On the rank of the elliptic curve $y^2 = x^3 + kx$. II

By Shoichi KIHARA

Department of Neuropsychiatry, School of Medicine, Tokushima University
3-18-15, Kuramoto-cho, Tokushima 770-8503

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 2004)

Abstract: We construct an elliptic curve of the form $y^2 = x^3 + kx$ with rank at least 6 over $Q(x_1, x_2, x_3)$.

Key words: Elliptic curve; rank.

We showed an elliptic curve of the form $y^2 = x^3 + kx$ of rank ≥ 5 over $Q(t)$ in [1]. (See [2] and [3] for the case of rank ≥ 4).

In this paper we improve our previous result and show the following two theorems.

Theorem 1. *There is an elliptic curve of the form $y^2 = x^3 + kx$ of rank ≥ 6 over $Q(x_1, x_2, x_3)$.*

Theorem 2. *There are infinitely many non-isomorphic elliptic curves of the form $y^2 = x^3 + kx$ of rank ≥ 6 over Q.*

We consider the projective curve, $C : x^4 - 2ax^2y^2 + y^4 - bz^4 = 0$. By $X = (a^2 - 1)x^2/z^2$, $Y = (a^2 - 1)x(y^2 - ax^2)/z^3$ and $k = (a^2 - 1)b$. We have the elliptic curve $E : Y^2 = X^3 + kX$. By the permutation of x and y, we have 2 points on the elliptic curve E. We assume that $k \neq 0$, then C is a non-singular curve of genus 3. The Jacobian $J(C)$ of the curve C splits completely and is isogenious to $E \times E \times F$, where the elliptic curve F is given by the following equation.

$$F : Y^2 = X(X + 2ab + 2b)(X + 2ab - 2b),$$

$$X = b^2z^4/(x^2y^2) \quad \text{and} \quad Y = b^2(x^4 - y^4)z^2/(x^3y^3).$$

The above fact and that C has many automorphisms give us high rank elliptic curves and interesting Diophantine relations.

Let x, y, u and w be variables, then we can solve for a and b from

$$x^4 - 2ax^2y^2 + y^4 - b = 0 \quad \text{and} \quad u^4 - 2au^2w^2 + w^4 - b = 0.$$

We have 4 points on the corresponding elliptic curve E over $Q(x, y, u, w)$. These points are independent. We show this by the following example.

Let x_i $(1 \leq i \leq 6)$ be variables, we solve for a and b from

$$x_i^4 - 2ax_i^2x_{i+1}^2 + x_{i+1}^4 - b = 0 \quad (i = 1, 3).$$

Then we have

$$a = (x_1^4 + x_2^4 - x_3^4 - x_4^4)/\left(2(x_1^2x_2^2 - x_3^2x_4^2)\right)$$

and

$$b = (x_2^2x_3^2 - x_1^2x_4^2)(x_1^2x_3^2 - x_2^2x_4^2)/(x_1^2x_2^2 - x_3^2x_4^2).$$

We construct another point on the affine curve

$$H : x^4 - 2ax^2y^2 + y^4 - b = 0.$$

Let us consider the case that the point (x_3, x_5) is on H. Then we have

(1)
$$x_5^2 = (-x_3^6 + x_1^4x_3^2 - x_1^2x_2^2x_4^2 + x_2^4x_3^2)/(x_1^2x_2^2 - x_3^2x_4^2).$$

We see that (1) has automorphisms $(x_4, x_5) \to (x_5, x_4)$ and $(x_1, x_2) \to (x_2, x_1)$.

Now we fix x_1, x_2 and x_3 and consider (1) as a curve of x_4 and x_5. Then we see that the point $(x_4, x_5) = P(x_1x_3/x_2, x_2x_3/x_1)$ is on (1). We consider the birational transformation

$$x_4 = x_1x_2(u - 1)/\left(x_3(u + 1)\right), \quad x_5 = w/(2ux_1x_2x_3).$$

The inverse is

$$u = (x_1x_2 + x_3x_4)/(x_1x_2 - x_3x_4),$$
$$w = 2x_1x_2x_3x_5(x_1x_2 + x_3x_4)/(x_1x_2 - x_3x_4).$$

Then (1) becomes

(2)
$$w^2 = u\big(-(x_1^4 - x_3^4)(x_2^4 - x_3^4)(u^2 + 1) + 2(x_1^4x_2^4 + x_1^4x_3^4 + x_2^4x_3^4 - x_3^8)u\big).$$

The point P corresponds to the point

$$Q\left((x_2^2 + x_3^2)/(x_2^2 - x_3^2),\ 2x_2^2x_3^2(x_2^2 + x_3^2)/(x_2^2 - x_3^2)\right)$$

on the elliptic curve (2). We see that $2Q = \big(-(x_1^4 - x_3^4)/(x_2^4 - x_3^4),\ -(x_1^4 + x_2^4)(x_1^4 - x_3^4)/(x_2^4 - x_3^4)\big)$.

2000 Mathematics Subject Classification. Primary 11G05.

This point corresponds to

$$x_4 = x_1 x_2 (2x_3^4 - x_1^4 - x_2^4) / \left(x_3 (x_1^4 - x_2^4) \right) \quad \text{and}$$
$$x_5 = (x_1^4 + x_2^4)/(2x_1 x_2 x_3).$$

We take this setting in the following. Next we consider the transformation $\sigma : x_3 \to x_5$ a and b do not change by σ but the point (x_3, x_4) goes to the point (x_5, x_6) where

$$x_6 = \left(x_1^{12} - 8x_1^4 x_2^4 x_3^4 + 3x_1^8 x_2^4 + 3x_1^4 x_2^8 + x_2^{12} \right) / \left(4x_1^2 x_2^2 x_3^3 (x_1^4 - x_2^4) \right).$$

In this way we have 8 points (x_1, x_2), (x_2, x_1), (x_3, x_4), (x_4, x_3), (x_3, x_5), (x_5, x_3), (x_5, x_6) and (x_6, x_5) on the affine curve H, and 8 points on the corresponding elliptic curve E. The six points on E coming from (x_1, x_2), (x_2, x_1), (x_3, x_4), (x_4, x_3), (x_5, x_3) and (x_6, x_5) are independent. In fact, let $x_1 = 1$, $x_2 = 2$, $x_3 = 3$ then the determinant of the Grammian height-pairing matrix of these 6 points is 8262681.77 since this is not 0 these points are independent.

So we have Theorem 1. The proof of Theorem 2 is similar as in [1].

We note that by the change of variables $x = u + w$ and $y = u - w$ and by multiplying the denominators we have the Diophantine relations

$$u_i^4 - 2cu_i^2 w_i^2 + w_i^4 = u_j^4 - 2cu_j^2 w_j^2 + w_j^4 \quad (1 \leq i,\, j \leq 4)$$

where $c = (a+3)/(a-1)$ and u_i w_i $(1 \leq i \leq 4)$ are all different polynomials of x_1, x_2 and x_3.

References

[1] Kihara, S.: On the rank of the elliptic curve $y^2 = x^3 + kx$. Proc. Japan Acad., **74A**, 115–116 (1998).

[2] Mestre, J.-F.: Rang de courbes elliptiques d'invariant donné. C. R. Acad. Sci. Paris Sér. I Math., **314**, 919–922 (1992).

[3] Nagao, K.: On the rank of elliptic curve $y^2 = x^3 - kx$. Kobe J. Math., **11**, 205–210 (1994).