On the rank of elliptic curves with a reational point of order 3

By Shoichi KIHARA

Department of Neuropsychiatry, School of Medicine, Tokushima University, 2-50-1, Kuramoto, Tokushima 770-8503

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 2000)

Abstract: We construct an elliptic curve over $\mathbf{Q}(t)$ of rank at least 6 with a rational point of order 3.

Key words: Elliptic curve; rank ; point of order 3.

In this paper we consider the rank of elliptic curves with a rational point of order 3 over $\mathbf{Q}$.

The elliptic curves of the form

$$\varepsilon \qquad y^2 = ax^3 + (bx - c)^2$$

has a rational point $\mathrm{P} = (0, c)$ of order 3.

Top showed this type of curves with rank 3 in [3].

Also Campbell showed this type of curves with rank at least 3 over $\mathbf{Q}(t)$ in [1].

We improve these results, and prove the

Theorem. *There are infinitely many elliptic curves over* $\mathbf{Q}$ *of rank at least* 6 *with a non-trivial rational point of order* 3.

We shall construct an elliptic curve ε_0 over $\mathbf{Q}(t)$ with 6 points $\mathrm{P}_1, \ldots, \mathrm{P}_6$.

Let $f(x) = x^3/(x-1)^2$, $g(t) = (t^2+3)/4$ and $h = f \circ g$, then the equation $f(x) = h(t)$ have the solutions,

$$x = \frac{t^2+3}{(t+1)^2}, \frac{t^2+3}{(t-1)^2} \quad \text{and} \quad \frac{t^2+3}{4}.$$

Next let $a_1 = 0$, $a_2 = h(2)$, $a_3 = h(4)$ and $a_4 = h(t)$.

We consider the polynomial $F(X) = \prod_{i=1}^{4}(X - a_i) \in K[X]$ of the 4th degree where $K = \mathbf{Q}(t)$. There exist uniquely $G(X)$, $r(X) \in K[X]$ of degree 2, 1, respectively such that $F(X) = (G(X))^2 - r(X)$.

In this way we have the following,

$$r(X) = \frac{A(t)X + B(t)^2}{2^{14}3^4 5^8 (t^2-1)^8}$$

where

$$\begin{aligned} A(t) = {} & 800 * (225t^6 - 13409t^4 + 36943t^2 - 9359) \\ & *(75t^6 + 103t^4 + 3169t^2 + 1453) \\ & *(75t^6 + 1247t^4 + 881t^2 + 2597) \\ & *(t+1)^2(t-1)^2. \\ B(t) = {} & 5625t^{12} - 670450t^{10} - 4315341t^8 \\ & -5988236t^6 + 22688079t^4 + 27728414t^2 \\ & -16408091. \end{aligned}$$

Let $s(x) = (A(t) * f(x) + B(t)^2) * (x-1)^2 = A(t)x^3 + (B(t)x - B(t))^2$ and at last we have the following elliptic curve

$$\varepsilon_0 \qquad y^2 = A(t)x^3 + (B(t)x - B(t))^2.$$

There are following 6 points on this curve

$$\begin{aligned} \mathrm{P}_1 = {} & \left(\frac{7}{9}, \frac{2}{9} * \left(5625t^{12} + 187050t^{10} - \frac{14558123}{3}t^8 \right.\right. \\ & + \frac{86238692}{3}t^6 - 31986121t^4 + \frac{92206142}{3}t^2 \\ & \left.\left. + \frac{613627}{3}\right)\right). \\ \mathrm{P}_2 = {} & \left(7, 6 * \left(5625t^{12} + 187050t^{10} - \frac{14558123}{3}t^8 \right.\right. \\ & + \frac{86238692}{3}t^6 - 31986121t^4 + \frac{92206142}{3}t^2 \\ & \left.\left. + \frac{613627}{3}\right)\right). \\ \mathrm{P}_3 = {} & \left(\frac{19}{4}, \frac{15}{4} * \left(5625t^{12} + 15450t^{10} + \frac{17151269}{3}t^8 \right.\right. \\ & - \frac{60161276}{3}t^6 + 41728663t^4 - \frac{35146226}{3}t^2 \\ & \left.\left. + \frac{22027019}{3}\right)\right). \end{aligned}$$

1991 Mathematics Subject Classification. Primary 11G05.

$$\mathrm{P}_4 = \Big(\frac{19}{9}, \frac{10}{9} * \Big(5625t^{12} + 15450t^{10} + \frac{17151269}{3}t^8 - \frac{60161276}{3}t^6 + 41728663t^4 - \frac{35146226}{3}t^2 + \frac{22027019}{3}\Big)\Big).$$

$$\mathrm{P}_5 = \Big(\frac{t^2+3}{(t-1)^2}, \frac{2(t+1)}{(t-1)^2} * (16875t^{12} - 467950t^{10} - 3450959t^8 + 2704236t^6 + 32430621t^4 + 46748386t^2 - 8861209)\Big).$$

$$\mathrm{P}_6 = \Big(\frac{t^2+3}{(t+1)^2}, \frac{2(t-1)}{(t+1)^2} * (16875t^{12} - 467950t^{10} - 3450959t^8 + 2704236t^6 + 32430621t^4 + 46748386t^2 - 8861209)\Big).$$

Now we prove

Proposition. $\mathbf{Q}(t)$ − rank *of* ε_0 *is at least* 6

Proof. We specialize $t = 11$. Then we have 6 rational points $\mathrm{R}_1, \ldots, \mathrm{R}_6$ obtained from $\mathrm{P}_1, \ldots, \mathrm{P}_6$. By using calculation system PARI, we see that the determinant of the matrix $(\langle R_i, R_j\rangle)$ $(1 \leq i, j \leq 6)$ associated to the canonical height is 521684.98. Since this determinant is non-zero, we see $\mathrm{P}_1, \ldots, \mathrm{P}_6$ are independent. □

Now this Proposition and Theorem 20.3 in [2] establish our Theorem.

References

[1] Campbell, G.: Finding elliptic curves and infinite families of elliptic curves defined over **Q** of large rank (1999) (Ph. D. Thesis, Rutgers University).

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

[3] Top, J.: Descent by 3-isogeny and 3-rank of quadratic fields. Advances in Number Theory. Oxford Science Publications, Oxford Univ. Press, Oxford, pp. 303–317 (1993).