ANNALES

DE

L'INSTITUT FOURIER

Pietro CORVAJA & Umberto ZANNIER

Finiteness of odd perfect powers with four nonzero binary digits

Tome 63, n° 2 (2013), p. 715-731.

<http://aif.cedram.org/item?id=AIF_2013__63_2_715_0>

Ann. Inst. Fourier, Grenoble
63, 2 (2013) 715-731

FINITENESS OF ODD PERFECT POWERS WITH FOUR NONZERO BINARY DIGITS

by Pietro CORVAJA & Umberto ZANNIER (*)

Abstract. — We prove that there are only finitely many odd perfect powers in $\mathbb{N}$ having precisely four nonzero digits in their binary expansion. The proofs in fact lead to more general results, but we have preferred to limit ourselves to the present statement for the sake of simplicity and clarity of illustration of the methods. These methods combine various ingredients: results (derived from the Subspace Theorem) on integer values of analytic series at S-unit points (in a suitable ν-adic convergence), Roth's general theorem, 2-adic Padé approximations (by integers) to numbers in varying number fields and lower bounds for linear forms in two logarithms (both in the usual and in the 2-adic context).

Résumé. — Nous démontrons la finitude de l'ensemble des puissances pures impaires ayant quatre chiffres non nuls dans leur écriture binaire. La preuve de ce théorème amène naturellement à des énoncés plus généraux, mais, pour simplifier, nous avons préféré nous borner à ce résultat. Notre méthode combine plusieurs ingrédients : des résultats (dérivés du théorème du sous-espace) sur les valeurs entières de séries analytiques aux points S-unités, le théorème de Roth généralisé, les approximations de Padé 2-adiques de nombres algébriques dans un corps variable, des minorations de formes linéaires en deux logarithmes (par rapport aux valeurs absolues archimédiennes et 2-adique).

1. Introduction

In the paper [3] it was shown among other things how to "classify" the perfect squares (or higher powers) having at most three nonzero digits in a given scale (see the Corollary and the final remarks in the Introduction therein). For instance, from those considerations one may easily derive that: *For $d \geqslant 2$, the perfect d-th powers in $\mathbb{N}$ having at most three nonzero digits in the binary scale form the union of finitely many sets of the shape $\{q2^{md} : m \in \mathbb{N}\}$ and, if $d = 2$, also the set $\{(2^a + 2^b)^2 : a, b \in \mathbb{N}\}$.*

Keywords: Diophantine equations, diophantine approximations, perfect powers.
Math. classification: 11J25, 11J86, 11J68.
(*) First author research partially supported by ERC program "Diophantine Problems".

One may get a similar conclusion on replacing the binary scale with the scale of any integer $g > 1$, and also interpreting "perfect power" in any given number field in place of $\mathbb{Q}$; however those methods would not apply in full generality if "three" would be replaced with "four". The purpose of the present note is to combine the said methods with a further one, to prove the following theorem:

THEOREM 1.1. — *There are only finitely many odd perfect powers in* $\mathbb{N}$ *having precisely four nonzero digits in their representation in the binary scale.*

Note that this asserts the finiteness of the set of solutions of the diophantine equation

$$y^d = 1 + 2^{m_1} + 2^{m_2} + 2^{m_3}, \quad d \geqslant 2, \quad 0 < m_1 < m_2 < m_3, \quad y \in \mathbb{Z}. \tag{1.1}$$

Of course removing the restriction "odd" leads to the diophantine equation $y^d = 2^{m_0} + 2^{m_1} + 2^{m_2} + 2^{m_3}$, for natural numbers y and $m_0 < m_1 < m_2 < m_3$, and this may be reduced to the previous one, since m_0 has then to be a multiple of d. Thus Theorem 1.1 may be rephrased by saying that:
The set of perfect powers having precisely four nonzero binary digits is a finite union of sets of the shape $\{q2^{md} : m \in \mathbb{N}\}$.

We shall split the theorem into two parts, according whether d is fixed or is larger than a certain computable number. More precisely, we shall prove the following two propositions, which imply Theorem 1.1 at once.

PROPOSITION 1.2. — *For each integer* $d \geqslant 2$, *equation (1.1) has only finitely many integer solutions.*

The proof of this result shall itself fall under various cases, depending on the relative magnitude of m_1, m_2, m_3. When either the ratio m_2/m_3 stays away from 1 or the ratio m_1/m_3 stays away from 0, we shall rely on results from [4] (which in turn depend on the Schmidt Subspace Theorem). An intermediate case of bounded m_1 shall be derived as an easy consequence of Roth's general theorem, whereas the remaining cases of Proposition 1.2 shall be dealt with by Padé approximation.

PROPOSITION 1.3. — *There exists a computable number* d_0 *such that equation (1.1) has no integer solutions for* $d \geqslant d_0$.

For this we shall use lower bounds for linear forms in two logarithms, both with respect to the usual absolute value and with respect to a 2-adic one; this last tool shall be combined again with the Padé approximation used for the previous proposition.

Acknowledgements. — One of our main motivations for this investigation has been a certain question in arithmetic dynamics which leads to similar (but more general) diophantine equation. Here we thank Dragos Ghioca for raising such issues to our attention and for relevant correspondence.

While preparing the present paper we learned from Yann Bugeaud that in very recent joint work with Mike Bennett and Maurice Mignotte [1] they have independently proved related effective results, and in particular that one may take $d_0 = 5$ in Proposition 1.3. Especially in view of this, we shall be brief in our proof of such proposition, also omitting any explicit value for d_0, since our argument would lead to admissible values rather larger than 5. The method of these authors is in part similar to our method for Proposition 1.3, but Padé approximations do not explicitly appear, whereas they use more refined versions of lower bounds for linear forms in logarithms. We thank Bugeaud for informing us of their work and for valuable comments and references, and the mentioned authors for sending us promptly a version of their paper.

We pause for a few other remarks:

Remark 1.4.

(i) Our conclusions are certainly of a very special type; however the present methods could be easily extended to cover other diophantine equations (with suitable modification of the statement), as for instance $y^d = 1+c_1g^{m_1}+c_2g^{m_2}+c_3g^{m_3}$, where d, g are any given integers $\geqslant 2$ and c_1, c_2, c_3 are any fixed rationals, and even more general ones in S-units. [(1)] We have chosen the present instance for simplicity and because it seems to us amusing. Also, the proof below shows how sometimes different principles can be combined in dealing with equations in S-units. The interested reader, on looking carefully at the arguments, shall be easily able to see what kind of generality can be extracted from the method.

(ii) A natural question is whether, given $d \geqslant 2$, the same finiteness of Proposition 1.2 may be proved allowing y to be an integer in any given number field. (By Kummer theory, this would amount to any equation like (1.1) but with ρy^d in place of y^d, where ρ is a given rational number.) For the above alluded result for "three digits" (in place of "four digits") this greater generality is immaterial for the methods. The same holds for the first three cases of the proof of Proposition 1.2; however this seemingly does not extend to the last step, involving Padé approximants.

[(1)] However changing the "1" into an arbitrary rational c_0 leads to problems, as pointed out in (ii), (iii) below.

(iii) Replacing "four" with "five" again leads to more difficult issues, which we do not know how to deal with. The same holds on changing "binary scale" with "scale of three", say. [(2)] To solve these kind of problems may be interesting, because it is likely it would lead to overcome important obstacles for other, more significant, diophantine equations.

(iv) Our method for Proposition 1.2 is ineffective at various stages and does not allow, not even for some d, to find the actual solutions to (1.1). We also note that there are some solutions; *e.g.*,

$$\begin{aligned} d=2: \quad & 13^2 = 1+2^3+2^5+2^7,\ 15^2 = 1+2^5+2^6+2^7, \\ & 47^2 = 1+2^5+2^7+2^{11},\ 111^2 = 1+2^5+2^{12}+2^{13}; \\ d=3: \quad & 3^3 = 1+2+2^3+2^4. \end{aligned}$$

As remarked above, the paper [1] proves that there are no solutions with $d \geqslant 5$.

2. Proof of Proposition 1.2

We have to prove that, for given $d \geqslant 2$, equation (1.1) has only finitely many integer solutions y, m_1, m_2, m_3 (also called "points") restricted as therein.

Note that we may assume that d is a prime number (which we shall use merely to restrict to d being either 2 or an odd integer). Also, in the sequel, for notational convenience we shall drop any index referring to a sequence, and shall work with a given solution, assuming tacitly that it runs through an infinite sequence (or possibly into infinite subsequences with further properties specified along the way); so in particular the integer m_3 shall tend to ∞. The notion of convergence shall be referred to such (sub)sequences. Our aim shall be to derive a contradiction.

We shall denote by $h(\cdot)$ the (logarithmic) Weil absolute height in $\overline{\mathbb{Q}}$. The absolute values of a number field k shall be normalized according to the standard normalization of the places they induce on $\mathbb{Q}$.

As anticipated, the proof shall fall into four cases; the first two of them are very close to each other, and implicitly involve methods similar to those

[(2)] Similarly to (ii) above, the reason now is that we can have 2 as the first digit, and this is not a perfect d-th power; this affects the arguments using Padé approximation. Of course for a scale larger than 2 finiteness does not hold: one would have also to take into account identities like $(1+T)^3 = 1+3T+3T^2+T^3$ to locate all the solutions into finitely many families; these would appear through Lemma 2.1 below. In this respect see also Remark 2.2.

of the already quoted paper [3], which we shall exploit by invoking results from [4]. (3) The third case shall be derived as an easy consequence of the general Roth's theorem (as described *e.g.* in [2]) or [10]). The fourth case shall be dealt with via Padé approximation, widely used in diophantine problems (however often in applications of somewhat different kind).

First case. — There exists an infinite subsequence of solutions such that $m_2 \leqslant \frac{15}{16} m_3$. (4)

In the present case we divide out equation (1.1) by 2^{m_3}, and we put put $n_1 = m_3 - m_2$, $n_2 = m_3 - m_1$, $n_3 = m_3$, $x_i := 2^{-n_i}$ for $i = 1, 2, 3$; we get $y^d 2^{-m_3} = 1 + x_1 + x_2 + x_3$.

Let us now introduce the series $F(X_1, X_2, X_3) \in \mathbb{Q}[[X_1, X_2, X_3]]$ defined by

$$F(X_1, X_2, X_3) = (1 + X_1 + X_2 + X_3)^{\frac{1}{d}} = 1 + \frac{1}{d}(X_1 + X_2 + X_3) + \frac{(1-d)}{2d^2}(X_1 + X_2 + X_3)^2 + \cdots, \tag{2.1}$$

obtained on expanding with the binomial theorem in the obvious way. This certainly converges absolutely for complex X_1, X_2, X_3 with $|X_i| \leqslant \frac{1}{4}$, to the function which is continuous therein, takes the value 1 at the origin and is a d-th root of $1 + X_1 + X_2 + X_3$.

In view of the property $m_2 \leqslant 15m_3/16$, we also have $n_3 > n_2 > n_1 \geqslant m_3/16$. Therefore, for large m_3 the series converges at (x_1, x_2, x_3), so that we may consider the value $z := F(x_1, x_2, x_3) \in \mathbb{C}$, to obtain

$$z^d = 1 + x_1 + x_2 + x_3 = 1 + 2^{-n_1} + 2^{-n_2} + 2^{-n_3}. \tag{2.2}$$

Letting K be the splitting field of $X^d - 2$ over $\mathbb{Q}$, we note that $z = y2^{-\frac{m_3}{d}}$ for some determination of the d-th root, so our sequence of solutions to (2.2) is defined over K. Also, letting S be the finite set of places of K consisting of the infinite ones and the ones lying above 2, we see that z is an S-integer, whereas x_1, x_2, x_3 are S-units. Further, the complex absolute value induces an absolute value on $\mathbb{Q}(z)$, and we extend this to an infinite place ν of K; so we may embed K in $\mathbb{C}$ by means of ν and still $z = F(x_1, x_2, x_3)$ with respect to ν-adic convergence.

We also have $\sum_{i=1}^{3} h(x_i) \leqslant 3m_3$, whence, noting that $\max_i |x_i|_\nu \leqslant 2^{-\frac{m_3}{16}}$,

$$\sum_{i=1}^{3} h(x_i) = O(-\log(\max_i |x_i|_\nu)). \tag{2.3}$$

(3) These results rely on the Schmidt's Subspace Theorem.

(4) The precise values $\frac{15}{16}$, and $\frac{1}{16}$ below in the Second case, are immaterial.

Further, $h(F(x_1,x_2,x_3)) = h(z) \leqslant 2m_3$. These verifications show that we are in position to apply Theorem 1 of [4][(5)] to the series F and our sequence of S-unit points (x_1,x_2,x_3). The corresponding conclusion delivers the following:

There exist a finite number of cosets $u_1H_1,\dots,u_rH_r$ of $\mathbb{G}_{\mathrm{m}}^3$, with $u_i \in \mathbb{G}_{\mathrm{m}}^3(K)$ and with H_i connected algebraic subgroups of G_{m}^3, such that:

(i) *$(x_1,x_2,x_3) \in \bigcup_{i=1}^r u_iH_i$ for all our relevant points;*
(ii) *for $i=1,\dots,r$, the restriction of $F(X_1,X_2,X_3)$ to u_iH_i coincides with a polynomial.*

Going to an infinite subsequence of solutions, we can in fact suppose that there is a single one among the said cosets which contains all of our points. Moreover, since our sequence consists of S-units, by a well-known theorem of Lang (see *e.g.* [2], Thm. 7.4.7) its Zariski closure in $\mathbb{G}_{\mathrm{m}}^3$ is anyway a finite union of cosets of algebraic subgroups, so by taking intersections with the previous coset (and then going to a further infinite subsequence) in fact we may also suppose that the sequence is Zariski-dense in our coset.

We denote by uH such coset, where $u=(\xi_1,\xi_2,\xi_3) \in \mathbb{G}_{\mathrm{m}}^3$ may be supposed to be any one of our points, so the ξ_i become powers of 2 (with negative integral exponent). This coset is not a single point, so $\dim H =: s > 0$.

Further, since our points converge ν-adically to the origin, by the equivalence between (iii) and (v) of Proposition 1 of [4], there exists a parametrization of uH given by monomials $X_i = \xi_i T_1^{a_{i1}} \cdots T_s^{a_{is}}$, $i=1,2,3$, such that $a_{ij} \geqslant 0$ for all i,j.

By property (ii) above we have that $F(X_1,X_2,X_3)$ becomes a certain polynomial in $T_1,\dots,T_s$ if the X_i are replaced by the above monomials. We have $F^d(x_1,x_2,x_3) = 1+x_1+x_2+x_3$, so, since our sequence is Zariski-dense in the coset, we have an identity $F^d(X_1,X_2,X_3) = 1+X_1+X_2+X_3$ for X_i equal to the above monomials in $T_1,\dots,T_s$.

Note now that each x_i converges ν-adically to 0. Hence if $i \neq j$ we cannot have identically $X_i = 1$ on the algebraic subgroup H. It follows that the three vectors $(a_{i1},\dots,a_{is}) \in \mathbb{N}^s$, $i=1,2,3$, are nonzero, so there exist positive integers $b_1,\dots,b_s$ such that the scalar products $l_i := \sum_{j=1}^s b_j a_{ij}$, are all positive and such that, for $i,j \in \{1,2,3\}$, $l_i = l_j$ if and only if $(a_{i1},\dots,a_{is}) = (a_{j1},\dots,a_{js})$. In view of the above, by substituting T^{b_j} for T_j we conclude that there is a nonconstant polynomial $P(T)$ such that

[(5)] In [4] the absolute values were normalized differently, but the validity of (2.3) is not affected by any change of normalizations.

$P^d(T) = 1 + \xi_1 T^{l_1} + \xi_2 T^{l_2} + \xi_3 T^{l_3}$, and on renumbering we may assume $0 < l_1 \leqslant l_2 \leqslant l_3$. (6)

Now, we have the following general

LEMMA 2.1. — *For $d \geqslant 2$, for nonzero $\xi_1, \xi_2, \xi_3 \in \mathbb{C}$ and for positive integers $l_1 \leqslant l_2 \leqslant l_3$, the polynomial $1 + \xi_1 T^{l_1} + \xi_2 T^{l_2} + \xi_3 T^{l_3}$ is a perfect d-th power of a nonconstant complex polynomial precisely in the following cases:*

A: $d = 2$, $l_1 = l_2 < l_3$ and $4\xi_3 = (\xi_1 + \xi_2)^2$.
B: $d = 2$, $l_1 < l_2 = l_3$ and $4(\xi_2 + \xi_3) = \xi_1^2$.
C: $d = 2$, $l_2 = 3l_1$, $l_3 = 4l_1$ and $8\xi_2 = -\xi_1^3$, $64\xi_3 = \xi_1^4$.
D: $d = 3$, $l_2 = 2l_1$, $l_3 = 3l_1$ and $3\xi_2 = \xi_1^2$, $27\xi_3 = \xi_1^3$.

Proof. — Let $P(T)^d = 1 + \xi_1 T^{l_1} + \xi_2 T^{l_2} + \xi_3 T^{l_3}$, for a nonconstant polynomial $P \in \mathbb{C}[T]$.

Note that for $c \in \mathbb{C}$, $1 + cT^l$ cannot have multiple roots if $l > 0$. This proves that not all the l_i may be equal.

If $d \geqslant 4$ the opening equation is impossible by virtue of a well-known easy result by Hajos (see Lemma 1 in [7]). For a direct argument, just observe that the polynomial $1 + \xi_1 T^{l_1} + \xi_2 T^{l_2} + \xi_3 T^{l_3}$ has no complex root of multiplicity 4 or more, as follows by differentiation and using a Vandermonde determinant. The same argument shows that $d = 3$ implies that the l_i are pairwise distinct. In particular, we must have $d = 2$ or $d = 3$. We could now use known results which bound the number of terms of $P(T)$, but it is simple enough to argue directly.

Let us then assume $d = 2$ first.

If $l_1 = l_2 = l$, say, then $l < l_3$ and $1 + \xi_1 T^{l_1} + \xi_2 T^{l_2} + \xi_3 T^{l_3} = 1 + \sigma T^l + \xi_3 T^{l_3}$, where $\sigma := \xi_1 + \xi_2 \neq 0$, as already observed. We have $\pm P(T) = 1 + \eta T^l + ... \gamma T^p + \delta T^q$, where $l < p < q$ and where possibly γ and/or δ vanish. Now on squaring we see that $2\eta = \sigma$ and that if $\gamma\delta \neq 0$ necessarily terms of degree $0, l, p+q, 2q$ appear in $P^2(T)$, which is impossible. Similarly if $\gamma = 0, \delta \neq 0$. Therefore $\pm P(T) = 1 + \eta T^l$, hence $l_3 = 2l$ and $\eta^2 = \xi_3$. Now we fall in case A above.

If $l_1 < l_2 = l_3 = l$ things are completely similar and we fall in case B.

From now on let us assume that $l_1 < l_2 < l_3$. For a suitable choice of the sign, we have $P(T) = \pm\sqrt{1 + \xi_1 T^{l_1}} + O(T^{l_2})$ (in the power series sense). Differentiating we find $P'(T) = \pm\frac{l_1}{2}\frac{\xi_1 T^{l_1 - 1}}{1 + \xi_1 T^{l_1}}\sqrt{1 + \xi_1 T^{l_1}} + O(T^{l_2 - 1})$. Using these two equations to eliminate the square-root term, we find that

(6) This might destroy the inequalities among n_1, n_2, n_3, but this shall be immaterial for what follows.

$2(1+\xi_1 T^{l_1})P'(T) - l_1\xi_1 T^{l_1-1}P(T) = O(T^{l_2-1})$. The left side is a nonzero [(7)] polynomial of degree $\leqslant l_1 + \frac{l_3}{2} - 1$, hence $l_2 \leqslant l_1 + \frac{l_3}{2}$ and $l_3 - l_2 \geqslant \frac{l_3}{2} - l_1$. It easily follows that $\max(l_1, l_3 - l_2) \geqslant \frac{l_3}{4}$. By replacing $P(T)$ if necessary with $\xi_3^{-\frac{1}{2}} T^{\frac{l_3}{2}} P(T^{-1})$, and ξ_1, ξ_2, ξ_3 resp. by $\xi_2/\xi_3, \xi_1/\xi_3, 1/\xi_3$, we may thus assume that $l_1 \geqslant \frac{l_3}{4}$ and that $l_3 - l_2 \leqslant l_1$. (Note that this substitution does not affect the statement of the lemma.)

We write $1 + \xi_1 T^{l_1} + \xi_2 T^{l_2} + \xi_3 T^{l_3} = 1 + T^{l_1}\rho(T)$, with $\rho(T) = \xi_1 + \xi_2 T^{l_2-l_1} + \xi_3 T^{l_3-l_1}$. Then, expanding $\sqrt{1+z}$ with $z := T^{l_1}\rho(T)$, we find $\pm P(T) = 1 + \frac{1}{2}T^{l_1}\rho(T) - \frac{\xi_1^2}{8}T^{2l_1} + O(T^{2l_1+1})$. On the other hand $\deg P = \frac{l_3}{2} \leqslant 2l_1$. Hence $\pm P(T)$ is a sub-sum of $1 + \frac{\xi_1}{2}T^{l_1} + \frac{\xi_2}{2}T^{l_2} - \frac{\xi_1^2}{8}T^{2l_1}$.

Assume first $l_1 > \frac{l_3}{4}$. Then a term of degree $2l_1$ cannot appear in $P(T)$, and certainly $P(T)$ cannot contain only two terms; hence $l_2 \neq 2l_1$ and $\pm P(T) = 1 + \frac{\xi_1}{2}T^{l_1} + \frac{\xi_2}{2}T^{l_2}$. But then $P(T)^2$ contains at least terms of degree $0, l_1, l_2, 2l_1, 2l_2, l_1 + l_2$, which are pairwise distinct, so we have a contradiction.

Assume now $l_1 = \frac{l_3}{4}$. Then from $l_3 - l_2 \leqslant l_1$ we have $l_2 \geqslant \frac{3l_3}{4} > 2l_1$. Hence a term of degree l_2 cannot appear in $P(T)$ and we have $\pm P(T) = 1 + \frac{\xi_1}{2}T^{l_1} - \frac{\xi_1^2}{8}T^{2l_1}$. Now $P(T)^2 = 1 + \xi_1 T^{l_1} - \frac{\xi_1^2}{4}T^{2l_1} - \frac{\xi_1^3}{8}T^{3l_1} + \frac{\xi_1^2}{4}T^{2l_1} + \frac{\xi_1^4}{64}T^{4l_1} = 1 + \xi_1 T^{l_1} - \frac{\xi_1^3}{8}T^{3l_1} + \frac{\xi_1^4}{64}T^{4l_1}$. We now fall in case C.

Let us now deal with the case $d = 3$. Similarly to the above we find that $3(1+\xi_1 T^{l_1})P'(T) - l_1\xi_1 T^{l_1-1}P(T) = O(T^{l_2-1})$, and now the left side (which is again nonzero) has degree at most $l_1 + \frac{l_3}{3} - 1$. Now this leads to $\max(l_1, l_3 - l_2) \geqslant \frac{l_3}{3}$. And thus, on replacing $P(T)$ if necessary with $\xi_3^{-\frac{1}{3}} T^{\frac{l_3}{3}} P(T^{-1})$ and ξ_1, ξ_2, ξ_3 as above (this again fits with the statement) we may assume that $l_1 \geqslant \frac{l_3}{3}$. In turn, expansion of $\sqrt[3]{1 + T^{l_1}\rho(T)}$ leads as above to $P(T) = 1 + \frac{\xi_1}{3}T^{l_1}$, up to a cube-root-of-1-factor, and it is now immediate to check that we fall into the other case predicted by the statement. This concludes the proof. □

This result implies a contradiction with our previous conclusions concerning the polynomial $P(T)$ arising from our infinite subsequence: it suffices to take into account that our ξ_1, ξ_2, ξ_3 are in $2^{\mathbb{Z}}$ and that if $l_i = l_j$ then $\xi_i \neq \xi_j$, because $x_i \neq x_j$ for $i \neq j$ (as follows from the fact that the n_i are positive and pairwise distinct). For instance, if we fall in case A, we have that $\xi_1 + \xi_2 \in 2^{\mathbb{Z}}$, which is impossible. Similarly for the case B. Further, we cannot fall neither in case C (since ξ_1, ξ_2 are positive) nor in case D (since ξ_1, ξ_2 are both 3-adic units).

[(7)] Otherwise $P(T)^2 = c(1 + \xi_1 T^{l_1})$.

Remark 2.2. — Note that the special shapes appearing in the lemma lead in fact to polynomial squares or cubes with exactly four terms. Actually, case C "almost" yields an infinite family of solutions to (1.1). In fact, on taking *e.g.* $\xi_1 = 2$ and T a power of 2, it obviously provides infinitely many integer solutions to the similar-looking equation $y^2 = 1 + 2^{m_1} - 2^{m_2} + 2^{m_3}$. The method of this paper would prove that in fact *all but finitely many solution to this last equation are obtained in this way*, namely may be parametrized by putting $T = 2^l$ in the formula $(1 + 2T - 2T^2)^2 = 1 + 4T - 8T^3 + 4T^4$.

Second case. — *There exists an infinite subsequence of solutions such that* $m_1 \geqslant \frac{1}{16} m_3$

We argue as before, keeping essentially that notation, except that now we set $x_i := 2^{m_i}$ and use a 2-adic valuation. Since $\max |x_i|_2 = |x_1|_2 \leqslant 2^{-\frac{m_3}{16}}$, for large enough m_3 (in terms of d) the series (2.1) converges in $\mathbb{Q}_2$, at the point (x_1, x_2, x_3), to a value $z := F(x_1, x_2, x_3) \in \mathbb{Q}_2$; also, we have $z^d = 1 + x_1 + x_2 + x_3$, hence $z = y\theta$ for some d-th root of unity θ. [(8)] The 2-adic place of $\mathbb{Q}$ induces a place on $\mathbb{Q}(z) \subset \mathbb{Q}_2$, which we may extend to a place ν of K, lying above 2. As before, we apply Theorem 1 of [4], this time with the present 2-adic place ν. By completely similar arguments, and applying Lemma 2.1 again, we obtain a contradiction.

We are now in position to assume that there is no infinite sequence of solutions verifying either the condition of the First case or of the Second case; and hence from now on we shall suppose that each element in our infinite sequence of solutions satisfies

$$0 < m_1 < \frac{m_3}{16}, \quad \frac{15m_3}{16} < m_2 < m_3. \tag{2.4}$$

Third case. — *There exists an infinite subsequence of solutions such that* m_1 *is bounded*

In this case we may assume that m_1 is a constant b on an infinite subsequence; we set $\Delta := 1 + 2^b$. We might use the results of [3], but it is easy to argue directly.

From the equation $y^d - \Delta = 2^{m_2}(1 + 2^{m_3 - m_2})$ we deduce, using the triangle's inequality, that there exists a fixed d-th root $\theta \in \mathbb{Q}_2$ of Δ such that for infinitely many $y \in \mathbb{Z}$, $|y - \theta|_2 \ll 2^{-m_2}$. Then setting $X - \infty := 1/X$, our equation yields

$$|y - \infty| \cdot |y - \theta|_2 \ll |y|^{-1} 2^{-m_2} \ll H(y)^{-\frac{5}{2}},$$

(8) We must in fact have $z = \pm y$, since for odd d there are no d-th roots of unity in $\mathbb{Q}_2$ except 1. However this is not needed here.

for large enough m_2, where $H(\cdot) = \exp h(\cdot)$ denotes the exponential Weil height and the constants implied in $\ll$ depend only on Δ, d. Also, note that the exponent $-5/2$ attributed to $H(y)$ is indeed admissible, in view of $|y|^d \leqslant \Delta + 2^{\frac{16}{15}m_2+1}$, so $|y| = H(y) \ll 2^{\frac{16}{30}m_2}$.

Now, the last displayed inequality eventually violates the general form of Roth's theorem, as presented for instance in [2], Ch. VI, or [10], Theorem 2.

Therefore we have a contradiction, proving that this case cannot in fact occur.

Then from now on we shall assume, as we may, to fall into the following

Fourth case. — Our solutions run through an infinite sequence satisfying (2.4) and moreover such that $m_1 \to \infty$.

In particular, we shall tacitly assume that m_1 is larger than any prescribed number.

For this case we shall argue by means of suitable Padé approximations to $(1-z)^{\frac{1}{d}}$, with the aim to approximate $(1+2^{m_1})^{\frac{1}{d}}$ with respect to a 2-adic place. We shall use certain identities derived from a well-known list by Kummer, of 24 solutions to a hypergeometric differential equation, as in Chapter II of [5]. We shall also need certain simple arithmetical properties of the involved coefficients. We thank Y. Bugeaud for informing us of the paper [6], where formulas similar to the ones below appear, together with other deductions as in the present Lemma 2.4. (In turn, the author refers to Siegel for proofs of the relevant identities.) Since our proofs are anyway short, we have decided to retain the present lemma, for the reader's convenience.

These identities shall be also crucial for the proof of Proposition 1.3, so we shall drop the above assumption that d is a prime number here.

Remark 2.3. — Naturally, Padé approximations have been widely used in Diophantine Equations, since Thue, Siegel and several others, until recent times. (See for instance the already mentioned paper by Le [6] and [2], Ch. V.) The present application follows similar lines; however two of the features important here seemingly appeared less frequently in the literature:

(i) We shall approximate (by integers) algebraic numbers (of the shape $(1+2^m)^{\frac{1}{d}}$) in a number field which is varying, whereas in many applications the targets are fixed or vary in a fixed number field; our approximations shall be with respect to a suitable 2-adic place, to targets lying in $\overline{\mathbb{Q}} \cap \mathbb{Q}_2$.

(ii) We shall consider approximations by *integers* rather than arbitrary rationals; this leads to work with "asymmetric" Padé approximations, in the sense that the bounds for the relevant polynomial degrees are not taken

to be equal. We remark that this integrality restriction on y corresponds to consider a "good" simultaneous approximation to ∞ (with respect to the usual absolute value) and to the relevant algebraic number (with respect to a 2-adic place).

Features similar to (i) and (ii) appear *e.g.* in the above quoted paper [6].

Finally, we stress that this fourth step of the proof, contrary to the previous three ones, is rather "rigid", and for instance requires a very special shape for the said target numbers; for instance, if these were replaced by *e.g.* $(c+2^m)^{\frac{1}{d}}$ (a general positive integer c) the method would not work as it stands. This represents of course a severe limitation of this technique.

As usual, $\Gamma(z)$ shall denote Euler's Gamma-function, while $(1+z)^{\frac{1}{d}}$ shall mean the binomial series $\sum_{n=0}^{\infty}\binom{\frac{1}{d}}{n}z^n \in \mathbb{Q}[[z]]$, interpreted for the moment in the formal sense; also, we shall adopt the following standard notation for a hypergeometric function:

$$F(a,b,c,z) = 1 + \frac{a\cdot b}{1\cdot c}z + \frac{a(a+1)\cdot b(b+1)}{1\cdot 2\cdot c(c+1)}z^2 + \cdots . \tag{2.5}$$

LEMMA 2.4. — *Let r,s be positive integers and set $t := r+s$. Also, put*

$$\begin{aligned} G(z) &:= \frac{\Gamma(\frac{1}{d}+1)\Gamma(1+t)}{\Gamma(\frac{1}{d}+r+1)\Gamma(s+1)}F(-\frac{1}{d}-r,-s,-t,z),\\ H(z) &:= F(\frac{1}{d}-s,-r,\frac{1}{d}+1,1-z),\\ E(z) &:= (-1)^{s+1}\frac{\Gamma(\frac{1}{d}+1)r!}{\Gamma(\frac{1}{d}-s)t!}F(-\frac{1}{d}+s+1,s+1,t+2,z). \end{aligned}$$

Then $G(z)$ and $H(z)$ are polynomials with rational coefficients, of degree resp. s,r and

$$G(z) - (1-z)^{\frac{1}{d}}H(z) = z^{t+1}E(z). \tag{2.6}$$

Finally, there is a positive integer A such that $AG(z)$ and $AH(z)$ have integer coefficients bounded in absolute value by $B := (2d)^{4t}$. More precisely, we may take $A = d^{4t}\binom{\frac{1}{d}+r}{r}$.

Proof. — Equation (2.6) appears as formula (43), Section 2.9 of [5], interpreted on using the notations (1), (17) and (21) therein, with the parameters a,b,c given by $a := -\frac{1}{d}-r$, $b := -s$, $c := -t = -r-s$.

That $G(z), H(z)$ are polynomials of the said degrees follows immediately from the defining formula (2.5) above, taking into account that $d \geqslant 2$ and that r,s are integers > 0.

Also, the coefficients in (2.5) are clearly rational if $a, b, c \in \mathbb{Q}$, as happens in our case. Moreover the term $\frac{\Gamma(\frac{1}{d}+1)\Gamma(1+t)}{\Gamma(\frac{1}{d}+r+1)\Gamma(s+1)}$ is also rational; in fact, it follows from the functional equation $\Gamma(z+1) = z\Gamma(z)$ that it equals $\binom{t}{s}/\binom{\frac{1}{d}+r}{r}$.

For the remaining assertions, let us first deal with the coefficients of $F(-\frac{1}{d}-r, -s, -t, z)$; the one of z^m vanishes for $m > s$ and is otherwise

$$\frac{(-\frac{1}{d}-r)\cdots(-\frac{1}{d}-r+m-1)\cdot(-s)(-s+1)\cdots(-s+m-1)}{m!\cdot(-t)(-t+1)\cdots(-t+m-1)}.$$

Multiplying by $\binom{t}{s} = \frac{t(t-1)\cdots(t-s+1)}{s!}$ this becomes $\pm\binom{\frac{1}{d}+r}{m}\binom{t-m}{s-m}$. Also, $\binom{\frac{1}{d}+r}{m}$ is p-integral at all primes p not dividing d (*e.g.* by p-adic continuity of binomial polynomials $\binom{x}{m}$). It is further easily seen that, for $m \leqslant t$, $d^{2t}\binom{\frac{1}{d}+r}{m}$ is p-integral also at primes p dividing d, whence it is an integer.

Now, $G(z)$ is obtained on multiplying the polynomial $F(-\frac{1}{d}-r, -s, -t, z)$ by $\frac{\Gamma(\frac{1}{d}+1)\Gamma(1+t)}{\Gamma(\frac{1}{d}+r+1)\Gamma(s+1)} = \binom{t}{s}/\binom{\frac{1}{d}+r}{r}$. Putting together these informations, and since $\binom{\frac{1}{d}+r}{m}, \binom{t-m}{s-m} \leqslant 2^t$ (for $m \leqslant t$), we obtain the sought assertion.

As to $H(z) = F(\frac{1}{d}-s, -r, \frac{1}{d}+1, 1-z)$, things are similar. We may replace $1-z$ by z, which may increase the maximal absolute value of the coefficients at most by a factor 2^t. Now, the coefficient of z^m in $F(\frac{1}{d}-s, -r, \frac{1}{d}+1, z)$ vanishes for $m > r$ and is $\frac{(\frac{1}{d}-s)\cdots(\frac{1}{d}-s+m-1)\cdot(-r)(-r+1)\cdots(-r+m-1)}{m!\cdot(\frac{1}{d}+1)\cdots(\frac{1}{d}+m)}$ otherwise, which in turn equals $\pm\binom{-\frac{1}{d}+s}{m}\frac{r(r-1)\cdots(r-m+1)}{(\frac{1}{d}+1)\cdots(\frac{1}{d}+m)}$. If we multiply this by $\binom{\frac{1}{d}+r}{r}$, we obtain (recalling $m \leqslant r$) $\pm\binom{-\frac{1}{d}+s}{m}\binom{\frac{1}{d}+r}{r-m}$. Then, the same argument as above shows that again the value $A = d^{4t}\binom{\frac{1}{d}+r}{r}$ is admissible for the claim. □

LEMMA 2.5. — *Keeping the notation of the previous lemma, let us define $G^*(z), H^*(z)$ resp. as the polynomials obtained in the same way as $G(z), H(z)$, but replacing (r, s) with $(r+1, s+1)$. Then $G^*(z)H(z) - H^*(z)G(z) = c \cdot z^{t+1}$ for some constant $c \neq 0$.*

Proof. — Both $G(z) - (1-z)^{\frac{1}{d}}H(z)$ and $G^*(z) - (1-z)^{\frac{1}{d}}H^*(z)$ are power series vanishing at the origin up to order at least $t+1$; hence, on eliminating $(1-z)^{\frac{1}{d}}$, we obtain that $G^*(z)H(z) - H^*(z)G(z)$ has order at least $t+1$ at the origin. On the other hand, this is a polynomial of degree at most $r+s+1 = t+1$, hence it is of the shape cz^{t+1}. From equation (2.6) and the similar one for G^*, H^* (where now the right side has order $\geqslant t+3$ at the origin), we find that the coefficient c of z^{t+1} is in fact up to sign the constant coefficient of $E(z)$, *i.e.* $\frac{\Gamma(\frac{1}{d}+1)r!}{\Gamma(\frac{1}{d}-s)t!}$ up to sign; this is plainly nonzero, so the lemma is proved. □

Let us now go ahead with the proof, in this fourth case. If d is odd we have necessarily $y \equiv 1 \pmod{2^{m_1}}$, and if $d = 2$ we may choose the sign of y so that $y \equiv 1 \pmod{2^{m_1-1}}$; thus we may assume that this last congruence holds anyway.

For $m_1 \geqslant 3$ the binomial series for $(1 + 2^{m_1})^{\frac{1}{d}}$ converges in $\mathbb{Q}_2$ (recall that d is a prime) to an element denoted $\xi \in \mathbb{Q}_2$, and we have $\xi \equiv 1 \pmod{2^{m_1-2}}$. Since $\xi^d = 1 + 2^{m_1} \equiv y^d \pmod{2^{m_2}}$, we have, taking into account the previous congruence for y,

$$y \equiv \xi \pmod{2^{m_2-1}}. \tag{2.7}$$

(In fact, d-th roots of unity are pairwise incongruent modulo a 2-adic place if d is odd, and incongruent mod 4 if $d = 2$.)

We now choose the positive integers r, s as the largest integers such that $r < \frac{1}{2m_1}(m_2 - \frac{m_3}{d})$ [9] and $s < \frac{1}{2m_1}(m_2 + \frac{m_3}{d})$.

In view of Lemma 2.5 we may assume that either $G(-2^{m_1}) \neq yH(-2^{m_1})$ or $G^*(-2^{m_1}) \neq yH^*(-2^{m_1})$. Therefore, by replacing if necessary r, s resp. with $r + 1, s + 1$, we may directly assume that

$$G(-2^{m_1}) \neq yH(-2^{m_1}) \tag{2.8}$$

and that

$$\left| r - \frac{1}{2m_1}\Big(m_2 - \frac{m_3}{d}\Big) \right| \leqslant 1, \quad \left| s - \frac{1}{2m_1}\Big(m_2 + \frac{m_3}{d}\Big) \right| \leqslant 1. \tag{2.9}$$

Let now A be a positive integer as in Lemma 2.4 such that the polynomials $AG(z), AH(z)$ have integer coefficients bounded in absolute value by $B := (2d)^{4t}$. Since $(1 - 4z)^{\frac{1}{d}}$ has 2-adic integral coefficients, for all primes d, it follows from (2.6) that $4^{t+1}AE(4z)$ has 2-adic integer coefficients. Putting $z = -2^{m_1}$ in equation (2.6) and recalling our notation ξ for the 2-adic value of the binomial series for $(1+2^{m_1})^{\frac{1}{d}}$, we obtain (using $m_1 > 2$)

$$\big|AG(-2^{m_1}) - \xi AH(-2^{m_1})\big|_2 \leqslant 2^{-(m_1-2)(t+1)}.$$

where $|\cdot|_2$ denotes the standard 2-adic absolute value in $\mathbb{Q}_2$. Now, in view of (2.9), we have $t + 1 = r + s + 1 \geqslant \frac{m_2}{m_1} - 1$, so

$$\big|AG(-2^{m_1}) - \xi AH(-2^{m_1})\big|_2 \leqslant 2^{(m_1-m_2)\frac{(m_1-2)}{m_1}}.$$

Using also (2.7) to eliminate ξ (note that $\frac{(m_2-m_1)(m_1-2)}{m_1} \leqslant m_2 - 1$) and recalling (2.8) we have

$$0 < |AG(-2^{m_1}) - yAH(-2^{m_1})|_2 \leqslant 2^{(m_1-m_2)\frac{(m_1-2)}{m_1}}. \tag{2.10}$$

[9] Recall that $m_2 > 15m_3/16$ and that $m_1 < m_3/16$, so $(m_2 - (m_3/d))/2m_1 \geqslant 3$.

Now we estimate the ordinary absolute value. By the said bound on the coefficients of $AG(z), AH(z)$ we have

$$|AG(-2^{m_1})| \leqslant 2B2^{m_1 s},$$
$$|AH(-2^{m_1})| \leqslant 2B2^{m_1 r}.$$

Also, $|y| \leqslant 2^{\frac{m_3+1}{d}}$. Hence

$$|AG(-2^{m_1}) - yAH(-2^{m_1})| \leqslant 2B(2^{m_1 s} + 2^{m_1 r + \frac{m_3+1}{d}}). \tag{2.11}$$

On the other hand, inequalities (2.9) above yield

$$t \leqslant \frac{m_2}{m_1} + 2, \quad m_1 s \leqslant \frac{m_2}{2} + \frac{m_3}{2d} + m_1, \quad m_1 r + \frac{m_3}{d} \leqslant \frac{m_2}{2} + \frac{m_3}{2d} + m_1.$$

Inserting these bounds in (2.11) we obtain

$$\left|AG(-2^{m_1}) - yAH(-2^{m_1})\right| \leqslant 2(2d)^8 (2d)^{\frac{4m_2}{m_1}} 2^{\frac{m_2}{2} + \frac{m_3}{2d} + m_1 + 1}. \tag{2.12}$$

Finally, comparing with (2.10) we deduce

$$(2d)^8 (2d)^{\frac{4m_2}{m_1}} 2^{\frac{2m_2}{m_1}} 2^{-\frac{m_2}{2} + \frac{m_3}{2d} + 2m_1} \geqslant 1. \tag{2.13}$$

However, in view of the present assumptions we have

$$-\frac{m_2}{2} + \frac{m_3}{2d} + 2m_1 \leqslant -\frac{15m_3}{32} + \frac{m_3}{4} + \frac{m_3}{8} = -\frac{3m_3}{32} \tag{2.14}$$

Taking into account that d is fixed and that $m_1 \to \infty$ along our sequence, this last inequality shows that (2.13) is eventually inconsistent. This final contradiction proves Proposition 1.2.

3. Proof of Proposition 1.3

The arguments here are in part similar to the previous section, but rely mainly on lower bounds for linear forms in logarithms. Here we do not assume that d is a prime (otherwise we would have to take into account the previous proposition and we would lose effectivity).

In the sequel we then let d be an integer, tacitly assumed to be larger than some computable fixed number d_0, suitably large to justify the coming inequalities; however d_0 shall remain unspecified. Also, we let y, m_1, m_2, m_3 be an integer solution to (1.1); note that this entails that $m_3 \geqslant d \geqslant d_0$, so m_3 is "large" as well. Our aim shall be to obtain a contradiction.

We define the integer $a \geqslant 0$ as the exponent of the largest power of 2 dividing d. We start by noting that if d is odd we must have $y \equiv 1$

(mod 2^{m_1}), whereas if d is even we may choose the sign of y so that $y \equiv 1$ (mod 4), and then necessarily

$$m_1 \geqslant a+2, \quad y \equiv 1 \pmod{2^{m_1-a}}. \tag{3.1}$$

Hence we may assume that this last congruence holds, so $2^{d(m_1-a-1)} \leqslant |y|^d \leqslant 2^{m_3+1}$, and hence

$$m_1 \leqslant \frac{m_3+1}{d} + a + 1 \leqslant \frac{m_3+1}{d} + \frac{\log 2d}{\log 2} \leqslant \frac{m_3+1}{d} + \frac{\log 2m_3}{\log 2}. \tag{3.2}$$

Now, as in the First case of the previous section, we go ahead by proving that m_2 has to be "nearly" m_3; for instance we have the following

LEMMA 3.1. — *For large enough d_0, and for any solution of (1.1) with $d \geqslant d_0$, we have $m_2 \geqslant \frac{15}{16} m_3$.*

Proof. — Assume that $m_2 < \frac{15}{16} m_3$. Then, from $\left||y|^d 2^{-m_3} - 1\right| \leqslant 2^{m_2-m_3+1}$ it is readily seen that

$$|d \log |y| - m_3 \log 2| \leqslant 2 \cdot 2^{-\frac{m_3}{16}}. \tag{3.3}$$

We shall use a suitable version of Alan Baker's lower bounds for linear forms in logarithms. Specifically, since clearly $\log|y|, \log 2$ are linearly independent over $\mathbb{Q}$, we can apply Theorem 5.1, p. 317 of [8]. (10) We choose the following data to be inserted in that general statement:

$$n = 2, \quad \alpha_1 = 2, \ \alpha_2 = |y|, \quad b_1 = m_3, \ b_2 = d, \quad E^* = E = \exp(1),$$
$$D = 1, \quad V_1 = 3\log 2, \ V_2 = 3\log|y|, \quad W = \log(2d).$$

It is immediate to check that for large d_0 (recall $d \geqslant d_0$), the inequalities prescribed in that statement are indeed satisfied. (Especially, it is required that $V_j \geqslant \max(1, Eh(\alpha_j))$ and that $e^W \geqslant \frac{|b_1|}{V_2} + \frac{|b_2|}{V_1}$. For this, one has merely to take into account that $m_3 \log 2 < d \log|y| < (m_3+1)\log 2$.)

The conclusion of that theorem (applied with the present data) delivers a computable absolute constant $C > 0$ such that

$$|d \log |y| - m_3 \log 2| \geqslant \exp(-C \log(2d) \log|y|).$$

Taking into account that $\log|y| \leqslant 2m_3/d$ and comparing with (3.3) we obtain, after taking logarithms,

$$-2C \frac{\log(2d)}{d} m_3 \leqslant \log 2 - \frac{\log 2}{16} m_3.$$

Finally, using that $m_3 \geqslant d \geqslant d_0$, this is clearly untenable for large enough d_0, proving that the conclusion of the lemma indeed must then hold. □

(10) See [1] and the related references for refined results by Bugeaud and Laurent, also in the 2-adic case, which are fundamental for the explicit results obtained therein.

The next step is to apply Padé approximation, similarly to what we have done for Proposition 1.2. We know from (3.2) that m_1 has to be small compared to m_3 (recall also $m_3 \geqslant d \geqslant d_0$), and this is one of the needed pieces of information. However, since here d is varying we also need that it is not too large with respect to m_1; specifically, we need that $\log d$ is negligible with respect to m_1, for otherwise the analogue of (2.13) will not yield the required contradiction.

To achieve the sought comparison between d and m_1 we shall use 2-adic linear forms in logarithms, exploiting that $y^d \equiv \Delta \pmod{2^{m_2}}$, where $\Delta := 1 + 2^{m_1}$.

More precisely, we apply the "*consequence of Theorem 1*" of Kunrui Yu's paper [9], stated at l. -6 of p. 1 of [9] (where the relevant "Theorem 1" may be also found).

The presently chosen data are $p = 2$, $d = 1$, $n = 2$, $\alpha_1 = y$, $\alpha_2 = 1 + 2^{m_1}$, $b_1 = d$, $b_2 = 1$. Here we work over $\mathbb{Q}$ so the ramification index and residual degree appearing therein are trivial. Also, $\max(d, 3) = d$, $h_1 = \log|y|$, $h_2 = \log\Delta \leqslant 2m_1$. The cited conclusion delivers the bound

$$\operatorname{ord}_2(y^d - \Delta) < 19(20\sqrt{3})^6 \frac{2}{\log^2 2} \log(2e^5)(\log|y|)(\log\Delta)(\log d).$$

Since $d \log|y| \leqslant (m_3+1)\log 2$, the right side is $\leqslant C' \frac{m_3}{d} m_1 \log d$, for a suitable computable absolute constant $C' > 0$. In view of (1.1) and Lemma 3.1, the left side is $\geqslant m_2 \geqslant \frac{15 m_3}{16}$. Comparing the last two estimates we get, for a positive computable absolute constant $c > 0$,

$$m_1 \geqslant c \frac{d}{\log d}. \tag{3.4}$$

We can now readily conclude the proof. We use the method in the Fourth case of the previous section, retaining that notation. We briefly indicate the few small modifications needed in the present case, with respect to those arguments.

First, in view of (3.4), for large d_0 we have $m_1 \geqslant 2a + 4$ and then (3.1) leads to an analogue of (2.7) above,*i.e.* $y \equiv \xi \pmod{2^{m_2 - a}}$. Then, exactly the same arguments lead to (2.13), however replacing therein the exponent $\frac{2m_2}{m_1}$ with $\frac{2am_2}{m_1}$. Also, inequality (3.2) and Lemma 3.1 lead to (2.14). Combining this with the said analogue of (2.13) yields,

$$(2d)^8 (2d)^{\frac{4m_2}{m_1}} 2^{\frac{2am_2}{m_1}} 2^{-\frac{3}{32}m_3} \geqslant 1,$$

whose logarithm gives

$$\left(\frac{4m_2}{m_1} + 8\right) \log(2d) + \frac{2am_2}{m_1} \log 2 \geqslant \frac{3\log 2}{32} m_3.$$

However since $a \log 2 \leqslant \log d$, since $m_2 < m_3$, and since $m_3 \geqslant d \geqslant d_0$, this is inconsistent with (3.4) for large enough d_0, concluding the proof.

BIBLIOGRAPHY

[1] M. Bennett, Y. Bugeaud & M. Mignotte, "Perfect powers with few binary digits and related diophantine problems", *Annali Scuola Normale Sup. Pisa* **XII, 4** (2013), p. 14.

[2] E. Bombieri & W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, 2006.

[3] P. Corvaja & U. Zannier, "On the diophantine equation $f(a^m, y) = b^n$", *Acta Arith.* **94** (2000), no. 1, p. 25-40.

[4] ———, "S-unit points on analytic hypersurfaces", *Ann. Sci. École Norm. Sup. (4)* **38** (2005), no. 1, p. 76-92.

[5] A. Erdélyi, W. Magnus, F. Oberhettinger & F. Tricomi, *Higher transcendental functions*, vol. I, McGraw-Hill, 1953.

[6] M. Le, "A note on the diophantine equation $\frac{x^m-1}{x-1} = y^n$", *Acta Arith.* **44** (1993), no. 1, p. 19-28.

[7] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of mathematics and its applications, Cambridge University Press, 2000.

[8] M. Waldschmidt, "Linear Independence Measures for Logarithms of Algebraic Numbers", in *Diophantine approximation* (F. Amoroso & U. Zannier, eds.), Lecture Notes in Math., vol. 1819, Springer, 2003 (Cetraro, 2000), p. 249-344.

[9] K. Yu, "p-adic logarithmic forms and group varieties. II", *Acta Arith.* **89** (1999), no. 4, p. 337-378.

[10] U. Zannier, "Roth Theorem, Integral Points and certain ramified covers of $\mathbb{P}_1$", in *Analytic Number Theory - Essays in Honour of Klaus Roth*, Cambridge University Press, 2009, p. 471-491.

Manuscrit reçu le 7 juillet 2011,
accepté le 16 septembre 2011.

Pietro CORVAJA
Dipartimento di Matematica e Informatica
Via delle Scienze, 206
33100 Udine (Italy)
pietro.corvaja@uniud.it

Umberto ZANNIER
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56100 Pisa (Italy)
u.zannier@sns.it