3 is proved in Section 4 and we conclude with the proofs of Theorems 1.1 and 1.2 in Section 5.

Acknowledgement. The first author would like to express his thanks to Karl Rubin for his helpful comments and suggestions, to Ken Kramer for a series of valuable discussions, and to Michael Rael and Josiah Sugarman for helpful conversations regarding the Erdős-Kac theorem. The first author was supported by NSF grants DMS-0457481, DMS-0757807, and DMS-0838210. The second author was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship, DMS-1303913.

2. Selmer Groups

We begin by recalling the definition of the 2-Selmer group. If E is an elliptic curve defined over a field K, then $E(K)/2E(K)$ maps into $H^1(K, E[2])$ via the Kummer map. The following diagram commutes for every place v of K, where δ is the Kummer map.

$$\begin{array}{ccc} E(K)/2E(K) & \xrightarrow{\delta} & H^1(K, E[2]) \\ \downarrow & & \downarrow Res_v \\ E(K_v)/2E(K_v) & \xrightarrow{\delta} & H^1(K_v, E[2]) \end{array}$$

We define a distinguished local subgroup $H^1_f(K_v, E[2]) \subset H^1(K_v, E[2])$ as the image $\delta\left(E(K_v)/2E(K_v)\right) \subset H^1(K_v, E[2])$ for each place v of K and we define the **2-Selmer group** of E/K, denoted $\mathrm{Sel}_2(E/K)$, by

$$\mathrm{Sel}_2(E/K) = \ker\left(H^1(K, E[2]) \xrightarrow{\sum res_v} \bigoplus_{v \text{ of } K} H^1(K_v, E[2])/H^1_f(K_v, E[2])\right).$$

The 2-Selmer group is a finite dimensional $\mathbb{F}_2$-vector space that sits inside the exact sequence of $\mathbb{F}_2$-vector spaces

$$0 \to E(K)/2E(K) \to \mathrm{Sel}_2(E/K) \to Ш(E/K)[2] \to 0$$

where $Ш(E/K)$ is the Tate-Shafarevich group of E.

If $E(K)$ has a single point of order two, then there is a two-isogeny $\phi : E \to E'$ between E and E' with kernel $C = E(K)[2]$. This isogeny gives rise to two Selmer groups.

We have a short exact sequence of G_K modules

$$0 \to C \to E(\overline{K}) \xrightarrow{\phi} E'(\overline{K}) \to 0 \tag{1}$$

which gives rise to a long exact sequence of cohomology groups

$$0 \to C \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, C) \to H^1(K, E) \to H^1(K, E') \dots$$

The map δ is given by $\delta(Q)(\sigma) = \sigma(R) - R$ where R is any point on $E(\overline{K})$ with $\phi(R) = Q$.

This sequence remains exact when we replace K by its completion K_v at any place v, which gives rise to the following commutative diagram.

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K,C) \\ \downarrow & & \downarrow Res_v \\ E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & H^1(K_v,C) \end{array}$$

In a manner similar to how we defined the 2-Selmer group, we define distinguished local subgroups $H^1_\phi(K_v,C) \subset H^1(K_v,C)$ as the image of $E'(K_v)/\phi(E(K_v))$ under δ for each place v of K. We define the **ϕ-Selmer group of E**, denoted $\mathrm{Sel}_\phi(E/K)$ as

$$\mathrm{Sel}_\phi(E/K) = \ker\left(H^1(K,C) \xrightarrow{\sum res_v} \bigoplus_{v \text{ of } K} H^1(K_v,C)/H^1_\phi(K_v,C) \right).$$

The isogeny ϕ on E gives gives rise to a dual isogeny $\hat{\phi}$ on E' with kernel $C' = \phi(E[2])$. Exchanging the roles of (E,C,ϕ) and $(E',C',\hat{\phi})$ in the above defines the **$\hat{\phi}$-Selmer group**, $\mathrm{Sel}_{\hat{\phi}}(E'/K)$, as a subgroup of $H^1(K,C')$. The groups $\mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E'/K)$ are finite dimensional $\mathbb{F}_2$-vector spaces and we can compare the sizes of the ϕ-Selmer group, the $\hat{\phi}$-Selmer group, and the 2-Selmer group using the following two theorems.

Theorem 2.1. *The ϕ-Selmer group, the $\hat{\phi}$-Selmer group, and the 2-Selmer group sit inside the exact sequence*

$$0 \to E'(K)[2]/\phi(E(K)[2]) \to \mathrm{Sel}_\phi(E/K) \to \mathrm{Sel}_2(E/K) \xrightarrow{\phi} \mathrm{Sel}_{\hat{\phi}}(E'/K). \tag{2}$$

Proof. This is a well known diagram chase. See Lemma 2 in [2] for example. □

The **Tamagawa ratio** $\mathcal{T}(E/E')$ defined as $\mathcal{T}(E/E') = \frac{\left|\mathrm{Sel}_\phi(E/K)\right|}{\left|\mathrm{Sel}_{\hat{\phi}}(E'/K)\right|}$ gives a second relationship between the $\mathbb{F}_2$-dimensions of $\mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E'/K)$.

Theorem 2.2 (Cassels)**.** *The Tamagawa ratio $\mathcal{T}(E/E')$ is given by*

$$\mathcal{T}(E/E') = \prod_{v \text{ of } K} \frac{\left|H^1_\phi(K_v,C)\right|}{2}.$$

Proof. This is a combination of Theorem 1.1 and equations (1.22) and (3.4) in [1]. □

Stepping back, we observe that if $\mathcal{T}(E/E') \geq 2^{r+2}$, then $d_\phi(E/K) \geq r+2$, and therefore by Theorem 2.1, $d_2(E/K) \geq r$. (If E does not have a cyclic 4-isogeny defined over K then we can in fact show that $\mathcal{T}(E/E') \geq 2^r$ implies that $d_2(E/K) \geq r$, but this is entirely unnecessary for our purposes.)

3. Local Conditions at Twisted Places

For the remainder of this paper, we will let E be an elliptic curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and let $\phi : E \to E'$ be the isogeny with kernel $C = E(K)[2]$.

If $\mathfrak{p} \nmid 2$ is a prime where E has good reduction, then $H^1_\phi(K_\mathfrak{p},C)$ is a 1-dimensional $\mathbb{F}_2$-subspace of $H^1(K_\mathfrak{p},C)$ equal to the unramified local subgroup $H^1_u(K_\mathfrak{p},C)$. If such a $\mathfrak{p}$ is ramified in the extension F/K cut out by a character χ, then the twisted curve E^χ will have bad reduction at $\mathfrak{p}$. The following lemma addresses the size of $H^1_\phi(K_\mathfrak{p},C^\chi)$.

Lemma 3.1. *Suppose $\mathfrak{p} \nmid 2$ is a prime where E has good reduction and $\mathfrak{p}$ is ramified in the extension F/K cut out by χ.*

(i) If $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z} \simeq E'(K_\mathfrak{p})[2]$, then $\dim_{\mathbb{F}_2} H^1_\phi(K_\mathfrak{p}, C^\chi) = 1$.
(ii) If $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq E'(K_\mathfrak{p})[2]$, then $\dim_{\mathbb{F}_2} H^1_\phi(K_\mathfrak{p}, C^\chi) = 1$.
(iii) If $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $E'(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then $\dim_{\mathbb{F}_2} H^1_\phi(K_\mathfrak{p}, C^\chi) = 2$.
(iv) If $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then $\dim_{\mathbb{F}_2} H^1_\phi(K_\mathfrak{p}, C^\chi) = 0$.

Proof. From Lemma 3.7 in [6], we have

$$E'^\chi(K_\mathfrak{p})[2^\infty]/\phi(E^\chi(K_\mathfrak{p})[2^\infty]) = E'^\chi(K_\mathfrak{p})[2]/\phi(E^\chi(K_\mathfrak{p})[2]).$$

All four results then follow immediately. □

Remark 3.2. Suppose that Δ and Δ' are discriminants of any integral models of E and E' respectively. The condition that $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ (resp. $E'(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z}$) is equivalent to the condition that Δ (resp. Δ') is not a square in $K_\mathfrak{p}$. Which case of Lemma 3.1 we are is therefore determined by the Legendre symbols $\left(\frac{\Delta}{\mathfrak{p}}\right)$ and $\left(\frac{\Delta'}{\mathfrak{p}}\right)$.

We use Theorem 2.2 and Lemma 3.1 to relate $\mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi)$ to the value $g(\chi)$ of an additive function g on $C(K)$ defined as follows: For $\chi \in C(K)$ cutting out F/K, let

$$g(\chi) = \sum_{\substack{\mathfrak{p} \text{ ramified in } F/K \\ \mathfrak{p} \nmid 2\Delta\infty}} \frac{\left(\frac{\Delta'}{\mathfrak{p}}\right) - \left(\frac{\Delta}{\mathfrak{p}}\right)}{2} \tag{3}$$

That is, $g(\chi)$ roughly counts the difference between the number of primes ramified in F/K where condition (iii) of Proposition 3.1 is satisfied and the number of primes ramified in F/K where condition (iv) is satisfied. We then have the following:

Proposition 3.3. *The order of 2 in the Tamagawa ratio $\mathcal{T}(E^\chi/E'^\chi)$ is given by*

$$\mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi) = g(\chi) + \sum_{v|2\Delta\infty} \left(\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^\chi) - 1\right).$$

Proof. By Thereom 2.2, $\mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi)$ is given by

$$\mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi) = \sum_{v|2\Delta\Delta_{F/K}\infty} \left(\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^d) - 1\right),$$

where $\Delta_{F/K}$ is the relative discriminant of the extension F/K cut out by χ. By Remark 3.2, Lemma 3.1 gives us that

$$\dim_{\mathbb{F}_2} H^1_\phi(K_\mathfrak{p}, C^\chi) - 1 = \frac{\left(\frac{\Delta'}{\mathfrak{p}}\right) - \left(\frac{\Delta}{\mathfrak{p}}\right)}{2}$$

for places $\mathfrak{p} \mid \Delta_{F/K}$ with $\mathfrak{p} \nmid 2\Delta\infty$ and the result follows. □

4. The Erdős-Kac Theorem For Quadratic Characters

Because the sum

$$\sum_{v|2\Delta\infty} \left(\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^\chi) - 1\right)$$

can be bounded uniformly for a fixed elliptic curve, Proposition 3.3 suggests that we should study the distribution of the additive function $g(\chi)$ in order to understand the distribution of $\mathcal{T}(E^\chi/E'^\chi)$ as χ varies.

When $f : \mathbb{N} \to \mathbb{C}$ is an additive function on the integers, then under mild hypotheses, the classical Erdős-Kac Theorem tells us that the distribution of f on natural numbers less than X approaches a normal distribution with mean $\mu(X)$ and variance $\sigma^2(X)$ as $X \to \infty$, where $\mu(X)$ and $\sigma(X)$ are the rational analogues of $\mu_f(X)$ and $\sigma_f(X)$ defined in the introduction. Theorem 1.3 is the statement that the same type of result holds for additive functions on quadratic characters of a number field.

We begin by observing that if $\chi_{d_1} = \chi_{d_2}$, then, if $(d_1) = \mathfrak{a}\mathfrak{b}_1^2$ and $(d_2) = \mathfrak{a}\mathfrak{b}_2^2$, $\mathfrak{b}_1$ and $\mathfrak{b}_2$ lie in the same ideal class of $\mathcal{O}_K$. Conversely, if $\mathfrak{b}_1$ and $\mathfrak{b}_2$ lie in the same class, then $\chi_{d_1} = \chi_{\varepsilon d_2}$ for some $\varepsilon \in \mathcal{O}_K^\times$. Thus, we see that elements of $C(K, X)$ correspond to triples $(\mathfrak{b}, \mathfrak{a}, \varepsilon)$ with $\mathfrak{b}$ a representative of its ideal class of minimal norm, $\mathfrak{a}$ a squarefree ideal of norm $\mathbf{N}\mathfrak{a} < X/\mathbf{N}\mathfrak{b}^2$ such that $\mathfrak{a}\mathfrak{b}^2$ is principal, and ε an element of $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$. From this discussion, it is apparent, for a prime ideal $\mathfrak{p}$ and a fixed choice $\mathfrak{b}_0$ of $\mathfrak{b}$, that

$$\begin{aligned}\lim_{X\to\infty} \frac{|\{\chi \in C(K,X) \leftrightarrow (\mathfrak{b}_0, \mathfrak{a}, \varepsilon) : \mathfrak{p} \mid \mathfrak{a}\}|}{|C(K,X)|} &= \Pr(\mathfrak{p} \mid \mathfrak{a} : \mathfrak{a} \text{ is squarefree}, \mathfrak{a}\mathfrak{b}_0^2 \text{ is principal}) \\ &= \frac{1}{\mathbf{N}\mathfrak{p}+1},\end{aligned}$$

whence, ranging over all χ, the probablity that $\mathfrak{p} \mid \mathfrak{a}$ is $\frac{1}{\mathbf{N}\mathfrak{p}+1}$.

Thus, treating the events $\mathfrak{p}_1 \mid \mathfrak{a}$ and $\mathfrak{p}_2 \mid \mathfrak{a}$ as independent, we might predict that

$$\frac{1}{|C(K,X)|} \sum_{\chi \in C(K,X)} f(\chi) \approx \tilde{\mu}_f(X),$$

where

$$\begin{aligned}\tilde{\mu}_f(X) &:= \sum_{\mathbf{N}\mathfrak{p}<X} \frac{f(\mathfrak{p})}{\mathbf{N}\mathfrak{p}+1} \\ &= \mu_f(X) + O(1).\end{aligned}$$

In fact, this prediction is true, which we establish using the method of moments, following the blueprint of Granville and Soundararajan [3]. This requires the following technical result about the function $g_\mathfrak{p}(\chi)$, defined to be

$$g_\mathfrak{p}(\chi) := \begin{cases} f(\mathfrak{p})\left(1 - \frac{1}{\mathbf{N}\mathfrak{p}+1}\right) & \text{if } \mathfrak{p} \mid \mathfrak{a}, \text{ and} \\ f(\mathfrak{p})\left(-\frac{1}{\mathbf{N}\mathfrak{p}+1}\right) & \text{if } \mathfrak{p} \nmid \mathfrak{a}. \end{cases}$$

Theorem 4.1. *With notation as above, uniformly for $k \le \sigma_f(z)^{2/3}$, we have that*

$$\frac{1}{|C(K,X)|} \sum_{\chi \in C(K,X)} \left(\sum_{\mathbf{N}\mathfrak{p}<z} g_\mathfrak{p}(\chi)\right)^k = c_k \sigma_f(z)^k \left(1 + O\left(\frac{k^3}{\sigma_f(z)^2}\right)\right) + O\left(X^{\lambda-1} 3^k \pi_K(z)^k\right)$$

if k is even, and

$$\frac{1}{|C(K,X)|} \sum_{\chi \in C(K,X)} \left(\sum_{\mathbf{N}\mathfrak{p}<z} g_\mathfrak{p}(\chi)\right)^k \ll c_k \sigma_f(z)^{k-1} k^{3/2} + X^{\lambda-1} 3^k \pi_K(z)^k$$

if k is odd. Here, $c_k = \Gamma(k+1)/2^{k/2}\Gamma(\frac{k}{2}+1)$ and $\lambda < 1$ depends only on the degree of K.

The proof of Theorem 4.1 relies upon a result about the distribution of squarefree ideals. To this end, given ideals $\mathfrak{c}$ and $\mathfrak{q}$ and squarefree $\mathfrak{d} \mid \mathfrak{q}$, define $N^{\mathrm{sf}}(X; \mathfrak{c}, \mathfrak{q}, \mathfrak{d})$ to be the number of squarefree ideals $\mathfrak{a}$ of norm up to X in the same class as $\mathfrak{c}$ and such that $(\mathfrak{a}, \mathfrak{q}) = \mathfrak{d}$. We then have:

Lemma 4.2. *With notation as above, we have that*

$$N^{\mathrm{sf}}(X; \mathfrak{c}, \mathfrak{q}, \mathfrak{d}) = \frac{1}{|\mathrm{Cl}(K)|}\frac{\mathrm{res}_{s=1}\zeta_K(s)}{\zeta_K(2)}\phi(\mathfrak{q}, \mathfrak{d})X + O(X^{\lambda}3^{\omega(\mathfrak{q})}),$$

where $\lambda = \frac{\deg K - 1}{\deg K + 1}$ if $\deg K \geq 3$ and $\lambda = 1/2$ otherwise, $\omega(\mathfrak{q})$ denotes the number of distinct primes dividing $\mathfrak{q}$, and

$$\phi(\mathfrak{q}, \mathfrak{d}) = \prod_{\mathfrak{p} \mid \mathfrak{d}} \frac{1}{\mathbf{N}\mathfrak{p} + 1} \prod_{\mathfrak{p} \mid \mathfrak{q}, \mathfrak{p} \nmid \mathfrak{d}} \frac{\mathbf{N}\mathfrak{p}}{\mathbf{N}\mathfrak{p} + 1}.$$

Proof. This follows from elementary considerations and the classical estimate

$$\sum_{\substack{\mathbf{N}\mathfrak{a} < X \\ \mathfrak{a}\mathfrak{c}^{-1} \text{ prin.}}} 1 = \frac{1}{|\mathrm{Cl}(K)|}\mathrm{res}_{s=1}\zeta_K(s) \cdot X + O(X^{\frac{\deg K - 1}{\deg K + 1}}).$$

□

Proof of Theorem 4.1. For any ideal $\mathfrak{q}$, define $g_{\mathfrak{q}}(\chi) := \prod_{\mathfrak{p}^{\alpha} || \mathfrak{q}} g_{\mathfrak{p}}(\chi)^{\alpha}$. We then have that

$$\begin{aligned}
\sum_{\chi \in C(K,X)} \left(\sum_{\mathbf{N}\mathfrak{p} < z} g_{\mathfrak{p}}(\chi) \right)^k &= \left| \mathcal{O}_K^{\times} / (\mathcal{O}_K^{\times})^2 \right| \cdot \sum_{\mathfrak{b}} {\sum_{\substack{\mathbf{N}\mathfrak{a} < \frac{X}{\mathbf{N}\mathfrak{b}^2} \\ \mathfrak{a}\mathfrak{b}^2 \text{ prin.}}}}' \left(\sum_{\mathbf{N}\mathfrak{p} < z} g_{\mathfrak{p}}(\mathfrak{a}) \right)^k \\
&= \left| \mathcal{O}_K^{\times} / (\mathcal{O}_K^{\times})^2 \right| \cdot \sum_{\mathfrak{b}} \sum_{\mathbf{N}\mathfrak{p}_1, \ldots, \mathbf{N}\mathfrak{p}_k < z} {\sum_{\substack{\mathbf{N}\mathfrak{a} < \frac{X}{\mathbf{N}\mathfrak{b}^2} \\ \mathfrak{a}\mathfrak{b}^2 \text{ principal}}}}' g_{\mathfrak{p}_1 \ldots \mathfrak{p}_k}(\mathfrak{a}),
\end{aligned}$$

where, as expected, the summation over $\mathfrak{b}$ is taken to be over representatives of minimal norm for each ideal class and the prime on the summation over $\mathfrak{a}$ indicates it is to be taken over squarefree ideals. Given an ideal $\mathfrak{c}$, we now consider for any $\mathfrak{q}$ the more general summation

$$\begin{aligned}
{\sum_{\substack{\mathbf{N}\mathfrak{a} < Y \\ \mathfrak{a}\mathfrak{c}^{-1} \text{ principal}}}}' g_{\mathfrak{q}}(\mathfrak{a}) &= \sum_{\mathfrak{d} \mid \sqrt{\mathfrak{q}}} g_{\mathfrak{q}}(\mathfrak{d}) N^{\mathrm{sf}}(Y; \mathfrak{c}, \mathfrak{q}, \mathfrak{d}) \\
&= \frac{Y}{|\mathrm{Cl}(K)|}\frac{\mathrm{res}_{s=1}\zeta_K(s)}{\zeta_K(2)} \sum_{\mathfrak{d} \mid \sqrt{\mathfrak{q}}} g_{\mathfrak{q}}(\mathfrak{d})\phi(\mathfrak{q}, \mathfrak{d}) + O\left(Y^{\lambda} 3^{\omega(\mathfrak{q})} \sum_{\mathfrak{d} \mid \sqrt{\mathfrak{q}}} |g_{\mathfrak{q}}(\mathfrak{d})| \right), \\
&=: \frac{Y}{|\mathrm{Cl}(K)|}\frac{\mathrm{res}_{s=1}\zeta_K(s)}{\zeta_K(2)} G(\mathfrak{q}) + O\left(Y^{\lambda} 3^{\omega(\mathfrak{q})} \right),
\end{aligned}$$

say, where $\sqrt{\mathfrak{q}} = \prod_{\mathfrak{p} \mid \mathfrak{q}} \mathfrak{p}$. We note that $G(\mathfrak{q})$ is multiplicative, and is given by

$$G(\mathfrak{q}) = \prod_{\mathfrak{p}^{\alpha} || \mathfrak{q}} \frac{f(\mathfrak{p})^{\alpha}}{\mathbf{N}\mathfrak{p} + 1} \left(\left(1 - \frac{1}{\mathbf{N}\mathfrak{p} + 1} \right)^{\alpha} + \mathbf{N}\mathfrak{p} \cdot \left(-\frac{1}{\mathbf{N}\mathfrak{p} + 1} \right)^{\alpha} \right).$$

Thus, $G(\mathfrak{q}) = 0$ unless each α is at least two, i.e. $\mathfrak{q}$ is square-full.

Returning to the original problem, we find that

$$\sum_{\chi \in C(K,X)} \left(\sum_{\mathbf{N}\mathfrak{p} < z} g_{\mathfrak{p}}(\chi) \right)^k = c(K) \cdot X \sum_{\mathbf{N}\mathfrak{p}_1, \dots, \mathbf{N}\mathfrak{p}_k < z} G(\mathfrak{p}_1 \dots \mathfrak{p}_k) + O\left(X^{\lambda} 3^k \pi_K(z)^k \right),$$

where $\pi_K(z) := \#\{\mathfrak{p} : \mathbf{N}\mathfrak{p} < z\}$ and

$$c(K) := \left| \mathcal{O}_K^{\times} / (\mathcal{O}_K^{\times})^2 \right| \frac{1}{|\mathrm{Cl}(K)|} \frac{\mathrm{res}_{s=1} \zeta_K(s)}{\zeta_K(2)} \sum_{\mathfrak{b}} \frac{1}{\mathbf{N}\mathfrak{b}^2}.$$

Noting that the above discussion also proves that $|C(K,X)| = c(K) \cdot X + O(X^{\lambda})$, the goal is to estimate the summation over $\mathfrak{p}_1, \dots, \mathfrak{p}_k$. Since $G(\mathfrak{q}) = 0$ unless $\mathfrak{q}$ is square-full, we have that

$$\sum_{\mathbf{N}\mathfrak{p}_1, \dots, \mathbf{N}\mathfrak{p}_k < z} G(\mathfrak{p}_1 \dots \mathfrak{p}_k) = \sum_{s \le k/2} \sum_{\substack{\alpha_1 + \dots + \alpha_s = k, \\ \text{each } \alpha_i \ge 2}} \frac{k!}{\alpha_1! \dots \alpha_s!} \sum_{\substack{\mathfrak{p}_1 < \dots < \mathfrak{p}_s \\ \mathbf{N}\mathfrak{p}_s < z}} G(\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_s^{\alpha_s}),$$

where $\mathfrak{p} < \mathfrak{p}'$ is determined by a norm-compatible linear ordering on the prime ideals of $\mathcal{O}_K$. We note that, since $G(\mathfrak{p}^{\alpha}) \le \frac{f(\mathfrak{p})^2}{N\mathfrak{p}}$, the inner summation contributes no more than $O(\sigma_f(z)^{2s})$, which will be an error term unless $s = \frac{k}{2}$; the dependence of this error on k can be sussed out exactly as in Granville and Soundararajan's work. In fact, the handling of the main term, arising when k is even and $s = \frac{k}{2}$, is also essentially the same. In particular, the inner summation is equal to

$$\begin{aligned} \frac{1}{(\frac{k}{2})!} \sum_{\substack{\mathbf{N}\mathfrak{p}_1, \dots, \mathbf{N}\mathfrak{p}_{\frac{k}{2}} < z \\ \text{distinct}}} G(\mathfrak{p}_1^2 \dots \mathfrak{p}_{\frac{k}{2}}^2) &= \frac{1}{(\frac{k}{2})!} \left(\sum_{\mathbf{N}\mathfrak{p} < z} G(\mathfrak{p}^2) + O(\log\log k) \right)^{k/2} \\ &= \frac{1}{(\frac{k}{2})!} \left(\sigma_f(z)^2 + O(\log\log k) \right)^{k/2}. \end{aligned}$$

This yields Theorem 4.1. □

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Recall that we wish to show that the quantity

$$\frac{f(\chi) - \mu_f(X)}{\sigma_f(X)}, \ \chi \in C(K,X),$$

is normally distributed as $X \to \infty$. As remarked above, we will do so using the method of moments. In particular, we have that

$$\begin{aligned} \frac{1}{|C(K,X)|} \sum_{\chi \in C(K,X)} (f(\chi) - \mu_f(X))^k &= \frac{1}{|C(K,X)|} \sum_{\chi \in C(K,X)} \left(\sum_{\mathfrak{p} \mid \mathfrak{a}} f(\mathfrak{p}) - \sum_{\mathbf{N}\mathfrak{p} < X} \frac{f(\mathfrak{p})}{\mathbf{N}\mathfrak{p} + 1} + O(1) \right)^k \\ &= \frac{1}{|C(K,X)|} \sum_{\chi \in C(K,X)} \left(\sum_{\mathbf{N}\mathfrak{p} < z} g_{\mathfrak{p}}(\mathfrak{a}) + O\left(\frac{\log X}{\log z} \right) \right)^k. \end{aligned}$$

Considering the error term in Theorem 4.1, we take $z = X^{\frac{1-\lambda}{k}}$. With this choice, the inner summation becomes

$$\left(\sum_{\mathbf{N}\mathfrak{p}<z} g_{\mathfrak{p}}(\mathfrak{a})\right)^k + O\left(\sum_{j=0}^{k-1} k^j \left|\sum_{\mathbf{N}\mathfrak{p}<z} g_{\mathfrak{p}}(\mathfrak{a})\right|^{k-j}\right),$$

hence Theorem 4.1, the Cauchy-Schwarz inequality, and the fact that $\sigma_f(z) = \sigma_f(X) + O(\log k)$ yield that

$$\frac{1}{|C(K,X)|}\sum_{\chi\in C(K,X)} (f(\chi) - \mu_f(X))^k = c_k \sigma_f(X)^k \left(1 + O\left(\frac{k^{3/2}}{\sigma_f(X)}\right)\right)$$

if k is even, and

$$\frac{1}{|C(K,X)|}\sum_{\chi\in C(K,X)} (f(\chi) - \mu_f(X))^k \ll c_k \sigma_f(X)^{k-1} k^{3/2}$$

if k is odd. This proves the theorem. □

5. Proof of Main Theorems

In order to apply Theorem 1.3 to the additive function $g(\chi)$ defined in (3), we need to evaluate the quantities $\mu_g(X)$ and $\sigma_g(X)$. We begin with the following

Proposition 5.1. *Let $c \in K^\times$ be non-square. Then*

$$\sum_{\mathbf{N}\mathfrak{p}\leq X} \frac{1 + \left(\frac{c}{\mathfrak{p}}\right)}{\mathbf{N}\mathfrak{p}} = \log\log X + O(1).$$

Proof. This is a consequence of the prime ideal theorem and the fact that the Hecke L-function attached to the non-trivial character of $\mathrm{Gal}(K(\sqrt{c})/K)$ is analytic and non-vanishing on the line $\Re(s) = 1$. □

We now decompose $\mu_g(X)$ as

$$\mu_g(X) = \frac{1}{2}\sum_{\substack{\mathbf{N}\mathfrak{p}<X\\ \mathfrak{p}\nmid 2\Delta\infty}} \frac{1 + \left(\frac{\Delta'}{\mathfrak{p}}\right)}{\mathbf{N}\mathfrak{p}} - \frac{1}{2}\sum_{\substack{\mathbf{N}\mathfrak{p}<X\\ \mathfrak{p}\nmid 2\Delta\infty}} \frac{1 + \left(\frac{\Delta}{\mathfrak{p}}\right)}{\mathbf{N}\mathfrak{p}},$$

and it immediately follows from Proposition 5.1 that $\mu_g(X) = O(1)$. We also rewrite $\sigma_g(X)$ as

$$\sigma_g(X) = \left(\sum_{\substack{\mathbf{N}\mathfrak{p}\leq X, \mathfrak{p}\nmid 2\Delta\infty\\ \left(\frac{\Delta}{\mathfrak{p}}\right)\neq\left(\frac{\Delta'}{\mathfrak{p}}\right)}} \frac{1}{\mathbf{N}\mathfrak{p}}\right)^{1/2} = \left(\frac{1}{2}\sum_{\substack{\mathbf{N}\mathfrak{p}\leq X\\ \mathfrak{p}\nmid 2\Delta\infty}} \frac{1 - \left(\frac{\Delta\Delta'}{\mathfrak{p}}\right)}{\mathbf{N}\mathfrak{p}}\right)^{1/2}.$$

In order to apply Proposition 5.1 to $\sigma_g(X)$, we therefore need $\Delta\Delta'$ to be non-square in K. This will be the case when E does not have a cyclic 4-isogeny defined over $K(E[2])$.

Proposition 5.2. *If E is an elliptic curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $K(E[2])$, then $\Delta\Delta' \notin (K^\times)^2$*

Proof. This follows from Lemma 4.2 in [6]. □

By Proposition 5.1, we therefore get that $\sigma_g(X) = \sqrt{\frac{1}{2}\log\log X} + O(1)$ whenever E does not have a cyclic 4-isogeny defined over $K(E[2])$.

Proof of Theorem 1.2. Applying Theorem 1.3 to $g(\chi)$, we get that

$$\lim_{X\to\infty} \frac{\left|\left\{\chi \in C(K,X) : g(\chi) - O(1) \le z\left(\sqrt{\frac{1}{2}\log\log X} + O(1)\right)\right\}\right|}{|C(K,X)|} = G(z) \tag{4}$$

for every $z \in \mathbb{R}$. By Proposition 3.3, there is some contant C, independent of χ, such that $|g(\chi) - \mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi)| < C$, so in fact (4) holds with $g(\chi)$ replaced by $\mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi)$ and the result follows. □

Proof of Theorem 1.1. By Theorem 1.2,

$$\lim_{X\to\infty} \frac{|\{\chi \in C(K,X) : \mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi) \ge r\}|}{|C(K,X)|} = \frac{1}{2}$$

for any fixed $r \ge 0$. As $d_2(E^\chi/K) \ge \mathrm{ord}_2\mathcal{T}(E^\chi/E'^\chi) - 2$, this shows that for any $\epsilon > 0$,

$$\frac{|\{\chi \in C(K,X) : d_2(E^\chi/K) \ge r\}|}{|C(K,X)|} \ge \frac{1}{2} - \epsilon$$

for sufficiently large X. □

References

[1] J.W.S. Cassels. Arithmetic on curves of genus 1. VIII: On the conjectures of Birch and Swinnerton-Dyer. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1965(217):180–199, 1965.

[2] E.V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *Journal of Symbolic Computation*, 43(4):293–303, 2008.

[3] A. Granville and K. Soundararajan. Sieving and the Erdős–Kac theorem. *Equidistribution in number theory, an introduction*, pages 15–27, 2007.

[4] D.R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Inventiones mathematicae*, 118(1):331–370, 1994.

[5] Daniel Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra Number Theory*, 7(5):1253–1279, 2013.

[6] 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.

[7] Z. Klagsbrun, B Mazur, and K. Rubin. A Markov model for Selmer ranks in families of twists. *Compositio Math.*, to appear.

[8] Z. Klagsbrun and R. L. Oliver. The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point. *In preparation.*

[9] Z. Klagsbrun and R. L. Oliver. Elliptic curves and the joint distribution of additive functions. *In preparation.*

[10] 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.

[11] Maosheng Xiong. On Selmer groups of quadratic twists of elliptic curves with a two-torsion over $\mathbb{Q}$. *Mathematika*, 59(2):303–319, 2013.

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121
E-mail address: zdklags@ccrwest.org

Department of Mathematics, Stanford University, Building 380, Stanford, CA 94305
E-mail address: rjlo@stanford.edu