J. Aust. Math. Soc. **98** (2015), 281–288
doi:10.1017/S1446788714000512

ON POSITIVE PROPORTION OF RANK-ZERO TWISTS OF ELLIPTIC CURVES OVER $\mathbb{Q}$

MAOSHENG XIONG

(Received 21 November 2013; accepted 21 September 2014; first published online 7 November 2014)

Communicated by I. E. Shparlinski

Abstract

Extending the idea of Dabrowski ['On the proportion of rank 0 twists of elliptic curves', *C. R. Acad. Sci. Paris, Ser. I* **346** (2008), 483–486] and using the 2-descent method, we provide three general families of elliptic curves over $\mathbb{Q}$ such that a positive proportion of prime-twists of such elliptic curves have rank zero simultaneously.

2010 *Mathematics subject classification*: primary 11G05; secondary 14H52.

Keywords and phrases: elliptic curves, 2-descent, Selmer group, rank.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ $(a, b, c \in \mathbb{Z})$. For any square-free integer d, the dth quadratic twist E_d of E is the elliptic curve given by the equation $y^2 = x^3 + a\,dx^2 + b\,d^2x + c\,d^3$. Denote by r_{E_d} the rank of the Mordell–Weil group $E_d(\mathbb{Q})$.

Statistics of rank-zero quadratic twists of elliptic curves have been an interesting subject of study for some time. It is known from the work of Waldspurger [19] (combined with the work of Kolyvagin [15], and of Wiles and others [2]) that $r_{E_d} = 0$ for infinitely many square-free ds. Hoffstein and Luo [10] proved that, for any fixed E, there exist infinitely many odd square-free d with no more than three prime factors such that $r_{E_d} = 0$. Ono and Skinner [16] proved that, for any fixed E, $|\{|d| \le X : r_{E_d} = 0\}| \gg X/\log X$. On the other hand, it is believed [9] that a positive proportion of twists E_d have rank zero, and this was proved by Iwaniec and Sarnak [12] under the Riemann hypothesis. Unconditionally, such positive proportion results are only known for a few specific curves [13, 14, 18, 20]. Ono and Skinner [16] proved that, when E has conductor less than or equal to 100, E_p or E_{-p} has rank zero for a positive proportion of primes p.

The author was supported by the Research Grants Council of Hong Kong under Project Nos. RGC606211 and RGC609513.

In an interesting and beautiful paper [4] Dabrowski proved the following result.

THEOREM 1.1. *For any positive integer k there are pairwise nonisogenous elliptic curves $E^1, \dots, E^k$ such that $r_{E^1_p} = \cdots = r_{E^k_p} = 0$ for a positive proportion of primes p.*

The ingenious idea of the proof of Theorem 1.1 [4] is based on the 2-descent method applied to the explicit family of elliptic curves $E^{A,-B} : y^2 = x(x + A)(x - B)$ where A is a prime, and B is a prime or a product of two primes such that $A + B = 2^{2m}$ for some positive integer m. Chen's theorem [3] is required here to show that there are infinitely many such elliptic curves $E^{A,-B}$. As was remarked by Dabrowski [4], Theorem 1 can be also be proved by using the 2-descent method on the Setzer–Neumann curves, and the existence of infinitely many such elliptic curves was guaranteed by a result of Iwaniec [11]. Previously Dabrowski and Wieczorek [5] proved Theorem 1.1 by using the 2-descent method on the specific elliptic curves $y^2 = x(x - 2^m)(x + q - 2^m)$ and by assuming the twin prime conjecture.

The purpose of this paper is to show that there is an abundance of elliptic curves which could be used to prove Theorem 1.1. Define

$$E^{A,B} : y^2 = x(x + A)(x + B). \tag{1.1}$$

Let $(\frac{\cdot}{\cdot})$ denote the Legendre symbol. We first prove the following theorem.

THEOREM 1.2. *Let $|A|, |B|$ be primes such that*

(1) $A \equiv 1 \bmod 8, B \equiv 3 \bmod 8$,
(2) $A + B \geq 0$ *or* $AB < 0$.

Let r be any prime number coprime to $AB(A - B)$ and satisfying the following three conditions:

(i) $r \equiv 7 \bmod 8$;
(ii) $(A/r) = (B/r) = -1$;
(iii) *for any odd prime $p|(A - B)$, we have $(-Br/p) = -1$.*

Then $r_{E^{A,B}_r} = 0$.

Now Theorem 1.1 can be proved easily: take distinct primes $p_1, \dots, p_r$ and q with $p_i \equiv 1 \bmod 8$ for all i and $q \equiv 5 \bmod 8$, and consider the r-twist of elliptic curves $E^{p_i,q}$. Let r be a prime number coprime to $p_i q(p_i - q)$ for all i and satisfying:

(i) $r \equiv 7 \bmod 8$;
(ii) $(q/r) = -1$ and $(p_i/r) = -1$ for all i;
(iii) for any odd prime $p|\prod_i (p_i - q)$, we have $(-qr/p) = -1$.

Then $r_{E^{p_i,q}_r} = 0$ for all i. The Chinese remainder theorem and Dirichlet's theorem on primes in arithmetic progressions clearly show a positive proportion of primes r satisfying the above conditions.

The proof of Theorem 1.2 is also based on the 2-descent method. Consider the 2-isogeny $\phi : E^{A,B}_r \to \widehat{E}^{A,B}_r : Y^2 = X^3 - 2(A + B)rX^2 + (A - B)^2 r^2 X$, defined by $\phi((x, y)) =$

https://doi.org/10.1017/S1446788714000512 Published online by Cambridge University Press

$(y^2/x^2, -y(x^2 - ABr^2)/x^2)$, and let $\widehat{\phi}$ denote the dual isogeny. Under the assumptions of Theorem 1.2, we actually prove that the Selmer groups satisfy $\mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}) \simeq \{0\}$ and $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Then Theorem 1.2 follows from the fundamental formula [17, page 314]

$$r_{E_r^{A,B}} = \dim_2 \mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}) + \dim_2 \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) - \dim_2 Ш(E_r^{A,B}/\mathbb{Q})[\phi] - \dim_2 Ш(\widehat{E}_r^{A,B}/\mathbb{Q})[\widehat{\phi}] - 2.$$

Theorem 1.2 is about rank-zero r-twists of $E^{A,B}$ for $|A|$ and $|B|$ being primes. If A, B are some integers in general, it is still possible to find rank-zero r-twists of $E^{A,B}$, given the elementary nature of the 2-descent method, however, the conditions on such rs are too complicated to write down. On the other hand, we prove the following result.

THEOREM 1.3. *Let A, B be integers such that $A \equiv 1 \bmod 8$, $B \equiv 3 \bmod 8$, and for $E^{A,B}$, we assume that*

$$\mathrm{Sel}^{(\phi)}(E^{A,B}/\mathbb{Q}) \simeq \{0\}, \quad \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}^{A,B}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2. \tag{1.2}$$

Then for any prime number r coprime to $AB(A - B)$ such that:

(i) $r \equiv 7 \bmod 8$; *and*
(ii) $(r/p) = 1$ *for any odd prime* $p|AB(A - B)$,

we have $r_{E_r^{A,B}} = 0$.

We remark that condition (1.2) is natural and easy to check for $E^{A,B}$. It also implies that $r_{E^{A,B}} = 0$. Many families of rank-zero elliptic curves have been found by this way (see, for example, [4–6, 8]). Moreover, via infinitely many elliptic curves $E^{A,B}$ satisfying condition (1.2), Theorem 1.1 can be proved easily.

The elliptic curve $E^{A,B}$ given in (1.1) can be characterized as having full 2-torsion points over $\mathbb{Q}$, that is, $E^{A,B}(\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Now we consider elliptic curves with one nontrivial 2-torsion point over $\mathbb{Q}$, that is, elliptic curves $E^{a,b}$ $(a, b \in \mathbb{Z})$ given by the equation

$$E^{a,b} : y^2 = x(x^2 + ax + b). \tag{1.3}$$

Consider the 2-isogeny $\phi : E_r^{a,b} \to \widehat{E}_r^{a,b} : Y^2 = X^3 - 2arX^2 + (a^2 - 4b)r^2X$, defined by $\phi((x, y)) = (y^2/x^2, -y(x^2 - br^2)/x^2)$, and let $\widehat{\phi}$ denote the dual isogeny. We also have the fundamental formula [17, page 314]

$$r_{E_r^{a,b}} = \dim_2 \mathrm{Sel}^{(\phi)}(E_r^{a,b}/\mathbb{Q}) + \dim_2 \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{a,b}/\mathbb{Q}) - \dim_2 Ш(E_r^{a,b}/\mathbb{Q})[\phi] - \dim_2 Ш(\widehat{E}_r^{a,b}/\mathbb{Q})[\widehat{\phi}] - 2.$$

We assume that neither $a^2 - 4b$ nor b is a perfect square, because otherwise either $E^{a,b}$ or $\widehat{E}^{a,b}$ would have full 2-torsion points over $\mathbb{Q}$, hence reducing to elliptic curves we have considered before. We prove the following theorem.

https://doi.org/10.1017/S1446788714000512 Published online by Cambridge University Press

THEOREM 1.4. *Let $a, b \in \mathbb{Z}$ such that neither $a^2 - 4b$ nor b is a perfect square. For $E^{a,b}$ given in (1.3), we assume that*

$$\mathrm{Sel}^{(\phi)}(E^{a,b}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}^{a,b}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}. \tag{1.4}$$

Then for any prime number r coprime to $b(a^2 - 4b)$ such that:

(i) $r \equiv 7 \bmod 8$;

(ii) $(r/p) = 1$ *for any odd prime* $p | b(a^2 - 4b)$;

(iii) *either*

$$\left(\frac{b}{r}\right) = \left(\frac{a^2 - 4b}{r}\right) = -1 \tag{1.5}$$

or

$$\left(\frac{b}{r}\right) = \left(\frac{a^2 - 4b}{r}\right) = -\left(\frac{a + \sqrt{b}}{r}\right) = -\left(\frac{a + \sqrt{a^2 - 4b}}{r}\right) = 1,$$

we have $r_{E_r^{a,b}} = 0$.

We remark that if $a = 2a', b = 2b'$ and $a' \equiv b' \equiv 3 \bmod 4$, then condition (1.5) is satisfied. On the other hand, condition (1.4) is natural and easy to check for $E^{a,b}$ as well, and many rank-zero elliptic curves have been found in this way [7]. Theorem 1.1 can also be proved via infinitely many elliptic curves $E^{a,b}$ satisfying the conditions of Theorem 1.4.

The main ingredient of the proofs of Theorems 1.2–1.4 is the 2-descent method applied to the elliptic curves considered above. We prove Theorems 1.2 and 1.3 in Section 2, and prove Theorem 1.4 in Section 3.

2. Proof of Theorems 1.2 and 1.3

The 2-descent method is explained in the last chapter of Silverman's book [17] (see also [1, 4]). For clarity we specify the 2-descent method for elliptic curves $E^{A,B}$ given by (1.1) below.

2.1. 2-descent and $E^{A,B}$. For any integer M, let $\Sigma(M)$ be the set of prime numbers dividing M, and let $\triangle(M)$ be set of (positive or negative) square-free divisors of M. Let

$$C_d^{(r)} : dw^2 = t^4 - 2(A + B)\frac{r}{d}t^2z^2 + (A - B)^2\frac{r^2}{d^2}z^4,$$
$$C_d'^{(r)} : dw^2 = t^4 + (A + B)\frac{r}{d}t^2z^2 + AB\frac{r^2}{d^2}z^4$$

be the principal homogeneous spaces under the actions of the elliptic curves $E_r^{A,B}$ and $\widehat{E}_r^{A,B}$ previously defined. Using [17, Proposition 4.9, page 302], we have the following identifications:

$$\mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}) \simeq \{d \in \triangle((A - B)r) : C_d^{(r)}(\mathbb{Q}_v) \neq \emptyset \ \forall v \in \Sigma(2AB(A - B)r) \cup \{\infty\}\},$$
$$\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) \simeq \{d \in \triangle(ABr) : C_d'^{(r)}(\mathbb{Q}_v) \neq \emptyset \ \forall v \in \Sigma(2AB(A - B)r) \cup \{\infty\}\},$$

https://doi.org/10.1017/S1446788714000512 Published online by Cambridge University Press

where $C_d^{(r)}(\mathbb{Q}_v) \neq \emptyset$ (or $C_d'^{(r)}(\mathbb{Q}_v) \neq \emptyset$) means that $C_d^{(r)}$ (or $C_d'^{(r)}$) has nontrivial solutions $(w,t,z) \neq (0,0,0)$ in $\mathbb{Q}_v$. We know that

$$\{1\} \subseteq \mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}), \quad \{1, AB, -Ar, -Br\} \subseteq \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}),$$

since each of the corresponding homogeneous spaces has nontrivial solutions in $\mathbb{Q}$.

Proof of Theorem 1.2. Let $|A|, |B|$ and r be primes under the conditions of Theorem 1.2. We first prove that $\mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}) = \{1\}$. For any $d \in \triangle((A-B)r)$, if $d < 0$, since $A + B \geq 0$ or $AB < 0$, clearly $C_d^{(r)}(\mathbb{R}) = \emptyset$. If $2|d$, let $(w,t,z) \neq (0,0,0)$ be a solution of $C_d^{(r)}$ in $\mathbb{Q}_2$. Since $A \equiv 1 \bmod 8$, $B \equiv 5 \bmod 8$, considering $C_d^{(r)}$, at least two numbers in the set $\{1 + 2v_2(w), 4v_2(t), 1 + 2v_2(t) + 2v_2(z), 2 + 4v_2(z)\}$ reach the same minimal value, where for any prime p we denote by v_p the standard p-adic exponential valuation. Clearly these two numbers must be $1 + 2v_2(w)$ and $1 + 2v_2(t) + 2v_2(z)$, which is impossible. Now we need to consider $d > 1$ such that there is an odd prime $p|(A-B)$ with $p|d$. Let $(w,t,z) \neq (0,0,0)$ be a solution of $C_d^{(r)}$ in $\mathbb{Q}_p$. Then at least two numbers in the set $\{1 + 2v_p(w), 4v_p(t), -1 + 2v_p(t) + 2v_p(z), 2v_p(A-B) - 2 + 4v_p(z)\}$ reach the same minimal value. These two numbers must be $1 + 2v_p(w)$ and $-1 + 2v_p(t) + 2v_p(z)$. Hence the equation

$$\frac{d}{p}w^2 \equiv -2(A+B)\frac{r}{d/p}t^2z^2 \mod p$$

must be solvable in $\mathbb{Z}_p^* := \mathbb{Z}_p - p\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the set of p-adic integers. By Hensel's lemma, this implies that

$$1 = \left(\frac{-2(A+B)r}{p}\right) = \left(\frac{-2(A-B+2B)r}{p}\right) = \left(\frac{-rB}{p}\right),$$

which contradicts condition (iii) of Theorem 1.2.

Finally, if $d = r$, let $(w,t,z) \neq (0,0,0)$ be a solution of $C_d^{(r)}$ in $\mathbb{Q}_r$. Then at least two numbers in the set $\{1 + 2v_r(w), 4v_r(t), 2v_r(t) + 2v_r(z), 4v_r(z)\}$ reach the same minimal value. We may assume that $v_r(t) = v_r(z) = 0$ and $v_r(w) \geq 0$, hence

$$t^4 - 2(A+B)t^2z^2 + (A-B)^2z^4 \equiv 0 \mod r$$

is solvable in $\mathbb{Z}_r{}^*$. That is,

$$(t^2 - (A+B)z^2)^2 \equiv 4ABz^4 \mod r.$$

Since $(AB/r) = 1$,

$$t^2 - (A + B - 2\sqrt{AB})z^2 \equiv 0 \mod r$$

or

$$t^2 - (A + B + 2\sqrt{AB})z^2 \equiv 0 \mod r.$$

This is not possible by Hensel's lemma and by conditions (i) and (ii) of Theorem 1.2, since

$$\left(\frac{A + B \pm 2\sqrt{AB}r}{r}\right) = \left(\frac{-1}{r}\right)\left(\frac{(\sqrt{-A} \pm \sqrt{-B})^2}{r}\right) = -1.$$

This shows that $\mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}) = \{1\}$.

https://doi.org/10.1017/S1446788714000512 Published online by Cambridge University Press

Next we prove that $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) = \{1, AB, -Ar, -Br\}$. For $d \in \triangle(ABr)$, for $d = -1$,

$$C_{-1}^{\prime(r)} : -w^2 = t^4 - (A+B)rt^2z^2 + ABr^2z^4.$$

Since $(-1/r) = -1$ and $(-AB/r) = -1$, by Hensel's lemma, we find that $C_{-1}^{\prime(r)}(\mathbb{Q}_r) = \emptyset$. For $d = A$,

$$C_A^{\prime(r)} : Aw^2 = t^4 + (A+B)\frac{r}{A}t^2z^2 + \frac{Br^2}{A}z^4.$$

Since $(A/r) = (B/r) = -1$, by Hensel's lemma, we find that $C_A^{\prime(r)}(\mathbb{Q}_r) = \emptyset$. For $d = r$,

$$C_r^{\prime(r)} : rw^2 = t^4 + (A+B)t^2z^2 + ABz^4.$$

Solving this in $\mathbb{Q}_2$, at least two numbers in the set $\{2v_2(w), 4v_2(t), 1 + 2v_2(t) + 2v_2(z), 4v_2(z)\}$ reach the same minimal value, which may be assumed to be zero. This implies that at least one of the equations

$$rw^2 \equiv t^4 \mod 8,$$

$$rw^2 \equiv ABz^4 \mod 8,$$

$$rw^2 \equiv t^4 + (A+B)t^2z^2 + ABz^4 = (t^2 + Az^2)(t^2 + Bz^2) \mod 8$$

is solvable in $\mathbb{Z}_2^*$. This is impossible by conditions (1) and (i) of Theorem 1.2. Since $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) \subset \triangle(ABr)$ is a group, we conclude that $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) = \{1, AB, -Ar, -Br\}$. This shows $r_{E_r^{A,B}} = 0$, completing the proof of Theorem 1.2. □

Proof of Theorem 1.3. For any $d' \in \triangle(A-B)$, let $d = d'$ or $d = d'r$. If $d \in \mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q})$, then $C_d^{(r)}(\mathbb{Q}_v) \neq \emptyset$ for any $v \in \Sigma(2AB(A-B)) \cup \{\infty\}$. Since, by (i) and (ii) of Theorem 1.3, r is a square in any such $\mathbb{Q}_v$, we find $d' \in \mathrm{Sel}^{\phi}(E^{A,B}/\mathbb{Q})$. Hence $d' = 1$ from condition (2) of Theorem 1.3. For $d = r$, since $AB \equiv 3 \bmod 4$ and by (ii) of Theorem 1.3,

$$\left(\frac{AB}{r}\right) = -1.$$

From the proof of Theorem 1.2, we find $C_r^{(r)}(\mathbb{Q}_r) = \emptyset$. Hence $\mathrm{Sel}^{(\phi)}(E_r^{A,B}/\mathbb{Q}) = \{1\}$.

For any $d' \in \triangle(AB)$, let $d = d'$ or $d = d'r$. If $d \in \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q})$, since r is a square in $\mathbb{Q}_v$ for any $v \in \triangle(2AB(A-B))$, by condition (2) of Theorem 1.3 we find $d' \in \{1, AB, -A, -B\}$. Hence $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) \subseteq \{1, AB, -A, -B, r, ABr, -Ar, -Br\}$.

For $d = r$, from the proof of Theorem 1.2, we find $C_r^{\prime(r)}(\mathbb{Q}_2) = \emptyset$. Using the fact that $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q})$ is a group, we conclude that $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{A,B}/\mathbb{Q}) = \{1, AB, -Ar, -Br\}$. This shows that $r_{E_r^{A,B}} = 0$, which completes the proof of Theorem 1.3. □

3. Proof of Theorem 1.4

For clarity we specify the 2-descent method for elliptic curves $E^{a,b}$ given by (1.3) below (see [1, 17]).

https://doi.org/10.1017/S1446788714000512 Published online by Cambridge University Press

3.1. 2-descent and $E^{a,b}$. Let

$$C_d^{(r)} : dw^2 = t^4 - 2a\frac{r}{d}t^2z^2 + (a^2 - 4b)\frac{r^2}{d^2}z^4,$$
$$C_d'^{(r)} : dw^2 = t^4 + \frac{ar}{d}t^2z^2 + b\frac{r^2}{d^2}z^4$$

be the principal homogeneous spaces under the actions of the elliptic curves $E_r^{a,b}$ and $\widehat{E}_r^{a,b}$ previously defined. Using [17, Proposition 4.9, page 302], we have the following identifications:

$$\mathrm{Sel}^{(\phi)}(E_r^{a,b}/\mathbb{Q}) \simeq \{d \in \triangle((a^2 - 4b)r) : C_d^{(r)}(\mathbb{Q}_v) \neq \emptyset\ \forall v \in \Sigma(2b(a^2 - 4b)r) \cup \{\infty\}\},$$
$$\mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{a,b}/\mathbb{Q}) \simeq \{d \in \triangle(br) : C_d'^{(r)}(\mathbb{Q}_v) \neq \emptyset\ \forall v \in \Sigma(2b(a^2 - 4b)r) \cup \{\infty\}\},$$

where $C_d^{(r)}(\mathbb{Q}_v) \neq \emptyset$ (or $C_d'^{(r)}(\mathbb{Q}_v) \neq \emptyset$) means that $C_d^{(r)}$ (or $C_d'^{(r)}$) has nontrivial solutions $(w, t, z) \neq (0, 0, 0)$ in $\mathbb{Q}_v$. We know that

$$\{1, a^2 - 4b\} \subseteq \mathrm{Sel}^{(\phi)}(E_r^{a,b}/\mathbb{Q}), \quad \{1, b\} \subseteq \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{a,b}/\mathbb{Q}),$$

since each of the corresponding homogeneous spaces has nontrivial solutions in $\mathbb{Q}$.

Proof of Theorem 1.4. Similar to the proof of Theorem 1.3, since r is a square in $\mathbb{Q}_v$ for any $v \in \triangle(2b(a^2 - 4b))$, by condition (4) of Theorem 1.4,

$$\mathrm{Sel}^{(\phi)}(E_r^{a,b}/\mathbb{Q}) \subseteq \{1, a^2 - 4b, r, (a^2 - 4b)r\}, \quad \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{a,b}/\mathbb{Q}) \subseteq \{1, b, r, br\}.$$

It suffices to prove that

$$r \notin \mathrm{Sel}^{(\phi)}(E_r^{a,b}/\mathbb{Q}), \quad r \notin \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}_r^{a,b}/\mathbb{Q}).$$

For

$$C_r^{(r)} : rw^2 = t^4 - 2at^2z^2 + (a^2 - 4b)z^4,$$

let $(w, t, z) \neq (0, 0, 0)$ be a solution of $C_r^{(r)}$ in $\mathbb{Q}_r$. Then at least two numbers in the set $\{1 + 2v_r(w), 4v_r(t), v_r(a) + 2v_r(t) + 2v_r(z), 4v_r(z)\}$ reach the minimal value, which we may assume to be zero. Hence $v_r(t) = v_r(z) = 0, v_r(w) \geq 0$. So

$$(t^2 - az^2)^2 \equiv 4bz^4 \mod r$$

is solvable in ${\mathbb{Z}_r}^*$. This requires that $(b/r) = 1$. Moreover, it implies that at least one of the equations

$$t^2 \equiv (a + 2\sqrt{b})z^2 \mod r,$$
$$t^2 \equiv (a - 2\sqrt{b})z^2 \mod r,$$

is solvable in ${\mathbb{Z}_r}^*$. This means, by Hensel's lemma, that

$$\left(\frac{a + 2\sqrt{b}}{r}\right) = 1 \quad \text{or} \quad \left(\frac{a - 2\sqrt{b}}{r}\right) = 1.$$

It is easy to see that this contradicts (iii) of Theorem 1.4.

For

$$C_r'^{(r)} : rw^2 = t^4 + at^2z^2 + bz^4,$$

similarly to the argument before, we see that $C_r'^{(r)}(\mathbb{Q}_r) = \emptyset$. This concludes the proof of Theorem 1.4. □

https://doi.org/10.1017/S1446788714000512 Published online by Cambridge University Press

Acknowledgement

The author is grateful to the anonymous referee for invaluable suggestions which helped improve the quality of the paper.

References

[1] D. Atake, 'On elliptic curves with large Tate–Shafarevich groups', *J. Number Theory* **87** (2001), 282–300.
[2] C. Breuil, B. Conrad, F. Diamond and R. Taylor, 'On the modularity of ellipitc curves over $\mathbb{Q}$', *J. Amer. Math. Soc.* **14** (2001), 843–939.
[3] J. R. Chen, 'On the representation of a large even number as the sum of a prime and the product of at most two primes', *Sci. Sinica* **16** (1973), 157–176.
[4] A. Dabrowski, 'On the proportion of rank 0 twists of elliptic curves', *C. R. Acad. Sci. Paris, Ser. I* **346** (2008), 483–486.
[5] A. Dabrowski and M. Wieczorek, 'On the equation $y^2 = x(x - 2^m)(x + 1 - 2^m)$', *J. Number Theory* **214** (2007), 364–379.
[6] K. Feng and M. Xiong, 'On elliptic curves $y^2 = x^3 - n^2x$ with rank zero', *J. Number Theory* **109**(1) (2004), 1–26.
[7] K. Feng and M. Xiong, 'On Selmer groups and Tate–Shafarevich groups for elliptic curves $y^2 = x^3 - n^3$', *Mathematika* **58**(2) (2012), 236–274.
[8] K. Feng and Y. Xue, 'New series of odd non-congruent numbers', *Sci. China Ser. A* **49**(11) (2006), 1642–1654.
[9] D. Goldfeld, 'Conjectures on elliptic curves over quadratic fields', in: *Number Theory, Carbondale 1979*, Lecture Notes in Mathematics, 751 (ed. M. B. Nathanson) (Springer, Berlin, 1979), 108–118.
[10] J. Hoffstein and W. Luo, 'Nonvanishing of L-series and the combinatorial sieve', *Math. Res. Lett.* **4** (1997), 435–444.
[11] H. Iwaniec, 'Almost-primes represented by quadratic polynomials', *Invent. Math.* **47** (1978), 171–188.
[12] H. Iwaniec and P. Sarnak, 'The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros', *Israel J. Math.* **120** (2000), 155–177.
[13] K. James, 'L-series with non-zero central critical value', *J. Amer. Math. Soc.* **11** (1998), 635–641.
[14] W. Kohnen, 'On the proportion of quadratic twists of L-functions attached to cusp forms not vanishing at the central point', *J. reine angew. Math.* **508** (1999), 179–187.
[15] V. A. Kolyvagin, 'Finiteness of $E(\mathbb{Q})$ and Ш$(E, \mathbb{Q})$ for a subclass of Weil curves', *Izv. Acad. Nauk USSR* **52** (1988), 522–540 (in Russian).
[16] K. Ono and C. Skinner, 'Non-vanishing of quadratic twists of modular L-functions', *Invent. Math.* **34** (1998), 651–660.
[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 1986).
[18] V. Vatsal, 'Rank-one twists of a certain elliptic curve', *Math. Ann.* **311** (1998), 791–794.
[19] J. L. Waldspurger, 'Sur les coefficients de Fourier des formes modulaires de poids demi-entier', *J. Math. Pures Appl.* (9) **60** (1981), 375–484.
[20] G. Yu, 'On the quadratic twists of a family of elliptic curves', *Mathematika* **52**(1–2) (2005), 139–154.

MAOSHENG XIONG, Department of Mathematics,
Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong
e-mail: mamsxiong@ust.hk