T. Hadano
Nagoya Math. J.
Vol. 66 (1977), 99-108

ELLIPTIC CURVES WITH A TORSION POINT

TOSHIHIRO HADANO

0. Introduction

Let E be an elliptic curve defined over the field $\boldsymbol{Q}$ of rational numbers, then the torsion subgroup of the Mordell-Weil group $E(\boldsymbol{Q})$ is finite and it is known that there exist the elliptic curves whose torsion subgroups $E(\boldsymbol{Q})^t$ are of the following types: (1), (2), (3), (2, 2), (4), (5), (2, 3), (7), (2, 4), (8), (9), (2, 5), (2, 2, 3), (3, 4) and (2, 8). It has been conjectured from various reasons that $E(\boldsymbol{Q})^t$ is exhausted by the above types only. If E has a torsion point of order precisely n, then it is known that E has an n-isogeny, that is to say, an isogeny of degree n.

In the present paper if E has a torsion point of order $n > 1$, we consider by the elementary calculation whether the p-isogenous curve E' to E possesses a torsion point of order n again, where p is a prime that divides n. Since this problem is obvious for $n = 2$, we may assume $n \geqq 3$ henceforth. As the Weierstrass normal models with a torsion point have been obtained by Nagell, Bergman etc., we can give their isogenies by the explicit forms. By transforming well these forms, we can solve the above problem in many cases, moreover, we calculate the conductor of such curves in case that $n = 3, 5$, for example.

1. $n = 3$

In this case as a minimal model for a curve E, we can take

$$E: y^2 + axy + by + x^3 = 0$$

with $a, b \in \boldsymbol{Z}$ (: rational integers), $b > 0$ which are neither $p \mid a$ nor $p^3 \mid b$ for any prime p. The discriminant Δ of E is

$$\Delta = -b^3(a^3 + 27b)$$

and the torsion group is $\{(0, 0), (0, -b), \infty\}$. Then the 3-isogenous curve E' to E is given by a model

Received May 10, 1976.

$$E' : y^2 + axy + by + x^3 + 5abx - a^3b + 7b^2 = 0 \tag{1.1}$$

and the discriminant Δ' is

$$\Delta' = -b(a^3 + 27b)^3 .$$

Now we consider whether the equation (1.1) can be transformed to the form

$$y^2 + Axy + By + x^3 = 0 \tag{1.2}$$

with $A, B \in \boldsymbol{Z}$. Transforming both (1.1) and (1.2) into Weierstrass models $y^2 + x^3 + g_2x + g_3 = 0$ ($g_2, g_3 \in \boldsymbol{Q}$), and comparing with the coefficients and the discriminants of both equations, we have

$$a(a^3 - 216b) = A(A^3 + 24B) \tag{1.3}$$

$$a^6 + 540a^3b - 2^33^6b^2 = A^6 + 36A^3B + 216B^2 \tag{1.4}$$

$$b(a^3 + 27b)^3 = B^3(A^3 + 27B) . \tag{1.5}$$

Then we can put

$$A^3 + 27B = c^3z , \qquad b = d^3z$$

with $c, d, z \in Z$, $c \neq 0$ and $d > 0$ (z: positive cubic-free), so from (1.3) and (1.5)

$$A^3 = c^3z - 27B , \qquad da^3 = Bc - 27d^4z . \tag{1.6}$$

From (1.4), hence,

$$(c^2 + 27d^2)(B + c^2dz + 9cd^2z + 27d^3z)(B - c^2dz + 9cd^2z - 27d^3z) = 0$$

and so, $B = d(\pm c^2 - 9cd \pm 27d^2)z$.
From (1.3) and (1.6), then it follows that

$$z = 1 , \quad A = c \mp 9d , \quad B = d(\pm c^2 - 9cd \pm 27d^2) ,$$
$$a = \pm c - 3d , \quad b = d^3 .$$

Hence we have

THEOREM 1.1. *The 3-isogenous curve to an elliptic curve* $y^2 + axy + by + x^3 = 0$ *with a torsion point of order* 3 *has a rational point of order* 3 *if and only if* b *is a cubic number* t^3 *with* $t > 0$. *Moreover the 3-isogenous curve is given by*

$$y^2 + (a - 6t)xy + (a^2 - 3at + 9t^2)ty + x^3 = 0 .$$

With regard to the degenerate reduction of such curves we have

THEOREM 1.2. *Let E be an elliptic curve, minimal at all primes, of the discriminant Δ, and the conductor N. Assume that both E and the 3-isogenous curve E' have a torsion point of order 3 i.e. $E: y^2 + axy + t^3y + x^3 = 0$. Then we have, for any prime p dividing Δ,*

$$p \neq 3 \Longrightarrow \operatorname{ord}_p N = 1$$

$$p = 3 \Longrightarrow \operatorname{ord}_3 N = \begin{cases} 1 & \text{if } 3 \nmid a \\ 2 & \text{if } 3 \mid a \text{ and } \operatorname{ord}_3 \Delta \geqq 6 \\ 3 & \text{if } \operatorname{ord}_3 \Delta = 3 \text{ or } 5\,. \end{cases}$$

Proof. We may take

$$E: y^2 + axy + t^3y + x^3 = 0$$

$$\Delta = -t^9(a^3 + 27t^3)\,, \qquad j = a^3(a^3 + 24t^3)^3\Delta^{-1} \ (=j\text{-invariant})$$

with $a, t \in \boldsymbol{Z}$, $(a, t) = 1$ and $t > 0$. And we know that $\operatorname{ord}_p N = 1$ if and only if $\operatorname{ord}_p \Delta = -\operatorname{ord}_p j$ for any prime p (Serre [4, p. 306]). Now the proof completes by means of the following Lemma 1.3.

LEMMA 1.3. *The 3-parts of the conductor of the minimal model*

$$y^2 + axy + by + x^3 = 0$$

are as follows:

	Néron type	$v(\Delta)$	$v(N)$	$v(j)(j \neq 0)$
(i) $v(a)=0,\ v(b)=0$	A	0	0	0
$v(a)=0,\ v(b)>0$	B	$3v(b)$	1	$-3v(b)$
(ii) $v(a)=1,\ a=3a'$				
$a' \equiv 1 \pmod 3,\ b \equiv 1, -2 \pmod 9$ $a' \equiv -1 \pmod 3,\ b \equiv -1, 2 \pmod 9$	C1	3	3	3
$a' \equiv 1 \pmod 3,\ b \equiv 4 \pmod 9$ $a' \equiv -1 \pmod 3,\ b \equiv -4 \pmod 9$	C2	3	2	3
$v(a'^3+b)=1$	C1	4	4	2
$v(a'^3+b)=2$	C3	5	3	1
$v(a'^3+b)=3$	C4	6	2	0
$v(a'^3+b)=s \geqq 4$	$C5_{s-3}$	$3+s$	2	$3-s$
$v(b)=1$	C3	6	4	3
$v(b)=2,\ b=9b'$				
$a' \not\equiv b' \pmod 3$	C6	9	3	3
$a' \equiv b' \pmod 3$	C6	9	3	$3+3v(a'^3+8b')$

	Néron type	$v(\Delta)$	$v(N)$	$v(j)(j\neq 0)$
(iii) $v(b)\geqq 2$				
$b\equiv\pm 1,\pm 4 \pmod 9$	C1	3	3	$3v(a)$
$b\equiv\pm 2 \pmod 9$	C2	3	2	$3v(a)$
$v(b)=1$	C3	7	5	$3v(a)-1$
$v(b)=2$	C6	11	5	$3v(a)-2$

, *where* $v(\ ) = \mathrm{ord}_3(\ )$.

The proof is due to Koike [2].

2. $n = 5$

In this case as a model for a curve E, by transforming an equation of Nagell [3, § 2] we can take

$$E: y^2 + ab^2y + x^3 - \tfrac{1}{4}(a^2 + 6ab + b^2)x^2 + \tfrac{1}{2}ab^2(a + b)x = 0 \tag{2.1}$$

with $a, b \in \boldsymbol{Z}$, $(a, b) = 1$ and $a > 0$. The discriminant Δ of E is

$$\Delta = -a^5b^5(a^2 + 11ab - b^2)$$

and the torsion group is $\{(0, 0), (0, -ab^2), (ab, -\tfrac{1}{2}ab(a + b)), (ab, \tfrac{1}{2}ab(a - b)), \infty\}$. Then the 5-isogenous curve E' to E is given by a model

$$\begin{aligned} E': y^2 + ab^2y + x^3 - \tfrac{1}{4}(a^2 + 6ab + b^2)x^2 + \tfrac{1}{2}ab(10a^2 - 19ab - 9b^2)x \\ - ab(a^4 - 10a^3b - 5a^2b^2 - 15ab^3 - b^4) = 0 \end{aligned} \tag{2.2}$$

by the method of Vélu [6] and the discriminant Δ' is

$$\Delta' = -ab(a^2 + 11ab - b^2)^5 .$$

Now we consider whether the equation (2.2) can be transformed to the form

$$y^2 + AB^2y + x^3 - \tfrac{1}{4}(A^2 + 6AB + B^2)x^2 + \tfrac{1}{2}AB^2(A + B)x = 0$$

with $A, B \in \boldsymbol{Z}$, $(A, B) = 1$ and $A > 0$. By means of the same calculation as **1**, we have

$$\begin{aligned} a^4 - 228a^3b + 494a^2b^2 + 228ab^3 + b^4 \\ = A^4 + 12A^3B + 14A^2B^2 - 12AB^3 + B^4 \end{aligned} \tag{2.3}$$

$$ab(a^2 + 11ab - b^2)^5 = A^5B^5(A^2 + 11AB - B^2) . \tag{2.4}$$

Then we can put

$$ABr = a^2 + 11ab - b^2\,, \qquad abr^5 = A^2 + 11AB - B^2$$

with $r \in \boldsymbol{Q}$. From these and (2.3)

$$\{s^2 + (r^5 + 5r^4 + 15r^3 + 25r^2 + 25r + 11)s - 1\}$$
$$\cdot\{s^2 - (r^5 - 5r^4 + 15r^3 - 25r^2 + 25r - 11)s - 1\} = 0\,,$$

where $s = a/b \in \boldsymbol{Q}$. So by a substitution $r + 1 = t$ or $r - 1 = t$ above equation is equivalent to

$$s^2 + (t^4 + 5t^2 + 5)st = 1\,. \tag{2.5}$$

Thus to find A, B (or a, b) satisfying (2.3) and (2.4) is reduced to finding all the rational solutions of a diophantine equation (2.5). Trivial solutions $(s, t) = (\pm 1, 0)$ of above equation (2.5) result in $AB = \pm 11$, which is no more than a familiar curve

$$y^2 + y + x^3 + x^2 = 0\,, \quad \Delta = -11\,, \quad N = 11\,. \tag{2.6}$$

And it may be conjectured that the 5-isogenous curve to an elliptic curve with a torsion point of order 5 has a rational point of order 5 if and only if a curve (2.6) is.

Remark. In case that both a and b are odd, the equation (2.1) may be a minimal model for E and in case that the parities of a and b are distinct, for example, if a is odd and b is even, the minimal model of Z-coefficients of (2.1) is as follows

$$y^2 + axy + ab^2y + x^3 - \tfrac{1}{4}(6a + b)bx^2 + \tfrac{1}{2}ab^2(2a + b)x = 0$$

and the 5-isogenous curve is as follows

$$y^2 + axy + ab^2y + x^3 - \tfrac{1}{4}(6a + b)bx^2 + \tfrac{1}{2}ab(10a^2 - 18ab - 9b^2)x$$
$$- ab(a^4 - 10a^3b - 5a^2b^2 - 15ab^3 - b^4) = 0\,.$$

With regard to the degenerate reduction we have

THEOREM 2.1. *Let E be an elliptic curve given by* (2.1) *with a torsion point of order* 5 *and N be the conductor of E. Then we have, for any prime p dividing Δ,*

$$p \neq 5 \Longrightarrow \operatorname{ord}_p N = 1$$
$$p = 5 \Longrightarrow \operatorname{ord}_5 N = \begin{cases} 1 & \text{if } 5 \mid a \text{ or } 5 \mid b \\ 2 & \text{if } 5 \nmid a \text{ and } 5 \nmid b\,. \end{cases}$$

Proof. At first we have $\Delta = -a^5b^5(a^2 + 11ab - b^2)$,

$$j = (a^4 + 12a^3b + 14a^2b^2 - 12ab^3 + b^4)^3\Delta^{-1} .$$

If either $p \nmid a$, $p \mid b$ or $p \mid a$, $p \nmid b$, it follows that $\mathrm{ord}_p \Delta = -\mathrm{ord}_p j$. Therefore we have $\mathrm{ord}_p N = 1$ in these cases. If $p \nmid a$ and $p \nmid b$, then $p \mid (a^2 + 11ab - b^2)$. Hence

$$\begin{aligned} &a^4 + 12a^3b + 14a^2b^2 - 12ab^3 + b^4 \\ &\quad = (a^2 + 11ab - b^2)(a^2 + ab + 4b^2) + 5b^3(b - 11a) \equiv 0 \end{aligned}$$

$(\mathrm{mod}\, p)$ if and only if $5b^3(b - 11a) \equiv 0 \,(\mathrm{mod}\, p)$. So because of $b(b - 11a) \equiv a^2 \not\equiv 0 \,(\mathrm{mod}\, p)$, we have

$$a^4 + 12a^3b + 14a^2b^2 - 12ab^3 + b^4 \equiv 0 \,(\mathrm{mod}\, p) \qquad \text{if and only if } p = 5 .$$

Thus we complete the proof.

3. $n = 7$

In this case as a minimal model for a curve E, by transforming an equation given by Nagell [3, § 4], we can take

$$E: y^2 - (a^2 - 3ab + b^2)xy + ab^2(a - b)^3y + x^3 - ab^2(a - b)x^2 = 0$$

with $a, b \in \boldsymbol{Z}$, $(a, b) = 1$ and $a > 0$. The discriminant Δ of E is

$$\Delta = a^7b^7(a - b)^7(a^3 - 8a^2b + 5ab^2 + b^3)$$

and the torsion group is $\{(0, 0), (0, -ab^2(a - b)^3), (ab^2(a - b), 0), (ab^2(a - b), -a^2b^3(a - b)), (-ab(a - b)^2, a^2b^2(a - b)^2), (-ab(a - b)^2, -a^2b(a - b)^3), \infty\}$. (cf. Tate [5, p. 195]). Then the 7-isogenous curve E' to E is given by a model

$$\begin{aligned} E': y^2 &- (a^2 - 3ab + b^2)xy + ab^2(a - b)^3y + x^3 - ab^2(a - b)x^2 \\ &- 5ab(a - b)(a^5 + a^4b - 6a^3b^2 + 8a^2b^3 - 6ab^4 + b^5)x \\ &+ ab(a - b)(a^9 + 9a^8b - 32a^7b^2 + 70a^6b^3 - 167a^5b^4 \\ &+ 281a^4b^5 - 252a^3b^6 + 111a^2b^7 - 23ab^8 + b^9) = 0 \end{aligned}$$

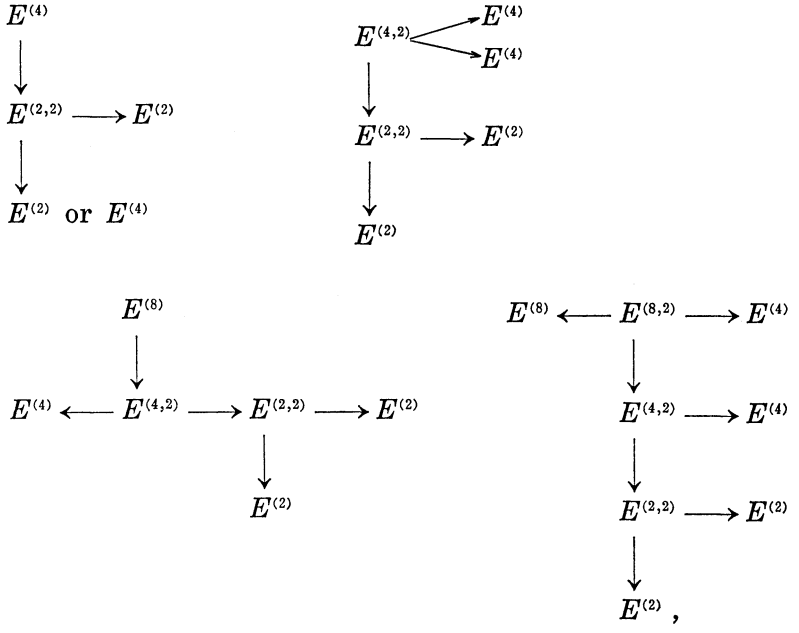
by the method of Vélu [6] and the discriminant Δ' is

$$\Delta' = ab(a - b)(a^3 - 8a^2b + 5ab^2 + b^3)^7 .$$

Beyond these we discuss nothing for $n = 7$ by reason of a complication of the calculation.

4. $n = 4, 8, 16$

In these cases the models are given in Bergman [1], so we consider only the 2-isogenous curves here. Then we have the diagrams below by the elementary (but troublesome a little) calculation.



where $E^{(\ )}$ denotes a curve that the torsion subgroup is of type ( ) and $\rightarrow$ denotes the 2-isogeny among them. And we can easily determine from the coefficients of its model whether it is $E^{(2)}$ or $E^{(4)}$.

5. $n = 6$

In this case the curve has a torsion point of order 2 and of order 3, as the model, minimal at all prime $p \neq 2$, we have

$$E_1 : y^2 - 2(a + b)xy + 2ab^2y + x^3 = 0$$

with $a, b \in \boldsymbol{Z}$, $(a, b) = 1$ and the discriminant

$$\Delta_1 = 2^4a^3b^6(2a - b)^2(a + 4b) .$$

The 2-isogenous curve

$$E_2 : y^2 + 2(a - 2b)xy + 4a^2by + x^3 = 0$$
$$\Delta_2 = -2^8a^6b^3(2a - b)(a + 4b)^2$$

has a torsion point of order 2 and of order 3 again.
The 3-isogenous curves to E_1, E_2 are as follows:

$$E_3: y^2 + x^3 - (a^2 - 10ab - 2b^2)x^2 - (2a - b)^3bx = 0$$
$$\Delta_3 = 2^4ab^2(2a - b)^6(a + 4b)^3 ,$$
$$E_4: y^2 + x^3 + 2(a^2 - 10ab - 2b^2)x^2 + a(a + 4b)^3x = 0$$
$$\Delta_4 = -2^8a^2b(2a - b)^3(a + 4b)^6$$

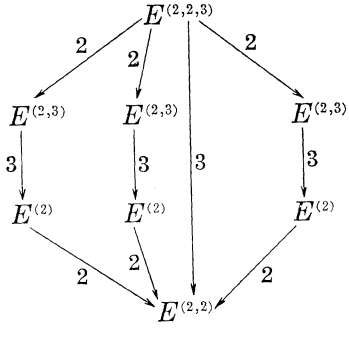
respectively.
Thus these curves E_3 and E_4 have a torsion point of order 2 and 2-isogenous to each other, that is to say,

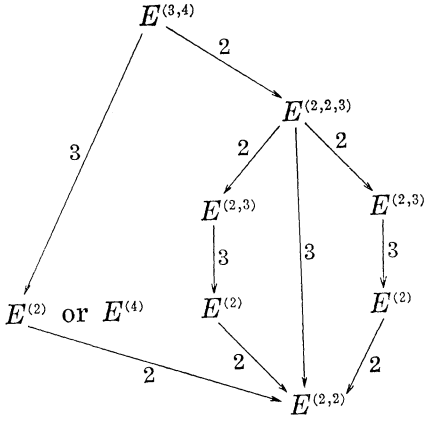
$$\begin{array}{ccc} E_1 & \underset{2}{\overset{2}{\rightleftarrows}} & E_2 \\ \downarrow 3 & & \downarrow 3 \\ E_3 & \underset{2}{\overset{2}{\rightleftarrows}} & E_4 , \end{array}$$

where $\xrightarrow{k}$ denotes the isogeny of degree k.

6. $n = 12$

In this case the model is given in Bergman [1], so we consider only the 2-isogenous and 3-isogenous curves here. Then we have as **4**





7. $n = 10$

In this case the curve has a torsion point of order 2 and of order 5, as the minimal model by transforming an equation given by Bergman [1], we have

$$E_1: y^2 + a^2b^4(a-b)(a+b)^2y + x^3 - \tfrac{1}{4}(a^6 - 2a^5b - 5a^4b^2 + 7a^2b^4 + 2ab^5 + b^6)x^2 + \tfrac{1}{2}a^2b^4(a-b)(a+b)^2(a^3 - a^2b - ab^2 - b^3)x = 0$$

with $a, b \in \boldsymbol{Z}$, $(a, b) = 1$ and the discriminant

$$\Delta_1 = a^{10}b^{10}(a-b)^5(a+b)^5(a^2 + ab - b^2)^2(a^2 - 4ab - b^2) .$$

The 2-isogenous curve

$$E_2: y^2 + ab^2(a+b)^2(a-b)^4y + x^3 - \tfrac{1}{4}(a^6 - 2a^5b + 7a^4b^2 + 12a^3b^3 + 7a^2b^4 - 10ab^5 + b^6)x^2 + \tfrac{1}{2}ab^2(a+b)^2(a-b)^4(a^3 + a^2b + 3ab^2 - b^3)x = 0$$

$$\Delta_2 = a^5b^5(a-b)^{10}(a+b)^{10}(a^2 + ab - b^2)(a^2 - 4ab - b^2)^2$$

has a torsion point of order 2 and of order 5 again. The 5-isogenous curves to E_1, E_2 are as follows:

$$E_3: y^2 + x^3 - \tfrac{1}{4}(a^2 + b^2)(a^4 + 22a^3b - 6a^2b^2 - 22ab^3 + b^4)x^2 + ab(a^2 + ab - b^2)^5x = 0$$

$$\Delta_3 = a^2b^2(a-b)(a+b)(a^2 + ab - b^2)^{10}(a^2 - 4ab - b^2)^5 ,$$

$$E_4: y^2 + x^3 + \tfrac{1}{2}(a^2 + b^2)(a^4 + 22a^3b - 6a^2b^2 - 22ab^3 + b^4)x^2 + \tfrac{1}{16}(a+b)(a-b)(a^2 - 4ab - b^2)^5x = 0$$

$$\Delta_4 = ab(a-b)^2(a+b)^2(a^2 + ab - b^2)^5(a^2 - 4ab - b^2)^{10}$$

respectively.

Thus these curves E_3 and E_4 have a torsion point of order 2 and 2-isogenous to each other, that is to say,

$$\begin{array}{ccc} E_1 & \underset{2}{\overset{2}{\rightleftarrows}} & E_2 \\ \downarrow 5 & & \downarrow 5 \\ E_3 & \underset{2}{\overset{2}{\rightleftarrows}} & E_4 . \end{array}$$

8. $n = 9$

In this case as a model, transforming an equation given by Nagell [3, § 5], we have

$$E_1: y^2 + (a^3 - 3ab^2 + b^3)xy + a^3b^3(a-b)^3y + x^3 = 0$$

with $a, b \in \boldsymbol{Z}$, $(a, b) = 1$ and the discriminant

$$\Delta_1 = -a^9b^9(a-b)^9(a^2 - ab + b^2)^3(a^3 + 3a^2b - 6ab^2 + b^3) .$$

Then the 3-isogenous curve E_2 to E_1 has a torsion point of order 3 from **1**, so there exists the 3-isogenous curve E_3 to E_2, that is,

$$E_2: y^2 + (a^3 - 6a^2b + 3ab^2 + b^3)xy + ab(a-b)(a^2 - ab + b^2)^3y + x^3 = 0$$
$$\Delta_2 = -a^3b^3(a-b)^3(a^2 - ab + b^2)^9(a^3 + 3a^2b - 6ab^2 + b^3)^3 ,$$
$$E_3: y^2 + (a^3 - 6a^2b + 3ab^2 + b^3)xy + ab(a-b)(a^2 - ab + b^2)^3y$$
$$+ x^3 + 5ab(a-b)(a^3 - 6a^2b + 3ab^2 + b^3)(a^2 - ab + b^2)^3x$$
$$- ab(a-b)(a^2 - ab + b^2)^3(a^9 - 25a^8b + 145a^7b^2 - 384a^6b^3$$
$$+ 406a^5b^4 - 127a^4b^5 - 15a^3b^6 - 19a^2b^7 + 16ab^8 + b^9) = 0$$
$$\Delta_3 = -ab(a-b)(a^2 - ab + b^2)^3(a^3 + 3a^2b - 6ab^2 + b^3)^9 .$$

Thus E_2 (resp. E_3) do not have a torsion point of order 9 (resp. of order 3).

REFERENCES

[1] Bergman, G., On the exceptional points of cubic curves, Ark för Mat., **2** (1953), 489–535.
[2] Koike, M., The 3-parts of the conductor of $y^2+x^3+ax+b=0$, unpublished (1974).
[3] Nagell, T., Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque, Nova Acta Reg. Soc. Upsaliensis, **15**, (1952), 1–66.
[4] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini der courbes elliptiques, Invent. Math., **15** (1972), 259–331.
[5] Tate, J., The arithmetic of elliptic curves, Invent. math., **23** (1974), 179–206.
[6] Vélu, J., Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris, **273** (1971), 238–241.

Department of Mathematics
Meijō University