Math. J. Okayama Univ. **56** (2014), 51–63

SUMS OF TWO BIQUADRATES AND ELLIPTIC CURVES OF RANK ≥ 4

F.A. IZADI, F. KHOSHNAM AND K. NABARDI

ABSTRACT. If an integer n is written as a sum of two biquadrates in two different ways, then the elliptic curve $y^2 = x^3 - nx$ has positive rank. We utilize Euler's parametrization to introduce some homogeneous equations to prove that E_n has rank ≥ 3. If moreover n is odd and the parity conjecture is true, then the curve has even rank ≥ 4. Finally, some examples of ranks equal to 4, 5, 6, 7, 8 and 10, are also obtained.

1. INTRODUCTION

In this paper, we consider the family of elliptic curves defined by

$$E_n : y^2 = x^3 - nx,$$

for positive integers n written as sums of two biquadrates in two different ways, i.e.,

$$n = p^4 + q^4 = r^4 + s^4,$$

where $\gcd(p, q) = \gcd(r, s) = 1$. Such a solution is referred to as a primitive solution. In what follows we deal with numbers n having only primitive solution. This Diophantine equation was first proposed by Euler [7] in 1772 and has since aroused the interest of numerous mathematicians. Among quartic Diophantine equations it has a distinct feature for its simple structure, the almost perfect symmetry between the variables and the close relationship with the theory of elliptic functions. The latter is demonstrated by the fact that this equation is satisfied by the four elliptic theta functions of Jacobi, $\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4$, in that order [19]. Here in this note, we show that it also has an obvious relationship with the theory of elliptic curves. To this end, we need some parametric solutions of the equation for which we use the one that was constructed by Euler as:

$$\begin{cases} p = a^7 + a^5b^2 - 2a^3b^4 + 3a^2b^5 + ab^6, \\ q = a^6b - 3a^5b^2 - 2a^4b^3 + a^2b^5 + b^7, \\ r = a^7 + a^5b^2 - 2a^3b^4 - 3a^2b^5 + ab^6, \\ s = a^6b + 3a^5b^2 - 2a^4b^3 + a^2b^5 + b^7. \end{cases} \tag{1.1}$$

(See Hardy and Wright [8] page 201, equation No.(13.7.11)).

Mathematics Subject Classification. Primary 11G05; Secondary 10B10.

Key words and phrases. elliptic curves, rank, biquadrates, sums of two biquadrates, parity conjecture.

Our main result is the following:

Theorem 1.1. *If the Euler parametrization is used to represent the integer n as a sum of two biquadrates in two different ways, then the curve E_n has rank ≥ 3. If moreover n is odd and the parity conjecture is true, then the curve has even rank ≥ 4.*

Remark 1.2. Our numerical results suggest that the odd ranks for even numbers should be at least 5.

It is easy to see that the two different integers n_1 and n_2 having primitive solutions are distinct modulo $\mathbb{Q}^{*4}$. For let n_1 and n_2 be two such numbers in which (p_1, q_1, r_1, s_1) is the solution for n_1 and $n_2 = k^4 n_1$ for non-zero rational number k. It follows that (kp_1, kq_1, kr_1, ks_1) is a solution for n_2 which contradicts our assumption for n_2 having only primitive solution. We see that this condition is sufficient for the curves E_{n_1} and E_{n_2} to be non-isomorphic over $\mathbb{Q}$ (the dependence modulo $\mathbb{Q}^{*k}$ for $k = 0, 1, 2, 3$ expresses one curve as the quartic twists of the other; Cf. [15] Prop. 5.4, Cor. 5.4.1, Ch.X). However, it is not plain that there are infinitely many integers having primitive solutions. To remedy this difficulty, Choudhry [4] presented a method of deriving new primitive solutions starting from a given primitive solution. This makes it possible to construct infinitely many non-isomorphic elliptic curves using the primitive solutions of the biquadrate equation.

2. Previous works

For questions regarding the rank, we assume without loss of generality that $n \not\equiv 0 \pmod 4$. This follows from the fact that $y^2 = x^3 - nx$ is 2-isogenous to $y^2 = x^3 + 4nx$. These curves form a natural family in the sense that they all have j-invariant $j(E) = 1728$ regardless of the different values or various properties that the integers n may have. There have been a lot of investigations concerning the distribution of ranks of elliptic curves in natural families, and it is believed that the vast majority of elliptic curves E over $\mathbb{Q}$ have rank ≤ 1. Consequently, the identification of elliptic curves of rank ≥ 2 is of great interest.

Special cases of the family of the curves E_n and their ranks have been studied by many authors including Bremner and Cassels [3], Kudo and Motose [10], Maenishi [11], Ono and Ono [13], Spearman [17, 18], and Hollier, Spearman and Yang [9]. The general cases were studied by Aguirre, Castaneda, and Peral [1].

The main purpose of Aguirre et al., [1] was to find the elliptic curves of high rank in this family without restricting n to have any prescribed property. They developed an algorithm for general n, and used it to find 4 curves of rank 13 and 22 of rank 12.

Breamner and Cassels [3] dealt with the case $n = -p$, where $p \equiv 5 \pmod 8$ and less than 1000. The rank is always 1 in accordance with the conjecture of Selmer and Mordell. For each prime in this range, the authors found the generator for the free part. In some cases the generators are rather large, the most startling being that for $p = 877$, the x has the value

$$x = \left(\frac{612776083187947368101}{7884153586063900210}\right)^2.$$

Kudo and Motose [10] studied the curve for $n = p$, a Fermat or Mersenne prime and found ranks of 0, 1, and 2. More precisely,

(1) For a Fermat prime $p = 2^{2^n} + 1$,

$$E(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{for } p = 3, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} & \text{for } p = 5, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} & \text{for } p > 5. \end{cases}$$

(2) In case $p = 2^q - 1$ is a Mersenne prime where q is a prime,

$$E(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{for } p = 3, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} & \text{for } p > 3. \end{cases}$$

Maenishi [11] investigated the case $n = pq$, where p, q are distinct odd primes and found a condition that the rank of E_{pq} equals 4. This can be done by taking natural numbers A, B, C, D and two pairs p and q satisfying the equations:

$$pq = A^2 + B^2 = 2C^2 - D^4 = S^4 - 4t^4 \qquad (p = s^2 - 2t^2, q = s^2 + 2t^2).$$

Then using these equations one can construct 4 independent points on the corresponding elliptic curve.

Ono and Ono [13] examined the elliptic curves for $n = b^2 + b$, where $b \neq 0, -1$ is an integer, and showed that, subject to the parity conjecture, one can construct infinitely many curves E_{b^2+b} with even rank ≥ 2. To be more precise they obtained the followings:

Let $b \neq 0, -1$ be an integer for which $n = b^2 + b$, is forth power free, and define T by

$$T := \operatorname{card}\{p \mid \textit{primes } 3 \leq p \equiv 3 \pmod 4,\ p^2 \parallel b^2 + b\}.$$

1. *If $b \equiv 1, 2 \pmod 4$ and T is odd, then $E(b)$ has even rank ≥ 2.*
2. *If $b \equiv 7, 8, 11, 12, 20, 23, 24, 28, 35, 39, 40, 43, 51, 52, 55, 56 \pmod{64}$ and T is even, then $E(b)$ has even rank ≥ 2.*
3. *If $b \equiv 3, 14, 19, 27, 36, 44, 59, 60 \pmod{64}$ and T is odd, then $E(b)$ has even rank ≥ 2.*
4. *In all other cases, $E(b)$ has odd rank.*

In two separate papers, Spearman [17], [18] gave the following two results: (1) If $n = p$ for an odd prime p written as $p = u^4 + v^4$ for some integers u and v, then

$$E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}.$$

(2) If $n = 2p$, where $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$ for some integers u and v, then

$$E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}.$$

In recent paper Spearman along with Hollier and Yang [9] assuming the parity conjecture constructed elliptic curves of the form E_{-pq} with maximal rank 4, here $p \equiv 1 \pmod 8$ and q be an odd prime different from p satisfying

$$q = p^2 + 24p + 400.$$

Finally, Yoshida [20] investigated the case $n = -pq$ for distinct odd primes p, q and showed that for general such p, q the rank is at most 5 using the fact that

$$\operatorname{rank}(E_n(\mathbb{Q})) \leq 2\#\{l \text{ prime; divides } 2n\} - 1.$$

If p is an odd prime, the rank of $E_p(\mathbb{Q})$ is much more restricted, i.e.,

$$\operatorname{rank}(E_p(\mathbb{Q})) \leq \begin{cases} 0 & \text{if} \quad p \equiv 7, 11 \pmod{16}, \\ 1 & \text{if} \quad p \equiv 3, 5, 13, 15 \pmod{16}, \\ 2 & \text{if} \quad p \equiv 1 \pmod 8. \end{cases}$$

If the Legendre symbol $(q/p) = -1$ and $q - p \equiv \pm 6 \pmod{16}$, then

$$E_{-pq}(\mathbb{Q}) = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}/2\mathbb{Z}.$$

If p, q are twin prime numbers, then $E_{-pq}(\mathbb{Q})$ has a non-torsion point $(1, (p+q)/2)$. If p, q be twin primes with $(q/p) = -1$, then

$$E_{pq}(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

In many cases above, they have the same j-invariant $j(E) = 1728$, have the torsion subgroup $T = \mathbb{Z}/2\mathbb{Z}$, and have positive ranks. In spite of these similarities our family has almost higher ranks among all the other families and can be taken as an extension of the previous results. Before we proceed to the proofs, we wish to make the following remarks.

Remark 2.1. In [2] Aguirre and Peral using the previous version of our work proved the following two results.

Theorem 1. *The family $y^2 = x^3 - nx$, with $n = p^4 + q^4$ has rank at least 2 over $\mathbb{Q}(p, q)$.*

Theorem 2. *The family $y^2 = x^3 - nx$, in which n given by the Euler parametrization has rank at least 4 over $\mathbb{Q}(a)$, where a is the parameter and $b = 1$.*

One may prove both results by a very straightforward way. Since the specialization map is injective for infinitely many numerical values of the parameters [15] (Appendix C, Theorem 20.1), it is enough to find one specialization such that the above curves have ranks at least 2 and 4 respectively. For the first theorem, we note that, by the same reasons as in [2] not only the point $Q(p,q) = (-p^2, pq^2)$, but also the point $R(p,q) = (-q^2, qp^2)$ is on the curve, where

$$E_n : y^2 = x^3 - nx,$$

defined over function field $\mathbb{Q}(n,p,q)$ with $n = p^4 + q^4$. Then the specialization by $(p,q) = (2,1)$ gives rise to the points $Q = (-4,2)$ and $R = (-1,4)$. Therefore by using the SAGE software, we see that the associated height matrix has non-zero determinant 1.8567 showing that the points are independent. For the second theorem, we see that the points $Q_1 = (-p^2, pq^2)$, $Q_2 = (-q^2, qp^2)$, $Q_3 = (-r^2, rs^2)$ and $Q_4 = (-s^2, sr^2)$ are on the curve, where

$$E_n : y^2 = x^3 - nx,$$

defined over function field $\mathbb{Q}(n,p,q,r,s)$ with $n = p^4 + q^4 = r^4 + s^4$, and the specialized points by Euler parametrization (1.1) at $a = 2, b = 1$ gives rise to

$$Q_1 = (-24964, 549998),\ Q_2 = (-3481, -1472876),$$

$$Q_3 = (-17956, 2370326),\ Q_4 = (-17689, 2388148).$$

By using the SAGE software we find that the elliptic height matrix associated to $\{Q_1, Q_2, Q_3, Q_4\}$ has non-zero determinant 5635.73654 showing that again the 4 points are independent.

Remark 2.2. We see that the map $(u,v) \to (-u^2, uv^2)$ from the quadric curve: $u^4 + v^4 = n$ to the elliptic curve: $y^2 = x^3 - nx$ with $n = u^4 + v^4$, takes the integral points of the first to the integrals of the second. Now to find the integral points of the quadric, it is enough to find the integrals of the elliptic curve. This might suggest that to find n with more representations as sums of two biquadrates, the corresponding elliptic curve should have many independent integral points.

3. Method of Computation

To prove the theorem 1.1 , a couple of facts are necessary from the literature. We begin by describing the torsion subgroup of the family. To this end, let $D \in \mathbb{Z}$ be a fourth-power-free integer, and let E_D be the elliptic curve

$$E_D : y^2 = x^3 + Dx.$$

Then we have

$$E_D(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } D = 4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } -D \text{ is a perfect square}, \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

See ([15] Proposition 6.1, Ch.X, page 311). Since $n = p^4 + q^4$ is not -4 and can not be a square, (see for example [5], Proposition 6.5.3, page 391), we conclude that E_n has the torsion subgroup $T = \mathbb{Z}/2\mathbb{Z}$.

The second fact that we need is the parity conjecture which takes the following explicit form (see Ono and Ono [13]): Let r be the rank of elliptic curve E_n, then

$$(-1)^r = \omega(E_n)$$

where

$$\omega(E_n) = \text{sgn}(-n) \cdot \epsilon(n) \cdot \prod_{p^2||n} \left(\frac{-1}{p}\right)$$

with $p \geq 3$ a prime and

$$\epsilon(n) = \begin{cases} -1, & n \equiv 1, 3, 11, 13 \pmod{16}, \\ 1, & n \equiv 2, 5, 6, 7, 9, 10, 14, 15 \pmod{16}. \end{cases} \tag{3.1}$$

As we see from the parity conjecture formula, the key problem is to calculate the product $\prod_{p^2||n} \left(\frac{-1}{p}\right)$. For this reason it is necessary to describe the square factors of the numbers n if there is any. Before discussing the general case, we look at some examples:

$(p, q, r, s) = (3364, 4849, 4288, 4303)$ with $17^2|n$,
$(p, q, r, s) = (17344243, 6232390, 12055757, 16316590)$ with $97^2|n$,
$(p, q, r, s) = (9066373, 105945266, 5839429, 105946442)$ with $17^2|n$,
$(p, q, r, s) = (160954948, 40890495, 114698177, 149599920)$ with $41^2|n$.

These examples suggest that the prime divisor of the square factor of n is of the form $p = 8k + 1$. We will see that not only this divisor but also other odd prime divisors of n are of that form according to the following proposition.

Proposition 3.1. Let $n = u^4 + v^4$ be such that $\gcd(u, v) = 1$. If $p|n$ for an odd prime number p, then $p = 8k + 1$.

Proof. We have already know that n is not divisible by 4. We use the following result from Cox [6]. Let p be an odd prime such that $\gcd(p, m) = 1$ and $p|x^2 + my^2$ with $\gcd(x, y) = 1$, then $(\frac{-m}{p}) = 1$. From one hand for $n =$

$u^4+v^4=(u^2-v^2)^2+2(uv)^2$, we get $(\frac{-2}{p})=1$ which implies that $p=8k+1$ or $p=8k+3$. On the other hand, for $n=u^4+v^4=(u^2+v^2)^2-2(uv)^2$, we get $(\frac{2}{p})=1$ which implies that $p=8l+1$ or $p=8l+7$. Putting these two results together we get $p=8k+1$. □

Remark 3.2. If $n=p^2m$ for an odd prime p, then $p=8k+1$ from which we get $(\frac{-1}{p})=1$. This last result shows that the square factor of n does not affect the root number of the corresponding elliptic curve on the parity conjecture formula.

Remark 3.3. First of all, by the above remark, we have

$$\omega(E_n)=\operatorname{sgn}(-n)\cdot\epsilon(n).$$

On the other hand, for $n=p^4+q^4$, we note that

$$p^4\equiv 0 \text{ or } 1 \pmod{16},$$
$$q^4\equiv 0 \text{ or } 1 \pmod{16}.$$

For odd n we note that

$$n\equiv 1 \pmod{16}.$$

Now the parity conjecture implies that

$$\omega(E_n)=\operatorname{sgn}(-n)\cdot\epsilon(n)=(-1)\cdot(-1)=1.$$

For even n we have $n\equiv 2 \pmod{16}$ and therefore $\omega(E_n)=-1$ in this case.

Finally, we need the Silverman-Tate computation formula [16] (Ch.3 §.5, p.83) to compute the rank of this family. Let G denote the group of rational points on elliptic curve E in the form $y^2=x^3+ax^2+bx$. Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers and let $\mathbb{Q}^{*2}$ denote the subgroup of squares of elements of $\mathbb{Q}^*$. Define the group homomorphism ϕ from G to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ as follows:

$$\phi(P)=\begin{cases} 1 \pmod{\mathbb{Q}^{*2}} & \text{if } P=\mathcal{O}, \\ b \pmod{\mathbb{Q}^{*2}} & \text{if } P=(0,0), \\ x \pmod{\mathbb{Q}^{*2}} & \text{if } P=(x,y) \text{ with } x\neq 0. \end{cases}$$

The image $\phi(G)$ consists of b and mod $\mathbb{Q}^{*2}$ together with those b_1 mod $\mathbb{Q}^{*2}$ with $b=b_1b_2$ such that the equation

$$N^2=b_1M^4+aM^2e^2+b_2e^4 \quad (M\neq 0) \tag{3.2}$$

has a solution in N, M, $e\in\mathbb{Z}$

Similarly we take the dual curve $y^2=x^3-2ax^2+(a^2-4b)x$ and call its group of rational points $\overline{G}$. Now the group homomorphism ψ from $\overline{G}$ to

$\mathbb{Q}^*/\mathbb{Q}^{*2}$ defined as

$$\psi(Q) = \begin{cases} 1 \pmod{\mathbb{Q}^{*2}} & \text{if} \quad Q = \mathcal{O}, \\ a^2 - 4b \pmod{\mathbb{Q}^{*2}} & \text{if} \quad Q = (0,0), \\ x \pmod{\mathbb{Q}^{*2}} & \text{if} \quad Q = (x,y) \text{ with } x \neq 0. \end{cases}$$

Then the rank r of the elliptic curve E satisfies

$$2^{r+2} = |\phi(G)||\psi(\overline{G})|. \tag{3.3}$$

4. Proof of Theorem 1.1

The following facts are important tools in the proof of our main result. Put

$$\begin{aligned} A &= b^4 + 6b^2a^2 + a^4, \\ B &= b^8 + 2b^6a^2 + 11b^4a^4 + 2b^2a^6 + a^8, \\ C &= b^8 - 4b^6a^2 + 8b^4a^4 - 4b^2a^6 + a^8, \\ D &= b^8 - b^4a^4 + a^8. \end{aligned}$$

Remark 4.1. Note that the above expressions arise from the factorization of n by using the Euler parametrization (1.1), namely we have

$$\begin{aligned} n =& (b^4 + 6b^2a^2 + a^4)(b^8 + 2b^6a^2 + 11b^4a^4 + 2b^2a^6 + a^8)\cdot \\ & (b^8 - 4b^6a^2 + 8b^4a^4 - 4b^2a^6 + a^8)(b^8 - b^4a^4 + a^8). \end{aligned}$$

We may write $C = (a^2 - b^2)^4 + 2a^4b^4$, and $D = (a^4 - b^4)^2 + a^4b^4$. These expressions together with the expressions for A and B show that all the numbers A, B, C, and D are positive and satisfy $n = ABCD$.

Lemma 4.2. *We have the following properties:*

1. *A is non-square.*
2. *D is non-square.*

Proof. For part 1, we get the diophantine equation $x^4 + 6x^2y^2 + y^4 = z^2$, which has only the solutions $x^2 = 1, y = 0$ and $y^2 = 1, x = 0$ (see [12] page 18). Similarly, for part 2, we consider the diophantine equation $x^4 - x^2y^2 + y^4 = z^2$, which has only the trivial solutions $x^2 = 1, y = 0$ and $y^2 = 1, x = 0$ (see [12] page 20). □

Lemma 4.3. *Let* $\gcd(a,b) = 1$, *where a and b have opposite parities, then AC, and BD are non-squares.*

Proof. Since A and D are non-squares, it is sufficient to show that $\gcd(A,C) = 1$ and $\gcd(B,D) = 1$. We prove the first assertion, the second one is similar. First of all, since $\gcd(a,b) = 1$ and a and b have opposite parities , A and D are not divisible by 2. Secondly, we show that they are

not divisible by 3 and 11. To do this we may write $A = a^4 + b^4 + 6a^2b^2$ and $D = (a^4 + b^4)^2 - 3a^4b^4$. If 3 divides either A or D, then it divides $a^4 + b^4$ which is not the case by Proposition 3.1. For $p = 11$ we may write $A = (a^2+b^2)^2+(2ab)^2$ and $D = (a^4-b^4)^2+(a^2b^2)^2$. Since $\gcd(a^2+b^2, 2ab) = \gcd(a^4-b^4, a^2b^2) = 1$, it follows that none of A and D are divisible by primes of the form $4k+3$, in particular by 11. Next we have the following identities:

$$\begin{aligned} B &= A(A - 10a^2b^2) + 33a^4b^4, \\ C &= A(A - 16a^2b^2) + 66a^4b^4, \\ B &= D + 2a^2b^2A, \\ D &= (C + a^2b^2)(4a^4 - 9a^2b^2 + 4b^4), \\ 16D &= (4a^4 - 9a^2b^2 + 4b^4)(4a^4 + 9a^2b^2 + 4b^4) + 33a^4b^4. \end{aligned}$$

Let p be a prime dividing both A and C. Clearly p is different from 2, 3, and 11. From the second relation p divides one of the numbers a or b ,say a. This implies that p divides D by the third relation and b by the fourth, which is a contradiction. □

The following corollary is an immediate consequence of the above lemma.

Corollary 4.4. Let $b_1 = BD$, $b_2 = -AC$, $n = -b_1b_2$, where A, B, C, and D defined as before, then the elements of the sets $\{1, -n, -1, n, b_1, -b_1, b_2, -b_2\}$ and $\{1, 2, n, 2n\}$ are distinct modulo $\mathbb{Q}^{*2}$.

Proof. Without loss of generality we check only the assertion for the positive numbers in both sets. By construction we know that the numbers n, b_1 and $-b_2$ are all non-squares. These imply that

$$\begin{aligned} \frac{n}{1} &= n \not\equiv 1 \pmod{\mathbb{Q}^{*2}}, \\ \frac{n}{b_1} &= -b_2 = AC \not\equiv 1 \pmod{\mathbb{Q}^{*2}}, \\ \frac{n}{-b_2} &= b_1 = BD \not\equiv 1 \pmod{\mathbb{Q}^{*2}}, \\ \frac{b_1}{-b_2} &= \frac{BD}{AC} = \frac{n}{(AC)^2} \not\equiv 1 \pmod{\mathbb{Q}^{*2}}, \\ \frac{2n}{n} &= 2 \not\equiv 1 \pmod{\mathbb{Q}^{*2}}. \end{aligned}$$

Finally, for $\frac{n}{2}$ and $\frac{2n}{1}$, we note that if $\gcd(a, b) = 1$ and a and b have opposite parities, then all of A, B, C, and D are odd numbers. Hence by letting $n = rs^2$ for odd and square-free r we get $\frac{n}{2} = 2r(\frac{s}{2})^2$ and $\frac{2n}{1} = (2r)s^2$, where $2r$ is square-free in both equalities. On the other hand, if $\gcd(a, b) = 1$ with both a and b are odd numbers, then $A = 2(2k + 1)$, $C = 2(2m + 1)$, and B

and D are both odd. This implies that n is divisible by 4 which is not the case by assumption on section 2. □

Proof of Theorem 1.1:

To prove the theorem, we use the fact (3.2) several times. In fact, we show that

$$\phi(G) \supseteq \{1, -n, -1, n\}.$$

The first two numbers 1 and $-n$ are obvious from the definition of the map ϕ. For the numbers -1 and n, we note that if $n = p^4+q^4$, then the homogenous equation

$$N^2 = -M^4 + ne^4$$

has solution $e = 1$, $M = p$, $N = q^2$. Similarly for $N^2 = nM^4 - e^4$ we have $M = 1$, $e = p$, $N = q^2$. Next from Remark 4.1, we know that

$$\begin{aligned} n =&(b^4 + 6b^2a^2 + a^4)(b^8 + 2b^6a^2 + 11b^4a^4 + 2b^2a^6 + a^8)\cdot \\ &(b^8 - 4b^6a^2 + 8b^4a^4 - 4b^2a^6 + a^8)(b^8 - b^4a^4 + a^8). \end{aligned}$$

Let $b_1 = BD$, $b_2 = -AC$, $n = -b_1b_2$ be the same as the Corollary 4.4. By taking $M = 1$ and $e = b$, we have

$$\begin{aligned} b_1M^4 &= BD, \\ b_2e^4 &= -b^4AC. \end{aligned}$$

Then adding them up we get

(4.1)

$$\begin{aligned} K = b_1M^4 + b_2e^4 =& (b^8 + 2b^6a^2 + 11b^4a^4 + 2b^2a^6 + a^8)(b^8 - b^4a^4 + a^8) \\ &- b^4(b^4 + 6b^2a^2 + a^4)(b^8 - 4b^6a^2 + 8b^4a^4 - 4b^2a^6 + a^8). \end{aligned}$$

Now, using Sage to factor K, we get $K = a^4(a^6 + b^2a^4 + 4b^4a^3 - 5b^6)^2$. Consequently, $N = a^2(a^6 + b^2a^4 + 4b^4a^3 - 5b^6)$. Since $\phi(G)$ is a subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$, we get

$$\phi(G) \supseteq \{1, -n, -1, n, b_1, -b_1, b_2, -b_2\}. \tag{4.2}$$

On the other hand, for the curve

$$y^2 = x^3 + 4nx$$

we have

$$\psi(\overline{G}) \supseteq \{1, n, 2, 2n\}. \tag{4.3}$$

Again the numbers 1 and n are immediate consequence of the definition of the map ψ. For the numbers 2 and $2n$ we note that the homogeneous equation

$$N^2 = 2M^4 + 2ne^4$$

has the solution $M = p+q$, $e = 1$, and $N = 2(p^2+pq+q^2)$, where $n = p^4+q^4$. From Corollary (4.4), we know that the right hand side of (4.2), (4.3) are distinct modulo $\mathbb{Q}^{*2}$. Therefore from these observations together with Eq. (3.3) we get

$$2^{r+2} = |\phi(G)||\psi(\overline{G})| \geq 4 \cdot 8 = 32.$$

This implies that $r \geq 3$. But from $\omega(E_n) = 1$, the rank should be even. Therefore we see that r is even and $r \geq 4$.

4.1. **Remark.** If n is an even number written in two different ways as sums of two biquadrates, then since $\omega(E_n) = -1$ in this case, the rank is odd and $r \geq 3$.

5. Numerical Examples

We conclude this paper by providing many examples of ranks 4, 5, 6, 7, 8 and 10 using the Sage software [14].

Table 1. Curves with even rank

p	q	r	s	$n = p^4 + q^4 = r^4 + s^4$	$rank$
114732	15209	106696	81321	173329443404113736737	10
3494	1623	3351	2338	155974778565937	8
43676	11447	41591	28544	3656080821185585057	8
500508	338921	485288	378327	75948917104718865094177	8
502	271	497	298	68899596497	6
292	193	257	256	8657437697	6
32187	6484	29812	23109	1075069703066384497	4
7604	5181	7037	6336	4063780581008977	4

TABLE 2. Curves with odd rank

p	q	r	s	$n = p^4 + q^4 = r^4 + s^4$	$rank$
989727	161299	913141	717447	960213785093149760746642	7
129377	20297	127037	66787	280344024498199948322	7
103543	47139	98049	72389	119880781585424489842	7
119183	49003	112199	83693	207536518650314617202	7
3537	661	3147	2767	156700232476402	7
266063	72489	230099	217443	5038767537882101285602	5
139361	66981	138631	72723	397322481336075317362	5
38281	25489	36001	30713	2569595578866824162	5

Acknowledgements. The authors would like to express their hearty thanks to the anonymous referee for a careful reading the paper and for many useful comments and remarks which improved its quality.

REFERENCES

1. Aguirre, J., Castaneda, A. and Peral, J.C. *High rank elliptic curves with torsion group* $\mathbb{Z}/2\mathbb{Z}$, Mathematic of Computation, vol. 73, No. 245, (2003), 323-331.
2. Aguirre, J. and Peral, J.C. *Elliptic curves and biquadrates*, preprint, arXiv: 1203.2576v1.
3. Bremner, A. and Cassels, J.W.S. *On the equation* $Y^2 = X(X^2 + p)$, Math Comp., 42 (1984), 257- 264.
4. Choudhry, A. *The diophantine equation* $A^4 + B^4 = C^4 + D^4$, Indian J. pure appl. Math., 22(1): 9-11, January, 1991.
5. Cohen, H. *Number theory vol. I: tools and diophantine equations*, Springer, New York, 2007.
6. Cox, D.A. *Primes of the form* $x^2 + ny^2$*: Fermat, class field theory, and complex multiplication* (Pure and Applied Mathematics: John Wiley and Sons, Oct 24, 2011).
7. Euler, L. *Novi Comm.* Acad. Petrop., v. 17, p. 64. 1772.
8. Hardy, G.H. and Wright, E.M. *An Introduction to the theory of the numbers*, 4th edt., Oxford Univ. press 1975.
9. Hollies, A.J., Spearman, B.K. and Yang, Q. *Elliptic curves* $y^2 = x^3 + pqx$ *with maximal rank*, International Mathematical Forum, 5, 2010, No. 23, 1105-1110
10. Kudo, T. and Motose, K. *On group structure of some special elliptic curves*, Math. J. Okayama Univ. 47 (2005), 81-84
11. Maenishi, M. *On the rank of elliptic curves* $y^2 = x^3 - pqx$, Kumamoto J. Math. 15 (2002), 1-5.
12. Mordell, L.J., *Diophantine equations*, volume30, Academic Press Inc., (London)LTD, England, 1969.

13. Ono, K. and Ono, T. *Quadratic form and elliptic curves III*, Proc. Japan Acad. Ser. A Math. Sci. 72 (1996), 204-205.
14. SAGE software, *Version 4.3.5*, http://sagemath.org .
15. Silverman, J.H. *The arithmetic of Elliptic curves*, Springer, New York, 1986.
16. Silverman, J.H. and Tate, J. *Rational points on elliptic curves*, Springer, New York, 1985.
17. Spearman, B.K, *Elliptic curves* $y^2 = x^3 - px$, Math. J. Okayama Univ. 49 (2007), 183-184.
18. Spearman, B.K, *On the group structure of elliptic curves* $y^2 = x^3 - 2px$, International Journal of Algebra, 1(5) (2007), 247-250.
19. Whittaker, E.T. and Watson, G. N. it A course of modern analysis, Cambridge univ. Press, Cambridge, 1927.
20. Yoshida, S. *On the equation* $y^2 = x^3 + pqx$, Comment. Math. Univ. St. Paul., 49 (2000), 23-42.

Mathematics Department, Azarbaijan Shahid Madani University,
Tabriz, Iran
e-mail address: f.izadi@utoronto.ca

Mathematics Department, Azarbaijan Shahid Madani University,
Tabriz, Iran
e-mail address: khoshnam@azaruniv.edu

Mathematics Department, Azarbaijan Shahid Madani University,
Tabriz, Iran
e-mail address: nabardi@azaruniv.edu

(*Received March 19, 2012*)
(*Revised April 4, 2013*)