ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 1, 2011

MAXIMAL RANKS AND INTEGER POINTS ON A FAMILY OF ELLIPTIC CURVES II

P.G. WALSH

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

1. Introduction. In two recent papers [**9, 10**], Spearman provided criteria for elliptic curves of the form $y^2 = x^3 - dx$, with $d = p, 2p$ and p prime, to have maximal rank. Specifically, in the case $d = p$, Spearman proved that if $p = u^4 + v^4$ for some integers u, v, then the rank of $y^2 = x^3 - px$ is 2, while in the case $d = 2p$, he proved that if $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$, for integers u, v, then the rank of $y^2 = x^3 - 2px$ is 3. In [**11**], it was shown that the above condition for the case $d = p$ can be described in terms of the set of integer points lying on such curves. The condition given includes all curves $y^2 = x^3 - px$ for which $p = u^4 + v^4$, but also includes a larger class of curves. We note however that although the result in [**11**] applies to more curves than those in [**9**], there is no closed form for those p, such as the polynomial given by Spearman. The purpose of the present paper is to give an analogous sufficient condition for curves of the form $y^2 = x^3 - 2px$ to have Mordell-Weil rank 3, where the condition is given in terms of rational points on these curves. This is more general than the approach taken in [**11**], wherein a similar condition was given, but stated in terms of integer points. We thank the anonymous referee for this suggestion. We note that, as in [**11**], there does not appear to be a closed form for those primes which satisfy the condition given in this paper.

As noted above, for curves of the form

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

2010 AMS *Mathematics subject classification.* Primary 11G05.
Keywords and phrases. Elliptic curve, prime number.
Received by the editors on May 13, 2008, and in revised form on August 5, 2008.
DOI:10.1216/RMJ-2011-41-1-311 Copyright ©2011 Rocky Mountain Mathematics Consortium

with p prime, it is known that the rank of the Mordell-Weil group is at most 3. This can be proved using the methods in [**8**, Section X.6]. We begin by some discussion on the rational points lying on these curves in order to formulate a generalization of Spearman's condition guaranteeing that the curve E_{-2p} has maximal rank.

Throughout the paper, p will denote an odd prime. Define $E^+_{-2p}(\mathbf{Q})$ to be the set of *positive* rational points on E_{-2p}, where a rational point (x, y) is defined to be positive if $y > 0$. We mention here that if $(x, y) \in E^+_{-2p}(\mathbf{Q})$, then $x = du^2$ for some rational u and squarefree integer $d \in \{-1, 2, -2, p, 2p\}$.

We will also make reference to the curve

$$E_{8p} : y^2 = x^3 + 8px.$$

We note that a positive rational point (x, y) on E_{8p} satisfies $x = du^2$ for some integer u, and $d \in \{1, 2, p, 2p\}$.

Theorem 1.1. *Assume that there are two positive rational points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ on E_{-2p}, and a positive rational point $P_3 = (x_3, y_3)$ on E_{8p}, with $x_i = d_i u_i^2$ $(1 \le i \le 3)$, where each d_i is squarefree, and $u_i \in \mathbf{Q}$. Assume further that*

1. $(d_1, d_2) \in \{(-1, 2), (-1, -2), (-1, p), (2, -2), (2, p)\}$,
2. $d_3 \in \{2, p\}$.

Then the rank of E_{-2p} is 3.

The conditions of the theorem are satisfied for odd primes p for which $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$ in positive integer u, v. In particular, $P_1 = (x_1, y_1) = (-(u^2 + 2v^2)^2, (u^2 + 2v^2)(u^2 - 2v^2)^2)$ and $P_2 = (x_2, y_2) = (-2(2uv)^2, 4uv|u^4 - 4v^4|)$ are positive integer points on E_{-2p} with $(d_1, d_2) = (-1, -2)$, and $P_3 = (2(2u^2)^2, 8u^2(3u^4 + 4v^4))$ is a positive integer point on E_{8p} satisfying $d_3 = 2$. Therefore, the set of curves for which the main result of [**10**] applies is included in Theorem 1.1.

2. Proof. We will compute the rank of E_{-2p} much as in [**10**] using the method from [**4**, Chapter 7]. As in [**10**], we denote by Γ the group

of rational points on E_{-2p}, and define a group map α on Γ by $\alpha(\mathcal{O}) = 1$,

$$\alpha((x,y)) = x \,(\mathrm{mod}\ \mathbf{Q}^{*\,2})$$

for $x \neq 0$, and $\alpha((0,0)) = -2p$.

We similarly define $\overline{\Gamma}$ and $\overline{\alpha}$ for the curve E_{8p}. We will use the fact, as pointed out in [**4**, Chapter 7], that if r is the rank of $E_{-2p}(\mathbf{Q})$, then

$$2^r = \frac{|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|}{4}.$$

In particular, we will show that if the conditions of the theorem are satisfied, then

$$|\alpha(\Gamma)| = 8, \qquad |\overline{\alpha}(\overline{\Gamma})| = 4.$$

This will be proved by showing that, when the conditions of the theorem are satisfied, then

$$\alpha(\Gamma) = \{1, -1, 2, -2, p, -p, 2p, -2p\},$$

and

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 2, p, 2p\}.$$

We note that a squarefree factor d of $-2p$ (respectively $8p$) is in $\alpha(\Gamma)$ (respectively $\overline{\alpha}(\overline{\Gamma})$) if the quartic equation $dX^4 + (-2p/d)Y^4 = Z^2$ (respectively $dX^4 + (8p/d)Y^4 = Z^2$) is solvable in nonzero integers X, Y, Z with $\gcd(X, (-2p/d)) = 1$ (respectively $\gcd(X, (8p/d)) = 1$).

For the curve E_{-2p}, we will deal with the case $(d_1, d_2) = (-1, 2)$, as the remaining cases can be proved in exactly the same manner. For simplicity of exposition, we further assume that the assumed given points on the curves in question have integral coordinates. Thus, by assumption, we have that $x_1 = -u_1^2$ and $x_2 = 2u_2^2$ for some nonzero integers u_1, u_2. The equation $y^2 = x^3 - 2px = x(x^2 - 2p)$ implies that there are integers v_1 and v_2 for which $u_1^4 - 2p = -v_1^2$ and $4u_2^4 - 2p = 2v_2^2$. These two equations can be rewritten as

$$2p - u_1^4 = v_1^2, \qquad 2u_2^4 - p = v_2^2.$$

We remark that $\gcd(u_2, p) = 1$. We first note that by the definition of the map α, we always have $1, -2p \in \alpha(\Gamma)$, and the above two equations

imply that $2, 2p \in \alpha(\Gamma)$. Since $\alpha(\Gamma)$ is a subgroup of $\mathbf{Q}^{*2}$, we get that $-1, -2, p, -p$ must also lie in $\alpha(\Gamma)$, giving the desired result. In all other cases stated in the theorem, one similarly finds that $|\alpha(\Gamma)| = 8$.

For the curve E_{8p}, we will deal with the case that $d_3 = p$, as the case $d_3 = 2$ was essentially proved in [**10**]. In this case, $x_3 = pu^2$ for some integer u, and from the equation $y^2 = x^3 + 8px = x(x^2 + 8p)$, there must be a positive integer v for which $p^2u^4 + 8p = pv^2$. Dividing through by p gives $pu^4 + 8 = v^2$. It is clear that u is odd, and so $p \in \overline{\alpha}(\overline{\Gamma})$. Since 1 and $2p$ are always in this subgroup of $\mathbf{Q}^{*2}$, we find that 2 is also in this group, and hence that $|\overline{\alpha}(\overline{\Gamma})| = 4$, as claimed.

3. The integer points on E_{-2p}. In [**11**], a complete description of $E_{-p^k}(\mathbf{Z})$ was given, which enabled the formulation in [**12**] of a generalization of Spearman's theorem in [**9**]. The purpose here is to give a precise description of the possible elements of $E^+_{-2p}(\mathbf{Z})$, along with the connection to family of quartic Diophantine equations, and the solutions thereof.

If (x, y) is a positive integer point on E_{-2p}, then the equation $y^2 = x^3 - 2px = x(x^2 - 2p)$ implies that $x = du^2$ and $x^2 - 2p = dv^2$ for some squarefree integer d and positive integers u, v. Combining these two equations yields $d^2u^4 - 2p = dv^2$; hence, d is a divisor of $2p$, and it follows that

$$du^4 - (2p/d) = v^2. \tag{3.1}$$

We examine each case separately.

1. $d = 1$. In this case (3.1) can be rewritten as $2p = u^4 - v^2$, which is evidently not possible modulo 8.

2. $d = -1$. In this case (3.1) can be rewritten as $2p = u^4 + v^2$, and as $2p$ has at most one representation as a sum of squares, we see that there are at most two solutions in positive integers (u, v) to this equation, and that $|u| < (2p)^{1/4}$.

3. $d = 2$. In this case (3.1) can be rewritten as $v^2 - 2u^4 = -p$. This type of quartic equation is the subject of current work by Akhtari and the author [**3**]. It follows from the methods therein that, apart from a set of at most 98 exceptional solutions in positive integers, all solutions in positive integers u, v to the equation $v^2 - 2u^4 = -p$

satisfy $u < 8 \cdot 10^6 p^{33/4}$. In practice, we never expect, nor have we ever seen, one example of an exceptional solution. As the bound we prove for nonexceptional solutions is comparatively small with those which arise from transcendence methods, we expect that integer solutions to $v^2 - 2u^4 = -p$ can be found quite readily if they do exist.

4. $d = -2$. In this case (3.1) can be rewritten as $p = v^2 + 2u^4$, which can have at most two solutions for the same reasoning as case 2 above, and moreover, that $|u| < (p/2)^{1/4}$.

5. $d = p$. In this case (3.1) can be rewritten as $pu^4 - v^2 = 2$, which by the main result of [**1**] (in particular, see [**2**]) has at most two solutions in positive integers u, v. According to the remarks in [**1**], we conjecture that there is at most one solution in positive integers (u, v) to $pu^4 - v^2 = 2$, and furthermore, if such a solution exists, then $(X, Y) = (u^2, v)$ is the fundamental solution to $pX^2 - Y^2 = 2$.

6. $d = -p$. In this case (3.1) can be rewritten as $pu^4 + v^2 = 2$, which evidently has no integer solutions.

7. $d = 2p$. In this case (3.1) can be rewritten as $v^2 - 2pu^4 = -1$, and by the theorem of Chen and Voutier in [**5**], there is at most one solution in positive integers. Furthermore, if a solution (u, v) does exist, then $(X, Y) = (v, u^2)$ is the fundamental solution to $X^2 - 2pY^2 = -1$.

8. $d = -2p$. In this case (3.1) can be rewritten as $v^2 + 2pu^4 = 1$, which evidently has no solutions in positive integers u, v.

Theorem 3.1. *For any odd prime p, there are at most 99 positive integer points on E_{-2p} with $|x| > 128 \cdot 10^{12} p^{33/2}$.*

Theorem 3.1 is not entirely satisfying because of the lack of information regarding the possible exceptionally large solutions. However, this theorem does improve upon results in the literature, such as the main result of [**8**].

From a computational point of view, if E_{-2p} has two positive integer points satisfying the hypotheses of Theorem 1.1, then this can be verified relatively efficiently by checking each of the four relevant cases above for which solutions can exist. In particular, the most time consuming aspects of such a computation would only require finding the factors of p in $\mathbf{Z}[\sqrt{2}]$, finding the factors of $2p$ in $\mathbf{Z}[i]$, computing the

minimal solution to $X^2 - 2Y^2 = -p$ and computing the fundamental solution to $X^2 - pY^2 = 1$.

Determining if E_{8p} has a positive integer point (x, y) with $x = 2u^2$ or pu^2 amounts to determining the solvability of $v^2 - 2u^4 = p$ and $v^2 - pu^4 = 8$. In practice, if solutions exist at all, then they arise from the product of the minimal solution to the corresponding quadratic equation times a small power of a unit. Thus, the most time consuming aspect of this computation would be the computation of the minimal solutions to the quadratic equations $X^2 - 2Y^2 = p$, $X^2 - pY^2 = 1$ and $X^2 - pY^2 = 8$. If the former is solvable, then bounds for the size of the minimal solution, such as those in [**6**, Theorem 108], show that determining solvability requires no more than $O(\sqrt{p})$ arithmetical operations. Determining the solvability of $X^2 - pY^2 = c$ $(c = 1, 8)$ can be accomplished by computing the continued fraction expansion of $\sqrt{p}$, as a solution (X, Y) in positive integers will have the property that X/Y is a convergent to $\sqrt{p}$ (provided that $p > 64$ if $c = 8$).

The purpose of the above discussion is to point out that the verification that E_{-2p} satisfies the hypotheses of Theorem 1.1 can in practice be achieved by relatively straightforward methods in computational algebraic number theory, as opposed to computations for computing the rank involving descent, searching for points on homogenous spaces, or other more technical methods involving elliptic curves.

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

REFERENCES

1. S. Akhtari, A. Togbe and P.G. Walsh, *The Diophantine equation* $aX^4 - bY^2 = 2$, Acta Arith. **131** (2008), 145–169.

2. ———, *Addendum on the Diophantine equation* $aX^4 - bY^2 = 2$, Acta Arith., to appear.

3. S. Akhtari and P.G. Walsh, *New bound for the number of integer points on certain cubic and quartic curves*, manuscript.

4. J.S. Chahal, *Topics in number theory*, Kluwer Academic/Plenum Publisher, New York, 1988.

5. 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.

6. T. Nagell, *Introduction to number theory*, Chelsea, New York, 1964.

7. W.M. Schmidt, *Integer points on curves of genus* 1, Comp. Math. **81** (1992), 33–59.

8. J.H. Silverman, *The arithmetic of elliptic curves*, GTM, Springer, New York, 1986.

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

10. ———, *On the group structure of elliptic curves* $y^2 = x^3 - 2px$, Int. J. Algebra **1** (2007), 247–250.

11. P.G. Walsh, *Integer solutions to the equation* $y^2 = x(x^2 \pm p^k)$, Rocky Mountain J. Math., to appear.

12. ———, *Maximal ranks and integer points on a family of elliptic curves*, Glasnik Math., to appear.

Department of Mathematics, University of Ottawa, 585 King Edward St., Ottawa, Ontario, Canada K1N-6N5
Email address: gwalsh@mathstat.uottawa.ca