ON THE DIOPHANTINE EQUATION $x^2 - p^m = \pm\, y^n$

Yann Bugeaud (Strasbourg)

1. Introduction

In all what follows, we denote by $\mathbf{N}$ 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 [13] and Maohua Le [9] studied the number of solutions of the diophantine equation

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

More precisely, Maohua Le proved that if $\max\{p, D\}$ is larger than an explicit constant, then Eq. (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. Further, he gave [8] an analogous result for the diophantine equation $x^2 - D^n = p^m$. His method being essentially ineffective, Maohua Le do not obtain computable upper bounds for the solutions of Eq. (1).

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

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

We show that, under some not very restrictive conditions, Eq. (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 $x^2 - 2^m = \pm\, y^n$, 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 [7] 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

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

and

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

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 Eq. (3) and Eq. (4) have only finitely many solutions (x, y, m, n). Moreover, those satisfy*

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

respectively.

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

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

respectively.

Remarks : If we apply a theorem of Shorey, Van der Poorten, Tijdeman & Schinzel [12, Theorem 2], we can 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 Eq. (3) or Eq. (4). However, it 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 Eq. (3) and Eq. (4) cannot be replaced by $n \geq 2$. Indeed, for any positive integer m we have $\left((p^m+1)/2\right)^2 - p^m = \left((p^m-1)/2\right)^2$, and, furthermore, it is well known (see e. g. Hardy & Wright [4, 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*

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

Then we have $n \leq 34000\, p \log p \, \log A$.

3. Auxiliary results

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

Proof : See Ko Chao [5]. $\square$

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 $n \geq 3$, there exist effectively computable constants c_1 and X_1 such that*

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

Proof : This is a particular case of a theorem due to Kotov [6]. $\square$

The next lemma is very closed to Lemma 6 of Maohua Le [10].

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

$$X^2 - d\, Y^2 = \pm\, k^Z,$$

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

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

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

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

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

where $\mathfrak{a}$ is an integer ideal in $\mathbf{K}$ and $\overline{\cdot}$ denotes the embedding $\sigma : \sqrt{d} \to -\sqrt{d}$. There exist Z_1 and $\alpha \in \mathbf{K}$ such that $Z_1 | h_d$ 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 $\mathbf{K}$.

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

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

where a and b are two integers satisfying $a \equiv b \bmod 2$ and a and b are even if $d \equiv 3 \bmod 4$. From $X+Y\sqrt{d} > \left|X - Y\sqrt{d}\right|$ and $\rho^{-1} < \rho$, 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 $\mathbf{Q}(\sqrt{p})$. Then, we have the upper bounds*

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

Proof : We recall that the discriminant of $\mathbf{Q}(\sqrt{p})$ is bounded from above by $4p$ and we refer to Narkiewicz [11], Proposition 8.7, p. 451, 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 $\mathbf{Z}$. 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 $\overline{\mathbf{Q}}_p$ be an algebraic closure of the field $\mathbf{Q}_p$ of p-adic numbers. We denote by v_p the unique extension to $\overline{\mathbf{Q}}_p$ of the standard p-adic valuation over $\mathbf{Q}_p$, 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 $\mathbf{Q}_p \hookrightarrow \mathbf{Q}_p(\alpha_1,\alpha_2)$ and put $D = [\mathbf{Q}(\alpha_1,\alpha_2):\mathbf{Q}]/f$. 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

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

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 the lower bound

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

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*

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

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

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

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

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

Proof : This is Corollaire 2 of [7], 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 $v_p(\Lambda) = m$. In order to bound m, we apply Proposition 1 to (7) with the parameters

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

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

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

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

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

The estimate (10) remains true if α_1 and α_2 are multiplicatively independent. 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 $-b/a = (x'/y')^v$. 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 $1.4\, m \log p \geq n u \log |y'|$.

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

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

Putting

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

we have

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

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

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

Applying Proposition 2 to the lefthand side of (14) with the parameters

$$\begin{aligned} &\alpha_1 = |y/x|, \;\; \alpha_2 = |-a/b|, \;\; b_1 = n, \;\; b_2 = 1, \\ &\log A_1 = \log Y, \;\; \log A_2 = 2 \log A, \;\; b' = \frac{n}{2 \log A} + \frac{1}{\log Y} \leq \frac{n}{\log A}, \end{aligned}$$

we obtain

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

provided that α_1 and α_2 are multiplicatively independent and $|\alpha_2| \geq 1$. 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 have

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

hence

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

Finally, by (8), (10), (11) and (16), we obtain

$$n \leq 34000\, p \log p \log A,$$

as claimed. $\square$

5. Proof of Theorems 1 and 2

Lemma 1 shows that Eq. (3) and Eq. (4) have no solution with $y = 1$. Thus, in all this section, we assume that y is at least equal to 2.

$\star$ *The case m even.*

Let (x, y, m, n) be a solution of Eq. (3) or Eq. (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

$$n \leq 48000\, p \log p,$$

which proves 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 Eq. (3) or Eq. (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 Eq. (3) and Eq. (4).*

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

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

where $\overline{\varepsilon}$ denotes the conjugate of ε over $\mathbf{Q}$ 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

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

and we put

$$\Lambda_u := \left(\frac{\varepsilon}{\overline{\varepsilon}}\right)^v - (\tau\rho^2)^t. \tag{21}$$

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 $\tau\,\rho^2$ are multiplicatively independent algebraic numbers, which, moreover, are p-adic units, since $\gcd(x, y) = 1$. Clearly, $v_p(\Lambda_u) = m/2$. In order to bound m, we apply Proposition 1 to (21) with the following parameters

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

Using Lemma 4 and the upper bound $\log\sqrt{p} \leq 1.31 \log\varepsilon$ deduced from Lemma 3 (the worst case occurs for $p = 13$ and $\varepsilon = (1 + \sqrt{13})/2$), we see that we can set

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

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

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

• *The case of equation (4).*

The result is clearly true if $m = 1$, thus we assume $m \geq 3$. From (18), we infer that $\varepsilon^v\, \rho^{-t} \leq 2\, p^{m/2}$, whence

$$2v \log \varepsilon \leq 2t \log \rho + \log 4 + m \log p.$$

Together with (22), it yields

$$2vm \leq 1232\, p\, (\log p)^{-3}\, R_p\, (m \log p + \log 4 + 2t R_p)\, \max\bigl\{\log v + 1.1, 5 \log p\bigr\}^2. \tag{23}$$

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

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

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

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

and

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

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

$$n \leq 44450\, p\, h_p\, R_p\, (R_p + 0.5),$$

whence, using $p \geq 3$ and the upper bounds for R_p and $h_p\, R_p$ given by Lemma 4, we obtain

$$n \leq 2.6\, 10^5\, p^2\, \log^2 p. \tag{25}$$

Assume now that $\max\bigl\{\log v + 1.1, 5 \log p\bigr\} = \log v + 1.1$. By (24), we then have

$$v \leq 1778\, p\, (\log p)^{-2}\, R_p\, (R_p + 0.5)\, \bigl(\log v + 1.1\bigr)^2.$$

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 $v \leq \gamma\, p\, R_p\, (R_p + 0.5)$, with a suitable constant γ. Since $p \geq 7$, we see that γ must satisfy the inequality $\gamma \geq 470\, (\log \gamma + 7.46)^2$. Thus, we may choose $\gamma = 1.8\, 10^5$ and, using (19) and the upper bounds for R_p and $h_p\, R_p$ given by Lemma 4, we get

$$n \leq 5.6\, 10^5\, p^2\, \log^2 p. \tag{26}$$

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

$$n \leq 5.6\, 10^5\, p^2\, \log^2 p,$$

as claimed.

- *The case of equation (3).*

Dividing (19) by $\varepsilon^v\, \rho^{-t}$, we obtain

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

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

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

Otherwise $\Lambda_a < 1/2$ and we get
$$\bigl|\log(1-\Lambda_a)\bigr| \leq 2\Lambda_a. \tag{29}$$
We apply Proposition 2 to the linear form
$$\left| v\log\left|\frac{\varepsilon}{\overline{\varepsilon}}\right| - t\log(\rho^2)\right| \leq \left| v\log\left(\frac{\varepsilon}{\overline{\varepsilon}}\right) - t\log(\tau\rho^2)\right| \leq \bigl|\log(1-\Lambda_a)\bigr|$$
with the following parameters :
$$\alpha_1 = |\varepsilon/\overline{\varepsilon}|,\ \ \alpha_2 = \rho^2,\ \ b_1 = v,\ \ b_2 = t,\ \ D = 2,$$
$$\log A_1 = \log\varepsilon,\ \ \log A_2 = \log\rho = R_p,\ \ b' = \frac{t}{2\log\varepsilon} + \frac{v}{2\,R_p}.$$
It follows from Lemma 4 and $\varepsilon \geq (1+\sqrt{13})/2$ that $b' \leq 1.64v$, and, using (29), we obtain
$$\log 2 + \log\Lambda_a \geq -517\,R_p\,\max\{\log v + 0.68, 5\}^2\,\log\varepsilon,$$
hence, by (27),
$$v\log\varepsilon - t\log\rho \leq \log 4 + (m\log p)/2 + 517\,R_p\,\max\{\log v + 0.68, 5\}^2\,\log\varepsilon. \tag{30}$$
From (22), (29) and (30) we infer that
$$\begin{aligned} v\log\varepsilon - tR_p \leq \log 4 &+ 517\,R_p\,\max\{\log v + 0.68, 5\}^2\,\log\varepsilon \\ &+ 616\,p\,(\log p)^{-2}\,R_p\,\max\bigl\{\log v + 1.1, 5\log p\bigr\}^2\,\log\varepsilon. \end{aligned} \tag{31}$$

First, assume that $\varepsilon < \exp\{2R_p\}$. From (18), we get $\varepsilon^v\,\rho^{-t} > y^{n/2}$, hence
$$v\log\varepsilon - t\log\rho > (n\log y)/2. \tag{32}$$
However, we have
$$\frac{\log\varepsilon}{\log y} \leq \frac{2R_p}{\log 3}, \tag{33}$$
since $y > 1$ is odd, and we deduce from (31), (32) and (33) that
$$\begin{aligned} n \leq 2.6 &+ 1883\,R_p^2\,\max\{\log n + 0.68, 5\}^2 \\ &+ 2243\,p\,(\log p)^{-2}\,R_p^2\,\max\bigl\{\log n + 1.1, 5\log p\bigr\}^2. \end{aligned}$$
As before, we search an upper bound for n of the shape $n \leq \gamma\,p^2\,\log^2 p$. Using Lemma 4 and a few calculation, we show that it suffices that γ satisfies
$$\gamma \geq 0.3 + 3214\,\{\log\gamma + 3.1\}^2 + 9508\,\{\log\gamma + 3.5\}^2,$$
thus we can choose $\gamma = 4.5\,10^6$, which gives the bound
$$n \leq 4.5\,10^6\,p^2\,\log^2 p. \tag{34}$$

Assume now that $\varepsilon \geq \exp\{2R_p\}$. Thus we have
$$v\log\varepsilon - tR_p \geq (v\log\varepsilon)/2, \tag{35}$$

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

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

hence, by (19),

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

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, it suffices to apply Lemma 2 to the polynomials $x^2 \pm y^n$, where $3 \le n \le 4.5\, 10^6\, p^2 \log^2 p$. $\square$

References

[1] Y. Bugeaud, *On the diophantine equation* $x^2 - 2^m = \pm\, y^n$, submitted.

[2] Y. Bugeaud and M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory, to appear.

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

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Clarendon Press, Oxford, 1990.

[5] Ko Chao, *On the diophantine equation* $x^2 = y^n + 1,\ xy \neq 0$, Sci. Sinica 14 (1965), 457–60.

[6] S. V. Kotov, *Ueber die maximale Norm der Idealteiler des Polynoms* $\alpha x^m + \beta y^n$ *mit den algebraischen Koeffizienten*, Acta Arith. 31 (1976), 219–230.

[7] M. Laurent, M. Mignotte and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321.

[8] Maohua Le, *On the generalized Ramanujan-Nagell equation III*, Dongbei Shuxue 4 (1988), 180–184.

[9] Maohua Le, *The diophantine equation* $x^2 + D^m = p^n$, Acta Arith. 52 (1989), 255–265.

[10] Maohua Le, *A note on the diophantine equation* $(x^m - 1)/(x-1) = y^n$, Acta Arith. 64 (1993), 19–28.

[11] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Berlin, 1990.

[12] 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.

[13] M. Toyoizumi, *On the diophantine equation* $x^2 + D^m = p^n$, Acta Arith. 42 (1983), 303–309.

Yann Bugeaud
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG (FRANCE)

e-mail : bugeaud@pari.u-strasbg.fr