40. *Remarks on the Conductor of an Elliptic Curve*

By Toshihiro HADANO
Tokyo Metropolitan University

(Comm. by Kunihiko KODAIRA, M. J. A., March 13, 1972)

1. In this note we treat, in a sense, a generalization of the results by Ogg [2] on the conductor of an elliptic curve defined over the field of rational numbers.

2. Extending the diophantine lemma of Ogg [2], we get

Proposition. *For a given odd prime p such that $p\equiv 3$ or $5 \pmod 8$*

i) *All the integer solutions of the equation $X^2-1=2^\alpha p^\beta$ are, including the trivial case $\alpha\beta=0$, $(|X|, 2^\alpha p^\beta)=(2,3), (3,2^3), (5,2^3 3), (7,2^4 3)$, $(9,2^4 5)$ and $(17,2^5 3^2)$.*

ii) *All the integer solutions of the equation $X^2+1=2^\alpha p^\beta$ are trivially $|X|=1$ if $p\equiv 3 \pmod 8$ and are given by $\alpha=0, \beta=1$ and $\alpha=1, \beta=1, 2$ or 4 if $p\equiv 5 \pmod 8$. Especially we have $\beta=4$ if and only if $p=13$, $X=239$.*

iii) *The equation $2X^2-1=p^\alpha (\alpha>0)$ has no integer solution.*

iv) *All the integer solutions of the equation $2X^2+1=p^\alpha (\alpha>0)$ are given by $\alpha=1$ or 2 and $(|X|, p^\alpha)=(11, 3^5)$ if $p\equiv 3 \pmod 8$ and none if $p\equiv 5 \pmod 8$.*

v) *We assume that here p satisfies the conjecture of Ankeny-Artin-Chowla and the analogy ([1] Chap. 8). Then all the integer solutions of the equation $|\pm p^\alpha - X^2|=2^\beta$ are, except trivial solutions $(\pm p^\alpha, |X|)=(1,3)$ and $(-1,1)$, given by $\alpha=\beta=1$; $(\pm p^\alpha, |X|)=(3^2,1), (3^2,5), (3^4,7)$, $(3,2), (-3,1)$ and $(3^3,5)$ if $p\equiv 3 \pmod 8$, $\alpha=1, \beta=0$; $\alpha=1, \beta=2$; $(\pm p^\alpha, |X|)=(5^2,3)$ and $(5^3,11)$ if $p\equiv 5 \pmod 8$.*

vi) *All the integer solutions of the equation $pX^2-Y=\pm 2^\alpha$, $Y=\pm 2^\beta$ are either $2|X, 4|Y$ or $(|X|, Y)=(1,4), (1,1), (1,2)$ and $(1,-1)$ if $p=3$, $(1,4)$ and $(1,1)$ if $p=5$ and none if $p\neq 3, 5$.*

3. For a given positive integer N, it is difficult in general to determine all the elliptic curves with the conductor N. This may be treated as problems in diophantine equations. However, when the curve is of special form, that is, when it has a rational point of order 2, we obtain the following theorems by using the above proposition.

Theorem 1. *All the elliptic curves with the coductor $N=2^m p^n$ (where $p\equiv 3$ or $5 \pmod 8$, $p\neq 3$; m and n are positive integers) that have a rational point of order 2 are effectively determined under the truth of the conjecture of Ankeny-Artin-Chowla and the analogy. Particularly if $p-2$ or $p-4$ is a square number, then the assumption on the con-*

jectures can be eliminated.

Theorem 2. *If* $p\equiv 3$ or $5 \pmod 8$ *and the class numbers of four quadratic fields* $\boldsymbol{Q}(\sqrt{\pm p}), \boldsymbol{Q}(\sqrt{\pm 2p})$ *are not divisible by then there are no elliptic curves with the conductor* $N=2p$.

Remarks. In Theorem 1, as is well known, $n=1$ or 2 only, the cases $N=2^m$ and $2^m 3^n$ have been treated by Ogg and Coghlan, $N=2^m\cdot 5$ and $2^m 11^n$ by [3]. Theorem 2 is, of course, proved independently of Theorem 1, since an elliptic curve with the conductor $N=2p$ under the condition on the class numbers would have a rational point of order 2 and we have a contradiction that such a curve would have an additive reduction at $p=2$. In Theorem 2, Ogg [2] has treated for $p=5$, 11 and as other admissible p, for example, we have here $p=37, 43, 67$, 197 etc.

Details will appear elsewhere (cf. [3]).

References

[1] L. J. Mordell: Diophantine Equations. Academic Press (1969).
[2] A. P. Ogg: Abelian curves of small conductor. J. reine und angew. Math., **226**, 205–215 (1967).
[3] T. Hadano: On the conductor of an elliptic curve. Master thesis (1972) (in Japanese) (unpublished).