Publ. Math. Debrecen
57 / 3-4 (2000), 535–545

Full powers in arithmetic progressions

By I. PINK (Debrecen) and SZ. TENGELY (Debrecen)

Dedicated to Professor Kálmán Győry on his 60th birthday

Abstract. For given positive integers a and n, we consider the three-term arithmetic progressions a^2, y^n, x^2, where x and y are unknown integers. We give explicit upper bounds both for the number of such arithmetic progressions and for $\max\{|x|,|y|\}$. Moreover, we find all such progressions with $1 \le a \le 1000$, and $3 \le n \le 80$.

1. Introduction

Let a and n be given integers with $a > 0$ and $n \ge 3$. In this paper we investigate the arithmetic progressions a^2, y^n, x^2, where x, y are coprime positive integers. Clearly, these three terms form an arithmetic progression if and only if (x, y) is a solution to the equation

$$(1) \qquad x^2 + a^2 = 2y^n, \quad \text{in } x, y \in \mathbb{N} \text{ with } \gcd(x, y) = 1.$$

Note that if a is also considered as a variable, then (1) has infinitely many solutions. There are many results in the literature concerning similar equations. In the case $n = 4$ equations of the form

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

Mathematics Subject Classification: 11D61.
Key words and phrases: exponential diophantine equation, full powers, arithmetic progression.
The second author was supported in part by the Universitas Foundation of Kereskedelmi Bank RT.

are of particular interest, cf. [3], [14], [21], [24], [28], [30], [32], [33]. There are also a lot of interesting papers dealing with equations of the form

$$aX^2 + b = cY^n,$$

we refer to [10], [12], [13], [18], [19], [22], [23], [25], [31].

Equation (1) is a special hyperelliptic equation. In 1969, Baker [2] gave an explicit bound for the solutions of hyperelliptic equations, i.e. of equations of type

$$f(x) = by^n \quad \text{in } x, y \in \mathbb{Z}, \tag{2}$$

where f is a polynomial with integer coefficients and non-zero discriminant, and b and n are given positive integers with $n \geq 2$. This result of Baker was improved and generalized by several authors, see e.g. [8] and the references given there. Moreover, in 1998 Bilu and Hanrot (see [5]) gave an algorithm for the practical solution of hyperelliptic equations.

On the other hand, it is possible to derive in (2) an upper bound for the exponent n in terms of f and b. The first result in this direction was obtained in [27]. This result also was improved and generalized, see e.g. [4] or [7] and the references given there.

In our paper we give an upper bound for $\max\{|x|, |y|\}$ (cf. Theorem 1), where (x, y) is an arbitrary solution to (1). Using the special form of our hyperelliptic equation, our bound will be much sharper than those provided by the general estimates. Further, we provide an algorithm for the practical solution of equations of type (1). This algorithm in this special case is much more efficient than that of Bilu and Hanrot [5]. In the last section, we use our algorithm to give a complete list of solutions of equation (1) for the ranges $1 \leq a \leq 1000$ and $3 \leq n \leq 80$. We also derive an upper bound for n (see also Theorem 1), by specializing an estimate of Bugeaud and Hajdu [9] to (1). Finally, we give an explicit upper bound for the number of solutions of (1), too (cf. Theorem 2).

2. Results

The following theorem provides an upper bound for the solutions of (1). Moreover, an estimate for n is also given.

Theorem 1. *Consider the diophantine equation*

(1) $$x^2 + a^2 = 2y^n, \quad \text{in } x, y \in \mathbb{N} \quad \text{with } \gcd(x,y) = 1,$$

where a and n are given positive integers with $n \geq 3$. Then the following inequalities hold.

(i) *If n is a power of 2 then*

$$\max\{x^2, y^n\} < 2^8 \cdot (45a)^{10^{64}}.$$

(ii) *If n is not a power of 2 and p denotes the smallest odd prime divisor of n, then*

$$\max\{x^2, y^n\} < 2 \cdot 3^p a^{2p(p-1)}.$$

(iii) *We have in both cases*

$$n \leq 2^{91} \cdot 5^{27} \cdot a^{10}.$$

As was mentioned above, (i) and (ii) of Theorem 1 give better bounds than the best known general bonds for (2).

It follows from a general theorem of Evertse and Silverman [15] concerning the number of solutions of (2), that our equation (1) has at most $17^{16}n^8$ solutions. Using our approach, we prove Theorem 2 below. We denote by $d(a)$ the number of positive divisors of a, and by $\omega(a)$ the number of distinct prime divisors of a.

Theorem 2. *If p denotes the smallest odd prime divisor of n, then the number of solutions of (1) is at most*

$$2(p-1)d(a).$$

Further, if n is a power of 2 then this number is at most

$$2800 \cdot 4^{\omega(a)+1}.$$

Our bounds are better than that of [15] when $d(a)$ and $\omega(a)$ are small.

Remark. It follows from the proof of Theorem 1 that this theorem is valid also for the more general equation

$$x^2 + z^2 = 2y^n \quad \text{in } x, y, z \in \mathbb{N},$$

with $\gcd(x,y) = 1$, $|z| \leq a$, where a and $n \geq 3$ are given positive integers. Further, Theorem 1 of Győry [16] concerning Thue inequalities implies that if n is a power of 2 then the number of solutions with $|x| \geq 3 \cdot 10^9 a^{\frac{9}{4}}$ is at most 100.

3. Proofs

To prove Theorem 1, we need some lemmas. Let $n \geq 3$ be an integer, and denote by $F_r(u,v)$ the real part of the polynomial $i^r(1+i)(u+iv)^n$ in u, v for $r=0,1,2,3$. Further, let $F_{-1}(u,v)=F_3(u,v)$. It is clear that $F_r(u,v)$ is a homogeneous polynomial in $\mathbb{Z}[u,v]$.

Lemma 1. *The pair $x,y \in \mathbb{Z}$ with $y>0$, $\gcd(a,x)=1$ is a solution to (1) if and only if there exist integers u, v such that for some $r \in \{0,1,2,3\}$,*

$$a = F_r(u,v), \quad x = F_{r-1}(u,v), \quad y = u^2+v^2. \tag{3}$$

Proof. This lemma can be easily proven by means of Gaussian integers; see e.g. [26] or [31]. $\square$

Lemma 2. *Let n and $F_r(u,v)$ be as in Lemma 1. If n is odd then in $\mathbb{Z}[u,v]$ we have*

$$(u+(-1)^r v) \mid F_r(u,v), \quad \text{if } n \equiv -1 \pmod 4$$
$$(u-(-1)^r v) \mid F_r(u,v), \quad \text{if } n \equiv 1 \pmod 4.$$

Proof. If $n \equiv 1 \pmod 4$ then

$$\begin{aligned} F_r((-1)^r v, v) &= \frac{i^r(1+i)((-1)^r v+iv)^n + (-i)^r(1-i)((-1)^r v - iv)^n}{2} \\ &= i^r(1+i)((-1)^r+i)^n v \left(\frac{1+(-1)^{n(r+1)+r}}{2}\right) = 0, \end{aligned}$$

since $n(r+1)+r$ is odd. Hence it follows that $(u-(-1)^r v)|F_r(u,v)$. The proof of the other case is similar. $\square$

The following lemma which is due to Bugeaud and Győry [11] provides an upper bound for the solutions of Thue equations. Throughout the paper we write $\log^* a$ for $\max\{\log a, 1\}$.

Lemma 3. *Let $F \in \mathbb{Z}[X,Y]$ be an irreducible binary form of degree $n \geq 3$, and let b be a non-zero integer. Then all solutions of the equation*

$$F(x,y) = b \quad \text{in } x,y \in \mathbb{Z}$$

satisfy

$$\max\{|x|,|y|\} < \exp\{cR(\log^* R)(R+\log(H\cdot|b|))\},$$

where $c = 3^{r+27}\cdot n^{2n+13r+33}$ *and* r, R *denote the unit rank and the regulator of the field* $\mathbb{Q}(\alpha)$, *where* α *is a zero of* $F(x,1)$, *and* H *is the maximum of the absolute values of the coefficients of* F.

Finally, we use the following result of Bugeaud and Hajdu [9] to derive an upper bound for n in (1).

Lemma 4. *Let* a *and* k *be non-zero integers and put* $f(x) = ax^m - k$. *Let* b *denote a non-zero integer and* n *a positive integer. Using the previous notation, the equation*

$$f(x) = by^n$$

in integers x, y *with* $|y| > 2$ *implies*

$$n \le 20^{5m+17} m^{5m+27} |ak|^{\frac{5m}{2}} (\log^* |b|)^{\frac{7}{3}}.$$

Proof of Theorem 1. (i) If $n = 2^m$, $m \ge 2$ then we have

$$x^2 + a^2 = 2z^4,$$

where $z = y^{2^{m-2}}$. For the binary forms defined in Lemma 1, we get

$$\begin{aligned}
F_0(u,v) &= u^4 - 4u^3v - 6u^2v^2 + 4uv^3 + v^4\\
F_1(u,v) &= -F_0(u,-v)\\
F_2(u,v) &= -F_0(u,v)\\
F_3(u,v) &= F_0(u,-v).
\end{aligned}$$

It is easy to see that F_0, F_1, F_2 and F_3 are irreducible over $\mathbb{Q}$. According to (3), to obtain an upper bound for $\max\{|x|,|z|\}$ it is sufficient to derive an upper bound for the solutions u, v of the quartic Thue equation

$$F_0(u,v) = \pm a.$$

We note that for $a = \pm 1$ and $a = \pm 4$, this equation was completely solved earlier by Lettl and Pethő in [20]. Using the notation of Lemma 3, we have

$$R \le 2.4418, \quad r = 3,\ n = 4,\ H = 6,$$

and by (4) we get

$$\max\{|u|,|v|\} \leq (45a)^{2^{160}\cdot 3^{31}}.$$

This implies that

$$x^2 \leq \left(16\left((45a)^{2^{160}\cdot 3^{31}}\right)^4\right)^2,$$

and

$$y^n \leq 16(45a)^{2^{163}\cdot 3^{31}},$$

which prove (i).

(ii) Let now a, n be given positive integers with $n > 1$, and suppose that n is not a power of 2. If p is the smallest odd prime dividing n, then (1) can be written in the form

$$x^2 + a^2 = 2(y^{\frac{n}{p}})^p.$$

Applying Lemma 1, we get

$$a = F_r(u,v), \quad x = F_{r-1}(u,v), \quad y^{\frac{n}{p}} = u^2 + v^2, \tag{5}$$

where $r \in \{0,1,2,3\}$ and u, v are integers. By Lemma 2 we deduce that the polynomial $F_r(u,v)$ is divisible by $u+v$ or $u-v$. Hence $a = F_r(u,v)$ implies that for some integer a_0 with $a_0 \mid a$ we have $u = a_0 \pm v$. Further, $(F(a_0 \pm v, v) - a)/a_0$ is a polynomial in v with integral coefficients whose constant term in absolute value is at most $a^{p-1}+1$. Thus we infer that

$$|v| \leq a^{p-1}+1 \quad \text{and so} \quad |u| \leq a^{p-1}+a+1.$$

Finally, it follows that

$$y^{n/p} = u^2 + v^2 \leq 2a^{2(p-1)} + 2a^p + 4a^{p-1} + a^2 + 2a + 2 \leq 3a^{2(p-1)},$$

and the assertion is proved.

(iii) Applying Lemma 4 to (1) we obtain

$$n \leq 2^{91}5^{27}a^{10}. \qquad \square$$

Proof of Theorem 2. First consider the case when n is not a power of 2. We follow a similar argument as in part (ii) of the proof of Theorem 1.

Denote by p the smallest odd prime divisor of n. It is clear that it sufficies to give a bound for the number of solutions in the particular case when $n = p$ is an odd prime.

First suppose that $n \equiv 1 \pmod 4$. The case $n \equiv -1 \pmod 4$ can be treated similarly. Denote by $F_r(u, v)$ the binary form in $\mathbb{Z}[u, v]$ defined above. By Lemma 2 it follows that

$$(u - (-1)^r v) \mid F_r(u, v) \quad \text{in } \mathbb{Z}.$$

Let x, y be an arbitrary but fixed solution of (1). Then Lemma 1 implies that $a = F_r(u, v)$ and $x = F_{r-1}(u, v)$ for some $r \in \{0, 1, 2, 3\}$ and some $u, v \in \mathbb{Z}$. Hence, by Lemma 2, we have $u - (-1)^r v \mid a$ in $\mathbb{Z}$. Further, it follows from Lemma 2 that there is a homogeneous polynomial $F(u, v)$ in $\mathbb{Z}[u, v]$ with $\deg F = p - 1$ such that $F_r(u, v) = (u - (-1)^r v)F(u, v)$ in $\mathbb{Z}[u, v]$. Hence, for the above $u, v \in \mathbb{Z}$ we obtain that $u - (-1)^r v = a_0$, and so

$$a = a_0 F(a_0 + (-1)^r v, v). \tag{6}$$

The possible values of a_0 is $2d(a)$. Further, for fixed a_0 equation (6) has at most $p - 1$ solutions in v. Thus equation (1) has at most $2(p - 1)d(a)$ solutions.

Next consider the case when n is a power of 2. Then we may assume that $n = 4$. Let again x, y be an arbitrary but fixed solution of (1). Then

$$a = F_r(u, v), \tag{7}$$

and $x = F_{r-1}(u, v)$ for some $r \in \{0, 1, 2, 3\}$ and some u, v, where F_r is a quartic binary form in $\mathbb{Z}[u, v]$. We have seen above that F_r is irreducible over $\mathbb{Q}$. Equation (7) is a quartic Thue equation. We can now apply a well-known theorem of Bombieri and Schmidt [6] on the number of solutions of Thue equations and we get that the number of solutions of (7) in $u, v \in \mathbb{Z}$ is at most $C4^{\omega(a)+1}$, where C is an absolute constant. Further, by a theorem of Stewart [29] one may take $C = 2800$. This gives immediately that in this case equation (1) has at most $2800 \cdot 4^{\omega(a)+1}$ solutions. $\square$

4. Numerical results

In this section we list all solutions of equation (1), with $3 \leq n \leq 80$ and $1 \leq a \leq 1000$. We used the method applied in the proof of our Theorem 1 to obtain these results. Namely, we reduced equation (1) in each concrete case to a quartic or to a reducible Thue equation, according as n is a power of 2 or not. In the first case we used the program package Kant [17] to solve the Thue equation in question. In the reducible case we reduced the Thue equation to systems of equations of lower degree and utilized elimination theory to find the solutions.

As $(a, x, y) = (1, 1, 1)$ is a trivial solution for all n, we will indicate only those values of n for which there are other solutions, too.

a	x	y
1	1	1
5	99	17
9	13	5
13	9	5
19	5291	241
27	545	53
37	55	13
55	37	13
71	275561	3361
73	161	25
77	207	29
91	305	37
99	5	17
99	27607	725
121	351	41
143	1099	85
143	1603	109
161	73	25
181	649	61
207	77	29
253	845	73

a	x	y
253	1079	85
253	9217	349
265	14325849	46817
297	679	65
305	91	37
337	1665	113
351	121	41
369	1432283	10085
377	18989	565
391	3537	185
433	2431	145
481	1917	125
517	531	65
517	79623	1469
531	517	65
541	3401	181
545	27	53
559	61525	1237
585	2191	137
611	1205	97
629	4103	205

a	x	y
649	181	61
661	4599	221
671	1269	101
679	297	65
693	7501	305
747	923	89
793	6049	265
819	6611	281
845	253	73
851	38493	905
923	747	89
935	472213	4813
937	7775	313
989	744675931	652081

The case $n = 3$

a	x	y
1	1	1
1	239	13
17	31	5
31	17	5
79	401	17
191	863	25
239	1	13
241	1921	37
401	79	17
799	881	29
863	191	25
881	799	29
911	10177	85

The case $n = 4$

a	x	y
1	1	1
3	79	5
79	3	5
475	719	13
719	475	13

The case $n = 5$

a	x	y
1	1	1
73	161	5
161	73	5

The case $n = 6$

a	x	y
1	1	1
249	307	5
307	249	5

The case $n = 7$

a	x	y
1	1	1
191	863	5
863	191	5

The case $n = 8$

a	x	y
1	1	1
481	1917	5

The case $n = 9$

Remark. We note that the case $n = 4$ with $a = 1$ was earlier solved by Ljunggren [21].

Acknowledgements. The authors are grateful to Professors Kálmán Győry, Lajos Hajdu, Attila Pethő and the referee for their valuable remarks and suggestions.

References

[1] A. Baker, Contributions to the theory of diophantine equations, *Phil. Trans. Roy. Soc. London* **A 263** (1968), 173–208.

[2] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439–444.

[3] M. A. Bennett and P. G. Walsh, The diophantine equation $b^2X^4 - dY^2 = 1$, *Proc. Amer. Math. Soc.* **127** (1999), 3481–3491.

[4] A. Bérczes, B. Brindza and L. Hajdu, On power values of polynomials, *Publ. Math. Debrecen* **53** (1998), 375–381.

[5] Y. F. Bilu and G. Hanrot, Solving superelliptic Diophantine equations by Baker's method, *Composito Math.* **112** (1998), 273–312.

[6] E. Bombieri and W. M. Schmidt, On Thue's equation, *Invent. Math.* **88** (1987), 69–81.

[7] B. Brindza, K. Győry and J. H. Evertse, Bounds for the solutions of some Diophantine equations in terms of discriminant, *J. Austral. Math. Soc. Ser. A* **51** (1991), 8–26.

[8] Y. Bugeaud, Bounds for the solutions of superelliptic equations, *Compositio Math.* **107** (1997), 187–219.

[9] Y. Bugeaud and L. Hajdu, Lower bounds for the difference $ax^n - by^m$, (*to appear*).

[10] Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan-Nagell equation, (*to appear*).

[11] Y. Bugeaud and K. Győry, Bounds for the solutions of Thue-Mahler equations and norm form equations, *Acta Arith.* **74** (1996), 273–292.

[12] M. Cipu, Bounds for the solutions of the Diophantine equation $D_1x^2 + D_2^m = 4y^n$, (*to appear*).

[13] J. H. E. Cohn, The diophantine equation $x^2 + C = y^n$, *Acta Arith.* **65** (1993), 367–381.

[14] J. Dawe and M. Lal, Solutions of the diophantine equation $x^2 - Dy^4 = k$, *Math. Comp.* **22** (1968), 679–682.

[15] J. H. Evertse and J. H. Silverman, Uniform bounds for the number of solutions to $Y^n = f(x)$, *Math. Proc. Camb. Phil. Soc.* **100** (1986), 237–248.

[16] K. Győry, Thue inequalities with a small number of primitive solutions, (*to appear*).

[17] Kant-Group, KASH Reference Manual, *Technische Universität Berlin* (1995).

[18] M.-H. Le, Some Exponential Diophantine Equations, I: The Equation $D_1x^2 - D_2y^2 = \lambda k^z$, *J. Number Th.* **55** (1995), 209–221.

[19] M.-H. Le, On the Diophantine Equation $D_1x^2 + D_2^m = 4y^n$, *Mh. Math.* **120** (1995), 121–125.

[20] G. Lettl and A. Pethő, Complete Solution of a Family of Quartic Thue Equations, *Abh. Math. Sem. Univ. Hamburg* **65** (1995), 365–383.

[21] W. Ljunggren, Zur Theorie der Gleichung $x^2+1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo* **5** (1942).

[22] W. Ljunggren, On the diophantine equation $Cx^2 + D = y^n$, *Pacific. J. Math.* **14** (1964), 585–596.

[23] W. Ljunggren, On the diophantine equation $Cx^2 + D = 2y^n$, *Math. Scand.* **18** (1966), 69–86.

[24] W. Ljunggren, On the Diophantine equation $Ax^4 - By^2 = C$ $(C = 1, 4)$, *Math. Scand.* **21** (1967), 149–158.

[25] F. Luca, On the Equation $x^2 + 2^a \cdot 3^b = y^n$ (*to appear*).

[26] L. J. Mordell, Diophantine equations, *Academic Press*, 1969.

[27] A. Schinzel and R. Tijdeman, On the equations $y^m = P(x)$, *Acta Arith.* **31** (1976), 199–204.

[28] R. Steiner and N. Tzanakis, Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$, *J. Number Theory* **37** (1991), 123–132.

[29] C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations, *J. Amer. Math. Soc.* **4** (1991), 793–835.

[30] N. Tzanakis, On the Diophantine equation $x^2 - Dy^4 = k$, *Acta Arith.* **46** (1986), 257–269.

[31] P. Yuan and J. Wang, On the diophantine equation $x^2 + b^y = c^z$, *Acta Arith.* **84** (1998), 145–147.

[32] P. G. Walsh, A note on Ljunggren's theorem about the Diophantine equation $aX^2 - bY^4 = 1$, *C. R. Math. Acad. Sci. Soc. R. Can.* **20** (1998), 113–118.

[33] P. G. Walsh, Diophantine equations of the form $aX^4 - bY^2 = \pm 1$, (*to appear*).

I. PINK
INSTITUTE OF MATHEMATICS AND INFORMATICS
UNIVERSITY OF DEBRECEN
H–4010, DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: pinki@math.klte.hu

SZ. TENGELY
INSTITUTE OF MATHEMATICS AND INFORMATICS
UNIVERSITY OF DEBRECEN
H–4010, DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: tengely@math.klte.hu

(Received April 5, 2000)