Kumamoto J. Math.
Vol. 15, 1-5 March (2002)

On the rank of elliptic curves $y^2=x^3-pqx$

Masayuki Maenishi

(Received September 10, 2001
Revised December 12, 2001)

Abstract

Let $C(\boldsymbol{Q})$ be the set of rational points on the elliptic curve C of the form $y^2=x^3-pqx$. The rank of $C(\boldsymbol{Q})$ as a $\boldsymbol{Z}$-module is less than or equal to 4 provided that p and q are distinct odd primes. We will construct some elliptic curves of the form with rank exactly 4.

§ 0. Introduction

The book [1] gives an elementary treatment of the algorithm to calculate the rank of elliptic curves of the form $y^2=x^3-kx$. Concerning with the construction of elliptic curves with higher rank, Menstre [2], Nagao [3] and Quer [4] gave some examples. In this paper we deal with elliptic curves C of the form $y^2=x^3-pqx$ where p and q are distinct odd primes. The rank r of the set $C(\boldsymbol{Q})$ of the rational points on C is less than or equal to 4. We will construct some families of the elliptic curves of the type of rank exactly 4.

§ 1. Definitions and fundamental formula

Let C denote the elliptic curve $y^2=x^3-kx$ and C' be the corresponding elliptic curve $y^2=x^3+4kx$. We denote the rational points of C and C' by $C(\boldsymbol{Q})$ and $C'(\boldsymbol{Q})$ respectively. Put $\boldsymbol{Q}^{*2}=\{u^2: u\in\boldsymbol{Q}^*\}$ and we define the map $\alpha: C(\boldsymbol{Q})\to\boldsymbol{Q}^*/\boldsymbol{Q}^{*2}$ and $\alpha': C'(\boldsymbol{Q})\to\boldsymbol{Q}^*/\boldsymbol{Q}^{*2}$ by $\alpha(\langle x,y\rangle)=x$ (if $x\neq 0$), $\alpha(\langle 0,0\rangle)=-k$, $\alpha(\infty)=1$, $\alpha'(\langle x,y\rangle)=x$ (if $x\neq 0$), $\alpha'(\langle 0,0\rangle)=4k$, $\alpha'(\infty)=1$.
Then the map α and α' are group homomorphisms by [1] and the rank r of $C(\boldsymbol{Q})$ can be calculated by [1] 3.6 as

$$2^{r+2}=\#\alpha(C(\boldsymbol{Q}))\cdot\alpha'(C'(\boldsymbol{Q}))$$

where # A denotes the cardinal number of the set A.

§ 2. Family of elliptic curves $y^2=x^3-pqx$ with rank 4

Lemma 2.1 *Let p and q be distinct odd primes. Let C be defined by $y^2=x^3-pqx$ and C' by*

$y^2=x^3+4pqx$. *Then the following holds.*

(a) $\alpha(C(\boldsymbol{Q}))\subset\{u \bmod \boldsymbol{Q}^{*2}: u=\pm 1, \pm p, \pm q \text{ or } \pm pq\}$

(b) $\alpha'(C'(\boldsymbol{Q}))\subset\{u \bmod \boldsymbol{Q}^{*2}: u=1, 2, p, 2p, q, 2q, pq \text{ or } 2pq\}$ and

(c) The rank of $C(\boldsymbol{Q})$ is at most 4

Proof. (a) Every point of $C(\boldsymbol{Q})$ has the form $(m/e^2, n/e^3)$ such that both m/e^2 and n/e^3 are irreducible fractions (see [1] chap 3 section 6). Thus the equation $y^2=x^3-pqx$ implies $n^2=m(m^2-pqe^4)$. The greatest common divisor $d=\gcd(m, m^2-pqe^4)$ divides pqe^4. Since $x=m/e^2$ is an irreducible fraction, we see $\gcd(m, e)=1$ and hence d divides pq. Let a prime l divide m and not divide pq. Then l doesn't divide e because of $\gcd(m, e)=1$. Hence l doesn't divide m^2-pqe^4.

On the other hand l divides n^2 because $n^2=m(m^2-pqe^4)$. Hence l divides n^2 with an even power and l divides m also with an even power because l does not divide m^2-pqe^4. Namely if a prime l divides m and does not divide pq, then it divides m with an even power. Hence we see that $\alpha(\langle m/e^2, n/e^3\rangle)=m=\pm 1, \pm p, \pm q$ or $\pm pg \bmod \boldsymbol{Q}^{*2}$

(b) By a similar argument we can prove that if a prime l divides m and does not divide $4pq$, then it divides m with an even power. Therefore $\alpha'(\langle m/e^2, n/e^3\rangle)=m=\pm 1, \pm p, \pm q, \pm pq, \pm 2, \pm 2p, \pm 2q$ or $\pm 2pq \bmod \boldsymbol{Q}^{*2}$. We can prove $m\geqq 0$ from the fact $n^2=m(m^2+4pqe^4)$. Hence $\alpha'(m/e^2, n/e^3)=m=1, p, q, pq, 2, 2p, 2q$, or $2pq \bmod \boldsymbol{Q}^{*2}$.

(c) By (a), (b) and (1.1) we have $2^{r+2}=\#\alpha(C(\boldsymbol{Q}))\cdot\#\alpha'(C'(\boldsymbol{Q}))\leqq 64=2^6$. Hence $r\leqq 4$

Proposition 2.2 *Suppose that four natural numbers A, B, C, D, and two primes p and q satisfy the equation* $pq=A^4+B^2=2C^2-D^4=s^4-4t^4$, $p=s^2-2t^2$ *and* $q=s^2+2t^2$. *Then the following holds.*

(a) *The point* $(q, 2qt)$ *is on the curve* $y^2=x^3-pqx$ *such that* $\alpha(\langle q, 2qt\rangle)=q$.

(b) *The point* $(2q, 4qs)$ *is on the curve* $y^2=x^3+4pqx$ *such that* $\alpha'(\langle 2q, 4qs\rangle)=2q$.

(c) *The point* $(pq/A^2, pqB/A^3)$ *is on the curve* $y^2=x^3-pqx$ *such that* $\alpha(\langle pq/A^2, pqB/A^3\rangle)=pq$.

(d) *The point* $(2D^2, 4DC)$ *is on the curve* $y^2=x^3+4pqx$ *such that* $\alpha'(\langle 2D^2, 4DC\rangle)=2$.

Proof. Clear

Proposition 2.3 *Under the same assumption as in Proposition* 2.2, *the following holds. In particular, the rank r of* $C(\boldsymbol{Q})$ *is* 4

(a) $\alpha(C(\boldsymbol{Q}))=\{u \bmod \boldsymbol{Q}^{*2}: u=\pm 1, \pm p, \pm q, \pm pq\}$

(b) $\alpha'(C'(\boldsymbol{Q}))=\{u \bmod \boldsymbol{Q}^{*2}: u=1, 2, p, 2p, q, 2q, pq, 2pq\}$.

Proof. (a) ($\supset$) We see that $q=\alpha(\!(q,\ 2qt)\!)\in\alpha(C(\boldsymbol{Q}))$ and $pq=\alpha(\!(pq/A^2,\ pqB/A^3)\!)\in\alpha(C(\boldsymbol{Q}))$ by Proposition 2.2 (a) and (c) and that $-pq=\alpha(\!(0,0)\!)\in\alpha(C(\boldsymbol{Q}))$. The three elements q, pq and $-pq$ can generate the right-hand side of (a), which provides the inclusion ($\supset$). The inclusion ($\subset$) is proved by Proposition 2.1 (a).

(b) ($\supset$) We see that $2q=\alpha(\!(2q,\ 4qs)\!)\in\alpha'(C'(\boldsymbol{Q}))$ and $2=\alpha'(\!(2D^2, 4DC)\!)\in\alpha'(C'(\boldsymbol{Q}))$ by Proposition 2.2 (b) and (d) and that $pq=4pq=\alpha'(\!(0,0)\!)\in\alpha'(C'(\boldsymbol{Q}))$. The three elements $2q$, 2 and pq can generate the right-hand side of (b), which implies the inclusion ($\supset$). The inclusion ($\subset$) is proved by Proposition 2.1 (b)

§ 3. Some concrete examples

We start from the following identities

$$(u+v)^4+(4v^2)^2=2(u^2+3v^2)^2-(u-v)^4 \tag{3.1}$$

and

$$(h^4-2k^4)^4+(4h^6k^2)^2=(h^4+2k^4)^4-4(2hk^3)^4. \tag{3.2}$$

If we put $A=u+v=h^4-2k^4$, $B=4v^2=4h^6k^2$, $C=u^2+3v^2$, $D=u-v$, $s=h^4+2k^4$, $t=2hk^3$, $p=s^2-2t^2$ and $q=s^2+2t^2$, then these A, B, C, D, s, t, p, q satisfy the assumption in Proposition 2.2. By a short calculation we can see that $v=h^3k$, $u=h^4-2k^4-h^3k$, $C=(h^4-2k^4-h^3k)^2+3h^6k^2$ and $D=h^4-2k^4-2h^3k$.

Example 3.1 (1) If $h=1$ and $k=2$, then $s=1^4+2\cdot2^4=33$ and $t=2\cdot2^3=16$, $p=33^2-2\cdot16^2=577$ and $q=33^2+2\cdot16^2=1601$. Both p and q are primes. Therefore $y^2=x^3-577\cdot1601x$ has the rank 4.

(2) If $h=3$ and $k=2$ then $s=3^4+2\cdot2^4=113$, $t=2\cdot3\cdot2^3=48$ and $p=113^2-2\cdot48^2=8161$, $q=113^2+2\cdot48^2=17377$. Both p and q are primes. Therefore $y^2=x^3-8161\cdot17377x$ has the rank 4.

(3) If $h=5$ and $k=2$, then $s=657$, $t=80$, $p=418849$ and $q=444449$. Both p and q are primes Therefore $y^2=x^3-418849\cdot444449x$ has the rank 4.

(4) The following list gives all prime pairs (p, q) with $1\leqq h\leqq11$ and $1\leqq k\leqq9$ so that $y^2=x^3-pqx$ has the rank 4.

(h, k)	(s, t)	(p, q)
(1, 2)	(33, 16)	(577, 1601)
(3, 2)	(113, 48)	(8161, 17377)
(3, 8)	(8273, 3072)	(49568161, 87316897)
(5, 2)	(657, 80)	(418849, 444449)
(7, 3)	(2563, 378)	(6283201, 6854737)
(9, 4)	(7073, 1152)	(47373121, 52681573)
(11, 1)	(14643, 22)	(214416481, 214418417)
(11, 3)	(14803, 594)	(218423137, 219834481)

To find more examples we use the following identity together with (3.1).

$$(8h^4-k^4)^4+(64h^6k^2)^2=(8h^4+k^4)^4-4(2hk^3)^4. \tag{3.3}$$

If we put $A=u+v=8h^4-k^4$, $B=4v^2=64h^6k^2$, $C=u^2+3v^2$, $D=u-v$, $s=8h^4+k^4$, $t=2hk^3$, $p=s^2-2t^2$ and $q=s^2+2t^2$, then these A, B, C, D, s, t, p, q satisfy the equation (2.4). By a short calculation, we have $v=4h^3k$, $u=8h^4-k^4-4h^3k$, $C=(8h^4-k^4-4h^3k)^2+48h^6k^2$ and $D=8h^4-k^4-8h^3k$.

Example 3.2 (1) If $h=1$ and $k=1$, then $s=8\cdot1^4+1^4=9$, $t=2\cdot1\cdot1^3=2$, $p=9^2-2\cdot2^2=73$ and $q=9^2+2\cdot2^2=89$. Both p and q are primes. Therefore $y^2=x^3-73\cdot89x$ has the rank 4.
(2) The following list gives all prime pairs (p, q) with $1\leqq h\leqq10$ and $1\leqq k\leqq11$ so that $y^2=x^3-pqx$ is of rank 4.

(h, k)	(s, t)	(p, q)
(1, 1)	(9, 2)	(73, 89)
(1, 7)	(2409, 686)	(4862089, 6744473)
(4, 7)	(4449, 2744)	(4734592, 34852673)
(5, 3)	(5081, 270)	(25670761, 25962361)

§ 4. Some comments

In the example 3.2, if $h=2$ and $k=1$, then $s=129$, $t=4$, $p=16609=17\cdot997$ and $q=16673$. Note that q is a prime but p is not a prime. In this case the elliptic curve does not have the form of $y^2=x^3-pqx$ with primes p, q. But we can prove the rank$\geqq4$ in the same way as in Propositions 2.2 and 2.3.

Remark. Professor Masao Koike at Kyushu University gave the following interesting example in the appendix of [2]. Let A, B, C, D be integers satisfying the relation $A^4+B^4=2C^4+2D^4$ and put $h=-(A^4+B^4+C^4-2A^4B^4-A^4C^4)/2^63^4$. Then the elliptic curve $E_h: y^2=x^3-hx$ has the following rational points:

$$R_1=(A^2B^2/2^23^2, AB(A^4+B^4-C^4)/2^43^3),$$
$$R_2=(A^2C^2/2^23^2, AC(A^4+C^4-B^4)/2^43^3),$$
$$R_3=(B^2C^2/2^23^2, BC(B^4+C^4-A^4)/2^43^3),$$
$$R_4=(D^2B^2/2^23^2, DB(D^4+B^4-C^4)/2^43^3) \text{ and}$$
$$R_5=(D^2C^2/2^23^2, DC(D^4+C^4-B^4)/2^43^3).$$

For $(A, B, C, D)=(21, 20, 7, 19)$, we get $h=4\cdot25\cdot11\cdot89$ and the rank of this curve is exactly 4.

References

1. J. H. Silverman and J. Tate: Rational points of elliptic curves, Springer-Verlag, New York 1992.
2. K. Nagao: On the rank of elliptic curve, Kobe Jour. Math. 11 (1994) 205-210.
3. J-F. Menstre: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, C. R. Acad. sci. Paris, ser. 1,305 (1987), 215-218.
4. J. Quer; Rang de courbes elliptiques d'invariant donne, C. R. Acad. sci. Paris, ser. 1,314 (1992), 919-923.
5. H. G. Zimmer: Computional Aspects of the theory of elliptic curves, R. A. Mollin (ed), Number Theory and Applications, 279-324.

Masayuki Maenishi
National College of Technology in Niihama
Yagumochou 7-1 Niihama city Ehime
Zip code 792-8580 JAPAN