TOKYO J. MATH.
VOL. 34, NO. 2, 2011

Integer Points and Independent Points on the Elliptic Curve $y^2 = x^3 - p^k x$

Yasutsugu FUJITA and Nobuhiro TERAI

Nihon University and Ashikaga Institute of Technology

(Communicated by J. Murakami)

Abstract. Let E_k be the elliptic curve given by $y^2 = x^3 - p^k x$, where p is a prime number and $k \in \{1, 2, 3\}$. In this paper, we first give a necessary and sufficient condition for the rank of $E_k(\mathbf{Q})$ to equal one or two, respectively, and in the rank two case, explicitly describe independent points of free part of the Mordell-Weil group $E_k(\mathbf{Q})$. Secondly, we show several subfamilies of E_k whose integer points and ranks can be completely determined.

1. Introduction

Let E_k be the elliptic curve given by

$$E_k : y^2 = x^3 - p^k x$$

with a prime number p and a positive integer k. It is well-known that the torsion subgroup $E_k(\mathbf{Q})_{\text{tors}}$ of the Mordell-Weil group $E_k(\mathbf{Q})$ is either $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z}$ depending on whether k is even or not, respectively (cf. [9]). Our interest are in free part of the group $E_k(\mathbf{Q})$ and in integer points on the curve E_k.

Draziotis [4] and Walsh [16] have recently studied integer points on E_k (and the elliptic curve $y^2 = x^3 + p^k x$) very closely. For example, they showed that E_1 has at most four integer points other than $(0, 0)$ (see at the beginning of Section 4). Although they gave determination of (the number of) integer points on E_k, it remains to be considered for what kind of p one can completely determine the integer points on E_k for each k.

In consideration of free part of $E_k(\mathbf{Q})$, we may assume that $k \in \{1, 2, 3\}$. It is easy to check that $\operatorname{rank} E_k(\mathbf{Q})$, the rank of $E_k(\mathbf{Q})$, is 0, 1 or 2. Spearman [14] recently used the method in [1, Chapter 7] or in [13, Chapter 3] to show that $\operatorname{rank} E_1(\mathbf{Q}) = 2$ whenever $p = a^4 + b^4$ for positive integers a, b. He, however, did not give any points of infinite order on E_1.

In this paper, we first give a necessary and sufficient condition for the rank of $E_k(\mathbf{Q})$ to equal one or two, respectively, and in the rank two case, explicitly describe independent

Received April 15, 2010; revised August 6, 2010
Mathematics Subject Classification: 11D25, 11G05
Key words and phrases: elliptic curves, integer points, independent points, generators

points of free part of the group $E_k(\mathbf{Q})$ (Main Theorem in Section 2). Secondly, we find several subfamilies of E_k whose integer points and ranks can be completely determined (Theorems 1 to 7 in Sections 4 to 6). In the rank two case, we give two integer points on E_k which are independent, using Main Theorem. In the rank one case, we give a generator, which is an integer point, of $E_k(\mathbf{Q})$ modulo the torsion subgroup $E_k(\mathbf{Q})_{\mathrm{tors}}$. This can be done because the integer points on our subfamilies are completely determined (see Lemma 3).

The most fruitful result is for the curve $E_1 : y^2 = x^3 - px$, which can have more integer points than the others, even than any curve of the form $y^2 = x^3 + p^k x$. This is the reason why we consider the curve E_k not the curve $y^2 = x^3 + p^k x$.

REMARK 1. Duquesne [6] recently investigated integer points on the elliptic curve

$$C_t : y^2 = x^3 - (t^2 + 16)x$$

(with t^2+16 indivisible by an odd square) and the structure of the Mordell-Weil group $C_t(\mathbf{Q})$. More precisely, using the canonical height, he showed that if rank $C_t(\mathbf{Q}) = 1$, then $C_t(\mathbf{Q}) = \langle (0, 0), (-4, 2t)\rangle$, and the integer points on C_t are $(0, 0)$ and $(-4, \pm 2t)$. Moreover, in the case of $t = 6k^2 + 2k - 1$ with an integer k, assuming rank $C_t(\mathbf{Q}) = 2$, he gave the generator of $C_t(\mathbf{Q})$ (and completely determined the integer points on $Q_t : y^2 = x^4 - tx^3 - 6x^2 + tx + 1$, which is isomorphic to C_t over $\mathbf{Q}$). Concerning this result, since $t^2 + 16 = (2k^2 - 2k + 1)(18k^2 + 30k + 17)$, the only corresponding cases to the main parts (for E_1 and E_2) of our results are $t^2 + 16 = 17$ and 25. (cf. Le [11].)

2. Main Theorem

Let E be an elliptic curve defined by

$$E : y^2 = x^3 - nx$$

with n integer. Denote by Γ the group $E(\mathbf{Q})$ of $\mathbf{Q}$-rational points of E. Then, there exists a homomorphism $\alpha : \Gamma \to \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ defined by

$$\alpha(P) = \begin{cases} x & \bmod (\mathbf{Q}^\times)^2 \quad \text{if } P = (x, y) \text{ with } x \neq 0\,; \\ -n & \bmod (\mathbf{Q}^\times)^2 \quad \text{if } P = (0, 0)\,; \\ 1 & \bmod (\mathbf{Q}^\times)^2 \quad \text{if } P = O\,. \end{cases}$$

Let $\overline{E}$ be the elliptic curve given by

$$\overline{E} : y^2 = x^3 + 4nx\,.$$

Denoting $\overline{E}(\mathbf{Q})$ by $\overline{\Gamma}$, we can define a homomorphism $\overline{\alpha} : \overline{\Gamma} \to \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ in the same way as α. Then, examining the orders $|\alpha(\Gamma)|$ and $|\overline{\alpha}(\overline{\Gamma})|$ reveals the rank r of Γ. In fact, we have

$$\frac{|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|}{4} = 2^r\,, \tag{1}$$

which can be found in [13, Chapter 3]. As seen in [13, Chapter 3], one may choose a square-free divisor of n as a representative of an element in $\alpha(\Gamma)$. Moreover, a square-free divisor n' of n, which equals neither 1 nor the square-free part of n, belongs to $\alpha(\Gamma)$ if and only if the equation

$$n'S^4 - \frac{n}{n'}T^4 = U^2$$

has an integer solution (s, t, u) with $s \neq 0$. Then, the point $(n's^2/t^2,\ n'su/t^3)$ is in Γ. The same is true for $\overline{\alpha}(\overline{\Gamma})$. These arguments seem to indicate how to find (independent) $\mathbf{Q}$-rational points of infinite order on an elliptic curve, which motivated us to assert the following.

MAIN THEOREM. *Let n be a fourth-power-free integer greater than one with the square-free part not equal to two. Let E be the elliptic curve given by*

$$E : y^2 = x^3 - nx.$$

rank $E(\mathbf{Q})$ *denotes the rank of E over $\mathbf{Q}$.*

(i) *If either the equation*

$$-S^4 + nT^4 = U^2 \tag{2}$$

has an integer solution (s_1, t_1, u_1) or the equation

$$2S^4 + 2nT^4 = U^2 \tag{3}$$

has an integer solution (s_2, t_2, u_2) with

$$s_i, t_i, u_i \geq 1 \ \text{ and } \ \gcd(s_i, t_i) = \gcd(t_i, u_i) = \gcd(u_i, s_i) = 1 \quad (i = 1, 2) \tag{4}$$

(*which we call a primitive solution*), *then* rank $E(\mathbf{Q}) \geq 1$. *Moreover*, *if* (2) *has a primitive solution*, *then*

$$P = \left(-\frac{s_1^2}{t_1^2}, \frac{s_1 u_1}{t_1^3} \right) \in E(\mathbf{Q}) \backslash E(\mathbf{Q})_{\mathrm{tors}}\,;$$

if (3) *has a primitive solution*, *then*

$$Q = \left(\frac{u_2^2}{4s_2^2 t_2^2}, \frac{u_2(u_2^2 - 4s_2^4)}{8s_2^3 t_2^3} \right) \in E(\mathbf{Q}) \backslash E(\mathbf{Q})_{\mathrm{tors}}\,.$$

(ii) *If both of equations* (2) *and* (3) *have primitive solutions*, *then* rank $E(\mathbf{Q}) \geq 2$, *and the points P and Q in* (i) *are independent modulo $E(\mathbf{Q})_{\mathrm{tors}}$.*

(iii) *If $n = p^k$ for a prime number p and $k \in \{1, 2, 3\}$*, *then* rank $E(\mathbf{Q}) \leq 2$, *and the following hold*:

- rank $E(\mathbf{Q}) = 1$ *if and only if exactly one of equations* (2) *and* (3) *has a primitive solution.*

- rank $E(\mathbf{Q}) = 2$ *if and only if both of equations* (2) *and* (3) *have primitive solutions.*

PROOF. (i) If (2) has a primitive solution (s_1, t_1, u_1), then the point P is in $E(\mathbf{Q})$. Since $E(\mathbf{Q})_{\rm tors} \simeq \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, we see from (4) that P is of infinite order. (cf. [9, Theorem 5.2, p. 134])

If (3) has a primitive solution (s_2, t_2, u_2), then the point Q is in $E(\mathbf{Q})$. If the y-coordinate of Q equals zero, then (4) implies that $u_2 = 2$, $s_2 = 1$ and $n = 1$, which contradicts the assumption. Therefore, Q is of infinite order.

(ii) Assume that both of the equations (2) and (3) have primitive solutions. It suffices to show that the points P and Q are independent modulo $E(\mathbf{Q})_{\rm tors}$. The assertion for non-square n follows from the argument in [13, Chapter 3]. Indeed, we have

$$\Gamma/2\Gamma \simeq \Gamma/\psi(\overline{\Gamma}) \oplus \psi(\overline{\Gamma})/2\Gamma \simeq \alpha(\Gamma) \oplus \overline{\alpha}(\overline{\Gamma})/\overline{\alpha}(\overline{\Gamma}_{\rm tors}),$$

where $\Gamma = E(\mathbf{Q})$, $\overline{\Gamma} = \overline{E}(\mathbf{Q})$ and $\psi : \overline{E} \to E$ is the isogeny whose kernel is $\{O, \overline{A}\}$ with $\overline{A} = (0, 0)$. Putting $\Gamma_0 = \Gamma/\Gamma_{\rm tors}$, we obtain an isomorphism

$$\Gamma_0/2\Gamma_0 \simeq \alpha(\Gamma)/\alpha(\Gamma_{\rm tors}) \oplus \overline{\alpha}(\overline{\Gamma})/\overline{\alpha}(\overline{\Gamma}_{\rm tors})$$

as $\mathbf{Z}/2\mathbf{Z}$-modules. Suppose now that n is non-square. Then, since $\alpha(P) = -1 \neq -n = \alpha(A)$, we have $\alpha(P) \in \alpha(\Gamma) \setminus \alpha(\Gamma_{\rm tors})$. Moreover, since the square-free part of n is not equal to two by the assumption and $\overline{\alpha}(\overline{Q}) = 2 \neq n = \overline{\alpha}(\overline{A})$, where $\overline{Q} = (2s_2^2/t_2^2, -2s_2u_2/t_2^3)$ is a point in $\overline{\Gamma}$, we have $\overline{\alpha}(\overline{Q}) \in \overline{\alpha}(\overline{\Gamma}) \setminus \overline{\alpha}(\overline{\Gamma}_{\rm tors})$. It follows from $\psi(\overline{Q}) = Q$ that P and Q give rise to elements in generators for $\Gamma_0/2\Gamma_0$. Therefore, P and Q are independent modulo $\Gamma_{\rm tors}$.

Suppose next that $n = n_0^2$ for some integer n_0. We may assume that n_0 is square-free and $n_0 > 1$. The proof for this case will proceed along the same lines as [5, Theorem 2]. Thus we will show that the points P, Q, $P + Q$ are not in 2Γ modulo $\Gamma_{\rm tors}$. Let $A = (0, 0)$, $A_1 = (n_0, 0)$ and $A_2 = (-n_0, 0)$ be the two torsion points in Γ. Denoting the x-coordinate of a point R on E by $x(R)$, we have the following:

$$x(P + A) = n\left(\frac{t_1}{s_1}\right)^2, \quad x(Q + A) = -n\left(\frac{2s_2t_2}{u_2}\right)^2,$$

$$x(P + Q) = -\left\{\frac{s_1t_1(u_2^2 - 4s_2^4) + 2u_1s_2t_2u_2}{4s_1^2s_2^2t_2^2 + t_1^2u_2^2}\right\}^2,$$

$$x(P + Q + A) = n\left\{\frac{s_1t_1(u_2^2 - 4s_2^4) - 2u_1s_2t_2u_2}{4nt_1^2s_2^2t_2^2 - s_1^2u_2^2}\right\}^2,$$

$$x(P + A_1) = -n_0\left(\frac{u_1}{s_1^2 + n_0t_1^2}\right)^2, \quad x(P + A_2) = n_0\left(\frac{u_1}{s_1^2 - n_0t_1^2}\right)^2,$$

$$x(Q+A_1) = n_0\left(\frac{s_2^2 + n_0 t_2^2}{s_2^2 - n_0 t_2^2}\right)^2, \qquad x(Q+A_2) = -n_0\left(\frac{s_2^2 - n_0 t_2^2}{s_2^2 + n_0 t_2^2}\right)^2,$$

$$x(P+Q+A_1) = -n_0\left\{\frac{2u_1(s_2^4 - n_0^2 t_2^4) + 4n_0 s_1 t_1 s_2 t_2 u_2}{4n_0(s_1^2 - n_0 t_1^2)s_2^2 t_2^2 - (s_1^2 + n_0 t_1^2)u_2^2}\right\}^2,$$

$$x(P+Q+A_2) = n_0\left\{\frac{2u_1(s_2^4 - n_0^2 t_2^4) - 4n_0 s_1 t_1 s_2 t_2 u_2}{4n_0(s_1^2 + n_0 t_1^2)s_2^2 t_2^2 + (s_1^2 - n_0 t_1^2)u_2^2}\right\}^2.$$

If a point R in Γ is in 2Γ, then $\alpha(R) = 1$. Since n_0 is square-free, we see that

$$P, Q+A, P+Q, P+A_1, P+A_2, Q+A_1, Q+A_2, P+Q+A_1, P+Q+A_2 \notin 2\Gamma.$$

If $Q = \psi(\overline{Q}) \in 2\Gamma$, then $\overline{\alpha}(\overline{Q}) = 2 \in \overline{\alpha}(\overline{\Gamma}_{\text{tors}}) = \{1, n\}$, which contradicts the assumption. Hence $Q \notin 2\Gamma$. In order to show $P+A, P+Q+A \notin 2\Gamma$, we need the following.

LEMMA 1 (cf. [9, Theorem 4.2, p. 85]). *Let C be an elliptic curve over $\mathbf{Q}$ given by*

$$C : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

with α, β, γ in $\mathbf{Q}$. For $S = (x, y) \in C(\mathbf{Q})$, there exists a $\mathbf{Q}$-rational point $T = (x', y')$ on C such that $[2]T = S$ if and only if $x-\alpha$, $x-\beta$ and $x-\gamma$ are all squares in $\mathbf{Q}$.

If $P + A \in 2E(\mathbf{Q})$, then Lemma 1 implies that

$$x(P+A) \pm n_0 = \frac{n_0(n_0 t_1^2 \pm s_1^2)}{s_1^2}$$

are squares in $\mathbf{Q}$, which is impossible, since n_0 is non-square and $\gcd(s_1, n) = 1$ by (4). If $P+Q+A \in 2\Gamma$, then Lemma 1 implies that

$$x(P+Q+A) \pm n_0 = \frac{n_0\big[n_0\{s_1 t_1(u_2^2 - 4s_2^4) - 2u_1 s_2 t_2 u_2\}^2 \pm (4n_0^2 t_1^2 s_2^2 t_2^2 - s_1^2 u_2^2)^2\big]}{(4n_0^2 t_1^2 s_2^2 t_2^2 - s_1^2 u_2^2)^2} \tag{5}$$

are squares in $\mathbf{Q}$. Since n_0 is square-free and the bracket expressions in (5) are congruent to $\pm s_1^4 u_2^4$ modulo n_0, we have $s_1 u_2 \equiv 0 \pmod{n_0}$, which contradicts $n_0 > 1$ and $\gcd(s_1, n) = \gcd(u_2, n) = 1$ by (4). Hence, $P+A, P+Q+A \notin 2\Gamma$.

Assume now that $[k]P + [l]Q \in \Gamma_{\text{tors}} = \{O, A, A_1, A_2\}$ for some integers k and l. Since we have seen that

$$P,\ Q,\ P+A,\ Q+A,\ P+A_1,\ P+A_2,\ Q+A_1,\ Q+A_2,\ P+Q,$$
$$P+Q+A,\ P+Q+A_1,\ P+Q+A_2 \notin 2\Gamma,$$

both k and l are even. Put $k = 2k_1$ and $l = 2l_1$. Since $A, A_1, A_2 \notin 2\Gamma$, we have $[2k_1]P + [2l_1]Q = O$, which implies that $[k_1]P + [l_1]Q \in \Gamma_{\text{tors}}$. In a similar fashion to the above, we see that both k_1 and l_1 are even. Continuing this process, we come to the conclusion that $k = l = 0$. This shows that P and Q are independent modulo Γ_{tors}.

(iii) Since $\alpha(\Gamma) \subset \{\pm 1, \pm p\}$ and $\overline{\alpha}(\overline{\Gamma}) \subset \{1, 2, p, 2p\}$, it follows from (1) that $\operatorname{rank} E(\mathbf{Q}) \le 2$.

Assume that $n = p$ or p^3. Then, since $\alpha(A) = -p$ and $\overline{\alpha}(\overline{A}) = p$, we have $\alpha(\Gamma) \supset \{1, -p\}$ and $\overline{\alpha}(\overline{\Gamma}) \supset \{1, p\}$. By the formula (1), $\operatorname{rank} \Gamma \ge 1$ if and only if either $\alpha(\Gamma) \ni -1$ or $\overline{\alpha}(\overline{\Gamma}) \ni 2$, which is equivalent to that either (2) or (3) has a primitive solution. Hence, the statement on $\operatorname{rank} \Gamma = 1$ holds. It is obvious from (1) that the statement on $\operatorname{rank} \Gamma = 2$ also holds.

Assume now that $n = p^2$. Then, since $\alpha(A_1) = p$ and $\alpha(A_2) = -p$, we have $\alpha(\Gamma) = \{\pm 1, \pm p\}$. By the formula (1), $\operatorname{rank} \Gamma \ge 1$ if and only if any of $p, 2p$ and 2 is in $\overline{\alpha}(\overline{\Gamma})$, which is equivalent to that any of the equations

$$pS^4 + 4pT^4 = U^2\,, \tag{6}$$

$$2pS^4 + 2pT^4 = U^2 \tag{7}$$

and (3) has a primitive solution. If (6) has a primitive solution (s, t, u), then

$$-(2st)^4 + p^2\left(\frac{u}{p}\right)^4 = (s^4 - 4t^4)^2\,.$$

If (7) has a primitive solution (s, t, u), then

$$-(st)^4 + p^2\left(\frac{u}{2p}\right)^4 = \left(\frac{s^4 - t^4}{2}\right)^2.$$

Hence, we see that if $\operatorname{rank} \Gamma \ge 1$, then either (2) or (3) has a primitive solution. Since the converse is also true by (2), the statements follow from the formula (1). □

3. Preliminary lemmas

LEMMA 2. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$. Let P_1, P_2 be rational points on E such that $P_2 = [n]P_1$. If $x(P_2) \in \mathbf{Z}$, then $x(P_1) \in \mathbf{Z}$.*

PROOF. See [6, Lemma 10.2] and [12, p. 275]. □

LEMMA 3. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbf{Z}$, $\operatorname{rank} E(\mathbf{Q}) = 1$ and $E(\mathbf{Q})_{\mathrm{tors}} \subset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. Denote by $P_1, \dots, P_l$ all the integer points on E. Suppose that at least one of the P_i's is of infinite order, and that $P_i + T \notin 2E(\mathbf{Q})$ for any $P_i \notin E(\mathbf{Q})_{\mathrm{tors}}$ and any $T \in E(\mathbf{Q})_{\mathrm{tors}}$. Then, $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}} = \langle P_j \rangle$ for some j.*

PROOF. Let $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}} = \langle U \rangle$ and let $P_i \notin E(\mathbf{Q})_{\mathrm{tors}}$. Then, there exist a positive integer m and $T \in E(\mathbf{Q})_{\mathrm{tors}}$ such that $P_i = [m]U + T$. By assumption, we have $[m]U = P_i + T \notin 2E(\mathbf{Q})$, that is, m is odd. Hence, we may also write $P_i = [m](U + T)$. It follows from Lemma 2 that $U + T = P_j$ for some j, and that $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}} = \langle P_j \rangle$. □

Now we show the following lemma, which gives us a necessary information about an existence of the integer point R on E_1 for a prime p of the form $p = a^2 + 4$:

LEMMA 4. *Let d be a square-free positive integer with $d > 5$. Consider the Diophantine equation*

$$x^2 - dy^4 = -1\,. \tag{8}$$

If $d = s^2 + 4$, then equation (8) *has only the positive integer solution $x = s(s^2+3)/2$, $y = t$, where $(s,\ t)$ is a positive integer solution to the Pell equation $X^2 - 2Y^2 = -1$.*

PROOF. Put $d = a^2 + 4$. Then $a + \sqrt{d}$ is the fundamental solution to the Pell equation $X^2 - dY^2 = -4$. Write $\varepsilon = \dfrac{a+\sqrt{d}}{2}$. Hence the fundamental solution to the Pell equation $X^2 - dY^2 = -1$ is given by

$$\varepsilon^3 = u + v\sqrt{d} \quad \textit{with}\ \ u = a(a^2+3)/2\,, \quad v = (a^2+1)/2\,.$$

It follows from Theorem D of Chen and Voutier [2] that equation (8) has a positive integer solution if and only if $v = (a^2+1)/2 = n^2$ for some positive integer n and so

$$a^2 - 2n^2 = -1\,.$$

This completes the proof of Lemma 4. □

4. $E_1 : y^2 = x^3 - px$

In this section, we consider the elliptic curve

$$E_1 : y^2 = x^3 - px\,,$$

where p is an odd prime number.

Throughout the paper, an integer point $(x,\ y)$ on an elliptic curve is defined to be *positive* if $y > 0$. Note that a positive integer point on E_1 is of infinite order, since $E_1(\mathbf{Q})_{\mathrm{tors}} = \{O,\ A\}$ with $A = (0,\ 0)$. Draziotis [4] and Walsh [16] showed that E_1 has at most four positive integer points and that possible four positive integer points on E_1 are given as follows:

(i) If $p = a^2 + b^4$, then $P = (-b^2,\ ab) \in E_1(\mathbf{Q})$. Moreover, only if $p = a^4 + b^4$, then two integer points $P = (-b^2,\ a^2b) \in E_1(\mathbf{Q})$ and $P' = (-a^2,\ ab^2) \in E_1(\mathbf{Q})$ can arise.

(ii) If $p = 2m^2 - 1$ for some positive integer m, then $Q = (m^2,\ m(m^2-1)) \in E_1(\mathbf{Q})$.

(iii) If $u^2 - pv^4 = -1$ has positive integer solutions $u,\ v$, then $R = (pv^2,\ puv) \in E_1(\mathbf{Q})$.

Denote by $P,\ P',\ Q,\ R$ the integer points on E_1 defined by the above (i), (ii), (iii), respectively. Whenever rational points $P,\ Q$ in Main Theorem become integer points on E_1, these points coincide with the integer points $P,\ Q$ on E_1 in the above (i), (ii).

We make some remarks on the integer points $P,\ R$ on E_1. In the case (i), Friedlander and Iwaniec [7] showed that there are infinitely many primes of the form $p = a^2 + b^4$. Spearman [14] has recently proved that if $p = a^4 + b^4$, then rank $E_1(\mathbf{Q}) = 2$. Spearman, however, did not explicitly give independent points on E_1.

In the case (iii), the Diophantine equation $u^2 - pv^4 = -1$ has at most one positive integer solution u, v for positive integer $p > 2$, which was solved completely by Chen and Voutier [2]. If this solution exists, then $(X,\ Y) = (u,\ v^2)$ must be the fundamental solution to the Pell equation $X^2 - pY^2 = -1$. It is worthy of stating that when $p = 17 = 2^4 + 1 = 2\cdot 3^2 - 1$, E_1 has exactly four positive integer points:

$$P = (-1,\ 4)\,, \quad P^{'} = (-4,\ 2)\,, \quad Q = (9,\ 24)\,, \quad R = (17, 68)\,.$$

Then rank $E_1(\mathbf{Q}) = 2$ and $P,\ Q$ are generators modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.

Now Main Theorem enables us to obtain Theorems from 1 to 5 concerning a generator of $E_1(\mathbf{Q})$ in the rank one case and independent points on E_1 in the rank two case.

4.1. A generator of $E_1(\mathbf{Q})$ with rank $E_1(\mathbf{Q}) = 1$**.** Using Main Theorem, we give some examples where each of the integer points $P,\ Q,\ R$ can be a generator modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.

THEOREM 1. *Let p be a prime number such that $p = (2t)^2 + 1$ for an odd t.*

(1) *The only positive integer points on E_1 are given by $P = (-1,\ 2t),\ R = (p,\ 2pt)$.*

(2) rank $E_1(\mathbf{Q}) = 1$, *and P is a generator modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.*

THEOREM 2. *Let p be a prime number such that $p = 2m^2 - 1$ for an even m.*

(1) *The only positive integer point on E_1 is given by $Q = (m^2,\ m(m^2 - 1))$.*

(2) rank $E_1(\mathbf{Q}) = 1$, *and Q is a generator modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.*

THEOREM 3. *Let p be a prime number such that $p = s^2 + 4$ with $s > 1$, where $(s,\ t)$ is a positive integer solution to the Pell equation $X^2 - 2Y^2 = -1$.*

(1) *The only positive integer point on E_1 is given by $R = (pv^2,\ puv)$, where $u = s(s^2 + 3)/2$ and $v = t$.*

(2) rank $E_1(\mathbf{Q}) = 1$, *and R is a generator modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.*

PROOF OF THEOREM 1. Theorem 1 was proved by Hollier–Spearman–Yang [8] except for the fact that P is a generator modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$. (cf. [8, Theorem 1.2]) It follows from Main Theorem and Lemma 3 that P is a generator modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.

PROOF OF THEOREM 2. (1) Note that $p \equiv -1 \mod 4$, since $p = 2m^2 - 1$ for an even m. E_1 has neither of the integer points $P,\ P^{'}$. Indeed, p cannot be written as $p = a^2 + b^4$, since $p \equiv -1 \mod 4$. From $p = 2m^2 - 1$, E_1 has the integer point Q. E_1 does not have the integer point R. Indeed, the Diophantine equation $x^2 - py^4 = -1$ has no positive integer solution $x,\ y$, since $p \equiv -1 \mod 4$.

(2) Since $p \equiv -1 \mod 4$, the equation $-S^4 + pT^4 = U^2$ has no positive integer solutions. From $p = 2m^2 - 1$, the equation $2S^4 + 2pT^4 = U^2$ has a solution $(1, 1, 2m)$. It follows from Main Theorem and Lemma 3 that rank $E_1(\mathbf{Q}) = 1$, and Q is a generator modulo $E_1(\mathbf{Q})_{\text{tors}}$.

Proof of Theorem 3. (1) Since $p = s^2 + 4$ and $s^2 - 2t^2 = -1$, s cannot be a square. Indeed, if $s = m^2 > 1$, then $m^4 + 1 = 2t^2$ and so

$$t^4 - m^4 = \left(\frac{m^4 - 1}{2}\right)^2,$$

which has no positive integer solutions, since $m > 1$. Hence E_1 has neither of the integer points $P,\ P'$. Moreover, E_1 does not have the integer point Q, since $p \equiv 5 \mod 8$. By Lemma 4, E_1 has the integer point R.

(2) Note that E_1 does not have the integer point P, but E_1 has the following rational point P:

$$R + A = P = \left(-\frac{1}{v^2}, \frac{u}{v^3}\right).$$

The equation $2S^4 + 2pT^4 = U^2$ has no positive integer solutions, since $p \equiv 5 \mod 8$. It follows from Main Theorem and Lemma 3 that rank $E_1(\mathbf{Q}) = 1$, and R is a generator modulo $E_1(\mathbf{Q})_{\text{tors}}$. □

4.2. Independent points on E_1 with rank $E_1(\mathbf{Q}) = 2$**.** Walsh [17] extended Spearman's theorem in [14] by showing that rank $E_1(\mathbf{Q}) = 2$ whenever there are at least two positive integer points on E_1 , except possibly if there are exactly two positive integer points on E_1 with one of them being of type (i) above and the other being of type (iii) above. Hollier–Spearman–Yang [8] also established that rank $E_1(\mathbf{Q}) = 2$ when p is a prime such that $p = a^2 + 1$ and $a = 41t^2 + 58t + 41$ with $t(\neq -1)$ integer.

Using Main Theorem, we show the following theorems:

Theorem 4. *Let p be a prime such that $p = a^4 + b^4 > 17$ for positive integers a, b.*

(1) rank $E_1(\mathbf{Q}) = 2$, *and $P = (-b^2,\ a^2 b)$ and $P' = (-a^2,\ ab^2)$ are independent modulo $E_1(\mathbf{Q})_{\text{tors}}$.*

(2) (i) *If $b = 1$, then the only positive integer points on E_1 are given by $P = (-1,\ a^2),\ P' = (-a^2,\ a),\ R = (p,\ pa^2)$.*
(ii) *If $b = 2$ and $97 < p < 10^{12}$, then the only positive integer points on E_1 are given by $P = (-4,\ 2a^2),\ P' = (-a^2,\ 4a)$.*
(iii) *If $b = a-1$ and $p < 10^{12}$, then the only positive integer points on E_1 are given by $P = (-(a-1)^2,\ a^2(a-1)),\ P' = (-a^2,\ a(a-1)^2),\ Q = (m^2,\ m(m^2-1))$, where $m = a^2 - a + 1$.*

THEOREM 5. *Let p be a prime such that $p = a^2 + 1 > 17$ for positive integer a.*

(1) *Suppose that $a = 2t$, where $(m,\ t)$ is a positive integer solution to the Pell equation $X^2 - 2Y^2 = 1$.*
(i) *The only positive integer points on E_1 are given by $P = (-1,\ a)$, $Q = (m^2,\ m(m^2-1))$, $R = (p,\ pa)$.*
(ii) rank $E_1(\mathbf{Q}) = 2$, *and P, Q are independent modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.*

(2) *Suppose that $a = ct^2 + 2dt + c$, where $(c,\ d)$ is a positive integer solution to the Pell equation $X^2 - 2Y^2 = -1$.*
(i) *If $a \equiv 2 \mod 9$, then the only positive integer points on E_1 are given by $P = (-1,\ a)$, $R = (p,\ pa)$.*
(ii) rank $E_1(\mathbf{Q}) = 2$, *and $P = (-1,\ a)$ and $Q = ((dt^2+ct+d)^2/t^2,\ (dt^2+ct+d)((dt^2+ct+d)^2-t^4)/t^3)$ are independent modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.*

PROOF OF THEOREM 4. (1) For any p of the form $p = a^4 + b^4$, the equation $-S^4 + pT^4 = U^2$ has a solution $(b, 1, a^2)$ and the equation $2S^4 + 2pT^4 = U^2$ has a solution $(a-b, 1, 2(a^2-ab+b^2))$. Hence these solutions yield two rational points

$$P = (-b^2,\ a^2 b)\,, \quad Q = \left(\frac{m^2}{(a-b)^2},\ \frac{m(m^2-(a-b)^4)}{(a-b)^3}\right) \qquad (*)$$

of infinite order on E_1, where $m = a^2 - ab + b^2$. Then the following important relation holds:

$$P' - P = Q\,,$$

where $P' = (-a^2,\ ab^2)$. It follows from Main Theorem that rank $E_1(\mathbf{Q}) = 2$, and P and P' are independent modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.

(2) (i) Since $p = a^4 + 1$, E_1 has the integer points $P,\ P',\ R$. But E_1 does not have the integer point Q. Indeed, if $p = a^4 + 1 = 2m^2 - 1$, then $m^2 - 8h^4 = 1$ with $a = 2h > 2$. This implies that $m \pm 1 = 2k^4,\ m \mp 1 = 4l^4$ with $h = kl > 1$. Hence $k^4 - 2l^4 = \pm 1$ and so

$$l^8 \pm k^4 = \left(\frac{k^4 \pm 1}{2}\right)^2,$$

which has no solutions since $kl > 1$.

(ii) Since $p = a^4 + 2^4$, E_1 has the integer points P, P'. But E_1 does not have the integer points Q, R. Indeed, in view of $(*)$ and $a - b > 2$, Q is not an integer point. By MAGMA, we checked that v is not a square in the range $17 < p < 10^{12}$, where $(u,\ v)$ is the fundamental solution to the Pell equation $X^2 - pY^2 = -1$. Hence the Diophantine equation $x^2 - py^4 = -1$ has no positive integer solution x, y. (cf. Theorem D of Chen and Voutier [2].) We therefore conclude that E_1 does not have the integer point R in the range $17 < p < 10^{12}$.

(iii) Since $p = a^4 + (a-1)^4$, E_1 has the integer points P, P', Q with $m = a^2 - a + 1$. But E_1 does not have the integer point R in the range $17 < p < 10^{12}$, since we checked that v is not a square as above. □

PROOF OF THEOREM 5. (1) (i) Since $p = a^2 + 1 = 2m^2 - 1$, E_1 has the integer points P, Q, R. But E_1 does not have the integer point P'. Indeed, if P' exists, then $a = (2n)^2$ for some integer $n > 1$ and so $m^2 - 8n^4 = 1$, which has no positive integer solutions with $n > 1$ as in the proof of Theorem 4.

(ii) Since $p = a^2 + 1 = 2m^2 - 1$, the equations $-S^4 + pT^4 = U^2$ and $2S^4 + 2pT^4 = U^2$ have solutions $(1, 1, a)$ and $(1, 1, 2m)$, respectively. It follows from Main Theorem that rank $E_1(\mathbf{Q}) = 2$, and P and Q are independent modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$.

(2) (i) Since $p = a^2 + 1$, E_1 has the integer points P, R. But E_1 has neither of the integer points P', Q. Indeed, if P' exists, then a must be a square, which contradicts $a \equiv 2 \mod 9$. If Q exists, then $a^2 + 1 = 2m^2 - 1$, which contradicts $a \equiv 2 \mod 9$.

(ii) Since $p = a^2 + 1$, the equation $-S^4 + pT^4 = U^2$ has a solution $(1, 1, a)$. In view of $c^2 - 2d^2 = -1$, the following identity holds:

$$(ct^2 + 2dt + c)^2 + 1 + t^4 = 2(dt^2 + ct + d)^2 .$$

Hence the equation $2S^4 + 2pT^4 = U^2$ has a solution $(t,\ 1,\ 2(dt^2 + ct + d))$. It follows from Main Theorem that rank $E_1(\mathbf{Q}) = 2$, and the rational points $P,\ Q$ are independent modulo $E_1(\mathbf{Q})_{\mathrm{tors}}$. $\square$

5. $E_2 : y^2 = x^3 - p^2 x$

In this section, we consider the elliptic curve

$$E_2 : y^2 = x^3 - p^2 x ,$$

where p is an odd prime number. The elliptic curve E_2 is known to be related to the congruent number problem (cf. Koblitz [10]).

By Draziotis [4] and Walsh [16], we see that E_2 has at most two positive integer points and that possible two positive integer points on E_2 are given as follows:

(i) If $p^2 = a^2 + b^4$, then $P = (-b^2,\ ab) \in E_2(\mathbf{Q})$.

(ii) If $p^2 = 2m^2 - 1$ for some positive integer m, then $Q = (m^2,\ m(m^2 - 1)) \in E_2(\mathbf{Q})$.

We make some remarks on the integer points $P,\ Q$ on E_2. In the case (i), the prime p can be written as

$$p = u^4 + 6u^2v^2 + v^4 ,$$

where u, v are positive integers such that $(u, v) = 1$ and $u \not\equiv v \mod 2$. Hence $p \equiv 1 \mod 8$. In the case (ii), the prime p can be obtained from

$$(1 + \sqrt{2})^n = p + m\sqrt{2} \quad \text{with } n \text{ odd} > 1$$

Note that $p \equiv \pm 1 \mod 8$, since $\left(\frac{2}{p}\right) = 1$.

Now we show the following theorem concerning E_2 similar to Theorem 2 concerning E_1.

THEOREM 6. *Let p be a prime number such that $p^2 = 2m^2 - 1$ with $p \equiv -1 \mod 8$.*

(1) *The only positive integer point on E_2 is given by $Q = (m^2,\ m(m^2-1))$.*

(2) rank $E_2(\mathbf{Q}) = 1$ *and Q is a generator modulo $E(\mathbf{Q})_{\text{tors}}$.*

PROOF. (1) Since $p \equiv -1 \mod 8$, E_2 does not have the integer point P on E_2. From $p^2 = 2m^2 - 1$, E_2 has the integer point $Q = (m^2,\ m(m^2-1))$ in the above (ii).

(2) Since $p \equiv -1 \mod 8$, the equation $-S^4 + p^2T^4 = U^2$ has no positive integer solutions. From $p^2 = 2m^2 - 1$, the equation $2S^4 + 2p^2T^4 = U^2$ has a solution $(1,1,\ 2m)$. It follows from Main Theorem and Lemma 3 that rank $E_2(\mathbf{Q}) = 1$, and Q is a generator modulo $E_2(\mathbf{Q})_{\text{tors}}$. □

Unlike E_1, it is difficult to give a number of examples where the integer points $P,\ Q$ on E_2 are generators modulo $E_2(\mathbf{Q})_{\text{tors}}$. By the above remarks, we see that both of the integer points $P,\ Q$ on E_2 exist if and only if

$$(u^4 + 6u^2v^2 + v^4)^2 + 1 = 2m^2\,, \quad u^4 + 6u^2v^2 + v^4 \text{ is prime}\,. \tag{9}$$

If $v = 1,\ 2,\ 3$, then equation (9) can be easily solved. In fact, we show the following:

PROPOSITION 1. *Let p be a prime number such that $p = u^4 + 6u^2v^2 + v^4$ with $v = 1, 2, 3$.*

(1) *If both of the integer points $P,\ Q$ on E_2 exist, then $v = 1, u = 2$, or $v = 2, u = 1$, and $m = 29$ and $p = 41$.*

(2) *When $p = 41$, the only positive integer points on E_2 are given by $P = (-9,\ 120)$, $Q = (841,\ 24360)$. Then* rank $E_2(\mathbf{Q}) = 2$ *and $P,\ Q$ are generators modulo $E_2(\mathbf{Q})_{\text{tors}}$.*

PROOF. When $v = 1$, we can reduce equation (9) to finding all integer points on the elliptic curve

$$Y^2 = X(X^2 - 32X + 260),$$

where $X = 2(u^2+3)^2$ and $Y = 4m(u^2+3)$. By MAGMA, we see that all integer points on the above elliptic curve are given by

$(0,\ 0)$, $(2,\ 20)$, $(5,\ 25)$, $(10,\ 20)$, $(13,\ 13)$, $(16,\ 8)$, $(18,\ 12)$, $(20,\ 20)$, $(26,\ 52)$, $(45,\ 195)$, $(52,\ 260)$, $(98,\ 812)$, $(130,\ 1300)$, $(250,\ 3700)$, $(4160,\ 267280)$

and its Mordell-Weil rank is equal to 2. Hence all integer solutions of equation (9) with $v = 1$ are given by $u = 2,\ m = 29,\ p = 41$. When $p = 41$, we see that E_2 has only the above integer points and rank $E_2(\mathbf{Q}) = 2$ and $P,\ Q$ are generators modulo $E_2(\mathbf{Q})_{\text{tors}}$.

Similarly, when $v = 2, 3$, we can reduce equation (9) to finding all integer points on the elliptic curve

$$Y^2 = X(X^2 - 32v^4X + (4 + 256v^8))\,,$$

where $X = 2(u^2 + 3v^2)^2$ and $Y = 4m(u^2 + 3v^2)$. Note that when $v = 2, 3$, its Mordell-Weil rank is equal to 3, 1, respectively. All integer points on the above elliptic curves yield only the solution $v = 2, u = 1, m = 29$ and so $p = 41$. □

6. $E_k : y^2 = x^3 - p^k x$ with $k \geq 3$

In this section, we consider the elliptic curve

$$E_k : y^2 = x^3 - p^k x \quad \text{with} \ \ k \geq 3\,,$$

where p is an odd prime number.

By Draziotis [4] and Walsh [16], we see that E_3 has at most three positive integer points and that possible three positive integer points on E_3 are given as follows:

(i) If $p^3 = a^2 + b^4$, then $P = (-b^2,\ ab) \in E_3(\mathbf{Q})$.

(ii) If $p^3 = 2m^2 - 1$ for some positive integer m, then $Q = (m^2,\ m(m^2 - 1)) \in E_3(\mathbf{Q})$.

(iii) If $u^2 - p^3 v^4 = -1$ has positive integer solutions $u,\ v$, then $R = (pv^2,\ puv) \in E_3(\mathbf{Q})$.

We make some remarks on the integer points $P,\ Q,\ R$ on E_3. In the case (i), the prime p can be parametrized as in Theorem 14.4.2 of Cohen [3], pp. 475–477. In the case (ii), the only solution of the equation is given by $p = 23$, $m = 78$ and so $Q = (6084,\ 474474)$. When $p = 23$, E_3 has only the integer points with nonnegative y-coordinates, $A = (0,\ 0)$, $Q = (6084,\ 474474)$, and Q is a generator modulo $E_3(\mathbf{Q})_{\text{tors}}$. In the case (iii), the equation has no positive integer solutions $u,\ v$ under Ankeny-Artin-Chowla conjecture (AAC), which states that if $p \equiv 1 \mod 4$ is prime, and $(t + u\sqrt{p})/2$ is the fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{p})$, then $u \not\equiv 0 \mod p$. It is verified that AAC conjecture is true for all primes $p < 10^{11}$. (cf. [15].)

On the other hand, when $k > 3$, E_k does not have corresponding integer points $P,\ Q,\ R$. Indeed, the Diophantine equations

$$p^k = a^2 + b^4\,, \quad p^k = 2m^2 - 1\,, \quad u^2 - p^k v^4 = -1 \quad \text{with} \ \ k > 3$$

have no solutions respectively, by assuming AAC conjecture to the third equation. (cf. Walsh [16], p. 1287, p. 1288, p. 1294, p. 1295, p. 1301.)

Now we show the following theorem concerning E_3 similar to Theorem 1 concerning E_1.

THEOREM 7. *Let p be a prime number such that $p^3 = a^2 + b^4$ with $p \equiv 5 \mod 8$. Suppose that AAC conjecture is true.*

(1) *The only positive integer point on E_3 is given by $P = (-b^2,\ ab)$.*

(2) rank $E_3(\mathbf{Q}) = 1$ *and P is a generator modulo $E_3(\mathbf{Q})_{\text{tors}}$.*

PROOF. (1) From $p^3 = a^2 + b^4$, E_3 has the integer point P. Since $p \equiv 5 \mod 8$, E_3 does not have the integer point Q. Indeed, otherwise $\left(\frac{2}{p}\right) = 1$, which is impossible.

(2) From $p^3 = a^2 + b^4$, the equation $-S^4 + p^3T^4 = U^2$ has a solution $(b, 1, a)$. Since $p \equiv 5 \mod 8$, the equation $2S^4 + 2p^3T^4 = U^2$ has no positive integer solutions. It follows from Main Theorem and Lemma 3 that rank $E_3(\mathbf{Q}) = 1$ and P is a generator modulo $E_3(\mathbf{Q})_{\mathrm{tors}}$. □

REMARK 2. Several values of p, a, b satisfying the conditions of Theorem 7 are given in the table below. (cf. Theorem 14.4.2 of Cohen [3], pp. 475–477.)

p	a	b
13	46	3
3498013	4631366566	67977
2268369373	108009260191126	1558089
2216593502653	2939897808856374166	1224439983
98010612150013	967129818036549973606	8858388591
10856414397166909	1088361569846456822875798	555212674575
28444712011720861	4755630851617686832575766	794593078695
36496032277056733	6731547875445229849014166	1347557334903
43927985163483901	8893244812064458871002726	1543556147055
168760260431980669	67164028008877260098008678	4145358872655

ACKNOWLEDGMENT. The authors would like to thank the referee for valuable suggestions, which especially made the proof of Main Theorem (ii) concise.

References

[1] J. S. CHAHAL, *Topics in number theory*, Kluwer Academic/Plenum Publisher, 1988.

[2] J. H. CHEN and P. VOUTIER, Complete solution of the Diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations, J. number theory **62** (1997), 71–99.

[3] H. COHEN, *Number Theory, Vol. II*, GTM 240, Springer-Verlag, 2007.

[4] K. A. DRAZIOTIS, Integer points on the curve $Y^2 = X^3 \pm p^k X$, Math. Comp. **75** (2006), 1493–1505.

[5] A. DUJELLA and A. PETHŐ, Integer points on a family of elliptic curves, Publ. Math. Debrecen **56** (2000), 321–335.

[6] S. DUQUESNE, Elliptic curves associated with simplest quartic fields, J. Theor. Nombres Bordeaux **19** (2007), 81–100.

[7] J. FRIEDLANDER and H. IWANIEC, The polynomial $X^2 + Y^4$ captures its primes, Annals of Mathematics **148** (1998), 945–1040.

[8] A. J. HOLLIER, B. K. SPEARMAN and Q. YANG, On the rank and integral points of elliptic curves $y^2 = x^3 - px$, International J. of Algebra **3** (2009), 401–406.

[9] A. W. KNAPP, *Elliptic Curves*, Princeton, Princeton Univ. Press, 1992.

[10] N. KOBLITZ, *Introduction to Elliptic Curves and Modular Forms*, GTM 97, Springer-Verlag, 1984.

[11] M. LE, On Cohn's conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$, Arch. Math. **78** (2002), 26–35.

[12] J. H. SILVERMAN, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.

[13] J. H. SILVERMAN and J. TATE, *Rational points on elliptic curves*, UTM, Springer-Verlag, 1992.

[14] B. K. SPEARMAN, Elliptic curves $y^2 = x^3 - px$ of rank two, Math. J. Okayama Univ. **49** (2007), 183–184.

[15] A. J. VAN DER POORTEN, H. J. J. TE RIELE and H. C. WILLIAMS, Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 10^{11}, Math. Comp. **70** (2000), 1311–1328.

[16] P. G. WALSH, Integer solutions to the equation $y^2 = x(x^2 \pm p^k)$, Rocky Mountain J. Math. **38** (2008), 1285–1302.

[17] P. G. WALSH, Maximal ranks and integer points on a family of elliptic curves, Glasnik Mat. **44** (2009), 83–87.

Present Addresses:
YASUTSUGU FUJITA
COLLEGE OF INDUSTRIAL TECHNOLOGY,
NIHON UNIVERSITY,
2–11–1 SHIN-EI, NARASHINO, CHIBA, 275–8576 JAPAN.
e-mail: fujita.yasutsugu@nihon-u.ac.jp

NOBUHIRO TERAI
DIVISION OF GENERAL EDUCATION,
ASHIKAGA INSTITUTE OF TECHNOLOGY,
268–1 OMAE, ASHIKAGA, TOCHIGI, 326–8558 JAPAN.
e-mail: terai@ashitech.ac.jp