On the rank of the elliptic curves with a rational point of order 4. 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., Oct. 12, 2004)

Abstract: We construct an elliptic curve with non-constant j-invariant of rank ≥ 5 with a rational point of order 4 over $\mathcal{Q}(t)$.

Key words: Elliptic curve; rank.

In [1] we constructed an elliptic curve of rank ≥ 4 with a rational point of order 4 over $\mathcal{Q}(t)$.

We improve our previous result and show the following theorem.

Theorem 1. *There is an elliptic curve with non-constant j-invariant of rank ≥ 5 with a rational point of order 4 over $\mathcal{Q}(t)$.*

As in [1] we consider the projective curve,

$$C : (x^2 - y^2)^2 + 2a(x^2 + y^2)z^2 + bz^4 = 0.$$

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 $4P = O$. We also 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 $P_3(s, p)$, $P_4(u, q)$ and $P_5(p, m)$ are on H, then we have

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

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

$$m^2 = 6s^2 + 3u^2 - 8r^2. \tag{3}$$

We solve these Diophantine equations as follows:

Let $s = 1$, $u = t + e$, $r = (t + 1)/2 + ew$ and $p = (t - 3)/2 + ce$, then from (1) we have $e = (3c + 2t - ct - 3w - 3tw)/(-1 + c^2 + 3w^2)$. From (2) we have

$$q^2 = I(c, t, w)/(4(-1 + c^2 + 3w^2)^2),$$

where $I(c, t, w) \in Z[c, t, w]$ and $I(c, t, w)$ is a degree 4 polynomial of w and the coefficient of w^4 is $9(3t - 1)^2$. Then we have the unique expression

$$(3t - 1)^6 I(c, t, w) = G(c, t, w)^2 + L(c, t, w)$$

where $G(c, t, w), L(c, t, w) \in Z[c, t, w]$ and $G(c, t, w)$ is a degree 2 polynomial of w, and $L(c, t, w)$ is a degree 1 polynomial of w.

We see that the polynomial $2(t^2-1)c-t^2+6t-1$ is a factor of $L(c, t, w)$. So we take $c = (t^2 - 6t + 1)/(2(t^2-1))$ to make $I(c, t, w)$ a square. From (3) we have $m^2 = J(t, w)/H(t, w)^2$ where $J(t, w), H(t, w) \in Z[t, w]$ and $J(t, w)$ is a degrre 4 polynomial of w and the coefficient of w^4 is a square. By the same method used to solve (2), we can make $J(t, w)$ a square. We have $w = A(t)/B(t)$, where

$$\begin{aligned} A(t) &= 3t^9 - 20t^8 + t^7 + 202t^6 - 627t^5 + 1248t^4 \\ &\quad - 1369t^3 + 946t^2 - 216t + 24. \\ B(t) &= 2(t - 2)^2(t - 1)(t + 1)^2(3t^4 - 17t^3 + 27t^2 \\ &\quad - 43t + 6). \end{aligned}$$

By multiplying the denominators, we have

$$\begin{aligned} r = &-(t^2 - 1)(12t^{11} - 219t^{10} + 1699t^9 - 7248t^8 \\ &+ 21004t^7 - 45434t^6 + 72862t^5 - 90128t^4 \\ &+ 77496t^3 - 46283t^2 + 10095t - 768). \\ s = &\ 3t^{13} - 128t^{12} + 1185t^{11} - 5018t^{10} + 13628t^9 \\ &- 27704t^8 + 44162t^7 - 63956t^6 + 84827t^5 \\ &- 100976t^4 + 92061t^3 - 52802t^2 + 10662t \\ &- 552. \\ u = &-21t^{13} + 330t^{12} + 2117t^{11} + 8532t^{10} \\ &- 24566t^9 + 51764t^8 - 83474t^7 + 99728t^6 \\ &- 92921t^5 + 63962t^4 - 39209t^3 + 21228t^2 \\ &- 8828t + 984. \end{aligned}$$

2000 Mathematics Subject Classification. Primary 11G05.

$$\begin{aligned}p = &-6t^{13} + 33t^{12} - 155t^{11} + 1911t^{10} - 11855t^9\\ &+ 43046t^8 - 106778t^7 + 187562t^6 - 236720t^5\\ &+ 215945t^4 - 128363t^3 + 53439t^2 - 9179t\\ &+ 336.\end{aligned}$$

$$\begin{aligned}q = &\ 30t^{13} - 443t^{12} + 2589t^{11} - 9725t^{10} + 28685t^9\\ &- 67490t^8 + 130502t^7 - 199886t^6 + 238460t^5\\ &- 201395t^4 + 109245t^3 - 15317t^2 - 7239t\\ &+ 1200.\end{aligned}$$

$$\begin{aligned}m = &-15t^{13} + 138t^{12} - 259t^{11} - 2160t^{10} + 17250t^9\\ &- 66700t^8 + 165618t^7 - 291384t^6 + 370045t^5\\ &- 325350t^4 + 195345t^3 - 54248t^2 + 5424t\\ &+ 120.\end{aligned}$$

Now we have 5 $\mathcal{Q}(t)$-rational points on the affine curve H, and 5 $\mathcal{Q}(t)$-rational points on the corresponding elliptic curve E. It is easy to see that the j-invariant $j(t)$ of E is not a constant. The 5 points on E are independent. For let $t = 4$ then the determinant of the Grammian height-pairing matrix of these 5 points is 23494465.07, since this is not 0 these points are independent.

So we have Theorem 1.

Since the j-invariant $j(t)$ of E is not a constant, we have infinitely many elliptic curve of rank ≥ 5 with a rational point of order 4 over Q by specializing t. So we again have Theorem 2 in [1] as a corollary of above Theorem 1. (See the Specialization Theorem of Silverman [3], p. 368).

We note that from (1), (2) and (3), we have the following equations.

$$5p^4 + q^4 - m^4 = 10s^4 + 5u^4 - 10r^4 \quad \text{and}$$
$$16p^2q^2 - 5q^2m^2 - m^2p^2 = 40s^2u^2 - 10u^2r^2 - 20r^2s^2.$$

Appendix. In this place we show the following little but beautiful claim which has played a center role in [2].

Claim 1. *Let x, y, z, p, q, r be rational numbers, then the following two conditions are equivalent*

(i) $x^4 + y^4 + z^4 = p^4 + q^4 + r^4$ *and* $x^2y^2 + y^2z^2 + z^2x^2 = p^2q^2 + q^2r^2 + r^2p^2$.

(ii) *There is a rational number s such that* $p^2 = ax^2 + by^2 + cz^2$, $q^2 = bx^2 + cy^2 + az^2$ *and* $r^2 = cx^2 + ay^2 + bz^2$, *where* $a = (2s + 2)/(s^2 + 3)$, $b = (s^2 - 1)/(s^2 + 3)$ *and* $c = (-2s + 2)/(s^2 + 3)$.

Proof. (ii) $\Rightarrow$ (i) trivial. (i) $\Rightarrow$ (ii) we avoid the trivial case $\{x^2, y^2, z^2\} = \{p^2, q^2, r^2\}$. In this case we take a suitable permutation and set $s = 1$. Now from (i) we have $(x^2 + y^2 + z^2)^2 = (p^2 + q^2 + r^2)^2$, so we have $x^2 + y^2 + z^2 = p^2 + q^2 + r^2$. There are non-zero rational numbers h and u such that $p^2 = z^2 + h$, $q^2 = x^2 + hu$ and $r^2 = y^2 - h - hu$. (note that we avoided the trivial case). From $x^4 + y^4 + z^4 = p^4 + q^4 + r^4$ we have $h = (-ux^2 + (1 + u)y^2 - z^2)/(I + u + u^2)$. So we have $s = -(u + 2)/u$. $\square$

References

[1] Kihara, S.: On the rank of elliptic curves with a rational points of order 4. Proc. Japan Acad. **80A**., 26–27 (2004).

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

[3] Silverman, J. H.: The Arithmetic of Elliptic Curves. Grad. Texts in Math., 106. Springer, New York (1986).