On the rank of elliptic curves with three rational points of order 2. III

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., March 12, 2004)

Abstract: We construct an elliptic curve of rank at least 6 over $Q(t)$ with three non-trivial rational points of order 2.

Key words: Elliptic curve; rank.

In this paper we show the following two theorems.

Theorem 1. *There is an elliptic curve over $Q(t)$ of rank ≥ 6, which have 3 non-trivial rational points of order 2.*

Theorem 2. *There are infinitely many elliptic curves over Q of rank ≥ 6, which have 3 non-trivial rational points of order 2.*

We follow the Kulesz's idea [4] (see also [1, 2] and [3]), let

$$x^4 + y^4 + z^4 = a(x^2y^2 + y^2z^2 + z^2x^2). \tag{1}$$

Then by $X = (2y^2 - ax^2 - az^2)^2/(xz)^2$ and $Y = (a^2-4)(z^4 - x^4)(2y^2 - ax^2 - az^2)/(xz)^3$. We have

$$Y^2 = X(X - 4a - 8)(X - 4a^2 - 4a + 8). \tag{2}$$

By the permutations of x, y, and z we have 3 points on (2). We solve the Diophantine equations

$$p^2 = ax^2 + by^2 + cz^2, \tag{3}$$

$$q^2 = bx^2 + cy^2 + az^2, \tag{4}$$

$$r^2 = cx^2 + ay^2 + bz^2, \tag{5}$$

where

$$a = (2s+2)/(s^2+3), \quad b = (s^2-1)/(s^2+3) \quad \text{and} \quad c = (-2s+2)/(s^2+3).$$

Because (3), (4) and (5) imply

$$x^4 + y^4 + z^4 = p^4 + q^4 + r^4$$

and

$$x^2y^2 + y^2z^2 + z^2x^2 = p^2q^2 + q^2r^2 + r^2p^2.$$

Now let

$$x = 1 \quad y - 1 + u \quad z = 1 + tu \quad \text{and} \quad p = 1 + wu$$

then from (3) we can solve for u. From (4) we have $q^2 = H(s,t,w)/G(s,t,w)^2$ where $H \in Z[s,t,w]$ and H is a degree 4 polynomial of w and the coefficient of w^4 is $(s^2+3)^2$. By the well known classical method we have the unique expression

$$(s^2+3)^2 H(s,t,w) = K(s,t,w)^2 + L(s,t)w + M(s,t),$$

where $K \in Z[s,t,w]$ and K is a degree 2 polynomial of w and L, $M \in Z[s,t]$. We see that the polynomial $s(t^2-1) - t^2 + 4t - 1$ is a common-factor of L and M.

So we take $s = (t^2 - 4t + 1)/(t^2 - 1)$, to make H a square. From (5) we have $r^2 = J(t,w)/I(t,w)^2$ where J is again a degree 4 polynomial of w and the coefficient of w^4 is a square. It is easy to see that there are infinitely many w's that make J squares. We take $w = -(2t-1)(t^3+6t-2)/(3(t^3-6t^2+3t+1))$. By multiplying the denominators we have

$$\begin{aligned}
x &= (t+1)(2t^8 - 14t^7 + 146t^6 - 473t^5 + 674t^4 \\
&\qquad - 473t^3 + 146t^2 - 14t + 2), \\
y &= (t-2)(2t^8 - 2t^7 + 104t^6 - 221t^5 + 149t^4 \\
&\qquad - 35t^3 - 7t^2 + 16t - 4), \\
z &= (2t-1)(4t^8 - 16t^7 + 7t^6 + 35t^5 - 149t^4 \\
&\qquad + 221t^3 - 104t^2 + 2t - 2), \\
p &= 2t^9 + 18t^8 - 144t^7 + 411t^6 - 477t^5 + 225t^4 \\
&\qquad - 75t^3 + 72t^2 - 36t + 2, \\
q &= (t-2)^3(t+1)^3(2t-1)^3, \\
r &= 2t^9 - 36t^8 + 72t^7 - 75t^6 + 225t^5 - 477t^4 \\
&\qquad + 411t^3 - 144t^2 + 18t + 2.
\end{aligned}$$

Now let $a = (x^4 + y^4 + z^4)/(x^2y^2 + y^2z^2 + z^2x^2)$ then we have 6 points on (2). These are independent points. For let $t = 3$ then we have

$$a = 27394784328959906/9864480201714353.$$

2000 Mathematics Subject Classification. Primary 11G05.

The determinant of the Grammian height-pairing matrix of these 6 points is 5197720554.13. Since this is not 0 these points are independent. So we have Theorem 1 and Theorem 2.

References

[1] Dujella, A.: Diophantine triples and construction of high-rank elliptic curves over Q with three non-trivial 2-torsion points. Rocky Mountain J. Math., **30**, 157–164 (2000).

[2] Kihara, S.: On the rank of elliptic curves with three rational points of order 2. Proc. Japan Acad., **73A**, 77–78 (1997).

[3] Kihara, S.: On the rank of elliptic curves with three rational points of order 2. II. Proc. Japan Acad., **73A**, 151 (1997).

[4] Kulesz, L.: Courbes elliptiques de rang ≥ 5 sur $Q(t)$ avec un groupe de torsion isomorphe á $Z/2Z \times Z/2Z$. C. R. Acad. Sci. Paris Sér. I Math., **329**, 503–506 (1999).