PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 134, Number 6, Pages 1623–1630
S 0002-9939(05)08494-7
Article electronically published on December 15, 2005

THE RANK OF ELLIPTIC CURVES WITH RATIONAL 2-TORSION POINTS OVER LARGE FIELDS

BO-HAE IM

(Communicated by David E. Rohrlich)

ABSTRACT. Let K be a number field, $\overline{K}$ an algebraic closure of K, G_K the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$, K_{ab} the maximal abelian extension of K and E/K an elliptic curve defined over K. In this paper, we prove that if all 2-torsion points of E/K are K-rational, then for each $\sigma \in G_K$, $E((K_{ab})^\sigma)$ has infinite rank, and hence $E(\overline{K}^\sigma)$ has infinite rank.

Let K be a number field, $\overline{K}$ an algebraic closure of K, and $G_K := \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of $\overline{K}$ over K. Let E/K be an elliptic curve defined over K.

In [4], M. Larsen proved that for any E/K over K, there exists a nonempty open subset Σ of G_K such that for every $\sigma \in \Sigma$, the Mordell-Weil group $E(\overline{K}^\sigma)$ of E over the fixed field under σ has infinite rank.

It is natural to ask if such an open subset can be the whole Galois group G_K. We have a positive answer for elliptic curves defined over $\mathbb{Q}$ and for elliptic curves with certain rational points over the ground field. In [2], we proved that for any elliptic curve $E/\mathbb{Q}$, the rank of $E(\overline{\mathbb{Q}}^\sigma)$ is infinite for every $\sigma \in G_{\mathbb{Q}}$. Our approach in [2] is arithmetic: taking advantage of the modularity of elliptic curves over $\mathbb{Q}$ and the theory of complex multiplication, and constructing an infinite supply of rational points of E consisting of Heegner points. Also, in [1], we proved that for any elliptic curve E/K over a number field K with a K-rational point which is neither 2-torsion nor 3-torsion, the rank of $E(\overline{K}^\sigma)$ is infinite for every $\sigma \in G_K$. In [1], by a geometric approach, we constructed rational points, essentially by searching for sufficiently rational subvarieties of certain quotients of the n-fold product E^n of E.

This paper has been motivated by [1], [2] and [4]. Extending a method of M. Larsen [4], we prove in this paper that if all 2-torsion points of E/K are K-rational, then there are three hyperelliptic curves X_1, X_2, X_3 defined over K of genus 1, 3, and 3 respectively forming a biquadratic extension of $\mathbb{P}^1$ such that each admits a nonconstant K-morphism to E. By this result, we prove that if all 2-torsion points of E/K are K-rational, then for each $\sigma \in G_K$, $E((K_{ab})^\sigma)$ has infinite rank, where K_{ab} is the maximal abelian extension of K, hence $E(\overline{K}^\sigma)$ has infinite rank. Here, we argue by using Diophantine geometry as in [4], which is a completely different method from the one that we used in [2].

Received by the editors January 28, 2005.
2000 *Mathematics Subject Classification.* Primary 11G05.

We will need the following lemmas to prove Proposition 4 and we will use the notation in Lemma 2 in the proof of Proposition 4.

Lemma 1. *If w_1, w_2 and w_3 are distinct elements in K, then there exists an ordered triple (i,j,k) such that $\{i,j,k\} = \{1,2,3\}$ as sets, and $w_i + w_j - 2w_k \neq 0$ and $w_i + w_j - w_k \neq 0$.*

Proof. Without loss of generality, suppose $w_1 + w_2 - 2w_3 = 0$. Then if $w_1 + w_3 - 2w_2 = 0$ or $w_2 + w_3 - 2w_1 = 0$, then it implies that $w_3 = w_2$ or $w_3 = w_1$ respectively, which is a contradiction to distinct w_i's. So if $w_1 + w_2 - 2w_3 = 0$, then $w_1 + w_3 - 2w_2 \neq 0$ and $w_2 + w_3 - 2w_1 \neq 0$.

If $w_1 + w_3 - w_2 \neq 0$, the ordered triple $(i,j,k) = (1,3,2)$ satisfies the condition. If $w_1 + w_3 - w_2 = 0$, then similarly we show that $w_1 + w_2 - w_3 \neq 0$ and $w_2 + w_3 - w_1 \neq 0$. So the ordered triple $(i,j,k) = (2,3,1)$ satisfies the condition. □

Lemma 2. *For given distinct elements α, β and $\gamma \in K$ such that $\beta + \gamma - 2\alpha \neq 0$ and $\beta + \gamma - \alpha \neq 0$, suppose that there exist elements p, q, and s in K satisfying the following conditions* (1) *through* (7)*:*

(1) *p, q and s are all distinct,*

(2) $(p-q)^3 + (s-q)(p-s)[s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma)] \neq 0$,

(3) $(p-q)^3(\beta+\gamma-\alpha) + \alpha(s-q)(p-s)[s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma)] \neq 0$,

(4) $(p-q)^3\alpha + (\beta+\gamma-\alpha)(s-q)(p-s)[s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma)] \neq 0$,

(5) $(p-q)^3(\gamma-\alpha) + (\alpha-\beta)(s-q)(p-s)[s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma)] \neq 0$,

(6) $(p-q)^3(\beta-\alpha) + (\alpha-\gamma)(s-q)(p-s)[s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma)] \neq 0$,

(7) $s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma) \neq 0$.

Then let F and G be the left-hand sides of (2) *and* (3) *respectively, and put*

$t = \dfrac{G}{F}$,
$A = (\beta+\gamma-2\alpha)(s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma))$,
$B_1 = (t-\alpha)(s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma))(p+q)$,
$B_2 = (t-(\beta+\gamma-\alpha))(s^2(\alpha-\beta) + s(p-q)(2\gamma-\alpha-\beta) + pq(\beta-\alpha))$,
$C_1 = (t-\alpha)(s(\alpha-\beta) + p(\gamma-\alpha) + q(\beta-\gamma))pq$,
$C_2 = (t-(\beta+\gamma-\alpha))(s^2(p(\gamma-\beta) + q(\alpha-\gamma)) + spq(\beta-\alpha))$.

Define three polynomials in x:

$h_1(x) = A(t-\beta)x^2 - ((\gamma-\alpha)B_1 - (\alpha-\beta)B_2)x + ((\gamma-\alpha)C_1 - (\alpha-\beta)C_2)$,
$h_2(x) = A(t-\gamma)x^2 - ((\beta-\alpha)B_1 - (\alpha-\gamma)B_2)x + ((\beta-\alpha)C_1 - (\alpha-\gamma)C_2)$,
$h_3(x) = Ax^2 - (B_1 - B_2)x + (C_1 - C_2)$.

Then, $A \neq 0$ and $t \neq 0, \beta+\gamma, \beta, \gamma, \beta+\gamma-\alpha, \alpha$. In particular, the h_i are quadratic polynomials in x defined over K.

Proof. Conditions (3) through (6) imply that $t \neq 0, \beta+\gamma, \beta, \gamma$. Since $\beta+\gamma-2\alpha \neq 0$, conditions (1) and (7) imply that $t \neq \beta+\gamma-\alpha$ and $t \neq \alpha$. By condition (7) and the assumption that $\beta+\gamma-2\alpha \neq 0$, we see that $A \neq 0$.

Since $A \neq 0$ and $t \neq \beta, \gamma$ and t, A, B_1, B_2, C_1, C_2 are in K, the h_i are quadratic polynomials in x defined over K. □

Lemma 3. *For given distinct elements α, β and $\gamma \in K$ such that $\beta + \gamma - 2\alpha \neq 0$ and $\beta + \gamma - \alpha \neq 0$, there exist elements p, q, and $s \in K$ satisfying the following*

conditions:

p, q, *and* s *satisfy conditions* (1) *through* (7) *in Lemma* 2,

(8) p, q *and* s *are not equal to* $\dfrac{s(p(\gamma-\beta)+q(\alpha-\gamma))+pq(\beta-\alpha)}{s(\alpha-\beta)+p(\gamma-\alpha)+q(\beta-\gamma)}$,

(9) $\alpha(p-s)-\beta(q-s)\neq 0$,

(10) *each quadratic polynomial* $h_i(x)$ *defined in Lemma* 2 *has no double zero,*

(11) *any two of three quadratic polynomials* $h_i(X)$ *have no common zero,*

(12) p, q, *and* s *are not zeros of any of* $h_i(x)$.

Proof. Note that the set of triples (p, q, s) satisfying each condition from (1) through (9) is a finite number of intersections of nonempty open subsets in $\mathbb{A}^3(K)$ defined by the nontrivial polynomials over K given in each condition. So by the Hilbert irreducibility theorem [3, Chapter 9], the set of $(p, q, s) \in \mathbb{A}^3(K)$ satisfying conditions (1) through (9) is infinite.

For any p, q, s satisfying (1) through (9), Lemma 2 shows that $h_i(x)$ are quadratic polynomials. Let $D(h_i)$ denote the discriminant of the quadratic polynomial h_i. Then,

$D(h_1) = ((\gamma-\alpha)B_1-(\alpha-\beta)B_2)^2 - 4A(t-\beta)((\gamma-\alpha)C_1-(\alpha-\beta)C_2)$,
$D(h_2) = ((\beta-\alpha)B_1-(\alpha-\gamma)B_2)^2 - 4A(t-\gamma)((\beta-\alpha)C_1-(\alpha-\gamma)C_2)$,
$D(h_3) = (B_1-B_2)^2 - 4A(C_1-C_2)$.

We can show that the discriminants $D(h_i)$ are nontrivial rational functions in p, q and s. For example, we show[1] that the coefficients of the s^{10}-term in $F^2D(h_1)$ (resp. $F^2D(h_2)$, $F^2D(h_3)$) is $-(\alpha-\beta)^6(\beta+\gamma-2\alpha)^2$ (resp. $-(\alpha-\beta)^4(\alpha-\gamma)^2(\beta+\gamma-2\alpha)^2$, $-(\alpha-\beta)^4(\beta+\gamma-2\alpha)^2$), which is not zero by the assumption on α, β and γ. Also the h_i have the nontrivial relation $h_1 - h_2 = (\gamma-\beta)h_3$. The set of triples (p, q, s) at which $D(h_i)$ for some $i = 1, 2, 3$ vanishes or two of $h_1(x), h_2(x), h_3(x)$ have a common zero is a finite number of unions of proper Zariski closed sets in $\mathbb{A}^3(K)$. Its complementary set is a finite number of intersections of nonempty Zariski open sets, which is infinite by the Hilbert irreducibility theorem. Also, the set of triples (p, q, s) such that p, q, and s are not zeros of any $h_i(x)$ is also an intersection of three nonempty Zariski open sets, which is infinite. So the set of $(p, q, s) \in \mathbb{A}^3(K)$ satisfying conditions (1) through (12) is a finite number of intersections of nonempty Zariski open sets, hence it is nonempty (in fact, it is infinite). □

Proposition 4. *If all* 2*-torsion points of* E/K *are* K*-rational (i.e.* $E[2] \subset E(K)$*), then there exist three hyperelliptic curves* X_1, X_2, X_3 *defined over* K *of genus* $1, 3, 3$ *respectively which map onto* E *over* K *and are defined by*

$$(*) \qquad \begin{cases} X_1 : y^2 = af(x)g(x), \\ X_2 : y^2 = bf(x)h(x), \\ X_3 : y^2 = abg(x)h(x) \end{cases}$$

for some constants $a, b \in K$*, and some polynomials* $f, g, h \in K[x]$*. Hence the curves* X_1, X_2 *and* X_3 *form a biquadratic extension of* $\mathbb{P}^1$ *over* K.

[1]This can be shown by a moderate amount of direct calculation and has been verified using **Maple** (full documentation available upon request).

Proof. Let $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ be a Weierstrass equation of E. Here, α, β, and γ are distinct elements in K, since the 2-torsion points of E are K-rational. Then, by Lemma 1, we may assume that

$$\beta+\gamma-2\alpha \neq 0 \text{ and } \beta+\gamma-\alpha \neq 0. \tag{13}$$

The main strategy for proving the proposition is to construct three curves defined by

$X_1 : y^2 = a(x-p)(x-q)(x-s)(x-r)$,
$X_2 : y^2 = b(x-p)(x-q)(x-x_1)(x-x_2)(x-x_3)(x-y_1)(y-y_2)(y-y_3)$,
$X_3 : y^2 = ab(x-s)(x-r)(x-x_1)(x-x_2)(x-x_3)(x-y_1)(y-y_2)(y-y_3)$

together with three dominant morphisms $\phi_i : X_i \to E$ for $i = 1, 2, 3$ defined by K-rational functions which map the set of ramification points of each X_i over $\mathbb{P}^1$ onto the set of ramification points of E over $\mathbb{P}^1$ as follows:

$$\phi_1 : (p,0) \mapsto (\alpha,0), \quad (q,0) \mapsto (\beta,0), \quad (r,0) \mapsto (\gamma,0), \text{ and } (s,0) \mapsto \infty, \tag{14}$$

$$\begin{aligned}\phi_2 : &(p,0),(q,0) \mapsto (\alpha,0), \quad (x_1,0),(x_2,0) \mapsto (\beta,0),\\ &(y_1,0),(y_2,0) \mapsto (\gamma,0), \text{ and } (x_3,0),(y_3,0) \mapsto \infty,\end{aligned} \tag{15}$$

$$\begin{aligned}\phi_3 : &(r,0),(s,0) \mapsto (\alpha,0), \quad (x_1,0),(x_2,0) \mapsto (\gamma,0),\\ &(y_1,0),(y_2,0) \mapsto (\beta,0), \text{ and } (x_3,0),(y_3,0) \mapsto \infty.\end{aligned} \tag{16}$$

First, under the assumption (13), by Lemma 3, we can choose $p, q, s \in K$ satisfying conditions (1) through (12).

Then we find X_1 and a dominant morphism $\phi_1 : X_1 \to E$ satisfying (14) in terms of the given p, q, s, α, β and γ. Since X_1 has genus 1 and ϕ_1 sends $(s,0) \in X_1$ to $\infty \in E$ as a dominant map, we try to set $\phi_1(x,y) = \left(\dfrac{c_1x+c_0}{(x-s)}, \dfrac{c_3}{(x-s)^2}y\right)$ as rational functions for some constants c_i and try to find constants r and c_i in terms of p, q, s, α, β and γ. For ϕ_1 to satisfy condition (14), we need three relations,

$$c_1p+c_0 = \alpha(p-s), \qquad c_1q+c_0 = \beta(q-s), \qquad c_1r+c_0 = \gamma(r-s). \tag{17}$$

Also, for ϕ_1 to be a dominant morphism to E, the following must be valid:

$$Z(\phi_1(x,y)) = 0, \text{ where } Z(x,y) = y^2-(x-\alpha)(x-\beta)(x-\gamma). \tag{18}$$

Next, we find X_2 and X_3 as well as dominant morphisms ϕ_2 and ϕ_3 satisfying conditions (15) and (16). Since $(x_3,0)$ and $(y_3,0) \in X_i$ are mapped to ∞ under ϕ_i for $i = 2, 3$ and two distinct points $(x_1,0)$ and $(x_2,0)$ (and $(y_1,0)$ and $(y_2,0)$) are mapped onto the same point in E, ϕ_i needs to be defined by rational functions with polynomials of degree at least 2 as numerators and with $(x-x_3)(x-y_3)$ as denominators. We let for some constants d_i and e_i,

$$\phi_2(x,y) = \left(\frac{d_2x^2+d_1x+d_0}{(x-x_3)(x-y_3)}, \frac{d_3}{((x-x_3)(x-y_3))^2}y\right), \text{ and}$$

$$\phi_3(x,y) = \left(\frac{e_2x^2+e_1x+e_0}{(x-x_3)(x-y_3)}, \frac{e_3}{((x-x_3)(x-y_3))^2}y\right).$$

In this setting, for ϕ_2 and ϕ_3 to satisfy conditions (15) and (16) respectively, the following six equations must hold:

(**)

$$\begin{cases} (d_2-\alpha)x^2+(d_1+\alpha(x_3+y_3))x+d_0-\alpha x_3y_3=(d_2-\alpha)(x-p)(x-q), \\ (d_2-\beta)x^2+(d_1+\beta(x_3+y_3))x+d_0-\beta x_3y_3=(d_2-\beta)(x-x_1)(x-x_2), \\ (d_2-\gamma)x^2+(d_1+\gamma(x_3+y_3))x+d_0-\gamma x_3y_3=(d_2-\gamma)(x-y_1)(x-y_2), \\ (e_2-\alpha)x^2+(e_1+\alpha(x_3+y_3))x+e_0-\alpha x_3y_3=(e_2-\alpha)(x-r)(x-s), \\ (e_2-\beta)x^2+(e_1+\beta(x_3+y_3))x+e_0-\beta x_3y_3=(e_2-\beta)(x-y_1)(x-y_2), \\ (e_2-\gamma)x^2+(e_1+\gamma(x_3+y_3))x+e_0-\gamma x_3y_3=(e_2-\gamma)(x-x_1)(x-x_2). \end{cases}$$

Then we find constants d_j, e_j, x_j, and y_j by equating the coefficients of constant terms, x and x^2-terms in each equation in (**) and requiring that

$$Z(\phi_i(x,y))=0, \text{ where } Z(x,y)=y^2-(x-\alpha)(x-\beta)(x-\gamma) \text{ and } i=2,3. \tag{19}$$

Now we solve for $r, x_i, y_i, c_i, d_i, e_i$ and give a solution to all equations from (17) to (**) and (19) listed in the above for X_i and ϕ_i as follows.

A moderate amount of direct calculation from (17) gives the following in terms of p, q, s, α, β, and γ:

$$r=\frac{s(p(\gamma-\beta)+q(\alpha-\gamma))+pq(\beta-\alpha)}{s(\alpha-\beta)+p(\gamma-\alpha)+q(\beta-\gamma)}\in K, \tag{20}$$

$$c_0=\frac{(\beta-\alpha)pq+s(\alpha q-\beta p)}{(p-q)}\in K, \tag{21}$$

$$c_1=\frac{\alpha(p-s)-\beta(q-s)}{(p-q)}\in K\setminus\{0\}. \tag{22}$$

Conditions (1), (7) and (8) imply that r, c_0 and c_1 are well-defined and that p, q, s and r are all distinct. Also, c_1 is nonzero by condition (9).

If we let

$$c_3=(\alpha-\beta)\in K\setminus\{0\}, \tag{23}$$

$$a=\frac{(s-q)(p-s)[s(\alpha-\beta)+p(\gamma-\alpha)+q(\beta-\gamma)]}{(p-q)^3}\in K\setminus\{0\}, \tag{24}$$

then $a\neq 0$ by conditions (1) and (7) and ϕ_1 is a nonconstant map since $c_3\neq 0$. We can verify[2] that ϕ_1 is a dominant morphism over K satisfying condition (14) and that (18) holds.

Next we let

$$b=(t-\alpha)(t-\beta)(t-\gamma)\in K. \text{ (Then } b\neq 0 \text{ by Lemma 2.)}$$

We can show[2] that a defined in (24) equals $\dfrac{\beta+\gamma-\alpha-t}{t-\alpha}$. Hence we get

$$ab=(\beta-t)(\gamma-t)(\beta+\gamma-\alpha-t)\in K\setminus\{0\}.$$

Then, for the quadratic polynomials $h_i(x)$ defined in Lemma 2, let x_1 and x_2 be zeros of $h_1(x)$, y_1 and y_2 zeros of $h_2(x)$, and x_3 and y_3 zeros of $h_3(x)$. Then p, q, s, r, x_i, y_j are all distinct by conditions (1), (10), (11) and (12).

[2]This can be shown by a moderate amount of direct calculation and has been verified using **Maple** (full documentation available upon request).

Using the same notation as in Lemma 2, we define the curves X_i and the maps $\phi_i : X_i \to E$ for $i = 1, 2, 3$ as follows (note that X_1 and ϕ_1 have been found in (20) through (24)):

$$
\begin{aligned}
X_1 : y^2 &= a(x-p)(x-q)(x-s)(x-\tfrac{s(p(\gamma-\beta)+q(\alpha-\gamma))+pq(\beta-\alpha)}{s(\alpha-\beta)+p(\gamma-\alpha)+q(\beta-\gamma)}),\\
X_2 : y^2 &= \frac{(t-\alpha)}{A^3}(x-p)(x-q)h_1(x)h_2(x)h_3(x)\\
&\left(= b(x-p)(x-q)(x-x_1)(x-x_2)(x-y_1)(x-y_2)(x-x_3)(x-y_3)\right),\\
X_3 : y^2 &= \frac{(\beta+\gamma-\alpha-t)}{A^3}(x-s)(x-\tfrac{s(p(\gamma-\beta)+q(\alpha-\gamma))+pq(\beta-\alpha)}{s(\alpha-\beta)+p(\gamma-\alpha)+q(\beta-\gamma)})h_1(x)h_2(x)h_3(x)\\
&\left(= ab(x-s)(x-r)(x-x_1)(x-x_2)(x-y_1)(x-y_2)(x-x_3)(x-y_3)\right),\\
\phi_1(x,y) &= \left(\tfrac{(\alpha(p-s)-\beta(q-s))x+(\beta-\alpha)pq+s(\alpha q-\beta p)}{(p-q)(x-s)},\quad \tfrac{(\alpha-\beta)}{(x-s)^2}y\right),\\
\phi_2(x,y) &= \left(\tfrac{h_1(x)+\beta h_3(x)}{h_3(x)},\quad \tfrac{A^2}{h_3(x)^2}y\right)\\
&\left(= \left(\tfrac{Atx^2-((\beta+\gamma-\alpha)B_1-\alpha B_2)x+((\beta+\gamma-\alpha)C_1-\alpha C_2)}{Ax^2-(B_1-B_2)x+(C_1-C_2)},\right.\right.\\
&\qquad\qquad \left.\left.\tfrac{A^2}{(Ax^2-(B_1-B_2)x+(C_1-C_2))^2}y\right)\right),\\
\phi_3(x,y) &= \left(\tfrac{-h_2(x)+\beta h_3(x)}{h_3(x)},\quad \tfrac{A^2}{h_3(x)^2}y\right)\\
&\left(= \left(\tfrac{A(\beta+\gamma-t)x^2-(\alpha B_1-(\beta+\gamma-\alpha)B_2)x+(\alpha C_1-(\beta+\gamma-\alpha)C_2)}{Ax^2-(B_1-B_2)x+(C_1-C_2)},\right.\right.\\
&\qquad\qquad \left.\left.\tfrac{A^2}{(Ax^2-(B_1-B_2)x+(C_1-C_2))^2}y\right)\right).
\end{aligned}
$$

Then, since p, q, s, r, x_i, y_i are all distinct and $a \neq 0, b \neq 0, A \neq 0, t \neq 0, \alpha, \beta + \gamma - \alpha, \beta + \gamma$, X_1, X_2, X_3 are nonsingular curves of genus 1,3,3 respectively and ϕ_i are nonconstant maps. And since $A, a, b \in K$ and $h_i(x)$ are defined over K, X_i and ϕ_i are defined over K.

Before we show that the maps ϕ_2 and ϕ_3 defined above satisfy (15) and (16) respectively (i.e. satisfy the equations in $(**)$) and satisfy (19), we verify the following identities[3]:

$$h_1(x) + (\beta - \alpha)h_3(x) = A(t - \alpha)(x - p)(x - q), \tag{25}$$

$$h_1(x) + (\beta - \gamma)h_3(x) = h_2(x), \tag{26}$$

$$-h_2(x) + (\beta - \alpha)h_3(x) = A(\beta + \gamma - \alpha - t)(x - s)(x - r), \tag{27}$$

$$-h_2(x) + (\beta - \gamma)h_3(x) = -h_1(x). \tag{28}$$

For the validity of (15) for ϕ_2, we show that

$$\phi_2(p,0) = \left(\frac{h_1(p)+\beta h_3(p)}{h_3(p)}, 0\right) = \left(\frac{(\alpha-\beta)h_3(p)+\beta h_3(p)}{h_3(p)}, 0\right) = (\alpha, 0) \text{ by (25)},$$

$$\phi_2(q,0) = \left(\frac{h_1(q)+\beta h_3(q)}{h_3(q)}, 0\right) = \left(\frac{(\alpha-\beta)h_3(q)+\beta h_3(q)}{h_3(p)}, 0\right) = (\alpha, 0) \text{ by (25)},$$

for $i = 1, 2$, $\phi_2(x_i, 0) = \left(\dfrac{h_1(x_i)+\beta h_3(x_i)}{h_3(x_i)}, 0\right) = (\beta, 0)$, since $h_1(x_i) = 0$,

[3]This can be shown by a moderate amount of direct calculation and has been verified using **Maple** (full documentation available upon request).

$\phi_2(y_i,0) = \left(\frac{h_1(y_i)+\beta h_3(y_i)}{h_3(y_i)},0\right) = \left(\frac{(\gamma-\beta)h_3(y_i)+\beta h_3(y_i)}{h_3(y_i)},0\right) = (\gamma,0)$ by (26), since $h_2(y_i)=0$, and $\phi_2(x_3,0)=\infty=\phi_2(x_3,0)$, since $h_3(x_3)=0=h_3(y_3)$.

Similarly, (16) can be verified for ϕ_3.

For the validity of (19) for $i=2$, by using (25) and (26), we show that

$$\begin{aligned}\frac{A^4}{h_3(x)^4}y^2 &= \left(\frac{h_1(x)+\beta h_3(x)}{h_3(x)}-\alpha\right)\left(\frac{h_1(x)+\beta h_3(x)}{h_3(x)}-\beta\right)\left(\frac{h_1(x)+\beta h_3(x)}{h_3(x)}-\gamma\right)\\ &= \frac{(h_1(x)+(\beta-\alpha)h_3(x))(h_1(x))(h_1(x)+(\beta-\gamma)h_3(x))}{h_3(x)^3}\\ &= \frac{A(t-\alpha)(x-p)(x-q)h_1(x)h_2(x)}{h_3(x)^3}\end{aligned}$$

which reduces to $y^2=\frac{(t-\alpha)}{A^3}(x-p)(x-q)h_1(x)h_2(x)h_3(x)$ and defines X_2.

Similarly, for the validity of (19) for $i=3$, by using (27) and (28), we show that

$$\begin{aligned}&\frac{A^4}{h_3(x)^4}y^2\\ &= \left(\frac{-h_2(x)+\beta h_3(x)}{h_3(x)}-\alpha\right)\left(\frac{-h_2(x)+\beta h_3(x)}{h_3(x)}-\beta\right)\left(\frac{-h_2(x)+\beta h_3(x)}{h_3(x)}-\gamma\right)\\ &= \frac{(-h_2(x)+(\beta-\alpha)h_3(x))(-h_2(x))(-h_2(x)+(\beta-\gamma)h_3(x))}{h_3(x)^3}\\ &= \frac{A(\beta+\gamma-\alpha-t)(x-s)(x-r)(-h_2(x))(-h_1(x))}{h_3(x)^3}\end{aligned}$$

which reduces to $y^2=\frac{(\beta+\gamma-\alpha-t)}{A^3}(x-s)(x-r)h_1(x)h_2(x)h_3(x)$ and defines X_3.

Note that all X_i and ϕ_i are defined over K. We have shown that there exist three nonsingular hyperelliptic curves X_i over K which map onto E via dominant morphisms $\phi_i: X_i \to E$ over K for $i=1,2,3$, and this completes the proof. □

Remark 5. We note that for an arbitrary elliptic curve E/K and for any integer $g\geq 1$, there exist three hyperelliptic curves X_1, X_2, X_3 of genus 1, g, g respectively over $\overline{K}$ which are defined as in $(*)$ of Proposition 4. But, in particular, Proposition 4 shows that when $g=3$ we can find three such curves X_i *defined over* K under the assumption that all 2-torsion points of E/K are K-rational.

Lemma 6. *Let K be an infinite field of finite type and $P_1(x), P_2(x), \ldots, P_k(x)$ a sequence of polynomials in $K[x]$ each of which has a zero of odd multiplicity. If L/K is a finite separable extension of K, then there exists $a\in K$ such that $P_i(a)$ is not a perfect square in L for $i=1,\ldots,k$.*

Proof. See [4, Lemma 4]. □

Theorem 7. *Let K be a number field, K_{ab} the maximal abelian extension of K, and E/K an elliptic curve with all K-rational 2-torsion points. Then for each $\sigma\in G_K$, the rank of $E((K_{ab})^\sigma)$ is infinite, therefore $E(\overline{K}^\sigma)$ is infinite.*

Proof. By Proposition 4 there are three hyperelliptic curves $(*)$ X_1, X_2, X_3 defined over K of genus 1, 3, and 3, respectively forming a biquadratic extension of $\mathbb{P}^1$ such that each admits a nonconstant K-morphism ϕ_i onto E.

We inductively construct quadratic extensions K_n of K and points $P_n \in E(K_n)$ as follows: for each n, we apply Lemma 6 to find $x_n \in K$ such that

$$K_1K_2\cdots K_{n-1}(\sqrt{af(x_n)g(x_n)}, \sqrt{bf(x_n)h(x_n)})$$

is a biquadratic extension of $K_1K_2\cdots K_{n-1}$. Then define L_n to be the biquadratic extension of K generated by the two square roots $\sqrt{af(x_n)g(x_n)}, \sqrt{bf(x_n)h(x_n)}$ above. Note that L_n contains $\sqrt{abg(x_n)h(x_n)}$ as well.

Then any element $\sigma \in G_K$ induces an action on L_n which must fix at least one of the three quadratic K-subfields of L_n. We choose K_n to be one of these fixed quadratic subfields of L_n over K under σ. Then one of the three curves X_i has a rational point Q_n over $K_n \subset (K_{ab})^\sigma \subset \overline{K}^\sigma$ with x-coordinate x_n, hence for the curve X_i containing Q_n, the image of Q_n under the corresponding K-morphism ϕ_i from X_i onto E is a rational point P_n of $E(K_n)$ fixed under σ.

By [5, Lemma], we may assume P_n is not a torsion point. Then by the linear disjointness of the quadratic extensions K_n over K, we can show that the points P_n are linearly independent in $E(K_{ab}^\sigma) \otimes \mathbb{Q}$ as in [4, Theorem 5]. Hence, they generate a submodule of $E(\prod_{n\geq 1} K_n) \otimes \mathbb{Q}$ of infinite rank. Since K_n are abelian extensions of K and fixed under σ, we conclude that $E((K_{ab})^\sigma)$ has infinite rank, so $E(\overline{K}^\sigma)$ has infinite rank as well. □

Remark 8. For a number field K and an elliptic curve E/K, if we let L be a finite extension of K over which all 2-torsion points of E/K are defined, then Theorem 7 implies that for every σ in the open subset $\mathrm{Gal}\,(\overline{K}/L)$ of G_K, $E(\overline{K}^\sigma)$ has infinite rank, which implies [4, Theorem 5]. Moreover, since $[L : K] \leq 6$, Theorem 7 gives a bound of 6 on the index of the open subset.

Acknowledgement

I wish to thank my thesis advisor, Michael Larsen, for suggesting this problem, his guidance, valuable discussions and helpful comments on this paper. I would like to thank the referee for the careful reading of the original manuscript and many helpful comments and suggestions that improved the presentation. I also thank David Rohrlich for his prompt correspondences and his efficient handling regarding this manuscript.

References

[1] B. Im: Mordell-Weil groups and the rank over large fields of elliptic curves over large fields, arXiv: math.NT/0411533, to appear in *Canadian J. Math.*

[2] B. Im: Heegner points and Mordell-Weil groups of elliptic curves over large fields, arXiv: math.NT/0411534, *submitted for publication*, 2003.

[3] S. Lang: Fundamentals of Diophantine Geometry, Springer-Verlag, 1983. MR0715605 (85j:11005)

[4] M. Larsen: Rank of elliptic curves over almost algebraically closed fields, *Bull. London Math. Soc.* **35** (2003) 817–820. MR2000029 (2004i:11054)

[5] J. H. Silverman: Integer points on curves of genus 1, *J. London Math. Soc.* **(2), 28**, (1983) 1-7. MR0703458 (84g:10033)

Department of Mathematics, University of Utah, Salt Lake City, Utah 84112
E-mail address: im@math.utah.edu