# On the rank of the elliptic curves with a rational point of order 6

By Shoichi Kihara

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

(Communicated by Shigefumi Mori, m.j.a., Sept. 12, 2006)

**Abstract:** We construct an infinite family of elliptic curves of rank at least 4 over $Q$ with a rational point of order 6, which is parametrized by the rational points of an elliptic curve of rank at least 1.

**Key words:** Elliptic curve; rank.

Lecacheux showed an elliptic curve of rank $\geq 3$ with a rational point of order 6 over $Q(a)$ (see [Lecacheux]). We improve her result and show the following theorem.

**Theorem 1.** *There are infinitely many elliptic curves of rank $\geq 4$ with a rational point of order 6 over $Q$.*

We consider the projective curve, $C$: $(x^2-y^2)^2+(2ax^2+2by^2)z^2+cz^4=0$. By $X=x^2/y^2$ and $Y=x(cz^2+ax^2+by^2)/y^3$, we have the elliptic curve $E$: $Y^2=X((a^2-c)X^2+(2ab+2c)X+(b^2-c))$. The point $P(1,a+b)$ is on $E$ and $2P=((a-b)^2/(4(a^2-c)), -(a-b)((a+b)^2-4c)/(8(a^2-c)))$.

We consider the case $3P=O$ that is $2P=-P$. then we have $c=(3a-b)(a+b)/4$. In this case the point $P_0=P+(0,0)=((-3a-5b)/(a-b),(a+b)(3a+5b)/(a-b))$ is a point of order 6. We set $a=(u+w)/2$ and $b=(-u+3w)/2$ then we have $c=uw$. Now we consider the affine curve

$$H:\ (x^2-y^2)^2+(2ax^2+2by^2)+c=0.$$

We assume that the point $P_1(e,f)$ is on $H$, then we have

$$w=(-(e^2-f^2)^2-(e^2-f^2)u)/(e^2+3f^2+u).$$

We further assume that the points $P_2(g,f)$ and $P_3(e,h)$ are on $H$, then we have

$$\begin{aligned} g^2 &= -(3e^2f^2-7f^4+e^2u+2f^2u \\ &\quad +u^2)/(e^2+3f^2+u), \\ h^2 &= (e^2+u)(5e^2-f^2+u)/(e^2+3f^2+u) \end{aligned}$$

we have $h^2-9g^2=(e^2+7f^2+2u)(5e^2-9f^2+5u)/(e^2+3f^2+u)$. So we set $u=-(e^2+7f^2)/2$, then we have $g^2=(e^2-7f^2)/2$ and $h^2=9(e^2-7f^2)/2$. We have the following solution;

$$\begin{aligned} e &= 3(2t^2+7), \\ f &= 2t^2-4t-7, \\ g &= 2t^2+14t-7, \\ h &= 3(2t^2+14t-7). \end{aligned}$$

Now we have 3 $Q(t)$-rational points on the affine curve $H$, and 3 $Q(t)$-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 $T\simeq Z/6Z$. Now we further assume that the point $P_4(m,h)$ is on $H$. Then we have

$$(1)\quad m^2=68t^4+1096t^3+3216t^2-3836t+833.$$

We consider the birational transformation $\sigma$,

$$\begin{aligned} t &= -(1096+13r-391s)/(2(274+13r \\ &\quad +116s)), \\ m &= 9(1951976+156180r+2197r^2 \\ &\quad +1004484s-299091s^2-4394s^3)/(2(274 \\ &\quad +13r+116s)^2). \end{aligned}$$

The inverse is

$$\begin{aligned} s &= (381-822t-126t^2-13m)/(1+2t)^2, \\ r &= (11375-31902t+10374t^2+2080t^3 \\ &\quad -391m+232mt)/(1+2t)^3. \end{aligned}$$

Then (1) becomes

$$(2)\qquad r^2=s(s+4)(s+137).$$

The point $(s,r)=(338,7410)$ is on (2), and it is easy to see that this point has non-zero canonical height. Hence it is not a torsion point by [Silverman, p.229, Theorem 9.3 (d)], so the elliptic curve (2) has positive rank. Now we parametrize $(t, m)$ on (1) and other 4 points on $H$ by the rational points on (2) via the birational transformation $\sigma$.

Then we have 4 rational points on $H$ and 4 rational points on the corresponding elliptic curve $E$. These 4 points are independent. For let $(s, r) = (338, 7410)$ then we have $(t, m) = (457/3574, -127317411/6386738)$. The determinant of the Grammian height-pairing matrix of these 4 points is 2269752.0316903, since this is not 0 these points are independent, which can be directly shown from [Silverman, p.229, Theorem 9.3(c),(d)]. So we have Theorem 1.

In order to check

1) The j-invariant of $E/Q(t)$ is not constant,
2) The canonical height of (338,7410) of $r^2 = s(s+4)(s+137)$ is about 1.8013214818,
3) The determinant of Grammian height-pairing matrix is 2269752.0316903,

we use the computer algebra system PARI/GP [Cohen], which has many useful functions of elliptic curve.

In the checks of 2) and 3), we compute these values with 28 digits-precision and 100 degits-precision, and obtains the same values up to the error terms. So, it is confirmed that these values are non-zero. Similarly we can compute that the j-invariant of this curve is written in the form $j(t) = f(t)/g(t)$, where $f(t)$ and $g(t)$ are co-prime polynomials with deg $f(t) = 48$, deg $g(t) = 45$. This settles 1).

## References

[Cohen] H. Cohen, PARI/GP. http://pari.math.u-bordeaux.fr/.

[Cremona] J. E. Cremona, mwrank and related programs for elliptic curves over Q. http://www.maths.nottingham.ac.uk/personal/jec/mwrank/.

[Lecacheux] O. Lecacheux: Rang de courbes elliptiques avec groupe de torsion non trivial, J. Théor. Nombers Bordeaux **15** (2003), 231–247.

[Mazur] B. Mazur, Rational isogenies of prime degree, Invent. Math. **44** (1978), 129–162.

[Silverman] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.