ACTA ARITHMETICA
LXXX.3 (1997)

On the diophantine equation $x^2 - p^m = \pm y^n$

by

Yann Bugeaud (Strasbourg)

1. Introduction. In all what follows, we denote by $\mathbb{N}$ the set of strictly positive integers. Let p be an odd prime number, and let D be a non-power integer with $D > 1$ and $\gcd(p, D) = 1$. Toyoizumi [16] and Maohua Le [10] (see also [11]) studied the number of solutions of the diophantine equation

$$x^2 + D^n = p^m, \quad x, m, n \in \mathbb{N}. \tag{1}$$

More precisely, Maohua Le [10] proved that if $\max\{p, D\}$ is larger than an explicit constant, then equation (1) has at most two solutions, except when, for a positive integer a, we have $D = 3a^2 + 1$ and $p = 4a^2 + 1$. In the latter case, there are at most three solutions, including the trivial one $(x, m, n) = (a, 1, 1)$. Further, he gave [9] an analogous result for the diophantine equation $x^2 - D^n = p^m$. His method being essentially ineffective, Maohua Le does not obtain computable upper bounds for the solutions of equation (1).

In this work, we deal with a generalization of equation (1), namely, we study the diophantine equation

$$x^2 \pm y^n = p^m, \quad x, y, m, n \in \mathbb{N},\ \gcd(p, y) = 1. \tag{2}$$

We show that, under some not very restrictive conditions, (2) has only finitely many solutions (x, y, m, n), and we provide a small explicit upper bound for n which only depends on p.

As in [1], where the author investigated the diophantine equation $x^2 - 2^m = \pm y^n$ (see also the work of Yongdong Guo & Maohua Le [4]), the proofs mainly depend on the sharp estimates for linear forms in two logarithms in archimedean and non-archimedean metrics, due to Laurent, Mignotte & Nesterenko [8] and Bugeaud & Laurent [2], respectively.

2. Statement of the results. Let p be an odd prime number. In this work, we consider the diophantine equations

$$x^2 - p^m = y^n, \quad x, y, m, n \in \mathbb{N},\ \gcd(x, y) = 1,\ n \geq 3, \tag{3}$$

and

$$x^2 + y^n = p^m, \quad x, y, m, n \in \mathbb{N},\ \gcd(x, y) = 1,\ n \geq 3. \tag{4}$$

We state our main result, depending only on the value of p modulo 4, in the following two theorems.

THEOREM 1. *If* $p \equiv 3 \bmod 4$, *then* (3) *and* (4) *have only finitely many solutions* (x, y, m, n). *Moreover*, *those solutions satisfy*

$$n \leq 4.5 \cdot 10^6 p^2 \log^2 p \quad \textit{and} \quad n \leq 5.6 \cdot 10^5 p^2 \log^2 p,$$

respectively.

THEOREM 2. *If* $p \equiv 1 \bmod 4$, *then* (3) *and* (4) *have only finitely many solutions* (x, y, m, n) *with even* m *or odd* y. *Moreover*, *those solutions satisfy*

$$n \leq 4.5 \cdot 10^6 p^2 \log^2 p \quad \textit{and} \quad n \leq 5.6 \cdot 10^5 p^2 \log^2 p,$$

respectively.

Remarks. The main interest of Theorems 1 and 2 is the small size of the upper bound for n. Indeed, if we apply a theorem of Shorey, Van der Poorten, Tijdeman & Schinzel [15, Theorem 2], we can also show that there exists some effective constant $c_0(p)$, depending only on p, such that $n < c_0(p)$ for any solution (x, y, m, n) of (3) or (4). However, their result does not provide an explicit value for $c_0(p)$, which has to be very large, in view of the method of proof.

The hypothesis $n \geq 3$ in the statement of equations (3) and (4) cannot be replaced by $n \geq 2$. Indeed, $((p^m + 1)/2)^2 - p^m = ((p^m - 1)/2)^2$ for any positive integer m, and, furthermore, it is well known (see e.g. Hardy & Wright [5, Theorem 366]) that p^m (resp. p^{2m}) is the sum of two squares if $p \equiv 1 \bmod 4$ (resp. $p \equiv 3 \bmod 4$).

In the course of the proof of Theorems 1 and 2, we need some information about prime powers in binary recurrence sequences with integer roots. To this end, we state the following result.

THEOREM 3. *Let* p *be a prime number. Let* $a := a_1/a_2$ *and* $b := b_1/b_2$ *be two irreducible rational numbers satisfying* $v_p(a) = v_p(b) = 0$ *and put* $A := \max\{a_1, a_2, b_1, b_2, 3\}$. *Consider the diophantine equation*

$$p^m = ax^n + by^n, \quad x, y, m, n \in \mathbb{N},\ \gcd(x, y) = 1,\ n \geq 2. \tag{5}$$

Then $n \leq 34000 p \log p \log A$.

3. Auxiliary results

LEMMA 1. *The equation* $x^2 - y^n = \pm 1$ *has no solution with* $y > 2$ *and* $n \geq 2$.

Proof. See Chao Ko [6]. ∎

For any integer x, we denote by $P[x]$ the greatest prime factor of x.

LEMMA 2. *Let a, b, x and y be non-zero integers with* $\gcd(x, y) = 1$. *Put $X = \max\{|x|, |y|\}$. For any integer $n \ge 3$, there exist effectively computable constants c_1 and X_1 such that*

$$P[ax^2 + by^n] \ge c_1(\log\log X \log\log\log X)^{1/2} \quad \text{whenever } X \ge X_1.$$

Proof. This is a particular case of a theorem due to Kotov [7]. ∎

The next lemma is very closed to Lemma 6 of Maohua Le [12]. For similar results, we refer the reader to [14].

LEMMA 3. *Let $d > 1$ be a squarefree integer, and let k be a positive odd integer, coprime to d. Denote by $\varrho > 1$ the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$. If X, Y and Z are three positive integers satisfying*

$$X^2 - dY^2 = \pm k^Z,$$

then there exist positive integers a, b, t and v, with $a \equiv b \bmod 2$ and a and b even if $d \not\equiv 1 \bmod 4$, such that

$$X + Y\sqrt{d} = \varrho^{-t}\left(\frac{a + b\sqrt{d}}{2}\right)^v.$$

Moreover, $0 < t \le v$ and the integer Z/v divides h_d, the class number of the field $\mathbb{Q}(\sqrt{d})$.

Proof. For any α in $\mathbb{Q}(\sqrt{d}) =: \mathbb{K}$, we denote by $[\alpha]$ the principal ideal of $\mathbb{K}$ generated by α. We infer from $\gcd(k, d) = 1$ that $\gcd([X - Y\sqrt{d}], [X + Y\sqrt{d}])$ divides $[2]$. Moreover, $\gcd([X - Y\sqrt{d}], [X + Y\sqrt{d}]) = [1]$, since k is assumed to be odd. Working in $\mathbb{K}$, we have the following equalities between ideals:

$$[X - Y\sqrt{d}] \cdot [X + Y\sqrt{d}] = [k]^Z = (\mathfrak{a}\overline{\mathfrak{a}})^Z,$$

where $\mathfrak{a}$ is an integer ideal in $\mathbb{K}$ and $\overline{\cdot}$ denotes the Galois transformation $\sigma : \sqrt{d} \to -\sqrt{d}$. There exist Z_1 and an algebraic integer α in $\mathbb{K}$ such that $Z_1 \mid h_d$ and $\mathfrak{a}^{Z_1}$ is the principal ideal generated by α. Thus, putting $v = Z/Z_1$, we have

$$X + Y\sqrt{d} = \eta\alpha^v \quad \text{and} \quad X - Y\sqrt{d} = \overline{\eta}\,\overline{\alpha}^v,$$

where η is a unit in $\mathbb{K}$.

Put $\omega = \sqrt{d}$ if $d \not\equiv 1 \bmod 4$ and $\omega = (1+\sqrt{d})/2$ otherwise and recall that $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{K}$. Modifying α if necessary, we can assume that $\eta = \varrho^{-t}$, with $0 < t \le v$. Thus we get

$$X + Y\sqrt{d} = \varrho^{-t}\left(\frac{a + b\sqrt{d}}{2}\right)^v,$$

where a and b are two integers satisfying $a \equiv b \bmod 2$ and a and b are even if $d \not\equiv 1 \bmod 4$. From $X + Y\sqrt{d} > |X - Y\sqrt{d}|$ and $\varrho^{-1} < \varrho$, we infer that $a+b\sqrt{d} > |a-b\sqrt{d}|$. Hence a and b are positive, and the lemma is proved. ∎

Lemma 4. *Let p be an odd prime. Denote by h_p and R_p the class number and the regulator of the quadratic field $\mathbb{Q}(\sqrt{p})$. Then we have the upper bounds*

$$h_p \le 0.5p^{1/2} \quad \text{and} \quad 0.4812 < R_p \le h_p R_p \le p^{1/2}\log(4p).$$

Proof. We refer respectively to Maohua Le [13] and to Faisant [3], p. 199. ∎

The next two propositions deal with lower bounds for linear forms in two logarithms. Let $\alpha = \alpha_1$ be a non-zero algebraic number with minimal defining polynomial $a_0(X-\alpha_1)\dots(X-\alpha_n)$ over $\mathbb{Z}$. The logarithmic height of α, denoted by $\mathrm{h}(\alpha)$, is defined by

$$\mathrm{h}(\alpha) = \frac{1}{n}\log\Big(a_0\prod_{i=1}^{n}\max\{1,|\alpha_i|\}\Big).$$

For any prime number 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 $v_p(p) = 1$.

Proposition 1. *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*

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

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

$$\log A_i \ge \max\{\mathrm{h}(\alpha_i), (\log p)/D\}, \qquad i = 1,2,$$

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 the lower bound

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

Proof. This is Théorème 4 of [2] with the choice $(\mu,\nu) = (10,5)$. ∎

Proposition 2. *Let $\alpha_1 \ge 1$ and $\alpha_2 \ge 1$ be two real algebraic numbers. Let b_1 and b_2 be two positive integers and put*

$$\Lambda_a = b_1\log\alpha_1 - b_2\log\alpha_2.$$

Set $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ *and denote by* $A_1 > 1$ *and* $A_2 > 1$ *two real numbers satisfying*

$$\log A_i \geq \max\{\mathrm{h}(\alpha_i), 1/D\}, \qquad i = 1, 2.$$

Finally, 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 the lower bound*

$$\log |\Lambda_a| \geq -32.31 D^4 (\max\{\log b' + 0.18, 0.5, 10/D\})^2 \log A_1 \log A_2.$$

Proof. This is Corollaire 2 of [8], where the numerical constants are given in Tableau 2 and correspond to the choice $h_2 = 10$. Notice that the hypotheses of the proposition imply that $\mathrm{h}(\alpha_i) \leq |\log \alpha_i|/D$. ■

4. Proof of Theorem 3. Let (x, y, m, n) be a solution of (5). Without loss of generality, we may suppose that $|y| \geq |x|$ and we set $Y := |y|$.

First, we make the assumption $p^m \geq Y^{n/1.4}$, whence

$$1.4 m \log p \geq n \log Y. \tag{6}$$

Putting

$$\Lambda_u := \frac{p^m}{a y^n} = \left(\frac{x}{y}\right)^n - \frac{-b}{a}, \tag{7}$$

we have $v_p(\Lambda_u) = m$. In order to bound m, we apply Proposition 1 to (7) with the parameters

$$\alpha_1 = x/y, \quad \alpha_2 = -b/a, \quad b_1 = n, \quad b_2 = 1, \quad f = D = 1.$$

Since $p \geq 2$ and $Y \geq 2$ we see that we can take

$$\log A_1 = \frac{\log Y}{\log 2} \log p, \qquad \log A_2 = 2 \frac{\log p}{\log 2} \log A,$$

and we have

$$b' \leq e^{-0.4} n / (\log p \log A)$$

provided that

$$n \geq 4 \log A. \tag{8}$$

Assuming that α_1 and α_2 are multiplicatively independent, we get

$$m \leq 100 p (\log p)^{-2} \log Y \log A \max\left\{10 \log p, \log \frac{n}{\log A}\right\}^2,$$

whence, by (6),

$$\frac{n}{\log A} \leq 140 \frac{p}{\log p} \max\left\{10 \log p, \log \frac{n}{\log A}\right\}^2. \tag{9}$$

From (9), we deduce the upper bound

$$n \le 34000 p \log p \log A. \tag{10}$$

The estimate (10) remains true if α_1 and α_2 are multiplicatively dependent. Indeed, in the latter case, there exist rational integers $x' > 0$, $y' > 0$, $u > 0$ and v such that $x = x'^u$, $y = y'^u$ and $-b/a = (x'/y')^v$. Hence, we infer from (5) that

$$\frac{p^m}{a x'^v y'^{un-v}} = \left(\frac{x'}{y'}\right)^{un-v} - 1,$$

and we conclude as before, using Proposition 1 together with $1.4 m \log p \ge nu \log |y'|$.

We now make the assumptions $p^m \le Y^{n/1.4}$ and

$$n \ge 500 \log A. \tag{11}$$

Putting

$$\Lambda_a := \frac{p^m}{b y^n} = \frac{a}{b}\left(\frac{x}{y}\right)^n + 1, \tag{12}$$

we have

$$\log |\Lambda_a| \le -(2n/7)\log Y - \log |b| \le -(2n/7)\log Y + \log A \tag{13}$$

and we deduce from (11) that $|\Lambda_a| \le 1/2000$. Hence, by (12), we get

$$\left| n \log\left|\frac{y}{x}\right| - \log\left|\frac{-b}{a}\right| \right| \le |\log(1-\Lambda_a)| \le 1.001 |\Lambda_a|. \tag{14}$$

Applying Proposition 2 to the left-hand side of (14) with the parameters

$$\alpha_1 = |y/x|, \quad \alpha_2 = |-a/b|, \quad b_1 = n, \quad b_2 = 1,$$
$$\log A_1 = \log Y, \quad \log A_2 = 2\log A, \quad b' = \frac{n}{2\log A} + \frac{1}{\log Y} \le \frac{n}{\log A},$$

we obtain

$$\log |\Lambda_a| \ge -0.002 - 32.31 \max\left\{ \log \frac{n}{\log A} + 0.18, 10 \right\}^2 \log A^2 \log Y, \tag{15}$$

provided that α_1 and α_2 are multiplicatively independent and $|\alpha_2| \ge 1$. However, it is easily seen that (15) remains true if one of the latter conditions is not fulfilled. Consequently, subject to the condition (11), we use (13) to get

$$n \le 227 \max\left\{ \log \frac{n}{\log A} + 0.18, 10 \right\}^2 \log A + 7 \log A,$$

hence

$$n \le 24000 \log A. \tag{16}$$

Finally, by (8), (10), (11) and (16), we obtain $n \leq 34000p \log p \log A$, as claimed. ∎

5. Proof of Theorems 1 and 2. The proofs of both Theorems 1 and 2 run parallel. Lemma 1 shows that equations (3) and (4) have no solution (x, y, m, n) with $y = 1$. Thus, in all this section, we assume that y is at least 2.

⋆ *The case* m *even*. Let (x, y, m, n) be a solution of (3) or (4) with m even. Thus we have

$$(x + p^{m/2})(x - p^{m/2}) = \pm y^n,$$

and, since $\gcd(x + p^{m/2}, x - p^{m/2})$ divides 2, we get

$$\begin{cases} x + p^{m/2} = a_1 d_1^n, \\ x - p^{m/2} = a_2 d_2^n, \end{cases} \tag{17}$$

where a_1, a_2, d_1 and d_2 are rational numbers satisfying $|a_1|, |a_2| \in \{1/2, 1, 2\}$, $|a_1 a_2| = 1$ and $\gcd(d_1, d_2) = 1$. From (17) we deduce that

$$p^{m/2} = \frac{a_1}{2} d_1^n - \frac{a_2}{2} d_2^n,$$

and, applying Theorem 2 with $A = 4$, we get the bound $n \leq 48000p \log p$, which proves the last parts of Theorems 1 and 2 when m is even.

⋆ *The case* m *odd*. Observe that if $p \equiv 3 \bmod 4$ and if (x, y, m, n) is a solution of equation (3) or (4), then $x^2 - p^m$ is equal to 1 or 2 modulo 4. Hence, y cannot be even, and, in order to complete the proof of Theorems 1 and 2, we may assume that y is an odd integer.

• *An upper bound for* m *valid for the solutions of* (3) *and* (4). Let (x, y, m, n) be a solution of (3) or (4) with odd m. Denote by ϱ (> 1) the fundamental unit of the field $\mathbb{Q}(\sqrt{p})$ and by h_p and $R_p := \log \varrho$ its class number and regulator, respectively. By Lemma 3, there exist an algebraic integer $\varepsilon := a + b\sqrt{p}$ in $\mathbb{Q}(\sqrt{p})$ and positive integers t and v such that $0 < t \leq v$ and

$$\begin{cases} x + p^{(m-1)/2}\sqrt{p} = \varepsilon^v \varrho^{-t}, \\ x - p^{(m-1)/2}\sqrt{p} = \overline{\varepsilon}^v (\tau\varrho)^t, \end{cases} \tag{18}$$

where $\overline{\varepsilon}$ denotes the conjugate of ε over $\mathbb{Q}$ and $\tau \in \{\pm 1\}$ is the norm of ϱ. Moreover,

$$v \text{ divides } n \quad \text{and} \quad n \text{ divides } h_p v. \tag{19}$$

From the system (18) we deduce the equation

$$2p^{(m-1)/2}\sqrt{p} = \varepsilon^v \varrho^{-t} - \overline{\varepsilon}^v (\tau\varrho)^t, \tag{20}$$

and we put

$$\Lambda_u := (\varepsilon/\overline{\varepsilon})^v - (\tau\varrho^2)^t. \tag{21}$$

Since $\varepsilon/\overline{\varepsilon}$ is a root of the irreducible polynomial $\varepsilon\overline{\varepsilon}X^2 - (\varepsilon^2 + \overline{\varepsilon}^2)X + \varepsilon\overline{\varepsilon}$, we have $\mathrm{h}(\varepsilon/\overline{\varepsilon}) = \log\varepsilon$ and $\varepsilon/\overline{\varepsilon}$ is not a unit. Thus $\varepsilon/\overline{\varepsilon}$ and $\tau\varrho^2$ are multiplicatively independent algebraic numbers, which, moreover, are p-adic units, since $\gcd(x,y) = 1$. By (20), we have $v_p(\Lambda_u) = m/2$. In order to bound m, we apply Proposition 1 to (21) with the following parameters:

$$\alpha_1 = \varepsilon/\overline{\varepsilon}, \quad \alpha_2 = \tau\varrho^2, \quad b_1 = v, \quad b_2 = t, \quad p = 2, \quad D = 2, \quad f = 1.$$

Using Lemma 4 and the upper bound $\log\sqrt{p} \le 1.54\log\varepsilon$ deduced from Lemma 3 (the worst case occurs for $p = 13$ and $\varepsilon = (1+\sqrt{13})/2$), we see that we can set

$$\log A_1 = 1.54\log\varepsilon, \quad \log A_2 = \frac{R_p\log p}{0.96} \quad \text{and} \quad b' = \frac{t}{3.08\log\varepsilon} + \frac{0.48v}{R_p\log p}.$$

Thus, by Proposition 1 and the estimate $b' \le 2v/\log p$, we get

$$m \le 1232p(\log p)^{-3}R_p\max\{\log v + 1.1, 5\log p\}^2\log\varepsilon. \tag{22}$$

• *The case of equation* (4). The result is clearly true if $m = 1$, thus we assume $m \ge 3$. From (18), we infer that $\varepsilon^v\varrho^{-t} \le 2p^{m/2}$, whence

$$2v\log\varepsilon \le 2t\log\varrho + \log 4 + m\log p.$$

Together with (22), it yields

$$\begin{aligned} 2vm \le{}& 1232p(\log p)^{-3}R_p(m\log p + \log 4 + 2tR_p) \\ &\times \max\{\log v + 1.1, 5\log p\}^2. \end{aligned} \tag{23}$$

From $p^m > y^n \ge 2^n$ and (19), we deduce that

$$\frac{t}{m} \le \frac{v}{m} \le \frac{n}{m} \le \frac{\log p}{\log 2},$$

hence, using (23) and $m \ge 3$, we get

$$v \le 616p(\log p)^{-3}R_p\left(\log p + \frac{\log 4}{3} + \frac{2}{\log 2}R_p\log p\right)\max\{\log v + 1.1, 5\log p\}^2$$

and

$$v \le 1778p(\log p)^{-2}R_p(R_p + 0.5)\max\{\log v + 1.1, 5\log p\}^2. \tag{24}$$

Assume first that $\max\{\log v + 1.1, 5\log p\} = 5\log p$. Then we infer from (19) and (24) that

$$n \le 44450ph_pR_p(R_p + 0.5),$$

and, using $p \ge 3$ and the upper bounds for R_p and h_pR_p given by Lemma 4, we obtain

$$n \le 2.6 \cdot 10^5p^2\log^2 p. \tag{25}$$

Assume now that $\max\{\log v + 1.1, 5\log p\} = \log v + 1.1$. In order to get a better bound for n, we treat separately the smallest two values of p. Hence, suppose that $p \notin \{3, 5\}$, and search an upper bound for v of the shape $v \le \gamma p R_p(R_p + 0.5)$, with a suitable constant γ. Since $p \ge 7$, we see that γ must satisfy the inequality $\gamma \ge 470(\log\gamma + 7.46)^2$. Thus, we may choose $\gamma = 1.8 \cdot 10^5$ and, using (19) and the upper bounds for R_p and h_pR_p given by Lemma 4, we get

$$n \le 5.6 \cdot 10^5 p^2 \log^2 p. \tag{26}$$

Finally, we easily see that (26) remains true for $p \in \{3, 5\}$ and it follows from (25) and (26) that (24) leads to the bound

$$n \le 5.6 \cdot 10^5 p^2 \log^2 p,$$

as claimed.

• *The case of equation* (3). Dividing (19) by $\varepsilon^v \varrho^{-t}$, we obtain

$$\frac{2p^{(m-1)/2}\sqrt{p}}{\varepsilon^v \varrho^{-t}} = \frac{2p^{(m-1)/2}\sqrt{p}}{x + p^{(m-1)/2}\sqrt{p}} = 1 - \left(\frac{\overline{\varepsilon}}{\varepsilon}\right)^v (\tau\varrho^2)^t =: \Lambda_a. \tag{27}$$

If $\Lambda_a \ge 1/2$, then we have $4p^{(m-1)/2}\sqrt{p} \ge \varepsilon^v \varrho^{-t}$ and

$$2v\log\varepsilon - 2t\log\varrho \le m\log p + \log 16. \tag{28}$$

Otherwise $\Lambda_a < 1/2$ and we get

$$|\log(1 - \Lambda_a)| \le 2\Lambda_a. \tag{29}$$

We apply Proposition 2 to the linear form

$$\left| v\log\left|\frac{\varepsilon}{\overline{\varepsilon}}\right| - t\log(\varrho^2)\right| \le \left| v\log\left(\frac{\varepsilon}{\overline{\varepsilon}}\right) - t\log(\tau\varrho^2)\right| \le |\log(1 - \Lambda_a)|$$

with the following parameters:

$$\alpha_1 = |\varepsilon/\overline{\varepsilon}|, \quad \alpha_2 = \varrho^2, \quad b_1 = v, \quad b_2 = t, \quad D = 2,$$
$$\log A_1 = \log\varepsilon, \quad \log A_2 = \log\varrho = R_p, \quad b' = \frac{t}{2\log\varepsilon} + \frac{v}{2R_p}.$$

It follows from Lemma 4 and $\varepsilon \ge (1 + \sqrt{13})/2$ that $b' \le 1.64v$, and, using (29), we obtain

$$\log 2 + \log\Lambda_a \ge -517R_p \max\{\log v + 0.68, 5\}^2 \log\varepsilon,$$

hence, by (27),

$$v\log\varepsilon - t\log\varrho \le \log 4 + (m\log p)/2 + 517R_p\max\{\log v + 0.68, 5\}^2\log\varepsilon. \tag{30}$$

From (22), (28) and (30) we infer that

$$\begin{aligned} v\log\varepsilon - tR_p \le\ & \log 4 + 517R_p\max\{\log v + 0.68, 5\}^2\log\varepsilon \\ & + 616p(\log p)^{-2}R_p\max\{\log v + 1.1, 5\log p\}^2\log\varepsilon. \end{aligned} \tag{31}$$

First, assume that $\varepsilon < \exp\{2R_p\}$. From (18), we get $\varepsilon^v \varrho^{-t} > y^{n/2}$, hence

$$v \log \varepsilon - t \log \varrho > (n \log y)/2. \tag{32}$$

However, we have

$$\frac{\log \varepsilon}{\log y} \le \frac{2R_p}{\log 3}, \tag{33}$$

since $y > 1$ is odd, and we deduce from (31), (32) and (33) that

$$\begin{aligned} n \le 2.6 &+ 1883 R_p^2 \max\{\log n + 0.68, 5\}^2 \\ &+ 2243 p (\log p)^{-2} R_p^2 \max\{\log n + 1.1, 5 \log p\}^2. \end{aligned}$$

As before, we search an upper bound for n of the shape $n \le \gamma p^2 \log^2 p$. Using Lemma 4 and a few calculation, we show that it suffices that γ satisfies

$$\gamma \ge 0.3 + 3214\{\log \gamma + 3.1\}^2 + 9508\{\log \gamma + 3.5\}^2.$$

Thus, we can choose $\gamma = 4.5 \cdot 10^6$, which gives the bound

$$n \le 4.5 \cdot 10^6 p^2 \log^2 p. \tag{34}$$

Assume now that $\varepsilon \ge \exp\{2R_p\}$. Then we have

$$v \log \varepsilon - t R_p \ge (v \log \varepsilon)/2, \tag{35}$$

since $t \le v$. Using (31), (35) and the lower bound $\varepsilon \ge (1 + \sqrt{13})/2$, we get

$$\begin{aligned} v \le 3.4 &+ 1034 R_p \max\{\log v + 0.68, 5\}^2 \\ &+ 1232 p (\log p)^{-2} R_p \max\{\log v + 1.1, 5 \log p\}^2, \end{aligned}$$

hence, by (19),

$$\begin{aligned} n \le 3.4 h_p &+ 1034 (h_p R_p) \max\{\log n + 0.68, 5\}^2 \\ &+ 1232 p (\log p)^{-2} (h_p R_p) \max\{\log n + 1.1, 5 \log p\}^2 \end{aligned}$$

and it is easy to show that (34) also holds in this case. Hence, the last statements of Theorems 1 and 2 are proved.

Now, in order to complete the proofs of Theorems 1 and 2, it suffices to apply Lemma 2 to the polynomials $x^2 \pm y^n$, where $3 \le n \le 4.5 \cdot 10^6 p^2 \log^2 p$. ∎

References

[1] Y. Bugeaud, *On the diophantine equation* $x^2 - 2^m = \pm y^n$, Proc. Amer. Math. Soc., to appear.

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

[3] A. Faisant, *L'équation diophantienne du second degré*, Hermann, Paris, 1991.

[4] Y. D. Guo and M. H. Le, *A note on the exponential diophantine equation* $x^2 - 2^m = y^n$, Proc. Amer. Math. Soc. 123 (1995), 3627–3629.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, 1990.
[6] C. Ko, *On the diophantine equation* $x^2 = y^n + 1,\ xy \neq 0$, Sci. Sinica 14 (1965), 457–460.
[7] S. V. Kotov, *Über die maximale Norm der Idealteiler des Polynoms* $ax^m + by^n$ *mit den algebraischen Koeffizienten*, Acta Arith. 31 (1976), 219–230.
[8] M. Laurent, M. Mignotte et Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321.
[9] M. H. Le, *On the generalized Ramanujan–Nagell equation*, *III*, Dongbei Shuxue 4 (1988), 180–184.
[10] —, *The diophantine equation* $x^2 + D^m = p^n$, Acta Arith. 52 (1989), 255–265.
[11] —, *Applications of Baker's method*, *IV*, J. Changsha Railway Inst. 9 (1991), no. 2, 87–92.
[12] —, *A note on the diophantine equation* $(x^m - 1)/(x - 1) = y^n$, Acta Arith. 64 (1993), 19–28.
[13] —, *Upper bounds for class number of real quadratic fields*, ibid. 68 (1994), 141–144.
[14] —, *Some exponential diophantine equations*, *I*, J. Number Theory 55 (1995), 209–221.
[15] 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, 1977, 59–78.
[16] M. Toyoizumi, *On the diophantine equation* $x^2 + D^m = p^n$, Acta Arith. 42 (1983), 303–309.

U.F.R. de mathématiques
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg, France
E-mail: bugeaud@pari.u-strasbg.fr

Received on 28.5.1996
and in revised form on 12.9.1996 (2996)