On the Rank of the Elliptic Curve $y^2 = x^3 + k$. II

By Shoichi KIHARA

Department of Neuropsychiatry School of Medicine, Tokusima University

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1996)

In this paper, we consider the elliptic curve

(1) $\varepsilon_k : y^2 = x^3 + k.$

In our previous paper [3], we have shown that there are infinitely many values of $k \in \boldsymbol{Q}$, for which the rank of ε_k is at least 5. We shall improve this result in this note. (See Theorem 2 below).

Let a, b, c be variables and put

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

Then there are the following 3 points on ε_k:

$$P_1(ab, (a^3 + b^3 - c^3)/2),$$
$$P_2(bc, (b^3 + c^3 - a^3)/2),$$
$$P_3(ca, (c^3 + a^3 - b^3)/2).$$

Now let t be a variable, and put

(2) $a = 3t^3 - 49, \quad b = 3t^3 + 16, \quad c = 39$

$$d = -\frac{21}{2}t^2 + \frac{196}{3t}, \quad e = \frac{24}{7}t^2 + \frac{196}{3t},$$

$$f = \frac{117}{14}t^2.$$

Then we have $E(a, b, c) = E(d, e, f)$ and

(3) $$k = k(t) = \frac{3080025}{4}t^{12} - \frac{37083501}{2}t^9 + \frac{905714433}{4}t^6 - 1884391236t^3 + 7953072400.$$

This polynomial $k(t)$ has the property

(4) $$k(t) = k\left(\frac{m}{t}\right)\frac{t^{12}}{m^6}, \text{ where } m = \frac{14}{3}$$

and our curve $\varepsilon_{k(t)}$ has the following 6 points:

$$P_1\left(9t^6 - 99t^3 - 784, \ 27t^9 - \frac{891}{2}t^6 + \frac{23913}{2}t^3 - 86436\right)$$

$$P_2\left(117t^3 + 624, \ \frac{1755}{2}t^6 - \frac{19305}{2}t^3 + 90532\right)$$

$$P_3\left(117t^3 - 1911, \ \frac{1755}{2}t^6 - \frac{19305}{2}t^3 + 31213\right)$$

$$P_4\left(-36t^4 - 462t + \frac{38416}{9t^2}, \ \frac{1701}{2}t^6 - \frac{23913}{2}t^3 + 45276 - \frac{7529536}{27t^3}\right)$$

$$P_5\left(\frac{1404}{49}t^4 + 546t, \ \frac{611091}{686}t^6 - \frac{19305}{2}t^3 + 89180\right)$$

$$P_6\left(-\frac{351}{4}t^4 + 546t, \ \frac{2457}{8}t^6 - \frac{19305}{2}t^3 + 89180\right).$$

We remark also that our $k(t) \in \boldsymbol{Q}[t]$ has no square factor in $\boldsymbol{Q}[t]$ and that two elliptic curves $\varepsilon_{k_1}, \varepsilon_{k_2}$ for $k_1, k_2 \in \boldsymbol{Q}^* = \boldsymbol{Q} - \{0\}$ are $\boldsymbol{Q}$-isomorphic if and only if $k_2/k_1 = i^6$ for some $i \in \boldsymbol{Q}^*$. (cf. [1], §10, Corollary 5.4.1). As the Diophantine equation $k_1u^6 = k(t)$ for $t, u \in \boldsymbol{Q}^*$ (with a given $k_1 \in \boldsymbol{Q}^*$) has only a finite number of solutions by Faltings' theorem, we obtain an infinite number of $\varepsilon_{k(t)}$ with $k(t) \in \boldsymbol{Q}^*$ with 6 rational points which are not $\boldsymbol{Q}$-isomorphic, in specializing $t \in \boldsymbol{Q}$ in different ways.

Now we shall show that our $\varepsilon_{k(t)}$ has another point $P_7(x_7, y_7)$, using the following elliptic curve.

(5) $C : q^2 = p^3 + n, \quad n = 9256741632090000.$

We have $n = 2^4 * 3^4 * 5^4 * 79^2 * 1831129$, where 1831129 is a prime number, which assures that C has no torsion point (cf. [1] p.323). On the other hand, C contains the point (443664,310783788), so that C has an infinite number of rational points (p, q). Put $t = -p/142200$ Then $\varepsilon_{k(t)}$ contains $P_7(x_7, y_7)$ where

$$x_7 = \frac{13p^3}{2^{10}3^45^679^3} - \frac{169q}{18960000} - \frac{235911}{800}$$

$$y_7 = \frac{13p^6}{2^{19}3^95^{11}79^6} + \frac{15821p^3}{2^{12}3^35^779^3} - \frac{6591q}{126400000} + \frac{1362504013}{16000}.$$

Theorem 1. *$P_1, \ldots, P_7$ are independent*

points on $\varepsilon_{k(t)}$.

Proof. We have noticed that $(p, q) = (443664, 310783788)$ is on C. By specializing $t \to -443664/142200 = t_0$, we obtain from $P_1, \ldots, P_7$ on $\varepsilon_{k(t)}$ 7 rational points $Q_1, \ldots, Q_7$ on $\varepsilon_{k(t_0)}$, which are shown to be independent as in [3] by using duplication formula on elliptic curves. So we see that $P_1, \ldots, P_7$ are independent. Q.E.D.

As seen in the above proof, $\varepsilon_{k(t)}$ can be taken as an elliptic curve defined over the function field $\boldsymbol{Q}(C)$ of C and as C contains an infinite number of rational points (p, q), t can be specialized also in an infinite number of ways. From Theorem 1 and the Theorem 20.3 in [1] follows now.

Theorem 2. *There are infinitely many elliptic curves of the form* $y^2 = x^3 + k$ *with rank at least* 7 *which are pairwise not* $\boldsymbol{Q}$*-isomorphic.*

References

[1] J. H. Silverman: The arithmetic of elliptic curves. Graduate Texts in Math., vol. 106, Springer-Verlag, New York (1986).

[2] S. Kihara: On coprime integral solutions of $y^2 = x^3 + k$. Proc. Japan Acad., **63A**, 13–16 (1987).

[3] S. Kihara: On the rank of the elliptic curve $y^2 = x^3 + k$. Proc. Japan Acad., **63A**, 76–78 (1987).