PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 104(118) (2018), 149–156 DOI: https://doi.org/10.2298/PIM1818149G

THE NUMBER OF SOLUTIONS TO $y^2 = px(Ax^2 + 2)$

Tarek Garici, Omar Kihel, and Jesse Larone

Abstract. We find a bound for the number of the positive solutions to the titled equation, improving a result of Togbé. As a consequence, we prove a conjecture of Togbé in a few cases.

1. Introduction

Cassels [**2**] was challenged to determine when the sum of three consecutive cubes equals a square. He [**2**] reduced the problem to finding integral points on the elliptic curve $y^2 = 3x(x^2+2)$. Using the arithmetic of certain quartic number fields, he obtained that the integral points on the above elliptic curve were $(x, y) = (0, 0)$, $(1, 3)$, $(2, 6)$, and $(24, 204)$.

Using the classical work of Ljunggren [**5**] and its generalizations (see [**1**, **4**, **10**, **11**]), Luca and Walsh [**6**] considered the problem of finding the number of positive integer solutions to the Diophantine equation $y^2 = nx(x^2 + 2)$, where $n > 1$ is a positive integer. They proved that the number of positive integer solutions to $y^2 = nx(x^2+2)$ is at most $3 \cdot 2^{\omega(n)} - 1$, where $\omega(n)$ is the number of distinct prime factors of n. In [**3**], Chen considered the case where n is a prime number greater than 3. He proved, in particular, that the Diophantine equation $y^2 = nx(x^2 + 2)$ has at most two positive integer solutions.

Recently, Togbé [**8**] considered the more general Diophantine equation

$$y^2 = px(Ax^2 + 2), \tag{1.1}$$

where p is a prime number and A is an odd integer greater than 1. He proved the following theorem.

Theorem 1.1. *For any prime p and any odd positive integer $A > 1$, the Diophantine equation* (1.1) *has at most seven positive integer solutions (x, y).*

2010 *Mathematics Subject Classification:* Primary 11D25; Secondary 11B39.

Key words and phrases: Diophantine equations; Legendre symbol; integral points on elliptic curves.

Communicated by Žarko Mijajlović.

Using results obtained through MAGMA, he then made the following conjecture on sharp bounds for the number of solutions to equation (1.1).

CONJECTURE 1.1. *Let p be a prime and $A > 1$ any odd positive integer.*

(1) *If* $(A, p) \equiv (1,1)$, $(1,5)$, $(1,7)$, $(3,1)$, $(3,3)$, $(3,7)$, $(5,1)$, $(5,5)$, $(5,7)$, $(7,3)$, *or* $(7,5) \pmod 8$*, then Diophantine equation* (1.1) *has at most one positive integer solution* (x, y).

(2) *If* $(A, p) \equiv (1,3)$ *or* $(7,1)$*, then Diophantine equation* (1.1) *has at most two positive integer solutions* (x, y).

(3) *If* $(A, p) \equiv (3,5)$ *or* $(7,7)$*, then Diophantine equation* (1.1) *has at most three positive integer solutions* (x, y).

Our aim is to improve the bound on the number of solutions to Diophantine equation (1.1) provided in Theorem 1.1, and to prove Conjecture 1.1 in some cases. The main result of the paper is the following theorem.

THEOREM 1.2. *Let p be a prime and let $A > 1$ be an odd integer.*

(i) *If* $p = 2$*, then Diophantine equation* (1.1) *has at most one positive integer solution* (x, y).

(ii) *Suppose that* $p \mid A$ *or* $\left(\frac{-2A}{p}\right) = -1$*, where p is odd.*

  (a) *If* $(A, p) \equiv (7,1)$ *or* $(7,7) \pmod 8$*, then Diophantine equation* (1.1) *has at most three positive integer solutions* (x, y).

  (b) *Diophantine equation* (1.1) *has at most one positive integer solution* (x, y) *otherwise.*

(iii) *Suppose that* $\left(\frac{-2A}{p}\right) = 1$*, where p is odd.*

  (1) *If* $(A, p) \equiv (1,5)$, $(1,7)$, $(3,3)$, $(5,5)$, $(7,3)$, *or* $(7,5) \pmod 8$*, then Diophantine equation* (1.1) *has at most one positive integer solution* (x, y).

  (2) *If* $(A, p) \equiv (1,1)$, $(3,1)$, $(3,7)$, $(5,1)$, $(5,3)$, *or* $(5,7) \pmod 8$*, then Diophantine equation* (1.1) *has at most two positive integer solutions* (x, y).

  (3) *If* $(A, p) \equiv (1,3)$ *or* $(3,5) \pmod 8$*, then Diophantine equation* (1.1) *has at most three positive integer solutions* (x, y).

  (4) *If* $(A, p) \equiv (7,7) \pmod 8$*, then Diophantine equation* (1.1) *has at most four positive integer solutions* (x, y).

  (5) *If* $(A, p) \equiv (7,1) \pmod 8$*, then Diophantine equation* (1.1) *has at most six positive integer solutions* (x, y).

We also prove the following result.

THEOREM 1.3. *Let p be a prime and let $A > 1$ be an even integer.*

(i) *If* $p = 2$*, then Diophantine equation* (1.1) *has at most two positive integer solutions* (x, y)*. Moreover, if* $A \equiv 0 \pmod 4$ *and* $A \neq 2^6 \cdot 1785$*, then Diophantine equation* (1.1) *has at most one positive integer solution* (x, y).

(ii) *Suppose that* $p \mid A$ *or* $\left(\frac{-2A}{p}\right) = -1$*, where p is odd.*

  (1) *If* $A \equiv 0 \pmod 4$*, then Diophantine equation* (1.1) *has at most one positive integer solution* (x, y).

(2) *If* $A \equiv 2 \pmod 4$*, then Diophantine equation* (1.1) *has at most two positive integer solutions* (x, y)*.*

(iii) *Suppose that* $\left(\frac{-2A}{p}\right) = 1$*, where* p *is odd.*

(1) *If* $(A, p) \equiv (0, 3) \pmod 4$*, then Diophantine equation* (1.1) *has at most one positive integer solution* (x, y)*.*

(2) *If* $(A, p) \equiv (0, 1) \pmod 4$*, then Diophantine equation* (1.1) *has at most two positive integer solutions* (x, y)*.*

(3) *If* $(A, p) \equiv (2, 3) \pmod 4$*, then Diophantine equation* (1.1) *has at most three positive integer solutions* (x, y)*.*

(4) *If* $(A, p) \equiv (2, 1) \pmod 4$*, then Diophantine equation* (1.1) *has at most four positive integer solutions* (x, y)*.*

2. Preliminary results

We present the results required to prove Theorem 1.2 and Theorem 1.3. Recall that if q is a prime number, $\nu_q(m)$ denotes the q-adic valuation of m.

Let a and b be odd positive integers for which the equation $aX^2 - bY^2 = 2$ has a solution in positive integers (X, Y). Let (a_1, b_1) be the minimal positive solution to this equation and define

$$\alpha = \frac{a_1\sqrt{a} + b_1\sqrt{b}}{\sqrt{2}}.$$

For an odd integer k, define a_k and b_k by

$$\alpha^k = \frac{a_k\sqrt{a} + b_k\sqrt{b}}{\sqrt{2}}.$$

Luca and Walsh proved the following result in [**6**] regarding the solutions to the equation

$$aX^2 - bY^4 = 2. \tag{2.1}$$

Theorem 2.1. (1) *If* b_1 *is not a square, then equation* (2.1) *has no solution.*

(2) *If* b_1 *is a square and* b_3 *is not a square, then* $(X, Y) = (a_1, \sqrt{b_1})$ *is the only solution to equation* (2.1)*.*

(3) *If* b_1 *and* b_3 *are both squares, then* $(X, Y) = (a_1, \sqrt{b_1})$ *and* $(a_3, \sqrt{b_3})$ *are the only solutions to equation* (2.1)*.*

Ljunggren proved the following result in [**5**].

Theorem 2.2. *Let* $a > 1$ *and* b *be two positive integers. The equation*

$$aX^2 - bY^4 = 1$$

has at most one solution in positive integers (X, Y)*.*

Let D be a positive non-square integer, and let $\epsilon_D = T_1 + U_1\sqrt{D}$ denote the minimal unit greater than 1, of norm 1, in $\mathbb{Z}[\sqrt{D}]$. Define ${\epsilon_D}^k = T_k + U_k\sqrt{D}$ for $k \geqslant 1$. Togbé, Voutier, and Walsh proved the following result in [**9**].

Theorem 2.3. *Let* D *be a positive non-square integer. There are at most two positive integer solutions* (X, Y) *to the equation* $X^2 - DY^4 = 1$*.*

(1) *If two solutions such that $Y_1 < Y_2$ exist, then ${Y_1}^2 = U_1$ and ${Y_2}^2 = U_2$, except only if $D = 1785$ or $D = 16 \cdot 1785$, in which case ${Y_1}^2 = U_1$ and ${Y_2}^2 = U_4$.*

(2) *If only one positive integer solution (X, Y) to the equation $X^2 - DY^4 = 1$ exists, then $Y^2 = U_\ell$ where $U_1 = \ell v^2$ for some square-free integer ℓ, and either $\ell = 1$, $\ell = 2$, or $\ell = p$ for some prime $p \equiv 3 \pmod 4$.*

We make Theorem 1.2 more precise when D is even.

Lemma 2.1. *Let D be a positive non-square integer. Suppose that $D = 2d$ where d is a positive integer different from $8 \cdot 1785$. Then the equation $X^2 - DY^4 = 1$ has at most one positive solution (X, Y).*

Proof. Suppose that there exist two solutions to the equation $X^2 - DY^4 = 1$. Then there exist positive integer solutions (X_1, Y_1) and (X_2, Y_2) such that $Y_1 < Y_2$. It follows from Theorem 2.3 that ${Y_1}^2 = U_1$, ${Y_2}^2 = U_2$, and $U_2 = 2T_1U_1$, so ${Y_2}^2 = 2T_1{Y_1}^2$. Then

$$2\nu_2(Y_2) = 1 + \nu_2(T_1) + 2\nu_2(Y_1). \tag{2.2}$$

Since $\epsilon_D = T_1 + U_1\sqrt{D}$ is a unit of norm 1 in $\mathbb{Z}[\sqrt{D}]$ and $D = 2d$, we obtain ${T_1}^2 - 2d{U_1}^2 = 1$, so that T_1 is odd. Then $\nu_2(T_1) = 0$, which is a contradiction with (2.2). □

3. Main results

Proof of Theorem 1.2. Let $p = 2$, and let A be an odd positive integer. Let x, y be positive integers such that $y^2 = 2x(Ax^2 + 2)$. It is not difficult to see that 4 divides x and y. Let $y = 4w$ and $x = 4z$. Then we obtain $w^2 = z(8Az^2 + 1)$. Since $\gcd(z, 8Az^2 + 1) = 1$, there exist positive integers u and v such that $z = u^2$, $8Az^2 + 1 = v^2$, and $v^2 - 8Au^4 = 1$. By Lemma 2.1, this equation has at most one positive integer solution (u, v).

Let p be an odd prime, and let A be an odd positive integer. Let x, y be positive integers such that $y^2 = px(Ax^2 + 2)$. We remark that $\gcd(x, Ax^2 + 2) = 1$ or 2, so we consider two cases depending on the parity of x, with each case yielding two equations. Suppose first that x is even, so we let $x = 2z$. Since p is prime, we let $y = 2pw$. Then we obtain $pw^2 = z(2Az^2 + 1)$. Since $\gcd(z, 2Az^2 + 1) = 1$, there exist positive integers u and v such that either $z = pu^2$, $2Az^2 + 1 = v^2$, and

$$v^2 - 2Ap^2u^4 = 1, \tag{3.1}$$

or $z = u^2$, $2Az^2 + 1 = pv^2$, and

$$pv^2 - 2Au^4 = 1. \tag{3.2}$$

Suppose next that x is odd. Since p is prime, we let $y = pw$. Then we obtain

$$pw^2 = x(Ax^2 + 2).$$

Since $\gcd(x, Ax^2 + 2) = 1$, there exist odd integers u and v such that either $x = pu^2$, $Ax^2 + 2 = v^2$, and

$$v^2 - Ap^2u^4 = 2, \tag{3.3}$$

or $x = u^2$, $Ax^2 + 2 = pv^2$, and

$$pv^2 - Au^4 = 2. \tag{3.4}$$

We consider each of the above four equations separately to determine upper bounds for the number of positive integer solutions to equation (1.1).

We begin with equation (3.1). Let $D = 2Ap^2$. By Lemma 2.1, equation (3.1) has at most one positive integer solution.

We next consider equation (3.2), which has at most one positive integer solution by Theorem 2.2. It follows from this equation that v is odd and that u is even if and only if $p \equiv 1 \pmod 8$. If $p \equiv 3, 5$, or $7 \pmod 8$, then u is odd, and we obtain $p - 2A \equiv 1 \pmod 8$. Then equation (3.2) has a solution only if $(A, p) \equiv (1, 1)$, $(3, 1)$, $(5, 1)$, $(7, 1)$, $(1, 3)$, $(5, 3)$, $(3, 7)$, or $(7, 7) \pmod 8$. Furthermore, equation (3.2) has a solution only if $\left(\frac{-2A}{p}\right) = 1$.

Equation (3.3) has at most two positive integer solutions by Theorem 2.1. Since u and v are both odd, we have $1 - A \equiv 2 \pmod 8$ so $A \equiv 7 \pmod 8$ and $v^2 \equiv 2 \pmod p$ so $\left(\frac{2}{p}\right) = 1$. Then $p \equiv 1$ or $7 \pmod 8$, and equation (3.3) has at least one solution only if $(A, p) \equiv (7, 1)$ or $(7, 7) \pmod 8$.

Equation (3.4) has at most two positive integer solutions by Theorem 2.1. Since u and v are odd, we have $p - A \equiv 2 \pmod 8$ so that equation (3.4) has a solution only if $(A, p) \equiv (1, 3)$, $(3, 5)$, $(5, 7)$, or $(7, 1) \pmod 8$. In particular, suppose that equation (3.4) has two solutions, and let (a_1, b_1) be the minimal positive solution of $pX^2 - AY^2 = 2$, so $p{a_1}^2 - A{b_1}^2 = 2$. Let

$$\alpha = \frac{a_1\sqrt{p} + b_1\sqrt{A}}{\sqrt{2}},$$

and compute α^3 to obtain

$$b_3 = \frac{3{a_1}^2pb_1 + {b_1}^3A}{2}.$$

Since we assume that two solutions exist to equation (3.4), b_1 and b_3 must both be squares by Theorem 2.1. It follows that there exist two positive integers B_1 and B_3 such that $b_1 = {B_1}^2$, $b_3 = {B_3}^2$, and

$$3{a_1}^2p{B_1}^2 + {B_1}^6A = 2{B_3}^2.$$

This yields $\left(\frac{2}{p}\right) = \left(\frac{A}{p}\right)$. Since $-Au^4 \equiv 2 \pmod p$, we obtain $\left(\frac{-A}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{A}{p}\right)$ so $\left(\frac{-1}{p}\right) = 1$. It follows that $p \equiv 1 \pmod 4$, so $p \equiv 1$ or $5 \pmod 8$. Therefore equation (3.4) has at most two positive integer solutions only if $(A, p) \equiv (3, 5)$ or $(7, 1) \pmod 8$, and it has at most one positive integer solution only if $(A, p) \equiv (1, 3)$ or $(5, 7) \pmod 8$. Furthermore, equation (3.4) has a solution only if $\left(\frac{-2A}{p}\right) = 1$.

Since the number of solutions to equations (3.2) and (3.4) depends on the value of $\left(\frac{-2A}{p}\right)$, we first suppose that $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$. Then equations (3.2) and (3.4) have no integer solution, equation (3.1) has at most one solution, and equation (3.3) has at most two positive integer solutions only if $(A, p) \equiv (7, 1)$, or $(7, 7) \pmod 8$. Therefore when $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$, equation (1.1) has at most three positive integer solutions if $(A, p) \equiv (7, 1)$, or $(7, 7) \pmod 8$, and it has at most one positive integer solution in all other cases.

We next suppose that $\left(\frac{-2A}{p}\right) = 1$. Then equation (3.2) has at most one positive integer solution.

If $A \equiv 1 \pmod 8$, then equation (3.1) has at most one solution, equation (3.2) has at most one solution and only if $p \equiv 1$ or $3 \pmod 8$, equation (3.3) has no solution, and equation (3.4) has at most one solution and only if $p \equiv 3 \pmod 8$.

If $A \equiv 3 \pmod 8$, then equation (3.1) has at most one solution, equation (3.2) has at most one solution and only if $p \equiv 1$ or $7 \pmod 8$, equation (3.3) has no solution, and equation (3.4) has at most two solutions and only if $p \equiv 5 \pmod 8$.

If $A \equiv 5 \pmod 8$, then equation (3.1) has at most one solution, equation (3.2) has at most one solution and only if $p \equiv 1$ or $3 \pmod 8$, equation (3.3) has no solution, and equation (3.4) has at most one solution and only if $p \equiv 7 \pmod 8$.

If $A \equiv 7 \pmod 8$, then equation (3.1) has at most one solution, equation (3.2) has at most one solution and only if $p \equiv 1$ or $7 \pmod 8$, equation (3.3) has at most two solutions and only if $p \equiv 1$ or $7 \pmod 8$, and equation (3.4) has at most tow solutions and only if $p \equiv 1 \pmod 8$. □

Proof of Theorem 1.3. If A is even and p is odd, we let $A = 2A'$. Then $y^2 = 2px(A'x^2 + 1)$. We let $y = 2pw$, and we obtain $2pw^2 = x(A'x^2 + 1)$. Since $\gcd(x, A'x^2+1) = 1$, there exist positive integers u and v such that either $x = 2pu^2$, $A'x^2 + 1 = v^2$, and

$$v^2 - 4A'p^2u^4 = 1, \tag{3.5}$$

or $x = 2u^2$, $A'x^2 + 1 = pv^2$ and

$$pv^2 - 4A'u^4 = 1, \tag{3.6}$$

or $x = u^2$, $A'x^2 + 1 = 2pv^2$ and

$$2pv^2 - A'u^4 = 1, \tag{3.7}$$

or $x = pu^2$, $A'x^2 + 1 = 2v^2$ and

$$2v^2 - A'p^2u^4 = 1. \tag{3.8}$$

If A' is a perfect square, then equation (3.5) has no positive integer solution, otherwise it has at most one positive integer solution by Lemma 2.1.

By Theorem 2.2, each of equations (3.6), (3.7), and (3.8) has at most one solution. Equation (3.6) has a solution only if $p \equiv 1 \pmod 4$ and $\left(\frac{-A'}{p}\right) = 1$, equation (3.7) has a solution only if A' is odd and $\left(\frac{-A'}{p}\right) = 1$, and equation (3.8) has a solution only if A' is odd. Since the number of solutions to equations (3.6) and (3.7) depends on the value of $\left(\frac{-A'}{p}\right) = \left(\frac{-2A}{p}\right)$, we first suppose that $p \mid A$ or $\left(\frac{-2A}{p}\right) = -1$. Then equations (3.6) and (3.7) have no integer solution.

If $A \equiv 0 \pmod 4$, then equation (3.5) has at most one solution, equation (3.6) has no solution, equation (3.7) has no solution, and equation (3.8) has no solution.

If $A \equiv 2 \pmod 4$, then equation (3.5) has at most one solution, equation (3.6) has no solution, equation (3.7) has no solution, and equation (3.8) has at most one solution.

We now suppose that $\left(\frac{-2A}{p}\right) = 1$. Then equations (3.6) and (3.7) have at most one positive integer solution.

If $A \equiv 0 \pmod 4$, then equation (3.5) has at most one solution, equation (3.6) has at most one solution only if $p \equiv 1 \pmod 4$, equation (3.7) has no solution, and equation (3.8) has no solution.

If $A \equiv 2 \pmod 4$, then equation (3.5) has at most one solution, equation (3.6) has at most one solution only if $p \equiv 1 \pmod 4$, equation (3.7) has at most one solution, and equation (3.8) has at most one solution.

If A is even and $p = 2$, we let $A = 2A'$. Then $y^2 = 2x(2A'x^2+2)$. We let $y = 2w$, and we obtain $w^2 = x(A'x^2+1)$. Since $\gcd(x, A'x^2+1) = 1$, there exist positive integers u and v such that $x = u^2$, $A'x^2+1 = v^2$, and

$$v^2 - A'u^4 = 1, \tag{3.9}$$

which has no solution if A' is a perfect square and at most two solutions by Theorem 2.3. Moreover, if A' is even and $A' \neq 2^5 \cdot 1785$, then by Lemma 2.1 equation (3.9) has at most one solution. □

Remark 3.1. When we had finished writing the paper, we noticed that a proof of the result stated in Lemma 2.1 already existed within the proof of Theorem 1 by Luca and Walsh in [**7**]. Our proof of Lemma 2.1 seems to be different from the proof of the result in [**7**].

Remark 3.2. Theorem 1.2 implies that Conjecture 1.1 is true if $(A,p) \equiv (1,5)$, $(1,7)$, $(3,3)$, $(3,5)$, $(5,3)$, $(7,3)$, or $(7,5) \pmod 8$.

Acknowledgment. The authors express their gratitude to the anonymous referee for constructive suggestions which improved the quality of the paper. The second author was supported in part by NSERC.

References

1. S. Akhtari, *The Diophantine equation $aX^4 - bY^2 = 1$*, J. Reine Angew. Math. **630** (2009), 33–57.
2. J. W. S. Cassels, *A Diophantine equation*, Glasg. Math. J. **27** (1985), 11–18.
3. L. M. Chen, *On the Diophantine equation $y^2 = px(x^2+2)$*, Acta Math. Sin., Chin. Ser. **50**(1) (2010), 83–86.
4. J. H. Chen, 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.
5. W. Ljunggren, *Ein Satz über die Diophantische Gleichung $Ax^2 - By^4 = C (C = 1, 2, 4)$*, in: *Tolfte Skandinaviska Matematikerkongressen*, Lunds Universitets Matematiska Inst., Lund, 1954, 188–194.
6. F. Luca, P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. **100** (2001), 47–62.
7. ———, *On a Diophantine equation of Cassels*, Glasg. Math. J. **47** (2005), 303–307.
8. A. Togbé, *A note on the Diophantine equation $y^2 = px(Ax^2+2)$*, Afr. Mat. **25**(3) (2014), 739–744.

9. A. Togbé, P. M. Voutier, P. G. Walsh, *Solving a family of Thue equations with an application to the equation $x^2 - dy^4 = 1$*, Acta Arith. **120** (2005), 39–58.
10. P. Yuan, *Rational and algebraic approximations of algebraic numbers and their applications*, Sci. China, Ser. A **40** (1997), 1045–1051.
11. P. Yuan, Y. Li, *Squares in Lehmer sequences and the Diophantine equation $Ax^4 - By^2 = 2$*, Acta Arith. **139** (2009), 275–302.

(Received 07 04 2016)

Department of Mathematics
USTHB
Algiers
Algeria
tgarici@usthb.dz

Department of Mathematics
Brock University
St. Catharines
Canada
okihel@brocku.ca

Département de mathématiques et de statisiques
Université Laval
Québec
Canada
jesse.larone.1@ulaval.ca