Quadratic Twists of Elliptic Curves Associated to the Simplest Cubic Fields

By Dongho BYEON

Department of Mathematics, Pohang University of Science and Technology, Korea

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1997)

1. Introduction. Let m be a rational integer such that m^2+3m+9 is square-free. Let K be the cubic field defined by the irreducible polynomial over the rational number field $\boldsymbol{Q}$

$$f(x) = x^3 + mx^2 - (m+3)x + 1.$$

We call K a simplest cubic field.

In [2], Washington has studied the elliptic curve E defined over $\boldsymbol{Q}$ by

$$E : y^2 = x^3 + mx^2 - (m+3)x + 1,$$

and has shown that the 2-rank of ideal class group of K is greater than the rank of the group of rational points of E.

In this paper, we consider quadratic twists of the elliptic curve E and applying Washington's idea to our twists, show that the 2-rank of ideal class group of K is also greater than the ranks of the groups of rational points of some infinitely many quadratic twists of the elliptic curve E.

2. Main theorem. Let $a\ (\neq 0)$ be a rational integer and E_a be the quadratic twist of E defined by

$$E_a : ay^2 = x^3 + mx^2 - (m+3)x + 1.$$

Multiply each side of E_a by a^3 and replace a^2y, ax by y, x respectively. Then we have

$$E_a : y^2 = x^3 + max^2 - (m+3)a^2x + a^3.$$

The discriminant of E_a is $16a^6(m^2+3m+9)$ and the J-invariant of E_a is $256(m^2+3m+9)$.

Let $f_a(x) = x^3 + max^2 - (m+3)a^2x + a^3$. Then the cubic field defined by the irreducible polynomial $f_a(x)$ is also K because

$$f_a(x) = (x - a\rho)(x - a\rho')(x - a\rho''),$$

where ρ is the negative root of $f(x)$ and $\rho' = 1/(1-\rho)$ and $\rho'' = 1 - 1/\rho$ are the other two roots of $f(x)$. Thus the 2-torsion points on E_a are the points $(a\rho, 0)$, $(a\rho', 0)$, $(a\rho'', 0)$, none of which is rational.

For each rational prime $p \leq \infty$, let $\boldsymbol{Q}_p$ denote the completion of $\boldsymbol{Q}$ at p and $E_a(\boldsymbol{Q}_p)$ be the group of $\boldsymbol{Q}_p$-points of E_a. If p does not split in the cubic field K, let K_p denote the completion of K at the prime above p and define the homomorphism

$$\lambda_p : E_a(\boldsymbol{Q}_p) \to K_p^\times/(K_p^\times)^2,\ (x, y) \to x - a\rho.$$

If p splits, let

$$\lambda_p : E_a(\boldsymbol{Q}_p) \to ((\boldsymbol{Q}_p^\times/(\boldsymbol{Q}_p^\times)^2)^3,$$
$$(x, y) \to (x - a\rho,\ x - a\rho',\ x - a\rho''),$$
$$x \neq a\rho,\ a\rho',\ a\rho'',$$
$$(a\rho, 0) \to (z,\ a(\rho - \rho'),\ a(\rho - \rho'')),$$

where z is chosen so that $za^2(\rho - \rho')(\rho - \rho'') \in (K^\times)^2$. One defines $\lambda_p(a\rho', 0)$ and $\lambda_p(a\rho'', 0)$ similarly. Let $S_2(E_a)$, the Selmer group, be the subgroup of elements of $K^\times/(K^\times)^2$ which are in the image of λ_p for all p. The Tate-Shafarevich group $\text{Ш}_2(E_a)$ is defined by the exactness of the sequence

$$0 \to E_a(\boldsymbol{Q})/2E_a(\boldsymbol{Q}) \to S_2(E_a) \to \text{Ш}_2(E_a) \to 0.$$

Then we have the following theorem:

Theorem. *Let $a\ (\neq 0)$ be a rational integer and assume that a has no prime divisor which splits in K. Let $E_a(\boldsymbol{Q})$ be the group of rational points of E_a and rank $E_a(\boldsymbol{Q})$ denote the rank of $E_a(\boldsymbol{Q})$ over $\boldsymbol{Z}$. Let $C_2(K)$ be the 2-part of ideal class group of K, and $rk_2(C_2(K))$ denote the 2-rank (i.e, the dimension as a $\boldsymbol{Z}/2\boldsymbol{Z}$-vector space) of $C_2(K)$. Then we have*

$$\text{rank } E_a(\boldsymbol{Q}) \leq rk_2(C_2(K)) + 1.$$

Proof. First we define the map $S_2(E_a) \to C_2(K)$. Let $\alpha \in K^\times$ represent an element of $S_2(E_a)$, so $\alpha \in Im\lambda_p$ for all p. If p does not split in K, then $\alpha = (x - a\rho)\beta^2$ for some $\beta \in K_p^\times$ and $(x, y) \in E_a(\boldsymbol{Q}_p)$. Let ν be the valuation at the prime above p in K_p. Then since $\nu(x - a\rho) = \nu(x - a\rho') = \nu(x - a\rho'')$ and $\nu(x - a\rho)\nu(x - a\rho')\nu(x - a\rho'') = \nu(y^2)$, $\nu(\alpha)$ is even. Now suppose p splits in K. Let α', α'' denote the conjugates of α over $\boldsymbol{Q}$. Then we have

$$(\alpha, \alpha', \alpha'') = ((x - a\rho)\beta_1^2,\ (x - a\rho')\beta_2^2,\ (x - a\rho'')\beta_3^2)$$

for some $\beta_i \in \boldsymbol{Q}_p$ and $(x, y) \in E_a(\boldsymbol{Q}_p)$. Let ν be

This research is supported by POSTECH/BSRI special fund.

the p-adic valuation in $\boldsymbol{Q}_p$. If $\nu(x - a\rho)$ and $\nu(x - a\rho')$ or $\nu(x - a\rho'')$ are positive, then so is $\nu(a(\rho - \rho'))$ or $\nu(a(\rho - \rho''))$, hence p divides $a^3(m^2 + 3m + 9)$. Since a has no prime divisor which splits in K, p can not divide a. So p should divide $(m^2 + 3m + 9)$. But since $m^2 + 3m + 9$ is assumed to be square-free, p should ramify in K by [2. Proposition 1]. Thus we have a contradiction. If only $\nu(x - a\rho)$ is positive, it must be even. If $\nu(x - a\rho)$ is negative, then $\nu(x - a\rho) = \nu(x - a\rho') = \nu(x - a\rho'')$ and they are even. Therefore, α must have even valuation at all primes in K, so the ideal (α) is the square of an ideal of K : $(\alpha) = I^2$. So we can define the map $S_2(E_a) \rightarrow C_2(K)$ by $\alpha \rightarrow I$.

Now we consider the kernel of the map. We compute it in detail only for the case that a is negative because it can be computed similarly for the case that a is positive. If I is principal, then $\alpha = \epsilon\beta^2$ for some $\beta \in K^\times$ and some unit ϵ. Since $x - a\rho < x - a\rho' < x - a\rho''$ and the product is $y^2 \geq 0$, the signs of $\alpha, \alpha', \alpha''$ should be $+, +, +$ or $-, -, +$. Therefore, for signs of $\epsilon, \epsilon', \epsilon''$, there are the two possibilities. Since ρ, ρ', ρ'' have signs $-, +, +$, we find that either ϵ or $-\rho'\epsilon$ is totally positive, hence square by [2]. Therefore, if I is principal, either α or $-\rho'\alpha$ is a square, so the kernel of the map is contained in $\{1, -\rho'\}(K^\times)^2/(K^\times)^2$. Similarly, for the case that a is positive, the kernel of the map is contained in $\{1, -\rho\}(K^\times)^2/(K^\times)^2$.

Surjectivity of the map is also derived from the slight modification of Washington's argument in the proof of [2. Theorem 1]. Thus we have

$$rk_2(S_2(E_a)) = rk_2(C_2(K)) + 1 \text{ or } rk_2(C_2(K))$$

and from the exact sequence

$$0 \rightarrow E_a(\boldsymbol{Q})/2E_a(\boldsymbol{Q}) \rightarrow S_2(E_a) \rightarrow Ш_2(E_a) \rightarrow 0$$

we have

$$rank E_a(\boldsymbol{Q}) \leq rk_2(S_2(E_a)).$$

Finally we have

$$rank E_a(\boldsymbol{Q}) \leq rk_2(C_2(K)) + 1.$$

Thus we have proved the theorem completely. □

Remark 1. The assumption that the rational integer a has no prime divisor which splits in K is essential for our proof. For example, let q be a rational prime which splits in K and $\alpha \in K^\times$ represent an element of $S_2(E_q)$. In this case, α need not have even valuation at all prime divisors in K above q. Let α', α'' denote the conjugates of α over $\boldsymbol{Q}$. Then we have

$$(\alpha, \alpha', \alpha'') = ((x - q\rho)\beta_1^2, (x - q\rho')\beta_2^2, (x - q\rho'')\beta_3^2)$$

for some $\beta_i \in \boldsymbol{Q}_q$ and $(x, y) \in E_q(\boldsymbol{Q})$. Let ν be the q-adic valuation of $\boldsymbol{Q}_q$. If one of $\nu(x - q\rho)$, $\nu(x - q\rho')$, $\nu(x - q\rho'')$ is positive, then so are all of them and $\nu(x) > 0$. If $\nu(x) \geq 2$ then $\nu(x - q\rho) = \nu(x - q\rho') = \nu(x - q\rho'') = 1$. But $\nu(x - q\rho)\nu(x - q\rho')\nu(x - q\rho'') = \nu(y^2)$ is even. So we have a contradiction. Thus $\nu(x) = 1$ and let $x = qb$, where $b \in \boldsymbol{Q}_q$ and $\nu(b) = 0$. If two of $\nu(b - \rho)$, $\nu(b - \rho')$, $\nu(b - \rho'')$ are positive, then so is $\nu(\rho - \rho')$, $\nu(\rho - \rho'')$ or $\nu(\rho', -\rho'')$, hence q divides $(m^2 + 3m + 9)$. Since $m^2 + 3m + 9$ is assumed to be square-free, q should ramify in K by [2. Proposition 1]. So we also have a contradiction. Thus only one of $\nu(b - \rho)$, $\nu(b - \rho')$, $\nu(b - \rho'')$ is positive and it must be odd. Therefore only one of $\nu(x - q\rho)$, $\nu(x - q\rho')$, $\nu(x - q\rho'')$ is even and the others are one. This means that for some prime divisor in K above q, α has odd valuation. Thus we cannot define the map $S_2(E_q) \rightarrow C_2(K)$.

Remark 2. In [1], Kawachi and Nakano have obtained an extension of Washington's result in [2] to some other kinds of cubic polynomials and using the twist E_{-1} in the notation in this paper, have improved the result of Washington.

Aknowledgement. The author would like to thank the refree for many valuable remarks.

References

[1] M. Kawachi and S. Nakano: The 2-class groups of cubic fields and 2-descents on elliptic curves. Tohoku Math. J., **44**, 557–565 (1992).

[2] L. C. Washington: Class numbers of the simplest cubic fields. Math. Computation, **48**, no. 177, 371–384 (1987).