On the rank of the elliptic curves with a rational point of order 4

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 rank at least 4 over $Q(t)$ with a rational point of order 4. We also show an infinite family of elliptic curves of rank at least 5 over Q with a rational point of order 4, which is parametrized by the rational points of an elliptic curve of rank at least 1.

Key words: Elliptic curve; rank.

In [2] Kulesz showed an elliptic curve of rank ≥ 3 with a rational point of order 4 over $Q(x_1, x_2, x_3)$. We improve his result and show the following two theorems.

Theorem 1. *There is an elliptic curve of rank ≥ 4 with a rational point of order 4 over $Q(t)$.*

Theorem 2. *There are infinitely many elliptic curves of rank ≥ 5 with a rational point of order 4 over Q.*

We consider the projective curve, $C : (x^2 - y^2)^2 + 2a(z^2+y^2)z^2 + bz^4 = 0$. By $X = (a^2-b)y^2/x^2$ and $Y = (a^2 - b)y(bz^2 + ax^2 + ay^2)/x^3$, we have the elliptic curve $E : Y^2 = X(X^2 + (2a^2 + 2b)X + (a^2 - b)^2)$. The point $P(a^2 - b, 2a(a^2 - b))$ is on E and $2P = (0, 0)$ and $4P = O$.

Now we consider the affine curve

$$H : (x^2 - y^2)^2 + 2a(x^2 + y^2) + b = 0.$$

We assume that the points $P_1(r, s)$ and $P_2(r, u)$ are on H, then we have $a = (2r^2 - s^2 - u^2)/2$ and $b = s^2u^2 + s^2r^2 + u^2r^2 - 3r^4$. We further assume that the points $P_3(s, q)$ and $P_4(u, p)$ are on H, then we have

$$p^2 = 3s^2 + u^2 - 3r^2, \tag{1}$$

$$q^2 = s^2 + 3u^2 - 3r^2. \tag{2}$$

We solve these Diophantine equations by the similar method in [1].

Let $r = 1$, $s = 1 + e$, $u = 1 + et$ and $p = 1 + ce$, then from (1) we have $e = 2(-t+c-3)/(t^2-c^2+3)$. From (2) we have $q^2 = J(c, t)/(t^2 - c^2 + 3)^2$, where $J(c, t) = G(c, t)^2 - 48(c - 6)(c - 2)(c^2 - 10c + 15 - 5t + 2ct)$, and $G(c, t) = t^2 - 6ct + 16t - 7c^2 + 62c - 93$. So we take $c = 6$ to make $J(c, t)$ a square. By multiplying the denominators, we have

$$\begin{aligned} r &= t^2 - 33, \\ s &= t^2 - 2t - 27, \\ u &= t^2 - 6t + 33, \\ p &= t^2 - 12t + 3, \\ q &= t^2 - 20t + 27. \end{aligned}$$

Now we have 4 $Q(t)$-rational points on the affine curve H, and 4 $Q(t)$-rational points on the corresponding elliptic curve E.

Let $E(Q(t))$ be the Mordell-Weil group of E. T be the torsion subgroup of $E(Q(t))$, then it is easy to see that $T \simeq Z/4Z$.

These 4 points are independent. We show this by the following example. Now we further assume that the point $P_5(p, w)$ is on H. Then we have

$$w^2 = t^4 - 60t^3 + 534t^2 - 540t - 1071. \tag{3}$$

We consider the birational transformation σ,

$$\begin{aligned} t &= (n + 30m - 2880)/(2(m - 480)), \\ w &= (n^2 + 23040n - 2m^3 + 1248m^2 + 184320m \\ &\quad - 22118400)/(4(m - 480)^2). \end{aligned}$$

The inverse is

$$\begin{aligned} m &= 2(t^2 - 30t - w + 57), \\ n &= 4(t^3 - 45t^2 - wt + 267t + 15w - 135). \end{aligned}$$

Then (3) becomes

$$n^2 = m(m^2 + 192m - 46080). \tag{4}$$

The point $(m, n) = (144, -576)$ is on (4), and it is easy to see that this point is of infinite order, so the elliptic curve (4) has positive rank. Now we parametrize the point (t, w) on (3) and other 5 points on H by the rational points on (4) via the birational transformation σ.

2000 Mathematics Subject Classification. Primary 11G05.

Then we have 5 rational points on H and 5 rational points on the corresponding elliptic curve E. These 5 points are independent. For let $(m, n) = (144, -576)$ then we have $(t, w) = (-9/7, 1236/49)$. The determinant of the Grammian height-pairing matrix of these 5 points is 112140.39 since this is not 0 these points are independent.

So we have Theorem 1 and Theorem 2.

Acknowledgements. The author wishes to express his hearty thanks to the referees for the valuable suggestions on this paper.

References

[1] Kihara, S.: On the rank of elliptic curves with three rational points of order 2. III. Proc. Japan Acad., **80A**, 13–14 (2004).

[2] Kulesz, L.: Families of elliptic curves of high rank with nontrivial torsion group over Q. Acta Arith., **108**, 339–356 (2003).