ACTA ARITHMETICA
158.1 (2013)

Infinite rank of elliptic curves over $\mathbb{Q}^{\mathrm{ab}}$

by

Bo-Hae Im (Seoul) and Michael Larsen (Bloomington, IN)

1. Introduction. In [FJ1], G. Frey and M. Jarden proved that every elliptic curve $E/\mathbb{Q}$ has infinite rank over $\mathbb{Q}^{\mathrm{ab}}$ and asked whether the same is true for all abelian varieties. For a general number field K (not necessarily contained in $\mathbb{Q}^{\mathrm{ab}}$), the question would be whether every abelian variety A over K is of infinite rank over $K\mathbb{Q}^{\mathrm{ab}}$. An affirmative answer to this question would follow from an affirmative answer to the original question, since every $\mathbb{Q}^{\mathrm{ab}}$-point of the Weil restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}}\, A$ gives a $K\mathbb{Q}^{\mathrm{ab}}$-point of A. We specialize the question to dimension 1.

Question 1.1. *If E is an elliptic curve over a number field K, must E have infinite rank over $K\mathbb{Q}^{\mathrm{ab}}$?*

Specializing further to the case that K is abelian over $\mathbb{Q}$, the question can be reformulated as:

Question 1.2. *Does every elliptic curve over $\mathbb{Q}^{\mathrm{ab}}$ have infinite rank over $\mathbb{Q}^{\mathrm{ab}}$?*

In a recent paper [K], E. Kobayashi considered Question 1.2 when $[K : \mathbb{Q}]$ is odd. In this setting, she gave an affirmative answer, conditional on the Birch–Swinnerton-Dyer conjecture.

We give an affirmative answer to Question 1.1 when E is defined over a field K of degree ≤ 4 over $\mathbb{Q}$ and satisfies some auxiliary condition. In all of our results, we can replace $\mathbb{Q}^{\mathrm{ab}}$ by $\mathbb{Q}(2)$, the compositum of all quadratic extensions of $\mathbb{Q}$. Our strategy for finding points over $\mathbb{Q}(2)$ entails looking for $\mathbb{Q}$-points on the Kummer variety $\mathrm{Res}_{K/\mathbb{Q}}\, E/(\pm 1)$ by looking for curves of genus ≤ 1 on that variety. When K is a quadratic field, $\mathrm{Res}_{K/\mathbb{Q}}\, E$ is an abelian surface isomorphic, over $\mathbb{C}$, to a product of two elliptic curves. Our construction of a curve on the Kummer surface $\mathrm{Res}_{K/\mathbb{Q}}\, E/(\pm 1)$ is modeled on the construction of a rational curve on $(E_1 \times E_2)/(\pm 1)$ due to

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 14H52.
Key words and phrases: elliptic curves.

DOI: 10.4064/aa158-1-3

J.-F. Mestre [M] and to M. Kuwata and L. Wang [KW]. For $[K:\mathbb{Q}]=3$, our proof depends on an analogous construction of a rational curve on $(E_1\times E_2\times E_3)/(\pm 1)$ which is presented in [I2]. We do not know of any rational curve on $(E_1\times E_2\times E_3\times E_4)/(\pm 1)$ for general choices of the E_i, but [I2, Lemma 1] constructs a curve of genus 1 in this variety.

2. A geometric construction. We now recall a geometric construction of a curve in

$$(E_1\times\cdots\times E_n)/(\pm 1), \tag{2.1}$$

where (± 1) acts diagonally on the product [I2, Lemma 1].

LEMMA 2.1 ([I2, Lemma 1]). *Let $\bar{K}$ be a separably closed field with $\mathrm{char}(\bar{K})\neq 2$, and for an integer $n\geq 2$, let $E_1,\ldots,E_n$ be pairwise non-isomorphic elliptic curves over $\bar{K}$. Then $(E_1\times\cdots\times E_n)/(\pm 1)$ contains a curve C_n with genus*

$$g_n := 2^{n-3}(n-4)+1.$$

In particular, $g_2=g_3=0$ and $g_4=1$.

Proof. Let E_i be written in Legendre form ([S2, p. 54, Proposition 1.7]): for $i=1,\ldots,n$,

$$E_i\colon y_i^2 = x_i(x_i-1)(x_i-\lambda_i), \qquad \lambda_i\in\bar{K}.$$

Since the E_i are non-isomorphic over $\bar{K}$, the λ_i are distinct.

We consider $E_1\times\cdots\times E_n$ as a $(\mathbb{Z}/2\mathbb{Z})^n$-cover of

$$E_1/(\pm 1)\times\cdots\times E_n/(\pm 1)\cong(\mathbb{P}^1)^n,$$

via $(P_1,\ldots,P_n)\mapsto(x(P_1),\ldots,x(P_n))$ where $x(P_i)$ is the x-coordinate of a point P_i of E_i if $P_i\neq O$ and $x(P_i)=\infty$ if $P_i=O$. We denote by X_n the inverse image in $(E_1\times\cdots\times E_n)/(\pm 1)$ of the diagonal curve $\mathbb{P}^1\subset(\mathbb{P}^1)^n$, i.e., the set of n-tuples where all coordinates are equal.

There exists an affine open subset of X_n with the following defining equations:

$$\begin{cases} z_{12}^2 = x^2(x-1)^2(x-\lambda_1)(x-\lambda_2),\\ \quad\vdots\\ z_{1n}^2 = x^2(x-1)^2(x-\lambda_1)(x-\lambda_n),\end{cases}$$

with $z_{12}=y_1y_2$, $z_{13}=y_1y_3$, $\ldots$, $z_{1n}=y_1y_n$ fixed under the action of (± 1). We can identify a point on this curve with an orbit of $E_1\times\cdots\times E_n$ under the diagonal action of ± 1 as follows:

$$(x,z_{12},\ldots,z_{1n})\mapsto((x,y_1),(x,z_{12}/y_1),(x,z_{13}/y_1),\ldots,(x,z_{1n}/y_1)),$$

where $y_1=\pm\sqrt{x(x-1)(x-\lambda_1)}$.

The function field of X_n is

$$\bar{K}\big(x, \sqrt{(x-\lambda_1)(x-\lambda_2)}, \sqrt{(x-\lambda_1)(x-\lambda_3)}, \ldots, \sqrt{(x-\lambda_1)(x-\lambda_n)}\,\big),$$

which is a finite extension of $\bar{K}(x)$ of degree 2^{n-1}. If we let $L_1 = \bar{K}(x)$ and $L_i = L_{i-1}\big(\sqrt{(x-\lambda_1)(x-\lambda_i)}\,\big)$ for $i = 2, \ldots, n$, then L_i is a quadratic extension of L_{i-1} for each $i = 2, \ldots, n$.

Therefore, there exists a non-singular projective curve C_n such that $\bar{K}(C_n) = L_n$ and there exists a non-constant morphism of degree 2^{n-1}, $\phi : C_n \to \mathbb{P}^1$, induced from the inclusion of $\bar{K}(x)$ into L_n. (See [H, Ch. I, §6] for details.)

Then ϕ is ramified at $P = [\lambda_i; 1] \in \mathbb{P}^1$ for each $i = 1, \ldots, n$ with the ramification degree 2 by investigating the local behavior of $\sqrt{(x-\lambda_1)(x-\lambda_i)}$ at each extension L_i over L_{i-1}. So by the Riemann–Hurwitz formula, the genus g_n of C_n is given by

$$2g_n - 2 = 2^{n-1}(2\cdot 0 - 2) + n2^{n-2}(2-1).$$

If $n = 2$ or $n = 3$, then $g_n = 0$, and if $n = 4$, then $g_n = 1$. ∎

It is difficult to tell when this construction produces a curve with infinitely many rational points over $\mathbb{Q}$ since a curve so obtained may not be defined over $\mathbb{Q}$. We do not use Lemma 2.1 directly in what follows, but it motivates the apparently *ad hoc*, explicit constructions of the remainder of the paper. Each of the following sections deals with one such construction.

3. The quadratic case. We begin with a lemma.

LEMMA 3.1. *Let k be a non-negative integer and $Q(u,v) \in \mathbb{Q}[u,v]$ a homogeneous polynomial of degree $2(2k+1)$ satisfying the functional equation*

$$Q(mu, v) = m^{2k+1}Q(v,u)$$

for a fixed square-free integer $m \neq 1$. Then $Q(u,v)$ cannot be a perfect square in $\mathbb{C}[u,v]$.

Proof. Let i be the largest integer such that v^i divides $Q(u,v)$. If i is odd, $Q(u,v)$ cannot be a perfect square in $\mathbb{C}[u,v]$. We therefore assume that $i = 2j$. Without loss of generality, we may assume that the $u^{4k+2-2j}v^{2j}$-coefficient is 1. If $q(u,v)$ is a square root of $Q(u,v)$ over $\mathbb{C}$, then the $u^{2k+1-j}v^j$-coefficient of $q(u,v)$ is ± 1. Every automorphism σ of the complex numbers sends $q(u,v)$ to $\pm q(u,v)$. However, σ fixes the $u^{2k+1-j}v^j$ coefficient of $q(u,v)$, so σ fixes $q(u,v)$, which means $q(u,v) \in \mathbb{Q}[u,v]$. From the given functional relation, $q(u,v)$ satisfies

$$q(mu, v) = \pm\sqrt{m}\,(m^k q(v,u)),$$

which gives a contradiction since $\sqrt{m} \notin \mathbb{Q}$. ∎

Theorem 3.2. *Let* $E\colon y^2 = P(x) := x^3 + \alpha x + \beta$ *be an elliptic curve defined over a quadratic extension* K *of* $\mathbb{Q}$. *If the* j*-invariant of* E *is not* 0 *or* 1728, *then* $E(\mathbb{Q}^{\mathrm{ab}})$ *has infinite rank.*

Proof. Let $K = \mathbb{Q}(\sqrt{m}\,)$, where $m \in \mathbb{Z}$ is a square-free integer and $m \neq 1$. By the hypothesis on the j-invariant, $\alpha \neq 0$ and $\beta \neq 0$. Replacing α and β by $\lambda^4\alpha$ and $\lambda^6\beta$ for suitable $\lambda \in K$, we may assume without loss of generality that $\alpha, \beta \notin \mathbb{Q}$.

Let $\alpha = a + c\sqrt{m}$ and $\beta = b + d\sqrt{m}$ for $a, b, c, d \in \mathbb{Q}$, $c, d \neq 0$. Then for $x_1 := -d/c \in \mathbb{Q}$, we have $P(x_1) \in \mathbb{Q}$, so

$$\big(x_1, \sqrt{P(x_1)}\,\big) \in E\big(K\big(\sqrt{P(x_1)}\,\big) \subseteq E(\mathbb{Q}^{\mathrm{ab}}).$$

Now replacing α by $\gamma^4\alpha$ and β by $\gamma^6\beta$ for $\gamma \in K$ such that $\gamma^4\alpha, \gamma^6\beta \notin \mathbb{Q}$, we get an isomorphism ϕ_γ over K from E to the elliptic curve

$$E_\gamma\colon y^2 = P_\gamma(x) := x^3 + \gamma^4\alpha x + \gamma^6\beta,$$

mapping (x, y) onto $(\gamma^2 x, \gamma^3 y)$.

Applying the above argument for E_γ rather than E, we find a point $\big(x_{\gamma,1}, \sqrt{P_\gamma(x_{\gamma,1})}\,\big) \in E_\gamma\big(K\big(\sqrt{P_\gamma(x_{\gamma,1})}\,\big)\big)$ with $x_{\gamma,1} \in \mathbb{Q}$ and $P_\gamma(x_{\gamma,1}) \in \mathbb{Q}$. Applying ϕ_γ^{-1} to the latter point, we get a point

$$\big(\gamma^{-2}x_{\gamma,1}, \gamma^{-3}\sqrt{P_\gamma(x_{\gamma,1})}\,\big) \in E\big(K\big(\sqrt{P_\gamma(x_{\gamma,1})}\,\big)\big) \subseteq E(\mathbb{Q}^{\mathrm{ab}}), \tag{3.1}$$

where $x_{\gamma,1} \in \mathbb{Q}$ and $P_\gamma(x_{\gamma,1}) \in \mathbb{Q}$.

Now we show that there are infinitely many quadratic fields L such that $\mathbb{Q}\big(\sqrt{P_\gamma(x_\gamma)}\,\big) = L$ for some $\gamma \in K$.

For $\gamma = u + v\sqrt{m}$ with variables u and v which will be specialized later, we write

$$x^3 + (u + v\sqrt{m}\,)^4\alpha x + (u + v\sqrt{m}\,)^6\beta = P_\gamma(x) = R + I\sqrt{m},$$

where

$$I = xT_1(u, v) + S_1(u, v) \quad \text{and} \quad R = x^3 + xT_2(u, v) + S_2(u, v)$$

and T_i and S_i are homogeneous polynomials in u and v over $\mathbb{Q}$ of degree 4 and 6 respectively. In fact, by using Maple 16 (refer to the quadratic case of the Appendix for the computation), we get

$$\begin{aligned}
I &= x(u^4c + 4u^3va + 6u^2v^2mc + 4uv^3ma + v^4m^2c) \\
&\quad + u^6d + 6u^5vb + 15u^4v^2md + 20u^3v^3mb \\
&\quad + 15u^2v^4m^2d + 6uv^5m^2b + v^6m^3d, \\
R &= x^3 + x(u^4a + 4u^3vmc + 6u^2v^2ma + 4uv^3m^2c + v^4m^2a) \\
&\quad + u^6b + 6u^5vmd + 15u^4v^2mb + 20u^3v^3m^2d \\
&\quad + 15u^2v^4m^2b + 6uv^5m^3d + v^6m^3b.
\end{aligned}$$

So we have

$$
(3.2)\qquad
\begin{aligned}
T_1(u,v) &= u^4c + 4u^3va + 6u^2v^2mc + 4uv^3ma + v^4m^2c,\\
S_1(u,v) &= u^6d + 6u^5vb + 15u^4v^2md + 20u^3v^3mb\\
&\quad + 15u^2v^4m^2d + 6uv^5m^2b + v^6m^3d,\\
T_2(u,v) &= u^4a + 4u^3vmc + 6u^2v^2ma + 4uv^3m^2c + v^4m^2a,\\
S_2(u,v) &= u^6b + 6u^5vmd + 15u^4v^2mb + 20u^3v^3m^2d\\
&\quad + 15u^2v^4m^2b + 6uv^5m^3d + v^6m^3b.
\end{aligned}
$$

Since $(mu + v\sqrt{m})^4 = m^2(v + u\sqrt{m})^4$ and $(mu + v\sqrt{m})^6 = m^3(v + u\sqrt{m})^6$, the T_i's and the S_i's satisfy the following relations:

$$
(3.3)\qquad T_i(mu,v) = m^2T_i(v,u), \qquad S_i(mu,v) = m^3S_i(v,u).
$$

We solve the equation $I = xT_1(u,v) + S_1(u,v) = 0$ for x and get

$$
x_\gamma := -\frac{S_1(u,v)}{T_1(u,v)}.
$$

We then substitute this value of x into the rational part R of $P_\gamma(x)$, and after clearing the denominator by multiplying by $(T_1(u,v))^4$, we obtain the polynomial

$$
-T_1(u,v)(S_1(u,v)^3 + S_1(u,v)\,T_1(u,v)^2\,T_2(u,v) - S_2(u,v)\,T_1(u,v)^3),
$$

which we denote by Q. Thus, Q is homogeneous of degree 22 over $\mathbb{Q}$ and from the relation (3.3), it satisfies

$$
(3.4)\qquad Q(mu,v) = m^{11}Q(v,u).
$$

Note that by direct computation referring to (3.2) or by using MAPLE 16 (refer to the quadratic case of the Appendix for the computation), the coefficients of the u^{22}-term and $u^{21}v$-term in $Q(u,v)$ are, respectively,

$$
A_0 = c(-d^3 - adc^2 + bc^3), \quad A_1 = 2(-6a^2dc^2 - 2ad^3 + 5abc^3 + mc^4d - 9cd^2b).
$$

If $Q(u,v)$ is identically 0, then $A_0 = A_1 = 0$. Since $c \neq 0$ and $d \neq 0$, we solve $A_0 = 0$ for a and substitute

$$
a = \frac{bc^3 - d^3}{c^2d}
$$

into $A_1 = 0$. Then we get

$$
-b^2c^6 - 4c^3d^3b - 4d^6 + mc^6d^2 = 0,
$$

whose discriminant in b is $4mc^{12}d^2$ (refer to the Appendix for the computation), which is not a square in $\mathbb{Q}$. Hence $A_1 \neq 0$. This shows that $Q(u,v)$ cannot be identically zero. By Lemma 3.1, $Q(u,v)$ cannot be a perfect square in $\mathbb{C}[u,v]$.

Hence $y^2 - Q(u,v)$ is irreducible over $\mathbb{C}$.

Let $f(t) \in \mathbb{Q}[t]$ be the polynomial of degree 22 in the variable $t = u/v$ obtained by replacing $Q(u,v)$ by $Q(u,v)v^{-22}$. For a finite extension L of K, we let

$$H(f,L) := \{t' \in \mathbb{Q} : f(t') - y^2 \text{ is irreducible over } L\},$$

the intersection of $\mathbb{Q}$ with the Hilbert set of f over L. By the Hilbert irreducibility theorem ([FJ2, Corollary 12.2.3]), such an intersection is non-empty.

Hence there exists $\gamma_0 = u_0 + v_0\sqrt{m} \in K$ such that

$$L_0 := \mathbb{Q}\big(\sqrt{P_{\gamma_0}(x_{\gamma_0})}\big) = \mathbb{Q}\big(\sqrt{Q(u_{\gamma_0}, v_{\gamma_0})}\big)$$

is a quadratic field not contained in L. Inductively, we get an infinite sequence of $\gamma_k = u_k + v_k\sqrt{m}$ such that the fields

$$L_k = \mathbb{Q}\big(\sqrt{P_{\gamma_k}(x_{\gamma_k})}\big) = \mathbb{Q}\big(\sqrt{Q(u_{\gamma_k}, v_{\gamma_k})}\big)$$

are not $\mathbb{Q}$-rational and are linearly disjoint over $\mathbb{Q}$.

Let V be the set

$$V := \big\{\big(\gamma_k^{-2}x_{\gamma_k}, \gamma_k^{-3}\sqrt{P_{\gamma_k}(x_{\gamma_k})}\big) \in E\big(K\big(\sqrt{P(x_{\gamma_k})}\big)\big)\big\}_{k=0}^{\infty}.$$

By [S1, Lemma], $\bigcup_{[L:K]\le d} E(L)_{\mathrm{tor}}$ is a finite set, where the union is over all finite extensions L of K whose degree over K is less than or equal to d. Therefore, V contains only finitely many torsion points. Then by linear disjointness of KL_i over K and by [I1, Lemma 3.12], infinitely many non-torsion points $\big(\gamma_k^{-2}x_{\gamma_k}, \gamma_k^{-3}\sqrt{P_{\gamma_k}(x_{\gamma_k})}\big) \in V$ are linearly independent in $E(K\mathbb{Q}^{\mathrm{ab}})$. Therefore the rank of $E(K\mathbb{Q}(2))$ is infinite, so the rank of $E(K\mathbb{Q}^{\mathrm{ab}}) \subseteq E(\mathbb{Q}^{\mathrm{ab}})$ is infinite. ∎

4. The cubic case

THEOREM 4.1. *Let λ denote an element of a cubic extension K of $\mathbb{Q}$. Then $E\colon y^2 = x(x-1)(x-\lambda)$ has infinite rank over $K\mathbb{Q}^{\mathrm{ab}}$.*

Proof. If $\lambda \in \mathbb{Q}$, then we are done (by the proof of [FJ1, Theorem 2.2]), so we assume that $\mathbb{Q}(\lambda) = K$.

Let

$$L(t) := t^3 - at^2 + bt - c$$

denote the minimal polynomial of λ. Expanding, we have

$$\left(\frac{b-t^2}{2} + (t-a)\lambda + \lambda^2\right)^2 = M(t) - L(t)\lambda,$$

where

$$M(t) := \frac{t^4 - 2bt^2 + 8ct + b^2 - 4ac}{4}.$$

Let

$$N(t) := L(t)M(t)(M(t) - L(t)).$$

Defining

$$x := \frac{M(t)}{L(t)}, \qquad y := \frac{(b - t^2)/2 + (t - a)\lambda + \lambda^2}{L(t)^2}\sqrt{N(t)} = \frac{M(t) - L(t)\lambda}{L(t)^2}\sqrt{N(t)},$$

we have

$$x(x-1)(x-\lambda) = \frac{N(t)(M(t) - L(t)\lambda)}{L(t)^4} = y^2,$$

which verifies that $(x, y) \in K\big(t, \sqrt{N(t)}\,\big)^2$ lies on E, that is, it belongs to $E\big(K\big(t, \sqrt{N(t)}\,\big)\big)$. Note that $\deg N = 11$, so $w^2 - N(t)$ is irreducible in $\mathbb{C}[w, t]$. Specializing t in $\mathbb{Q}$, and applying Hilbert irreducibility, as before, we obtain points of $E(KL_i)$ for an infinite sequence of linearly disjoint quadratic extensions L_i over $\mathbb{Q}$. It follows that by [S1, Lemma] and by [I1, Lemma 3.12], E has infinite rank over $K\mathbb{Q}(2)$ and therefore over $K\mathbb{Q}^{\mathrm{ab}}$. ∎

Note that the idea of the proof of Theorem 4.1 has been applied in [I2, Theorem 4].

5. The quartic case

THEOREM 5.1. *Let λ denote an element generating a quartic extension K of $\mathbb{Q}$. Let $P(x)$ be the (monic) minimal polynomial of λ over $\mathbb{Q}$ (hence P has no multiple roots). If the curve defined by*

$$v^2 = P(u) := u^4 + pu^3 + qu^2 + ru + s \tag{5.1}$$

has infinitely many $\mathbb{Q}$-rational points, then $E\colon y^2 = x(x-1)(x-\lambda)$ has infinite rank over $K\mathbb{Q}^{\mathrm{ab}}$.

Proof. If (u, v) satisfies (5.1), then setting

$$\begin{aligned} A(u,v) &:= (2u^4 + pu^3 - ru - 2s)v \\ &\quad + \frac{8u^6 + 8pu^5 + (p^2 + 4q)u^4 - (8s + 2pr)u^2 - 8psu + r^2 - 4qs}{4}, \\ B(u,v) &:= (4u^3 + 3pu^2 + 2qu + r)v \\ &\quad + 4u^5 + 5pu^4 + (p^2 + 4q)u^3 + (4r + pq)u^2 + (4s + rp)u + ps, \end{aligned}$$

and

$$C(u,v) := \frac{-2uv - 2u^3 - pu^2 + r}{2} + (v + u^2 + pu + q)\lambda + (u + p)\lambda^2 + \lambda^3,$$

we have

$$C(u,v)^2 = A(u,v) - B(u,v)\lambda$$

by explicit computation using MAPLE 16 (refer to the quartic case of the Appendix). Thus, if for $(u,v) \in \mathbb{Q}^2$ we let

$$x_{(u,v)} := \frac{A(u,v)}{B(u,v)} \quad \text{and} \quad y_{(u,v)} := C(u,v)\sqrt{\frac{A(u,v)(A(u,v)-B(u,v))}{B(u,v)^3}},$$

then

$$x_{(u,v)}(x_{(u,v)}-1)(x_{(u,v)}-\lambda) = \frac{C(u,v)A(u,v)(A(u,v)-B(u,v))}{B(u,v)^3} = y_{(u,v)}^2.$$

So we have a point

$$P_{(u,v)} := (x_{(u,v)}, y_{(u,v)}) \in E\big(K\mathbb{Q}\big(\sqrt{D(u,v)}\,\big)\big), \tag{5.2}$$

where

$$D(u,v) := A(u,v)B(u,v)(A(u,v)-B(u,v)) \in \mathbb{Q}[u,v].$$

We note that since $P(u)$ has no multiple roots, (5.1) is an elliptic curve of genus 1 by [FJ2, Proposition 3.8.2].

There are two embeddings of the function field F of (5.1) in the field $F_\infty := \mathbb{C}((t))$ of Laurent series which map u to $1/t$, determined by which square root of $P(1/t)$ the element v maps to. We choose the embedding sending v to the Laurent series

$$t^{-2} + \frac{p}{2}t^{-1} + \left(\frac{q}{2} - \frac{p^2}{8}\right) + \cdots.$$

This defines a discrete valuation on F with respect to which $A(u,v)$, $B(u,v)$ and $A(u,v) - B(u,v)$ have value -6, -5, and -6 respectively. It follows that $F_\infty\big(\sqrt{D(u,v)}\,\big) = \mathbb{C}((t^{1/2}))$. This implies that $\sqrt{D(u,v)}$ does not lie in F. Therefore, $\sqrt{D(u,v)} \notin F$. Let X denote the projective non-singular curve over $\mathbb{C}$ with function field $F[z]/(z^2 - D(u,v))$. Then there exists a morphism from X to the projective non-singular curve with function field F, which is ramified at the pole of t. Since the genus of F is 1, the genus of X is at least 2. By Faltings' theorem [F], $X(\mathbb{Q}(\sqrt{d}\,))$ is finite for all $d \in \mathbb{Q}$. If there are infinitely many $\mathbb{Q}$-points $\{Q_k := (u_k, v_k)\}_{k=1}^\infty$ on (5.1), their inverse images in X generate infinitely many different quadratic extensions of $\mathbb{Q}$, and so the points $\{P_{(u_k,v_k)}\}_{k=1}^\infty$ of E in (5.2) are defined over different quadratic extensions $K\mathbb{Q}\big(\sqrt{D(u_k,v_k)}\,\big)$ of $\mathbb{Q}$. By [S1, Lemma] and by [I1, Lemma 3.12] again, it follows that $E(K\mathbb{Q}(2))$ has infinite rank. ■

Appendix. We present some machine computations, using MAPLE 16, which verify the assertions in the proofs of Theorems 3.2 and 5.1. The notations are compatible with those proofs, except that I in the proof of Theorem 3.2 is represented by J below.

The quadratic case (for the proof of Theorem 3.2):

```
> f := sort(expand(x^3 + (u + v*sqrt(m))^4*(a + c*sqrt(m))*x + (u + v*sqrt(m))^6*
(b + d*sqrt(m))), m);
```

$$f := u^4ax + 4uv^3cm^2x + 4u^3vcmx + 6u^2v^2amx + v^6bm^3 + u^6b + 20u^3v^3dm^2 + 15u^2v^4bm^2 + 6u^5vdm + 6uv^5dm^3 + 15u^4v^2bm + v^4am^2x + x^3 + xv^4cm^{5/2} + 15u^2v^4dm^{5/2} + 6uv^5bm^{5/2} + 15u^4v^2dm^{3/2} + 20u^3v^3bm^{3/2} + u^4cx\sqrt{m} + 6u^5vb\sqrt{m} + v^6dm^{7/2} + u^6d\sqrt{m} + 4xuv^3am^{3/2} + 6xu^2v^2cm^{3/2} + 4u^3vax\sqrt{m}$$

```
> J := sort(expand((v^6*d*m^(7/2) + x*v^4*c*m^(5/2) + 15*u^2*v^4*d*m^(5/2)
+ 6*u*v^5*b*m^(5/2) + 4*x*u*v^3*a*m^(3/2) + 15*u^4*v^2*d*m^(3/2)
+ 6*x*u^2*v^2*c*m^(3/2) + 20*u^3*v^3*b*m^(3/2) + u^4*c*x*sqrt(m)
+ u^6*d*sqrt(m) + 6*u^5*v*b*sqrt(m) + 4*u^3*v*a*x*sqrt(m))/sqrt(m)), x);
```

$$J := 4muv^3ax + m^2v^4cx + 6mu^2v^2cx + 4u^3vax + u^4cx + 15mu^4v^2d + 15m^2u^2v^4d + 6m^2uv^5b + m^3v^6d + u^6d + 6u^5vb + 20mu^3v^3b$$

```
> R := sort(expand(f - J*sqrt(m)), x);
```

$$R := x^3 + 4u^3vcmx + 6u^2v^2amx + v^4am^2x + u^4ax + 4uv^3cm^2x + 6u^5vdm + 6uv^5dm^3 + 15u^4v^2bm + u^6b + v^6bm^3 + 20u^3v^3dm^2 + 15u^2v^4bm^2$$

```
> T1 := expand((4*m*u*v^3*a*x + m^2*v^4*c*x + 6*m*u^2*v^2*c*x + 4*u^3*v*a*x
+ u^4*c*x)/x);
```

$$T_1 := 4muv^3a + m^2v^4c + 6mu^2v^2c + 4u^3va + u^4c$$

```
> S1 := 15*m*u^4*v^2*d + 15*m^2*u^2*v^4*d + 6*m^2*u*v^5*b + m^3*v^6*d + u^6*d
+ 6*u^5*v*b + 20*m*u^3*v^3*b;
```

$$S_1 := 15mu^4v^2d + 15m^2u^2v^4d + 6m^2uv^5b + m^3v^6d + u^6d + 6u^5vb + 20mu^3v^3b$$

```
> T2 := expand((4*u^3*v*c*m*x + 6*u^2*v^2*a*m*x + v^4*a*m^2*x + u^4*a*x
+ 4*u*v^3*c*m^2*x)/x);
```

$$T_2 := 4u^3vcm + 6u^2v^2am + v^4am^2 + u^4a + 4uv^3cm^2$$

```
> S2 := 6*u^5*v*d*m + 6*u*v^5*d*m^3 + 15*u^4*v^2*b*m + u^6*b + v^6*b*m^3
+ 20*u^3*v^3*d*m^2 + 15*u^2*v^4*b*m^2;
```

$$S_2 := 6u^5vdm + 6uv^5dm^3 + 15u^4v^2bm + u^6b + v^6bm^3 + 20u^3v^3dm^2 + 15u^2v^4bm^2$$

```
> Q := -T1*(S1^3 + S1*T1^2*T2 - S2*T1^3);
```

$$Q := -(4muv^3a + m^2v^4c + 6mu^2v^2c + 4u^3va + u^4c)\Big((15mu^4v^2d + 15m^2u^2v^4d + 6m^2uv^5b + m^3v^6d + u^6d + 6u^5vb + 20mu^3v^3b)^3 + (15mu^4v^2d + 15m^2u^2v^4d + 6m^2uv^5b + m^3v^6d + u^6d + 6u^5vb + 20mu^3v^3b)(4muv^3a + m^2v^4c + 6mu^2v^2c + 4u^3va + u^4c)^2 \cdot (4u^3vcm + 6u^2v^2am + v^4am^2 + u^4a + 4uv^3cm^2) - (6u^5vdm + 6uv^5dm^3 + 15u^4v^2bm + u^6b + v^6bm^3 + 20u^3v^3dm^2 + 15u^2v^4bm^2) \cdot (4muv^3a + m^2v^4c + 6mu^2v^2c + 4u^3va + u^4c)^3\Big)$$

```
> A0 := factor(coeff(Q, u, 22));
```

$$A_0 := -c(-bc^3 + dac^2 + d^3)$$

```
> A1 := expand(coeff(Q, u, 21)/v);
```

$$A_1 := 10c^3ba - 12a^2dc^2 - 4ad^3 - 18cd^2b + 2c^4dm$$

```
> discrim( -b^2*c^6 - 4*c^3*d^3*b - 4*d^6 + m*c^6*d^2, b);
```

$$4mc^{12}d^2$$

The quartic case (for the proof of Theorem 5.1):

```
> A := (2*u^4 + p*u^3 - r*u - 2*s)*v + (8*u^6 + 8*p*u^5 + (p^2 + 4*q)*u^4
- (8*s + 2*p*r)*u^2 - 8*p*s*u + r^2 - 4*q*s)*(1/4);
```

$$A := (2u^4 + pu^3 - ru - 2s)v + 2u^6 + 2pu^5 + \tfrac{1}{4}(p^2 + 4q)u^4 - \tfrac{1}{4}(8s + 2pr)u^2 - 2psu + \tfrac{1}{4}r^2 - qs$$

```
> B := (4*u^3 + 3*p*u^2 + 2*q*u + r)*v + 4*u^5 + 5*p*u^4 + (p^2 + 4*q)*u^3
+ (4*r + p*q)*u^2 + (4*s + p*r)*u + p*s;
```

$$B := (4u^3 + 3pu^2 + 2qu + r)v + 4u^5 + 5pu^4 + (p^2 + 4q)u^3 + (4r + pq)u^2 + (4s + pr)u + ps$$

```
> C := (-2*u*v - 2*u^3 - p*u^2 + r)*(1/2) + (v + u^2 + p*u + q)*lambda
+ (u + p)*lambda^2 + lambda^3;
```

$$C := -uv - u^3 - \tfrac{1}{2}pu^2 + \tfrac{1}{2}r + (v + u^2 + pu + q)\lambda + (u + p)\lambda^2 + \lambda^3$$

```
> l5 := expand(subs(lambda^4 = -p*lambda^3 - q*lambda^2 - r*lambda - s,
expand( -lambda*(p*lambda^3 + q*lambda^2  + r*lambda + s))));
```

$$l_5 := p^2\lambda^3 + pq\lambda^2 + pr\lambda + ps - q\lambda^3 - r\lambda^2 - \lambda s$$

```
> l6 := expand(subs(lambda^4 = -p*lambda^3 - q*lambda^2 - r*lambda - s,
expand(lambda*l5)));
```

$$l_6 := -p^3\lambda^3 - p^2q\lambda^2 - p^2r\lambda - p^2s + 2\lambda^3qp + r\lambda^2p + \lambda ps + \lambda^2q^2 + r\lambda q + qs - r\lambda^3 - \lambda^2 s$$

```
> simplify(subs(v^2 = u^4 + p*u^3 + q*u^2 + r*u + s, lambda^4 = -p*lambda^3
- q*lambda^2 - r*lambda - s, lambda^5 = l5, lambda^6 = l6,
expand(C^2 - A + B*lambda)));
```

$$0$$

Acknowledgments. We would like to thank the referee for a number of helpful suggestions. We would also like to thank Bartosz Naskręcki for confirming the correctness of our machine computations.

Bo-Hae Im was supported by the National Research Foundation of Korea grant funded by the Korean Government (MEST) (NRF-2011-0015557). Michael Larsen was partially supported by NSF grants DMS-0800705 and DMS-1101424.

References

[F] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[FJ1] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. (3) 28 (1974), 112–128.

[FJ2] M. D. Fried and M. Jarden, *Field Arithmetic*, 3rd ed., Ergeb. Math. Grenzgeb. 11, Springer, Berlin, 2008.

[H] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

[I1] B.-H. Im, *Mordell–Weil groups and the rank of elliptic curves over large fields*, Canad. J. Math. 58 (2006), 796–819.

[I2] B.-H. Im, *Positive rank quadratic twists of four elliptic curves*, J. Number Theory 133 (2013), 492–500.

[K] E. Kobayashi, *A remark on the Mordell–Weil rank of elliptic curves over the maximal abelian extension of the rational number field*, Tokyo J. Math. 29 (2006), 295–300.

[KW] M. Kuwata and L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Int. Math. Res. Notices 1993, 113–123.

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

[S1] J. H. Silverman, *Integer points on curves of genus 1*, J. London Math. Soc. (2) 28 (1983), 1–7.

[S2] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

Bo-Hae Im
Department of Mathematics
Chung-Ang University
221 Heukseok-dong, Dongjak-gu
Seoul, 156-756, South Korea
E-mail: imbh@cau.ac.kr

Michael Larsen
Department of Mathematics
Indiana University
Bloomington, IN 47405, U.S.A.
E-mail: mjlarsen@indiana.edu

Received on 10.5.2012
and in revised form on 12.12.2012 (7062)