# 5. On Coprime Integral Solutions of $y^2=x^3+k$

By Shoichi KIHARA
Department of Mathematics, Hyogo University of Teacher Education

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1987)

**1.** Consider an elliptic curve

$$E(k): y^2=x^3+k \tag{1}$$

with $k \in \boldsymbol{Z}$. The number of integral solutions of the diophantine equation (1), i.e. the number of points $P=(x, y)\ (x, y \in \boldsymbol{Z})$ on $E(k)$, which is well-known to be finite, will be denoted by $N(k)$, and the number of coprime solutions by $N'(k)$. The value of $\limsup_{k\to\infty} N'(k)$, which will be denoted by $c$ for simplicity's sake, has been studied by Stephens [7], Mohanty and Ramasamy [3], [5]. After $c \geqq 6$ was proved in [3], $c \geqq 8$, $c \geqq 12$ were proved in [7] and [5]. In the next paragraph § 2, we shall improve these results to $c \geqq 20$.

Integral solutions $(x_1, y_1)$, $(x_2, y_2)$, $(x_3, y_3)$ of (1) with $y_1-y_2=y_2-y_3=1$ are called *consecutive*. Mohanty [4] gave four series of such solutions for certain $k$ and asked if there are still other solutions. In § 3, we shall give an affirmative answer to this question.

We recall that the rational points on $E(k)$ form an abelian group with respect to a well-known addition (cf. [1], p. 11).

**2.** We begin with the following simple lemma.

**Lemma 1.** *Let* $k=(f^6+g^6+h^6-2f^3g^3-2g^3h^3-2h^3f^3)/4$, *then the following three points* $P_i=(x_i, y_i)\ (i=1, 2, 3)$ *are on* $E(k)$.

$$\begin{aligned} x_1&=fg & y_1&=(f^3+g^3-h^3)/2 \\ x_2&=fh & y_2&=(f^3-g^3+h^3)/2 \\ x_3&=gh & y_3&=(-f^3+g^3+h^3)/2. \end{aligned}$$

We shall omit the straightforward proof.

**Remark.** Let $f, g, h \in \boldsymbol{Z}$. Then $k \in \boldsymbol{Z}$ if one of $f, g, h$ is even and two others are odd, and $P_i$ are integral (i.e. $x_i, y_i \in \boldsymbol{Z}$, $i=1, 2, 3$).

Now let $a, b, c \in \boldsymbol{Z}$, $a \equiv d \equiv 0 \pmod 2$, $b \equiv c \equiv 1 \pmod 2$ and put $P_i=(x_i, y_i)$ $(i=1, \cdots, 6)$ where

$$\begin{aligned} x_1&=ab & y_1&=(a^3+b^3-c^3)/2 \\ x_2&=ac & y_2&=(a^3-b^3+c^3)/2 \\ x_3&=bc & y_3&=(-a^3+b^3+c^3)/2 \\ x_4&=bd & y_4&=(-d^3-b^3+c^3)/2 \\ x_5&=cd & y_5&=(-d^3+b^3-c^3)/2 \\ x_6&=bc & y_6&=(d^3-b^3-c^3)/2. \end{aligned} \tag{2}$$

Then by our Lemma 1, $P_1, P_2, P_3$ are on $E(k)$ and $P_4, P_5, P_6$ on $E(k')$ where

$$k=(a^6+b^6+c^6-2a^3b^3-2b^3c^3-2c^3a^3)/4,$$
$$k'=(b^6+c^6+d^6-2b^3c^3-2c^3d^3-2d^3b^3)/4.$$

We have $k=k'$, $P_3=P_6$ if

$$a^3+d^3=2(b^3+c^3)$$

which has a parametric solution

$$(3)\qquad \begin{aligned} a&=72t^4\\ b&=36t^3-1\\ c&=1\\ d&=-72t^4+6t \end{aligned}$$

(cf. [6], p. 6). Substituting (3) in (2), we see that the following five points $Q_i=(x_i, y_i)$ $(i=1, \cdots, 5)$ are on $E(k)$ with

$$\begin{aligned} k=k(t)=&2^{16}\cdot 3^{12}t^{24}-2^{14}3^{12}t^{21}+2^{10}\cdot 3^{11}\cdot 7t^{18}-2^9\cdot 3^9\cdot 11t^{15}\\ &+2^6\cdot 3^9\cdot 5t^{12}-2^5\cdot 3^6\cdot 11t^9+2^2\cdot 3^5\cdot 7t^6-2^2\cdot 3^3t^3+1 \end{aligned}$$

$$\begin{aligned} x_1&=2^5\cdot 3^4t^7-2^3\cdot 3^2t^4 & y_1&=2^8\cdot 3^6t^{12}+2^5\cdot 3^6t^9-2^3 3^5t^6+2\cdot 3^3t^3-1\\ x_2&=2^3\cdot 3^2t^4 & y_2&=2^8\cdot 3^6t^{12}-2^5\cdot 3^6t^9+2^3\cdot 3^5t^6-2\cdot 3^3t^3+1\\ x_3&=2^2\cdot 3^2t^3-1 & y_3&=-2^8\cdot 3^6t^{12}+2^5\cdot 3^6t^9-2^3\cdot 3^5t^6+2\cdot 3^3t^3\\ x_4&=-2^5\cdot 3^4t^7+2^5\cdot 3^2t^4-2\cdot 3t & y_4&=2^8\cdot 3^6t^{12}-2^5\cdot 3^7t^9+2^3\cdot 3^6t^6-2\cdot 3^4t^3+1\\ x_5&=-2^3\cdot 3^2t^4+2\cdot 3t & y_5&=2^8\cdot 3^6t^{12}-2^5\cdot 3^6t^9+2^3\cdot 3^5t^6-2\cdot 3^3t^3-1. \end{aligned}$$

We shall define now $Q_6=-Q_2-Q_4$, $Q_7=Q_1-Q_6$, $Q_8=-Q_2-Q_3$, $Q_9=-Q_2+Q_5$, $Q_{10}=Q_3+Q_5$. Then the twenty points $\pm Q_i$ $(i=1, \cdots, 10)$ are on $E(k)$ and all these points are mutually distinct in the following sense. Two points $(x_1(t), y_1(t))$, $(x_2(t), y_2(t))$ with $x_i(t), y_i(t)\in \boldsymbol{Z}[t]$ $(i=1,2)$ coincide if $x_1(t)=x_2(t)$, $y_1(t)=y_2(t)$ as elements of $\boldsymbol{Z}[t]$. Otherwise they are distinct. It is clear in the latter case that for a sufficiently large $t_0\in \boldsymbol{Z}$, two points $(x_1(t_0), y_1(t_0))$, $(x_2(t_0), y_2(t_0))$ are distinct. We have indeed

$$\begin{aligned} x_6&=2^5\cdot 3^4t^7-2^2\cdot 3^2t^4+2\cdot 3t & y_6&=2^8\cdot 3^6t^{12}+2^5\cdot 3^6t^9+2\cdot 3^3t^3+1\\ x_7&=m_1^2-x_1-x_6 & y_7&=m_1^3-(2x_1+x_6)m_1-y_1\\ x_8&=m_2^2-x_2-x_3 & y_8&=m_2^3-(2x_2+x_3)m_2+y_2\\ x_9&=m_3^2-x_2-x_5 & y_9&=m_3^3-(2x_2+x_5)m_3+y_2\\ x_{10}&=m_4^2-x_3-x_5 & y_{10}&=m_4^3-(2x_3+x_5)m_4-y_3 \end{aligned}$$

where

$$\begin{aligned} m_1&=2^7\cdot 3^4t^8-2^4\cdot 3^3t^5+2\cdot 3^2t^2\\ m_2&=2^6\cdot 3^4t^8+2^5\cdot 3^4t^7+2^4\cdot 3^4t^6-2^3\cdot 3^2t^4-2^3\cdot 3^2t^3+1\\ m_3&=2^5\cdot 3^4t^8-2^3\cdot 3^3t^5+2\cdot 3^2t^2\\ m_4&=2^6\cdot 3^4t^8-2^5\cdot 3^4t^7+2^4\cdot 3^4t^6-2^5\cdot 3^3t^5+2^5\cdot 3^2t^4-2^3\cdot 3^2t^3+2^2\cdot 3^2t^2-2\cdot 3t+1. \end{aligned}$$

**Lemma 2.** *If* $t\in \boldsymbol{Z}$, $t\equiv 0$, 3, 5 *or* 6 (mod 7). *Then* $x_i(t)$, $y_i(t)$ *are coprime for all* $i=1, \cdots, 10$.

*Proof.* We shall exhibit the proof only for $i=9$ as it is done similarly in all other cases. We calculate the $GCD(x_9, y_9)$ by Euclid's algorithm;

$$\begin{aligned} (x_9, y_9)&=(m_3^2-x_2-x_5,\ m_3^3-(2x_2+x_5)m_3+y_2)=(m_3^2-x_2-x_5,\ -x_2m_3+y_2)\\ &=(2^{10}\cdot 3^8t^{16}-2^9\cdot 3^7t^{13}+2^6\cdot 3^7t^{10}-2^5\cdot 3^5t^7+2^2\cdot 3^4t^4-6t,\ -2^5\cdot 3^5t^9+2^3\cdot 3^4t^6\\ &\quad -2\cdot 3^3t^3+1)=(2^5\cdot 3^3t^7-2^3\cdot 3^2t^4,\ -2^5\cdot 3^5t^9+2^3\cdot 3^4t^6-2\cdot 3^3t^3+1)\\ &=(2^5\cdot 3^3t^7-2^3\cdot 3^2t^4,\ -2\cdot 3^3t^3+1)=(-2^3\cdot 7t^4,\ -2\cdot 3^3t^3+1)\\ &=(7,\ -2\cdot 3^3t^3+1)=1, \end{aligned}$$

because $-2\cdot 3^3t^3+1\equiv 0$ (mod 7) is impossible.

As $k(t)\to\infty$ when $t\in \boldsymbol{Z}$ and $t\to\infty$, we obtain

**Theorem 1.** *If $N'(k)$ denotes the number of coprime integral solutions of the diophantine equation $y^2=x^3+k$, then we have*

$$\limsup_{k\to\infty} N'(k) \geqq 20.$$

**3.** The following lemma is proved in [4].

**Lemma 3.** *If $(x_i, y_i)$ $(i=1,2,3)$ are consecutive solutions of (1), then*

$$y_1=(x_1^3-x_2^3+1)/2$$

*and*

$$x_1^3+x_3^3=2(1+x_2^3). \tag{4}$$

*Conversely, if (4) holds for $x_1, x_2, x_3 \in \boldsymbol{Z}$, then consecutive solutions of (1) for a certain $k$ are obtained by putting*

$$y_1=(x_1^3-x_2^3+1)/2, \quad y_2=y_1-1, \quad y_3=y_2-1.$$

Mohanty gave consecutive solutions of (1) for suitable values of $k$ using the four following parametric solutions of (4) (due to Segre [6]);

(a) $x_1=1+2t-4t^2$ $x_2=-4t^2$ and $x_3=1-2t-4t^2$
(b) $x_1=1+3t^3$ $x_2=3t^2$ and $x_3=1-3t^3$
(c) $x_1=2t$ $x_2=-1$ and $x_3=-2t$
(d) $x_1=72t^4$ $x_2=36t^3-1$ and $x_3=-72t^4+6t$.

He posed a problem at the end of his paper if there are any other consecutive solutions of (1) for some values of $k$. We show that this is indeed the case. We start from the identity

$$(-2U^2+4UV-10V^2)^3+(2U^2+4UV+10V^2)^3$$
$$=2\{(-U^2+8UV+5V^2)^3+(U^2+8UV-5V^2)^2\}.$$

If $U$ and $V$ satisfy the Pell equation

$$U^2+8UV-5V^2=(U+4V)^2-21V^2=1,$$

then we have a parametric solution of (4) given by

$$x_1=-2U^2+4UV-10V^2$$
$$x_2=-U^2+8UV+5V^2$$
$$x_3=2U^2+4UV+10V^2.$$

Putting, for example, $U=3/2$ and $V=5/2$, we have

$$(-52)^3+82^3=2(1+59^3)$$

which cannot be obtained from (a), (b), (c) or (d). From this we have consecutive solutions (82, 172995), (59, 172994), (−52, 172993) of $y^2=x^3+29926718657$. This is an answer to the problem raised by Mohanty.

Lastly, we remark that we can also use the solution (d) above to generate another parametric solution of (4):

$$x_1=2^{11}\cdot 3^5t^{10}-2^3\cdot 3^3\cdot 5t^4,$$
$$x_2=2^{10}\cdot 3^5t^9-2^7\cdot 3^4t^6-2^2\cdot 3^2t^3-1,$$
$$x_3=-2^{11}\cdot 3^5t^{10}+2^9\cdot 3^4t^7-2^3\cdot 3^4t^4-6t,$$

by the theory of Pell's equation (cf. Lehmer [2]).

**Acknowledgement.** The author wishes to express his hearty thanks to Prof. S. Iyanaga and Dr. S. Nakano for their advice in preparing this paper.

## References

[1] S. Lang: Elliptic curve. Diophantine Analysis. Springer-Verlag, Berlin/Heidelberg/New York (1978).
[2] D. H. Lehmer: On the Diophantine equation $x^3+y^3+z^3=1$. J. London Math. Soc., **31**, 275–280 (1956).
[3] S. P. Mohanty: A note on Mordell's equation $y^2=x^3+k$. Proc. Amer. Math. Soc., **39**, 645–646 (1973).
[4] ——: On consecutive integer solutions for $y^2-k=x^3$. ibid., **48**, 281–285 (1975).
[5] S. P. Mohanty and A. M. S. Ramasamy: On the number of coprime integral solutions of $y^2=x^3+k$. J. Number Theory, **17**, 323–326 (1983).
[6] B. Segre: On the rational solutions of homogeneous cubic equations in four variables. Mathematical Notae, **11**, 1–68 (1951).
[7] N. M. Stephens: On the number of coprime solutions of $y^2=x^3+k$. Proc. Amer. Math. Soc., **48**, 325–327 (1975).