Research Article
On the Rank of Elliptic Curves in Elementary Cubic Extensions

Rintaro Kozuma

College of International Management, Ritsumeikan Asia Pacific University, Oita 874-8577, Japan

Correspondence should be addressed to Rintaro Kozuma; rintaro@apu.ac.jp

Received 21 July 2015; Accepted 6 September 2015

Academic Editor: Andrej Dujella

Copyright © 2015 Rintaro Kozuma. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We give a method for explicitly constructing an elementary cubic extension $L$ over which an elliptic curve $E_D : y^2 + Dy = x^3 \ (D \in \mathbb{Q}^*)$ has Mordell-Weil rank of at least a given positive integer by finding a close connection between a 3-isogeny of $E_D$ and a generic polynomial for cyclic cubic extensions. In our method, the extension degree $[L : \mathbb{Q}]$ often becomes small.

1. Introduction

Let $E$ be an elliptic curve defined over a number field $F$. It is well-known that the Mordell-Weil group $E(F)$ of $F$-rational points on $E$ forms a finitely generated abelian group, and its rank $\text{rank}(E(F)) = \dim_{\mathbb{Q}} E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$ is of great interest in arithmetic geometry. The present paper is motivated by the following general problem:

To understand the behavior of ranks of elliptic curves in towers of finite extensions over $F$.

This problem dates back at least to [1], which first introduced an Iwasawa theory for elliptic curves. In the context of Iwasawa theory, Kurcanov [2] showed that if an elliptic curve $E$ over $\mathbb{Q}$ without complex multiplication has good reduction at a prime number $p > 3$ satisfying a mild condition then $E$ has infinite rank in a certain $\mathbb{Z}_p$-extension, and Harris [3] showed that if $E$ is a modular elliptic curve over $F$ having good ordinary reduction at $p$ and a specific $F$-rational point arising from the modular curve then there is a $p$-adic Lie extension of $F$ in which the rank of $E$ grows infinitely. On the other hand, Kida [4] constructed a tower of elementary 2-extensions in which the rank of $y^2 = x^3 - n^2x$ becomes arbitrarily large by using a result in theory of congruent numbers. Also, Dokchitser [5] proved that for any elliptic curve $E$ over $F$ there are infinitely many cubic extensions $K/F$ so that the rank of $E$ increases in $K/F$. In the present paper, we consider the specific curve

$$E_D : y^2 + Dy = x^3, \quad D \in \mathbb{Q}^*, \quad (1)$$

and give an explicit construction of an elementary cubic extension over which the elliptic curve $E_D$ is of rank of at least a given positive integer $l$ by finding a close connection between a 3-isogeny of $E_D$ and a generic polynomial for cyclic cubic extensions. We shall call an extension $K/F$ an elementary cubic extension if $K$ is a finite compositum of cubic extensions over $F$. Compared with related results as above, in our method, the extension degree $[L : \mathbb{Q}]$ often becomes small. The question of finding a small elementary cubic extension with rank $\geq l$ seems to be of independent interest.

2. Main Results

Let

$$S_{D} = \{ b \in \mathbb{Z} \mid D = a^2 + 3ab + 9b^2 \ (a, b \in \mathbb{Z}, \ b > 0) \}, \quad (2)$$

where $a$ is relatively prime to $b$.

We denote by $\overline{F}$ a fixed algebraic closure of $F$. Let $F(\sqrt[3]{S_D})$ denote the field obtained by adjoining a real number $\sqrt[3]{b}$ for each $b \in S_D$ to $F$. Since the set $S_D$ is finite, the extension $F(\sqrt[3]{S_D})/F$ is also finite. The main result of the paper is the following theorem.

**Theorem 1.** Let $D$ be any square-free product of distinct primes $p_1, \ldots, p_k \in \mathbb{Z}$ satisfying $p_i \equiv 1 \pmod{3}$. Then, for any positive
Table 1: rank $E_D(L) \geq k$.

<table>
<thead>
<tr>
<th>$D$</th>
<th>$L$</th>
<th>rank $E_D(L)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 ⋅ 421</td>
<td>$\mathbb{Q}$</td>
<td>$\geq 2$</td>
</tr>
<tr>
<td>19 ⋅ 277</td>
<td>$\mathbb{Q}$</td>
<td>$\geq 2$</td>
</tr>
<tr>
<td>31 ⋅ 373</td>
<td>$\mathbb{Q}$</td>
<td>$\geq 2$</td>
</tr>
<tr>
<td>109 ⋅ 1153</td>
<td>$\mathbb{Q}$</td>
<td>$\geq 2$</td>
</tr>
<tr>
<td>7 ⋅ 19 ⋅ 37</td>
<td>$\mathbb{Q}(\sqrt{17})$</td>
<td>$\geq 3$</td>
</tr>
<tr>
<td>7 ⋅ 19 ⋅ 229</td>
<td>$\mathbb{Q}(\sqrt{3})$</td>
<td>$\geq 3$</td>
</tr>
<tr>
<td>7 ⋅ 43 ⋅ 127</td>
<td>$\mathbb{Q}(\sqrt{61})$</td>
<td>$\geq 3$</td>
</tr>
<tr>
<td>7 ⋅ 43 ⋅ 127</td>
<td>$\mathbb{Q}(\sqrt{73})$</td>
<td>$\geq 3$</td>
</tr>
<tr>
<td>109 ⋅ 349 ⋅ 457</td>
<td>$\mathbb{Q}(\sqrt{307})$</td>
<td>$\geq 3$</td>
</tr>
</tbody>
</table>

integer $l \leq k$, we can construct a subfield $L$ of $\mathbb{Q}(\sqrt{D})$ such that

$$\text{rank } E_D(L) \geq l, \quad [L : \mathbb{Q}] \leq 3^l. \tag{3}$$

As we will see in Section 4, the field $L$ in Theorem 1 is effectively computable from the decomposition of the primes $p_1, \ldots, p_k$ in $\mathbb{Z}[\zeta_3]$, where $\zeta_3$ denotes a primitive cube root of unity. See Remark 4 for this computation. It will also turn out in Section 4 that the field $L$ is constructed using certain products of prime elements in $\mathbb{Z}[\zeta_3]$ above each prime $p_i$, and in particular $L$ depends only on the primes $p_1, \ldots, p_k \equiv 1 \pmod{3}$ and a positive integer $l \leq k$. One question arises here: how small can $[L : \mathbb{Q}]$ be when $p_1, \ldots, p_k$ vary through the set of all primes $p \equiv 1 \pmod{3}$ for a fixed integer $l \leq k$? We give some examples in the case $l = k$ (Table 1).

Corollary 2. Let $D$ be any square-free product of distinct primes $p_1, \ldots, p_k \in \mathbb{Z}$ satisfying $p_i \equiv 1 \pmod{3}$. Then, for any positive integer $l$, we can construct a subfield $L'$ of $\mathbb{Q}(\sqrt{D}, \sqrt{3})$ with some integer $d$ such that

$$\text{rank } E_D(L') \geq l, \quad [L' : \mathbb{Q}] \leq 3^{l+1}. \tag{4}$$

Note that our construction in Theorem 1 (resp., Corollary 2) differs from Dokchitser’s [5], and the extension degree $[L : \mathbb{Q}]$ (resp., $[L' : \mathbb{Q}]$) is often smaller than or equal to $3^{l+1}$ (resp., $3^l$).

3. A Connection between the Elliptic Curve $E_D$ and a Generic Polynomial for Cyclic Cubic Extensions

In this section, let $F$ be a perfect field with characteristic not equal to 3, and let $D$ be any element in $F^*$. The elliptic curve $E_D$ has a rational 3-torsion point $(0, 0)$ and admits a 3-isogeny $\phi : E_D \to \hat{E}_D = E_D / \langle (0, 0) \rangle$ over $F$. The 3-isogeny $\phi$ can be explicitly written as

$$\phi : E_D \to \hat{E}_D$$
$$ (x, y) \mapsto \left( \frac{x^3 + D^2}{Dx^2}, \frac{-(y/D)^3 + 3(-y/D) - 1}{(-y/D)(-y/D - 1)} \right). \tag{5}$$

The isogenous elliptic curve is given by the form

$$\hat{E}_D^* : t^2 + 3t + 9 = Ds^3. \tag{6}$$

Taking Galois cohomology of the short exact sequence $0 \to E_D[\phi] \to E_D \xrightarrow{\phi} \hat{E}_D \to 0$ yields a Kummer map

$$\frac{\hat{E}_D(F)}{\phi(E_D(F))} \to H^1(F, E_D[\phi]) \tag{7}$$

$$P \mapsto \{ \sigma \mapsto \phi^{-1}(P)^{\sigma-1} \}.$$ Combining this map with the map

$$H^1(F, E_D[\phi]) = \text{Hom}(\text{Gal}(\overline{F} / F), \mathbb{Z}/3\mathbb{Z})$$
$$\to \mathfrak{Gal}(\mathbb{C}_3 / F)$$
$$\xi \mapsto F^{Ker \xi},$$

where $\mathfrak{Gal}(\mathbb{C}_3 / F)$ denotes the set of all cyclic cubic extensions over $F$ together with $F$,

$$\mathfrak{Gal}(\mathbb{C}_3 / F) := \{ K / F : \text{a Galois extension in } \overline{F} \big| \text{Gal} \left( \frac{K}{F} \right) \hookrightarrow C_3 \} \tag{9}$$

$$= \mathbb{Z}/3\mathbb{Z},$$

we have a map

$$\delta_F : \hat{E}_D(F) / \phi(E_D(F)) \to \mathfrak{Gal}(\mathbb{C}_3 / F) \tag{10}$$
$$P \mapsto F^{\phi^{-1}(P)}.$$ It is well-known that the set $\mathfrak{Gal}(\mathbb{C}_3 / F)$ is parametrized by a generic polynomial for $C_3$-extensions [6]

$$g(x; t) = x^3 + tx^2 - (t + 3)x + 1 \quad \text{with } t \in F, \tag{11}$$

which has discriminant $(t^2 + 3t + 9)^2$. We shall denote by $K_t$ the minimal splitting field of $g(x; t)$ over $F_0(t)$, where $F_0$ stands for the prime field in $F$. By the property of $g(x; t)$, for any $K/F \in \mathfrak{Gal}(\mathbb{C}_3 / F)$ there is some $t \in F$ so as to be $K = K_t$ in $F$.

The following proposition is the key observation in the present paper.

Proposition 3. The connecting homomorphism $\delta_F$ is given by

$$\delta_F(s, t) = K_t F$$

for any $(s, t) \in \hat{E}_D^*(F)$. Furthermore, in the case where $F$ is a number field, for any prime ideal $\mathfrak{p}$ of $F$ not dividing 3, the $\mathfrak{p}$-component of the conductor of $K_t F / F$ is

$$\mathfrak{p} \text{ if } v_F(Ds^3) > 0, \quad v_F(D) \equiv 0 \pmod{3} \quad \text{or otherwise.} \tag{12}$$

Here $v_F : F^*_F \to \mathbb{Z}$ denotes the normalized valuation of the $\mathfrak{p}$-adic completion $F_\mathfrak{p}$.
Proof. For any \((s, t) \in \overline{E}_D(F)\), take a point \((x, y)\) on \(E_D\) satisfying \(\phi(x, y) = (s, t)\). By the form of the \(y\)-coordinate of (5), the splitting field \(K_i\) coincides with \(F_0(t, y)\). Here \(F(x, y) = F(x) = F(y)\). The latter part of the proposition follows from the equation \(t^2 + 3t + 9 = D_3^2\) by using Proposition 8.1 in [7].

4. A Method for Constructing an Elementary Cubic Extension

From now on, let \(D\) be a square-free product of distinct primes \(p_1, \ldots, p_k \in \mathbb{Z}\) satisfying \(p_i \equiv 1 \, (\mod 3)\), and let \(l\) be a positive integer \(\leq k\).

Recall a result of Komatsu [8] that the set of all cyclic cubic fields (i.e., cyclic cubic extensions over \(Q\)) of conductor \(D = p_1 \ldots p_k\) has a one-to-one correspondence to the subset of the algebraic torus \(T(Q) = \mathbb{Q} \cup \{ \infty \}\) consisting of \(2^{k-1}\) elements of the form

\[
c_{p_i}^{e_i} c_{p_{i-1}}^{e_{i-1}} \cdots c_{p_1}^{e_1} c_{\infty}^{e_{\infty}},
\]

where \(e_{\infty}\) is the composition of \(T(Q)\) given by \(a/b_{\infty} c/d = (a/b \cdot c/d - 1)/(a/b + c/d + 1)\), \(c_{p_i}\) denotes the inverse of \(c_{p_i}\) given by \(c_{p_i}^{-1} = a_i/b_i \cdot c_{p_i} - 1\), and \(e_{p_i} = e_{p_i}/f_{p_i} \in T(Q)\) is a rational number so that the pair \((e_{p_i}, f_{p_i})\) of integers is unique in the sense of Lemma 2.1 in [8] (especially \(f_{p_i} \equiv 0 \, (\mod 3)\), which will be used in the following) and satisfies

\[
e^2_{p_i} + e_{p_i} f_{p_i} + f^2_{p_i} = (e_{p_i} - f_{p_i} \zeta_3) (e_{p_i} - f_{p_i} \zeta_3^2) = p_i.
\]

There is a group isomorphism \(\phi : T \rightarrow G_m\) mapping \(t\) to \((t - \zeta_3)/(t - \zeta_3^{-1})\), where \(G_m\) denotes the multiplicative group. Then the composition \(\tau\) is written as \(a/b + c/d = \tau^{-1}(\phi(a/b)\phi(c/d))\).

Now, let \(n_i := e_{p_i} - f_{p_i} \zeta_3\), which is a prime element in \(Z[\zeta_3]\) dividing \(p_i\), and let \(\overline{a}\) denote the complex conjugation of \(a\). For each \(i (1 \leq i \leq l)\), let

\[
t_i = \begin{cases} \sum e_{p_i} c_{p_i}^{e_{p_i}} & \text{if } i = 1 \\ \sum e_{p_i} c_{p_{i-1}}^{e_{p_i-1}} c_{p_i}^{e_{p_i}} & \text{if } i \neq 1 \end{cases}
\]

Since \(f_{p_i} \equiv 0 \, (\mod 3)\) for each \(i\), there exist unique integers \(a_i, b_i\) so that

\[
a_i - 3b_i \zeta_3 = \begin{cases} \prod a_i \zeta_3 & \text{if } i = 1 \\ \prod a_i a_{i-1} \zeta_3 & \text{if } i \neq 1 \end{cases}
\]

where \(a_i\) is relatively prime to \(3b_i\). Then \(\phi(t_i/3) = (a_i - 3b_i \zeta_3)/(a_i - 3b_i \zeta_3^2)\), and thus \(t_i = 3 \cdot \phi^{-1}(\phi(t_i/3)) = a_i/b_i\).

Let \(L := \mathbb{Q}(\sqrt[3]{p_i} \mid 1 \leq i \leq l)\).

Remark 4. In order to calculate \(t_i = a_i/b_i\), we have only to know the values \(c_{p_i}\) by the definition of \(t_i\). For example, one can use Table 5.1 in [8], in which the values \(c_{p_i}\) for \(p < 1000\) are listed. From the construction of \(L\), the field \(L\) depends only on \(D = p_1 \ldots p_k\) and a positive integer \(l \leq k\).

Lemma 5. Every prime number \(p_i (1 \leq i \leq l)\) is unramified in \(L\).

Proof. Since \(p_i\) does not divide \(3b_i \cdots b_l\) and is unramified in \(Q(\zeta_3)\), it turns out that \(p_i\) is unramified in \(Q(\zeta_3, \sqrt[3]{b_i} \mid 1 \leq i \leq l)\) by Kummer theory. Hence, \(p_i\) is also unramified in \(L = Q(\sqrt[3]{b_i} \mid 1 \leq i \leq l)\).

Proposition 6. \(K_i \cap L \cap L = 1 \cap \delta_l - L \cap L = 1 \cap l\) for any \(i (1 \leq i \leq l)\).

Proof. Since \((a_i - 3b_i \zeta_3)/(a_i - 3b_i \zeta_3^2) = D, we have

\[
t_i^2 + 3t_i + 9 = D \left(\sqrt[3]{b_i} \right)^3.
\]

Thus \((\sqrt[3]{b_i}^2, t_i) \in \overline{E}_D(L)\). It follows from Proposition 3 that \(\delta_l(\sqrt[3]{b_i}^2, t_i) = K_i \cap L\), and hence \(K_i \cap L \in 1 \cap \delta_l\). Combining Proposition 3 with Lemma 5 yields \(K_i \cap L \neq L\).

Proposition 7. \(\dim_{\mathbb{Q}} \overline{E}_D(L)/\phi(\overline{E}_D(L)) = l\).

Proof. One can easily verify that \((0, 3\zeta_3)\) is a 3-torsion point in \(\overline{E}_D(L(\zeta_3^3))\), and the rational function \(f = (t - 3\zeta_3)/D^3\) on \(\overline{E}_D\) has a zero of order 3 at \(0, 3\zeta_3\) and a pole of order 3 at infinity and satisfies

\[
f \circ \phi = \left(\frac{y - D\zeta_3}{Dx} \right)^3.
\]

Then there exists an injective homomorphism (see [9] for details):

\[
\overline{E}_D(L(\zeta_3)) \xrightarrow{\phi} L(\zeta_3)^* \xrightarrow{L(\zeta_3)^*} L(\zeta_3)^3.
\]

Thus

\[
(s, t) \mapsto D(t - 3\zeta_3) L(\zeta_3)^3.
\]

Combining this with the natural map

\[
\overline{E}_D(L) \xrightarrow{\phi} \overline{E}_D(L(\zeta_3)) \xrightarrow{\phi} L(\zeta_3)^3
\]

we have the homomorphism

\[
\overline{E}_D(L) \xrightarrow{\phi} L(\zeta_3)^3.
\]

By Proposition 6, the point \((\sqrt[3]{b_i}^2, t_i) \in \overline{E}_D(L)\) corresponds to \(D(t_i - 3\zeta_3)L(\zeta_3)^3 = D(a_i - 3b_i \zeta_3)L(\zeta_3)^3\) via the above homomorphism. It thus suffices to show that \([D(a_i - 3b_i \zeta_3) \mid 1 \leq i \leq l]\) is linearly independent in \(L(\zeta_3)^* / L(\zeta_3)^3\). Then the points \(\{(\sqrt[3]{b_i}^2, t_i) \mid 1 \leq i \leq l\}\) must be linearly independent in \(\overline{E}_D(L)/\phi(\overline{E}_D(L))\). Assume that

\[
y := \prod_{1 \leq i \leq l} \left(D(a_i - 3b_i \zeta_3) \right)^{t_i} \in L(\zeta_3)^3
\]
for some integers \( \{ \tau_i \}_{1 \leq i \leq l} \). For each \( i \), let \( p_i \) be a prime ideal of \( L(\zeta_3) \) above the prime element \( \tau_i \in \mathbb{Q}(\zeta_3) \). For any prime ideal \( p \) of \( L(\zeta_3) \), we denote by \( v_p : L(\zeta_3) \rightarrow \mathbb{Z} \) the normalized (additive) valuation of the \( p \)-adic completion \( L(\zeta_3)_p \). By Lemma 5, we have \( v_{\overline{F}}(\overline{\tau}) = 1 \). Then

\[
y_{\overline{F}_l}(y) = \begin{cases} 
\sum_{i=1}^{l} \tau_i \equiv 0 \pmod{3} & \text{if } j = 1 \\
\sum_{i=1}^{l} \tau_i + r_j \equiv 0 \pmod{3} & \text{if } j \neq 1,
\end{cases}
\]

(23)

and hence \( \tau_i \equiv 0 \pmod{3} \) for each \( i \). This proves that \( \{ D(a_i - 3b \zeta_3) \mid 1 \leq i \leq l \} \) is linearly independent in \( L(\zeta_3)^*/L(\zeta_3)^{3*} \).

Let \( \widehat{\Phi} : \widehat{E}_D \rightarrow \widehat{E}_D \) be the dual isogeny to \( \Phi \). Since the composition \( \Phi \circ \Phi \) (resp., \( \Phi \circ \Phi \)) is the multiplication-by-3 map on \( \widehat{E}_D \) (resp., \( \widehat{E}_D \)), we have an exact sequence of \( \mathbb{F}_3 \)-vector spaces

\[
0 \rightarrow \widehat{E}_D(L)[3] \rightarrow \widehat{E}_D(L) \rightarrow \overline{\Phi}(\widehat{E}_D(L)) \rightarrow \overline{E}_D(L) \rightarrow 0,
\]

(24)

and thus

\[
\begin{aligned}
\dim_{\mathbb{F}_3} \overline{E}_D(L) &= \dim_{\mathbb{F}_3} \overline{E}_D(L) - \dim_{\mathbb{F}_3} \widehat{E}_D(L)[3] - \dim_{\mathbb{F}_3} \overline{E}_D(L)[3] \\
\end{aligned}
\]

(25)

Since \( \zeta_3 \notin L \), the group \( \widehat{E}_D(L)[\overline{\Phi}] \) is trivial and the group \( E_D(L)[3] \) is generated by the point \((0,0)\). We see that

\[
\begin{aligned}
\dim_{\mathbb{F}_3} \overline{E}_D(L) &= \dim_{\mathbb{F}_3} \overline{E}_D(L) - \dim_{\mathbb{F}_3} \overline{E}_D(L) - 1 \\
\end{aligned}
\]

(26)

Proof of Corollary 2. By Theorem 1, we have only to consider the case \( l > k \). In the case where \( l = k \), take \( d = 1 \). Take distinct prime numbers \( \{ q_1, \ldots, q_{l-k} \} \) not dividing \( D \) with \( q_i \equiv 1 \pmod{3} \). Let \( d := q_1 \cdots q_{l-k} \). Then, applying Theorem 1 to the elliptic curve \( E_{dD} \), there exists some subfield \( L \subset \mathbb{Q}(\sqrt[3]{d}) \) so as to be \( \operatorname{rank} E_{dD}(L) \geq 1 \) with \( [L : \mathbb{Q}] \leq 3^l \). Let \( L' := L(\sqrt[3]{d}) \). Then, it is easily seen that \( E_{dD} \) is isomorphic over \( L' \) to \( E_D \). Therefore, \( \operatorname{rank} E_D(L') = \operatorname{rank} E_{dD}(L') \geq \operatorname{rank} E_{dD}(L) \geq l \). Here \( [L' : \mathbb{Q}] \leq 3 \cdot [L : \mathbb{Q}] \leq 3^{l+1} \).

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The author is supported by APU Academic Research Subsidy.

References
