Toshihiro Hadano
Nagoya Math. J.
Vol. 53 (1974), 199-210

ON THE CONDUCTOR OF AN ELLIPTIC CURVE WITH A RATIONAL POINT OF ORDER 2

TOSHIHIRO HADANO

1. Introduction

Let C be an elliptic curve (an abelian variety of dimension one) defined over the field $\boldsymbol{Q}$ of rational numbers. A minimal Weierstrass model for C at all primes p in the sense of Néron [3] is given by a plane cubic equation of the form

$$y^2 + a_1xy + a_3y + x^3 + a_2x^2 + a_4x + a_6 = 0 , \qquad (1.1)$$

where a_j belongs to the ring $\boldsymbol{Z}$ of integers of $\boldsymbol{Q}$, the zero of C being the point of infinity.

Following Weil, we define the conductor N of C by

$$N = \prod_{\text{all } p} p^{(\operatorname{ord}_p \Delta + 1 - n_p)} ,$$

where Δ denotes the discriminant of C, and n_p is the number of components of the Néron reduction of C over $\boldsymbol{Q}$ without counting multiplicities. It is well-known that the p-exponent of N is

$$\operatorname{ord}_p \Delta + 1 - n_p = \begin{cases} 0 & \text{for non-degenerate reduction} \\ 1 & \text{for multiplicative reduction} \\ 2 & \text{for additive reduction and } p \neq 2,3 \\ \geqq 2 & \text{for additive reduction and } p = 2,3 . \end{cases}$$

Therefore both N and Δ of a minimal model are divisible exactly by those primes at which C has degenerate reduction. (See Ogg [6], [7]).

We consider the problem to find all the elliptic curves over $\boldsymbol{Q}$ of given conductor N. As we may reduce this problem to find the rational solutions of the diophantine equation $y^2 = x^3 + k$ with $k \in \boldsymbol{Z}$, there are only finitely many such curves by virtue of Thue's theorem. Ogg [5], [6] has found all the curves by showing that they have a rational point

Received September 27, 1973.

of order 2 for $N = 2^m$, $3 \cdot 2^m$ $9 \cdot 2^m$, while Vélu [8] found all the curves of $N = 11^m$ under the Weil's conjecture for $\Gamma_0(N)$. On the other hand, Miyawaki [1] has calculated all the curves of prime power conductor with a rational point of finite order >2.

In this paper we treat the curves of $N = p^m$ and $2^m p^n$ (for this case, see [10] as résumé) with a rational point of order 2. For $N = p^m$, we can find all admissible p, and, a fortiori, all the curves for each p. (Section 3). For $N = 2^m p^n$, we can find all the curves under an assumption which can be eliminated for 'non-large' p with $p \equiv 3$ or 5 (mod 8). Moreover, we get some results on the elliptic curve which has multiplicative reduction at 2 and p, and these are generalizations of the results of Ogg [6]. (Section 4). In Appendix all the elliptic curves of 3-power conductor are determined.

2. Diophantine lemma

We prepare all the diophantine results we need afterwards.

LEMMA. *The only non-zero integral solutions of the equations below for a given odd prime p are as follows:*

1) *If* $X^2 - 1 = 2^\alpha p^\beta$, *then* $(|X|, 2^\alpha p^\beta) = (2,3), (3,2^3), (5,2^3 3), (7,2^4 3), (9,2^4 5), (17,2^5 3^2)$ *for* $p \equiv 3$ *or* 5 (mod 8), *and* $\beta = 1$, $p = 2^{\alpha-2} \pm 1$ $(\alpha \geqq 5)$ *for* $p \equiv 1$ *or* 7 (mod 8).

2) *If* $X^2 + 1 = 2^\alpha p^\beta$, *then* $(|X|, 2^\alpha p^\beta) = (1,2)$ *for* $p \equiv 3$ (mod 4), *and either* $\alpha = 0$, $\beta = 1$ *or* $\alpha = 1$, $\beta = 1, 2, 4$ *for* $p \equiv 1$ (mod 4). *In particular we have* $\beta = 4$ *if and only if* $p = 13$, $|X| = 239$.

3) *If* $2X^2 - 1 = p^\alpha$, $\alpha > 0$, *then there is no solution for* $p \equiv 3$ *or* 5 (mod 8).

4) *If* $2X^2 + 1 = p^\alpha$, $\alpha > 0$, *then* $\alpha = 1, 2$ *or* $(|X|, p^\alpha) = (11, 3^5)$ *for* $p \equiv 1$ *or* 3 (mod 8), *and there is no solution for* $p \equiv 5$ *or* 7 (mod 8).

5) *We assume here that p satisfies the conjecture of Ankeny-Artin-Chowla and the analogy* (*See* [2], *Chapter* 8) *for* $p \equiv 3$ *or* 5 (mod 8). *If* $|\pm p^\alpha - X^2| = 2^\beta$, *then* $(\pm p^\alpha, |X|) = (1,3), (-1,1), (3,2), (-3,1), (3^2,1), (3^2,5), (3^3,5), (3^4,7)$ *or* $\alpha = \beta = 1$ *for* $p \equiv 3$ (mod 8), *and* $(\pm p^\alpha, |X|) = (1,3), (-1,1), (5^2,3), (5^3,11)$, $\alpha = 1$, $\beta = 0$ *or* $\alpha = 1$, $\beta = 2$ *for* $p \equiv 5$ (mod 8).

6) *If* $pX^2 - Y = \pm 2^\alpha$, *and* $Y = \pm 2^\beta$, *then either* $2 | X, 4 | Y$, *or* $(|X|, Y) = (1,4), (1,2), (1,1), (1,-1)$ *for* $p = 3$, $(1,4), (1,1)$ *for* $p = 5$, *and there is no solution for* $p \neq 3, 5$.

7) *If* $X^2 - 64 = p^\alpha$, *then* $(|X|, p^\alpha) = (9, 17)$.

8) *If* $X^2 + 64 = p^\alpha$, *then* $(|X|, p^\alpha) = (15, 17^2)$ *or* $\alpha = 1$ *for all p.*

This lemma except 7) and 8) is a generalization of Diophantine lemma of Ogg [6]. The methods for solving these equations are standard and elementary. We refer to each parts of this lemma as $D_1, \cdots, D_8$. D_1 is easy by [2], Chapter 30. D_2 may be solved by factorization in $\boldsymbol{Z}[\sqrt{-1}]$ and Ljunggren's result in [2], Chapter 28. D_3 is easy. D_4 and D_5 may be solved by the congruence method and the results of Pell's equation. D_6 and D_7 are easy. D_8 may be solved by factorization in $\boldsymbol{Z}[\sqrt{-1}]$.

3. The case of $N = p^m$

Let C be an elliptic curve of conductor $N = p^m$ with a rational point of order 2. Then we have $m = 1$ or 2 from Section 1 if $p \neq 2, 3$ (cf. Appendix) and we have a defining equation for C of the form

$$y^2 + x^3 + a_2x^2 + a_4x = 0 \tag{3.1}$$

with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2$, and such that we do not have $2^2 | a_2$ and $2^4 | a_4$. This curve is isomorphic to

$$y^2 + xy + x^3 + \left(\frac{a_2 + 1}{4}\right)x^2 + \frac{a_4}{16}x = 0\ , \tag{3.2}$$

minimal at all p. If these coefficients are not integers, they can be made integers by a translation.

Now we propose to find all possible p such that the discriminant of (3.2) is

$$\Delta = 2^{-8}a_4^2(a_2^2 - 4a_4) = \pm p^\lambda\ .$$

This result will give the determination of all C above up to isomorphisms. At first, dividing the curve (3.2) by the group generated by $(x, y) = (0, 0)$, we have an isogenous curve of degree 2 given by

$$y^2 + xy + x^3 + \left(\frac{1 - 2a_2}{4}\right)x^2 + \left(\frac{a_2^2 - 4a_4}{16}\right)x = 0\ , \tag{3.3}$$

which also has a rational point $(x, y) = (0, 0)$ of order 2. Its discriminant is $2^{-4}a_4(a_2^2 - 4a_4)^2 = \pm p^u 2^{12k}$ $(k \in \boldsymbol{Z},\ k \geqq 0)$, since (3.3) is not necessarily minimal at $p = 2$ and there is a relation, in general, $12 | (\operatorname{ord}_p \Delta' - \operatorname{ord}_p \Delta)$ between the discriminant Δ' of a non-minimal model and the discriminant Δ of its minimal model. Hence we have $p^{2\lambda} = \pm 2^{12k-12}a_4^3p^u$, and so $|a_4| = 1$, 16, p^α or $16p^\alpha$ and $k = 0$ or 1. On the other hand, either a_2 is odd or

$2 \| a_2$ as we see below, and we see that only if $a_2 \equiv 3 \pmod 4$ or $a_2 \equiv 2 \pmod 8$ according as $2 \nmid a_2$ or $2 \| a_2$ respectively, we may rewrite the equation (3.3) to the minimal equation of integral coefficients by a suitable translation.

If $a_4 = \pm 1$, then $a_2 = 2b_2$ is even, so $|b_2^2 \pm 1| = 2^6 p^\lambda$, and by D_1 and D_2 we get $(p, a_2, a_4) = (17, 66, 1)$. If $a_4 = \pm 16$, then $|a_2^2 \pm 64| = p^\lambda$; by D_7 and D_8 we get $(p, a_2, a_4) = (17, -9, 16), (17, 15, -16)$, or $(X^2 + 64, X, -16)$. If $a_4 = \pm p^\alpha$, then $a_2 = 2b_2$ is even, so $|b_2^2 \pm p^\alpha| = 2^6 p^{\lambda - 2\alpha}$. Suppose first $\lambda = 2\alpha$, then $|b_2^2 \pm 64| = p^\alpha$; by D_7 and D_8 we get $(p, a_2, a_4) = (17, 18, 17)$, $(17, -30, 17^2)$ or $(X^2 + 64, -2X, X^2 + 64)$. Henceforth put $b_2 = p^t c_2$ $(p \nmid c_2)$ so that $|p^{2t} c_2^2 \pm p^\alpha| = 2^6 p^{\lambda - 2\alpha}$. If $\alpha \geqq 4$, then $t = 1$ since otherwise we can find a better model, so $c_2^2 \pm p^{\alpha - 2} = \pm 2^6 p^{\lambda - 2\alpha - 2}$ and by D_7 and D_8 we get $(p, a_2, a_4) = (17, -510, 17^4)$. If $\alpha = 3$, then $|c_2^2 \pm p^{3-2t}| = 2^6 p^{\lambda - 2t - 6}$ or $|p^{2t-3} c_2^2 \pm 1| = 2^6 p^{\lambda - 9}$, and by D_7 and D_8 we get $(p, a_2, a_4) = (17, 306, 17^3)$, $(X^2 + 64, 2X(X^2 + 64), (X^2 + 64)^3)$ or $(7, -294, -7^3)$. If $\alpha = 2$, then $|c_2^2 \pm p^{2-2t}| = 2^6 p^{\lambda - 2t - 4}$ or $|p^{2t-2} c_2^2 \pm 1| = 2^6 p^{\lambda - 6}$, and by D_1, D_2, D_7 and D_8 we get $(p, a_2, a_4) = (17, 66 \cdot 17, 17^2)$. If $\alpha = 1$, then $|p^{2t-1} c_2^2 \pm 1| = 2^6 p^{\lambda - 3}$ and we get $(p, a_2, a_4) = (7, 42, -7)$. Lastly if $a_4 = \pm 16 p^\alpha$, then $|a_2^2 \pm 2^6 p^\alpha| = p^{\lambda - 2\alpha}$. Therefore similarly to above, we get $(p, a_2, a_4) = (17, -33, 16 \cdot 17)$, $(17, -17 \cdot 9, 16 \cdot 17^2)$, $(17, 17 \cdot 15, -16 \cdot 17^2)$, $(17, 17 \cdot 33, 16 \cdot 17^3)$, $(7, 147, 16 \cdot 7^3)$, $(X^2 + 64, X(X^2 + 64), -16(X^2 + 64)^2)$ or $(7, -21, 16 \cdot 7)$. This completes all cases.

By identifying the isomorphic curves each other we have

THEOREM I. *There are elliptic curves of conductor $N = p^m$, (where $p \neq 2$ and $m = 1$ or 2), with a rational point of order 2 for $p = 7$, 17 and primes p such that $p - 64$ is square.*

The minimal models with integral coefficients for $p = 7, 17, 73$ are following:

Table 1.

N	minimal equation	Δ	2-division points $(x,y) \neq \infty$
7^2	$y^2 + xy + x^3 - 5x^2 + 7x = 0$	-7^3	$(0,0)$
	$y^2 + xy + x^3 - 5x^2 - 28x + 3 \cdot 7^2 = 0$	7^3	$\left(\frac{21}{4}, -\frac{21}{8}\right)$
	$y^2 + xy + x^3 + 37x^2 + 7^3 x = 0$	-7^9	$(0,0)$
	$y^2 + xy + x^3 + 37x^2 - 4 \cdot 7^3 x - 3 \cdot 7^5 = 0$	7^9	$\left(-\frac{147}{4}, \frac{147}{8}\right)$

https://doi.org/10.1017/S0027763000016147 Published online by Cambridge University Press

N	minimal equation	Δ	2-division points $(x,y)\neq\infty$
17	$y^2+xy+x^3-2x^2+x=0$	17	$(0,0),(1,0),(1,-1)$
	$y^2+xy+x^3+16x^2-8x+1=0$	17	$\left(\frac{1}{4},-\frac{1}{8}\right)$
	$y^2+xy+x^3+4x^2-x=0$	17^2	$(0,0),(-4,2),\left(\frac{1}{4},-\frac{1}{8}\right)$
	$y^2+xy+x^3-20x^2+136x-17^2=0$	-17^4	$\left(\frac{17}{4},-\frac{17}{8}\right),(0,\pm 17)$
17^2	$y^2+xy+x^3-38x^2+17^2x=0$	17^7	$(0,0),(-17,9\cdot 17),$ $(-17,-8\cdot 17)$
	$y^2+xy+x^3+268x^2-8\cdot 17^2x+17^3=0$	17^7	$\left(\frac{17}{4},-\frac{17}{8}\right)$
	$y^2+xy+x^3-140x^2+17^3x=0$	17^8	$(0,0),(68,-34),\left(\frac{17^2}{4},-\frac{17^2}{8}\right)$
	$y^2+xy+x^3-344x^2+8\cdot 17^3x-17^5=0$	-17^{10}	$\left(\frac{17^2}{4},-\frac{17^2}{8}\right)$
73	$y^2+xy+x^3+x^2-x=0$	73	$(0,0)$
	$y^2+xy+x^3+x^2+4x+3=0$	-73^2	$\left(-\frac{3}{4},\frac{3}{8}\right)$
73^2	$y^2+xy+x^3+55x^2-73^2x=0$	73^7	$(0,0)$
	$y^2+xy+x^3+55x^2+4\cdot 73^2x+3\cdot 73^3=0$	-73^8	$\left(-\frac{219}{4},\frac{219}{8}\right)$

Remark. We see that the members in each N above are isogenous to each other. (See Vélu [9]). For $p=2$, see Ogg [5]. It is well known that $N\neq 7$.

4. The case of $N=2^mp^n$

In this section we deal with the case $N=2^mp^n$ for odd prime p and generalize the results of Ogg using his ideas ([6], § 2).

Let $K=\boldsymbol{Q}(C_2)$ be a Galois field generated by the group C_2 of 2-division points on the elliptic curve C defind over $\boldsymbol{Q}$. For each prime p, e_p denotes the ramification degree of $K/\boldsymbol{Q}$ at p. Then we know the following results:

LEMMA (Ogg [6]). (1) *If C has non-degenerate reduction at each $p\neq 2$, then $e_p=1$.*

(2) *If C has multiplicative reduction at all p, then $e_p=1$ or 2.*

(3) *Suppose C has no non-zero point of order 2 in rational coordinates, then K/k is cyclic of degree 3 over a field k of degree 1 or 2 over $\boldsymbol{Q}$. Suppose furthermore $e_p=1$ or 2 for all p. Then the class number of*

k is divisible by 3.

Now let p be an odd prime such that none of the class numbers of four fields $\boldsymbol{Q}(\sqrt{\pm p})$, $\boldsymbol{Q}(\sqrt{\pm 2p})$ is divisible by 3, and fix this p. Suppose C has non-degenerate reduction (i.e. good reduction) at all primes $q \neq 2$, p. Then $e_q = 1$ by (1) in Lemma, and if the first conditions of (3) in Lemma is satisfied, then k in (3) is $\boldsymbol{Q}$, $\boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{\pm 2})$, $\boldsymbol{Q}(\sqrt{\pm p})$ or $\boldsymbol{Q}(\sqrt{\pm 2p})$. Hence $3 \mid e_2$ or $3 \mid e_p$. Therefore $3 \mid e_2$ by virtue of (2) in Lemma if $N = 2^m p$, that is, C has a rational point of order 2 if $e_2 = 1$ or 2 and $N = 2^m p$. In particular by (2) in Lemma C has a rational point of order 2 if $N = 2p$. So we can generalize Ogg's result:

THEOREM II. *If none of the class numbers of four quadratic fields* $\boldsymbol{Q}(\sqrt{\pm p})$, $\boldsymbol{Q}(\sqrt{\pm 2p})$ *for a prime* $p \equiv 3$ *or* 5 (mod 8) *is divisible by* 3, *then there are no elliptic curves of conductor* $N = 2p$.

Proof. If there exists such a curve, we can choose an equation

$$y^2 + x^3 + a_2x^2 + a_4x = 0$$

with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2$. We also assume that we do not have $2^2 \mid a_2$ and $2^4 \mid a_4$. Since we have multiplicative reduction at 2 and p, $\mathrm{ord}_2 j < 0$ and $p \nmid a_2$ (cf. [3]), where $j = 2^{12}(a_2^2 - 3a_4)^3 \Delta^{-1}$ is the invariant of the curve with the discriminant $\Delta = 2^4 a_4^2(a_2^2 - 4a_4) = \pm 2^\mu p^\nu$. Hence we have $\mu = \mathrm{ord}_2 \Delta > 12$. If a_2 is odd, then $a_2^2 - 4a_4 = \pm p^\alpha$, $\mathrm{ord}_2(4a_4) > 6$. If $p \mid a_4$, then $a_2^2 \pm 1 = 4a_4 = 2^\alpha p^\beta$, which is impossible by D_1 and D_2 since $\alpha > 6$. If $p \nmid a_4$, then $|\pm p^\alpha - a_2^2| = |4a_4| = 2^\beta$, $\beta > 6$, which is also impossible by D_5 (without the assumption there). Then we see that this theorem can be proven by the same method as used by Ogg to show $N \neq 10$, 12 in [6], § 4. (Replace Diophantine lemma there with our D_1 and D_5! 'Of type $C1$' in his proof should be 'of type $C2$'.)

For example, we have $p = 37, 43, 67, 197, 227$ etc. except $p = 3, 5, 11$. However, it is well-known that this is not true for $p \equiv 1$ or 7 (mod 8), but on the other hand we have

THEOREM III. *If none of the class numbers of four quadratic fields* $\boldsymbol{Q}(\sqrt{\pm p})$, $\boldsymbol{Q}(\sqrt{\pm 2p})$ *for a prime* $p \equiv 1$ *or* 7 (mod 8) *is divisible by* 3, *then the elliptic curves of conductor* $N = 2^m p$, $(m > 0)$, *have a rational point of order* 2.

Proof. As a defining equation for a curve C of $N = 2^m p$, we can take

$$y^2 + x^3 + a_2x^2 + a_4x + a_6 = 0$$

with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2$. If $3 \nmid a_2$, then we get an equation

$$y^2 + x^3 + a_4x + a_6 = 0 \tag{4.1}$$

with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2, 3$ and such that we do not have $2^4 | a_4$ and $2^6 | a_6$. The discriminant Δ of this curve is

$$\Delta = -2^4(4a_4^3 + 27a_6^2) = \pm 2^\mu 3^{12} p^\nu\,, \qquad (\mu, \nu > 0)\,.$$

Suppose that C has no rational point of order 2, then an irrational point (x, y) of order 2 is $(r, 0)$, where r is a root of $f(X) = X^3 + a_4X + a_6$ and $r \notin \boldsymbol{Q}$. Therefore the ramification degree e_2 at the prime 2 of $\boldsymbol{Q}(r)/\boldsymbol{Q}$ is 3 under the assumption as we have seen. Considering the discriminant of this cubic field, we see that a_6 is even. If a_4 is odd, then $x = 0$ refines to a root r of $f(X)$ in $\boldsymbol{Q}_2$ by Newton's method. This is a contradiction. Put $a_4 = -2u$, $a_6 = 2v$. Then $8u^3 - 27v^2 = \pm 2^{\mu-6}3^{12}p^\nu$, so v is even, since otherwise $8u^3 - 27v^2 = \pm 3^{12}p^\nu$, which is impossible modulo 8 for $p \equiv 1$ or $7 \pmod 8$. Put $v = 2v_1$. Then we have $f(X) = X^3 - 2uX + 2^2v_1$, hence u is even by $e_2 = 3$. Put $u = 2u_1$, then $16u_1^3 - 27v_1^2 = \pm 2^{\mu-8}3^{12}p^\nu$, so v_1 is even, since otherwise $16u_1^3 - 27v_1^2 = \pm 3^{12}p^\nu$, which is impossible as above. Therefore we have $2^2 | a_4$ and $2^3 | a_6$. Thus to solve $f(X) = 0$ is the same thing as to solve

$$2^{-3}f(2X) = X^3 + 2^{-2}a_4X + 2^{-3}a_6\,.$$

Hence repeating the above arguments, we have $2^4 | a_4$ and $2^6 | a_6$, and this is a contradiction. If $3 | a_2$, then we get (4.1) with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2$, such that the discriminant

$$\Delta = -2^4(4a_4^3 + 27a_6^2) = \pm 2^\mu p^\nu \qquad (\mu, \nu > 0)$$

and such that we do not have $2^4 | a_4$ and $2^6 | a_6$. In the same manner as above, we can complete the proof of this case, too.

For example we have $p = 7, 17, 41, 47, 73, 97$ etc. as such p.

In another direction:

THEOREM IV. *All the elliptic curves of the conductor* $N = 2^m p^n$, *where* $p \equiv 3$ *or* $5 \pmod 8$ *and* $p \neq 3$, *that have a rational point of order*

2 are effectively determined under the conjecture of Ankeny-Artin-Chowla and the analogy. In particular if $p-2$ or $p-4$ is a square number, then the assumption on the conjecture can be eliminated.

Proof. We can take a defining equation for C of the form

$$y^2 + x^3 + a_2x^2 + a_4x = 0 \tag{4.2}$$

with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2$, and such that we do not have $2^2 | a_2$ and $2^4 | a_4$. The discriminant of this model is

$$\Delta = 2^4 a_4^2(a_2^2 - 4a_4) = \pm 2^\mu p^\nu \,. \tag{4.3}$$

It is sufficient to find all the pairs (a_2, a_4) satisfying (4.3) for a given p. Noting that $p \nmid a_2$ (resp. $p | a_2$) if $N = 2^m p$ (resp. $N = 2^m p^2$), we can get all the pairs (a_2, a_4), up to isomorphisms, by virtue of Diophantine lemma $D_1, \cdots, D_6$ in view of the fact that $2^2 \nmid a_2$ and $2^4 \nmid a_4$. (For details, see Ogg [6], § 3.)

Remark. We know that $n = 1$ or 2 only if $p \geqq 5$. For $p = 3$, Ogg [6] has found all the curves of conductor $N = 3\cdot 2^m$ and $9\cdot 2^m$ by showing that they have a rational point of order 2 (cf. [4]), and Coghlan has found in his thesis all the curves of conductor $N = 2^m 3^n$. For example, if $N = 2^m 5$ in our case, then $2 \leqq m \leqq 7$ and there are 56 curves with a rational point of order 2. We can prove, in general, that the integer m is not larger than 8. Moreover, we see that the equation (4.2) is minimal at all p (including $p = 2$), in fact, otherwise we can consider the same situation as in Section 3 for $N = 2^m p^n$ to show that we cannot find the pairs (a_2, a_4) of the equation (3.2) since the equation $|X^2 \pm p^\alpha| = 2^\beta$, $\beta > 6$, has no integer solutions for $p \equiv 3$ or $5 \pmod 8$ by D_5. For $p \equiv 1$ or $7 \pmod 8$, it seems to be difficult to solve the equations of D_3, D_5 (especially D_5) in general, but the theorem remains valid for all $p > 3$ so long as those equations are solved.

5. Supplementary discussions

We can find all the curves of some other conductors N with a rational point of order 2 so long as the corresponding diophantine equations can be solved as in the previous sections. In fact, for example, we can find all the curves of conductor $N = p^m q^n$, where m, $n > 0$, p and q are primes such that $p \equiv 3$, $q \equiv 5 \pmod 8$, with a rational point of order 2. By solving the equations

$$X^2 \pm 64 = \pm p^\alpha q^\beta\,, \quad X^2 \pm 1 = 2^6 p^\alpha q^\beta\,, \quad |p^\alpha X^2 \pm 1| = 2^6 q^\beta\,,$$
$$|p^\alpha \pm 2^6 q^\beta| = X^2\,, \qquad |p^\alpha X^2 \pm 64| = q^\beta$$

induced from the defined equation (3.2) in Section 3 with $\Delta = \pm p^\mu q^\nu$, we get 136 curves of $(p, q) = (3, 5), (3, 13), (11, 5), (19, 5), (3, 37), (3, 61), (59, 5), (11, 53)$ and m, $n = 1$ or 2. Moreover, a fortiori, we can find all the curves of a given conductor N with a rational point of order $r > 2$ so long as the corresponding diophantine equations can be solved. In fact, for example, if $N = 2^m p^n$, and $r = 4$ (cyclic), then such curves can be defined by

$$y^2 + x^3 \pm (s^2 + 2t)x^2 + t^2 x = 0$$

with $s, t \in \boldsymbol{Z}$, $s > 0$, minimal at all $p \neq 2$, and these curves are isogenous to

$$y^2 + x(x \mp s^2)(x \mp s^2 \mp 4t) = 0\,,$$

which have three rational points of order 2. Then we have either $p = 2^k \pm 1$ $(k \geqq 1)$ or $N = 2^5 p^2$, $2^6 p^2$ for all p. In particular, we have only $N = 17^n$ for $m = 0$ and the curves are included in Table 1 in section 3. As another example, suppose $N = 2^m p^n$ and $r = 6$ (non-cyclic, that is, curves which have both a rational point of order 2 and of order 3); then we have $N = 14, 20, 34$ and 36 as Table 2 below. Note that there exist two curves; $y^2 + xy + x^3 - 45x^2 + 2^9 x = 0$, $y^2 + xy + x^3 - 45x^2 - 2^{11}x + 2^9 181 = 0$ (resp. $y^2 + x^3 + 11x^2 - x = 0$, $y^2 + x^3 - 22x^2 + 125x = 0$; $y^2 + x^3 - 9x^2 + 27x = 0$, $y^2 + x^3 + 18x^2 - 27x = 0$) in addition to these for $N = 14$ (resp. 20; 36), and the 6 or 4 curves for $N = 14, 20, 36$ are isogenous to each other of degree 2 or 3.

Table 2.

N		minimal model	Δ	j	2-isogenous to:
14	1	$y^2 + xy + y + x^3 = 0$	$-2^2 7$	$-5^6 2^{-2} 7^{-1}$	2,*
14	2	$y^2 - 5xy + y + x^3 = 0$	$2 \cdot 7^2$	$5^3 101^3 2^{-1} 7^{-2}$	1,**
14	3	$y^2 - 5xy + 7y + x^3 = 0$	$-2^6 7^3$	$5^3 43^3 2^{-6} 7^{-3}$	4,*
14	4	$y^2 - 11xy + 49y + x^3 = 0$	$2^3 7^6$	$5^3 11^3 31^3 2^{-3} 7^{-6}$	3,**
20	5	$y^2 + x^3 - x^2 - x = 0$	$2^4 5$	$2^{14} 5^{-1}$	6
20	6	$y^2 + x^3 + 2x^2 + 5x = 0$	$-2^8 5^2$	$2^4 11^3 5^{-2}$	5
34	7	$y^2 + xy + x^3 + 6x^2 + 8x = 0$	$2^6 17$	$5^3 29^3 2^{-6} 17^{-1}$	8

N		minimal model	Δ	j	2-isogenous to:
34	8	$y^2 + xy + x^3 - 43x - 105 = 0$	$2^3 17^2$	$5^3 7^3 59^3 2^{-3} 17^{-2}$	7
36	9	$y^2 + x^3 + 3x^2 + 3x = 0$	$-2^4 3^3$	0	10
36	10	$y^2 + x^3 - 6x^2 - 3x = 0$	$2^8 3^3$	$2^4 3^3 5^3$	9

* (resp. **) denotes the isogeny of degree 3 between the curves with the same symbol.

APPENDIX

We can find all the elliptic curves of 3-power conductor defined over $\boldsymbol{Q}$, up to isomorphism, as listed in Table below. Coghlan found all the curves of $N = 2^m 3^n$ in his thesis, in which the curves of $N = 3^n$ are dealt with in a manner different from below.

The minimal model (1.1) in Section 1 with $\Delta = \pm 3^\mu$ is reduced to

$$y^2 + x^3 + a_4 x + a_6 = 0 \tag{A–1}$$

with $a_j \in \boldsymbol{Z}$, minimal at all $p \neq 2, 3$, and with the discriminant

$$-2^4(4a_4^3 + 27a_6^2) = \pm 2^{12} 3^\nu .$$

This may be reduced to the diophantine equation

$$y^2 = x^3 \pm 3^{\nu-3} \quad \text{with} \quad a_4 = -2^2 3x,\ a_6 = 2^4 y\ , \tag{A–2}$$

where $\nu \geqq 3$ and $x, y \in \boldsymbol{Z}$. In fact, it is well-known that there are no elliptic curves of the conductor $N = 3^n$ with $0 \leqq n \leqq 2$. In order to show that $x, y \in \boldsymbol{Z}$, we have to show that the equations $y^2 = x^3 \pm 2^6 3^{\nu-3}$ have no odd integral solutions. Since the ranks of the Mordell-Weil groups of the elliptic curves $y^2 = x^3 \pm 1$, $y^2 = x^3 - 3$ and $y^2 = x^3 - 9$ are all zero, it is sufficient to show that $y^2 = x^3 + k$ for $k = 2^6 3^2, 2^6 3, -2^6 3^4$, and $-2^6 3^5$ has only integral solutions. This is easily done in a familiar manner.

LEMMA. *The elliptic curve with the conductor $N = 3^m$ is of the form*

$$y^2 + y + x^3 + a_4 x + a_6 = 0$$

with $a_j \in \boldsymbol{Z}$, minimal at all p.

Proof. By a transformation the equation (1.1) is reduced to

$$y^2 + x^3 + (4a_2 - a_1^2)x^2 + 8(2a_4 - a_1a_3)x + 16(4a_6 - a_3^2) = 0$$

or

$$y^2 + x^3 + 3^4\{24(2a_4 - a_1a_3) - (4a_2 - a_1^2)^2\}x + 3^3\{2(4a_2 - a_1^2)^3 + 16\cdot 3^3(4a_6 - a_3^2) - 8\cdot 3^2(4a_2 - a_1^2)(2a_4 - a_1a_3)\} = 0$$

with the discriminant $\pm 2^{12}3^\mu$ or $\pm 2^{12}3^{\mu+12}$ respectively. Then, since this should coincide with (A–1), a_1 is even by (A–2). If a_3 is even, then (A–2) is minimal at 2, and so the conductor of the model is 2^m3^n $(m > 0)$. Hence we may put $a_3 = 1$ by a transformation $x \to x + r (r \in \boldsymbol{Z})$. Finally $3 | a_2$ in (1.1) since C has an additive reduction at 3. Hence we may put $a_2 = 0$.

Now we can determine all the curves of $N = 3^n$. By the above Lemma, the discriminant is

$$\Delta = -2^6a_4^3 - 27(1 - 4a_6)^2 = \pm 3^\mu ,$$

and so $(1 - 4a_6)^2 = (4c_4)^3 + 3^{\mu-3}$ with $a_4 = -3c_4$. We see that ν is odd, looking modulo 8. On the other hand, all the integral solutions of the equation $y^2 = x^3 + 3^n$ with $x \equiv 0 \pmod 4$, $2 | n$ and $n \leqq 10$ are given by:

n	0	2	4	6	8	10
solutions $(x, \lvert y \rvert)$	(0,1)	(0,3) (40,253)	$(0,3^2)$	$(0,3^3)$	$(0,3^4)$ $(40\cdot 3^2, 253\cdot 3^3)$	$(0,3^5)$

Therefore we get the Table below by taking into consideration that we have a better model whenever $\mu \geqq 15$. The 8 curves listed are all non-isomorphic and the 4 curves of $N = 27$ are isogenous to each other of degree 3.

Table: Curves of conductor $N = 3^\lambda$ and of the form $y^2 + y + x^3 + a_4x + a_6 = 0$

Curve	a_4	a_6	Δ	N	3-type	j	$C_{Q,3} \neq 0$?	3-isogenous to:	isomorphic $/Q(\sqrt{-3})$ to:
1	0	0	-3^3	3^3	$C1$	0	yes	2,3	3
2	-30	-63	-3^5	3^3	$C3$	$-2^{15}\cdot 3\cdot 5^3$	yes	1	4
3	0	7	-3^9	3^3	$C6$	0	yes	1,4	1
4	-270	1708	-3^{11}	3^3	$C8$	$-2^{15}\cdot 3\cdot 5^3$		3	2
5	0	1	-3^5	3^5	$C1$	0		7	7
6	0	-2	-3^7	3^5	$C3$	0	yes	8	8
7	0	-20	-3^{11}	3^5	$C6$	0	yes	5	5
8	0	61	-3^{13}	3^5	$C8$	0		6	6

REFERENCES

[1] I. Miyawaki, Elliptic curves of prime power conductor with Q-rational points of finite order, Osaka J. Math., **10** (1973), 309–323.
[2] L. J. Mordell, Diophantine equations, Academic Press London and New York, (1969).
[3] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I.H.E.S. no. **21** (1965), 5–125.
[4] O. Neumann, Die elliptischen Kurven mit den Führern 3.2^m und 9.2^m, Math. Nachr., **48** (1971), 387–389.
[5] A. P. Ogg, Abelian curves of 2-power conductor, Proc. Camb. Phil. Soc., **62** (1966), 143–148.
[6] ——, Abelian curves of small conductor, J. reine angew. Math., **226** (1967), 205–215.
[7] ——, Elliptic curves and wild ramification, Amer. J. Math., **89** (1967), 1–21.
[8] J. Vélu, Courbes elliptiques sur Q ayant bonne réduction en dehors de {11}, C. R. Acad. Sci. Paris, **273** (1971), 73–75.
[9] ——, Isogénies entre courbes elliptiques, C.R. Acad. Sci. Paris, **273** (1971), 238–241.
[10] T. Hadano, Remarks on the Conductor of an Elliptic Curve, Proc. Jap. Acad., **48** (1972), 166–167.

Nagoya University