On the Diophantine equation $(x^k-1)(y^k-1)=(z^k-1)$

Yann Bugeaud (Strasbourg)

À Rob Tijdeman, pour son soixantième anniversaire

Abstract. Let $k \geq 3$ be an integer. We study the possible existence of pairs of distinct positive integers (a,b) such that any of the three numbers $a+1$, $b+1$, and $ab+1$ is a k-th power. We further investigate several related questions.

1. Introduction

For any integer $n \geq 2$ we have

$$(n^2-1)\big((n+1)^2-1\big) = (n^2+n-1)^2-1,$$

which implies that the Diophantine equation $(x^2-1)(y^2-1)=(z^2-1)$ has infinitely many solutions. Equivalently, there are infinitely many pairs of integers (a,b) with $2 \leq a < b$ such that $a+1$, $b+1$, and $ab+1$ are perfect squares. This observation resembles the celebrated problem (dating back to Diophantus) on the existence of quadruples (a_1,a_2,a_3,a_4) of positive rational numbers such that a_ia_j+1 is a perfect square whenever $1 \leq i < j \leq 4$. The reader wishing more information on this question and on related problems is directed to the remarkable paper of Dujella [5] and to the references quoted therein.

Recently, Bugeaud & Dujella [3] proposed a generalization of the problem of Diophantus to higher powers $k \geq 3$. They investigated the possible existence of m-tuples $(a_1,\ldots,a_m)$ of positive integers such that any number a_ia_j+1, with $1 \leq i < j \leq m$, is a k-th power. They proved that m is at most equal to 3 if k is greater than 176. In the present note, we show among other results that if $(1,a,b)$ is such a triple (that is, if $a+1$, $b+1$, and $ab+1$ are k-th powers), then k cannot exceed 74. Furthermore, we study several variants of the Diophantine equation $(x^k-1)(y^k-1)=(z^k-1)$.

Our results are stated in Section 2 and proved in Section 4, with the help of auxiliary lemmas collected in Section 3. Section 5 is devoted to a brief discussion around some of our results.

2000 *Mathematics Subject Classification :* 11D61.

2. Statement of the results

We state our first result in terms of an exponential Diophantine equation.

Theorem 1. *The Diophantine equation* $(x^k-1)(y^k-1)=(z^k-1)$, *in positive integers* x,y,z,k *with* $z\geq 2$, *has no solution satisfying* $k\geq 75$. *Furthermore, there is an absolute, effectively computable constant* c_1 *such that it has no solution with* $k\geq 5$ *and* $\min\{x,y\}\geq c_1$.

Unfortunately, we are not able to drop the assumption $\min\{x,y\}$ large enough in Theorem 1. In case of Theorem 4 of [3], the situation is quite different, and there is no such restriction. Furthermore, we have no relevant results on the Diophantine equations $(x^3-1)(y^3-1)=(z^3-1)$ and $(x^4-1)(y^4-1)=(z^4-1)$. Notice that Kashihara [7] (see also Katayama & Kashihara [9]) described the set of all integer solutions to the equation $(x^2-1)(y^2-1)=(z^2-1)$.

Our second result deals with variants of the problem of Diophantus.

Theorem 2. *Let* $2\leq a<b$ *and* $k\geq 3$ *be integers such that* $a+1$ *and* $ab+1$ *are* k*-th powers. Then, if* $k\geq 150$, *none of the numbers* $b+1$, ab^2+1, *and* a^2b+1 *is a* k*-th power. Furthermore, if* $k\geq 8$ *and if* a *is sufficiently large, then none of the numbers* $b+1$, ab^2+1, *and* a^2b+1 *is a* k*-th power.*

The proofs of Theorems 1 and 2 follow an idea already used in [3]: thanks to a strong gap principle, we are able to use the full strength of the estimates of linear forms in two logarithms obtained via Schneider's method by Laurent, Mignotte & Nesterenko [10]. This yields a very sharp upper bound for k. The key point is that we deal with rational numbers very close to 1. This allows us furthermore to use strong results on irrationality measures of roots of rational numbers to treat the remaining values of k, up to the smallest ones. The reader is directed to Section 2 of [3] for more information and bibliographical references.

Actually, our method offers much flexibility and allows us to get similar results for families of related equations.

Theorem 3. *Let* α *be a positive real number. If the Diophantine equation* $(x^k-u)(y^k-v)=(z^k-w)$, *in positive integers* x,y,z,u,v,w,k, *has a solution with*

$$z\geq 2,\ \ k\geq 3,\ \ 1\leq u\leq x^{\alpha},\ \ 1\leq v\leq y^{\alpha},\ \ 1\leq w\leq z^{\alpha},$$

then k *is bounded from above by some effectively computable number depending only on* α.

It is worth to point out an immediate consequence of Theorem 3.

Corollary 1. *Let* n *be a non-negative integer. There exists an effectively computable constant* $c_2(n)$ *such that the Diophantine equation*

$$x^n(x^k-1)y^n(y^k-1)=z^n(z^k-1)$$

has no solution with $z\geq 2$ *and* $k\geq c_2(n)$.

The (infinite) set of solutions to the Diophantine equation $x(x-1)y(y-1)=z(z-1)$ has been described by Katayama [8] (see also Baragar [2] who showed that, up to a change of variables, this equation is a Markoff–type equation).

In Section 4, we do not give full proofs of Theorems 2 and 3, but we merely content ourselves to explain how the proof of Theorem 1 should be adapted to get Theorems 2 and 3.

3. Auxiliary lemmas

We begin by stating a strong gap principle, whose proof is close to that of the beginning of Theorem 1 of Gyarmati [6].

Lemma 1. *Let $k \geq 3$ be an integer. Let $2 \leq a \leq b$ be integers such that $a+1$, $b+1$ and $ab+1$ are k-th powers. Then we have $b \geq (k^k a^{k-1})/2$.*

Proof : Since $ab+1$ is strictly less than $(a+1)(b+1)$ and both are k-th powers, we get

$$\left((ab+1)^{1/k}+1\right)^k \leq (a+1)(b+1),$$

thus

$$k(ab+1)^{(k-1)/k} \leq a+b.$$

This implies that

$$k^k(ab)^{k-1} \leq k^k(ab+1)^{k-1} \leq (a+b)^k \leq b^k + 2^k ab^{k-1},$$

and the claimed result follows. □

We need the following refinement, due to Mignotte [11], of a theorem of Laurent, Mignotte & Nesterenko [10] on linear forms in two logarithms. For any non-zero algebraic number α, we denote by $\mathrm{h}(\alpha)$ its logarithmic absolute height. For instance, for any non-zero rational number p/q, written under its irreducible form, we have $\mathrm{h}(p/q) = \log \max\{|p|, |q|\}$.

Lemma 2. *Consider the linear form*

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

where b_1 and b_2 are positive integers. Suppose that α_1 and α_2 are multiplicatively independent. Put

$$D = [\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}] \,/\, [\mathbf{R}(\alpha_1, \alpha_2) : \mathbf{R}].$$

Let a_1, a_2, h be real positive numbers, and ρ a real number > 1. Put $\lambda = \log \rho$ and $\chi = h/\lambda$. Suppose that there exists a number $\chi_0 \geq 0$ such that $\chi \geq \chi_0$ and

$$\begin{aligned} h &\geq D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\lambda + f(\lceil K_0 \rceil)\right) + 0.023, \\ a_i &\geq \max\left\{1, \rho\,|\log \alpha_i| - \log|\alpha_i| + 2D\mathrm{h}(\alpha_i)\right\}, \quad (i = 1, 2), \\ a_1 a_2 &\geq \lambda^2 \end{aligned}$$

where

$$f(x) = \log \frac{\left(1+\sqrt{x-1}\right)\sqrt{x}}{x-1} + \frac{\log x}{6x(x-1)} + \frac{3}{2} + \log\frac{3}{4} + \frac{\log \frac{x}{x-1}}{x-1},$$

and

$$K_0 = \frac{1}{\lambda}\left(\frac{\sqrt{2+2\chi_0}}{3} + \sqrt{\frac{2(1+\chi_0)}{9} + \frac{2\lambda}{3}\left(\frac{1}{a_1}+\frac{1}{a_2}\right) + \frac{4\lambda\sqrt{2+\chi_0}}{3\sqrt{a_1a_2}}}\right)^2 a_1a_2.$$

Put

$$v = 4\chi + 4 + 1/\chi \quad \text{and} \quad m = \max\left\{2^{5/2}(1+\chi)^{3/2}, (1+2\chi)^{5/2}/\chi\right\}.$$

Then we have the lower bound

$$\log|\Lambda| \geq -\frac{1}{\lambda}\left(\frac{v}{6} + \frac{1}{2}\sqrt{\frac{v^2}{9} + \frac{4\lambda v}{3}\left(\frac{1}{a_1}+\frac{1}{a_2}\right) + \frac{8\lambda m}{3\sqrt{a_1a_2}}}\right)^2 a_1a_2$$
$$- \max\left\{\lambda(1.5+2\chi) + \log\left(\left((2+2\chi)^{3/2} + (2+2\chi)^2\sqrt{k^*}\right)A + (2+2\chi)\right), D\log 2\right\}$$

where

$$A = \max\{a_1, a_2\} \quad \text{and} \quad k^* = \frac{1}{\lambda^2}\left(\frac{1+2\chi}{3\chi}\right)^2 + \frac{1}{\lambda}\left(\frac{2}{3\chi} + \frac{2}{3}\frac{(1+2\chi)^{1/2}}{\chi}\right).$$

Proof : This is Theorem 2 of [11]. □

Finally, we need a result proved by means of the hypergeometric method first developed by Thue and Siegel.

Lemma 3. *Let $k \geq 3$ be an integer and $\varepsilon > 0$ be a real number. There exist effectively computable positive constants c_3 and c_4 depending only on k and on ε such that*

$$\left|\left(1+\frac{1}{a}\right)^{1/k} - \frac{p}{q}\right| > \frac{c_3}{a\,q^{2+\varepsilon}}$$

holds for any $a > c_4$ and any rational number p/q.

Proof : This is a straightforward corollary of a theorem of Baker [1]. □

4. Proofs

Proof of Theorem 1 :

Let x, y, z, k be positive integers with $k \geq 3$, $z \geq 2$, and

$$(x^k - 1)(y^k - 1) = (z^k - 1).$$

Clearly, there exist integers a and b with $2 \leq a \leq b$ and

$$a+1 = x^k, \quad b+1 = y^k, \quad \text{and} \quad ab+1 = z^k.$$

We assume that $k \geq 75$ and we aim to get a contradiction. Since $a+1 \geq 2^k$, we have

$$b \geq a > 2^{74}. \tag{1}$$

Furthermore, it follows from Lemma 1 that

$$\log b \geq (k-1)\log a + k \log k - \log 2 \tag{2}$$

holds. We set

$$\alpha_1 = \frac{xy}{z}, \quad \alpha_2 = \frac{a+1}{a},$$

and we consider the linear form in logarithms

$$\Lambda = |\log \alpha_2 - k \log \alpha_1| = \left| \log\left(\frac{a+1}{a}\right) - k \log\left(\frac{xy}{z}\right) \right|.$$

Before applying Lemma 2 with $b_2 = 1$ and $b_1 = k$ in order to bound Λ, we need some estimates.

Firstly, we have

$$|\alpha_2 - 1| = \alpha_2 - 1 = 1/a. \tag{3}$$

Secondly, from (1) and the estimation

$$\left| \frac{a+1}{a} - \left(\frac{xy}{z}\right)^k \right| = \frac{a^2-1}{a(ab+1)} \leq \frac{1}{b}, \tag{4}$$

we deduce that

$$\Lambda \leq \frac{2}{b}. \tag{5}$$

Let us now define the quantities a_1, a_2, h, ρ appearing in Lemma 2. We set

$$\rho = a \quad (\text{thus} \quad \lambda = \log a),$$

and, by (1) and (3), we may take

$$a_1 = 1 + \frac{2}{k}\log\big((a+1)(b+1)\big) \quad \text{and} \quad a_2 = 1 + 2\log(a+1).$$

Indeed, we easily see that $k\mathrm{h}(\alpha_1) = \mathrm{h}((a+1)(b+1))$, and $a_1 a_2 \geq 4(\log a)^2$ holds, by (2). Furthermore, since $a \geq 2^{k-1}$, we may take $h = \lambda/2$ and $\chi = \chi_0 = 1/2$.

We should also check that α_1 and α_2 are multiplicatively independent. However, a look at the proof of Theorem 1.5 of [11] shows that this is not needed. Indeed, we apply

it with the choice $L = 3$, hence it is sufficient to check that the three numbers 1, α_1 and α_2 are distinct, which is clearly the case.

Since $\chi = 1/2$, we have $v = 8$ and $m = 8\sqrt{2}$. Using (1) and (2), we get the lower bound

$$\log \Lambda \geq -\frac{1}{\log a}\left(\frac{4}{3} + \frac{1}{2}\sqrt{\frac{64}{9} + \frac{32}{3} + \frac{32\sqrt{2}}{3}}\right)^2 a_1 a_2 - 2.5 \log a - \log(7.5 a_1),$$

hence

$$\log \Lambda \geq -\frac{17.64}{\log a}\, a_1 a_2 - 2.5 \log a - \log(7.5 a_1).$$

By (5) and after some rearrangement, we get

$$\frac{72}{k} \log a + 2.5 \log a + \log(15 a_1) \geq \log b - \frac{71.3}{k} \log b$$

and, using (2), we obtain

$$1 - \frac{71.3}{k} \leq \frac{72}{k(k-1)} + \frac{2.5}{k-1} + 0.003,$$

which contradicts our assumption $k \geq 75$. This proves the first statement of the theorem.

Assume now that k is fixed with $3 \leq k \leq 74$. The constants c_5 to c_8 occurring below are effectively computable and depend only on k. It follows from (4) and Lemma 3 that we have

$$b \leq c_5\, a (ab)^{5/(2k)}$$

if $a > c_6$. Combined with Lemma 1, this gives

$$b^{2k(k-1)} \leq c_7\, b^{2k+5+5k-5}$$

hence a contradiction for $b > c_8$ as soon as $2k(k-1) > 7k$, that is, for $k \geq 5$. Consequently, there exist an absolute, effectively computable, constant c_9 such that there is no pair of integers (a, b) with $\min\{a, b\} \geq c_9$ and such that $a+1$, $b+1$, $ab+1$ are perfect k-th powers for some integer $k \geq 5$. This gives the second assertion of Theorem 1. □

Proofs of Theorems 2 and 3 :

Theorem 1 covers the case where $a+1$, $b+1$ and $ab+1$ are assumed to be k-th powers.

To get a gap principle when $a+1$, $ab+1$ and ab^2+1 are assumed to be k-th powers, we simply observe that $(ab+1)^2$ and $(a+1)(ab^2+1)$ are both k-th powers and satisfy $(a+1)(ab^2+1) > (ab+1)^2$. We obtain however a slightly weaker result than in Lemma 1, namely the lower bound $b \geq (k^k a^{k-2})^{1/2}/2$. This affects both bounds for k: the application of Lemma 2 yields that $k \leq 149$ and we can apply Lemma 3 only if $k \geq 8$.

To get a gap principle when $a+1$, $ab+1$ and a^2b+1 are assumed to be k-th powers, we simply observe that (a^2b+1) and $(a+1)(ab+1)$ are both k-th powers and satisfy

$(a+1)(ab+1) > (a^2b+1)$. We obtain a result comparable to that stated in Lemma 1, namely the lower bound $b \geq k^k a^{k-2}/2$. This affects solely one bound for k: the application of Lemma 2 yields that $k \leq 74$ and we can apply Lemma 3 only if $k \geq 6$.

As for Theorem 3, setting $a = x^k - u$ and $b = y^k - v$, we observe that $(a+u)(b+v) > (ab+w)$ if x, y, z, u, v, w, k satisfy the assumption of the theorem and if k is sufficiently large compared to α. Indeed, we cannot have $xy = z$ in that case. Hence, we get a gap principle, which, although not as strong as Lemma 1, is powerful enough to enable us to apply Lemma 2. □

5. Some observations

Results of Theorem 2 can be viewed as a multiplicative analogue of a deep theorem of Darmon & Merel [4], who proved that, for $k \geq 3$, there are no three terms arithmetic progressions composed of k-th powers, that is, that the numbers a, $a+b$, and $a+2b$ cannot be all k-th powers. Commonly, the triple $(a+1, ab+1, ab^2+1)$ is viewed as the 'multiplicative analogue' of the triple $(a, a+b, a+2b)$.

The result of Darmon & Merel is proved thanks to tools developed for the resolution of the Fermat equation (actually, they solved the Diophantine equation $x^k + y^k = 2z^k$), and it may seem very surprising that results from the transcendental number theory yield results as sharp as Theorem 2. As an explanation, we emphasize that the conditions of application of Lemma 2 in the question considered here are such that even if we would have used the most optimistic conjectural estimates for lower bounds of linear forms in logarithms, we would not have been able to improve Theorem 2 significantly.

References

[1] A. Baker, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, Quart. J. Math. Oxford (2) 15 (1964), 375–383.

[2] A. Baragar, *Products of consecutive integers and the Markoff equation*, Aequationes Math. 51 (1996), 129–136.

[3] Y. Bugeaud and A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. 135 (2003), 1–10.

[4] H. Darmon and L. Mérel, *Winding quotients and some variants of Fermat's last theorem*, J. reine angew. Math. 490 (1997), 81–100.

[5] A. Dujella, *There are only finitely many Diophantine quintuples*, J. reine angew. Math. To appear.

[6] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (2001), 53–65.

[7] K. Kashihara, *The Diophantine equation $(x^2-1)(y^2-1) = (z^2-1)$*, Res. Rep. Anan College Tech. 26 (1990), 119–130.

[8] S. Katayama, *On products of consecutive integers*, Proc. Japan Acad. Ser. A Math. Sci. 66 (1990), 305–306.

[9] S. Katayama and K. Kashihara, *On the structure on the integer solutions of* $z^2 = (x^2-1)(y^2-1)+a$, J. Math. Tokushima Univ. 24 (1990), 1–11.

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

[11] M. Mignotte, *A corollary to a theorem of Laurent–Mignotte–Nesterenko*, Acta Arith. 86 (1998), 215–225.

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

e-mail : `bugeaud@math.u-strasbg.fr`