GLASNIK MATEMATIČKI
Vol. 44(64)(2009), 83 – 87

MAXIMAL RANKS AND INTEGER POINTS ON A FAMILY OF ELLIPTIC CURVES

P. G. Walsh
University of Ottawa, Canada

Abstract. We extend a result of Spearman which provides a sufficient condition for elliptic curves of the form $y^2 = x^3 - px$, with p a prime, to have Mordell-Weil rank 2. As in Spearman's work, the condition given here involves the existence of integer points on these curves.

1. Introduction

There are numerous publications which connect the rank of an elliptic curve to the size of the set of integral points on that curve. In [5], Silverman showed that the number of integer solutions to a cubic Thue equation $F(x, y) = m$ is bounded in terms of the rank of the Mordell-Weil group of the corresponding cubic curve $F(x, y) = mz^3$. Ingram [3] has recently proved that under suitable hypotheses, a rank one subgroup of a minimal elliptic curve with integer coefficients can have at most 6 integer points. For curves of the form

$$E_p : \ y^2 = x^3 - px, \tag{1.1}$$

with p prime, it is known that the rank of the Mordell-Weil group is at most 2, which can be proved using the methods in section X.6 of [6]. Extending a result of Kudo and Motose [4], Spearman [7] has recently proved that if p is a prime of the form $p = u^4 + v^4$ for some rational integers u, v, then the rank r_p of E_p attains the maximal $r_p = 2$. This formulation of Spearman can be interpreted in terms of the set $E_p(\mathbb{Z})$ of integer points on E_p.

Throughout the paper, p denotes an odd prime. Define $E_p^+(\mathbb{Z})$ to be the set of *positive* integer points on E_p, where an integer point (x, y) is defined to be positive if $y > 0$. It is clear that $|E_p(\mathbb{Z})| = 2|E_p^+(\mathbb{Z})| + 1$ since $(0, 0)$ lies

2000 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Elliptic curve, prime number.

on E_p. The purpose of specifying that integer points be positive is to avoid the effect of torsion on the discussion at hand, as it is well known that the rational torsion on E_p is precisely the group of order 2 generated by $(0,0)$.

In the proof of Theorem 2 of [9], the complete set of positive integer points on curves of the form (1.1) were explicitly given as follows. Let $\epsilon_p = T + U\sqrt{p}$ denote the fundamental unit in $\mathbb{Z}[\sqrt{p}]$.

(i) If $p = 2u^2 - 1$ for some positive integer u, then $(x, y) = (u^2, u(u^2-1)) \in E_p$.
(ii) If $norm(\epsilon_p) = -1$ and $U = u^2$ for some positive integer u, then $(x, y) = (pu^2, puT) \in E_p$.
(iii) If $p = u^4 + v^2$ for positive integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.

We remark that it is a consequence of the main result of [2] that there are at most four positive integer points on E_p. In particular, there is obviously at most one positive integer point of type (i), at most one of type (ii) by the main result in [2], and at most two of type (iii). Furthermore, two positive integer points of type (iii) exist precisely if $p = u^4 + v^4$ for positive integers u, v.

Concerning the rank of the Mordell-Weil group of $E_p(\mathbb{Q})$, as noted earlier, such curves can have rank no larger than 2. The authors of [4] showed that if p is a Fermat prime, then the rank of E_p is equal to 2. We note that this set of primes is not only thin, but assuredly finite. This result has recently been extended by Spearman in [7], who employed the ideas in Ch. 7 of [1] to show that the rank of E_p is equal to 2 whenever $p = u^4 + v^4$ for positive integers u, v. Although thin, this set of primes is conjecturally infinite.

In the present paper, we extend Spearman's theorem by showing that the rank of E_p is 2 whenever there are at least two positive integer points on E_p, except possibly if there are exactly two positive integer points, with one of them being of type (ii) above and the other being of type (iii) above. We use the above notation in the statement of the following theorem.

THEOREM 1.1. *If there are at least two positive integer points on E_p, then the rank of the Mordell-Weil group of $E_p(\mathbb{Q})$ is equal to 2, unless all of the following conditions hold, in which case the rank is either equal to 1 or to 2.*

1. *$p = u^4 + v^2$ with v a nonsquare integer,*
2. *$norm(\epsilon_p) = -1$ and $\epsilon_p = T + U\sqrt{p}$ satisfies the property that U is a square,*
3. *$(p+1)/2$ is a nonsquare integer.*

2. Proof

Assume that there are two positive integer points P_1, P_2 on E_p. The hypotheses of the theorem allow us to assume that P_1 and P_2 are not simultaneously of the form given by (ii) and (iii) above. Furthermore, by the result

of Spearman, we need not deal with the case that both P_1 and P_2 are of type (iii). Thus, there are only two cases to consider.

CASE I P_1 is of type (i) and P_2 is of type (ii).

We let E_p be as above, and as in [7], we define

$$\overline{E_p}: \quad y^2 = x^3 + 4px.$$

To compute the rank of E_p as in Chapter 7 of [1], we first need to determine the number of quartic equations of the form

$$dX^4 + cY^4 = Z^2$$

which are solvable in integers X, Y, Z, with $\gcd(X, c) = 1$, where, as in the proof of Theorem 1 of [7], $(d, c) = (p, -1)$ or $(-1, p)$. Furthermore, as remarked in that proof, the number of such equations which are so solvable is $2^\omega - 2$ for some integer $\omega \geq 1$. The hypothesis that P_2 is of type (ii) implies that $\epsilon_p = T + U\sqrt{p}$ satisfies $norm(\epsilon_p) = -1$ and $U = z^2$ for some integer z. We therefore have that $pz^4 - 1 = T^2$. Thus, $2^\omega - 2 > 0$, and so $\omega \geq 2$.

Following the method of Chapter 7 of [1] one step further, we now need to determine the number of quartic equations of the form

$$dX^4 + cY^4 = Z^2$$

which are solvable in integers X, Y, Z, with $\gcd(X, c) = 1$, where, as in the proof of Theorem 1 of [7], $(d, c) = (2p, 2)$ or $(2, 2p)$. Furthermore, as remarked in that proof, the number of such equations which are so solvable is $2^{\overline{\omega}} - 2$ for some integer $\overline{\omega} \geq 1$. Since P_1 is of type (i), it follows that $p = 2u^2 - 1$ for some integer u, and hence that $2p + 2 = (2u)^2$. Thus, $2^{\overline{\omega}} - 2 > 0$, and so $\overline{\omega} \geq 2$.

Finally, as in the proof of Theorem 1 of [7], or appealing directly to Corollary 7.5 of [1], the rank of E_p is given by $\omega + \overline{\omega} - 2$. We now deduce that

$$2 \geq rank(E_p) = \omega + \overline{\omega} - 2 \geq 2 + 2 - 2 = 2,$$

yielding the result as claimed.

CASE II P_1 is of type (i) and P_2 is of type (iii).

The proof for this case is identical to the previous case, except only that the equation $p - u^4 = v^2$ is used in the estimation of ω in place of the equation $pz^4 - 1 = T^2$ used above.

To complete the proof, we need only consider the case that E_p contain two positive integer points, one of which being of type (ii) and the other of type (iii). Both of these points are of infinite order, whence the rank is positive. Since the rank is at most 2, the proof of the theorem is complete.

3. Examples and Heuristics

It is not difficult to construct examples of curves which satisfy the property of having rank equal to 2 by way of Theorem 1.1, and which are not in the set of curves already found by Spearman in [7]. The following approach finds curves of rank 2 with one positive integer point of type (i) and one positive integer point of type (iii).

Let v denote an odd integer such that $(v^4+1)/2$ is divisible only by primes $q \equiv \pm 1 \pmod 8$, so that $X^2 - 2Y^2 = (v^4+1)/2$ is solvable. If $x_0 + y_0\sqrt{2}$ is an element in $\mathbb{Z}[\sqrt{2}]$ of norm $(v^4+1)/2$, let

$$x_i + y_i\sqrt{2} = (x_0 + y_0\sqrt{2})(3 + 2\sqrt{2})^i,$$

for $i \in \mathbb{Z}$. For each value $i \in \mathbb{Z}$, determine if $2x_i^2 - 1$ is prime and if $|2y_i|$ is nonsquare. If these conditions are satisfied, let $p = 2x_i^2 - 1$. Then it follows that E_p has one positive integer point of type (i) and exactly one positive integer point of type (iii). By choosing $v = 1$, one obtains the examples $p = 17, 97, 577$ in this way.

It is conjecturally the case that for each fixed v, the above construction leads to infinitely many examples. According to standard conjectures on the distributions of primes, the integer $2x_i^2 - 1$ is to be prime for infinitely many i. More precisely, the sequence $\{x_i\}$ grows exponentially, roughly like c^i for some $c > 0$, and so the probability that $2x_i^2 - 1$ is prime is roughly $(\log c)/(2i)$, which forces the sum of the probabilities, over all i, to diverge. Furthermore, one can also let v vary as well, thereby increasing the set of primes for which Theorem 1.1 applies.

Although we do not have a precise heuristic for the number of primes up to x for which the rank of E_p is 2, our computations indicate that this number grows roughly in size with $x^{1/2}$. Standard heuristics for the number of primes of the form u^4+v^4 show that Spearman's theorem will apply slightly more than about $x^{1/4}$ of the primes up to x. Similarly, using estimates for the number of primes simultaneously satisfying conditions (i) and (ii) or conditions (i) and (iii), we conjecture that Theorem 1.1 will also only apply to slightly more than $x^{1/4}$ of the primes up to x. Therefore, although Theorem 1.1 increases the set of primes p for which one can deduce that E_p has rank 2, this set of primes appears to be substantially smaller than the entire set of p for which E_p has rank 2.

It is worth noting that if E_p has one positive integer point of type (ii) and another of type (iii), then the rank of E_p can be equal to 1. It is not difficult to find many such examples, the smallest one being $p = 5$. Other such examples can be found by finding primes p of the form $p = u^2 + 1$, with u nonsquare, and we conjecture that there are infinitely such p for which the rank of $E_p = 1$. Thus, in this sense, Theorem 1.1 is best possible. However,

we are unable to prove that there are infinitely many primes p for which E_p has rank 2 using Theorem 1.1.

In [8], Spearman proves an analogous theorem for curves of the form $y^2 = x^3 - 2px$, where p is of the form $p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$. In future work, we will prove an analogue of Theorem 1.1 for these curves.

Acknowledgements.

The author gratefully acknowledges support from the Natural Sciences and Engineering Research council of Canada.

References

[1] J. S. Chahal, Topics in Number Theory, Plenum Press, New York, 1988.

[2] J. H. Chen and P. M. Voutier, *A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quartic Thue equations,* J. Number Theory **62** (1997), 71–99.

[3] P. Ingram, *Multiples of integer points on elliptic curves,* preprint.

[4] T. Kudo and K. Motose, *On group structures of some special elliptic curves,* Math. J. Okayama Univ. **47** (2005), 81–84.

[5] J. H. Silverman, *Integer points and the rank of Thue elliptic curves*, Invent. Math. **66** (1982), 395–404.

[6] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, New York, 1986.

[7] B. K. Spearman, *Elliptic curves $y^2 = x^3 - px$ of rank two*, Math. J. Okayama Univ. **49** (2007), 183–184.

[8] B. K. Spearman, *On the group structure of elliptic curves $y^2 = x^3 - 2px$*, Int. J. Algebra **1** (2007), 247–250.

[9] P. G. Walsh. *Integer solutions to the equation $y^2 = x(x^2 \pm p^k)$*, Rocky Mountain J. Math **38** (2008), 1285–1302.

P. G. Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, K1N-6N5
Canada
E-mail: gwalsh@uottawa.ca

Received: 30.4.2008.