ON THE DISTRIBUTION OF 2-SELMER RANKS WITHIN QUADRATIC TWIST FAMILIES OF ELLIPTIC CURVES WITH PARTIAL RATIONAL TWO-TORSION

ZEV KLAGSBRUN

Abstract. This paper presents a new result concerning the distribution of 2-Selmer ranks in the quadratic twist family of an elliptic curve 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 $\mathbb{Q}$ and let $\text{Sel}_2(E/\mathbb{Q})$ be its 2-Selmer group (see Section 2 for its definition). We define the 2-Selmer rank of $E/\mathbb{Q}$, denoted $d_2(E/\mathbb{Q})$, by

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

For a given elliptic curve and non-negative integer $r$, we are able to ask what proportion of the quadratic twists of $E$ have 2-Selmer rank equal to $r$.

Let $S(X)$ be the set of squarefree natural numbers less than or equal to $X$. Heath-Brown proved that for the congruent number curve $y^2 = x^3 - x$, there are explicit constants $\alpha_0, \alpha_1, \alpha_2, \ldots$ summing to one such that

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

for every $r \in \mathbb{Z}_{\geq 0}$, where $E^d$ is the quadratic twist of $E$ by $d$ [HB94]. This result was extended by Swinnerton-Dyer and Kane 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 $\mathbb{Q}$ [Kan10, SD08]. More recently, Klagsbrun, Mazur, and Rubin showed that a version of this result is true for curves $E$ with $E(\mathbb{Q})[2] = 0$ and $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$ when a different method of counting is used [KMR11]. These results state that if the mod-4 representation of a curve $E$ satisfies certain conditions, then there is a discrete distribution on 2-Selmer ranks within the quadratic twist family of $E$. We show that this is not the case when $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $E$ does not have a cyclic 4-isogeny defined over $\mathbb{Q}(E[2])$. Specifically, we prove the following:

**Theorem 1.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic isogeny defined over $\mathbb{Q}(E[2])$. Then for any fixed $r$,

$$\liminf_{X \to \infty} \frac{|\{d \in S(X) : d_2(E^d/\mathbb{Q}) \geq r\}|}{|S(X)|} \geq \frac{1}{2}$$
and
\[
\liminf_{X \to \infty} \left| \left\{ \pm d \in S(X) : d_2(E^d/Q) \geq r \right\} \right| \geq \frac{1}{2} |S(X)|.
\]

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

Theorem 1 is proved by way of the result.

**Theorem 2.** Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) with \( E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \) that does not have a cyclic isogeny defined over \( \mathbb{Q}(E[2]) \). Then the normalized distribution
\[
P_r(\mathcal{T}(E/E'), X) \sqrt{\frac{1}{2} \log \log X}
\]
converges weakly to the Gaussian distribution
\[
G(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{w^2/2} dw,
\]
where
\[
P_r(\mathcal{T}(E/E'), X) = \frac{|\{ d \in S(X) : \text{ord}_2 \mathcal{T}(E^d/E'^d) \leq r \}|}{|S(X)|}
\]
for \( X \in \mathbb{R}^+ \), \( r \in \mathbb{Z}^\geq 0 \), and \( \mathcal{T}(E^d/E'^d) \) as defined in Section 2.

Theorem 2 will follow from a variant of the Erdös-Kac theorem for squarefree numbers which is proved in Appendix A.

Xiong and Zaharescu proved results similar to Theorems 1 and 2 in the special case when \( E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \) and \( E \) has a cyclic 4-isogeny defined over \( \mathbb{Q} \) [XZ08].

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 \( \phi \) and presenting some of the connections between them. Section 3 examines the behavior of the local conditions for the \( \phi \)-Selmer groups under quadratic twist. We prove Theorems 1 and 2 in Section 4 by combining the results of Sections 2 and 3 with a variant of the Erdös-Kac theorem for squarefree numbers which we prove in Appendix A.

1.3. **Acknowledgements.** I would like to express my thanks to Karl Rubin for his helpful comments and suggestions, to Ken Kramer for a series of valuable discussions, as well as to Michael Rael and Josiah Sugarman for helpful conversations regarding the Erdös-Kac theorem.

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 \( E(K)/2(K) \) maps into \( H^1(K, E[2]) \) via the Kummer map. The following diagram commutes for every place \( p \) of \( \mathbb{Q} \), where \( \delta \) is the Kummer map.
\[
\begin{array}{ccc}
E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[2]) \\
\downarrow & & \downarrow_{\text{Res} \ p} \\
E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) & \xrightarrow{\delta} & H^1(\mathbb{Q}_p, E[2])
\end{array}
\]
For each place $p$ of $\mathbb{Q}$, we define a distinguished local subgroup $H^1_\phi(Q_p, E[2]) \subset H^1(Q_p, E[2])$ by Image($\delta : E(Q_p)/2E(Q_p) \hookrightarrow H^1(Q_p, E[2])$). We define the **2-Selmer group** of $E/\mathbb{Q}$, denoted $\text{Sel}_2(E/\mathbb{Q})$, by

$$\text{Sel}_2(E/\mathbb{Q}) = \ker \left( H^1(Q, E[2]) \xrightarrow{\sum_{p \text{ of } \mathbb{Q}} \text{res}_p} \bigoplus_{p \text{ of } \mathbb{Q}} H^1(Q_p, E[2]) / H^1_\phi(Q_p, E[2]) \right).$$

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

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \text{Sel}_2(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[2] \to 0$$

where $\text{III}(E/\mathbb{Q})$ is the Tate-Shafaravich group of $E$.

**Definition 2.1.** We define the **2-Selmer rank** of $E$, denoted $d_2(E/\mathbb{Q})$, by

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

If $E(\mathbb{Q})$ has a point of order two, then we can define a Selmer group arising from the two-isogeny with kernel generated by that point. Explicitly, if $E$ is an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, then $E$ can be given by a model $y^2 = x^3 + Ax^2 + Bx$ with $A, B \in \mathbb{Z}$. The subgroup $C = E(\mathbb{Q})[2]$ is then generated by the point $P = (0, 0)$.

Given this model, we are able to define an isogeny $\phi : E \to E'$ with kernel $C$, where $E'$ is given by the model $y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$ and $\phi$ is given by $\phi(x, y) = \left( \left( \frac{x}{y} \right)^2, \frac{y(B-x^2)}{x} \right)$ for $(x, y) \notin C$. The isogeny $\phi$ gives rise to a pair of Selmer groups.

The isogeny $\phi$ gives a short exact sequence of $G_{\mathbb{Q}}$ modules

$$0 \to C \to E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \to 0.$$

This sequence gives rise to a long exact sequence of cohomology groups

$$0 \to C \to E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\delta} H^1(Q, C) \to H^1(Q, E) \to H^1(Q, E') \ldots$$

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

This sequence remains exact when we replace $\mathbb{Q}$ by its completion $\mathbb{Q}_p$ at any place $p$, which gives rise to the following commutative diagram.

$$\begin{array}{ccc}
E'(\mathbb{Q})/\phi(E(\mathbb{Q})) & \xrightarrow{\delta} & H^1(Q, C) \\
\downarrow & & \downarrow \text{Res}_p \\
E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) & \xrightarrow{\delta} & H^1(Q_p, C)
\end{array}$$

In a manner similar to how we defined the 2-Selmer group, we define distinguished local subgroups $H^1_\phi(Q_p, C) \subset H^1(Q_p, C)$ as the image of $E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p))$ under $\delta$ for each place $p$ of $\mathbb{Q}$. We define the **$\phi$-Selmer group** of $E$, denoted $\text{Sel}_\phi(E/\mathbb{Q})$ as

$$\text{Sel}_\phi(E/\mathbb{Q}) = \ker \left( H^1(Q, C) \xrightarrow{\sum_{p \text{ of } \mathbb{Q}} \text{res}_p} \bigoplus_{p \text{ of } \mathbb{Q}} H^1(Q_p, C) / H^1_\phi(Q_p, C) \right).$$

The group $\text{Sel}_\phi(E/\mathbb{Q})$ is a finite dimensional $\mathbb{F}_2$-vector space and we denote its dimension $\dim_{\mathbb{F}_2} \text{Sel}_\phi(E/\mathbb{Q})$ by $d_\phi(E/\mathbb{Q})$. 
The isogeny \( \phi \) on \( E \) gives rise to a dual isogeny \( \hat{\phi} \) on \( E' \) with kernel \( C' = \phi(E[2]) \). Exchanging the roles of \((E, C, \phi)\) and \((E', C', \hat{\phi})\) in the above defines the \( \hat{\phi} \)-Selmer group, \( \text{Sel}_{\hat{\phi}}(E'/Q) \), as a subgroup of \( H^1(Q, C') \). The following two theorems allow us to compare the \( \phi \)-Selmer group, the \( \hat{\phi} \)-Selmer group, and the 2-Selmer group.

**Theorem 2.2.** The \( \phi \)-Selmer group, the \( \hat{\phi} \)-Selmer group, and the 2-Selmer group sit inside the exact sequence

\[
0 \to E'(Q)[2]/\phi(E(Q)[2]) \to \text{Sel}_{\phi}(E/Q) \to \text{Sel}_2(E/Q) \xrightarrow{\hat{\phi}} \text{Sel}_{\hat{\phi}}(E'/Q).
\]

**Proof.** This is a well known diagram chase. See Lemma 2 in [FG08] for example. \( \square \)

The Tamagawa ratio \( T(E/E') \) gives a second relationship between \( d_\phi(E/Q) \) and \( d_{\hat{\phi}}(E'/Q) \).

**Definition 2.3.** The ratio

\[
T(E/E') = \frac{|\text{Sel}_{\phi}(E/Q)|}{|\text{Sel}_{\hat{\phi}}(E'/Q)|}
\]

is called the **Tamagawa ratio** of \( E \).

**Theorem 2.4** (Cassels). The Tamagawa ratio \( T(E/E') \) is given by

\[
T(E/E') = \prod_p \left| \frac{H^1_\phi(Q_p, C)}{2} \right|.
\]

**Proof.** This is a combination of Theorem 1.1 and equations (1.22) and (3.4) in [Cas65]. \( \square \)

Stepping back, we observe that if the Tamagawa ratio \( T(E/E') \geq 2^{r+2} \), then \( d_\phi(E/Q) \geq r + 2 \), and therefore by Theorem 2.2, \( d_2(E/Q) \geq r \). (If \( E \) does not have a cyclic 4-isogeny defined over \( Q \) then we can in fact show that \( T(E/E') \geq 2^r \) implies that \( d_2(E/Q) \geq r \), 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 \( E(Q)[2] \simeq \mathbb{Z}/2\mathbb{Z} \) that does not have a cyclic 4-isogeny defined over \( Q(E[2]) \) and let \( \phi \) be the isogeny with kernel \( C = E(Q)[2] \) defined in Section 2.

If \( p \nmid 2\infty \) is prime where \( E \) has good reduction, then \( H^1_\phi(Q_p, C) \) is a 1-dimensional \( \mathbb{F}_2 \) subspace of \( H^1(Q_p, C) \) equal to the unramified local subgroup \( H^1_{\text{ur}}(Q_p, C) \). If \( E \) has good reduction at \( p \nmid 2 \) and \( p \nmid d \), then the twisted curve \( E^d \) will have bad reduction at \( d \). The following lemma addresses the size of \( H^1_\phi(Q_p, C^d) \).

**Lemma 3.1.** Suppose \( p \neq 2 \) is a prime where \( E \) has good reduction and \( d \in \mathbb{Z} \) is squarefree with \( p \nmid d \).

(i) If \( E(Q_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \simeq E'(Q_p)[2] \), then \( \dim_{\mathbb{F}_2} H^1_\phi(Q_p, C^d) = 1 \).

(ii) If \( E(Q_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq E'(Q_p)[2] \), then \( \dim_{\mathbb{F}_2} H^1_\phi(Q_p, C^d) = 1 \).

(iii) If \( E(Q_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \) and \( E'(Q_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \), then \( \dim_{\mathbb{F}_2} H^1_\phi(Q_p, C^d) = 2 \).

(iv) If \( E(Q_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) and \( E'(Q_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \), then \( \dim_{\mathbb{F}_2} H^1_\phi(Q_p, C^d) = 0 \).

**Proof.** Lemma 3.7 in [Kla11] shows that \( E^d(Q_p)[2\infty]/\phi(E^d(Q_p)[2\infty]) = E^d(Q_p)[2]/\phi(E^d(Q_p)[2]) \). All four results then follow immediately. \( \square \)
The following proposition suggests that each of the cases in Lemma 3.1 should occur equally often.

**Proposition 3.2.** If $E$ is an elliptic curve with $E(Q)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over $Q(E[2])$, then $E'(Q)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $Q(E[2]) \neq Q(E'[2])$.

**Proof.** Let $Q' \in E'[2] - C'$, $C = \langle P \rangle$, and take $Q \in E[4]$ with $\phi(Q) = Q'$. Since $Q' \in E'(Q)[2] - C'$, and both $\phi \circ \hat{\phi} = [2]_{E'}$ and $\hat{\phi} \circ \phi = [2]_E$, it follows that $2Q = \hat{\phi}(Q') = P$. Let $M = Q(E[2])$. Since $E$ has no cyclic 4-isogeny defined over $M$, there exists $\sigma \in G_M$ such that $\sigma(Q) \notin \langle Q \rangle = \{0, Q, P, Q + P\}$. In particular, since $\phi^{-1}(Q') \subset \langle Q \rangle$, we get that $\phi(\sigma(Q)) \neq Q'$. We then get that

$$\sigma(Q') = \sigma(\phi(Q)) = \phi(\sigma(Q)) \neq Q',$$

showing that $Q'$ is not defined over $M$, and therefore that $Q(E'[2]) \not\subset M$. It then follows that $Q(E[2])$ and $Q(E'[2])$ are disjoint quadratic extensions of $Q$ and that $E'(Q)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. □

### 4. Proof of Main Theorems

In this section we prove Theorems 1 and 2 by analyzing the behavior of $\mathcal{T}(E/E')$ under quadratic twist and employing a variant of the Erdős-Kac theorem.

We begin by recalling the following definition.

**Definition 4.1.** A function $g : \mathbb{N} \to \mathbb{R}$ is called additive if $g(nm) = g(n) + g(m)$ whenever $n$ and $m$ are relatively prime.

If $g(n)$ is an additive function, then the classical Erdős-Kac theorem gives the distribution of $g(n)$ under mild hypothesis. The following variant of the Erdős-Kac theorem is for additive functions defined on the set of squarefree numbers $S$.

**Theorem 4.2.** Let $S$ be the set of squarefree natural numbers and suppose that $g : S \to \mathbb{R}$ is an additive function such that $|g(p)| \leq 1$ for all primes $p$. Let

$$A(x) = \sum_{p \leq x} \frac{g(p)}{p} \quad \text{and} \quad B(x) = \sqrt{\sum_{p \leq x} \frac{g(p)^2}{p}},$$

where the sums are taken over all primes less than or equal to $x$. If $B(x) = \omega \left( \log \log \log(x) \right)$ (in the asymptotic sense), then

$$v_x(n; g(n) - A(x) \leq zB(x)) = \frac{\left| \{n \in S(x) : g(n) - A(x) \leq zB(x)\} \right|}{|S(x)|}$$

converges weakly (i.e. pointwise in $z$) to

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

**Proof.** See Appendix A.

For $n \in S$, define an additive function $g(n)$ by

$$g(n) = \sum_{p|n, p \not\mid 2\Delta_{\infty}} \left( \frac{\Delta'}{p} - \left( \frac{\Delta}{p} \right) \right).$$
where \( \Delta \) is the discriminant of some integral model of \( E \) and \( \Delta' \) is the discriminant of some integral model of \( E' \). That is, \( g(d) \) roughly counts the difference between the number of primes dividing \( d \) where condition (iii) of Proposition 3.1 is satisfied and the number of primes dividing \( d \) where condition (iv) is satisfied. The value \( g(d) \) can therefore be connected to the Tamagawa ratio \( T(E^d/E'^d) \) in the following manner.

**Proposition 4.3.** The order of 2 in the Tamagawa ratio \( T(E^d/E'^d) \) is given by

\[
\text{ord}_2 T(E^d/E'^d) = g(d) + \sum_{v|2\Delta} \left( \dim_{\mathbb{F}_2} H^1_{\phi}(\mathbb{Q}_v, \mathcal{C}^d) - 1 \right).
\]

**Proof.** By Theorem 2.4, \( \text{ord}_2 T(E^d/E'^d) \) is given by

\[
\text{ord}_2 T(E^d/E'^d) = \sum_{v|2d} \left( \dim_{\mathbb{F}_2} H^1_{\phi}(\mathbb{Q}_v, \mathcal{C}^d) - 1 \right).
\]

Since \( E(\mathbb{Q}_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) if and only if \( \left( \frac{\Delta}{p} \right) = 1 \) and \( E'(\mathbb{Q}_p)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) if and only if \( \left( \frac{\Delta'}{p} \right) = 1 \) for primes \( p | d \) with \( p \nmid 2\Delta \), Lemma 3.1 gives us that

\[
\dim_{\mathbb{F}_2} H^1_{\phi}(\mathbb{Q}_p, \mathcal{C}^d) - 1 = \frac{\left( \frac{\Delta'}{p} \right) - \left( \frac{\Delta}{p} \right)}{2}
\]

for places \( p | d \) with \( p \nmid 2\Delta \). \( \square \)

The following proposition will allow us to evaluate \( A(x) \) and \( B(x) \) for \( g(n) \).

**Proposition 4.4.** Let \( c \) be a non-square integer. Then

\[
\sum_{p \leq x} \frac{1 + \left( \frac{c}{p} \right)}{p} = \log \log x + O(1).
\]

**Proof.** This is an application of Lemma 2.11 in [Ell79]. \( \square \)

**Proof of Theorem 2.** We wish to apply Theorem 4.2 to \( g(n) \). We may rewrite \( A(x) \) as

\[
\frac{1}{2} \sum_{\text{ord}_p n \text{ odd}} \frac{1 + \left( \frac{\Delta'}{p} \right)}{p} - \frac{1}{2} \sum_{\text{ord}_p n \text{ odd}} \frac{1 + \left( \frac{\Delta}{p} \right)}{p}.
\]

As \( \Delta' \) is not a square by Proposition 3.2, we therefore get that \( A(x) = O(1) \) by Proposition 4.4. We can rewrite \( B(x) \) as

\[
B(x) = \left[ \sum_{p \leq x, p \nmid 2\Delta} \frac{1}{p} \right] = \left[ \frac{1}{2} \sum_{p \leq x, p \nmid 2\Delta} \frac{1 - \left( \frac{\Delta}{p} \right)}{p} \right].
\]
By Proposition 3.2, $\Delta$ and $\Delta'$ do not differ by a square, so therefore $B(x) = \sqrt{\frac{1}{2} \log \log x} + O(1)$ by Proposition 4.3. Applying Theorem 4.2 to $g(n)$, we then get that

$$v_{x}\left(n; \frac{g(n)}{\sqrt{\frac{1}{2} \log \log x}} \leq z \right)$$

converges weakly to $G(z)$. By Proposition 4.3, $g(d) = \text{ord}_2 T(E^d/E'^d) + O(1)$, so the result follows.

□

Proof of Theorem 7. By Theorem 2,

$$\lim_{X \to \infty} \frac{|\{d \in S(X) : \text{ord}_2 T(E^d/E'^d) \geq r\}|}{|S(X)|} = \frac{1}{2}$$

for any fixed $r \geq 0$. As $d_2(E^d/Q) \geq \text{ord}_2 T(E^d/E'^d) - 2$, this shows that for any $\epsilon > 0$,

$$\frac{|\{d \in S(X) : d_2(E^d/Q) \geq r\}|}{|S(X)|} \geq \frac{1}{2} - \epsilon$$

for sufficiently large $X$. As twisting $E$ by $-d$ is equivalent to twisting $E^{-1}$ by $d$, the remainder of the result follows.

□

References

[Cas65] 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.

[CR62] E. Cohen and RL Robinson. On the distribution of the k-free integers in residue classes. Acta Arith. 8:283–293, 1962.

[Ell79] P. Elliott. Probabilistic number theory I: Mean-value theorems. Grundlehren der mathematischen Wissenschaften, 1979.

[FG08] EV Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. Journal of Symbolic Computation, 43(4):293–303, 2008.

[GS07] A. Granville and K. Soundararajan. Sieving and the Erdős–Kac theorem. Equidistribution in number theory, an introduction, pages 15–27, 2007.

[HB94] DR Heath-Brown. The size of Selmer groups for the congruent number problem, II. Inventiones mathematicae, 118(1):331–370, 1994.

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

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

[KMR11] Z. Klagsbrun, B Mazur, and K. Rubin. Selmer ranks of quadratic twists of elliptic curves. Preprint available at http://arxiv.org/pdf/1111.2321v1, 2011.

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

[XZ08] M. Xiong and A. Zaharescu. Distribution of Selmer groups of quadratic twists of a family of elliptic curves. Advances in Mathematics, 219(2):523–553, 2008.
Appendix A. An Erdős-Kac Theorem for Squarefree Numbers

The purpose of this appendix is to prove the following:

**Theorem 4.2.** Let $S$ be the set of squarefree natural numbers and suppose that $g : S \to \mathbb{R}$ is an additive function such that $|g(p)| \leq 1$ for all primes $p$. Let

$$A(x) = \sum_{p \leq x} \frac{g(p)}{p} \quad \text{and} \quad B(x) = \sqrt{\sum_{p \leq x} \frac{g(p)^2}{p}}.$$  

If $B(x) = o((\log \log \log(x)))$ (in the asymptotic sense), then

$$v(x; n; g(n) - A(x) \leq zB(x)) = \frac{|\{n \in S(x) : f(n) - A(x) \leq zB(x)\}|}{|S(x)|}$$

converges weakly (i.e. pointwise in $z$) to

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

The proof we present here is based on the framework developed by Granville and Soundararajan in [GS07] which is outlined in the following section.

A.1. Sieving and the Erdős-Kac Theorem. Let $\mathcal{A}$ be a finite sequence of natural numbers $a_1, a_2, \ldots, a_N$, $\mathcal{P}$ a set of primes, and $g : \mathcal{A} \to \mathbb{R}$ an additive function supported on $\mathcal{P}$ such that $|g(p)| \leq 1$ for every prime $p \in \mathcal{P}$. The goal is to identify the distribution of $g(n)$ on $\mathcal{A}$ and we pursue this by approximating its moments.

For any $d \in \mathcal{A}$, we define $\mathcal{A}_d = \{n \in \mathcal{A} : d \mid n\}$. Suppose that there is some multiplicative function $h(n) : \mathcal{A} \to \mathbb{R}$ such that we may write $|\mathcal{A}_d|$ as $|\mathcal{A}_d| = \frac{h(d)}{d} N + r_d$ for every $d \in \mathcal{A}$, where we think of $\frac{h(d)}{d}$ as the approximate proportion of elements $\mathcal{A}$ divisible by $d$ and $r_d$ as the error. If the errors $r_d$ are sufficiently small, then the moments will be close to those of a normal distribution. We define approximations of the mean and variance of $g(n)$ by

$$\mu_\mathcal{P}(g) = \sum_{p \in \mathcal{P}} g(p) \frac{h(p)}{p} \quad \text{and} \quad \sigma_\mathcal{P}(g)^2 = \sum_{p \in \mathcal{P}} g(p)^2 \frac{h(p)}{p} \left(1 - \frac{h(p)}{p}\right).$$

We then have the following:

**Theorem A.1** (Theorem 4 in [GS07]). For $k \in \mathbb{N}$, let $\mathcal{D}_k(\mathcal{P})$ be the set of squarefree products of $k$ or fewer primes in $\mathcal{P}$ that are contained in $\mathcal{A}$. Define $C_k = \frac{\Gamma(k + 1)}{\Gamma(k/2 + 1)}$. Then, uniformly for all even positive integers $k \leq \sigma_\mathcal{P}(g)^2$, we have

$$\sum_{n \in \mathcal{A}} (g(n) - \mu_\mathcal{P}(g))^k = C_k N \sigma_\mathcal{P}(g)^k \left(1 + O\left(\frac{k^3}{\sigma_\mathcal{P}(g)^2}\right)\right) + O\left(\sum_{p \in \mathcal{P}} \frac{h(p)}{p} \right)^k \sum_{d \in \mathcal{D}_k(\mathcal{P})} |r_d|$$

and uniformly for all odd positive integers $k \leq \sigma_\mathcal{P}(g)^2$, $\sum_{n \in \mathcal{A}} (g(n) - \mu_\mathcal{P}(g))^k$ satisfies

$$\sum_{n \in \mathcal{A}} (g(n) - \mu_\mathcal{P}(g))^k \ll C_k N \sigma_\mathcal{P}(g)^k \frac{k^3}{\sigma_\mathcal{P}(g)} + \left(\sum_{p \in \mathcal{P}} \frac{h(p)}{p} \right)^k \sum_{d \in \mathcal{D}_k(\mathcal{P})} |r_d|.$$
Theorem A.1 can be used in the following way. Suppose \( A \) is an infinite sequence and \( g : A \rightarrow \mathbb{R} \) an additive function with \( |g(p)| \leq 1 \) for every prime \( p \). For \( N \in \mathbb{N} \), we may define \( A(N) \) as \( a_1, a_2, \ldots a_N \) and \( \mathcal{P}(N) = \{ p \text{ prime } : p \leq Y(N) \} \) for some appropriately chosen function \( Y(N) \). We then define \( g_N(n) \) as

\[
g_N(n) = \sum_{p \in \mathcal{P}(N)} g(p)
\]

and apply Theorem A.1 to \( g_N \) on \( A(N) \). For notational purposes, let \( \mu_N := \mu_{\mathcal{P}(N)}(g_N) \) and \( \sigma_N := \sigma_{\mathcal{P}(N)}(g_N) \). If \( Y(N) \) is chosen appropriately so that

(i) the errors \( \frac{k^3}{\sigma_N^3} \) and \( \frac{k^2}{\sigma_N^2} \) both tend to 0 and \( N \rightarrow \infty \),

(ii) \[
\frac{\left( \sum_{p \in \mathcal{P}(N)} \frac{h(p)}{p} \right)^k \sum_{d \in D_k(\mathcal{P}(N))} |r_d|}{\sigma_N^k} = o(N), \quad \text{and}
\]

(iii) \( g_N(n) = g(n) + o(\sigma_N) \),

then the moments of \( \frac{g(n) - \mu_N}{\sigma_N} \) tend to \( C_k \) for \( k \) even and to zero for \( k \) odd as \( N \rightarrow \infty \).

Suppose that we are in the special case where \( A \) is an increasing sequence and let \( \mu_g(N) = \sum_{p \leq a_N} g(p) \frac{h(p)}{p} \) and \( \sigma_g^2(N) = \sum_{p \leq a_N} g(p)^2 \frac{h(p)}{p} \left( 1 - \frac{h(p)}{p} \right) \). If we additionally have that \( \sigma_g(N) \rightarrow \infty \) and that

\[
\sigma_g(N) = \sigma_N + o(\sigma_N) \quad \text{and} \quad \mu_g(N) = \mu_N + o(\sigma_N),
\]

then we actually get that the moments of \( \frac{g(n) - \mu_g(N)}{\sigma_g(N)} \) tend to \( C_k \) for \( k \) even and 0 for \( k \) odd as \( N \rightarrow \infty \). Since the \( k^{th} \) moments of the standard normal distribution \( \mathcal{N}(0,1) \) are 0 for \( k \) odd and \( C_k \) for \( k \) even and the normal distribution \( \mathcal{N}(0,1) \) is determined by its moments, we then have that

\[
v_x \left( n; \frac{g(n) - \mu_g(x)}{\sigma_g(x)} \leq z \right) = \frac{|\{ n \in A, n \leq x : \frac{g(n) - \mu_g(x)}{\sigma_g(x)} \leq z \}|}{|\{ n \in A, n \leq x \}|}
\]

converges weakly to

\[
G(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-w^2/2} \, dw.
\]

This will all be the case for the set of squarefree numbers which we examine in the next section.

A.2. Application to Squarefree Numbers. Let \( S \) be the sequence of squarefree natural numbers and suppose that \( g : S \rightarrow \mathbb{R} \) is an additive function with \( |g(p)| \leq 1 \) for every prime \( p \). As \( S \) is increasing and \( a_N = O(N) \), rather than considering the first \( N \) elements of \( S \), we will instead work with \( S(X) = \{ n \in S : n \leq X \} \) and adjust the notation accordingly. Define \( h(d) = \frac{d}{\sigma(d)} \) where \( \sigma(d) \) is the sum of the divisors of \( d \). The function \( h(d) \) is multiplicative and we have the following:

**Proposition A.2.** For \( d \in S(X) \), \( r_d = O(X^{\frac{3}{4}}) \).
Proof. The basic idea here is that if $d$ is squarefree, then the squarefree numbers should distribute approximately uniformly within the set of squarefree classes modulo $d^2$. Let $a$ be a squarefree integer with $0 < a < d^2$. By Corollary 1 to Theorem 1 in [CR62],

$$\left|\{n \in S(X) : n \equiv a \pmod{d^2}\}\right| = \frac{6}{\pi^2} \prod_{p \mid d} \frac{1}{(p^2 - 1)} X + O\left(\sqrt{X}\right).$$

There are $\phi(d)$ squarefree classes modulo $d^2$ that are congruent to zero modulo $d$. This yields

(4) \quad \left|\{n \in S(X) : d \mid n\}\right| = \frac{6}{\pi^2} \prod_{p \mid d} \frac{1}{(p + 1)} X + O\left(d\sqrt{X}\right) = \frac{6}{\pi^2} \frac{1}{\sigma(d)} X + O\left(d\sqrt{X}\right).

As $|S(X)| = \frac{6}{\pi^2} X + O\left(\sqrt{X}\right)$ and $\frac{h(d)}{d} = \frac{1}{\sigma(d)}$, this proves the result for $d = O(X^{\frac{1}{2}})$.

However, for $d = \Omega(X^{\frac{1}{2}})$, both $|S(X)_d| = O(N^{\frac{1}{2}})$ and $\frac{h(d)}{d} X = O(X^{\frac{1}{2}})$, so it follows that $r_d = O(X^{\frac{1}{2}})$ for such $d$ as well.

We can now prove Theorem 1.2.

Proof of Theorem 1.2. Set $Y(X) = X^{\frac{1}{B(Y(X))}}$ and define

$$\mu_X = \sum_{p \leq Y(X)} g(p) \frac{h(p)}{p} \quad \text{and} \quad \sigma_X^2 = \sum_{p \leq Y(X)} g(p)^2 \frac{h(p)}{p} \left(1 - \frac{h(p)}{p}\right).$$

As $\frac{h(p)}{p} = \frac{1}{p + 1}$, we then get that

$$\mu_X = \sum_{p \leq Y(X)} \frac{g(p)}{p + 1} = \sum_{p \leq Y(X)} \frac{g(p)}{p} + O(1) = A(Y(X)) + O(1)$$

and

$$\sigma_X^2 = \sum_{p \leq Y(X)} \frac{g(p)^2}{p} + O(1) = B(Y(X))^2 + O(1).$$

As we assume that $B(X) \to \infty$ as $X \to \infty$, it then follows that $Y(X) \to \infty$ as $X \to \infty$ and therefore that $B(Y(X)) \to \infty$ and $\sigma_X \to \infty$ as $X \to \infty$. We therefore get that the error terms $\frac{k^3}{\sigma_X^3}$ and $\frac{k^2}{\sigma_X^2}$ both tend to 0 as $X \to \infty$ for fixed $k$.

Next, consider

$$\frac{\left(\sum_{p \leq Y(X)} \frac{h(p)}{p}\right)^k}{\sigma_X^k} \sum_{d \mid D_k(Y(X))} |r_d|,$$

where $D_k(Y(X))$ is the set of products of $k$ or fewer primes less than or equal to $Y(X)$ contained in $S(X)$. Trivial estimates show that $|D_k(Y(X))| = O\left(kX^{\frac{k}{B(Y(X))}}\right)$. As $B(X) \to \infty$, for fixed $k$ we therefore have that $|D_k(Y(X))| = o(X^\epsilon)$ for any $\epsilon \geq 0$. Similarly, Mertens’ Theorem shows that

$$\left(\sum_{p \leq Y(X)} \frac{1}{p + 1}\right)^k = (\log \log Y(X) + O(1))^k.$$
and therefore that
\[
\left( \sum_{p \leq Y(X)} \frac{1}{p+1} \right)^k = o(X^\epsilon)
\]
for any \( \epsilon \geq 0 \) as well. Combined with Proposition A.2, we then get that
\[
\left( \sum_{p \leq Y(X)} \frac{h(p)}{p} \right)^k \sum_{d \in \mathcal{D}_n(Y(X))} |r_d| \sigma_X^k = O(X^{3/2+\epsilon})
\]
for any \( \epsilon > 0 \).

Since a number \( n \leq X \) can have at most \( B(X)^{2/3} \) prime factors greater than \( X^{B(X)^{2/3}} \), it therefore follows
\[
g(n) - g_X(n) = g(n) - \sum_{p \leq Y(X)} g(p) = \sum_{Y(X) < p \leq X} g(p) \leq B(X)^{2/3}.\]

In order for \( g(n) - g_X(n) = o(\sigma_X) \), it therefore suffices for \( B(X) = \sigma_X + o(\sigma_X) \). Along with the discussion at the end of Section A.1, it is then enough to show that \( B(X) = \sigma_X + o(\sigma_X) \) and that \( A(X) = \mu_X + o(\sigma_X) \) to complete the proof.

Recalling that \( \mu_X = A(Y(X)) + O(1) \) and \( \sigma_X = B(Y(X)) + O(1) \), we have
\[
A(X) - A(Y(X)) \leq \sum_{X^{B(X)^{2/3}} \leq p \leq X} \frac{1}{p} = \log \log X - \log \log X^{B(X)^{2/3}} + O(1) = O(\log \log \log X),
\]
with the first equality coming from Mertens's theorem and the final equality following from the fact that \( B(X) = O(\sqrt{\log \log X}) \).

Similarly, for sufficiently large \( X \), we have
\[
B(X) - B(Y(X)) \leq B(X)^2 - B(Y(X))^2 = \sum_{X^{B(X)^{2/3}} \leq p \leq X} \frac{1}{p} = O(\log \log \log X).
\]

The fact that \( B(X) = O(\sqrt{\log \log X}) \) and the assumption that \( B(X) = \omega(\log \log (x)) \) then give that \( B(X) = \sigma_X + o(\sigma_X) \) and \( A(X) = \mu_X + o(\sigma_X) \). \( \square \)