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

Yann Bugeaud (Strasbourg)

Abstract. One of the purposes of this note is to correct the proof of a recent result of Y. Guo & M. Le on the equation $x^2 - 2^m = y^n$. Moreover, we prove that the diophantine equation $x^2 - 2^m = \pm\, y^n$, x, y, m, $n \in \mathbf{N}$, $\gcd(x, y) = 1$, $y > 1$, $n > 2$ has only finitely many solutions, all of which satisfying $n \le 7.3\,10^5$.

1991 *Mathematics Subject Classification.* Primary 11D61, 11J86. *Key words.* exponential equations, linear forms in logarithms.

1. Introduction

Very recently, Yongdong Guo & Maohua Le [2] considered the diophantine equation

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

where $\mathbf{N}$ denotes the set of strictly positive integers. They claimed that (1) has only finitely many solutions, all of which satisfying $n < 2.10^9$. Unfortunately, their proof is incorrect, since they misuse a result of Ping-Ping Dong. Indeed, the $|\Lambda|$ occurring in the statement of Lemma 1 in [2] denotes the p-adic absolute value of Λ and not its archimedean absolute value. Consequently, their inequality (14) is not proved. Fortunately, it happens that the idea of using both archimedean and non-archimedean linear forms in logarithms can be applied and leads to the proof of a slight sharpening of the Theorem in [2], however some extra work is needed.

In parallel with equation (1), we also treat the diophantine equation

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

Maohua Le [6, inequality (22)] applies a theorem of Shorey, Van der Poorten, Tijdeman & Schinzel [7, Theorem 2] to show that there exists some effective constant c_0 such that $n < c_0$ for any solution (x, y, m, n) of (2). However, he does not give an explicit value for c_0, which has to be very large, in view of the method of proof. Here, we use a totally different argument in order to compute a rather small bound for n.

The main tools of our proofs are the sharp estimates for linear forms in two logarithms in archimedean and non-archimedean metrics, due to Laurent, Mignotte & Nesterenko [5] and Bugeaud & Laurent [1], respectively.

2. Statement of the results

Theorem. *If (x, y, m, n) is a solution of equation (1) or equation (2), then m and n are odd and we have*

$$n \leq 5.5\,10^5 \quad \textit{and} \quad n \leq 7.3\,10^5,$$

respectively. Moreover, equations (1) and (2) have only finitely many solutions.

Remark : The hypothesis $n > 2$ in equation (1) is necessary. Indeed, for $m \geq 3$, a solution of $x^2 - 2^m = y^2$ is given by $(x, y) = (2^{m-2} + 1, 2^{m-2} - 1)$.

3. Auxiliary results

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

Proof : The lemma immediately follows from Satz 3 of Hyyrö [3]. □

For an integer x, we denote by $P[x]$ its greatest prime factor.

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, depending only on a, b and n, such that*

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

Proof : This is a particular case of a theorem due to Kotov [4]. □

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

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

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 the lower bound

$$v_p(\Lambda) \leq \frac{18p(p^f-1)}{(p-1)(\log p)^4} D^4 \left(\max\left\{\log b' + \log\log p + 0.4, \frac{15\log p}{D}, 10\right\}\right)^2 \log A_1 \, \log A_2.$$

Proof : This is Théorème 4 of [1] with the choice $(\mu,\nu)=(15,10)$. □

Proposition 2. *Let $\alpha_1 \geq 1$ and $\alpha_2 \geq 1$ 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

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

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

$$\log |\Lambda| \geq -24.7\, D^4 \left(\max\{\log b' + 0.18, 0.5, 20/D\}\right)^2 \log A_1 \, \log A_2.$$

Proof : This is Corollaire 2 of [5], where the numerical constants are given in Tableau 2 and correspond to the choice $h_2 = 20$. Notice that the hypotheses of the proposition imply that $\mathrm{h}(\alpha_i) \leq |\log \alpha_i|/D$. □

4. Proof of the Theorem

- *Elementary analysis of equations (1) and (2).*

Let (x, y, m, n) be a solution of (1) with $n \geq 4$ and $2|n$. Then we have

$$(x + y^{n/2})(x - y^{n/2}) = 2^m$$

and, since x and y are odd, it follows that $x + y^{n/2} = 2^{m-1}$ and $x - y^{n/2} = 2$. Hence, we get $y^{n/2} = 2^{m-2} - 1$, which is impossible by Lemma 1. Consequently, n must be odd. Moreover, reasoning modulo 4, we easily see that (2) has no solution with even n.

Now let (x, y, m, n) be a solution of (1) or (2) and assume that m is even. There exists $\delta \in \{1, -1\}$ such that $(x - 2^{m/2})(x + 2^{m/2}) = \delta y^n$ and, since x is odd, we get

$$x + 2^{m/2} = y_1^n, \;\; x - 2^{m/2} = \delta y_2^n,$$

with y_1 and y_2 positive integers, and we deduce that $2^{(m+2)/2} = y_1^n - \delta y_2^n$. Since x, y_1, y_2 and n (see above) are odd, the quotient $(y_1^n - \delta y_2^n)/(y_1 - \delta y_2)$ is an odd integer and it follows that $y_1^n - \delta y_2^n = y_1 - \delta y_2$, a contradiction. Hence n and m are both odd integers.

For any α in $\mathbf{Q}(\sqrt{2}) =: \mathbf{K}$, denote by $[\alpha]$ the principal ideal of $\mathbf{K}$ generated by α. From the equation $x^2 - 2^m = \delta y^n$, we get

$$\left[x + 2^{(m-1)/2}\sqrt{2}\,\right] \left[x - 2^{(m-1)/2}\sqrt{2}\,\right] = [y]^n$$

and there exists β in $\mathbf{Z}[\sqrt{2}]$, the ring of algebraic integers in $\mathbf{K}$, such that

$$\left[x + 2^{(m-1)/2}\sqrt{2}\,\right] = [\beta]^n, \tag{3}$$

for $\gcd\left(\left[x + 2^{(m-1)/2}\sqrt{2}\,\right], \left[x - 2^{(m-1)/2}\sqrt{2}\,\right]\right) = [1]$ and $\mathbf{K}$ has unique factorisation.

Put $\rho = 1 + \sqrt{2}$, then $\rho^{-1} = \sqrt{2} - 1$ and ρ is the fundamental unit of $\mathbf{K}$. We infer from (3) that

$$x + 2^{(m-1)/2}\sqrt{2} = \delta'\, \beta^n\, \rho^u,$$

where u is an integer and $\delta' = \pm 1$. As n is odd, using Euclidean division, we can write $\delta'\, \beta^n \rho^u = (a + b\sqrt{2})^n\, \rho^{-t}$, with $0 < t \leq n$. Set $\tau := 1$ or $\tau := -1$ according as t is even or odd. Then $a^2 - 2b^2 = \tau\,\delta y$ and we infer from $x + 2^{(m-1)/2}\sqrt{2} > \left|x - 2^{(m-1)/2}\sqrt{2}\right|$ and $\rho^{-1} < \rho$ that $a + b\sqrt{2} > |a - b\sqrt{2}|$. Thus we have $a > 0$ and $b > 0$. Finally, setting $\varepsilon := a + b\sqrt{2}$, we get in both cases of equations (1) and (2)

$$\begin{cases} x + 2^{(m-1)/2}\sqrt{2} &= \varepsilon^n\,\rho^{-t} \\ x - 2^{(m-1)/2}\sqrt{2} &= (\tau\,\overline{\varepsilon})^n\,\rho^t. \end{cases} \tag{4}$$

- *An upper bound for m valid for the solutions of both equations (1) and (2).*

From the system (4) we deduce the equation

$$2^{(m+1)/2}\sqrt{2} = \varepsilon^n\,\rho^{-t} - (\tau\,\overline{\varepsilon})^n\,\rho^t, \tag{5}$$

and we put

$$\Lambda_u := \left(\frac{\varepsilon}{\tau\,\overline{\varepsilon}}\right)^n - \rho^{2t}. \tag{6}$$

Since $\tau\,\varepsilon/\overline{\varepsilon}$ is a root of the irreducible polynomial $\varepsilon\,\overline{\varepsilon}X^2 - \tau\,(\varepsilon^2 + \overline{\varepsilon}^2)X + \varepsilon\overline{\varepsilon}$, we have $\mathrm{h}(\tau\,\varepsilon/\overline{\varepsilon}) = \log\varepsilon$ and $\tau\,\varepsilon/\overline{\varepsilon}$ is not a unit. Thus $\tau\,\varepsilon/\overline{\varepsilon}$ and ρ^2 are multiplicatively independent algebraic numbers, which, moreover, are 2-adic units, since a is odd. Clearly, $v_2(\Lambda_u) = (m+2)/2$. In order to bound m, we apply Proposition 1 to (6) with the following parameters

$$\alpha_1 = \tau\,\varepsilon/\overline{\varepsilon},\ \ \alpha_2 = \rho^2 = 3 + 2\sqrt{2},\ \ b_1 = n,\ \ b_2 = t,\ \ p = 2,\ \ D = 2,\ \ f = 1,$$
$$\log A_1 = \log\varepsilon,\ \ \log A_2 = \log(1+\sqrt{2}),\ \ b' = \frac{n}{2\log(1+\sqrt{2})} + \frac{t}{2\log\varepsilon}$$

and we get, in both cases of equations (1) and (2),

$$m + 2 \le 4400\,\max\{\log b' + 0.034, 10\}^2\,\log\varepsilon. \tag{7}$$

- *The case of equation (2).*

Here, we have $\delta = -1$, $\tau\overline{\varepsilon} < 0$ and $x < 2^{(m-1)/2}\sqrt{2}$. From (5), we deduce that $\varepsilon^n\,\rho^{-t} \le 2^{(m+1)/2}\sqrt{2}$, whence

$$2n\log\varepsilon \le 2t\log\rho + (m+2)\log 2.$$

Together with (7), we obtain

$$2n(m+2) \le 4400\,\big((m+2)\log 2 + 2t\log\rho\big)\,\max\{\log b' + 0.034, 10\}^2. \tag{8}$$

Since $2^m > y^n$, we have $m\log 2 > n\log y$ and

$$\frac{t}{m+2} \le \frac{n}{m} \le \frac{\log 2}{\log y} \le \frac{\log 2}{\log 3}.$$

Moreover, $b' \le n\Big(\dfrac{1}{2\log\rho} + \dfrac{1}{2\log\varepsilon}\Big) \le 0.94\, n$, since $\varepsilon \ge 1 + 2\sqrt{2}$. Hence, together with (8), we get

$$n \le 3972 \ \max\{\log n - 0.02, 10\}^2$$

and

$$n \le 7.3\,10^5,$$

as claimed.

- *The case of equation (1).*

Here, we have $\delta = 1$, $\tau\,\bar\varepsilon > 0$ and $x > 2^{(m-1)/2}\sqrt{2}$. Dividing (5) by $\varepsilon^n\,\rho^{-t}$, we obtain

$$\frac{2^{(m+1)/2}\sqrt{2}}{\varepsilon^n\,\rho^{-t}} = \frac{2^{(m+1)/2}\sqrt{2}}{x + 2^{(m-1)/2}\sqrt{2}} = 1 - \Big(\frac{\tau\,\bar\varepsilon}{\varepsilon}\Big)^n \rho^{2t} =: \Lambda_a. \tag{9}$$

If $\Lambda_a \ge 1/2$, then we have $2^{(m+3)/2}\sqrt{2} \ge \varepsilon^n\,\rho^{-t}$ and

$$2n\log\varepsilon - 2t\log\rho \le (m+4)\log 2. \tag{10}$$

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

$$\big|\log(1-\Lambda_a)\big| \le 2\Lambda_a. \tag{11}$$

We apply Proposition 2 to the linear form

$$\big|\log(1-\Lambda_a)\big| = \Big|n\log\Big(\frac{\varepsilon}{\tau\,\bar\varepsilon}\Big) - t\log(3+2\sqrt{2})\Big|$$

with the following parameters :

$$\begin{gathered}\alpha_1 = \tau\,\varepsilon/\bar\varepsilon,\ \ \alpha_2 = \rho^2 = 3+2\sqrt{2},\ \ b_1 = n,\ \ b_2 = t,\ \ D = 2,\\ \log A_1 = \log\varepsilon,\ \ \log A_2 = \log(1+\sqrt{2}),\ \ b' = \frac{n}{2\log(1+\sqrt{2})} + \frac{t}{2\log\varepsilon}\end{gathered}$$

and, by (11), we obtain

$$\log 2 + \log\Lambda_a \ge -349\ \max\{\log b' + 0.18, 10\}^2\ \log\varepsilon,$$

hence, by (9),

$$n\log\varepsilon - t\log\rho \le \big((m+4)\log 2\big)/2 + 349\ \max\{\log b' + 0.18, 10\}^2\ \log\varepsilon. \tag{12}$$

From (7), (10) and (12) we infer that

$$\begin{aligned} n\log\varepsilon - t\log\rho \le \log 2 + 1525\ \max\{\log b' + 0.034, 10\}^2\ \log\varepsilon \\ +349\ \max\{\log b' + 0.18, 10\}^2\ \log\varepsilon. \end{aligned} \tag{13}$$

In the other hand, we have

$$n \log \varepsilon - t \log \rho \geq n \left(1 - \frac{\log \rho}{\log \varepsilon}\right) \log \varepsilon.$$

In order to get a better bound for n, we pay a particular attention to the smallest value of ε. To this end, we put $\mathcal{E} = \{1+2\sqrt{2}, 1+3\sqrt{2}, 1+4\sqrt{2}, 1+5\sqrt{2}, 3+\sqrt{2}, 5+\sqrt{2}, 5+2\sqrt{2}\}$ and we assume that $\varepsilon \notin \mathcal{E}$. Since $\varepsilon := a + b\sqrt{2}$ with coprime positive integers a and b and with odd a, we then have $\varepsilon \geq 7 + \sqrt{2}$ and $\left(1 - \frac{\log \rho}{\log \varepsilon}\right)^{-1} \leq 1.71$. Moreover, $b' \leq 0.81\, n$ and, using (13), we get the upper bound

$$n \leq 0.56 + 2608 \max\{\log b' - 0.17, 10\}^2 + 597 \max\{\log b' - 0.03, 10\}^2. \tag{14}$$

We have to treat separately the cases when ε belongs to $\mathcal{E}$. Then we have $y = \tau\, \varepsilon\, \overline{\varepsilon}$ and, using the lower bound $\varepsilon^n \rho^{-t} \geq y^{n/2}$ together with $\log \varepsilon / \log y \leq 0.77$, we infer from (13) that (14) holds too. Thus, we obtain the upper bound

$$n \leq 5.5\, 10^5,$$

which completes the proof of the first part of the Theorem.

It only remains to show that the solutions of equations (1) and (2) are in finite number and are effectively computable. To this end, it suffices to apply Lemma 2 to the polynomials $x^2 \pm y^n$, where $3 \leq n \leq 7.3\, 10^5$. □

References

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

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

[3] S. Hyyrö, *Ueber das Catalansche Problem*, Ann. Univ. Turku, Ser AI, 79 (1964), 3–10.

[4] 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.

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

[6] Maohua Le, *The Diophantine Equation* $x^2 + D^m = 2^{n+2}$, Comment. Univ. St Pauli 43 (1994), 127–133.

[7] 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.

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

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