Publ. Math. Debrecen
65/1-2 (2004), 205–213

On the diophantine equation $x^2 + ({p_1}^{z_1} \dots {p_s}^{z_s})^2 = 2y^n$

By ISTVÁN PINK (Debrecen)

Abstract. We give an explicit upper bound for the exponent n in the title equation which depends only on $\max p_i$ and s.

1. Introduction

There are many special results concerning equations of the form

$$Ax^2 + p_1^{z_1} \dots p_s^{z_s} = By^n,$$

where A, B are positive integers, $p_1, \dots, p_s$ are distinct primes and $x, y, z_1, \dots, z_s$ are unknown non-negative integers, see e.g. [1]–[7], [9], [10], [12]–[18] and the references given there. For fixed a, PINK and TENGELY [19] dealt with the equation

$$x^2 + a^2 = 2y^n \tag{1}$$

in $x, y \in \mathbb{N}$ and $n \geq 3$ with $\gcd(x, y) = 1$, and gave an explicit upper bound for the exponent n depending only on a. In the case when n is a prime, this bound has been recently improved by TENGELY [21]. The purpose of this paper is to generalize these results of [19] and [21] to the case when

---

Mathematics Subject Classification: 11D41, 11D61.
Key words and phrases: exponential diophantine equation, perfect powers, Baker's method.
Research supported in part by the Netherlands Organization for Scientific Research (NWO), by grant F034981 of the Hungarian National Foundation for Scientific Research and by the FKFP grant 3272-13/066/2001.

$a = {p_1}^{z_1} \dots {p_s}^{z_s}$, where $p_1, \dots, p_s$ are given primes and $z_1, \dots, z_s$ are also unknown non-negative integers.

2. New results

Let $p_1, \dots, p_s$ be distinct primes. As a generalization of (1), consider the equation

$$x^2 + ({p_1}^{z_1} \dots {p_s}^{z_s})^2 = 2y^n \tag{2}$$

in $x, y \in \mathbb{N}$, $n \geq 3$ and $z_1, \dots, z_s \in \mathbb{Z}_{\geq 0}$, where $\gcd(x, y) = 1$. It is clear that $x = y = 1$, $z_1 = \dots = z_s = 0$ is always a solution which will be called *trivial*. Put $P = \max\{p_1, \dots, p_s\}$. It follows from Theorem 2 of [20] that apart from the trivial solution, in (2) $n \leq C(P, s)$ holds with an effectively computable constant C depending only on P and s. We make this constant C explicit, and prove the following generalization of Theorem 1 of [19] and Theorem 1 of [21].

Theorem. *For every non-trivial solution of* (2) *with n odd, we have*

$$n \leq 90813 \quad \textit{if} \quad (P, s) = (3, 1),$$

and

$$n < 5371sP(P + 1)\log P$$

otherwise.

3. Auxiliary results

We use $h(\alpha)$ for the absolute logarithmic height of the algebraic number α. Recall that if $a_0(X - \alpha_1)\cdots(X - \alpha_D)$ is the minimal defining polynomial of $\alpha = \alpha_1$ over $\mathbb{Z}$, then $h(\alpha)$ is defined by

$$h(\alpha) = \frac{1}{D}\log\left(|a_0|\prod_{i=1}^{D}\max(|\alpha_i|, 1)\right).$$

Similarly as in the papers [9] and [10], we shall combine in our proof the best known estimates for linear forms in two logarithms in the complex and in the p-adic case.

Lemma 1. *Let α be a complex algebraic number with $|\alpha| = 1$, but not a root of unity, and $\log \alpha$ the principal value of the logarithm (that is, $-\pi < \operatorname{Im} \log \alpha \leq \pi$). Consider the linear form*

$$\Lambda = b_1 i\pi - b_2 \log \alpha$$

with positive integers coefficients b_1 and b_2. Let λ be a real number with $1.8 \leq \lambda < 4$, and put

$$D = [\mathbb{Q}(\alpha) : \mathbb{Q}]/2,$$

$$\rho = e^{\lambda}, \quad K = 0.5\rho\pi + Dh(\alpha), \quad B = \max(13, b_1, b_2),$$

$$t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1 + 2\pi\rho/3\lambda)}, \quad k = \left(\frac{1/3 + \sqrt{1/9 + 2\lambda t}}{\lambda} \right)^2,$$

$$H = \max\left\{ 3\lambda, D\left(\log B + \log\left(\frac{1}{\pi\rho} + \frac{1}{2K} \right) - \log\sqrt{k} + 0.886 \right) \right.$$
$$\left. + \frac{3\lambda}{2} + \frac{1}{k}\left(\frac{1}{6\pi\rho} + \frac{1}{3K} \right) + 0.023 \right\}.$$

Then

$$\log|\Lambda| > -(8\pi k\rho\lambda^{-1}H^2 + 0.23)K - 2H - 2\log H$$
$$+ 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

Proof. This is Theorem A.1.3 of [8]; its proof is due to Mignotte. □

For any prime p, let $\overline{\mathbb{Q}}_p$ be an algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers. We denote by v_p the unique extension to $\overline{\mathbb{Q}}_p$ of the standard p-adic valuation over $\mathbb{Q}_p$, normalized by $v_p(p) = 1$.

Lemma 2. *Let p be a prime number. Let α_1 and α_2 be two algebraic numbers which are p-adic units. Denote by f the residual degree of the extension $\mathbb{Q}_p \hookrightarrow \mathbb{Q}_p(\alpha_1, \alpha_2)$ and put $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/f$. Let b_1 and b_2 be two positive integers and put*

$$\Lambda = {\alpha_1}^{b_1} - {\alpha_2}^{b_2}.$$

Denote by $A_1 > 1$ *and* $A_2 > 1$ *two real numbers such that*

$$\log A_i \geq \max\{h(\alpha_i),\ \log p/D\}, \quad i = 1, 2$$

and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 *and* α_2 *are multiplicatively independent, then we have*

$$v_p(\Lambda) \leq \frac{24p(p^f - 1)}{(p-1)(\log p)^4} D^4 \left(\max\left\{\log b' + \log\log p + 0.4,\ \frac{10\log p}{D},\ 5\right\}\right)^2 \times \log A_1 \log A_2.$$

Proof. This is Théorème 4 of Bugeaud and Laurent [11] with the choice $(\mu, \nu) = (10, 5)$. $\square$

4. Proof of the theorem

Proof. Without loss of generality we may assume that $\min\{p_1, \dots, p_s\} \geq 3$. Otherwise, if $p_i = 2$ and $z_i \geq 1$ for some $i \in \{1, 2, \dots, s\}$, then by (2) x must be even. Now, since y is odd, the right-hand side of (2) is congruent to 2 mod 4 and the left-hand side is congruent to 0 mod 4, so we get a contradiction.

Put $a = {p_1}^{z_1} \dots {p_s}^{z_s}$. Since $\mathbb{Z}[i]$ is a unique factorization domain, equation (2) leads to

$$x + ai = i^r(1+i)(u+iv)^n, \quad x - ai = (-i)^r(1-i)(u-iv)^n, \qquad y = u^2 + v^2, \tag{3}$$

where $r \in \{0, 1, 2, 3\}$ and $u, v \in \mathbb{Z}$. This implies that here $uv = 0$ and $u = \pm v$ cannot hold. In the opposite case $y = u^2, v^2$ or $2u^2$, whence $u^n \mid 2ai$ or $v^n \mid 2ai$ would follow in $\mathbb{Z}[i]$. This would yield $x = y = 1$, which leads to the trivial solution. Consequently, $y = u^2 + v^2$ implies that $y \geq 5$.

First suppose that

$$a \leq y^{\frac{n}{3.128}}. \tag{4}$$

Using (4) we get that

$$\left|\frac{x+ai}{x-ai} - 1\right| = \frac{2a}{\sqrt{2}y^{n/2}} < \sqrt{2}y^{-\frac{n}{5.547}}. \tag{5}$$

and, by (3),

$$\left|\frac{x+ai}{x-ai} - 1\right| = \left|(-1)^r i\left(\frac{u+iv}{u-iv}\right)^n - 1\right| = \left|\left(\frac{\pm(v-iu)}{u-iv}\right)^n - 1\right| \tag{6}$$

follows, where we used that for n odd i or $-i$ is an n-th power.

It is easy to see that $\frac{x+ai}{x-ai}$ can be a root of unity only if $x = y = 1$. Hence $\frac{\pm(v-iu)}{u-iv}$ is not a root of unity. But (5) and $y \geq 5$ imply that for $n \geq 6$, $\left|\frac{x+ai}{x-ai} - 1\right| \leq \frac{1}{3}$. Since for every $z \in \mathbb{C}$ with $|z-1| \leq \frac{1}{3}$ we have $|z-1| \geq \frac{1}{2}|\log z|$, we deduce from (5) and (6) that

$$\sqrt{2}y^{-\frac{n}{5.547}} > \frac{1}{2}\left|2m\pi i + n\log\left(\frac{\pm(v-iu)}{u-iv}\right)\right|, \tag{7}$$

where m is an integer with $|2m| \leq n$ and log denotes the principal value of the logarithm. Now we apply Lemma 1. Choose $\alpha = \left(\frac{\pm(v-iu)}{u-iv}\right)^{-1}$, $b_1 = 2m$, $b_2 = n$, if $m \geq 0$, and $\alpha = \frac{\pm(v-iu)}{u-iv}$, $b_1 = 2m$, $b_2 = n$, if $m < 0$. It is clear that $|\alpha| = 1$. Further, it is easy to check that $h(\alpha) = \frac{1}{2}\log y$. Putting $\lambda = 1.8$ and $D = 1$, and using the notation of Lemma 1, for $n \geq 230$ we get $K < 9.503 + \frac{1}{2}\log y$ and

$$H < \log n + 2.512. \tag{8}$$

Setting $\Lambda = 2mi\pi - n\log\alpha$ we obtain that

$$\begin{aligned}\log|\Lambda| > &-(13.1576H^2 + 0.23)\cdot\left(9.503 + \frac{1}{2}\log y\right)\\ &-2(H + \log H) - 0.003.\end{aligned} \tag{9}$$

Comparing (7) with (9) and using $y \geq 5$, we deduce that

$$n < 5.547(84.27H^2 + 1.243(H + \log H) + 2.121),$$

whence in view of (8), we infer that

$$n \leq 90813. \tag{10}$$

Next consider the case when

$$a > y^{\frac{n}{3.128}}. \tag{11}$$

It follows from (3) that

$$2ai = i^r(1+i)(u+iv)^n - (-i)^r(1-i)(u-iv)^n, \tag{12}$$

whence

$$\frac{2ai}{(-i)^r(u-iv)^n} = \left(\frac{\pm(u+iv)}{(u-iv)}\right)^n (1+i) - (1-i). \tag{13}$$

Since

$$(1+i)^n = \begin{cases} \pm 2^{\frac{n-1}{2}}(1+i), & \text{if } n \equiv 1 \mod 4 \\ \pm 2^{\frac{n-1}{2}}(1-i), & \text{if } n \equiv -1 \mod 4, \end{cases}$$

we obtain from (13) that

$$\pm 2^{\frac{n+1}{2}}(-1)^r i^{1-r}(u+iv)^n \frac{a}{y^n} = \left(\frac{\pm(u+iv)}{(u-iv)}(1\pm i)\right)^n - (1\mp i)^n. \tag{14}$$

Put $\Lambda = \left(\frac{\pm(u+iv)}{(u-iv)}(1\pm i)\right)^n - (1\mp i)^n$. If $p \mid a$ then in view of $\gcd(x,y)=1$, we get $p \nmid xy$. It follows from (14) that

$$v_p(a) = v_p\left(\pm 2^{\frac{n+1}{2}}(-1)^r i^{1-r}(u+iv)^n \frac{a}{y^n}\right) = v_p(\Lambda), \tag{15}$$

since p is relatively prime to $2i$ and $u+iv$ in $\mathbb{Z}[i]$.

Assume first that $\left(\frac{\pm(u+iv)}{(u-iv)}(1\pm i)\right)$ and $(1\mp i)$ are multiplicatively dependent. Then there exists $(r,s) \in \mathbb{Z}^2$ with $(r,s) \neq (0,0)$ such that

$$\left(\frac{\pm(u+iv)}{(u-iv)}(1\pm i)\right)^r (1\mp i)^s = 1. \tag{16}$$

Setting $\alpha = u+iv$, (16) yields

$$\left(\frac{\alpha}{\bar{\alpha}}(1\pm i)\right)^{4r}(1\mp i)^{4s} = 1. \tag{17}$$

Taking norms on both sides of (17), we infer that

$$2^{4(r+s)} = 1,$$

which yields $r + s = 0$. Thus, by (17),

$$(\alpha/\bar{\alpha})^{4r} = 1$$

whence

$$\bar{\alpha}/\alpha = \pm 1 \quad \text{or} \quad \bar{\alpha}/\alpha = \pm i. \tag{18}$$

From (18) we deduce that $uv = 0$ or $u = \pm v$. But as was seen above, this leads to the trivial solution.

Consider now the case when $\big(\frac{\pm(u+iv)}{(u-iv)}(1 \pm i)\big)$ and $(1 \mp i)$ are multiplicatively independent. We apply Lemma 2 to Λ with the following choice of parameters:

$$\alpha_1 = \left(\frac{\pm(u+iv)}{(u-iv)}(1 \pm i)\right), \quad \alpha_2 = 1 \mp i,$$

$$b_1 = b_2 = n, \quad f = 2, \quad D = 1.$$

Since $p \geq 3$ and $y \geq 5$, we may choose $\log A_1 = \frac{\log 10}{2 \log 5} \log y \log p$, $\log A_2 = \log p$, $b' = \frac{2+\log 10}{\log 10} \frac{n}{\log p}$. Then we get

$$\begin{aligned} v_p(a) &= v_p(\Lambda) \\ &< 17.17 \frac{p(p+1)}{\log^2 p} \left(\max\{\log(1.869n) + 0.4,\ 10 \log p\}\right)^2 \log y. \end{aligned} \tag{19}$$

It follows that

$$\begin{aligned} \log a &= \sum_{p|a} v_p(a) \log p \\ &< 17.17 \sum_{p|a} \frac{p(p+1)}{\log p} \left(\max\{\log(1.869n) + 0.4,\ 10 \log p\}\right)^2 \log y. \end{aligned} \tag{20}$$

Comparing (11) with (20) we get

$$n < 17.17 \cdot 3.128 \sum_{p|a} \frac{p(p+1)}{\log p} \left(\max\{\log(1.869n) + 0.4,\ 10 \log p\}\right)^2. \tag{21}$$

Thus we deduce that if

$$\max\{\log(1.869n) + 0.4,\ 10 \log p\} = \log(1.869n) + 0.4,$$

then

$$\frac{n}{(\log(1.869n) + 0.4)^2} < 3.128 \cdot 17.17s\frac{P(P+1)}{\log P}. \tag{22}$$

If

$$\max\{\log(1.869n) + 0.4,\ 10\log p\} = 10\log p,$$

then (21) gives

$$n < 5371sP(P+1)\log P. \tag{23}$$

Finally, except for the case $P = 3$, $s = 1$, we obtain from (10), (22) and (23) that

$$n < 5371sP(P+1)\log P$$

while if $P = 3$ and $s = 1$, we deduce that (10) holds. □

Acknowledgements. The author is grateful to Professors Kálmán Győry, Ákos Pintér and Lajos Hajdu for their help and numerous valuable remarks.

References

[1] S. A. Arif and F. S. A. Muriefah, On the Diophantine equation $x^2 + 2^k = y^n$, *Internat. J. Math. Math. Sci.* **20** (1997), 299–304.

[2] S. A. Arif and F. S. A. Muriefah, On a Diophantine equation, *Bull. Austral. Math. Soc.* **57** (1998), 189–198.

[3] S. A. Arif and F. S. A. Muriefah, The Diophantine equation $x^2 + 3^m = y^n$, *Internat. J. Math. Math. Sci.* **21** (1998), 619–620.

[4] S. A. Arif and F. S. A. Muriefah, The Diophantine equation $x^2 + 5^{2k+1} = y^n$, *Indian J. Pure Appl. Math.* **30** (1999), 229–231.

[5] S. A. Arif and F. S. A. Muriefah, The Diophantine equation $x^2 + q^{2k} = y^n$, *Arab. J. Sci. Eng. Sect. A Sci.* **26** (2001), 53–62.

[6] S. A. Arif and F. S. A. Muriefah, On the Diophantine equation $x^2 + 2^k = y^n$ II, *Arab J. Math. Sci.* **7** (2001), 67–71.

[7] S. A. Arif and F. S. A. Muriefah, On the Diophantine equation $x^2+q^{2k+1} = y^n$, *J. Number Theory* **95** (2002), 95–100.

[8] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte., *J. Reine Angew. Math.* **539** (2001), 75–122.

[9] Y. Bugeaud, On the diophantine equation $x^2 - p^m = \pm y^n$, *Acta Arith.* **80** (1997), 213–223.

[10] Y. Bugeaud and K. Győry, On binomial Thue–Mahler equations (*to appear*).

[11] Y. Bugeaud and M. Laurent, Minoration effective de la distance p-adique entre puissances de nombres algébriques, *J. Number Theory* **61** (1996), 311–342.

[12] J. H.E. Cohn, The diophantine equation $x^2 + 2^k = y^n$, *Arch. Math (Basel)* **59** (1992), 341–344.

[13] J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$, II, *Int. J. Math. Math. Sci.* **22** (1999), 459–462.

[14] F. Luca, On a diophantine equation, *Bull. Austral. Math. Soc.* **61** (2000), 241–246.

[15] F. Luca, On the equation $x^2 + 2^a 3^b = y^n$, *Int. J. Math. Sci.* **29** (2002), 239–244.

[16] M. Mignotte, On the Diophantine equation $D_1 x^2 + D_2^m = 4y^n$, *Portugal. Math.* **54** (1997), 457–460.

[17] F. S. A. Muriefah, On the Diophantine equation $px^2 + 3^n = y^p$, *Tamkang J. Math.* **31** (2000), 79–84.

[18] F. S. A. Muriefah, On the Diophantine equation $Ax^2 + 2^{2m} = y^n$, *Int. J. Math. Math. Sci.* **25** (2001), 373–381.

[19] I. Pink and Sz. Tengely, Full powers in arithmetic progressions, *Publ. Math. Debrecen* **57** (2000), 535–545.

[20] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, Applications of the Gel'fond-Baker method to Diophantine equations, in: Transcendence Theory: Advances and Applications, *Academic Press*, *London – New York, San Francisco*, 1977, 59–77.

[21] Sz. Tengely, On the diophantine equation $x^2 + a^2 = 2y^p$, (in preparation).

ISTVÁN PINK
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: pinki@math.klte.hu

(Received July 14, 2003; revised January 15, 2004)