Ranks of Elliptic Curves in Families of Quadratic Twists

Karl Rubin and Alice Silverberg

CONTENTS

The authors thank NSF and NSA for financial support.

We show that the unboundedness of the ranks of the quadratic twists of an elliptic curve is equivalent to the divergence of certain infinite series.

1. INTRODUCTION

In this paper we reformulate the question of whether the ranks of the quadratic twists of an elliptic curve over $\mathbb{Q}$ are bounded, into the question of whether certain infinite series converge. Our results were inspired by ideas in [Gouvêa and Mazur 1991].

Fix integers a, b, c such that the polynomial

$$f(x) = x^3 + ax^2 + bx + c$$

has 3 distinct complex roots, and let E be the elliptic curve $y^2 = f(x)$. For $D \in \mathbb{Z} - \{0\}$, let $E^{(D)}$ be the elliptic curve $Dy^2 = f(x)$.

For every rational number x which is not a root of $f(x)$, there are a unique squarefree integer D and rational number y such that $(x, y) \in E^{(D)}(\mathbb{Q})$. For all but finitely many x, the point (x, y) has infinite order on the elliptic curve $E^{(D)}$. Gouvêa and Mazur [1991] counted the number of D that occur this way as x varies, and thereby obtained lower bounds for the number of D in a given range for which $E^{(D)}(\mathbb{Q})$ has positive rank.

Building on their idea, in this paper we keep track not only of the number of D which occur, but also how often each D occurs. The philosophy is that the greater the rank of $E^{(D)}$, the more often D should occur, i.e., curves of high rank should "rise to the top". By implementing our approach, Rogers [2000] found a curve of rank 6 in the family $Dy^2 = x^3 - x$.

Let

$$F(u, v) = v(u^3 + au^2v + buv^2 + cv^3) = v^4 f(u/v),$$

© A K Peters, Ltd.
1058-6458/2000 $0.50 per page

and

$$\Psi = \{(u,v) \in \mathbb{Z}^2 : \gcd(u,v) = 1 \text{ and } F(u,v) \neq 0\}.$$

We define three families of infinite series as follows.

If $n \in \mathbb{Q}^\times$, let $s(n)$ denote the squarefree part of n, i.e., $s(n)$ is the unique squarefree integer such that $n = s(n)m^2$ with $m \in \mathbb{Q}$. Note that

$$s(f(u/v)) = s(F(u,v))$$

for all $u, v \in \mathbb{Z}$ such that $F(u,v) \neq 0$. If α is a non-zero rational number, and $\alpha = u/v$ with u and v relatively prime integers, define

$$h(\alpha) = \max\{1, \log|u|, \log|v|\}.$$

For non-negative real numbers j and k define the infinite sums

$$S_E(j,k) = \sum_{(u,v)\in\Psi} \frac{1}{|s(F(u,v))|^k h(u/v)^j},$$

$$R_E(j,k) = \sum_{t=1}^{\infty} \sum_{\substack{(u,v)\in\Psi \\ t^2|F(u,v)}} \frac{t^{2k}}{|F(u,v)|^k h(u/v)^j}.$$

Further, if d is a positive integer, let

$$\Omega_d = \{\alpha \in \mathbb{Z}/d^2\mathbb{Z} : f(\alpha) \equiv 0 \pmod{d^2}\}.$$

If d and d' are positive integers and $\alpha \in \Omega_d$, let $\omega_{\alpha,d,d'}$ be a shortest non-zero vector in the lattice

$$\mathcal{L}_{\alpha,d,d'} = \{(u,v) \in \mathbb{Z}^2 : u \equiv \alpha v \pmod{d^2} \text{ and } v \equiv 0 \pmod{d'^2}\}.$$

(In general there will be more than one shortest vector; just choose one of them.) Define

$$Q_E(j,k) = \sum_{\substack{d,d'=1 \\ \gcd(d,d')=1}}^{\infty} \frac{(dd')^{2k}}{\max(1,\log(dd'))^j} \sum_{\substack{\alpha\in\Omega_d \\ \omega_{\alpha,d,d'}\in\Psi}} \|\omega_{\alpha,d,d'}\|^{-4k}.$$

Our main result is the following, which will be proved in Sections 2–4.

Theorem 1.1. *If j is a positive real number, then the following conditions are equivalent*:

(a) $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) < 2j$ *for every* $D \in \mathbb{Z} - \{0\}$.
(b) $S_E(j,k)$ *converges for some* $k \geq 1$.
(c) $S_E(j,k)$ *converges for every* $k \geq 1$.
(d) $R_E(j,k)$ *converges for some* $k \geq 1$.
(e) $R_E(j,k)$ *converges for every* $k \geq 1$.
(f) $Q_E(j,k)$ *converges for some* $k \geq 1$.
(g) $Q_E(j,k)$ *converges for every* $k \geq 1$.

It follows from Theorem 1.1 that for many elliptic curves E and for small values of j, $S_E(j,k)$, $R_E(j,k)$, and $Q_E(j,k)$ diverge for all real numbers k.

Example 1.2. Consider the case $f(x) = x^3 - x$. Here, $F(u,v) = uv(u+v)(u-v)$. If $\gcd(u,v) = 1$ and $F(u,v) \neq 0$, then

$$s(F(u,v)) = s(u)s(v)s(u+v)s(u-v)/m,$$

with $m = 1$ or 4. The family of quadratic twists $Dy^2 = x^3 - x$ has been extensively studied.

Ranks in families of twists of elliptic curves have also been studied by Heegner [1952], Kramarz [1986], Satgé [1987], Zagier and Kramarz [1987], Gouvêa and Mazur [1991], Heath-Brown [1993; 1994], Stewart and Top [1995], and Mestre [1992; 1998], among others.

2. RELATING $S_E(j,k)$ TO TWISTS OF E

If A is an elliptic curve over $\mathbb{Q}$, let $\hat{h}_A : A(\bar{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ denote the canonical height function on $A(\bar{\mathbb{Q}})$. We abbreviate $\hat{h}_D = \hat{h}_{E^{(D)}}$ for squarefree integers D.

If $X \subset \mathbb{R}$, define

$$T_E(j,k,X) = \sum_{\substack{D\in\mathbb{Z}-0 \\ D \text{ squarefree}}} |D|^{-k} \sum_{\substack{P\in E^{(D)}(\mathbb{Q})-E^{(D)}(\mathbb{Q})_{\text{tors}} \\ x(P)\in X}} \hat{h}_D(P)^{-j}$$

where $x(P)$ is the x-coordinate of P, and define

$$S_E(j,k,X) = \sum_{(u,v)\in\Psi, u/v\in X} \frac{1}{\left|s(F(u,v))\right|^k h(u/v)^j},$$

$$R_E(j,k,X) = \sum_{t=1}^{\infty} \sum_{\substack{(u,v)\in\Psi \\ u/v\in X, t^2|F(u,v)}} \frac{t^{2k}}{\left|F(u,v)\right|^k h(u/v)^j}.$$

Then

$$S_E(j,k,\mathbb{R}) = S_E(j,k),$$
$$R_E(j,k,\mathbb{R}) = R_E(j,k),$$

as defined in Section 1. Let $T_E(j,k) = T_E(j,k,\mathbb{R})$.

If $X \subset \mathbb{R}$, define

$$\Sigma_{D,X} = \{(u,v) \in \Psi : u/v \in X,\ v > 0, \text{ and } s(F(u,v) = D)\}. \quad (2\text{–}1)$$

If A is an elliptic curve over $\mathbb{Q}$, let A_N denote the N-torsion on A. The following fact is easily proved:

Lemma 2.1. *If D is a squarefree integer and $X \subset \mathbb{R}$, then the map*

$$\varphi_D(u,v) = \left(\frac{u}{v}, \frac{\sqrt{F(u,v)/D}}{v^2}\right)$$

defines a bijection

$$\varphi_D : \Sigma_{D,X} \to \{P \in E^{(D)}(\mathbb{Q}) - E_2^{(D)}(\mathbb{Q}) : x(P) \in X\}/\pm 1.$$

Proposition 2.2. *If $j,k \geq 0$ and $X \subset \mathbb{R}$, then the convergence of $T_E(j,k,X)$ is equivalent to the convergence of $S_E(j,k,X)$.*

Proof. We have

$$\begin{aligned} S_E(j,k,X) &= \sum_{\substack{(u,v)\in\Psi \\ u/v\in X}} \bigl|s(F(u,v))\bigr|^{-k} h(u/v)^{-j} \\ &= 2 \sum_{D\,\text{squarefree}} |D|^{-k} \sum_{(u,v)\in\Sigma_{D,X}} h(u/v)^{-j}. \end{aligned}$$

By Lemma 2.1,

$$T_E(j,k,X) = 2 \sum_{D\,\text{squarefree}} |D|^{-k} \sum_{\substack{(u,v)\in\Sigma_{D,X} \\ \varphi_D(u,v)\notin E^{(D)}(\mathbb{Q})_{\text{tors}}}} \hat{h}_D(\varphi_D(u,v))^{-j}.$$

For $(x,y) \in E^{(D)}(\mathbb{Q})$ we have

$$\hat{h}_D(x,y) = \hat{h}_E(x, \sqrt{D}y);$$

see [Silverman 1986, hint in Exercise 8.17, p. 239]. For $(x,y) \in E(\bar{\mathbb{Q}})$ with $x \in \mathbb{Q}$,

$$\bigl|\hat{h}_E(x,y) - \tfrac{1}{2}h(x)\bigr|$$

is bounded independently of x and y; see [Silverman 1986, Theorem VIII.9.3(e)]. Therefore there is a constant C (independent of u, v, D, and X) such that for $(u,v) \in \Sigma_{D,X}$,

$$\bigl|\hat{h}_D(\varphi_D(u,v)) - \tfrac{1}{2}h(u/v)\bigr| \leq C.$$

Except for finitely many rational numbers u/v, we have $\frac{1}{4}h(u/v) > C$. Therefore if either $|u|$ or $|v|$ is sufficiently large, then

$$\tfrac{1}{4}h(u/v) \leq \hat{h}_D(\varphi_D(u,v)) \leq h(u/v). \tag{2–2}$$

Thus the convergence or divergence of $S_E(j,k,X)$ is equivalent to that of $T_E(j,k,X)$. □

If A is an elliptic curve defined over $\mathbb{R}$, let $A(\mathbb{R})^0$ denote the connected component of the identity in $A(\mathbb{R})$.

Lemma 2.3. *Suppose A is an elliptic curve over $\mathbb{R}$, $P_1, \dots, P_r \in A(\mathbb{R})^0$ are $\mathbb{Z}$-linearly independent in $A(\mathbb{R})/A(\mathbb{R})_{\text{tors}}$, and U is an open subset of $A(\mathbb{R})^0$. Then*

$$\lim_{B\to\infty} \frac{\#\{(n_1,\dots,n_r) \in \mathbb{Z}^r : |n_i| \leq B,\ \sum n_i P_i \in U\}}{(2B+1)^r} = \mu(U),$$

where μ is a Haar measure on $A(\mathbb{R})^0$ normalized so that $\mu(A(\mathbb{R})^0) = 1$.

Proof. Let $\langle z \rangle = z - \lfloor z \rfloor \in [0,1)$ denote the fractional part of a real number z. By [Koksma 1974, Satz 10, p. 93], if $\alpha_1, \dots, \alpha_r \in \mathbb{R}$ are $\mathbb{Z}$-linearly independent in $\mathbb{R}/\mathbb{Q}$ and $0 \leq a \leq b \leq 1$, then the limit as $B \to \infty$ of

$$\frac{\#\{(n_1,\dots,n_r) \in \mathbb{Z}^r : |n_i| \leq B,\ a < \langle \sum n_i \alpha_i \rangle < b\}}{(2B+1)^r}$$

equals $b - a$. Since $A(\mathbb{R})^0 \cong \mathbb{R}/\mathbb{Z}$, the lemma follows easily. □

If A is an elliptic curve over $\mathbb{Q}$, let

$$h_A^{\min} = \min_{\substack{P\in A(\mathbb{Q}) \\ \hat{h}_A(P)\neq 0}} \hat{h}_A(P) > 0.$$

Proposition 2.4. *Suppose A is an elliptic curve over $\mathbb{Q}$ and j is a positive real number. Let $r = \operatorname{rank}_{\mathbb{Z}} A(\mathbb{Q})$.*

1. *If $r \geq 2j$ and U is a nonempty open subset of $A(\mathbb{R})^0$, then*
$$\sum_{P\in(A(\mathbb{Q})-A(\mathbb{Q})_{\text{tors}})\cap U} \hat{h}_A(P)^{-j}$$
diverges.
2. *If $r < 2j$, then there exists a constant C_j depending only on j (and independent of A) such that*
$$\sum_{P\in A(\mathbb{Q})-A(\mathbb{Q})_{\text{tors}}} \hat{h}_A(P)^{-j} \leq \#A(\mathbb{Q})_{\text{tors}} (h_A^{\min})^{-j} C_j.$$

Proof. Suppose $P_1, \dots, P_r$ is a $\mathbb{Z}$-basis of

$$A(\mathbb{Q}) \cap A(\mathbb{R})^0$$

modulo torsion. The canonical height function $\hat{h}_A$ is a quadratic form on the lattice $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$, and

$$\sum_{P\in A(\mathbb{Q})-A(\mathbb{Q})_{\text{tors}}} \hat{h}_A(P)^{-j} \geq \sum_{n_1,\dots,n_r=-\infty}^{\infty} \hat{h}\bigl(\sum n_i P_i\bigr)^{-j}.$$

By the theory of Epstein zeta functions, the latter sum diverges if $2j \leq r$. Using Lemma 2.3 it is now straightforward to deduce (i).

By [Terras 1988, IV.4.4, Proposition 1(c)], there exist a positive constant K_r depending only on r, and a $\mathbb{Z}$-basis $P_1, \dots, P_r$ for $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$, such that for all $(n_1, \dots, n_r) \in \mathbb{Z}^r$,

$$\hat{h}_A\Big(\sum_{i=1}^r n_i P_i\Big) \geq K_r \sum_{i=1}^r n_i^2 \hat{h}_A(P_i) \geq K_r h_A^{\min} \sum_{i=1}^r n_i^2.$$

Let $\mathcal{E}_r(j) = \sum_{0 \neq \omega \in \mathbb{Z}^r} \|\omega\|^{-2j}$. Then

$$\begin{aligned}\sum_{P \in A(\mathbb{Q}) - A(\mathbb{Q})_{\text{tors}}} \hat{h}_A(P)^{-j} &\leq \#A(\mathbb{Q})_{\text{tors}} \sum_{0 \neq \omega \in \mathbb{Z}^r} (h_A^{\min})^{-j} K_r^{-j} \|\omega\|^{-2j} \\ &= \#A(\mathbb{Q})_{\text{tors}} (h_A^{\min})^{-j} K_r^{-j} \mathcal{E}_r(j).\end{aligned}$$

The Epstein zeta function $\mathcal{E}_r(j)$ converges if $r < 2j$; see [Terras 1985, I.1.4]. Thus assertion (ii) is true with $C_j = \max_{r<2j}(K_r^{-j}\mathcal{E}_r(j))$. □

Remark 2.5. Proposition 2.4(ii) remains true, with the same proof, when $\mathbb{Q}$ is replaced by a number field. Proposition 2.4(i) remains true, with the same proof, when $\mathbb{Q}$ is replaced by a number field with a real embedding, or when $\mathbb{Q}$ is replaced by an arbitrary number field and U is replaced by $A(\mathbb{C})$.

Definition 2.6. Write $e_{\max}$ and $e_{\min}$ for the largest and smallest real root of f, respectively. We say that X is *broad* if X is an open subset of $\mathbb{R}$ which has nontrivial intersection with both of the intervals $(e_{\max}, \infty)$ and $(-\infty, e_{\min})$.

Theorem 2.7. *If j is a positive real number, then the following are equivalent*:

(a) $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) < 2j$ *for every* $D \in \mathbb{Z} - \{0\}$,
(b) $S_E(j,k,X)$ *converges for some* $k \geq 1$ *and some broad* X,
(c) $S_E(j,k)$ *converges for every* $k \geq 1$.

Proof. Fix a positive real number j. Clearly, (c) $\Longrightarrow$ (b), by taking $X = \mathbb{R}$.

If $S_E(j,k,X)$ converges for some $k \geq 1$, and some broad X, then by Proposition 2.2, $T_E(j,k,X)$ converges as well. In particular for every squarefree D the inner sum

$$\sum_{\substack{P \in E^{(D)}(\mathbb{Q}) - E^{(D)}(\mathbb{Q})_{\text{tors}} \\ x(P) \in X}} \hat{h}_D(P)^{-j}$$

converges. Since X is broad, the set

$$U = \{P \in E^{(D)}(\mathbb{R}) : x(P) \in X\} \cap E^{(D)}(\mathbb{R})^0$$

is nonempty. Proposition 2.4(i) now shows that $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) < 2j$. This proves that (b) $\Longrightarrow$ (a).

Now suppose that $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) < 2j$ for every $D \in \mathbb{Z} - \{0\}$. Let

$$h_D^{\min} = h_{E^{(D)}}^{\min} = \min_{\substack{P \in E^{(D)}(\mathbb{Q}) \\ \hat{h}_{E^{(D)}}(P) \neq 0}} \hat{h}_{E^{(D)}}(P).$$

By Mazur's Theorem [Mazur 1977], $\#E^{(D)}(\mathbb{Q})_{\text{tors}} \leq 16$. By Proposition 2.4(ii),

$$\sum_{P \in E^{(D)}(\mathbb{Q}) - E^{(D)}(\mathbb{Q})_{\text{tors}}} \hat{h}_D(P)^{-j} \leq 16 (h_D^{\min})^{-j} C_j.$$

Therefore

$$T_E(j,k) \leq 16 C_j \sum_{\substack{D \in \mathbb{Z} - 0 \\ D \text{ squarefree}}} |D|^{-k} (h_D^{\min})^{-j}.$$

It follows from [Silverman 1986, Exercise 8.17c on p. 239] that there exists $D_0 > 1$, depending on E, such that

$$h_D^{\min} > \frac{1}{12} \log |D| \quad \text{if } |D| > D_0.$$

Thus, for a new constant C'_j,

$$T_E(j,k) \leq C'_j \Bigg(\sum_{\substack{|D| \leq D_0 \\ D \text{ squarefree}}} |D|^{-k} (h_D^{\min})^{-j} + \sum_{D>1} |D|^{-k} (\log |D|)^{-j} \Bigg).$$

It follows that $T_E(j,k)$ converges if $k > 1$, or if $k = 1$ and $j > 1$. There exists a D such that

$$\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) \geq 2$$

(by [Mestre 1992] when the j-invariant of E is not 0 or 1728; however, Mestre says he shows this in general in unpublished work). Therefore $j > 1$, so $T_E(j,k)$ converges. By Proposition 2.2, $S_E(j,k)$ converges. Therefore, (a) $\Longrightarrow$ (c). □

3. RELATING $R_E(j,k)$ AND $S_E(j,k)$

Proposition 3.1. *If $k > \frac{1}{2}$, $j \geq 0$, and $X \subset \mathbb{R}$, then*:

(i) $S_E(j,k,X) \leq R_E(j,k,X) \leq \zeta(2k) S_E(j,k,X)$.
(ii) $R_E(j,k,X)$ *converges if and only if* $S_E(j,k,X)$ *converges*.

Proof. We have

$$\begin{aligned} S_E(j,k,X) &= \sum_{(u,v)\in\Psi,u/v\in X} \bigl|s(F(u,v))\bigr|^{-k} h(u/v)^{-j} \\ &\le \sum_{t=1}^{\infty} \sum_{\substack{(u,v)\in\Psi \\ u/v\in X, t^2|F(u,v)}} t^{2k}\bigl|F(u,v)\bigr|^{-k} h(u/v)^{-j} \\ &= R_E(j,k,X) \\ &\le \sum_{n=1}^{\infty} \sum_{\substack{(u,v)\in\Psi \\ u/v\in X}} n^{-2k}\bigl|s(F(u,v))\bigr|^{-k} h(u/v)^{-j} \\ &= \zeta(2k)\, S_E(j,k,X), \end{aligned}$$

since $k > \frac{1}{2}$. This is (i), and part (ii) follows immediately. □

Corollary 3.2. *If j is a positive real number, then the following are equivalent:*

(a) $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) < 2j$ *for every* $D \in \mathbb{Z} - \{0\}$,
(b) $R_E(j,k,X)$ *converges for some* $k \ge 1$ *and some broad* X,
(c) $R_E(j,k)$ *converges for every* $k \ge 1$.

Proof. This is immediate from Proposition 3.1 and Theorem 2.7. □

4. RELATING $Q_E(j,k)$ AND $R_E(j,k)$

Let $\nu(d)$ denote the number of prime divisors of d. Let

$$\mathcal{S} = \{(\alpha,d,d') : d,d' \in \mathbb{Z}^+, \gcd(d,d') = 1, \alpha \in \Omega_d\}.$$

Lemma 4.1. *Suppose $(u,v) \in \Psi$, $t \in \mathbb{Z}$, and $t^2|F(u,v)$. Then there exists a unique triple $(\alpha,d,d') \in \mathcal{S}$ such that $(u,v) \in \mathcal{L}_{\alpha,d,d'}$ and $dd' = t$.*

Proof. Note that $F(u,v) = v(v^3 f(u/v))$ and $v^3 f(u/v)$ is an integer. Since u and v are relatively prime, so are v and $v^3 f(u/v)$. Let

$$\begin{aligned} d &= \sqrt{\gcd(t^2, v^3 f(u/v))}, \\ d' &= \sqrt{\gcd(t^2, v)}, \\ \alpha &= uv' \pmod{d^2}, \end{aligned}$$

where v' is the inverse of $v \pmod{d^2}$. The proof is now straightforward. □

Proposition 4.2. *If $k > \frac{1}{2}$ and $j \ge 0$, then $Q_E(j,k)$ converges if and only if $R_E(j,k)$ converges.*

Proof. It follows from Lemma 4.1 that

$$\{(u,v) \in \Psi : t^2 \mid F(u,v)\} = \coprod_{\substack{dd'=t \\ \gcd(d,d')=1}} \coprod_{\alpha\in\Omega_d} \Psi \cap \mathcal{L}_{\alpha,d,d'}. \tag{4–1}$$

Hence if $X \subset \mathbb{R}$ we have

$$R_E(j,k,X) = \sum_{\substack{d,d'=1 \\ \gcd(d,d')=1}}^{\infty} (dd')^{2k} \times \sum_{\alpha\in\Omega_d} \sum_{\substack{(u,v)\in\Psi\cap\mathcal{L}_{\alpha,d,d'} \\ u/v\in X}} \bigl|F(u,v)\bigr|^{-k} h(u/v)^{-j}. \tag{4–2}$$

In the remainder of this proof, unless otherwise noted (by a subscript denoting additional dependence on something else), "$\ll$" and "$\gg$" mean up to a multiplicative constant that depends only on F, j, and k.

Suppose $(\alpha,d,d') \in \mathcal{S}$ and $\omega_{\alpha,d,d'} \in \Psi$. Then $\omega_{\alpha,d,d'}$ contributes to one of the terms in (4–2) when $X = \mathbb{R}$. Since F has degree 4, $|F(\omega_{\alpha,d,d'})| \ll \|\omega_{\alpha,d,d'}\|^4$, so $\|\omega_{\alpha,d,d'}\|^{-4k} \ll |F(\omega_{\alpha,d,d'})|^{-k}$. Since the lattice $\mathcal{L}_{\alpha,d,d'}$ has area $(dd')^2$, Minkowski's Theorem implies that $\|\omega_{\alpha,d,d'}\| \ll dd'$, so $\log(dd')^{-j} \ll h(u/v)^{-j}$ where $\omega_{\alpha,d,d'} = (u,v)$. Therefore $Q_E(j,k) \ll R_E(j,k)$, so if $R_E(j,k)$ converges then $Q_E(j,k)$ converges.

Conversely, suppose $Q_E(j,k)$ converges. We will show that for some broad X, $R_E(j,k,X)$ converges. Then by Corollary 3.2, $R_E(j,k)$ converges as well.

Let X be a broad bounded subset of $\mathbb{R}$ such that f is nonzero on the closure of X (for example, we could take $X = (e_{\min} - 2, e_{\min} - 1) \cup (e_{\max} + 1, e_{\max} + 2)$). Then on X, $|f| \gg_X 1$. Therefore if $u/v \in X$, then

$$|F(u,v)| = |v^4 f(u/v)| \gg_X |v|^4 \gg_X |u|^4,$$

the final inequality because X is bounded. It follows that if $u/v \in X$ then

$$|F(u,v)| \gg_X \|(u,v)\|^4. \tag{4–3}$$

If $(u,v) \in \mathcal{L}_{\alpha,d,d'}$ then $(dd')^2$ divides $F(u,v)$; if further $F(u,v) \ne 0$, then

$$(dd')^2 \le |F(u,v)| \ll \max(|u|,|v|)^4. \tag{4–4}$$

Thus $h(u/v) \gg \max(1, \log(dd'))$. By (4–2) and (4–3) we have $R_E(j,k,X) \ll_X R_1 + R_2$, where

$$R_1 = \sum_{\substack{d,d'=1 \\ \gcd(d,d')=1}}^{\infty} \sum_{\substack{\alpha\in\Omega_d \\ \omega_{\alpha,d,d'}\in\Psi}} \frac{(dd')^{2k}}{\max(1,\log dd')^j} \sum_{\substack{\omega\in\mathcal{L}_{\alpha,d,d'} \\ \omega\ne 0}} \|\omega\|^{-4k},$$

and

$$R_2 = \sum_{d,d'=1}^{\infty} \sum_{\substack{\alpha\in\Omega_d \\ \omega_{\alpha,d,d'}\notin\Psi}} \frac{(dd')^{2k}}{\max(1,\log(dd'))^j} \sum_{\omega\in\Psi\cap\mathcal{L}_{\alpha,d,d'}} \|\omega\|^{-4k}.$$

Exactly as in the proof of Proposition 2.4(ii), the theory of Epstein zeta functions shows that there is an absolute constant C such that

$$\sum_{\substack{\omega\in\mathcal{L}_{\alpha,d,d'} \\ \omega\neq 0}} \|\omega\|^{-4k} \leq C\|\omega_{\alpha,d,d'}\|^{-4k}.$$

Therefore $R_1 \leq CQ_E(j,k)$, so R_1 converges.

It remains to show that R_2 converges. (Note that the terms in R_2 have no counterparts in $Q_E(j,k)$.) Fix positive integers d and d' and $\alpha\in\Omega_d$ such that $\omega_{\alpha,d,d'}\notin\Psi$. Let $t = dd'$ and let ω' be a shortest vector in $\mathcal{L}_{\alpha,d,d'} - \mathbb{Z}\omega_{\alpha,d,d'}$. Then $\{\omega_{\alpha,d,d'},\omega'\}$ is a basis of $\mathcal{L}_{\alpha,d,d'}$,

$$\|\omega_{\alpha,d,d'}\|\,\|\omega'\| \gg \operatorname{Area}(\mathcal{L}_{\alpha,d,d'}) = t^2,$$

and

$$\|\omega_{\alpha,d,d'}\| \ll \sqrt{\operatorname{Area}\left(\mathcal{L}_{\alpha,d,d'}\right)} = t. \tag{4–5}$$

One can check that for every $m,n\in\mathbb{Z}$,

$$\|m\omega_{\alpha,d,d'} + n\omega'\|^2 \geq \tfrac{1}{2}\left(m^2\|\omega_{\alpha,d,d'}\|^2 + n^2\|\omega'\|^2\right).$$

Clearly $\Psi\cap\mathcal{L}_{\alpha,d,d'} \subset \mathcal{L}_{\alpha,d,d'} - \mathbb{Z}\omega_{\alpha,d,d'}$, so

$$\begin{aligned}
\sum_{\omega\in\Psi\cap\mathcal{L}_{\alpha,d,d'}} \|\omega\|^{-4k}
&\leq 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty} \|m\omega_{\alpha,d,d'} + n\omega'\|^{-4k} \\
&\ll \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} (m^2\|\omega_{\alpha,d,d'}\|^2 + n^2t^4\|\omega_{\alpha,d,d'}\|^{-2})^{-2k} \\
&\ll t^{-4k},
\end{aligned}$$

where the last inequality follows from (4–5) and a computation of the corresponding integral. Thus

$$\begin{aligned}
R_2 &\ll \sum_{d,d'=1}^{\infty}\sum_{\alpha\in\Omega_d} \frac{(dd')^{-2k}}{\max(1,\log(dd'))^j} \\
&\ll \sum_{d=1}^{\infty} \frac{3^{\nu(d)}}{d^{2k}} \sum_{d'=1}^{\infty} \frac{1}{d'^{2k}},
\end{aligned}$$

since $\#(\Omega_d) \ll 3^{\nu(d)}$. It is easy to see that $3^{\nu(d)} \ll_\varepsilon d^\varepsilon$ for every $\varepsilon > 0$. Therefore these sums converge, if $k > \frac{1}{2}$. This completes the proof. □

Corollary 4.3. *If j is a positive real number, then the following are equivalent:*

(a) $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) < 2j$ *for every* $D\in\mathbb{Z}-\{0\}$,
(b) $Q_E(j,k)$ *converges for some* $k\geq 1$,
(c) $Q_E(j,k)$ *converges for every* $k\geq 1$.

Proof. This is immediate from Proposition 4.2 and Corollary 3.2. □

Theorem 1.1 is now immediate from Theorem 2.7 and Corollaries 3.2 and 4.3.

5. ADDITIONAL REMARKS

Remark 5.1. As in (4–4) and (4–5), each $\omega_{\alpha,d,d'}$ lies in an annulus A_t of inner radius $C_1\sqrt{t}$ and outer radius C_2t, with positive constants C_1 and C_2 depending only on F. If the lattices $\mathcal{L}_{\alpha,d,d'}$ were "random" lattices of area t^2 (with $F(\omega_{\alpha,d,d'})\neq 0$) then one can compute that for large t, the expected value of $\frac{t^{2k}}{\|\omega_{\alpha,d,d'}\|^{4k}}$ in the annulus A_t would be $\frac{1}{C_1^{4k-2}C_2^2(2k-1)t}$. If we replace the corresponding terms of $Q_E(j,k)$ with this expected value, we obtain a "heuristic upper bound" for $Q_E(j,k)$ of

$$O\left(\frac{1}{C_1^{4k}(2k-1)}\sum_{t=1}^{\infty}\frac{1}{t\log^{j-3}(t)}\right). \tag{5–1}$$

Here we have used that the number of $(\alpha,d,d')\in\mathcal{S}$ with $dd'=t$ is $O(4^{\nu(t)})$, and

$$\sum_{1\leq t\leq x} 4^{\nu(t)} = O\left(x\log^3(x)\right).$$

The heuristic upper bound (5–1) correctly captures the fact that the divergence of $Q_E(j,k)$ is independent of k. On the other hand, the heuristic upper bound does not correctly predict the divergence of $Q_E(j,k)$. Note that (5–1) converges if and only if $j>4$. However, it cannot be the case that $Q_E(j,k)$ converges for all E and all $j>4$, by Theorem 1.1 and the existence of elliptic curves over $\mathbb{Q}$ of rank greater than 8.

Remark 5.2. Another way of studying the "randomness" of the lattices $\mathcal{L}_{\alpha,d,d'}$ or their shortest vectors $\omega_{\alpha,d,d'}$ is as follows. For every $(\alpha,d,d')\in\mathcal{S}$, choose a random point $z_{\alpha,d,d'}$ in the annulus $A_{dd'}$. If $B,C\in\mathbb{R}^+$ define

$$\mathcal{S}_{B,C} = \left\{(\alpha,d,d')\in\mathcal{S} : dd' < B,\ \|z_{\alpha,d,d'}\| \leq C\sqrt{dd'}\right\}.$$

It is straightforward to compute that for fixed C and large B,

$$\text{the expected value of } \#\mathcal{S}_{B,C} \text{ is } O(\log^4(B)). \quad (5\text{–}2)$$

Now suppose that E and D are fixed and that $E^{(D)}(\mathbb{Q})$ has rank r. Fix r independent points $P_1, \ldots, P_r$ in $E^{(D)}(\mathbb{Q}) \cap E^{(D)}(\mathbb{R})^0$, and let

$$c = \left(\sum_i \sqrt{\hat{h}_{E^{(D)}}(P_i)} \right)^2.$$

As in the proof of Proposition 4.2, fix a broad bounded subset X of $\mathbb{R}$ such that f is nonzero on the closure of X, and for $B \in \mathbb{R}^+$ define

$$M_B = \left\{ \sum_{i=1}^r n_i P_i : n_i \in \mathbb{Z}, |n_i| < \sqrt{\log(B)/2c} \right\} \cap \{P \in E^{(D)}(\mathbb{Q}) : x(P) \in X\}.$$

Suppose P is a non-zero point in M_B. Then

$$\hat{h}_D(P) \le \log(B)/2. \quad (5\text{–}3)$$

Write $x(P) = u/v$ in lowest terms. By Lemma 2.1, $F(u,v) \neq 0$ and $s(F(u,v)) = D$. By Lemma 4.1, there is a unique triple $(\alpha, d, d') \in \mathcal{S}$ such that $(u,v) \in \mathcal{L}_{\alpha,d,d'}$ and $D(dd')^2 = F(u,v)$. Exactly as in (4–3), we have

$$\|\omega_{\alpha,d,d'}\| \le \|(u,v)\| \ll_X |F(u,v)|^{1/4} = |D|^{1/4}\sqrt{dd'},$$

so

$$\|\omega_{\alpha,d,d'}\| \le C'\sqrt{dd'} \quad (5\text{–}4)$$

for some constant C' (depending only on F and X). Using (4–4), (2–2), (5–3), and Lemma 2.1 we have

$$dd' = \sqrt{F(u,v)/D} \ll \max(|u|,|v|)^2 \ll B. \quad (5\text{–}5)$$

By Lemma 2.3,

$$\#M_B \gg_X \log^{r/2}(B). \quad (5\text{–}6)$$

It is not difficult to check that the fibers of the map from M_B to $\mathcal{S}$ all have order bounded by 6 times the number of divisors of D, and it follows from this, (5–4), (5–5), and (5–6) that

$$\#\{(\alpha,d,d') \in \mathcal{S} : dd' < B, \|\omega_{\alpha,d,d'}\| \le C'\sqrt{dd'}\} \gg_X \log^{r/2}(B). \quad (5\text{–}7)$$

Comparing (5–2) and (5–7) we conclude that if for at least one D we have $\operatorname{rank}_{\mathbb{Z}} E^{(D)}(\mathbb{Q}) > 8$, then the vectors $\omega_{\alpha,d,d'}$ are *not* distributed randomly in the annuli $A_{dd'}$.

Remark 5.3. The sum $Q_E(j,k)$ is very sensitive to the terms where $\omega_{\alpha,d,d'}$ lies close to the inner edge of the annulus A_t.

Remark 5.4. The reason for introducing X in the sums is for the proof of Proposition 4.2 (see (4–3)).

Remark 5.5. By working a little harder in the proofs, one can show that Theorem 1.1 remains true if one replaces $Q_E(j,k)$ by a new sum where the condition $\omega_{\alpha,d,d'} \in \Psi$ in the definition of $Q_E(j,k)$ is replaced by the condition $F(\omega_{\alpha,d,d'}) \neq 0$.

Remark 5.6. Suppose we replace the cubic polynomial $f(x)$ by a polynomial of degree $d \ge 5$ (with distinct complex roots), and replace $F(u,v)$ by $v^m f(u/v)$ where m is even and $m \ge d$. Then the resulting hyperelliptic curve has genus greater than one. Caporaso, Harris, and Mazur [Caporaso et al. 1995] conjectured that the number of rational points on curves of genus greater than one is bounded by a constant depending only on the genus of the curve. The conjecture of Caporaso–Harris–Mazur implies that the corresponding sums $S_E(j,k)$ and $R_E(j,k)$ converge for all $k > 1$ and $j \ge 0$, since, conjecturally, $\#\Sigma_{D,\mathbb{R}}$ is bounded by a constant that is independent of D, where $\Sigma_{D,\mathbb{R}}$ is defined in equation (2–1).

REFERENCES

[Caporaso et al. 1995] L. Caporaso, J. Harris, and B. Mazur, "How many rational points can a curve have?", pp. 13–31 in *The moduli space of curves* (Texel Island, 1994), edited by R. Dijkgraaf et al., Prog. Math. **129**, Birkhäuser, Boston, 1995.

[Gouvêa and Mazur 1991] F. Gouvêa and B. Mazur, "The square-free sieve and the rank of elliptic curves", *J. Amer. Math. Soc.* **4**:1 (1991), 1–23.

[Heath-Brown 1993] D. R. Heath-Brown, "The size of Selmer groups for the congruent number problem", *Invent. Math.* **111**:1 (1993), 171–195.

[Heath-Brown 1994] D. R. Heath-Brown, "The size of Selmer groups for the congruent number problem. II", *Invent. Math.* **118**:2 (1994), 331–370.

[Heegner 1952] K. Heegner, "Diophantische Analysis und Modulfunktionen", *Math. Z.* **56** (1952), 227–253.

[Koksma 1974] J. F. Koksma, *Diophantische Approximationen*, Springer, Berlin, 1974. Reprint.

[Kramarz 1986] G. Kramarz, "All congruent numbers less than 2000", *Math. Ann.* **273**:2 (1986), 337–340.

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186 (1978).

[Mestre 1992] J.-F. Mestre, "Rang de courbes elliptiques d'invariant donné", *C. R. Acad. Sci. Paris Sér. I Math.* **314**:12 (1992), 919–922.

[Mestre 1998] J.-F. Mestre, "Rang de certaines familles de courbes elliptiques d'invariant donné", *C. R. Acad. Sci. Paris Sér. I Math.* **327**:8 (1998), 763–764.

[Rogers 2000] N. Rogers, "Rank computations for the congruent number elliptic curves", *Experiment. Math.* **9**:4 (2000), 591–594.

[Satgé 1987] P. Satgé, "Un analogue du calcul de Heegner", *Invent. Math.* **87**:2 (1987), 425–439.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106, Graduate Texts in Math., Springer, New York, 1986.

[Stewart and Top 1995] C. L. Stewart and J. Top, "On ranks of twists of elliptic curves and power-free values of binary forms", *J. Amer. Math. Soc.* **8**:4 (1995), 943–973.

[Terras 1985] A. Terras, *Harmonic analysis on symmetric spaces and applications, I*, Springer, Berlin, 1985.

[Terras 1988] A. Terras, *Harmonic analysis on symmetric spaces and applications, II*, Springer, Berlin, 1988.

[Zagier and Kramarz 1987] D. Zagier and G. Kramarz, "Numerical investigations related to the L-series of certain elliptic curves", *J. Indian Math. Soc.* (*N.S.*) **52** (1987), 51–69.

Karl Rubin, Department of Mathematics, Stanford University, Stanford, CA 94305, United States (rubin@math.stanford.edu)

Alice Silverberg, Department of Mathematics, Ohio State University, Columbus, OH 43210, United States (silver@math.ohio-state.edu)

Received November 24, 1999; accepted March 6, 2000