ON PRODUCTS OF QUADRATIC TWISTS AND RANKS OF ELLIPTIC CURVES OVER LARGE FIELDS

BO-HAE IM AND ÁLVARO LOZANO-ROBLEDO

Abstract. In this paper, we give examples of elliptic curves E/K over a number field K satisfying the property that there exist $P_1, P_2 \in K[t]$ such that the twists E^{P_1}, E^{P_2} and $E^{P_1P_2}$ are of positive rank over $K(t)$. As a consequence of this result on twists, we show that for those elliptic curves E/K, and for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the rank of E over the fixed field under σ, $(K^{ab})^\sigma$, is infinite, where K^{ab} is the maximal abelian extension of K.

1. Introduction

The purpose of this note is twofold. First, let K be a number field and let E/K be an elliptic curve with a Weierstrass equation $y^2 = g(x)$ defined over K. For $d \in K$, the curve given by $dy^2 = g(x)$ is a quadratic twist of E by d, and we will denote it by E^d. In 1979, Goldfeld [2] conjectured that, for every fixed elliptic curve E/K, the average rank of the quadratic twists of E is $1/2$ (see also the survey [14]). Suppose that E has root number $+1$ and let d and d' be fundamental discriminants relatively prime to the conductor of E/K and to each other. It is well-known that if E^d and $E^{d'}$ are distinct twists of E, and ϵ and ϵ' are respectively their root numbers, then the root number of $E^{dd'}$ is $\epsilon\epsilon'$. If E^d and $E^{d'}$ are both of rank 1 then according to the parity conjecture their root number is -1, thus the root number of $E^{dd'}$ is $+1$, so the rank should be even. By Goldfeld's conjecture, we expect that the rank of $E^{dd'}$ drops generically to zero. In this note, however, we give examples of elliptic curves E/K which satisfy the following property:

> (A) There are infinitely many triples $(d, d', dd') \in K \times K \times K$, pairwise distinct in $(K^*/K^{*2})^3$, such that the twists E^d, $E^{d'}$ and $E^{dd'}$ are all of positive rank over K.

In particular, if E^d and $E^{d'}$ are of rank 1 and the twist $E^{dd'}$ is of positive rank, then according to the parity conjecture it must have even rank ≥ 2. Our results are stated in a slightly stronger fashion, since we actually show families of elliptic curves E/K which satisfy:

> (B) There exist 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 $K(t)$.

We note that if $P(t)$ is not in $K \cdot (K[t])^2$ then $P(t)$ is non-constant and has a zero of odd multiplicity over $\overline{K}$.

In Section 2, we prove that Silverman's specialization theorem [15, Theorem 11.4] shows that the property (B) implies (A). In Section 3, we show that certain results of D. Rohrlich on root numbers combined with Hilbert's irreducibility imply that all elliptic curves over $\mathbb{Q}$ verify the property (A), subject to the parity conjecture. In addition, we construct examples of curves which satisfy the property (B). In Section 4, we introduce a certain algebraic variety associated to the property (A) or (B) for elliptic curves.

The second purpose of the note is to give more evidence towards a conjecture of Larsen. Let K be an infinite field of finite type, let n be a positive integer and denote a fixed separable closure of K and the maximal abelian extension of K by $\overline{K}$ and K^{ab}, respectively. For every $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in \mathrm{Gal}(\overline{K}/K)^n$ we write $\overline{K}^{(\sigma)}$ for the fixed field in $\overline{K}$ of $(\sigma_1, \ldots, \sigma_n)$. Let $A/\overline{K}^{(\sigma)}$ be an abelian variety defined over $\overline{K}^{(\sigma)}$ with $\dim A \geq 1$. G. Frey and M. Jarden have shown in [1] that for almost all $\sigma \in \mathrm{Gal}(\overline{K}/K)^n$ the rank of $A(\overline{K}^{(\sigma)})$ is infinite. In fact, M. Larsen has conjectured in [9] that the rank of $A(\overline{K}^{(\sigma)})$ is infinite for all $(\sigma) \in \mathrm{Gal}(\overline{K}/K)^n$. This conjecture has been shown to hold for $n = 1$ in [7]. The problem remains open for $n > 1$.

The simplest case, $\dim A = 1$ (so that A is an elliptic curve) and $n = 1$, has been studied to some extent (see [4],[5],[6]).

In Section 5 of this note, we define a property (B_n), which is a generalization of (B), and we show that if an elliptic curve E/K satisfies property (B_n), for some $n \geq 2$, then the rank of $E((K^{ab})^{(\sigma)})$ is infinite, so the rank of $E(\overline{K}^{(\sigma)})$ is infinite, for all $(\sigma) \in \mathrm{Gal}(\overline{K}/K)^n$ (see Theorem 5.2). As a consequence of this, and the results on twists of section 3, we provide a simple proof of the fact that Larsen's conjecture holds for $n = 1$ for certain families of elliptic curves (see Corollary 5.3). We note that this result is stronger than the results in [4], [5], [6], and [7] for certain elliptic curves in the sense that this result gives examples of elliptic curves (other than those given in [6]) which have infinite rank over a smaller field $(K^{ab})^{\sigma}$ than $\overline{K}^{(\sigma)}$.

2. Property (B) implies property (A)

In this section, and again in Section 5, we will make use of the following lemma, which appears in [9, Lemma 4]. Here we state a stronger statement which follows from the proof presented in [9].

Lemma 2.1. *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 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 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 [8, Chapter 9] or [13, Chapter 3].

Silverman's specialization theorem (see [15, p. 271, Theorem 11.4]) states that 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 an specialization theorem for split surfaces due to Dem'janenko and Manin). In order to apply Silverman's specialization theorem, we show that certain elliptic curves over $K(t)$ are non-split.

Lemma 2.2. *Let E/K be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in K$, and let $h(t) \in K[t]$ be a polynomial not in $K \cdot (K[t])^2$. Then the twist $E^{h(t)}/K(t)$, given by $y^2 = x^3 + Ah(t)^2x + Bh(t)^3$ is non-split.*

Proof. Notice that $j(E^{h(t)}) = j(E) \in K$ is constant. In [15, p. 280], it is shown that an elliptic curve $E_t/K(t)$ splits if and only if one of the following conditions is true:

(1) $j(E_t) = 0$ and $c_6 \in (K(t))^6$.
(2) $j(E_t) = 1728$ and $c_4 \in (K(t))^4$.
(3) $j(E_t) = k \in K$ with $k \neq 0, 1728$ and $c_6/c_4 \in (K(t))^2$.

In our case, let $h(t) \in K(t)$ be a polynomial which is not in $K \cdot (K(t))^2$. Then:

(1) If $j(E^{h(t)}) = 0$ then $A = 0$ and $c_6 = -864 \cdot B \cdot h(t)^3$, which implies that $c_6 \notin (K(t))^6$.
(2) If $j(E^{h(t)}) = 1728$ then $B = 0$ and $c_4 = -48 \cdot A \cdot h(t)^2$, which implies that $c_4 \notin (K(t))^4$.
(3) If $j(E^{h(t)}) = k \in K$ with $k \neq 0, 1728$ then $c_6/c_4 = \frac{18 \cdot B}{A \cdot h(t)}$, which implies that $c_6/c_4 \notin (K(t))^2$.

Hence, in all cases the curve $E^{h(t)}$ is non-split over $K(t)$. □

Next we define a weaker property than (B), which we call (wB):

> (wB) There exist non-constant polynomials P_1 and P_2 in $K[t]$ such that P_1, P_2 and P_1P_2 are not in $K \cdot (K[t])^2$, the twists $E^{P_1(t)}$, $E^{P_2(t)}$ are of positive rank over $K(t)$ and for every finite separable extension L/K there are infinitely many specializations $t_0 \in K$ such that $E^{P_1(t_0)P_2(t_0)}$ is of positive rank and $P_1(t_0)$, $P_2(t_0)$ and $P_1(t_0)P_2(t_0)$ are not squares in L.

Proposition 2.3. *The property* (B) *implies the property* (wB).

Proof. Suppose E/K satisfies (B), i.e. there exist non-constant polynomials P_1 and P_2 in $K[t]$ such that P_1, P_2 and P_1P_2 are not in $K \cdot (K[t])^2$ (so each one has a zero of odd multiplicity) and the twists $E^{P_1(t)}$, $E^{P_2(t)}$, $E^{P_1P_2(t)}$ are of positive rank over $K(t)$. By the specialization theorem and Lemma 2.2, there is a finite set $S \subset K$ such that for all numbers $q \notin S$, the twists $E^{P_1(q)}$, $E^{P_2(q)}$ and $E^{P_1(q)P_2(q)}$ are of positive rank over K. Finally, if L/K

is a finite separable extension, by Lemma 2.1, the set of all elements $q \in K$ but $q \notin S$ such that $P_1(t_0)$, $P_2(t_0)$ and $P_1(t_0)P_2(t_0)$ are not squares in L is infinite. □

Theorem 2.4. *If E/K satisfies the property* (wB)*, then it also satisfies* (A)*.*

Proof. The idea of the proof is similar to that of Theorem 5 in [9]. Suppose that E/K is an elliptic curve satisfying (wB) and let $P_1(t)$, $P_2(t) \in K[t]$ be the given polynomials such that $E^{P_1(t)}, E^{P_2(t)}$ are of positive rank over $K(t)$. Then, by the specialization theorem and the property (wB) with $L = K$, there is a finite set $S \subset K$ and $q_0 \notin S$ such that the twists $E^{P_1(q_0)}$, $E^{P_2(q_0)}$ and $E^{P_1(q_0)P_2(q_0)}$ are of positive rank and $d_0 = P_1(q_0)$, $d_0' = P_2(q_0)$ and $d_0 d_0'$ are not perfect squares in K. It remains to show that there are infinitely many pairwise distinct $(d_i, d_i', d_i d_i')$ for $i \geq 1$ in $(K^*/K^{*2}) \times (K^*/K^{*2}) \times (K^*/K^{*2})$.

We finish the proof by induction. Let $n \geq 1$ be fixed and let $q_1, \ldots, q_n \in K$ be chosen such that the elements $(d_i, d_i', d_i d_i')$ are pairwise distinct in $(K^*/K^{*2})^3$, where d_i, d_i', $d_i d_i'$ are not in K. Define a finite extension L/K by:

$$L = K(\{\sqrt{d_i}, \sqrt{d_i'} : i = 1, \ldots, n\}).$$

The property (wB) implies that there exists $q_{n+1} \in K$ but not in S such that for $j = 1, 2, 3$, $P_j(q)$ is not a perfect square in L and $E^{P_j(q_{n+1})}/K$ is of positive rank. Put $d_{n+1} = P_1(q_{n+1})$ and $d_{n+1}' = P_2(q_{n+1})$. Then, $d_{n+1} \neq d_i$ in K^*/K^{*2} for $i = 0, 1, \ldots, n$ (because if $d_{n+1} = d_i k^2$ for some $k \in K$ then $\sqrt{d_{n+1}} = k\sqrt{d_i} \in L$) and similarly $d_{n+1}' \neq d_i'$ and $d_{n+1} d_{n+1}' \neq d_i d_i'$ in K^*/K^{*2} for $i = 0, 1, \ldots, n$. Hence all the elements $(d_i, d_i', d_i d_i') \in K^3$ are pairwise distinct in $(K^*/K^{*2})^3$, for $i = 1, \ldots, n, n+1$. □

As a consequence of the two previous results we obtain the following important corollary which will be useful:

Corollary 2.5. *The property* (B) *implies the property* (A)*.*

3. Results on twists

3.1. **Conditional results.** We begin by showing that, if we assume the parity conjecture then all elliptic curves over $\mathbb{Q}$ satisfy the property (A).

Conjecture 3.1 (Parity Conjecture)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $W(E/\mathbb{Q})$ be the root number of $E/\mathbb{Q}$. Then $W(E/\mathbb{Q}) = (-1)^{rank(E(\mathbb{Q}))}$.*

We will need the following result by D. Rohrlich on the behaviour of the root number in families of elliptic curves (the reader may also be interested in [3], [10]). Here we state Rohrlich's result in [11] in a stronger way.

Theorem 3.2 (Rohrlich, [11, Theorem 2])**.** *Let $f(t) \in \mathbb{Q}[t]$ be a non-zero polynomial, define*

$$T^+ = \{t_0 \in \mathbb{Q} : f(t_0) \neq 0 \text{ and } W(E^{f(t)}/\mathbb{Q}) = +1\}$$

and similarly define T^-. One of two mutually exclusive alternatives hold:

(1) *There exist a finite set of (bad) primes $p \in S$ and open sets U_p^+ and U_p^- of $\mathbb{Q}$ (for the p-adic topology of $\mathbb{Q}$) such that the sets T^+ and T^- contain the intersection $\bigcap_{p\in S} U_p^+$ or $\bigcap_{p\in S} U_p^-$ respectively. In particular T^+ and T^- are both dense in $\mathbb{R}$; or*
(2) *One of the sets $T^\pm$ is $\{t_0 \in \mathbb{Q} : f(t_0) > 0\}$ and the other is $\{t_0 \in \mathbb{Q} : f(t_0) < 0\}$.*

The following result is an extension of Corollary 2.5 of [8]:

Proposition 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 [8, 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. □

We will need the following lemma from [12] to prove Theorem 3.5 below and in Section 4 later.

Lemma 3.4. *Suppose E/K is an elliptic curve defined by $y^2 = g(x)$. Then for every nonconstant $h \in K(t)$ the twist $E^{g(h(t))} : g(h(t))y^2 = g(x)$ is of positive rank over $K(t)$. Moreover, if $E^{p(t)}$ is a twist of positive rank over $K(t)$ then there is some $h \in K(t)$ such that $E^{p(t)}$ is isomorphic (over $K(t)$) to $E^{g(h(t))}$.*

Proof. See [12, Lemma 2.3, Remark 2.4]. The twist $E^{g(h(t))}$ has a point $(h(t), 1)$, which is non-constant, therefore it is not a torsion point.

If $E^{p(t)}$ is of positive rank then there is a point of infinite order $(h(t), k(t))$, with $h, k \in K(t)$, such that $p(t)k(t)^2 = g(h(t))$. Thus, the twists $E^{p(t)}$ and $E^{g(h(t))}$ are isomorphic. □

As a consequence of Proposition 3.3, we obtain the conditional result:

Theorem 3.5. *If the parity conjecture holds, then every elliptic curve $E/\mathbb{Q}$ satisfies the property* (A).

Proof. Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = g(x)$ where $g(x)$ is a monic cubic polynomial in $\mathbb{Q}[x]$. By Theorem 2.4, it suffices to show that $E/\mathbb{Q}$ satisfies the property (wB).

Note that the twist $E^{g(t)}$ is of positive rank over $\mathbb{Q}(t)$ by Lemma 3.4. Hence there is a finite set $S \subset \mathbb{Q}$ such that $E^{g(t_0)}$ is of positive rank for all $t_0 \notin S$, by Silverman's specialization theorem. Put $P_1(t) = g(t)$, $P_2(t) = g(t + 1)$ and $P_3(t) = g(t)g(t + 1)$. Since $g(x)$ has distinct roots, P_1, P_2 and P_3 are not in $\mathbb{Q} \cdot (\mathbb{Q}[t])^2$ (and so each one has a zero of odd multiplicity) and $E^{P_1(t)}$ and $E^{P_2(t)}$ are of positive rank over $\mathbb{Q}(t)$.

Consider $E^{P_3(t)}$. Let $S' = \{t_0 \in \mathbb{Q} : t_0 \text{ or } t_0 + 1 \in S\}$. By the discussion above, for all $t_0 \notin S'$, both $E^{g(t_0)}$ and $E^{g(t_0+1)}$ are of positive rank. We claim that the fact that $g(x)$ is a monic cubic polynomial implies that both sets $P_3^+ = \{t_0 \in \mathbb{Q} : P_3(t_0) > 0\}$ and $P_3^- = \{t_0 \in \mathbb{Q} : P_3(t_0) < 0\}$ are infinite. Indeed, let $\alpha_1, \alpha_2 \in \mathbb{R}$ be respectively the smallest and largest real roots of $g(x)$, so that $\alpha_1 \leq \alpha_2$. Then $g(x) > 0$ and $P_3(x) > 0$ for all $x > \alpha_2$, thus P_3^+ is infinite (and contains an open set of $\mathbb{Q}$ for the ordinary topology). Moreover, since E/K is non-singular, α_1 is a simple zero of $g(x)$ and, since $g(x)$ is monic, $g(x) < 0$ for all $x < \alpha_1$ and there is $0 < \delta < 1$ such that $g(x) > 0$ for $\alpha_1 < x < \alpha_1 + \delta$. Then for all $t_0 \in \{t_0 \in \mathbb{Q} : \alpha_1 - 1 < t_0 < \alpha_1 - 1 + \delta\}$ one has $g(t_0) < 0$, $g(t_0 + 1) > 0$ and $P_3(t_0) < 0$. Hence P_3^- is infinite as well (and contains an open set of $\mathbb{Q}$ for the ordinary topology).

Let $L/\mathbb{Q}$ be an arbitrary finite separable extension. Let

$$H = \{t \in \mathbb{Q} : P_j(t) \text{ is not a perfect square in } L, \text{ for } j = 1, 2, 3\}.$$

Then, by Lemma 2.1, H is a Hilbert set of $\mathbb{Q}$. In the above, we have shown that both P_3^+ and P_3^- contain non-empty open sets of $\mathbb{Q}$ for the ordinary topology. By Theorem 3.2 and Proposition 3.3, regardless of what alternative occurs in Theorem 3.2, there are infinitely many $t_0 \in H$ such that $E^{P_3(t_0)}/\mathbb{Q}$ has root number -1 and therefore, of positive rank if the parity conjecture holds and $P_j(t_0)$ is not a square in L for $j = 1, 2, 3$.

Hence $E/\mathbb{Q}$ satisfies the property (wB), and therefore (A), if the parity conjecture holds. □

3.2. **Unconditional results.** In this subsection, we show examples of elliptic curves which satisfy the properties (A) and (B), without assuming the parity conjecture. The first result is an application of Proposition 4 of [6]:

Proposition 3.6. *Let K be a number field and let E/K be an elliptic curve such that all 2-torsion points are K-rational, given by $y^2 = x^3 + ax + b$ with $a, b \in K$. There exist polynomials $f(t), g(t), h(t) \in K[t]$ and non-zero constants $c, d \in K$ such that the twists:*

$$X_t^1 : cf(t)g(t)y^2 = x^3 + ax + b,$$
$$X_t^2 : df(t)h(t)y^2 = x^3 + ax + b,$$
$$X_t^3 : cdg(t)h(t)y^2 = x^3 + ax + b,$$

are pairwise non-isomorphic and of rank ≥ 1 over $K(t)$. In particular, E/K satisfies the properties (A) *and* (B).

Proof. Let K and E/K be as in the statement of the proposition. In [6], Prop 4., Im shows that there exist polynomials $f(t), g(t), h(t) \in K[t]$, such that $f \cdot g$, $f \cdot h$ and $g \cdot h$ are not in $K \cdot (K[t])^2$ and non-zero constants $c, d \in K$

such that the hyperelliptic curves defined by

$$X_1 : y^2 = cf(x)g(x),$$
$$X_2 : y^2 = df(x)h(x),$$
$$X_3 : y^2 = cdg(x)h(x),$$

map onto E/K via K-morphisms $\phi_i : X_i \to E$, for $i = 1, 2, 3$. More concretely, all three morphisms ϕ_i are of the form $\phi_i(x, y) = (\alpha_i(x), \beta_i(x)y)$, where $\alpha_i(x), \beta_i(x)$ are in $K(x)$, for $i = 1, 2, 3$. Now define twists of E/K by

$$X_t^1 : cf(t)g(t)y^2 = x^3 + ax + b,$$
$$X_t^2 : df(t)h(t)y^2 = x^3 + ax + b,$$
$$X_t^3 : cdg(t)h(t)y^2 = x^3 + ax + b.$$

Then X_t^i has a rational point $(\alpha_i(t), \beta_i(t))$ defined over $K(t)$ which can be verified to be non-torsion. Notice also that X_t^3 is trivially isomorphic to the twist by $cdf^2(t)g(t)h(t)$. Hence E/K satisfies the property (B) and, as a consequence of Corollary 2.5, also satisfies the property (A). □

Before we proceed, it is worth pointing out that the properties (A) and (B) are isogeny-invariant. In other words, E/K satisfies one of these two properties if and only if all the curves in the same isogeny class satisfy the same property. Indeed, let $E/K : y^2 = f(x)$ and $E'/K : y^2 = g(x)$ be elliptic curves and let $\phi : E \to E'$ be an isogeny, defined by $\phi(x, y) = (\phi_x(x, y), \phi_y(x, y))$, where ϕ_x, ϕ_y are rational functions in $K(x, y)$. Since $\phi(-P) = -\phi(P)$ for any $P \in E(K)$, the function ϕ_x is even in the variable y and ϕ_y is an odd function in y. In particular, if $a(t) \in K(t)$ then $\phi_x(x, \sqrt{a(t)}y) \in K(x, y, t)$ and $\phi_y(x, \sqrt{a(t)}y)/\sqrt{a(t)} \in K(x, y, t)$. Hence, for any $a(t) \in K(t)$, the isogeny ϕ induces an isogeny $\phi^{a(t)} : E^{a(t)} \to E'^{a(t)}$ over K defined by

$$\phi^{a(t)}(x, y) = \left(\phi_x(x, \sqrt{a(t)}y), \frac{\phi_y(x, \sqrt{a(t)}y)}{\sqrt{a(t)}}\right).$$

Finally, if $a(t), b(t) \in K(t)$ and $E^{a(t)}$, $E^{b(t)}$ and $E^{ab(t)}$ are of rank ≥ 1 over $K(t)$, so are $E'^{a(t)}$, $E'^{b(t)}$ and $E'^{ab(t)}$, because isogenous curves have the same rank over any finite extension of K (since the kernel of an isogeny is finite).

As a consequence of Proposition 3.6 and the previous discussion, we obtain the following result.

Corollary 3.7. *Let K be a number field. Then the elliptic curve E/K defined by $y^2 = x^3 + ax^2 + c^2x$ for some $a, c \in K$ satisfies the properties* (A) *and* (B).

Proof. Note that $c(a^2 - 4c^2) \neq 0$ for the non-singularity of an elliptic curve.

An elliptic curve of the form $E/K : y^2 = x^3 + ax^2 + c^2x$ is 2-isogenous to the elliptic curve $E'/K : y^2 = x^3 - 2ax^2 + (a^2 - 4c^2)x$, via:

$$\phi : E \to E', \quad \phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(c^2 - x^2)}{x^2} \right).$$

Moreover $E'[2]$ is K-rational since $x^3 - 2ax^2 + (a^2 - 4c^2)x = x(x - (a - 2c))(x - (a + 2c))$. Thus, by Proposition 3.6, both E'/K and E/K satisfy the desired properties. □

Proposition 3.8. *Let K be a number field and let E/K be an elliptic curve with a Weierstrass equation $y^2 = x(x^2 - k)$ where $k \in K$ satisfies $1 + k = e^2 + f^2$ for some $e, f \in K$. Then E/K satisfies the properties* (A) *and* (B)*.*

Proof. Let K, k and E be as in the statement of the proposition and put $g(x) = x^2 - k$. Notice that the case $k = -1$ (and $e = f = 0$) is covered by Corollary 3.7 (by setting $a = 0$ and $c = 1$), so we may assume that $k \neq -1$ and $e^2 + f^2 \neq 0$. We define a curve C/K with equation:

$$C : g(uv) - g(u)g(v) = 0$$

and notice that C is a conic given explicitly by $u^2 + v^2 - (1 + k) = 0$. Since $1 + k = e^2 + f^2$, the curve C has a point defined over K and, therefore, there are infinitely many solutions over K which can be parametrized as follows:

$$P_t = \left(\frac{et^2 - 2ft - e}{t^2 + 1}, \frac{-ft^2 - 2et + f}{t^2 + 1} \right), \quad t \in K.$$

We define polynomials

$$h(x) = x^2 + 1, \quad g_1(x) = ex^2 - 2fx - e \quad \text{and} \quad g_2(x) = -fx^2 - 2ex + f.$$

Notice that the discriminants of the polynomials g_1, g_2, h are, respectively, given by $\Delta_{g_1} = \Delta_{g_2} = 4(e^2 + f^2) \neq 0$ and $\Delta_h = -4$. Thus, the roots (over $\mathbb{C}$) of $g_1(x)$ (resp. $g_2(x)$ or $h(x)$) are distinct. Moreover, it is easily checked that the roots of $g_1(x)$ and $g_2(x)$ are also distinct (otherwise $(0, 0) \in C(K)$ and $1 + k = 0$), and different from the roots of $h(x)$. Therefore, the roots of $g_1(x)$ and $h(x)$ also differ from those of $(g_1(x)^2 - kh(x)^2)$. Similarly, the roots of $g_2(x)$, $h(x)$ and $(g_2(x)^2 - kh(x)^2)$ are all distinct, and so are the roots of g_1, g_2 and $(g_1(x)^2 g_2(x)^2 - kh^4(x))$.

We define polynomials $P_1(x), P_2(x)$ and $P_3(x)$ by:

$$\begin{aligned} P_1(x) &= h(x)g_1(x)(g_1(x)^2 - kh(x)^2), \\ P_2(x) &= h(x)g_2(x)(g_2(x)^2 - kh(x)^2), \\ P_3(x) &= g_1(x)g_2(x)(g_1(x)^2 g_2(x)^2 - kh(x)^4). \end{aligned}$$

Thus, by the remarks above, none of the polynomials $P_i(x) \in K[x]$ can be a square in $\mathbb{C}[x]$ and, in fact, they are not in $K \cdot (K[t])^2$. Moreover, notice that in $K(x)/K(x)^2$, the polynomials $P_1(x)$, $P_2(x)$ and $P_3(x)$ are equivalent

to

$$\widehat{P}_1(x) = \frac{g_1(x)}{h(x)}\left(\frac{g_1(x)^2}{h(x)^2}-k\right) = \frac{g_1(x)}{h(x)}g\left(\frac{g_1(x)}{h(x)}\right), \tag{1}$$

$$\widehat{P}_2(x) = \frac{g_2(x)}{h(x)}\left(\frac{g_2(x)^2}{h(x)^2}-k\right) = \frac{g_2(x)}{h(x)}g\left(\frac{g_2(x)}{h(x)}\right), \tag{2}$$

$$\widehat{P}_3(x) = \frac{g_1(x)g_2(x)}{h^2(x)}\left(\frac{g_1(x)^2g_2(x)^2}{h(x)^4}-k\right) \tag{3}$$

$$= \frac{g_1(x)g_2(x)}{h^2(x)}g\left(\frac{g_1(x)g_2(x)}{h^2(x)}\right) = \widehat{P}_1(x)\widehat{P}_2(x) \tag{4}$$

where in the last equality we have used the fact that $g(uv) = g(u)g(v)$ whenever $(u, v) \in C$. Finally, we define twists of E over $K(t)$ by the equations:

$$E_t^1 : P_1(t)y^2 = x(x^2-k), \quad E_t^2 : P_2(t)y^2 = x(x^2-k), \quad E_t^3 : P_3(t)y^2 = x(x^2-k)$$

and notice that by equations (1) through (3), the curves E_t^i, for $i = 1, 2, 3$, are isomorphic to $\widehat{E}_t^i : \widehat{P}_i(t)y^2 = x(x^2 - k)$ over $K(t)$ and E_t^3 is isomorphic to $P_1(t)P_2(t)y^2 = x(x^2 - k)$ over $K(t)$ by equation (4). Clearly, again by the numbered equations above, the curves $\widehat{E}_t^i$ have a rational point which can be easily checked to be non-torsion over $K(t)$. Therefore, the curves E_t^i, $i = 1, 2, 3$, are of positive algebraic rank over $K(t)$. □

Remark 3.9. *Let $E : y^2 = x(x^2 - k)$ be an elliptic curve as before. Notice that if $K = \mathbb{Q}$ and k, e, f are integers, then the twists E_t^i are defined over $\mathbb{Z}[t]$ and, upon specialization at $t \in \mathbb{Z}$, we obtain, generically, twists $E^d, E^{d'}$ and $E^{dd'}$ with rank ≥ 1 and defined over $\mathbb{Z}$.*

Proposition 3.10. *Let $E/K : y^2 = x^3 + k$ be an elliptic curve, with $k \in K$, $k \neq 1$, such that $E(K)$ is trivial. Further suppose that the elliptic curve $x^3 + y^3 = 1 - k$ contains a point of infinite order. Then E/K satisfies the property* (A).

Proof. Put $g(x) = x^3 + k$ and define a curve C/K by:

$$C/K : g(uv) - g(u)g(v) = 0$$

and notice that the equation defining C is equivalent to $x^3 + y^3 = 1 - k$. Therefore, if $k \neq 1$ then C/K is an elliptic curve. Suppose that $C(K)$ contains a point $P = (x_1, y_1)$ of infinite order and, for every $n \geq 1$, put $nP = (x_n, y_n)$. Then, for every $n \geq 1$, consider the three twists of E given by

$$(x_n^3 + k)y^2 = g(x),\ (1 - x_n^3)y^2 = g(x),\ (x_n^3 + k)(1 - x_n^3)y^2 = g(x) \tag{5}$$

and note that

$$(x_n^3 + k)(1 - x_n^3) = (x_n^3 + k)(y_n^3 + k) = g(x_n)g(y_n) = g(x_ny_n).$$

Moreover, notice that since we are assuming that $E(K)$ is trivial, the elements $g(x_n), g(y_n), g(x_ny_n)$ cannot be squares in K. Therefore, the (infinitely many) distinct twists given in Eq. (5) are all of rank ≥ 1 over K and

they are of the form $E^d, E^{d'}, E^{dd'}$. The fact that there are infinitely many of these (d, d', dd') which are pairwise distinct in $(K^*/K^{*2})^3$ follows from results in Section 5, in particular Lemma 5.5 and an argument similar to the proof of Corollary 2.5. □

4. The underlying algebraic variety

Even though the methods of Proposition 3.8 and Proposition 3.10 may seem 'ad-hoc', it is worth remarking that, in fact, in all cases there is a certain algebraic variety inherently associated to the question of whether an elliptic curve E/K satisfies the properties (A) or (B), and which plays the role of C/K in the proofs of the propositions given in Section 2.

Definition 4.1. *Let K be a number field and let E/K be an elliptic curve given by $y^2 = g(x)$, for some monic cubic polynomial $g(x) \in K[x]$. Let $\mathbb{A}^4(K)$ be the four-dimensional affine space over K. We define an algebraic variety V_E/K in $\mathbb{A}^4(K)$ given by the equation:*

$$V_E/K : g(x_1)g(x_2) = g(x_3)x_4^2.$$

Lemma 4.2. *Suppose E/K is an elliptic curve defined in projective coordinates by $ZY^2 = g(X/Z)Z^3$, where $g(x)$ is a monic cubic polynomial in $K[t]$. Then, for every non-constant $k(t) \in K(t)$ the rational function $g(k(t))$ is not in $K \cdot (K(t))^2$.*

Proof. Let $k(t) \in K(t)$ be non-constant and suppose, for a contradiction, that there is $h(t) \in K(t)$ and non-zero $d \in K$ with $g(k(t)) = d \cdot (h(t))^2$. Then we obtain a non-constant rational map:

$$\psi : \mathbb{P}^1(K) \to E^d/K$$

given by $\psi(t) = [k(t), h(t), 1]$. But this is clearly impossible because the genus of $\mathbb{P}^1(K)$ is 0 and the genus of E^d/K is 1. □

Theorem 4.3. *The elliptic curve E/K satisfies the property* (B) *if and only if $V_E(K(t))$ has a point with non-constant coordinates $x_1(t)$, $x_2(t)$, $x_3(t) \in K(t)$ with $x_i(t) \neq x_j(t)$ for $i \neq j$, $1 \leq i, j \leq 3$.*

Proof. Suppose first that E/K satisfies property (B), i.e. there are polynomials $P_1(t), P_2(t)$, $P_3(t) = P_1(t)P_2(t)$, not in $K \cdot (K[t])^2$, such that E^{P_1}, E^{P_2} and $E^{P_1P_2}$ are all of positive rank over $K(t)$. Then, by the previous lemma, there exist $x_i(t), y_i(t) \in K(t)$, for $i = 1, 2, 3$, such that $g(x_i(t)) = P_i(t)y_i(t)^2$ (thus $g(x_i(t))$ is not in $K \cdot (K(t))^2$ and $x_i(t)$ is non-constant) and E^{P_1}, E^{P_2} and $E^{P_1P_2}$ are isomorphic to $E^{g(x_1(t))}, E^{g(x_2(t))}$ and $E^{g(x_3(t))}$ respectively. Hence, there exists $x_4(t) \in K(t)$ such that

$$g(x_1(t))g(x_2(t)) = g(x_3(t))x_4(t)^2. \tag{6}$$

Thus, $(x_1(t), x_2(t), x_3(t), x_4(t)) \in V_E(K(t))$ with non-constant coordinates $x_1(t), x_2(t)$ and $x_3(t)$. Moreover, the fact that $g(x_i(t)) \notin K \cdot (K(t))^2$ together with the equation (6), show that $x_i(t) \neq x_j(t)$ for $i \neq j$, $1 \leq i, j \leq 3$.

Conversely, if $(x_1(t), x_2(t), x_3(t), x_4(t)) \in V_E(K(t))$ with pairwise distinct non-constant x_1, x_2, x_3, then by Lemma 4.2 and the equation (6), it is clear that if we set $P_1 = g(x_1)$ and $P_2 = g(x_2)$, then P_1, P_2 and P_1P_2 are not in $K \cdot (K(t))^2$, and by Lemma 3.4, the twists E^{P_1}, E^{P_2} and $E^{P_1P_2}$ are all of positive rank. □

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 E/K satisfies the property (B) and, therefore, the variety V_E has a point $(x_1(t), x_2(t), x_3(t), x_4(t))$ with non-constant coordinates $x_1(t)$, $x_2(t)$, $x_3(t) \in K(t)$ with $x_i(t) \neq x_j(t)$ for $i \neq j$, $1 \leq i, j \leq 3$.

Theorem 4.5. *The curve E/K satisfies the property* (A) *if and only if V_E has infinitely many K-rational points $(x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}) \in K^4$, $i \geq 1$, such that:*

1. *For all $i \geq 1$, $x_{s,i} \neq x_{t,i}$ in K and $g(x_{s,i}) \neq g(x_{t,i})$ in K^*/K^{*2}, for all $s \neq t$, $1 \leq s, t \leq 3$.*
2. *For all $i \neq j$ and $1 \leq s \leq 3$, $g(x_{s,i}) \neq g(x_{s,j})$ in K^*/K^{*2}.*

Proof. Notice that if there is $d \in K$ such that E^d is of positive rank, then $E^d(K)$ has a point of infinite order (a, b) defined over K such that $g(a) = db^2$ and E^d is isomorphic to $E^{g(a)}$. If E/K satisfies (A) then d is a square for at most one triple (d, d', dd'), and similarly d' and dd' are squares for at most one triple each. If $d_1, d_2, d_3 = d_1d_2$ are all non-squares of K and $g(a_s) = d_sb_s^2$, for $s = 1, 2, 3$, then for $s \neq t$, one has $a_s \neq a_t$ in K and $g(a_s) \neq g(a_t)$ in K^*/K^{*2}. Further, if $(d_1, d_2, d_3 = d_1d_2) \neq (d_1', d_2', d_3' = d_1'd_2')$ in $(K^*/K^{*2})^3$ then there are a_s, b_s, a_s', b_s', for $s = 1, 2, 3$ such that $g(a_s) = d_sb_s^2$, $g(a_s') = d_s'(b_s')^2$ and, therefore, $g(a_s) \neq g(a_s')$ in K^*/K^{*2}. All the previous statements when put together show that if E/K satisfies the property (A) then $V_E(K)$ has infinitely many K-rational points satisfying (1) and (2).

Next we prove the converse. Suppose V_E has infinitely many K-rational points $(x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}) \in K^4$, $i \geq 1$, satisfying (1) and (2) and

$$g(x_{1,i})g(x_{2,i}) = g(x_{3,i}) \cdot (x_{4,i})^2. \tag{7}$$

Since for all $i \neq j$ and for $s = 1, 2, 3$, $g(x_{s,i}) \neq g(x_{s,j})$ in K^*/K^{*2}, we can conclude that there is at most one i_0, one i_1 and one i_2 such that $g(x_{1,i_0}) \in K^2$, $g(x_{2,i_1}) \in K^2$ and $g(x_{3,i_2}) \in K^2$, and by (2), i_0, i_1, i_2 are all distinct (if they exist).

Further, the twist $E^{g(t)}/K(t)$ is of positive rank, by Lemma 3.4. By Silverman's specialization theorem there is a finite set $S \subset K$ such that for all $k \notin S$, the curve $E^{g(k)}/K$ is of positive rank. Let S_I be the set of all $i \geq 1$ such that $x_{s,i} \in S$ for some $s \in \{1, 2, 3\}$. Thus, by (1), the set S_I is necessarily finite. Finally, for $i \geq 1$ with $i \notin S_I \cup \{i_0, i_1, i_2\}$ the infinite set of all $(d_i, d_i', d_i d_i')$ with $d_i = g(x_{1,i})$ and $d_i' = g(x_{2,i})$, makes E/K satisfy the property (A). □

5. Application to large fields

Before we state the first lemma, we set some notation. Let K be a number field and let $G_K = \mathrm{Gal}(\overline{K}/K)$. For a natural number $n \geq 1$, and $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in G_K^n$ we define $\overline{K}^{(\sigma)} = \cap_i \overline{K}^{\sigma_i}$.

Lemma 5.1. *Let $n \geq 1$ be an integer and let $a_1, \ldots, a_{n+1}$ be elements in a number field K. Let $L = K(\sqrt{a_1}, \ldots, \sqrt{a_{n+1}})$ be a number field with $[L : K] = 2^{n+1}$, and let $\sigma = (\sigma_1, \ldots, \sigma_n)$ be an n-tuple in G_K^n with $\sigma_i \neq \sigma_j$ for $i \neq j$. Then there is at least one quadratic extension K'/K with $K \subset K' \subset L \cap \overline{K}^{(\sigma)}$.*

Proof. Let $n \geq 1$ be an integer and let L/K and $(\sigma) \in G_K^n$ be as in the statement of the lemma. For a quadratic extension M/K we define the signature of M with respect to (σ) as $M_{(\sigma)} = (\delta_1, \ldots, \delta_n)$ where, for $i = 1, \ldots, n$, the number $\delta_i = 1$ if M is fixed by σ_i and $\delta_i = -1$ otherwise. Notice that there are 2^n possible signatures for a given quadratic extension M/K. On the other hand, there are precisely

$$\binom{n+1}{1} + \binom{n+1}{2} + \cdots + \binom{n+1}{n+1} = 2^{n+1} - 1$$

distinct quadratic extensions of K contained in L, and $2^{n+1} - 1 > 2^n$ since $n \geq 1$. Thus, by the pigeonhole principle, there are b_1 and $b_2 \in K$ and two distinct quadratic extensions of K, $M_1 = K(\sqrt{b_1})$ and $M_2 = K(\sqrt{b_2})$, with $M_1, M_2 \subset L$ with the same signature with respect to (σ). Hence, the signature of $K' = K(\sqrt{b_1 b_2})$ is $K'_{(\sigma)} = (M_1)_{(\sigma)} \cdot (M_2)_{(\sigma)} = (\delta_1^2, \ldots, \delta_n^2) = (1, \ldots, 1)$ and therefore K' is fixed by (σ). Moreover, the fact that $M_1 \neq M_2$ ensures that K'/K is a quadratic extension, contained in L, as desired. □

For any $n \geq 2$, the property (B) of an elliptic curve E/K can be generalized to the following property (B_n).

> (B_n) There exist polynomials $P_1, \ldots, P_n \in K[t]$ such that every polynomial of the form:
>
> $$Q(t) = \prod_{i=1}^{n} P_i(t)^{e_i} \quad \text{with } e_i = 0 \text{ or } 1$$
>
> has a zero (over $\overline{K}$) of odd degree and the twist $E^{Q(t)}$ is of positive rank over $K(t)$.

Of course, the property (B_2) is equivalent to the property (B). Now we are ready to state the main theorem:

Theorem 5.2. *Let K be a number field, K^{ab} the maximal abelian extension of K, let $n \geq 1$ be a fixed integer and let E/K be an elliptic curve satisfying the property (B_{n+1}). Then for each $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in \mathrm{Gal}(\overline{K}/K)^n$, the rank of $E((K^{ab})^{(\sigma)})$ is infinite, therefore $E(\overline{K}^{(\sigma)})$ is infinite.*

Proof. The idea of the proof is a generalization of the proof of Corollary 2.5. We inductively construct quadratic extensions K_n of K and points $T_n \in E(K_n)$ as follows. Let E/K be an elliptic curve satisfying the property (B_{n+1}) and let $P_1(t), \ldots, P_{n+1}(t) \in K[t]$ be polynomials satisfying the claimed properties. Let S be the set of all polynomials of the form

$$Q(t) = \prod_{i=1}^{n} P_i(t)^{e_i} \quad \text{with } e_i = 0 \text{ or } 1.$$

By assumption, every polynomial $Q(t) \in S$ has a zero of odd degree, which implies that the extension $K(\sqrt{P_1(t)}, \ldots, \sqrt{P_{n+1}(t)})/K$ is of degree 2^{n+1}.

Now, put $F_0 = K$. For each $k \geq 1$ we apply Lemma 2.1 to find a_k such that, for all $Q \in S$, the value $Q(a_k)$ is not a square in the compositum $F_k = K_1 K_2 \cdots K_{k-1}$. In particular, since $Q(a_k)$ is not a square in F_k (for any $Q \in S$), the field $F_k(\sqrt{P_1(a_k)}, \ldots, \sqrt{P_{n+1}(a_k)})$ is an extension of F_k of degree 2^{n+1}.

We define $L_k = K(\sqrt{P_1(a_k)}, \ldots, \sqrt{P_{n+1}(a_k)})$ which is an extension of K of degree 2^{n+1}, and let $(\sigma) \in G_K^n$ be arbitrary. By Lemma 5.1, there exists a quadratic extension K_k/K, such that $K \subset K_k \subset L_k$, which is fixed by (σ). Thus (σ) fixes at least one of $\sqrt{Q(a_k)}$, for some $Q \in S$, and in fact $K_k = K(\sqrt{Q(a_k)})$. Since the curve $E^{Q(a_k)}$ has a K-rational non-torsion point, the elliptic curve E has a non-torsion point T_k defined over K_k. Moreover, the linear disjointness of the quadratic extensions K_k over K (which is guaranteed by the fact that $F_k(\sqrt{P_1(a_k)}, \ldots, \sqrt{P_{n+1}(a_k)})/F_k$ is an extension of degree 2^{n+1} for every $k \geq 1$) implies that the points T_n are linearly independent in $E((K^{\mathrm{ab}})^{(\sigma)})$. Hence $E((K^{\mathrm{ab}})^{(\sigma)})$ has infinite rank and so does $E(\overline{K}^{(\sigma)})$. □

As a corollary of Theorem 5.2 and propositions 3.6, 3.8 and corollary 3.7, we obtain the following result.

Corollary 5.3. *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 E/K satisfies the property $(B)(=(B_2))$ and, therefore, for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the rank of $E((K^{ab})^{\sigma})$ is infinite, so the rank of $E(\overline{K}^{\sigma})$ is infinite.

As a consequence of the methods in the proof of Theorem 5.2 and Theorem 3.5 we obtain:

Theorem 5.4. *Let $E/\mathbb{Q}$ be an elliptic curve. If the parity conjecture holds (over $\mathbb{Q}$) then for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the rank of $E((\mathbb{Q}^{ab})^{\sigma})$ is infinite, therefore $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite.*

Proof. If the parity conjecture holds then, by Theorem 3.5, every elliptic curve over $\mathbb{Q}$ satisfies property (A), i.e. there are infinitely many triples $(d, d', dd') \in \mathbb{Q}^3$, pairwise distinct in $(\mathbb{Q}^*/\mathbb{Q}^{*2})^3$, such that the twists E^d, $E^{d'}$ and $E^{dd'}$ are all of positive rank over $\mathbb{Q}$. Moreover, for every finite extension $L/\mathbb{Q}$, the kernel of $\mathbb{Q}^*/\mathbb{Q}^{*2} \to L^*/L^{*2}$ is finite (use Hilbert's theorem 90, for example) and therefore there exist infinitely many (d, d', dd') as above such that d, d' and dd' are not squares in L. The proof can be finished now as in the proof of Theorem 5.2. □

Next, we show similar result for curves of the form $y^2 = x^3 + k$. We start with a lemma which is an analogue of Lemma 2.1.

Lemma 5.5. *Let K be a number field and let L/K be a finite extension. Let $0, -1 \neq k \in K$ be such that the elliptic curve $C : x^3 + y^3 = 1 - k$ has a point Q defined over K. Put $P_1(x) = x^3 + k$, $P_2(x) = 1 - x^3$, $P_3(x) = P_1(x)P_2(x) = k + (1-k)x^3 - x^6$. Then there are infinitely many $n \geq 1$ such that $P_1(x(nQ)), P_2(x(nQ))$ and $P_3(x(nQ))$ are not squares in L. Therefore, for such values of n, the field $L\left(\sqrt{P_1(x(nQ))}, \sqrt{P_2(x(nQ))}\right)$ is a biquadratic extension of L.*

Proof. Let L/K and C/K be as in the statement of the theorem. It is clear that all the roots of $P_1(x)$ and $P_2(x)$ are distinct. We claim that the sets $T_i = \{P_i(x(nQ)) = z^2 : z \in L\}$ are finite for $i = 1, 2, 3$. Suppose for a contradiction that T_1 is infinite. Then there exist infinitely many solutions to the system:

$$x^3 + y^3 = 1 - k, \quad z^2 = x^3 + k. \tag{8}$$

However, Eq. (8) defines a curve $\widehat{C}/K$ with a (ramified) map to C/K. By Hurwitz genus formula, the genus of $\widehat{C}$ is strictly greater than 1. Hence, by Faltings' theorem, $\widehat{C}(L)$ is finite and a contradiction occurs.

Similarly, Faltings' theorem implies that T_2 and T_3 are finite. Thus, $T = \{z \in L : P_i(x(nQ))$ is not a square for $i = 1, 2, 3\}$ is, in fact, infinite. □

Theorem 5.6. *Let K be a number field, K^{ab} the maximal abelian extension of K, and let $E : y^2 = x^3 + k$ be an elliptic curve, where $0, -1 \neq k \in K$ is such that $x^3 + y^3 = 1 - k$ has a point of infinite order defined over K. Then*

for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$*, the rank of* $E((K^{ab})^{\sigma})$ *is infinite, therefore* $E(\overline{K}^{\sigma})$ *is infinite.*

Proof. The proof is exactly the same than the proof of Theorem 5.2, where $P_i(x)$ are the polynomials defined in Lemma 5.5 and instead of Lemma 2.1 we make use of the results in Lemma 5.5. □

References

[1] G. Frey and M. Jarden, 'Approximation theory and the rank of abelian varieties over large algebraic fields', *Proc. London Math. Soc.* **28** (1974) 112-128.

[2] 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.

[3] H. A. Helfgott, 'On the behaviour of root numbers in families of elliptic curves', to appear, in the ArXiv: math.NT/0408141.

[4] B-H. Im, 'Heegner points and Mordell-Weil groups of elliptic curves over large fields', *Trans. Amer. Math. Soc.* to appear, arXiv: math NT/0411534.

[5] B-H. Im, 'Mordell-Weil groups and the rank of elliptic curves over large fields', *Canad. J. Math.* **58** (4) (2006), 796-819, arXiv: math NT/0411533.

[6] B-H. Im, 'The rank of elliptic curves with rational 2-torsion points over large fields', *Proc. Amer. Math. Soc.* **134** (2006), no. 6, 1623–1630.

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

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

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

[10] E. Manduchi, 'Root numbers of fiber of elliptic surfaces', *Compositio Mathematica*, tome 99, no. 1 (1995), p. 33-58.

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

[12] K. Rubin, A. Silverberg, 'Rank frequencies for quadratic twists of elliptic curves', *Experiment. Math.* 10, no. 4 (2001), 559570.

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

[14] A. Silverberg, 'The distribution of ranks in families of quadratic twists of elliptic curves', to appear in the *Proceedings of the Newton Institute Workshop on Ranks of Elliptic Curves and Random Matrix Theory*, London Mathematical Society Lecture Note Series, Cambridge University Press.

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

Department of Mathematics, Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul 156-756, South Korea

E-mail address: imbh@cau.ac.kr

Dept. of Math., 584 Malott Hall, Cornell University, Ithaca, NY 14853.

E-mail address: alozano@math.cornell.edu