ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 38, Number 4, 2008

INTEGER SOLUTIONS TO THE EQUATION $y^2 = x(x^2 \pm p^k)$

P.G. WALSH

1. Introduction. Let p be a prime number and $k \geq 1$ an integer. In a recent paper [**8**], Draziotis determines the integer solutions (x, y), with $y > 0$, to the diophantine equations

$$y^2 = x(x + p^k)(x - p^k), \tag{1.1}$$

$$y^2 = x(x^2 - p^k), \quad (k \text{ odd}) \tag{1.2}$$

and

$$y^2 = x(x^2 + p^k). \tag{1.3}$$

Note that if (x, y) is a solution to any one of these equations, then (p^2x, p^3y) is a solution to the same equation, but with k replaced by $k + 4$. This remark motivates the notion of a primitive integer solution to the above equations.

Definition. An integer solution (x, y) to a Diophantine equation of the form $y^2 = x^3 \pm p^k x$ is *primitive* if $y > 0$ and p^2 does not divide x. If p^2 divides x, then (x, y) is referred to as an *imprimitive* solution.

In order to determine all of the integer solutions to the equations above, it is sufficient to determine the primitive and imprimitive integer solutions. In [**8**], there are a number of shortcomings in the statements of the results that we endeavor to clarify and sharpen. In particular, no consideration to the concept of primitive solutions is given, thereby resulting in an algorithm which has endless running time (as k goes to infinity), and repeatedly finds imprimitive points of the form $(p^{2t}x, p^{3t}y)$ for some positive integer t. Furthermore, the description of the integer solutions to (1.1)–(1.3) in [**8**] is given in terms of the solutions (a, b) to the equation $a^4 \pm b^2 = p^k$, which seems to simply be

Received by the editors on September 22, 2005, and in revised form on February 15, 2006.

DOI:10.1216/RMJ-2008-38-4-1285

essentially a restatement of the original problem, rather than an actual determination of the integer solutions.

There are four goals of the present paper. The first goal is to determine a bound for the number of primitive integer solutions to (1.1)–(1.3) for a given prime p and exponent $k > 0$ (there are evidently no such solutions for $k = 0$). The second goal is to show that there is an upper bound on k for the existence of primitive integer solutions. Since a primitive integer solution to any one of (1.1)–(1.3) gives rise to a p-integral point on the corresponding curve (1.1)–(1.3) with $0 \leq k \leq 3$, there are only finitely many primitive integer solutions on the union of all curves (1.1)–(1.3) for k ranging from 0 to infinity. Therefore, for k sufficiently large, there cannot be a primitive integer solution on any of (1.1)–(1.3). Such an upper bound of computable type can be obtained using methods and results from transcendence theory (in particular the work of Brindza [**4**]), but the shortcoming is that such a bound depends on the prime p. Recent applications of modular curves to Diophantine analysis shows that there is an upper bound for k which is absolute, that is, independent of p. At the moment however, such an absolute upper bound is not computable. The third goal is to describe the source of primitive integer solutions when they do exist.It will be evident from the proofs given here that, typically, all such solutions can be obtained by a combination of computing the fundamental unit in the ring of integers in $\mathbf{Q}(\sqrt{p})$, and by writing p^k as a sum of squares. Finally, the last goal is to describe the source of imprimitive solutions and give evidence that all such solutions have $y = 0$.

We first make a passing remark in order to deal with the case $p = 2$ once and for all. As noted earlier, a primitive integer solution to one of equations (1.1)–(1.3), with $p = 2$, gives rise to a 2-integral point on a curve of the form (1.1)–(1.3), but with $0 \leq k \leq 3$. Using any one of several programs to do this (we use Magma), we found that equation (1.1) has no primitive integer points, equation (1.2) has the primitive integer points coming from $(x, k) \in \{(-1, 1), (2, 1), (9, 5), (338, 1)\}$, and that equation (1.3) has the primitive integer point coming from $(x, k) = (2, 2)$. For the remainder of the paper, we restrict our attention to the case that p is an odd prime.

Theorem 1. *Let p denote an odd prime number.*

(i) *If $k = 1$, then equation (1.1) has at most two primitive integer solutions.*

(ii) *If $k > 1$, then equation (1.1) has at most one primitive integer solution.*

(iii) *There is a computable constant $c_1 = c_1(p)$, depending only on p, and an absolute constant c_1^*, for which if $k > \min(c_1(p), c_1^*)$, then equation (1.1) does not have any primitive integer solutions. Moreover, (1.1) has no primitive integer solutions if k is divisible by $2, 3, 5, 7$, or a prime $q \geq 211$.*

(iv) *If $p \equiv 3 \pmod 4$, then there is at most one primitive integer solution when $k = 1$, and no primitive integer solutions when $k > 1$. A primitive integer solution exists when $k = 1$ only if $p^2 = 2u^2 - 1$ for some integer u.*

Remark. For $p = 41$ and $k = 1$, there are two solutions to (1.1), and so the result is sharp.

Theorem 2. *Let p denote an odd prime number.*

(i) *If $k = 1$, then equation (1.2) has at most four primitive integer solutions.*

(ii) *If $k > 1$ is odd, then equation (1.2) has at most three primitive integer solutions.*

(iii) *There is a computable constant $c_2 = c_2(p)$, depending only on p, and an absolute constant c_2^*, for which if $k > \min(c_2(p), c_2^*)$, then equation (1.2) does not have any primitive integer solutions. Moreover, (1.2) has no primitive integer solutions if k is divisible by $5, 7$, or a prime $q \geq 211$.*

(iv) *If $p \equiv 3 \pmod 4$, then there is at most one primitive integer solution when $k = 1$, and no primitive integer solutions when $k > 1$. A primitive integer solution exists when $k = 1$ only if $p = 2u^2 - 1$ for some integer u.*

Remark. For $p = 17$ and $k = 1$, there are indeed four primitive integer solutions to (1.2), namely $x = -4, -1, 9, 17$.

There is currently work in progress[1] by Bennett et al. [**2**] to completely solve $X^2 + Y^4 = Z^n$ for all $n \geq 4$, and in particular, show that there are in fact no nontrivial solutions for those values of n. This result would substantially improve part (iii) of both Theorems 1 and 2.

Theorem 3. *Let p denote an odd prime number.*

For $p = 3$, the only primitive integer solutions to (1.3) *come from $(x, k) = (1, 1), (3, 1), (4, 2), (121, 5)$. Assume now that $p > 3$.*

(i) *If $k = 1$, then equation* (1.3) *has at most two primitive integer solutions.*

(ii) *If $k = 2$, then equation* (1.3) *has at most two primitive integer solutions.*

(iii) *For $k > 2$, there are no primitive integer solutions to equation* (1.3).

The above theorems provide fairly sharp estimates for the number of primitive integer points. We are left with the problem of determining the imprimitive integer points. Imprimitive integer points on any curve of the form $y^2 = x^3 - p^k x$ with $k > 3$ are of the form $(x, y) = (p^2 u, p^3 v)$ for some integer point (u, v) on the curve $y^2 = x^3 - p^{k-4} x$. Therefore, we may restrict our attention to the case that $0 \leq k \leq 3$. For this, we remind the reader of the Ankeny-Artin-Chowla conjecture (AAC) [**1**], which states that if $p \equiv 1 \pmod 4$ is prime, and $(X, Y) = (T, U)$ is the fundamental solution to the Pell equation $X^2 - pY^2 = 1$, then p does not divide U. Despite the restriction to primes $p \equiv 1 \pmod 4$ in the original AAC conjecture, there is no known counterexample to the conjecture if one allows p to range over the set of all odd primes. Therefore, in reference to the AAC conjecture, we will allow p to be any odd prime.

Theorem 4. *If the Ankeny-Artin-Chowla conjecture is true, then all imprimitive integer solutions to an equation of the form $y^2 = x^3 - p^k x$, with $0 \leq k \leq 3$, have $y = 0$.*

From a computational perspective, in order to determine the imprimitive integer points with $0 \leq k \leq 3$, it will be apparent from the proof

of this theorem that one only needs to compute the fundamental unit in the quadratic field $\mathbf{Q}(\sqrt{p})$. In so doing, one simply verifies the AAC conjecture, in which case no imprimitive solutions occur for $0 \leq k \leq 3$. On the other hand, if an imprimitive solution were to exist, it can be written explicitly in terms of this fundamental unit.

2. The equation $x^2 + y^4 = z^7$. It is well known, see for example [**5**, Lemma 3.2.3], that for $1 \leq n \leq 3$, the equation $x^2 + y^4 = z^n$ has infinitely many solutions in coprime integers x, y, z. On the other hand, for $n = 4$ there are no coprime solutions, as proved by Fermat, and similarly for $n = 5$ and $n = 6$, which was proved by Bruin in his thesis [**5**]. Recently, Ellenberg [**9**] has proved that for all primes $p \geq 211$, the equation $x^2 + y^4 = z^p$ has no solutions in coprime integers, and so, to completely solve $x^2 + y^4 = z^n$, it remains to deal with $n = 9$, and n prime between 7 and 211. This is work which is currently underway in [**2**]. Such a result would entail a considerable sharpening of Theorems 1 and 2, and in fact, it would likely imply that the constants $c_1(p)$ and c_1^* in the statement of Theorems 1 and 2 would be replaced by 3. However, we do have the following now, which enables us to include 7 in part (iii) of Theorems 1 and 2. We are grateful to Andrew Bremner for suggesting the argument given below.

Proposition 1. *If x, y, z are coprime integers satisfying $x^2+y^4 = z^7$, then $xy = 0$.*

Proof. The equation $x^2 + y^4 = z^7$ with x, y, z coprime integers leads by unique factorization in $\mathbf{Z}[i]$ to an equation of type $x+iy^2 = \eta(a+bi)^7$ for coprime integers a, b, and unit $\eta = \pm 1, \pm i$ of $\mathbf{Z}[i]$. Comparing imaginary coefficients,

$$y^2 = \pm b(7a^6 - 35a^4b^2 + 21a^2b^4 - b^6),$$

or

$$y^2 = \pm a(a^6 - 21a^4b^2 + 35a^2b^4 - 7b^6).$$

By symmetry in a, b, it is only necessary to find all solutions to the first of these two equations. Now the greatest common divisor of b and

$7a^6 - 35a^4b^2 + 21a^2b^4 - b^6$ divides 7, so necessarily

$$7a^6 - 35a^4b^2 + 21a^2b^4 - b^6 = du^2, \quad b = dv^2,$$

where $d = \pm 1, \pm 7$. Now $(X, Y) = (7da^2/b^2, 7d^2u/b^3)$ is a rational point on the elliptic curve

$$X^3 - 35dX^2 + 147d^2X - 49d^3 = Y^2,$$

and, for $d = \pm 7$, the rational rank of this curve is 0, and the rational torsion group is trivial. No solutions for a, b arise. Furthermore, $(X, Y) = (-db^2/a^2, d^2u/a^3)$ is a rational point on the elliptic curve

$$X^3 + 21dX^2 + 35d^2X + 7d^3 = Y^2,$$

which for $d = -1$ has rational rank 0 and trivial rational torsion. Again, no solutions for a, b arise. It remains to consider the case $d = 1$, namely, finding all rational points on

$$7a^6 - 35a^4b^2 + 21a^2b^4 - b^6 = u^2.$$

However, this equation is 2-adically insolvable. Congruences modulo 4 show that a and b must both be odd, forcing $u \equiv 0 \pmod 4$. Put $b = a + 2c$, $u = 4v$, to give

$$a^6 - 2a^5c - 38a^4c^2 - 64a^3c^3 - 12a^2c^4 + 24ac^5 + 8c^6 = 2v^2,$$

contradicting a being odd.

3. Proof of Theorem 1. We will first consider the case that $x > 0$. Let d_1, d_2, d_3 denote square-free positive integers, and u, v, w positive integers for which

$$x = d_1u^2, x + p^k = d_2v^2, x - p^k = d_3w^2.$$

Let q denote a prime factor of d_1. Equation (1.1) implies that q divides d_2d_3, and so it divides one of d_2 or d_3. Since q divides x, and also one of $x \pm p^k$, the only possibility is that $q = p$. Since d_1 is square-free, it follows that either $d_1 = 1$ or $d_1 = p$, and so either $x = u^2$ or $x = pu^2$.

Case 1.1. $x = u^2$. Since the d_i are square-free, $d_1 d_2 d_3$ is a square, and $d_1 = 1$ by assumption, it follows that $d_3 = d_2$. We conclude that

$$u^2 + p^k = d_2 v^2, u^2 - p^k = d_2 w^2, \tag{3.1}$$

and so subtracting these two equations shows that

$$2p^k = d_2(v^2 - w^2). \tag{3.2}$$

Therefore, d_2 is one of $1, 2, p, 2p$, each of which will be dealt with separately.

Case 1.1a. $d_2 = 2p$. Equation (3.2), with $d_2 = 2p$, shows that $p^{k-1} = v^2 - w^2$, from which it follows that $k > 1$. Since x arises from a primitive solution to (1.1), we have that p^2 does not divide x, and it follows that $\gcd(v, w) = 1$ Consequently, $v = (p^{k-1} + 1)/2$ and $w = (p^{k-1} - 1)/2$. Equation (3.1) gives the relation $2u^2 = 2p(v^2 + w^2)$, and so letting $u_1 = u/p$, which is an integer, we get that $pu_1^2 = v^2 + w^2 = (p^{2k-2} + 1)/2$, which is not possible.

Case 1.1b. $d_2 = p$. In this case we have $2p^{k-1} = v^2 - w^2$, which is not possible modulo 4.

Case 1.1c. $d_2 = 1$. Equation (3.1) becomes $u^2 + p^k = v^2$ and $u^2 - p^k = w^2$, and so $p^k = v^2 - u^2 = u^2 - w^2$ shows that p can be written in two distinct ways as a difference of coprime squares, which is not possible, as $p^k = X^2 - Y^2$ with X, Y positive coprime integers implies that $X = (p^k + 1)/2$ and $Y = (p^k - 1)/2$ for any odd prime p and $k \geq 1$.

Case 1.1d. $d_2 = 2$. We obtain $u^2 + p^k = 2v^2$ and $u^2 - p^k = 2w^2$, from which it follows that $2p^k = 2v^2 - 2w^2 = 2(v^2 - w^2)$, and by the remark in the preceding case, $v = (p^k + 1)/2$ and $w = (p^k - 1)/2$. Substituting $v = (p^k + 1)/2$ in $u^2 + p^k = 2v^2$ gives the equation $u^2 = (p^{2k} + 1)/2$. The results in [**3**] imply that the equation $X^n + Y^n = 2Z^2$ has no nontrivial solutions for $n > 2$ and even. Therefore, the relation $p^{2k} + 1 = 2u^2$ implies that $k = 1$, and so a primitive integer point arises only in the case $k = 1$, provided that p^2 is of the form $2u^2 - 1$.

Case 1.2. $x = pu^2$. As before, let $x + p^k = d_2v^2$ and $x - p^k = d_3w^2$ with d_2 and d_3 positive square-free integers. Since pd_2d_3 is a square, it follows that $d_2d_3 = pz^2$ for some integer z. In particular, this forces either $d_3 = pd_2$ or $d_2 = pd_3$, and without loss of generality, we will assume the former case, as the latter case is proved in exactly the same way.

Therefore, analogous to equation (3.1), we have

$$pu^2 + p^k = d_2v^2, \qquad pu^2 - p^k = pd_2w^2,$$

from which it follows that $p^2(u^4 - p^{2k-2}) = p(d_2vw)^2$. This shows that $(d_2vw)/p$ is an integer, and that $u^4 - p^{2k-2} = p((d_2vw)/p)^2$. If $k > 1$, then p divides u, and hence p^2 divides x, contradicting primitivity. Therefore, $k = 1$, and we obtain the equation $u^4 - 1 = p((d_2vw)/p)^2$. By a result of Samuel [**17**], $p = 5$ and $u = 3$, or $p = 29$ and $u = 99$.

Case 1.3. $x = -u^2$. In this case we obtain that

$$-u^2 + p^k = d_2v^2, \qquad -u^2 - p^k = -d_2w^2, \tag{3.3}$$

with d_2 a square-free positive integer, and v, w positive integers which are coprime if $k > 3$. Furthermore, as in Case 1.1, d_2 is one of $1, 2, p, 2p$.

Case 1.3a. $d_2 = cp$, $c = 1$ or 2. Equation (3.3) becomes

$$-u^2 + p^k = cpv^2, -u^2 - p^k = -cpw^2. \tag{3.4}$$

Adding these two equations gives $-2u^2 = cp(v^2 - w^2)$, which shows p^2 divides x, contradicting primitivity.

Case 1.3b. $d_2 = 1$. Equation (3.3) becomes

$$-u^2 + p^k = v^2, \qquad -u^2 - p^k = -w^2. \tag{3.5}$$

Therefore, $2p^k = v^2 + w^2$ and $-2u^2 = v^2 - w^2$. Note that v and w are necessarily odd, and they are also coprime because of primitivity. The equation $-2u^2 = v^2 - w^2$ implies that there are coprime integers

m, n, m odd, for which $w \pm v = 2m^2$ and $w \mp v = 4n^2$. From this, it follows that $w = m^2 + 2n^2$ and $v = \pm(-m^2 + 2n^2)$, and by substituting these expressions into $2p^k = v^2 + w^2$ gives $p^k = m^4 + 4n^4$. Since $m^4 + 4n^4 = (m^2 - 2mn + 2n^2)(m^2 + 2mn + 2n^2)$, and the two factors are coprime, it follows that $1 = m^2 - 2mn + 2n^2 = (m - n)^2 + n^2$. Therefore, one deduces that $m = n = 1$, $w = 3, v = 1$, $u = 2$ and $p^k = 5$.

Case 1.3c. $d_2 = 2$. In this case, equation (3.3) becomes

$$-u^2 + p^k = 2v^2, \qquad -u^2 - p^k = -2w^2, \tag{3.6}$$

which give the equations $p^k = v^2 + w^2$ and $-u^2 = v^2 - w^2$. Note that by primitivity, we have that $\gcd(v, w) = 1$. Thus, (u, v, w) form a primitive pythagorean triple with w odd, and consequently, v even. Therefore, there are coprime integers m, n for which $w = m^2 + n^2$, $v = 2mn$, $u = m^2 - n^2$, and by substituting v and w into $p^k = v^2 + w^2$ shows that $p^k = m^4 + 6m^2n^2 + n^4$. When p^k is of this form, then $x = -(m^2 - n^2)^2$ is the unique corresponding primitive integer solution to equation (1.1). Note that there is at most one representation of p^k in the form $m^4 + 6m^2n^2 + n^4$, and from the fact that $x = -(m^2 - n^2)$, such a representation gives only one solution to equation (1.1). It follows that for p and k fixed, there is at most one primitive integer solution to equation (1.1) arising from representations of p^k in the form $m^4 + 6m^2n^2 + n^4$. Note that equation (3.6) implies that $u^4 + (2vw)^2 = p^{2k}$, and so by the proposition above, k is not divisible by $2, 3, 5, 7$ or any prime $q \geq 211$. For k not divisible by such a prime, a computable upper bound $c_1(p)$ for k follows from the work of Brindza [**4**]. Also, for the remaining ternary equations of the form $X^2 + Y^4 = Z^q$, with q prime and $7 < q < 211$, the result of Darmon and Granville in [**7**] implies that the set of coprime integer solutions (X, Y, Z) to this finite set of equations is finite, from which it follows that k is bounded by some absolute constant c_1^* which is independent of the prime p.

Case 1.4. $x = -pu^2$. In this case we have that $d_2 d_3 = -pz^2$ for some integer z. Since d_2 and d_3 are positive and square-free, we may assume that $d_3 = -pd_2$. Equation (3.1) in this case becomes

$$-pu^2 + p^k = d_2 v^2, \qquad -pu^2 - p^k = -pd_2 w^2,$$

and so after some deductions, it follows that $u^4 - p^{2k-2} = -p((d_2vw)/p)^2$. As in Case 1.2, a descent argument shows that u is divisible by $p^{(k-1)/2}$, and so by putting $u_1 = u/p^{(k-1)/2}$, it follows that $u_1^4 - 1 = -p((d_2vw)/p^k)^2$, which is not possible.

Part (iv) is a consequence of the above analysis, as only in Case 1.1d can a primitive integer solution exist.

4. Proof of Theorem 2. Equation (1.2) implies that there is a square-free integer d, and positive integers u, v for which $x = du^2$ and $x^2 - p^k = dv^2$. Combining these two equations gives

$$d^2u^4 - p^k = dv^2, \tag{4.1}$$

and since d is square-free, it follows that d is one of $1, -1, p, -p$. We will deal with each of these cases separately.

Case 2.1. $d = 1$. In this case, equation (4.1) gives $u^4 - v^2 = p^k$. By primitivity, we may assume that $\gcd(u, v) = 1$. Therefore, $u^2 + v = p^k$ and $u^2 - v = 1$, from which it follows that $2u^2 - 1 = p^k$. By a recent result of Bennett and Skinner [**3**], there is no solution for $k > 3$. If $k = 3$, then (u, p) is an integer point on the elliptic curve $2X^2 - 1 = Y^3$, which implies that $p = 23$. In the case $k = 1$, p is therefore of the form $2u^2 - 1$, giving the unique solution $x = (p + 1)/2$.

Case 2.2. $d = p$. In this case, equation (4.1) gives $p^2u^4 - p^k = pv^2$, and it follows from primitivity that $k = 1$. Dividing through by p gives the equation $pu^4 - 1 = v^2$. This equation was solved completely by Chen and Voutier in [**6**]. In particular, when this occurs, $(X, Y) = (v, u^2)$ must be the fundamental solution to the Pellian equation $X^2 - pY^2 = -1$.

Case 2.3. $d = -1$. In this case, equation (4.1) gives $u^4 - p^k = -v^2$, and so p^k has the representation as a sum of squares $p^k = u^4 + v^2$. This representation is evidently unique, and so at most one solution can arise in this case, unless only if v is a square, that is, $p^k = u^4 + v_1^4$ for positive integers u, v_1, in which case two solutions to (1.2) arise. Finally, by the aforementioned results in [**5, 9**], if k is divisible by $5, 7$

or a prime $q \geq 211$, then $p^k = u^4 + v^2$ is not solvable. For k not divisible by such a prime q, then a computable upper bound $c_2(p)$ for k follows from the results of [**4**], and as in the proof of Theorem 1, an absolute bound c_2^* for k exists in light of the results in [**7**].

Case 2.4. $d = -p$. In this case, equation (4.1) gives $p^2u^4 - p^k = -pv^2$, and by primitivity, it follows that $k = 1$. Dividing through by p gives the equation $pu^4 - 1 = -v^2$, which is clearly not possible.

For part (iv) of the theorem, the above analysis, with $p \equiv 3 \pmod 4$, shows that a primitive solution can exist only in Case 2.1.

Remark. We conjecture that the Diophantine equation $X^2 - p^kY^4 = -1$ has no positive integer solutions for any prime p if $k > 1$ is odd. Moreover, in Case 2.3, it is likely that no primitive solution can arise. This would follow if the result of Ellenberg is extended to cover all primes $q \geq 5$. Therefore, we conjecture that for $k > 3$, there are no primitive integer solutions to equation (1.2).

5. Proof of Theorem 3. Throughout the proof, we let u and v be positive integers for which $x = du^2, x^2 + p^k = dv^2$, with $d > 0$ and square-free. Evidently, the only possible values for d are 1 and p.

We first show that there is no solution to equation (1.3) for $k > 3$. In the case $d = 1$, we obtain the equation $u^4 + p^k = v^2$, and so $(v - u)(v + u) = p^k$, forcing $v = u^2 + 1$ and $p^k = 2u^2 + 1$. By the result in [**3**], this equation is not solvable for $k > 3$. In the case $d = p$, we obtain the equation $p^2u^4 + p^k = pv^2$. If $k > 3$, then p divides v, and hence p divides u, contradicting primitivity.

We now consider the cases $k \in \{1, 2, 3\}$ separately.

Assume first that $k = 1$ and $d = 1$. Then we have the equation $u^4 + p = v^2$. It follows, as in previous cases, that $v = u^2 + 1$ and $p = 2u^2 + 1$. Conversely, for p of the form $2u^2 + 1$, then $x = u^2$ gives a primitive integer solution to (1.3). For $k = 1$ and $d = p$, we obtain the equation $p^2u^4 + p = pv^2$, which can be rewritten as $pu^4 + 1 = v^2$. For $p = 3$, there is a solution $u = 2$; hence, $x = 12$ yields a solution to equation (1.3). Assume that $p > 3$. By the result of [**15**], the equation

$pu^4 + 1 = v^2$ has at most one solution in positive integers, and such a solution must come from the minimal solution to $X^2 - pY^2 = 1$. Note that when a solution to $pu^4 + 1 = v^2$ does exist (with $u > 0$), then $x = pu^2$ gives rise to a primitive integer solution to equation (1.3).

Now assume that $k = 2$ and $d = 1$. Then we have the equation $u^4 + p^2 = v^2$, which evidently implies that $\gcd(u, v) = 1$. Moreover, from the factorization $p^2 = (v - u^2)(v + u^2)$, it follows that $v - u^2 = 1$, and hence $p^2 = v + u^2 = 2u^2 + 1$. Conversely, if an odd prime p satisfies the equation $p^2 = v + u^2 = 2u^2 + 1$, then $x = u^2$ gives rise to a primitive integer solution to equation (1.3) with $k = 2$. If $k = 2$ and $d = p$, then we obtain the quartic equation $p^2u^4 + p^2 = pv^2$, from which it follows that p divides v, and that $u^4 + 1 = p(v/p)^2$. By a classical result of Ljunggren [**11**], there is at most one positive integer solution to this quartic equation, and if a solution exists, it can be determined explicitly from the fundamental solution of the Pell equation $X^2 - pY^2 = -1$.

We consider the case $k = 3$. If $d = 1$, we obtain the equation $u^4 + p^3 = v^2$. By primitivity, p does not divide $\gcd(u, v)$, and so it follows that $v - u^2 = 1$ and $v + u^2 = 2u^2 + 1 = p^3$. Since there are no integer points (X, Y) on the curve $2Y^2 + 1 = X^3$ with $Y > 0$, there are no solutions to (1.3) arising from this case. If $d = p$, then we obtain the equation $p^2u^4 + p^3 = pv^2$, from which it follows that p divides v, and u. Hence, the solution is imprimitive. Thus, there are no primitive solutions to equation (1.3) when $k = 3$.

6. Proof of Theorem 4. We deal with the equations $y^2 = x(x^2 - p^k)$ and $y^2 = x(x^2 + p^k)$ separately. We may assume throughout the proof that $k > 0$, since all of the rational points on the curves $y^2 = x^3 \pm x$ have $y = 0$.

Assume first that (x, y), $y > 0$, is an imprimitive integer solution to the equation $y^2 = x(x^2 - p^k)$, with $0 \leq k \leq 3$. Then there is a positive integer u for which x is of one of the forms $u^2, pu^2, -u^2, -pu^2$, and by assumption, p divides u. In the case $x = u^2$, we see that $u^4 - p^k = v^2$ for some positive integer v and notice that p divides v. Therefore, $k = 1$ is not possible since p^2 divides the other two terms. If $k = 2$, then dividing $u^4 - p^2 = v^2$ through by p^2 gives $p^2(u/p)^4 - 1 = (v/p)^2$, which is not possible. If $k = 3$, then dividing $u^4 - p^3 = v^2$ through by p^3 gives $p(u/p)^4 - 1 = p(v/p^2)^2$, which again is not possible. The

cases $x = -u^2$ and $x = -pu^2$ are also straightforward to dismiss, as one obtains equations of the form $u^4 - p^k = -v^2$ (in the case $x = -u^2$), and upon dividing through by p^k $(k = 1, 2, 3)$, it becomes evident that the left side cannot be negative. Therefore, we may assume that $x = pu^2$, for some positive integer u which is divisible by p. We then obtain the equation $p^2u^4 - p^k = pv^2$, with $1 \leq k \leq 3$. The case $k = 2$ is evidently not possible, since upon dividing through by p^2 in this case, exactly two of the terms in the expression are divisible by p. So we are left with the cases $k = 1$ and $k = 3$.

If $k = 1$, then we obtain the equation

$$pu^4 - 1 = v^2, \quad (p \mid u). \tag{6.1}$$

By the main result of [**6**], equation (6.1) implies that $v + u^2\sqrt{p}$ is the fundamental solution to the Pell equation $X^2 - pY^2 = -1$. Moreover, as $p \mid u$, such a solution to equation (6.1) is a counterexample to the Ankeny-Artin-Chowla conjecture. If $k = 3$, then p divides v, and so by letting $u_1 = u/p, v_1 = v/p$, we obtain the equation

$$p^3u_1^4 - 1 = v_1^2. \tag{6.2}$$

The main result of [**6**] implies that $v_1 + u_1^2 p\sqrt{p}$ is either the fundamental solution, or the pth power thereof, to the Pellian equation $X^2 - pY^2 = -1$. The former case would violate the Ankeny-Artin-Chowla conjecture, and so we need only consider the latter case.

Assume that $v_1 + u_1^2 p\sqrt{p}$ is the pth power of the fundamental solution to the Pell equation $X^2 - pY^2 = -1$. Let $\alpha = T + U\sqrt{p}$ denote the fundamental solution to the Pellian equation $X^2 - pY^2 = -1$, and for $i \geq 1$, put $\alpha^i = T_i + U_i\sqrt{p}$. Thus, we are assuming that $U_p = pu_1^2$. By the divisibility properties of the sequence $\{U_i\}$, it is easy to deduce that either $U_1 = s^2$ or $U_1 = ps^2$ for some integer s. If $U_1 = ps^2$, then the AAC conjecture is violated. If $U_1 = s^2$, then $U_p/U_1 = p(u_1/s)^2$, which is not possible by a result of Rotkiewicz, see [**16**, Theorem 5].

Now assume that (x, y) is an imprimitive solution to the equation $y^2 = x^3 + p^k x$ with $1 \leq k \leq 3$. In this case, either $x = u^2$ or $x = pu^2$ for some integer u which is divisible by p. The case $x = u^2$ leads to $u^4 + p^k = v^2$ for some integer v, also divisible by p, and by an analysis similar to that given above, it is seen that this case is not possible. In

the case that $x = pu^2$ for some integer u divisible by p, we obtain the equation $p^2u^4 + p^k = pv^2$, and as above, it is readily verified that $k = 2$ is not possible.

If $k = 1$, then dividing through by p gives $pu^4 + 1 = v^2$. By the main result of [**14**], it follows that $(X, Y) = (v, u^2)$ is the fundamental solution to $X^2 - pY^2 = 1$, provided that $p > 3$, which we may assume since we have verified that the corresponding equations for $p = 3$ have no imprimitive integer solutions. Since p divides u, we obtain a counterexample to the AAC conjecture.

Assume that $k = 3$. Then dividing the equation $p^2u^4 + p^3 = pv^2$ by p^3 (recall that p divides u), yields $p^3(u/p)^4 + 1 = (v/p)^2$, that is, $(X, Y) = (v/p, (u/p))$ is a solution to $X^2 - p^3Y^4 = 1$. By the main result of [**15**], it follows that $v/p + p(u/p)^2\sqrt{p}$ is the fundamental solution to $X^2 - p^3Y^2 = 1$. By the divisibility properties of solutions to the Pell equation, it follows that $v/p + p(u/p)^2\sqrt{p}$ is the fundamental solution, or pth power thereof, to $X^2 - pY^2 = 1$. If it is the fundamental solution, then we have a counterexample to the AAC conjecture. Therefore, we will assume that $v/p + p(u/p)\sqrt{p}$ is the pth power of the fundamental solution.

We first show that v is even. Recall that $(X, Y) = (v/p, (u/p))$ is a solution to $X^2 - p^3Y^4 = 1$. If v is odd, then there are integer r, s with $u/p = 2rs$, such that one of the following holds

$$v/p \pm 1 = 2p^3r^4, \quad v/p \mp 1 = 8s^4,$$

or

$$v/p \pm 1 = 8p^3r^4, \quad v/p \mp 1 = 2s^4.$$

It follows that one of the following four equations holds

$$4s^4 - 1 = p^3r^4, \quad s^4 - 1 = 4p^3r^4,$$
$$4s^4 + 1 = p^3r^4, \quad s^4 + 1 = 4p^3r^4.$$

It is easy to see that the first two are not possible, since they give rise to solutions to the Pell equation $X^2 - pY^2 = 1$ of which $v/p + p(u/p)\sqrt{p}$ is the square, contradicting the fact that it is the pth power of the fundamental solution (with p odd). As the equation $s^4 + 1 = 4p^3r^4$ is

not possible modulo 4, we are left to consider the equation $4s^4 + 1 = p^3r^4$. Notice that $4s^4 + 1 = (2s^2 + 2s + 1)(2s^2 - 2s + 1)$, from which it follows that for some choice of sign, $2s^2 \pm 2s + 1 = t^4$ for some positive integer t. This equation can be rewritten as $(2s \pm 1)^2 + 1 = 2t^4$, and by Ljunggren's result in [**12**] on the equation $X^2 - 2Y^4 = -1$, it follows that $t = 1$ or $t = 13$, leading to the possibilities $s = 0, 1, 119, 120$, none of which giving solutions to an equation of the form $4s^4 + 1 = p^3r^4$. Therefore, we may henceforth assume that v above is even.

Since $(v/p)^2 - 1 = p^3(u/p)^4$, there are odd integers r, s for which $v/p \pm 1 = r^4$ and $v/p \mp 1 = p^3s^4$. Therefore, $(X, Y) = (r^2, ps^2)$ is a solution to the Pellian equation $X^2 - pY^2 = \pm 2$. By the relationship between this equation, and the equation $X^2 - pY^2 = 1$ (see, for example, [**13**]), it follows that $(X, Y) = (r^2, ps^2)$ is the pth power of the fundamental solution to the equation $X^2 - pY^2 = \pm 2$. It follows from the divisibility properties of solutions to these Pell equations that the fundamental solution to $X^2 - pY^2 = \pm 2$ is either of the form $(X, Y) = (r_1^2, ps_1^2)$, or of the form $(X, Y) = (r_1^2, s_1^2)$. In the first case, the fundamental solution $T + U\sqrt{p} = (r_1^2 + ps_1^2\sqrt{p})^2$ to $X^2 - pY^2 = 1$ violates the AAC conjecture. In the second case, we must appeal to [**12**, Theorem 1] as follows. Let $\alpha = r_1^2 + s_1^2\sqrt{p}$ denote the fundamental solution to $X^2 - pY^2 = \pm 2$. Then $\alpha^p = r^2 + ps^2\sqrt{p}$. Also, let $\beta = r_1^2 - s_1^2\sqrt{p}$. The Lehmer sequence $\{U_i\}$ defined by $U_i = (\alpha^i - \beta^i)/(\alpha - \beta)$ satisfies the conditions of [**12**, Theorem 1]. We deduce from that theorem that the equation $U_p/U_1 = px^2$ is not solvable for $p > 3$. In our situation, we have precisely that $U_p = p(s/s_1)^2$, a contradiction. This completes the proof of Theorem 4. □

7. Determining all integer points. The proofs of the above theorems allow one to completely solve the respective Diophantine equations (1.1), (1.2) and (1.3). Evidently, one needs to determine all primitive and imprimitive integer solutions. As remarked in the introduction, imprimitive integer solutions to one of (1.1)–(1.3), with $k > 3$, arise from primitive integer solutions to the same equation, but with k replaced by $k - 4i$ for some $1 \leq i \leq k/4$. Therefore, the procedure is simply to determine the primitive integer solutions to (1.1)–(1.3) with exponents $k, k - 4, \ldots, k - 4t$, where $0 \leq k - 4t \leq 3$, and then multiply the x and y coordinates of all found points with the appropriate powers of p to form the corresponding imprimitive solutions at exponent k.

Example 1. We show how the results obtained are used to determine all integer points on $y^2 = x(x^2 - 7^5)$.

Part (iv) of Theorem 2 shows that this equation has no primitive integer solutions. Imprimitive integer solutions arise from integer solutions to the equation $y^2 = x(x^2 - 7)$. Also from part (iv) of Theorem 2, the only possible primitive integer solution to $y^2 = x(x^2-7)$ can arise from a representation of the from $7 = 2u^2 - 1$, and evidentally, such a representation exists with $u = 2$. This gives the integer solutions $(x, y) = (4, \pm 6)$ to $y^2 = x(x^2 - 7)$, and hence the integer solutions $(x, y) = (4 \cdot 7^2, \pm 6 \cdot 7^3)$ to $y^2 = x(x^2 - 7^5)$. As for the imprimitive integer solutions to $y^2 = x(x^2 - 7)$, they are either the point $(x, y) = (0, 0)$, or they arise from solutions to the Pellian equation $X^2 - 7Y^2 = -1$, which is not possible. We conclude that the integer solutions (x, y) to $y^2 = x(x^2 - 7^5)$ are $(0, 0), (4 \cdot 7^2, 6 \cdot 7^3), (4 \cdot 7^2, -6 \cdot 7^3)$.

Example 2. We determine the integer solutions to $y^2 = x(x^2 - 13^7)$.

The proof of Theorem 2 shows that primitive integer solutions arise from solutions to either of the equations $13^7 = X^4 + Y^2$, $X^2 - 13^7 y^4 = -1$. The proposition shows that the first equation is not solvable. For the second equation, we need only compute the minimal solution to $X^2 - 13Y^2 = -1$ and verify that the value of Y is not a square. Thus, it is readily verified that there are no primitive integer solutions to $y^2 = x(x^2 - 13^7)$. The imprimitive integer solutions to this equation come from integer solutions to $y^2 = x(x^2 - 13^3)$. Similarly, going through the different cases in the proof of Theorem 2 shows that the only case that gives rise to a primitive integer solution is the case stemming from the representation of 13^3 as a sum of squares. In particular, since $13^3 = 3^4 + 46^2$, this gives the integer solutions $(x, y) = (-9, \pm 138)$. Moreover, as in the previous example, it is readily verified that the only imprimitive integer solution to $y^2 = x(x^2 - 13^3)$ is $(x, y) = (0, 0)$. We conclude that the only integer solutions (x, y) to $y^2 = x(x^2 - 13^7)$ are $(0, 0), (-9 \cdot 13^2, 138 \cdot 13^3), (-9 \cdot 13^2, -138 \cdot 13^3)$.

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

ENDNOTES

1. Note added in proof: Bennett, Ellenberg and Ng have since completed the proof that the equation $x^2 + y^4 = z^n$ has no nontrivial integer solutions for $n \geq 4$. This result substantially improves part (iii) of both Theorems 1 and 2 in that the equations being considered in these theorems have primitive integer solutions for all $k > 3$.

REFERENCES

1. N.C. Ankeny, E. Artin and S. Chowla, *The class number of real quadratic number fields*, Ann. Math. **52** (1952), 479–493.

2. M.A. Bennett, J. Ellenberg and N. Ng, *On the integer solutions to the ternary equation* $x^2 + y^4 = z^n$, in preparation.

3. M.A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canadian J. Math. **56** (2004), 23–54.

4. B. Brindza, *On S-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hung. **44** (1984), 133–139.

5. N. Bruin, *Chabauty methods and covering techniques applied to generalised Fermat equations*, Ph.D. thesis, University of Leiden, 1999.

6. 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.

7. H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513–543.

8. K. Draziotis, *Integral solutions of the equation* $Y^2 = X^3 \pm p^k X$, Math. Comp., to appear.

9. J. Ellenberg, *Galois representations attached to Q curves, and the generalized Fermat equation* $A^4 + B^2 = C^p$, Amer. J. Math. **126** (2004), 763–787.

10. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norsk. Vid. Akad. Oslo Volume **1** (1942), 1–27.

11. ———, *Ein Satz über die Diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skand. Matemheikerkongressen, Lund, 1953, 188–194, (1954).

12. F. Luca and P.G. Walsh, *Squares in Lehmer sequences with Diophantine applications*, Acta Arith. **100** (2001), 47–62.

13. T. Nagell, *On a special class of Diophantine equations of the second degree*, Ark. Math. **3** (1954), 51–65.

14. D. Poulakis and P.G. Walsh, *A note on the Diophantine equation* $x^2 - dy^4 = 1$ *with prime discriminant*, Comptes Rendues Math. Rep. Acad. Sci. Canada, to appear.

15. ———, *A note on the Diophantine equation* $x^2 - dy^4 = 1$ *with prime discriminant* II, Colloq. Math., to appear.

16. A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. **42** (1983), 163–187; J. Number Theory **74** (1999), 134–147.

17. P. Samuel, *Résultats élémentaires sur certaines équations diophantennes*, J. Théorie des Nombres (Bordeaux) **14** (2002), 629–646.

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