Twists of elliptic curves of rank at least four

K. Rubin and A. Silverberg

Abstract

We give infinite families of elliptic curves over $\mathbb{Q}$ such that each curve has infinitely many non-isomorphic quadratic twists of rank at least 4. Assuming the Parity Conjecture, we also give elliptic curves over $\mathbb{Q}$ with infinitely many non-isomorphic quadratic twists of odd rank at least 5.

1 Introduction

Mestre [Me92] showed that every elliptic curve over $\mathbb{Q}$ has infinitely many (non-isomorphic) quadratic twists of rank at least 2 over $\mathbb{Q}$, and he gave [Me98, Me00] several infinite families of elliptic curves over $\mathbb{Q}$ with infinitely many (non-isomorphic) quadratic twists of rank at least 3. Further, he stated ([Me98]) that if E is an elliptic curve over $\mathbb{Q}$ with torsion subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then there are infinitely many (non-isomorphic) quadratic twists of E with rank at least 4 over $\mathbb{Q}$.

In this paper (Theorems 3.2 and 3.6) we give additional infinite families of elliptic curves over $\mathbb{Q}$ with infinitely many (non-isomorphic) quadratic twists of rank at least 4. The family of elliptic curves in Theorem 3.2 is parametrized by the projective line. The family of elliptic curves in Theorem 3.6 is parametrized by an elliptic curve of rank one. In both cases, the twists are parametrized by an elliptic curve of rank at least one.

In addition, we find elliptic curves over $\mathbb{Q}$ that, assuming the Parity Conjecture, have infinitely many (non-isomorphic) quadratic twists of odd rank at least 5 (see Theorem 5.1 and Corollary 5.2). The proof relies on work of Rohrlich [R93].

In Theorem 5.6 of [RS01] we gave an infinite family of elliptic curves over $\mathbb{Q}$ for which the number of twists of even rank at least 4 grows at least like $X^{1/6}$, if the Parity Conjecture holds. In Theorem 3.5 below we give a different infinite family for which this holds.

The results are obtained by extending the method of [RS01] (we learned at [Me00] that this was one of the methods used independently and earlier by Mestre to obtain the results announced in [Me98]).

[1] Supported by NSF grant DMS-0140378.

[2] Supported by NSA grant MDA904-03-1-0033.

Definition 1.1. If $E : y^2 = f(x)$ is an elliptic curve, let $E^{(d)}$ denote $dy^2 = f(x)$, the quadratic twist of E by d.

2 The general method

We first give a more explicit version of Lemma 2.1 of [RS01].

Lemma 2.1. Suppose that E is an elliptic curve over a field F, that $K_1, \ldots, K_n$ are distinct separable extensions of F of degree at most 2, and that for $i = 1, \ldots, n$, there are points $P_i \in E(K_i)$ of infinite order. Suppose also that if $K_i \neq F$, then $\sigma(P_i) = -P_i$, where σ is the non-trivial element of $\mathrm{Gal}(K_i/F)$. Let K denote the compositum $K_1 \cdots K_n$. Then $\{P_1, \ldots, P_n\}$ is an independent set in $E(K)$.

Proof. Let $G = \mathrm{Gal}(K/F)$. Let $\chi_i : \mathrm{Gal}(K_i/F) \to \{\pm 1\}$ denote the non-trivial character if $K_i \neq F$, and the trivial character if $K_i = F$. Let $e_i = \sum_{\sigma \in G} \chi_i(\sigma)\sigma$. Then for all i and j,

$$\begin{aligned} e_i(P_j) = \sum_{\sigma \in G} \chi_i(\sigma)(\sigma(P_j)) &= \sum_{\sigma \in G} \chi_i(\sigma)(\chi_j(\sigma)P_j) \\ &= (\sum_{\sigma \in G} \chi_i(\sigma)\chi_j(\sigma))P_j = \begin{cases} O & \text{if } i \neq j \\ |G|P_j & \text{if } i = j. \end{cases} \end{aligned}$$

Suppose $\sum_j n_j P_j = O$. Then $O = e_i(\sum_j n_j P_j) = |G| n_i P_i$ for every i. Since P_i has infinite order, $n_i = 0$ for every i. □

Definition 2.2. (i) If $k(t) \in \mathbb{Z}[t]$, we say that $k(t)$ is *squarefree* if $k(t)$ is not divisible by the square of any non-constant polynomial in $\mathbb{Z}[t]$.

(ii) Suppose $g(t) \in \mathbb{Q}(t)$. A *squarefree part* of $g(t)$ is a squarefree $k(t) \in \mathbb{Z}[t]$ such that $g(t) = k(t)j(t)^2$ for some $j(t) \in \mathbb{Q}(t)$.

The following result is a variant of Corollary 2.2 of [RS01].

Proposition 2.3. Suppose $f(x) \in \mathbb{Q}[x]$ is a separable cubic, and E is the elliptic curve $y^2 = f(x)$. Let $h_1(t) = t$, suppose we have non-constant $h_2(t), \ldots, h_r(t) \in \mathbb{Q}(t)$, let $k_i(t)$ be a squarefree part of $f(h_i(t))/f(t)$, and suppose that $k_1(t), \ldots, k_r(t)$ are distinct modulo $(\mathbb{Q}^*)^2$. Then:

(i) the rank of $E^{(f(t))}(\mathbb{Q}(t, \sqrt{k_2(t)}, \ldots, \sqrt{k_r(t)}))$ is at least r;

(ii) if C is the curve defined by the equations $s_i^2 = k_i(t)$ for $i = 1, \ldots, r$, then for all but at most finitely many rational points $(\tau, \sigma_1, \ldots, \sigma_r) \in C(\mathbb{Q})$, the rank of $E^{(f(\tau))}(\mathbb{Q})$ is at least r.

Proof. Apply Lemma 2.1 to the elliptic curve $E^{(f(t))}$ over the field $F = \mathbb{Q}(t)$, with $K_i = F(\sqrt{k_i(t)})$ (so $K_1 = F$). Since the polynomials k_i are squarefree and distinct modulo $(\mathbb{Q}^*)^2$, the fields K_i are distinct. For $i = 1, \dots, r$, let

$$P_i = (h_i(t), \sqrt{f(h_i(t))/f(t)}) \in E^{(f(t))}(\mathbb{Q}(t, \sqrt{k_i(t)})).$$

Note that P_i has infinite order, since its x-coordinate is not constant. Now (i) follows. Part (ii) now follows from Theorem C of [S83]. □

Retain the setting of Proposition 2.3. Suppose from now on that each h_i is a linear fractional transformation that permutes the roots of f. Then by Proposition 2.9 of [RS01], $k_i(t)$ is linear. More precisely, $k_1(t) = 1$, and if $h_i(t) = \frac{\alpha t+\beta}{t+\delta}$ with $\alpha, \beta, \delta \in \mathbb{Q}$, then $k_i(t) = f(\alpha)(t+\delta)$ and $f(h_i(t))/f(t) = k_i(t)(t+\delta)^{-4}$.

In [RS01] we considered the case where $r \leq 3$. Suppose $r = 3$. Then

$$\mathbb{Q}(C) = \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}),$$

and the genus of C is zero, where C was defined in Proposition 2.3(ii). Our goal was to choose h_2 and h_3 so that the corresponding curve C has a rational point (and therefore has infinitely many rational points). We considered pairs of the five non-trivial linear fractional transformations that permute the roots of f, until we found h_2 and h_3 for which we could find a rational point on the corresponding curve C. We used this to parametrize the rational points on C, i.e., we found an explicit $u \in \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)})$ so that

$$\mathbb{Q}(C) = \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}) = \mathbb{Q}(u).$$

We then computed t as a function of u, i.e., $t = t(u) \in \mathbb{Q}(u)$. The map $u \mapsto (t(u), \sqrt{k_2(t(u))}, \sqrt{k_3(t(u))})$ defines an isomorphism from $\mathbb{P}^1(\mathbb{Q})$ onto $C(\mathbb{Q})$. By Proposition 2.3(ii), for all but finitely many $u \in \mathbb{Q}$, the rank of $E^{(f(t(u)))}(\mathbb{Q})$ is at least 3.

In this paper, we consider the case $r = 4$. Then the genus of C is one. We will start with a pair h_2, h_3 as above, and, among the remaining three candidates for h_4, look for one for which we can see enough rational points on the corresponding curve C to ensure that C is an elliptic curve of positive rank. We have

$$\mathbb{Q}(C) = \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}, \sqrt{k_4(t)}) = \mathbb{Q}(u, v)$$

with $v^2 = k_4(t(u))$. A rational point on the elliptic curve C corresponds to a pair $u_0, v_0 \in \mathbb{Q}$ such that $v_0^2 = k_4(t(u_0))$. By Proposition 2.3(ii), for all but finitely many such (u_0, v_0), the rank of $E^{(f(t(u_0)))}(\mathbb{Q})$ is at least 4.

3 Rank ≥ 4

From now on we consider elliptic curves of the form

$$y^2 = x(x-1)(x-\lambda)$$

where $\lambda \in \mathbb{Q} - \{0, 1\}$.

Definition 3.1. We fix a numbering of the linear fractional transformations $h_i(t)$ in $\mathbb{Q}(t)$ that permute the set $\{0, 1, \lambda\}$, along with corresponding squarefree parts $k_i(t)$:

$$\begin{array}{ll}
h_1(t) = t, & k_1(t) = 1, \\
h_2(t) = \dfrac{t-\lambda}{(2-\lambda)t-1}, & k_2(t) = (1-\lambda)((\lambda-2)t+1), \\
h_3(t) = \dfrac{\lambda^2(t-1)}{(\lambda^2-\lambda+1)t-\lambda}, & k_3(t) = \lambda(1-\lambda)((\lambda^2-\lambda+1)t-\lambda), \\
h_4(t) = \dfrac{\lambda t}{(\lambda+1)t-\lambda}, & k_4(t) = \lambda((\lambda+1)t-\lambda), \\
h_5(t) = \dfrac{\lambda^2(t-1)}{t(2\lambda-1)-\lambda^2}, & k_5(t) = \lambda(\lambda-1)((1-2\lambda)t+\lambda^2), \\
h_6(t) = \dfrac{\lambda(2-\lambda)}{(\lambda^2-\lambda+1)t-\lambda^2}, & k_6(t) = \lambda((\lambda-1)((\lambda^2-\lambda+1)t-\lambda^2).
\end{array}$$

Theorem 3.2. Suppose $a \in \mathbb{Q} - \{0, 1, -1\}$. Let $\eta = a^2$, let

$$f_\eta(x) = x(x-1)(x - \frac{1-\eta}{\eta+2}),$$

and let E_η be $y^2 = f_\eta(x)$. Let C_η be the curve

$$\begin{aligned}
v^2 = {} & (\eta+1)^2u^4 + 4\eta(2\eta^2+3\eta+1)u^3 + \\
& 2(7\eta^4+7\eta^3+2\eta^2+\eta+1)u^2 + 4(2\eta^5+\eta^4-2\eta^2-\eta)u + (\eta^3-1)^2,
\end{aligned}$$

and let

$$t_\eta(u) = \frac{2(1-\eta)T_\eta(u)}{3((\eta+1)u^2+1-\eta^3)^2}$$

where

$$\begin{aligned}
T_\eta(u) = {} & (\eta+1)^2u^4 + 2\eta(2\eta^2+3\eta+1)u^3 + \\
& 2(3\eta^4+3\eta^3+\eta^2+\eta+1)u^2 + 2\eta(\eta^3-1)(2\eta+1)u + \eta^6 - 2\eta^3 + 1.
\end{aligned}$$

Then:

(i) E_η and C_η are elliptic curves over $\mathbb{Q}$;

(ii) $\mathrm{rank}(C_\eta(\mathbb{Q})) \geq 1$;

(iii) for all but possibly finitely many $(u, v) \in C_\eta(\mathbb{Q})$, the quadratic twist of E_η by $f_\eta \circ t_\eta(u)$ has rank at least 4 over $\mathbb{Q}$;

(iv) there are infinitely many non-isomorphic quadratic twists of E_η of rank at least 4 over $\mathbb{Q}$.

Proof. We proved Theorem 4.2(a) of [RS01] by noticing that when $\tau = \frac{2\lambda}{\lambda+1}$, then

$$k_3(\tau)/k_2(\tau) = \lambda^2 \quad \text{and} \quad k_2(\tau) = \frac{(\lambda-1)^2(-2\lambda+1)}{\lambda+1}.$$

We wanted $k_2(\tau)$ and $k_3(\tau)$ to be squares. Note that $\frac{-2\lambda+1}{\lambda+1} = a^2$ if and only if $\lambda = \frac{1-a^2}{2+a^2}$, and when these hold then $k_2(\frac{2\lambda}{\lambda+1})$ and $k_3(\frac{2\lambda}{\lambda+1})$ are both squares, and $(\frac{2\lambda}{\lambda+1}, (\lambda-1)a, \lambda(\lambda-1)a) \in C_{a^2} = C_\eta$. Further, we found that

$$\mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}) = \mathbb{Q}(u)$$

with $t = t_\eta(u)$ as in the statement of this theorem.

The curve C_η in the statement of this theorem is $v^2 = k_4(t_\eta(u))$. We observed that $(0, \eta^3 - 1) \in C_\eta(\mathbb{Q})$. We have

$$\mathbb{Q}(C_\eta) = \mathbb{Q}(u, \sqrt{k_4(t_\eta(u))}) = \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}, \sqrt{k_4(t)}).$$

By Proposition 2.3(i) (or Corollary 2.2 of [RS01] with $g_i(t) = k_i(t)f_\eta(t)$), the rank of $E_\eta^{(f_\eta \circ t_\eta(u))}(\mathbb{Q}(C_\eta))$ is at least 4. By Proposition 2.3(ii), the rank of $E_\eta^{(f_\eta \circ t_\eta(u))}(\mathbb{Q})$ is at least 4 for all but finitely many $(u, v) \in C_\eta(\mathbb{Q})$. More explicitly, for $i = 1, \ldots, 4$, write

$$f_\eta \circ h_i(t) = f_\eta(t) \cdot k_i(t) \cdot j_i(t)^2$$

with $j_i(t) \in \mathbb{Q}(t)$. Then the points

$$(h_i \circ t_\eta(u), j_i \circ t_\eta(u)\sqrt{k_i \circ t_\eta(u)}) \in E_\eta^{(f_\eta(t_\eta(u)))}(\mathbb{Q}(u, v))$$

are

$$\begin{aligned}
&(t_\eta(u), 1),\\
&(h_1 \circ t_\eta(u), (\frac{-(\eta+1)u^2 + \eta^3 - 1}{a((\eta+1)u^2 + 2(\eta^2-1)u + \eta^3 - 1)})^3),\\
&(h_2 \circ t_\eta(u), (\frac{-(\eta+1)u^2 + \eta^3 - 1}{a((\eta+1)u^2 + 2(\eta^2+\eta+1)u + \eta^3 - 1)})^3),\\
&(h_3 \circ t_\eta(u), (\frac{-(\eta+1)u^2 + \eta^3 - 1}{v})^3).
\end{aligned}$$

They give four independent points in $E_\eta^{(f_\eta \circ t_\eta(u))}(\mathbb{Q}(C_\eta))$, by Lemma 2.1 above. (The fact that the first three are independent in $E_\eta^{(f_\eta \circ t_\eta(u))}(\mathbb{Q}(u))$ was essentially shown in the proof of Theorem 4.2 of [RS01].)

We next write down a (generalized) Weierstrass model for C_η. Let B_η be the elliptic curve $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ where

$$\begin{aligned}\alpha &= -2(\eta^2-1)(\eta^2+\eta+1),\\ \beta &= -2(\eta^2-1)(3\eta^2+\eta-1),\\ \gamma &= -2(\eta^2+\eta+1)(3\eta^2+2\eta+1).\end{aligned}$$

There is a birational isomorphism from C_η to B_η that takes $(0, \eta^3-1) \in C_\eta(\mathbb{Q})$ to the identity element and takes the point

$$P_a := (-(a+1)(\eta+a+1), -(a+1)(\eta+a+1)(\eta+2)(a\eta-2\eta-1))$$

in $C_\eta(\mathbb{Q})$ (with $a^2=\eta$) to

$$Q_a := (2(\eta^3-1), 8a\eta(\eta+2)(\eta^3-1)) \in B_\eta(\mathbb{Q}).$$

We used PARI/GP and Mathematica to check that for $1 \le n \le 10$ and $n = 12$, the denominator of the x-coordinate of nQ_a has no nonzero rational roots. Thus by Mazur's Theorem [Ma77], Q_a has infinite order for every $a \in \mathbb{Q} - \{0, 1, -1\}$, giving (ii). (In fact, $\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2Z \subseteq B_\eta(\mathbb{Q})$, since

$$(2(\eta^2-1)(\eta^2+\eta+1), 8\eta(2\eta+1)(\eta^2-1)(\eta^2+\eta+1))$$

is a point of order four in $B_\eta(\mathbb{Q})$.)

Suppose $\eta \in \mathbb{Q} - \{0, 1\}$ is the square of a rational number. We checked that the degree 12 polynomial $f_\eta \circ t_\eta(u)$ is then always separable, so for each squarefree $d \in \mathbb{Z}$, the hyperelliptic curve $f_\eta \circ t_\eta(u) = dz^2$ has genus 5, and thus has only finitely many rational solutions (u, z). In other words, for each such η and d, the set of $u \in \mathbb{Q}$ such that $f_\eta \circ t_\eta(u)$ and d differ by a rational square is finite. Thus, since $C_\eta(\mathbb{Q})$ is infinite, for each w there are infinitely many non-isomorphic quadratic twists of E_η of rank at least 4 over $\mathbb{Q}$, proving (iv). □

Corollary 3.3. There are infinitely many $j \in \mathbb{Q}$ such that every elliptic curve E over $\mathbb{Q}$ with $j(E) = j$ has infinitely many quadratic twists of rank at least 4 over $\mathbb{Q}$.

Proof. Apply Theorem 3.2(iv) with $j = j(E_\eta^{(f_\eta \circ t_\eta(u))})$. □

Corollary 3.3 also follows from results stated in [Me98].

Remark 3.4. Among the E_η in Theorem 3.2 are infinitely many elliptic curves that are not twists of curves isogenous to elliptic curves with torsion subgroup $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and thus give many new examples not given in [Me98]. For example, if E_η has good reduction at $p = 3$ or 5 or 7 (for example, if $a \in \mathbb{Z}$ and

a is divisible by 3 or 5 or 7), then E_η has no quadratic twist $E_\eta^{(d)}$ isogenous over $\mathbb{Q}$ to an elliptic curve A with torsion subgroup $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, as can be seen as follows. If A has good reduction at p, then the Weil bound gives $\#A(\mathbb{F}_p) \leq 1+p+2\sqrt{p} < 16$, a contradiction (since the 2-torsion injects under reduction modulo primes of good reduction). Therefore A and $E_\eta^{(d)}$ have bad reduction at p, so p ramifies in $K = \mathbb{Q}(\sqrt{d})$. If $\mathcal{P}$ is a prime of K above p, then A has bad reduction at $\mathcal{P}$, since otherwise

$$16 \leq \#A(\mathcal{O}_K/\mathcal{P}) \leq 1 + N(\mathcal{P}) + 2\sqrt{N(\mathcal{P})} = 1 + p + 2\sqrt{p} < 16.$$

Thus $E_\eta^{(d)}$ has bad reduction at $\mathcal{P}$, contradicting the fact that $E_\eta^{(d)}$ is isomorphic over K to E_η which has good reduction at $\mathcal{P}$.

We next show that if we assume the Parity Conjecture, we can obtain a stronger conclusion than that of Theorem 3.2 for a larger class of elliptic curves.

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

$$N_*(X) = \#\{\text{squarefree } d \in \mathbb{Z} : |d| \leq X, \text{ rank}(E^{(d)}(\mathbb{Q})) \text{ is } *\}.$$

In [RS01] we showed that for $y^2 = x(x-1)(x-\frac{1-a^2}{a^2+2})$ with $a \in \mathbb{Q}-\{0,1,-1\}$, we have $N_3(X) \gg X^{1/6}$ (for $X \gg 1$). We also showed, subject to the Parity Conjecture, that for every elliptic curve with all its two-torsion rational and a rational cyclic subgroup of order four, $N_{\geq 4,\text{even}}(X) \gg X^{1/6}$ (for $X \gg 1$).

Theorem 3.5. Let E be $y^2 = x(x-1)(x-\frac{1-a^2}{a^2+2})$ where $a \in \mathbb{Q} - \{0,1,-1\}$ (as in Theorem 3.2). Suppose that the Parity Conjecture holds for all quadratic twists of E. If $|a| > 1$, then $N_{\geq 4,\text{even}}(X) \gg X^{1/6}$ for $X \gg 1$.

Proof. Suppose t_η is the function defined in Theorem 3.2 above (with $\eta = a^2$). In Theorem 4.2(a) of [RS01] we showed that there is a degree 12 polynomial $g(u) \in \mathbb{Q}[u]$ that differs from $f \circ t_\eta(u)$ by a square, is a product of 3 quartics, and satisfies $\text{rank}(E^{(g(u))}(\mathbb{Q}(u)) \geq 3$. One can show that for every $a \in \mathbb{Q}-\{0,1,-1\}$ with $|a| > 1$, $g(u)$ has at least one real root. The result now follows from Corollary 5.2 of [RS01]. □

Theorem 3.6. Let A be the elliptic curve $y^2 = 4x^4 - 2x^2 - 1$. For every $a \in \mathbb{Q}^*$, let

$$f_a(x) = x(x-1)(x+2a^2),$$

and let E_a be the elliptic curve $y^2 = f_a(x)$. Let C_a be the genus one curve $v^2 = (4a^2+1)^2(4a^4-2a^2-1)u^4 + 4a(4a^2+1)(4a^4+2a^2+1)u^3 - 2(16a^8 + 4a^6 + 10a^4 + 3a^2 - 1)u^2 + a(a^2+1)(4a^4+2a^2+1)u + (a^2+1)^2(4a^4-2a^2-1)$, and let

$$t_a(u) = \frac{T_a(u)}{2((4a^2+1)u^2+a^2+1)^2}$$

where $T_a(u) = -(2a^2-1)(4a^2+1)^2u^4 - 4a(4a^2+1)(2a^2+1)u^3 + 2(4a^4+3a^2+1)(2a^2-1)u^2 + 4a(a^2+1)(2a^2+1)u - (a^2+1)^2(2a^2-1)$. Then:

(i) $A(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$;

(ii) if $(a,b) \in A(\mathbb{Q})$, then C_a is an elliptic curve over $\mathbb{Q}$ and
$$\operatorname{rank}(C_a(\mathbb{Q})) \geq 1;$$

(iii) for all but possibly finitely many $(u,v) \in C_a(\mathbb{Q})$, the quadratic twist of E_a by $f_a \circ t_a(u)$ has rank at least 4 over $\mathbb{Q}$;

(iv) if $(a,b) \in A(\mathbb{Q})$, then there are infinitely many non-isomorphic quadratic twists of E_a of rank at least 4 over $\mathbb{Q}$.

Proof. Part (i) is easy. The rest of the proof proceeds in the same way as that of Theorem 3.2, where now we use the functions h_1, h_2, h_5, and h_3 given at the beginning of this section. Since the curve C_a is $v^2 = k_3(t_a(u))$, we have (see also Theorem 4.1 of [RS01])
$$\mathbb{Q}(C_a) = \mathbb{Q}(u, \sqrt{k_3(t_a(u))}) = \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_5(t)}, \sqrt{k_3(t)}).$$
Let B_a be $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ where
$$\begin{aligned} \alpha &= 2(4a^4 - 2a^2 - 1)(4a^2+1)(a^2+1), \\ \beta &= 2(4a^6 + 2a^4 + 5a^2 + 1)(4a^2+1), \\ \gamma &= -2(16a^6 + 4a^4 - 2a^2 + 1)(a^2+1). \end{aligned}$$

It is easy to check that B_a is an elliptic curve whenever $a \in \mathbb{Q}^*$. Suppose that $(a,b) \in A(\mathbb{Q})$. Then there is a birational isomorphism from C_a to B_a that takes the rational point $(0, (a^2+1)b)$ to the identity element and takes the point $(a, (4a^4+2a^2+1)b) \in C_a(\mathbb{Q})$ to the point
$$Q_{(a,b)} := \left(\frac{g(a)(4a^6 - 2a^4 - a^2 - 2)}{a^2}, \frac{-4g(a)(4a^4+2a^2+1)b}{a^3}\right) \in B_a(\mathbb{Q}),$$
where $g(a) = 2(a^2+1)(4a^2+1)$. For $a \notin \{0, 1, -1\}$, we used PARI/GP and Mathematica to check that $nQ_{(a,b)} \neq O$ for $1 \leq n \leq 10$ and $n = 12$. Thus by Mazur's Theorem [Ma77], $\operatorname{rank}(B_a(\mathbb{Q})) \geq 1$. Further, the rank of $B_1(\mathbb{Q})$ $(= B_{-1}(\mathbb{Q}))$ is one. We now have (ii). The points
$$\begin{aligned} &(t_a(u), 1), \\ &(h_2 \circ t_a(u), (\frac{2a((4a^2+1)u^2 + a^2 + 1)}{-(4a^2+1)u^2 + 2a(4a^2+1)u + a^2 + 1})^3), \\ &(h_5 \circ t_a(u), (\frac{(4a^2+1)u^2 + a^2 + 1}{a(4a^2+1)u^2 + 2(a^2+1)u - a(a^2+1)})^3), \\ &(h_3 \circ t_a(u), (\frac{2a((4a^2+1)u^2 + a^2 + 1)}{v})^3) \end{aligned}$$
give four independent points in $E_a^{(f_a \circ t_a(u))}(\mathbb{Q}(C_a))$. □

4 Root numbers

Definition 4.1. If E is an elliptic curve over $\mathbb{Q}$, let N_E denote the conductor of E, let w_E denote the global root number, i.e., the sign in the functional equation for $L(E,s)$, and let $w_{E,p}$ denote the local root number at a prime $p \leq \infty$. Write $w_E(d)$ for $w_{E^{(d)}}$ and write $w_{E,p}(d)$ for $w_{E^{(d)},p}$.

Definition 4.2. If $\alpha \in \mathbb{Q}^*$ and $n \in \mathbb{Z}^+$, then:

(i) $\alpha \equiv 1 \bmod^{\times} n$ means that $\alpha - 1 \in n\mathbb{Z}_\ell$ for all primes $\ell \mid n$;

(ii) $\alpha \equiv 1 \bmod^{\times} n\infty$ means that $\alpha \equiv 1 \bmod^{\times} n$ and $\alpha > 0$.

Lemma 4.3. Suppose E is an elliptic curve over $\mathbb{Q}$, $d, d' \in \mathbb{Q}^*$, and there exists $\beta \in \mathbb{Q}^*$ such that $\beta^2 d/d' \equiv 1 \bmod^{\times} 8N_E\infty$. Then $w_E(d) = w_E(d')$.

Proof. Taking the squarefree parts of d and d', we can reduce to the case where d and d' are squarefree integers.

If $p < \infty$ and $p \nmid dN_E$, then $E^{(d)}$ has good reduction over $\mathbb{Q}_p$, so $w_{E,p}(d) = 1$ (see Proposition 2(iv) of [R93]). Similarly for d'. Thus,

$$w_E(d) = \prod_{p \leq \infty} w_{E,p}(d) = \prod_{p \mid dN_E\infty} w_{E,p}(d). \tag{1}$$

If d/d' is a square in $\mathbb{Q}_p^*$, then $E^{(d)}$ and $E^{(d')}$ are isomorphic over $\mathbb{Q}_p$, so $w_{E,p}(d) = w_{E,p}(d')$ for all $p \leq \infty$. In particular, since $d/d' > 0$, it follows that $w_{E,\infty}(d) = w_{E,\infty}(d')$. If $p \mid 2N_E$, then d/d' is a square in $\mathbb{Q}_p^*$ (since $\beta^2 d/d' \equiv 1 \bmod^{\times} 8N_E$), so $w_{E,p}(d) = w_{E,p}(d')$. If $p \mid 2N_E$, then p divides d if and only if p divides d' (since $2\mathrm{ord}_p(\beta) + \mathrm{ord}_p(d) = \mathrm{ord}_p(d')$, and d and d' are squarefree). Thus,

$$\frac{\prod_{p \mid dN_E\infty} w_{E,p}(d)}{\prod_{p \mid dN_E\infty} w_{E,p}(d')} = \frac{\prod_{p \mid d, p \nmid 2N_E} w_{E,p}(d)}{\prod_{p \mid d', p \nmid 2N_E} w_{E,p}(d')}. \tag{2}$$

Suppose $p \nmid N_E$, so E has good reduction at p. Since E and $E^{(d)}$ are isomorphic over $\mathbb{Q}_p(\sqrt{d})$, $E^{(d)}$ has good reduction over $\mathbb{Q}_p(\sqrt{d})$. If $p \mid d$, then $\mathbb{Q}_p(\sqrt{d})$ is the smallest extension of $\mathbb{Q}_p$ over which $E^{(d)}$ has good reduction (and similarly for d'). By (iii) and (v) of Proposition 2 of [R93] with $e = 2$, we have

$$w_{E,p}(d) = \left(\frac{-1}{p}\right) \tag{3}$$

if $p \mid d$ and $p \nmid 2N_E$, where $\left(\frac{-1}{m}\right)$ is the Jacobi symbol.

By (1), (2), and (3), we have

$$\frac{w_E(d)}{w_E(d')} = \frac{\prod_{p \mid d, p \nmid 2N_E} \left(\frac{-1}{p}\right)}{\prod_{p \mid d', p \nmid 2N_E} \left(\frac{-1}{p}\right)} = \frac{\left(\frac{-1}{f}\right)}{\left(\frac{-1}{f'}\right)},$$

where $f = d/\gcd(d, 2N_E)$ and $f' = d'/\gcd(d', 2N_E)$. Note that $f/f' = d/d'$. Then $\beta^2 f/f' \equiv 1 \bmod^{\times} 4$, so $f \equiv f' \pmod 4$, so $\left(\frac{-1}{f}\right) = \left(\frac{-1}{f'}\right)$. □

Lemma 4.4. Suppose E and B are elliptic curves over $\mathbb{Q}$, $B(\mathbb{Q})$ has infinite order, $P \in B(\mathbb{Q})$, r is a rational function in $\mathbb{Q}(B)$, and P is not a zero or pole of r. Then there exist a $Q \in B(\mathbb{Q})$ of infinite order and an open neighborhood U of O in $B(\mathbb{R})$ such that if $k \in \mathbb{Z}$ and $kQ \in U$ then $w_E(r(P+kQ)) = w_E(r(P))$.

Proof. Let

$$V = B(\mathbb{R}) \times \prod_{p \mid 2N_E} B(\mathbb{Q}_p)$$

and let $g(z) = r(P+z)/r(P) \in \mathbb{Q}(B)$. Then $g(O) = 1$, and g induces a function

$$g : V - \{\text{poles of } g\} \to \mathbb{R} \times \prod_{p \mid 2N_E} \mathbb{Q}_p,$$

which is continuous at O. Let $B_n(\mathbb{Q}_p)$ denote the subset of $B(\mathbb{Q}_p)$ of points that, in a minimal Weierstrass model for B, have

$$\mathrm{ord}_p(x\text{-coordinate}) \leq -2n$$

(see Exercise 7.4 on p. 187 of [S86]). Then the $B_n(\mathbb{Q}_p)$'s form a basis for the open sets around O in $B(\mathbb{Q}_p)$, and are subgroups of finite index in $B(\mathbb{Q}_p)$. Since g is continuous at O, there is an open neighborhood U of O in $B(\mathbb{R})$ and for every $p \mid 2N_E$ there is an $n_p \in \mathbb{Z}^{\geq 0}$ such that

$$g\big(U \times \prod_{p \mid 2N_E} B_{n_p}(\mathbb{Q}_p)\big) \subseteq \mathbb{R}^+ \times \prod_{p \mid 2N_E} (1 + 8N_E\mathbb{Z}_p).$$

Let $k_p = [B(\mathbb{Q}_p) : B_{n_p}(\mathbb{Q}_p)]$ and let $Q_0 \in B(\mathbb{Q})$ be a point of infinite order. Let $Q = (\mathrm{lcm}_{p \mid 2N_E}\{k_p\})Q_0 \in B(\mathbb{Q})$. Then Q has infinite order, and $Q \in B_{n_p}(\mathbb{Q}_p)$ for all $p \mid 2N_E$. Now apply Lemma 4.3 with $d = r(P+kQ)$, $d' = r(P)$, and $\beta = 1$. □

Lemma 4.5. Suppose B is an elliptic curve over $\mathbb{Q}$, $Q \in B(\mathbb{Q})$ is a point of infinite order, and U is an open subset of the identity component $B(\mathbb{R})^0$ of $B(\mathbb{R})$. Then $\{k \in \mathbb{Z} : kQ \in U\}$ is infinite.

Proof. Replacing Q by $2Q$, we may assume that $Q \in B(\mathbb{R})^0$. Note that $B(\mathbb{R})^0$ is isomorphic to the unit circle in $\mathbb{C}^*$, so every infinite subgroup is dense. Thus $\{kQ : k \in \mathbb{Z}\}$ is dense in $B(\mathbb{R})^0$, and the lemma follows. □

5 Rank ≥ 5

Theorem 5.1. Suppose $a \in \mathbb{Q} - \{0, 1, -1\}$ and $\eta = a^2$. Suppose E_η, f_η, and t_η are as in Theorem 3.2. If $w_{E_\eta}(f_\eta \circ t_\eta(u_1)) = -1$ for some $(u_1, v_1) \in B_\eta(\mathbb{Q})$, and the Parity Conjecture holds for all quadratic twists of E_η, then E_η has infinitely many non-isomorphic quadratic twists of odd rank ≥ 5 over $\mathbb{Q}$.

Proof. Let $P = (u_1, v_1)$, and let $r(z) = f_\eta \circ t_\eta \circ x(z) \in \mathbb{Q}(B_\eta)$, where the function x gives the x-coordinate of a point. By Lemmas 4.4 and 4.5 with $E = E_\eta$ and $B = B_\eta$, there are $Q \in B_\eta(\mathbb{Q})$ and infinitely many $k \in \mathbb{Z}$ such that

$$w_{E_\eta}(r(P + kQ)) = w_{E_\eta}(r(P)) = -1,$$

so by the Parity Conjecture, $E_\eta^{(r(P+kQ))}(\mathbb{Q})$ has odd rank.

By Theorem 3.2(iii), for all but finitely many $k \in \mathbb{Z}$, the rank of $E_\eta^{(r(P+kQ))}(\mathbb{Q})$ is at least 4. Thus for infinitely many k, the rank of $E_\eta^{(r(P+kQ))}(\mathbb{Q})$ is at least 5. As argued in the proof of Theorem 3.2, for each squarefree $d \in \mathbb{Q}^*$, the set of $u \in \mathbb{Q}$ such that $f_\eta \circ t_\eta(u)$ and d differ by a rational square is finite, since the hyperelliptic curve $f_\eta \circ t_\eta(u) = dz^2$ has only finitely many rational solutions (u, z). Thus there are infinitely many non-isomorphic quadratic twists of E_η of odd rank at least 5 over $\mathbb{Q}$. □

Corollary 5.2. Suppose

$$a \in \{2, 5, 6, 7, 8, 12, 13, 14, 15, 16, 17, 18, 21, 22, \\ 23, 24, 25, 26, 28, 30, 32, 33, 35, 36, 37, 39, 40, 41\}.$$

If the Parity Conjecture holds for all quadratic twists of

$$E_{a^2} : y^2 = x(x-1)(x - \frac{1-a^2}{a^2+2}),$$

then E_{a^2} has infinitely many non-isomorphic quadratic twists of odd rank ≥ 5 over $\mathbb{Q}$.

Proof. With $\eta = a^2$ and $P_a = (u_0, v_0) \in C_\eta(\mathbb{Q})$ as in the proof of Theorem 3.2, and $P'_\eta = (u_1, v_1) = (1 - \eta, (1 - \eta)(2 + \eta)) \in C_\eta(\mathbb{Q})$, one can check that for each of the above a's, at least one of $w_{E_\eta}(f_\eta \circ t_\eta(u_0))$ and $w_{E_\eta}(f_\eta \circ t_\eta(u_1))$ is -1. The result now follows from Theorem 5.1. □

References

[Ma77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[Me92] J-F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **314** (1992), 919–922.

[Me98] J-F. Mestre, *Rang de certaines familles de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **327** (1998), 763–764.

[Me00] J-F. Mestre, *Ranks of twists of elliptic curves*, lecture at MSRI, September 11, 2000.

[R93] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. **87** (1993), 119–151.

[RS01] K. Rubin, A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Exper. Math. **10** (2001), 559–569.

[S83] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.

[S86] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[ST95] C. L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

Department of Mathematics,
University of California at Irvine,
Irvine, CA 92697, USA