A note on the growth of Mordell-Weil ranks of elliptic curves in cyclotomic $\mathbf{Z}_p$-extensions

By Kazuo MATSUNO

Department of Mathematics, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397

(Communicated by Heisuke HIRONAKA, M. J. A., May 12, 2003)

Abstract: In this note, we exhibit some examples of elliptic curves whose Mordell-Weil ranks grow in lower layer of the cyclotomic $\mathbf{Z}_p$-extension over the rationals.

Key words: Elliptic curve; Mordell-Weil group; Iwasawa theory; $\mathbf{Z}_p$-extension.

1. Introduction.

For a prime number p, let $F_{p,\infty}$ be the cyclotomic $\mathbf{Z}_p$-extension of the rational number field $\mathbf{Q}$ and denote by $F_{p,n}$ its n-th layer. When p is odd, $F_{p,n}$ is the unique cyclic extension of degree p^n over $\mathbf{Q}$ unramified outside p.

By results of Kato, Rohrlich and Rubin, we know that $E(F_{p,\infty})$ is finitely generated for any elliptic curve E defined over $\mathbf{Q}$. Especially, there exists an integer n_0 such that

$$\mathrm{rank}_{\mathbf{Z}} E(F_{p,n}) = \mathrm{rank}_{\mathbf{Z}} E(F_{p,n_0})$$

holds for any $n \geq n_0$. We denote by $n_p = n_p(E)$ the smallest one of such n_0.

Greenberg asked in [2] whether $n_p(E)$ is bounded or not when E or p varies. According to a recent result of Chinta ([1, Theorem 2]), $n_p(E)$ is bounded as p varies for a fixed E. As for the variation of $n_p(E)$ when E varies for a fixed p, we only know the existence of elliptic curves such that $n_p = 0$ for all p (e.g., elliptic curves of conductor 11), and the existence of curves with positive n_p for small p's. In [2, §1], Greenberg showed that an elliptic curve of conductor 195 (resp. 34) has $n_2 = 2$ (resp. $n_3 = 1$). He also mentioned that one can find examples of elliptic curves such that $n_2 \geq 3$, $n_3 \geq 2$, $n_5 \geq 1$ and $n_7 \geq 1$, respectively, by using a result of Rohrlich [4]. In this note, we present such examples explicitly by investigating some properties of Rohrlich's curves as a family of elliptic curves (§2 and §3). We also give another proof of the main result of [4] (Corollary 5).

In §4, we will discuss a similar question for cyclotomic extensions of the rational function field over a finite field. We will prove that there exists an elliptic curve with arbitrary large n_p in this situation.

2. Rohrlich's construction and a family of elliptic curves.

In this section, let K be a number field of finite degree and $f(x) \in K[x]$ a monic of degree 9. We denote by $a_i \in K$ the coefficient of x^i in f and assume that $a_8 = 0$. We also set $a_i = 0$ for $i < 0$. Let $\alpha_i \in \overline{K}$ $(i = 1, \ldots, 9)$ be the roots of $f(x)$.

For any elements $u, v \in K(t)$, we consider a (projective) plane cubic curve $E_{u,v}$ defined by the equation

$$u \sum_{i=0}^{2} \sum_{j=0}^{3} a_{9-2i-3j} x^i y^j + v(x^3 - y^2) = 0.$$

If $E_{u,v}$ is non-singular and $E_{u,v}(K(t))$ is non-empty, we can regard $E_{u,v}$ as an elliptic curve defined over $K(t)$. When $u, v \in K$ and $E_{u,v}(K)$ is non-empty, we consider $E_{u,v}$ as an elliptic curve over K.

In [4], Rohrlich treats the curve $E_{1,b}$, where $b = -a_5 - a_7 - a_9$. This curve has a rational point $(1, 0) \in E_{1,b}(K)$. Therefore $E_{1,b}$ is an elliptic curve over K if $E_{1,b}$ is non-singular. Rohrlich shows that, for any finite extension L/K satisfying $[L : K] \leq 9$, one can take an $f(x)$ so that $L = K(\alpha_1)$ and $E_{1,b}$ is an elliptic curve such that $E_{1,b}(M) \otimes \mathbf{Q}$ contains $V'_{L/K}$, where M is the Galois closure of L/K with $G = \mathrm{Gal}(M/K)$ and $V'_{L/K}$ is a $\mathbf{Q}[G]$-module defined later.

In this note, we treat two cubic curves $E_{t,1}$ and $E_{r(t),s(t)}$ defined over $K(t)$, and treat also their specializations to K. Here we define a polynomial $q(t) \in K[t]$ by

$$q(t) = \left(\sum_{i=0}^{1} a_{3i+2}\right) t^2 + \left(\sum_{i=0}^{2} a_{3i+1}\right) t + \sum_{i=0}^{3} a_{3i}$$

and set $r(t) = (1 - t^3)/\gcd(1 - t^3, q(t))$ and $s(t) = q(t)/\gcd(1 - t^3, q(t))$. We remark that $q(t) \neq 0$ and $\deg(r(t))$ is positive. The following lemmas imply

2000 Mathematics Subject Classification. Primary 11G05, 11R23.

that two cubic curves above are elliptic curves indeed (under a condition for $E_{t,1}$).

Lemma 1. *Cubic curves $E_{t,1}$ and $E_{r(t),s(t)}$ are non-singular.*

Proof. Assume that $P \in E_{t,1}(\overline{K(t)})$ is a singular point. Since $E_{t,1}$ is an irreducible cubic curve, P is a unique singular point on $E_{t,1}$. This implies $P \in E_{t,1}(K(t))$. Write $P = [x(t) : y(t) : z(t)]$ in homogeneous coordinates, where $x, y, z \in K[t]$ with $\gcd(x, y, z) = 1$. Since $[x(0) : y(0) : z(0)]$ should be a singular point on a cubic curve $y^2 = x^3$, we see that $x(0) = y(0) = 0$ and $z(0) \neq 0$. Then we have

$$\sum_{i=0}^{2}\sum_{j=0}^{3} a_{9-2i-3j}x(t)^i y(t)^j z(t)^{3-i-j} + (t^2\widetilde{x}(t)^3 - t\widetilde{y}(t)^2 z(t)) = 0,$$

where $\widetilde{x} = x/t$ and $\widetilde{y} = y/t$. By the substitution $t = 0$, we have $a_9 z(0)^3 = z(0)^3 = 0$. This is a contradiction. Thus $E_{t,1}$ is non-singular. Non-singularity of $E_{r(t),s(t)}$ is similar. □

Lemma 2. (i) *Assume that α_1 is contained in K. Then $E_{t,1}(K(t))$ has a rational point $O = (1/\alpha_1^2, 1/\alpha_1^3)$. (When $\alpha_1 = 0$, O is the point $[0 : 1 : 0]$ in the homogeneous coordinate.)*

(ii) *$E_{r(t),s(t)}(K(t))$ has a rational point $O = (t, 1)$.*

Proof. Clear. □

Thus we obtain elliptic curves $E_{t,1}$ and $E_{r(t),s(t)}$ defined over $K(t)$ from the polynomial $f(x)$ of degree 9. Let M be the minimal splitting field of f over K, i.e., $M = K(\alpha_1, \dots, \alpha_9)$. For any element $x \in M$, let V_x be the additive $\mathbf{Q}[G]$-submodule of M generated by x, where $G = \mathrm{Gal}(M/K)$. We prove the following

Theorem 3. (i) *Assume that $\alpha_1 \in K$. Then $E_{t,1}(M(t)) \otimes \mathbf{Q}$ contains a $\mathbf{Q}[G]$-submodule isomorphic to $V_{\alpha_i - \alpha_1}$ for each $i \geq 2$.*

(ii) *Assume that $f(1) \neq 0$. Then $E_{r(t),s(t)}(M(t)) \otimes \mathbf{Q}$ contains a $\mathbf{Q}[G]$-submodule isomorphic to $V_{\alpha_i - 1}$ for each i.*

Remark. We use the assumption $a_9 = 1$ (i.e., $\deg(f) = 9$) only for proving Lemma 1. This theorem holds even in the case $\deg(f) \leq 7$ if our curves $E_{t,1}$, $E_{r(t),s(t)}$ are non-singular.

The idea of the proof is to consider the specialization to a fiber with cusp (cf. Shioda [5]).

Proof. Since both cases are proven similarly, we treat only (ii). For each i, we have a rational point

$$P_i = \left(\frac{1}{\alpha_i^2}, \frac{1}{\alpha_i^3}\right) \in E_{r(t),s(t)}(M(t)).$$

Let W_i be a $\mathbf{Q}[G]$-submodule of $E_{r(t),s(t)}(M(t)) \otimes \mathbf{Q}$ generated by $P_i \otimes 1$. The substitution $t = 1$ induces a $\mathbf{Q}[G]$-homomorphism $W_i \to E^{\mathrm{ns}}_{r(1),s(1)}(M) \otimes \mathbf{Q}$. Here $E^{\mathrm{ns}}_{r(1),s(1)}(M)$ is the non-singular points of $E_{r(1),s(1)}(M)$ and we regard it as an abelian group with identity element $(1, 1)$ in the usual way. Since we have $r(1) = 0$ and $s(1) \neq 0$ by the assumption $f(1) \neq 0$, $E_{r(1),s(1)}$ is a singular cubic curve defined by $y^2 = x^3$. Hence we have a $\mathbf{Q}[G]$-isomorphism $E^{\mathrm{ns}}_{r(1),s(1)}(M) \otimes \mathbf{Q} \xrightarrow{\sim} M$ defined by $(x, y) \otimes a \mapsto (x/y - 1)a$. The image of $P_i \otimes 1 \in W_i$ in M is $\alpha_i - 1$ and we have a surjective $\mathbf{Q}[G]$-homomorphism $W_i \to V_{\alpha_i - 1}$. Since $\mathbf{Q}[G]$ is semisimple, W_i has a $\mathbf{Q}[G]$-submodule isomorphic to $V_{\alpha_i - 1}$. □

By the specialization theorem due to Silverman (cf. [6]), we also have an infinite family of elliptic curves over K with similar property:

Corollary 4. *Assume that $f(1) \neq 0$. Then there exists a finite set $I \subset K$ such that $E_{r(t_0),s(t_0)}$ is an elliptic curve over K and $E_{r(t_0),s(t_0)}(M) \otimes \mathbf{Q}$ contains $V_{\alpha_i - 1}$ for each i and any $t_0 \in K \setminus I$.*

Let L be an extension of K of degree at most 9 and M the Galois closure of L/K with Galois group G. We consider a $\mathbf{Q}[G]$-module $V_{L/K} = \mathbf{Q}[G] \otimes_{\mathbf{Q}[\mathrm{Gal}(M/L)]} \mathbf{Q}$. (We regard $\mathbf{Q}$ as a $\mathbf{Q}[H]$-module by the trivial H-action for any subgroup $H \subset G$.) $V_{L/K}$ is decomposed as $V_{L/K} \cong V'_{L/K} \oplus \mathbf{Q}$. Rohrlich's result mentioned before is that $E_{1,b}(M) \otimes \mathbf{Q}$ contains a $\mathbf{Q}[G]$-submodule isomorphic to $V'_{L/K}$ for a suitable $f \in K[x]$. Our theorem gives an elliptic curve whose Mordell-Weil group contains $V_{L/K}$.

Corollary 5. (i) *In the notation above, there exists an elliptic curve E defined over K such that $E(M) \otimes \mathbf{Q}$ contains a $\mathbf{Q}[G]$-submodule isomorphic to $V_{L/K}$.*

(ii) *We have $\mathrm{rank}_{\mathbf{Z}} E(K) > 0$ and*

$$\mathrm{rank}_{\mathbf{Z}} E(L) > \mathrm{rank}_{\mathbf{Z}} E(K')$$

for any $K \subset K' \subsetneq L$.

Proof. Let $\alpha' \in M$ be a generator of a normal basis of M/K. Then we have $\mathrm{Tr}_{L/K}(\alpha) = 0$, where $\alpha = [L : K]\,\mathrm{Tr}_{M/L}(\alpha') - \mathrm{Tr}_{M/K}(\alpha') \in L$. Let $g(x)$ be the minimal polynomial of α over K and $f(x) = x^{9-[L:K]}g(x) \in K[x]$. Then a monic $f(x)$ of degree 9 satisfies $a_8 = 0$, $f(1) \neq 0$ and $f(\alpha) = 0$. For the elliptic curve $E_{r(t),s(t)}$ corresponding to this f, there exists a $t_0 \in K$ such that $E_{r(t_0),s(t_0)}(M) \otimes \mathbf{Q} \supset$

$V_{\alpha-1}$. We see that $\dim_{\mathbf{Q}} V_{\alpha-1} = [L : K]$. Hence we have $V_{\alpha-1} = V_{L/K}$ and $E = E_{r(t_0),s(t_0)}$ satisfies the assertion (i). (ii) follows from the definition of $V_{L/K}$. □

3. Examples. By using Theorem 3 and its corollaries, we can easily find an elliptic curve $E_{r(t),s(t)}$ over $\mathbf{Q}(t)$ such that $E_{r(t_0),s(t_0)}$ satisfies $n_2 \geq 3$ (resp. $n_3 \geq 2$, $n_5 \geq 1$, $n_7 \geq 1$) for all but finitely many $t_0 \in \mathbf{Q}$. However, it is difficult in general to determine all the exceptional t_0's explicitly. We give here a sufficient condition that $E_{r(t_0),s(t_0)}$ satisfies the above property for a given $t_0 \in \mathbf{Q}$. In the following, we denote by A_{tors} the torsion subgroup of an abelian group A. We also write $N_{p,n}$ for the map $E(F_{p,n}) \to E(F_{p,n-1})$ defined by $x \mapsto \sum_{\sigma \in \mathrm{Gal}(F_{p,n}/F_{p,n-1})} x^{\sigma}$.

Lemma 6. *Let E be an elliptic curve defined over $\mathbf{Q}$ and assume that there is a point $Q \in E(F_{p,n})$ not in $E(F_{p,n-1})$. Then $\mathrm{rank}_{\mathbf{Z}} E(F_{p,n}) > \mathrm{rank}_{\mathbf{Z}} E(F_{p,n-1})$ if one of the following conditions holds*:

(i) $Q \notin E(F_{p,n})_{\mathrm{tors}}$ *and* $N_{p,n}(Q) \in E(F_{p,n-1})_{\mathrm{tors}}$.

(ii) $E(F_{p,n})_{\mathrm{tors}} = E(F_{p,n-1})_{\mathrm{tors}}$ *and* $E(F_{p,n})[p] = 0$.

Proof. It suffices to show that $R = Q^{\sigma} - Q$ for a generator σ of $\mathrm{Gal}(F_{p,n}/F_{p,n-1})$ has infinite order since this implies that $kQ \notin E(F_{p,n-1})$ for any positive integer k. We have $N_{p,n}(Q) = pQ + \sum_{i=1}^{p-1} iR^{\sigma^{i-1}}$. If (i) holds, $\sum_{i=1}^{p-1} iR^{\sigma^{i-1}}$ has infinite order. In particular, $R \notin E(F_{p,n})_{\mathrm{tors}}$. If (ii) holds and R has a finite order, R is in $E(F_{p,n-1})$. This implies $pQ \in E(F_{p,n-1})$ and so $pR = pQ^{\sigma} - pQ = 0$. This contradicts to $E(F_{p,n})[p] = 0$ since $R \neq 0$ by assumption. □

In the following examples, we denote by ζ_m a primitive m-th root of unity for each $m > 1$.

Example 1. Let $p = 2$ and $f(x) = x(x^8 - 8x^6 + 20x^4 - 16x^2 + 2)$. Then $\alpha = \zeta_{32} + \zeta_{32}^{-1}$ satisfies $f(\alpha) = 0$ and we have $F_{2,3} = \mathbf{Q}(\alpha)$. By Theorem 3, $E_{r(t),s(t)}(F_{2,3}(t)) \otimes \mathbf{Q}$ contains a $\mathbf{Q}[\mathrm{Gal}(F_{2,3}/\mathbf{Q})]$-submodule isomorphic to $V_{\alpha-1}$, where $r(t) = 1 - t^3$ and $s(t) = 20t^2 - 6t - 15$. Consider the curve $E_{1,-15}$ obtained by the substitution $t = 0$. This curve has a minimal Weierstrass model $E : y^2 = x^3 - 2x + 1$. The conductor of E is 40 and we have $E(\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}$. Moreover, we have $E(F_{2,3})_{\mathrm{tors}} = E(\mathbf{Q})$. Indeed, for a prime $l = 31$ (resp. 97, 127), the prime-to-l part of $E(F_{2,3})_{\mathrm{tors}}$ maps injectively to $E(\mathbf{F}_l)$ since l splits completely in $F_{2,3}/\mathbf{Q}$. The order of $E(\mathbf{F}_l)$ is 40 (resp. 112, 140), and this implies the order of $E(F_{2,3})_{\mathrm{tors}}$ divides 4. A rational point

$$P = \left(\frac{2\alpha^3 - 6\alpha}{\alpha^3 - 3\alpha - 1}, \frac{\alpha^6 - 8\alpha^4 + 15\alpha^2 - 1}{(\alpha^3 - 3\alpha - 1)^2} \right) \in E(F_{2,3})$$

corresponding to $(1/\alpha^2, 1/\alpha^3) \in E_{1,-15}(F_{2,3})$ is not in $E(\mathbf{Q})$. Hence P has infinite order. Since $N_{2,3}(P) = (1,0)$ has order 2, we have $\mathrm{rank}_{\mathbf{Z}} E(F_{2,3}) > \mathrm{rank}_{\mathbf{Z}} E(F_{2,2})$, i.e., $n_2(E) \geq 3$ by Lemma 6.

Example 2. Let $p = 3$ and $f(x) = x^9 - 9x^7 + 27x^5 - 30x^3 + 9x + 1$. We have $F_{3,1} = \mathbf{Q}(\alpha)$ and $f(\alpha) = 0$, where $\alpha = \zeta_{27} + \zeta_{27}^{-1}$. Consider the curve $E_{1,28}$, which is obtained from $E_{1-t^3,28-27t^2}$ by the substitution $t = 0$, corresponding to this f. $E_{1,28}$ has a minimal Weierstrass model $E : y^2 + y = x^3 - 18x + 28$. The conductor of E is 9495 and $E(\mathbf{Q}) \cong \mathbf{Z}^2$. By considering the reduction of E at 19 and 37, we see that $E(F_{3,2})_{\mathrm{tors}} = E(F_{3,1})_{\mathrm{tors}} = 0$. Therefore, $\mathrm{rank}_{\mathbf{Z}} E(F_{3,2}) > \mathrm{rank}_{\mathbf{Z}} E(F_{3,1})$ by Lemma 6. Especially we have $n_3(E) \geq 2$.

Example 3. Let $p = 5$ and $g(x) = x^5 - 10x^3 + 5x^2 + 10x + 1$. Then $F_{5,1}$ is generated over $\mathbf{Q}$ by a root α of $g(x)$. For $f(x) = xg(x)$, the curve $E_{r(t),s(t)} = E_{1-t^3,10t^2-9t+6}$ is non-singular. By Theorem 3, $E_{r(t),s(t)}(F_{5,1}) \otimes \mathbf{Q}$ contains $V_{\alpha-1}$ (see the remark after Theorem 3). If we take $t = 0$, $E_{1,6}$ has a minimal Weierstrass model $y^2 = x^3 - 99x + 379$ of conductor 7704. We see that $E_{1,6}(\mathbf{Q}) \cong \mathbf{Z}$ and $E_{1,6}(F_{5,1})_{\mathrm{tors}} = 0$. Hence we have $n_5(E_{1,6}) \geq 1$ by Lemma 6. Another construction of elliptic curves with $n_5 \geq 1$ will be found in [3]. For example, we see that the elliptic curve defined by $y^2 = x^3 - 7x$ (conductor 3136) satisfies $n_5 \geq 1$.

Example 4. Let $p = 7$ and $f(x) = x^7 - 70x^5 - 21x^4 + 91x^3 + 63x^2 + 14x + 1$. We have $F_{7,1} = \mathbf{Q}(\alpha)$ for a root α of f. The curve $E_{r(0),s(0)} = E_{1,92}$ has a minimal Weierstrass model $y^2 + xy = x^3 - x^2 - 491x + 4315$ of conductor 714362. We see that $E_{1,92}(\mathbf{Q}) \cong \mathbf{Z}^2$ and $E_{1,92}(F_{7,1})_{\mathrm{tors}} = 0$. Hence we have $n_7(E_{1,92}) \geq 1$.

4. Function field case. In the preceding sections, we discussed about the behavior of the Mordell-Weil rank of elliptic curves in the cyclotomic $\mathbf{Z}_p$-extension over $\mathbf{Q}$. We consider an analogous question for elliptic curves over a function field $\mathbf{F}_l(t)$. For a prime $p \neq l$, let $\mathcal{F}_{p,\infty}$ be the unique $\mathbf{Z}_p$-extension of $\mathbf{F}_l(t)$ contained in $\overline{\mathbf{F}_l}(t)$. The n-th layer of this $\mathbf{Z}_p$-extension is $\mathbf{F}_{l^{p^n}}(t)$. For any elliptic curve A defined over $\mathbf{F}_l(t)$, we know that $A(\mathcal{F}_{p,\infty})$ is finitely generated (modulo torsion when A is defined over $\mathbf{F}_l$), so the rank of $A(\mathbf{F}_{l^{p^n}}(t))$ is bounded as n varies. We denote by $n_p(A)$ the smallest non-negative integer n satisfying $\mathrm{rank}_{\mathbf{Z}} A(\mathbf{F}_{l^{p^n}}(t)) = \mathrm{rank}_{\mathbf{Z}} A(\mathcal{F}_{p,\infty})$, similarly to the number field case. We prove the existence of elliptic curves with arbitrary large n_p in this function field situation.

Proposition 7. *For any non-negative integer n, there exists an elliptic curve A over $\mathbf{F}_l(t)$ with $n_p(A) = n$.*

This proposition is easily deduced from the following result of Ulmer ([7]). For a positive integer d, let A_d be an elliptic curve over $\mathbf{F}_l(t)$ defined by the equation $A_d : y^2 + xy = x^3 - t^d$.

Theorem 8 (Ulmer)**.** *Assume that d divides $l^m + 1$ for some m. Then we have*

$$\mathrm{rank}_{\mathbf{Z}} A_d(\mathbf{F}_{l^i}(t)) = \sum_{\substack{e \mid d \\ e \nmid 6}} [(\mathbf{Z}/e\mathbf{Z})^\times : \langle l^i \rangle] + \epsilon(d,i)$$

for each $i \geq 1$. Here $\epsilon(d,i)$ is a non-negative integer less than 4.

Proof of Proposition 7. We have $\mathrm{rank}_{\mathbf{Z}} A_1(\overline{\mathbf{F}_l}(t)) = 0$ and so $n_p(A_1) = 0$ for any $p \neq l$. Assume that $n > 0$ in the following. When d is a prime number greater than 3 and $l^m \equiv -1 \pmod{d}$ for some m, we have $\epsilon(d,i) = 0$ and $\mathrm{rank}_{\mathbf{Z}} A_d(\mathbf{F}_{l^i}(t)) = [(\mathbf{Z}/d\mathbf{Z})^\times : \langle l^i \rangle]$ for any $i \geq 1$ by Theorem 8. Hence we have $n_p(A_d) = n$ for a prime $d > 3$ such that $o_d(l)$ is even and $p^n || o_d(l)$, where $o_d(l)$ is the order of l in $(\mathbf{Z}/d\mathbf{Z})^\times$. Let K be an extension of $\mathbf{Q}(\zeta_{p^n})$ of degree p contained in $L = \mathbf{Q}(\zeta_{p^{n+1}}, \sqrt{l}, \sqrt[p]{l})$, neither $\mathbf{Q}(\zeta_{p^{n+1}})$ nor $\mathbf{Q}(\zeta_{p^n}, \sqrt[p]{l})$. Applying Chebotarev's density theorem to a Galois extension $L/\mathbf{Q}$, we can take a prime $d > 3$ such that a Frobenius element σ at d in $\mathrm{Gal}(L/\mathbf{Q})$ is a generator of $\mathrm{Gal}(L/K)$. Since the restriction of σ to $\mathbf{Q}(\sqrt{l})$ is non-trivial, l is not quadratic residue modulo d, i.e., $o_d(l)$ is even. Similarly, l is p-th power free in $(\mathbf{Z}/d\mathbf{Z})^\times$ since the restriction of σ to $\mathbf{Q}(\zeta_p, \sqrt[p]{l})$ is a generator of $\mathrm{Gal}(\mathbf{Q}(\zeta_p, \sqrt[p]{l})/\mathbf{Q}(\zeta_p))$. Hence $(d-1)/o_d(l)$ is prime to p. The restriction of σ to $\mathbf{Q}(\zeta_{p^{n+1}})$ is a generator of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{n+1}})/\mathbf{Q}(\zeta_{p^n}))$ and this implies $p^n || (d-1)$. Hence we have $p^n || o_d(l)$ as desired. □

Acknowledgments. The author thanks Masato Kuwata for many valuable suggestions. He was partially supported by Grant-in-Aid for Young Scientists.

References

[1] Chinta, G.: Analytic ranks of elliptic curves over cyclotomic fields. J. Reine Angew. Math., **544**, 13–24 (2002).

[2] Greenberg, R.: Introduction to Iwasawa theory for elliptic curves. Arithmetic Algebraic Geometry (Park City, UT, 1999), IAS/Park City Math. Ser. 9, Amer. Math. Soc., Providence, pp. 407–464 (2001).

[3] Matsuno, K.: Mordell-Weil group of an elliptic curve associated with a polynomial of degree five. (In preparation).

[4] Rohrlich, D. E.: Realization of some Galois representations of low degree in Mordell-Weil groups. Math. Research Letters, **4**, 123–130 (1997).

[5] Shioda, T.: An infinite family of elliptic curves over $\mathbf{Q}$ with large rank via Néron's method. Invent. Math., **106**, 109–119 (1991).

[6] Silverman, J. H.: Heights and the specialization map for families of abelian varieties. J. Reine Angew. Math., **342**, 197–211 (1983).

[7] Ulmer, D.: Elliptic curves with large rank over function fields. Ann. of Math., **155**, 295–315 (2002).