ON THE PRODUCT OF TWISTS OF RANK TWO AND A CONJECTURE OF LARSEN

ÁLVARO LOZANO-ROBLEDO

Abstract. In this note we present examples of elliptic curves and infinite parametric families of pairs of integers (d, d') such that, if we assume the parity conjecture, we can show that $E^d, E^{d'}$ and $E^{dd'}$ are all of positive even rank over $\mathbb{Q}$. As an application, we show examples where a conjecture of M. Larsen holds.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve, given by a Weierstrass equation $y^2 = f(x)$, for some monic cubic polynomial $f(x) \in \mathbb{Q}[x]$. Let N_E be the conductor of $E/\mathbb{Q}$. The twist of $E/\mathbb{Q}$ by $d \in \mathbb{Q}^\times$, denoted by $E^d/\mathbb{Q}$, is an elliptic curve given by $dy^2 = f(x)$. Let $W(E) = W(E/\mathbb{Q})$ and $W(E, d) = W(E^d/\mathbb{Q})$ be the root numbers of E and E^d respectively. Suppose that d, d' are fundamental discriminants, relatively prime to N_E. Then, it is well known that:

$$W(E, dd') = W(E, d)W(E, d')W(E). \tag{1}$$

Suppose further that the rank of E is even and the ranks of E^d and $E^{d'}$ are even and positive. If we assume the parity conjecture then Eq. (1) implies that the rank of $E^{dd'}$ is also even, i.e. $W(E, dd') = 1$. In light of a well-known conjecture of Goldfeld (see [1]), it seems reasonable to believe that the rank of $E^{dd'}$ should be generically equal to zero, even under the imposed assumptions on d and d'.

In this note we present examples of elliptic curves and infinite parametric families of pairs of integers (d, d') as above such that $E^d, E^{d'}$ and $E^{dd'}$ are of positive even rank over $\mathbb{Q}$. As an application, we show examples where a conjecture of M. Larsen holds for $n = 2$. Before we state his conjecture we need the following piece of notation: if $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$ and $F \subset \overline{\mathbb{Q}}$ is a field then the symbol $F^{(\sigma)}$ stands for the intersection of all fixed fields $F^{\langle\sigma_i\rangle}$, for $i = 1, \ldots, n$, where $\langle\sigma_i\rangle$ is the subgroup generated by σ_i.

Conjecture 1.1 (Larsen, [5]). *Let $A/\mathbb{Q}$ be an abelian variety. Then the rank of $A(\overline{\mathbb{Q}}^{(\sigma)}) \otimes \mathbb{Q}$ is infinite for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$.*

In fact, our results provide examples for a stronger conjecture (see [6], Conj. 1.2), namely that $\mathrm{rank}_{\mathbb{Z}}(A((\mathbb{Q}^{ab})^{(\sigma)}) \otimes \mathbb{Q})$ is infinite (although here we only provide examples for $n = 2$). Here is one such example:

1991 *Mathematics Subject Classification.* Primary: 14H52.

Theorem 1.2. *Let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = x^3 - x$ and define:*

$$\begin{aligned} P_1(t) &= 4t^7 - 8t^6 - 4t^5 - 4t^3 + 8t^2 + 4t, \\ P_2(t) &= 4t^7 + 8t^6 - 4t^5 - 4t^3 - 8t^2 + 4t. \end{aligned}$$

Assume that the parity conjecture holds for all rational quadratic twists of $E/\mathbb{Q}$. Then the three twists of E by d_i, d_i' and d_id_i', for $i \geq 1$, are all of even positive rank, where the twists are explicitly given by:

$$d_i = P_1(4+32i) \quad \text{and} \quad d_i' = P_2(4+32i).$$

Further:

1. *One can extract out of this family infinitely many triples $(d, d', dd') \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, pairwise distinct in $(\mathbb{Q}^*/\mathbb{Q}^{*2})^3$;*
2. *The rank of $E((\mathbb{Q}^{ab})^{(\sigma)})$ is infinite for all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^2$.*

Larsen's conjecture has been proved for $n = 1$ by B-H. Im and Larsen (see [2]). In [6], the author has shown that Larsen's conjecture holds for all $n \geq 0$ for elliptic curves over $\mathbb{Q}$ of odd rank and for curves without wild ramification at 2 and 3, subject to the parity conjecture (notice that the curve $y^2 = x^3 - x$ has even rank equal to zero and wild ramification at 2, hence it is not covered by previous results). One can use Theorems 2.4 and 3.1 to construct many other analogous examples.

Acknowledgements. I would like to thank Ravi Ramakrishna for his help and comments, and also I thank the anonymous referee for a careful reading and several corrections.

2. Background on Twists

In this section we provide a number of well-known results on twists of elliptic curves, which will be used in subsequent proofs. If $d \in \mathbb{Q}^\times$ is a square-free rational number, the symbol E^d stands for the quadratic twist of the elliptic curve $E/\mathbb{Q}$ by d. Let N_E be the conductor of E and let $W(E/\mathbb{Q})$ be the global root number (or $W(E)$ if the field of definition is clear from the context), i.e., the sign in the functional equation for $L(E/\mathbb{Q}, s)$. We will write $W(E, d)$ for $W(E^d)$.

Definition 2.1. *If $\alpha \in \mathbb{Q}^*$ and $n \in \mathbb{Z}^+$, then:*

1. *$\alpha \equiv 1 \bmod^\times n$ means that $\alpha - 1 \in n\mathbb{Z}_l$ for all primes $l|n$;*
2. *$\alpha \equiv 1 \bmod^\times n\infty$ means that $\alpha \equiv 1 \bmod^\times n$ and $\alpha > 0$.*

Lemma 2.2 ([7])**.** *Suppose E is an elliptic curve over $\mathbb{Q}$, let N_E be the conductor of $E/\mathbb{Q}$ and let $d \in \mathbb{Z}$ be a fundamental discriminant (i.e. either $d \equiv 1 \mod 4$ or $d = 4d'$ with $d' \equiv 2, 3 \mod 4$, and d, d' square-free).*

1. *If $\gcd(N_E, d) = 1$ then $W(E, d) = \left(\frac{d}{-N_E}\right) \cdot W(E)$ where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol.*

(2) *If d, d' are fundamental discriminants, relatively prime to N_E and to each other, then $W(E, dd') = W(E, d) \cdot W(E, d') \cdot W(E)$.*

(3) ([8], Lemma 4.3) *Suppose c, c' are non-zero rational numbers such that there exists $\beta \in \mathbb{Q}^*$ such that $\beta^2 c/c' \equiv 1 \bmod^{\times} 8N_E\infty$. Then $W(E, c) = W(E, c')$.*

Lemma 2.3 ([10], X.§5)**.** *Let $d \in \mathbb{Q}^{\times}$ be a square free integer and let $E/\mathbb{Q}$ be an elliptic curve. Then:*

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}(\sqrt{d})) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + \operatorname{rank}_{\mathbb{Z}}(E^d(\mathbb{Q})).$$

The following result is shown in [3]. Although we will not use it here, it provides examples for which the main hypothesis of Theorem 3.1 is satisfied:

Theorem 2.4 ([3], Corollary 4.4)**.** *Let K be a number field and let E/K be an elliptic curve satisfying one of the following:*

(1) *All 2-torsion points are K-rational;*

(2) *E/K has a Weierstrass equation of the form $y^2 = x^3 + ax^2 + c^2x$, for some $a, c \in K$;*

(3) *E/K has a Weierstrass equation of the form $y^2 = x(x^2 - k)$, with $1 + k = e^2 + f^2$, for some $k, e, f \in K$.*

(4) *E/K is K-isogenous to an elliptic curve as in (1), (2) or (3) above.*

Then there exist explicit polynomials P_1 and P_2 in $K[t]$ such that P_1, P_2 and P_1P_2 are not in $K \cdot (K[t])^2$ and the twists $E^{P_1(t)}$, $E^{P_2(t)}$, $E^{P_1P_2(t)}$ are of positive rank over $K(t)$.

3. Product of twists

The main theorem of this section is:

Theorem 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve and suppose there exist polynomials P_1 and P_2 in $\mathbb{Q}[t]$ such that P_1, P_2 and P_1P_2 are not in $\mathbb{Q} \cdot (\mathbb{Q}[t])^2$ and the twists $E^{P_1(t)}$, $E^{P_2(t)}$, $E^{P_1P_2(t)}$ are of positive rank over $\mathbb{Q}(t)$. Further, suppose that there is a value $t_0 \in \mathbb{Q}$ such that $E^{P_1(t_0)}$, $E^{P_2(t_0)}$, $E^{P_1P_2(t_0)}$ are of positive even rank over $\mathbb{Q}$ and assume the parity conjecture for all quadratic twists of $E/\mathbb{Q}$. Then there are infinitely many triples $(d, d', dd') \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$, pairwise distinct in $(\mathbb{Q}^*/\mathbb{Q}^{*2})^3$, such that the twists E^d, $E^{d'}$ and $E^{dd'}$ are all of positive even rank over $\mathbb{Q}$.*

In the proof of Theorem 3.1 we will make use of a number of lemmas. The first lemma appears in [5, Lemma 4]. Here we state a stronger statement which follows from the proof presented in [5].

Lemma 3.2. *Let F be a number field and $P_1(t), P_2(t), \ldots,$ $P_{n+1}(t)$ a sequence of polynomials in $F[t]$ each of which has a zero (over $\overline{F}$) of odd multiplicity. If $\mathcal{L}/F$ is a finite separable extension of F, then the set of all $a \in F$ such that $P_i(a)$ is not a perfect square in $\mathcal{L}$, for $i = 1, \ldots, n+1$, is a Hilbert set of F and therefore infinite.*

For a definition of a Hilbert set, a Hilbertian field and for a proof of the fact that number fields are Hilbertian, see [4, Chapter 9] or [9, Chapter 3].

The following result is an extension of Corollary 2.5 of [4]:

Lemma 3.3. *A Hilbert set H of $\mathbb{Q}$ is dense for the ordinary topology and every p-adic topology on $\mathbb{Q}$. Moreover, if S is a finite set of primes of $\mathbb{Z}$ and U_p are open sets of $\mathbb{Q}$ for the p-adic topology, then $H \cap (\bigcap_{p\in S} U_p)$ is infinite.*

Proof. The first statement is [4, Corollary 2.5]. For the second statement, put $N = \prod_{p\in S} p$. If $f(t,X)$ is irreducible over $\mathbb{Q}(t)$ and $a \in \bigcap_{p\in S} U_p$, then so is $f(a+tN^\nu, X)$ for large ν. □

Also, the reader should recall Silverman's specialization theorem (see [11, p. 271, Theorem 11.4]): if $E_t/K(t)$ is a non-split elliptic curve defined over $K(t)$ then for all but finitely many $t_0 \in K$ the rank of the specialization E_{t_0}/K is at least that of $E_t/K(t)$ (there is also a specialization theorem for split surfaces due to Dem'janenko and Manin). It is easy to see that if $h(t) \in K[t]$ is a polynomial not in $K \cdot (K[t])^2$ then the twist $E^{h(t)}/K(t)$ is non-split, for any elliptic curve E/K (see [3], Lemma 2.2, for a proof). The last lemma we need is this technical result:

Lemma 3.4. *Let $P = \{P_1(t), P_2(t), \cdots, P_k(t)\}$ be a finite set of non-zero polynomials in $\mathbb{Q}[t]$, let $N > 0$ be an integer, let t_0 be a fixed rational number which is not a root of any polynomial in P and define*

$$T = \{s \in \mathbb{Q} : \frac{P_i(s)}{P_i(t_0)} \equiv 1 \mod {}^\times N\infty \textit{ for all } 1 \le i \le k\}.$$

Then there are non-empty open sets V_∞ of $\mathbb{R}$ and V_p of $\mathbb{Q}_p$, for every p dividing N, such that if we let $U_\nu = V_\nu \cap \mathbb{Q}$ then set T contains their intersection $\bigcap U_\nu$. In particular, T is infinite.

Proof. Let $1 \le i \le k$ be fixed. There is a non-empty open neighborhood V_∞^i of t_0 in the usual topology of $\mathbb{Q}$ such that if $s \in V_\infty^i$ then $P_i(s)$ and $P_i(t_0)$ have the same sign and $P_i(s)/P_i(t_0) > 0$. Let p be a prime dividing N and let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ at p. Similarly, there is a non-empty open neighborhood V_p^i of t_0 in $\mathbb{Q}_p$ such that if $s \in V_p^i$ then $P_i(s)/P_i(t_0) - 1 \in N\mathbb{Z}_p$. Put $V_\nu = \bigcap_{i=1}^k V_\nu^i$, for any ν dividing $N\infty$. Since each set V_ν is an intersection of a finite number of non-empty open neighborhoods of a fixed $t_0 \in \mathbb{Q}$, it follows that each V_ν is also a non-empty open neighborhood of t_0. The intersection $U_\nu = V_\nu \cap \mathbb{Q}$ forms an open subset of $\mathbb{Q}$ in the ν-adic topology. By Lemma 3.3 and since there are only finitely many places of $\mathbb{Q}$ which divide $N\infty$, any Hilbert set of $\mathbb{Q}$ has infinite intersection with $\bigcap U_\nu$ and, in particular, $\mathbb{Q} \cap (\bigcap U_\nu) = \bigcap U_\nu$ is infinite. Since the set T contains $\bigcap U_\nu$ we conclude that T is infinite. □

Now we are ready to prove Theorem 3.1.

3.1. **Proof of Theorem 3.1.** Let $E/\mathbb{Q}$ is an elliptic curve and suppose there exist $t_0 \in \mathbb{Q}$ and polynomials P_1 and P_2 in $\mathbb{Q}[t]$ such that P_1, P_2 and $P_3 := P_1P_2$ are not in $\mathbb{Q} \cdot (\mathbb{Q}[t])^2$ and the twists $E^{P_i(t)}$ are of positive rank over $\mathbb{Q}(t)$, and $E^{P_i(t_0)}$ are of positive rank over $\mathbb{Q}$, for $i = 1, 2, 3$. Put $d_0 = P_1(t_0), d'_0 = P_2(t_0)$ and define:

$$T = \{s \in \mathbb{Q} : \frac{P_i(s)}{P_i(t_0)} \equiv 1 \mod {}^{\times}8N_E\infty \text{ for all } i = 1, 2, 3\}.$$

By Lemma 3.4, for every place ν dividing $8N_E\infty$ there are non-empty open neighborhoods U_ν of t_0 such that the set T contains $\bigcap U_\nu$ and therefore T is infinite.

We will use induction to recursively construct triples $D_j = (d_j, d'_j, d_jd'_j)$, for all $j \geq 0$, satisfying the required properties. Put $D_0 = (d_0, d'_0, d_0d'_0)$ and suppose that we have chosen $D_1, \ldots, D_n \in \mathbb{Q}^3$, pairwise distinct in $(\mathbb{Q}^*/\mathbb{Q}^{*2})^3$, such that the twists E^{d_j}, $E^{d'_j}$ and $E^{d_jd'_j}$ are all of positive even rank over $\mathbb{Q}$, for all $j = 0, \ldots, n$. Define a finite (separable) extension of $\mathbb{Q}$ by:

$$L = \mathbb{Q}\left(\{\sqrt{d_j}, \sqrt{d'_j} : j = 0, 1, \ldots, n\}\right).$$

By Lemma 3.2, the set H of rational numbers s such that $P_i(s)$ is not a square in L, for $i = 1, 2, 3$, is a Hilbert set of $\mathbb{Q}$ (notice that the fact that P_1, P_2, P_1P_2 are not in $\mathbb{Q} \cdot (\mathbb{Q}[t])^2$ implies that they all have a zero of odd order). Combining Lemma 3.3 with 3.4, we can conclude that $H \cap T$ is infinite. By Silverman's specialization theorem, since $E^{P_i(t)}$ are of positive rank over $\mathbb{Q}(t)$, there is a finite set $S \in \mathbb{Q}$ such that if $s \notin S$ then $E^{P_i(s)}$ is of positive rank over $\mathbb{Q}$, for $i = 1, 2, 3$.

Let $s \in H \cap T$, with $s \notin S$, and put $d_{n+1} = P_1(s)$, $d'_{n+1} = P_2(s)$ and $d_{n+1}d'_{n+1} = P_3(s) = P_1P_2(s)$. By construction, $d = d_{n+1}$, $d' = d'_{n+1}$ and $dd' = d_{n+1}d'_{n+1}$ are not squares in L, thus they are distinct in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ to any of $d_j, d'_j, d_jd'_j$, for $0 \leq j \leq n$. Furthermore, the fact that $s \in T$ implies that $P_i(s)/P_i(t_0) \equiv 1 \mod {}^{\times}8N_E\infty$ and so, if we assume the parity conjecture, Lemma 2.2 implies

$$\begin{aligned} W(E,d) &= W(E,d_0) = +1, \quad W(E,d') = W(E,d'_0) = +1, \\ W(E,dd') &= W(E,d_0d'_0) = +1. \end{aligned}$$

Thus, again by the parity conjecture, $E^d, E^{d'}$ and $E^{dd'}$ are of even rank. Moreover, since we chose $s \notin S$, the rank of the mentioned twists is positive, as desired. This concludes the proof of the Theorem.

4. On a conjecture of Larsen

In this section we explain how Theorem 3.1 can be used to provide examples where Conjecture 1.1 holds for $n = 2$.

Definition 4.1 (cf. [6], Defn. 3.2)**.** *We say that an elliptic curve $E/\mathbb{Q}$ satisfies property (A^n) if for all $i \geq 1$ there exist $D_i = (d_{i,1}, \dots, d_{i,n+1}) \in (\mathbb{Q}^\times)^{n+1}$ such that:*

(A1) *Put $L_0 = \mathbb{Q}$ and define $L_i = L_{i-1}(\{\sqrt{d_{i,j}} : j = 1, \dots, n+1\})$ for all $i \geq 1$. Then $[L_i : L_{i-1}] = 2^{n+1}$;*

(A2) *For all $i \geq 1$ and $d \in \mathbb{Q}^\times$ of the form*

$$d = \prod_{j=1}^{n+1} (d_{i,j})^{e_j} \quad \textit{with } e_j = 0, 1$$

the rank of $E(\mathbb{Q}(\sqrt{d}))$ is strictly greater than that of $E(\mathbb{Q})$.

As before, the symbol $\mathbb{Q}^{ab}$ is the maximal abelian extension of $\mathbb{Q}$ and $\mathbb{Q}^{(2)}$ is the compositum of all quadratic extensions of $\mathbb{Q}$.

Proposition 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying the property (A^2). Then for each $(\sigma) = (\sigma_1, \sigma_2) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^2$, the rank of $A((\mathbb{Q}^{(2)})^{(\sigma)})$ is infinite.*

Proof. This is a special case of Theorem 3.1 in [6], for $n = 2$ and when the set S contains all primes. □

Theorem 4.3. *Let $E/\mathbb{Q}$ be an elliptic curve and suppose the following hypotheses hold:*

1. *There exist polynomials P_1 and P_2 in $\mathbb{Q}[t]$ such that P_1, P_2 and P_1P_2 are not in $\mathbb{Q} \cdot (\mathbb{Q}[t])^2$ and the twists $E^{P_1(t)}$, $E^{P_2(t)}$, $E^{P_1P_2(t)}$ are of positive rank over $\mathbb{Q}(t)$;*
2. *The parity conjecture holds for all quadratic twists of $E/\mathbb{Q}$;*
3. *There is a value $t_0 \in \mathbb{Q}$ such that $E^{P_1(t_0)}$, $E^{P_2(t_0)}$, $E^{P_1P_2(t_0)}$ are of positive rank over $\mathbb{Q}$ (note that the existence of such a value t_0 follows from (1) and Silverman's specialization theorem);*
4. *There is a $d \in \mathbb{Q}^\times$ such that d, $dP_1(t_0)$, $dP_2(t_0)$ and $dP_1(t_0)P_2(t_0)$ are not perfect squares and*

$$W(E, d) = W(E, dP_1(t_0)) = W(E, dP_2(t_0)) = W(E, dP_1(t_0)P_2(t_0)) = -1.$$

Then $E/\mathbb{Q}$ satisfies property (A^2). Consequently, for each $(\sigma) = (\sigma_1, \sigma_2) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^2$, the rank of $A((\mathbb{Q}^{(2)})^{(\sigma)})$ is infinite.

Proof. Let $E/\mathbb{Q}$, P_1, P_2, $P_1P_2(= P_3)$, $t_0 \in \mathbb{Q}$ and d be as in the statement of the theorem. Let $\mathcal{P}$ be the infinite set of primes congruent to $1 \mod 8N_E$ (of course, the fact that $\mathcal{P}$ is infinite may be proven using Dirichlet's theorem on primes in arithmetic progressions) and define a set:

$$T = \{s \in \mathbb{Q} : \frac{P_i(s)}{P_i(t_0)} \equiv 1 \mod {}^\times 8N_E\infty \text{ for } i = 1, 2, 3\}.$$

By Lemma 3.4, for every place ν dividing $8N_E\infty$ there are non-empty open neighborhoods U_ν of t_0 such that the set T contains $\bigcap U_\nu$ and therefore T is infinite. By Silverman's specialization theorem, since $E^{P_i(t)}$ are of positive rank over $\mathbb{Q}(t)$, there is a finite set $S \in \mathbb{Q}$ such that if $s \notin S$ then $E^{P_i(s)}$ is of positive rank over $\mathbb{Q}$, for $i = 1, 2, 3$.

We will define integers $d_{i,j}$, for $j = 1, 2, 3$ and $i \geq 1$, and $D_i = (d_{i,1}, d_{i,2}, d_{i,3})$ recursively, so that the triples D_i satisfy conditions (A1) and (A2) of Definition 4.1. We put $d_{1,1} = P_1(t_0)$ and $d_{1,2} = P_2(t_0)$. Also put $d_{1,3} = d$. Then, by the hypotheses in the theorem and the parity conjecture, the triple $D_1 = (d_{1,1}, d_{1,2}, d_{1,3})$ satisfies properties (A1) and (A2). Suppose $D_1, \ldots, D_m$ have been chosen so that (A1) and (A2) are verified. In particular, by (A1), none of the numbers of the form:

$$c = \prod_{j=1}^{3} \prod_{i=1}^{m} (d_{i,j})^{e_{i,j}} \quad \text{with } e_{i,j} = 0, 1 \tag{2}$$

are squares of $\mathbb{Q}$ (otherwise $L_m/\mathbb{Q}$ would not be of degree 2^{3m} as it should be).

Define a finite (separable) extension $\mathcal{L}/\mathbb{Q}$ by:

$$\mathcal{L} = \mathbb{Q}\left(\{\sqrt{d_{i,1}}, \sqrt{d_{i,2}}, \sqrt{d_{i,3}} : i = 1, \ldots, m\}\right).$$

By Lemma 3.2, the set H of rational numbers s such that $P_i(s)$ is not a square in $\mathcal{L}$, for $i = 1, 2, 3$, is a Hilbert set of $\mathbb{Q}$. Combining Lemma 3.3 with 3.4, we can conclude that $H \cap (T \setminus S)$ is infinite. Let $t_{m+1} \in H \cap (T \setminus S)$ and define $d_{m+1,1} = P_1(t_{m+1})$ and $d_{m+1,2} = P_2(t_{m+1})$. Thus, by construction, $\mathcal{L}' = \mathcal{L}(\sqrt{d_{m+1,1}}, \sqrt{d_{m+1,2}})$ is a biquadratic extension of $\mathcal{L}$. Let p_{m+1} be a prime of the set P, so that $p_{m+1} = 1 + 8N_E s$ for some integer $s \geq 1$, such that p_{m+1} is relatively prime to all coordinates of D_i, for $1 \leq i \leq m$, and relatively prime to $d_{m+1,j}$ for $j = 1, 2$. Define $d_{m+1,3} = dp_{m+1}$ and let $c \in \mathbb{Q}^\times$ be a number of the form:

$$c = \prod_{j=1}^{3} \prod_{i=1}^{m+1} (d_{i,j})^{e_{i,j}} \quad \text{with } e_{i,j} = 0, 1. \tag{3}$$

If c is already listed in Eq. (2) then $c \notin \mathbb{Q}^{\times 2}$, by (A1) as explained before. Otherwise, $e_{m+1,j} = 1$ for $j = 1, 2$ or 3. If $e_{m+1,j} = 1$ for $j = 1$ or 2, since $\mathcal{L}'/\mathcal{L}$ is biquadratic, then $c \notin \mathbb{Q}^{\times 2}$. Finally, if $e_{m+1,3} = 1$ then p_{n+1} divides c but p_{n+1}^2 does not divide c. Thus c is not a square of $\mathbb{Q}$ and, hence, $[L_{m+1} : \mathbb{Q}] = 2^{3(m+1)}$ and $[L_{m+1} : L_m] = 2^3$. This shows that the triples D_i for $1 \leq 1 \leq m + 1$ satisfy (A1).

It remains to show that D_{m+1} satisfies (A2). To this end, we need to check that $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}(\sqrt{c})) > \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ for any integer c in the list:

$$d_{m+1,1} = P_1(t_{m+1}),\ d_{m+1,2} = P_2(t_{m+1}),\ (d_{m+1,1})(d_{m+1,2}), \tag{4}$$

$$dp_{m+1},\ (d_{m+1,1})dp_{m+1},\ (d_{m+1,2})dp_{m+1},\ (d_{m+1,1})(d_{m+1,2})dp_{m+1}. \tag{5}$$

If c is one of the values in Eq. (4) then $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}(\sqrt{c})) > \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ because $t_{m+1} \in H \cap (T \setminus S)$ and Lemma 2.3. Let $c = (d_{m+1,1})dp_{m+1}$ (the proof is the same for the rest of the values in Eq. (5)). Since $(d_{m+1,1})/d_1 \equiv 1$

mod ${}^{\times}8N_E\infty$ and $p_{m+1} \equiv 1 \mod 8N_E$, it follows that $(d_{m+1,1})dp_{m+1}/d_1d \equiv 1 \mod {}^{\times}8N_E\infty$. By Lemma 2.2:

$$W(E,c) = W(E,(d_{m+1,1})dp_{m+1}) = W(E,(d_{1,1})d) = W(E,P_1(t_0)d) = -1.$$

Thus, by the parity conjecture, $E^c/\mathbb{Q}$ is of positive rank and the rank of $E(\mathbb{Q}(\sqrt{c}))$ is greater than $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. This finishes the proof of the theorem. □

5. An explicit example

In this final section we provide a proof of Theorem 1.2, i.e. we show an explicit elliptic curve which exemplifies how the theory we developed can be used. If a,b are non-zero elements of a field F, the notation $a \sim b$ means that $[a] = [b] \in F^{\times}/F^{\times 2}$.

Let $E/\mathbb{Q}$ be the elliptic curve $E : y^2 = x^3 - x$ and put $f(x) = x^3 - x$. The group of rational points $E(\mathbb{Q})$ is finite of order 4. The curve $E/\mathbb{Q}$ has complex multiplication and rank 0, so in this case by the work of Kolyvagin-Rubin-Zagier (or by direct computation!), we know that the sign in the functional equation of $L(E/\mathbb{Q},s)$ is $W(E/\mathbb{Q}) = 1$. The conductor of E is $N_E = 32$.

The construction of [3], Proposition 3.8, yields the following polynomials P_1 and P_2. Put:

$$g_1(x) = x^2 - 2x - 1,\ g_2(x) = -x^2 - 2x + 1,\ h(x) = x^2 + 1$$

and

$$\begin{aligned} P_1(x) &= h(x)g_1(x)(h(x)^2 - g_1(x)^2) = 4x^7 - 8x^6 - 4x^5 - 4x^3 + 8x^2 + 4x, \\ P_2(x) &= h(x)g_2(x)(h(x)^2 - g_2(x)^2) = 4x^7 + 8x^6 - 4x^5 - 4x^3 - 8x^2 + 4x, \\ P_3(x) &= P_1(x)P_2(x). \end{aligned}$$

The elliptic surfaces $E^{P_1(t)}$, $E^{P_2(t)}$ and $E^{P_3(t)}$ are of positive rank over $\mathbb{Q}(t)$ (the reason is that, $P_1(t) \sim f(\frac{g_1(t)}{h(t)})$ modulo squares, $P_2(t) \sim f(\frac{g_2(t)}{h(t)})$ and $P_3(t) \sim f(\frac{g_1(t)g_2(t)}{h(t)^2})$).

Now, let $t_0 = 4$ and calculate:

$$P_1(4) = 28560 \sim 1785, \quad P_2(4) = 93840 \sim 5865, \quad P_1P_2(4) \sim 161.$$

The numbers 1785, 5865, 161 are all $\equiv 1 \mod 4$ and squarefree, and so they are fundamental discriminants. Thus, by Lemma 2.2, and after calculating some Kronecker symbols, one obtains:

$$W(E,1785) = W(E,5865) = W(E,161) = 1.$$

In fact, a quick calculation with the software MAGMA reveals that the ranks of E^{1785}, E^{5865} and E^{161} are equal to 2. Hence, the hypotheses of Theorem 3.1 are satisfied and there exist infinitely many triples $(d,d',dd') \in \mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}$, pairwise distinct in $(\mathbb{Q}^*/\mathbb{Q}^{*2})^3$, such that the twists E^d, $E^{d'}$ and $E^{dd'}$ are all of positive even rank over $\mathbb{Q}$. In fact, by making the proof explicit, one can pick d, d' among the infinite family:

$$d_i = P_1(4+32i) \quad \text{and} \quad d_i' = P_2(4+32i) \quad \text{for all} \quad i \geq 1.$$

Finally, let $d > 0$ be a fundamental discriminant (with $d \in \mathbb{Z}$ square-free, $d \equiv 1 \mod 4$) such that the Kronecker symbol $\left(\frac{d}{-32}\right) = -1$, for example, pick $d = 5$. Then, by Lemma 2.2:

$$W(E,5) = W(E, 1785 \cdot 5) = W(E, 5865 \cdot 5) = W(E, 161 \cdot 5) = -1.$$

Hence, by Theorem 4.3 and if the parity conjecture holds for quadratic twists of E, the rank of $E((\mathbb{Q}^{ab})^{(\sigma)})$ is infinite, for all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^2$.

References

[1] D. Goldfeld, "Conjectures on elliptic curves over quadratic fields", in Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), M. B. Nathanson, ed., Lect. Notes in Math. **751**, Springer, Berlin, 1979, 108118.

[2] B-H. Im, M. Larsen, "Abelian varieties over cyclic fields", *Amer. J. Math.* to appear, arXiv: math.NT/0605444.

[3] B-H. Im, Á. Lozano-Robledo, "On products of quadratic twists and ranks of elliptic curves over large fields", to appear.

[4] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York, 1983.

[5] M. Larsen, "Rank of elliptic curves over almost algebraically closed fields", *Bull. London Math. Soc.* **35** (2003) 817-820.

[6] Á. Lozano-Robledo, "Ranks of abelian varieties over infinite extensions of the rationals", to appear.

[7] D. Rohrlich, "Variation of the root number in families of elliptic curves", *Compositio Mathematica*, tome 87, no. 2, (1993), p. 119-151.

[8] K. Rubin, A. Silverberg, "Twists of elliptic curves of rank at least four", in *Ranks of Elliptic Curves and Random Matrix Theory*, Cambridge University Press (2007), 177-188.

[9] J-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones and Bartlett Publishers, London, 1992.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[11] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

Dept. of Math., 584 Malott Hall, Cornell University, Ithaca, NY 14853.
E-mail address: `alozano@math.cornell.edu`