On the Diophantine equation $a\frac{x^n-1}{x-1} = y^q$

*Yann Bugeaud**

Abstract. We extend earlier work of Inkeri and solve completely the Diophantine equation $a\,\frac{x^n-1}{x-1} = y^q$ for $1 \le a < x \le 100$.

1991 Mathematics Subject Classification: 11D61.

Dedicated to Kustaa Inkeri

1. Introduction

Obláth [6] proved that 4, 8 and 9 are the only numbers which are perfect powers and whose digits $a \neq 1$ in base ten are identical. This exactly means that the Diophantine equation

$$a\,\frac{x^n-1}{x-1} = y^q, \quad \text{in integers} \quad n \ge 3,\ x \ge 2,\ 1 \le a < x,\ y \ge 2,\ q \ge 2 \qquad (1)$$

has no solution when $x = 10$ and $a \neq 1$. Later, Obláth's result was extended by Inkeri [5] to arbitrary $x \in \{3, \ldots, 10\}$ and $a \neq 1$, in which case the only solution is given by $4\,\frac{7^4-1}{7-1} = 40^2$. The methods employed in [5] and [6] are based mainly on ingenious use of classical techniques in the study of Diophantine equations.

The case $a = 1$ remained open until last year, when Bugeaud & Mignotte solved it for $2 \le x \le 10$ [2], and then, jointly with Roy, for $x = z^t$ with $t \ge 1$ and $11 \le z \le 10^4$ [3, 4] : the only three solutions are given by

$$\frac{3^5-1}{3-1} = 11^2, \quad \frac{7^4-1}{7-1} = 20^2 \quad \text{and} \quad \frac{18^3-1}{18-1} = 7^3.$$

Their method rests on various more or less classical techniques in Diophantine approximation, including linear forms in p–adic logarithms [1], together with some heavy computations.

The aim of the present note is to explain how Inkeri's result can be extended to other values of the basis x, and to solve (1) completely for $x \le 100$ and $x = 1000$.

* The author would like to thank the CCCI for providing him a financial support to attend the Conference in Turku.

2. Statement of the results

We obtain the following extension of Theorem 7 of Inkeri [5].

Theorem. *The only solutions of equation (1) with $x \leq 100$ or $x = 1000$ are given by*

$$\begin{aligned}(a, x, y, n, q) \in \{&(1,3,11,5,2),(1,7,20,4,2),(4,7,40,4,2),\\ &(1,18,7,3,3),(7,18,49,3,2),(7,18,7,3,4),\\ &(8,18,14,3,3),(3,22,39,3,2),(12,22,78,3,2),\\ &(19,30,133,3,2),(21,41,1218,4,2),(13,68,247,3,2),\\ &(52,68,494,3,2),(58,99,7540,4,2)\}.\end{aligned}$$

Remarks. All these solutions have been already found by Inkeri, but he did not show that these are the only ones. Our proof depends considerably on the case $a = 1$, when (1) is already solved. As pointed out by Inkeri [5], "this reveals the decisive importance of the case $a = 1$ in the study of the Diophantine equation (1)".

From the results of [4], [3] and of the present note, it turns out that we have at our disposal an algorithm which enables one to solve (1) for any fixed given value of x ... provided, of course, that x is not too large, otherwise the computation would take too much time.

Our Theorem includes the fact that, if a, b and c denote any digits $0, \ldots, 9$, then none of the non-zero numbers

$$aa\ldots aa, \quad abab\ldots abab \text{ and } abcabc\ldots abcabc$$

written in basis ten is a perfect power, except, of course, the numbers a, ab and abc when these are perfect powers.

3. Auxiliary results

In the sequel of this note, we use the following notation. For a prime number p and an integer ℓ non divisible by p, we denote by $\mathrm{ord}_p(\ell)$ the least positive integer m such that $\ell^m \equiv 1 \pmod p$.

The proof of our theorem rests on two elementary lemmas, but, before stating them, we recall a crucial result concerning equation (1) in the most difficult case $a = 1$.

Proposition 1. *Equation (1) has no solution with $a = 1$ and $x = z^t$, for $2 \leq z \leq 10^4$ and $t \geq 1$.*

Proof : This is the main result of [3]. □

Lemma 1. *Let $p_1,\dots,p_\ell$ be prime numbers and assume that there are positive integers $u_1,\dots,u_\ell$, $n\ge 3$, $x\ge 2$, $y\ge 2$, $q\ge 2$ with q prime, $\gcd(q,u_1\dots u_\ell)=1$ and*

$$p_1^{u_1}\dots p_\ell^{u_\ell}\,\frac{x^n-1}{x-1}=y^q. \tag{2}$$

Then there exist a subset $S\subset\{1,\dots,\ell\}$, integers $v\ge 1$ and $y_1\ge 2$ and a prime P such that

$$\prod_{i\in S} p_i^{u_i}\,\frac{x^{P^v}-1}{x-1}=y_1^q. \tag{3}$$

Further, if S is non–empty, then we have, for $i\in S$, that either $\mathrm{ord}_{p_i}(x)$ is a power of P, or $p_i=P$ and $x\equiv 1 \pmod P$.

Proof : Denote by P the greatest prime factor of n, and write $n=P^vm$, with $\gcd(m,P)=1$. Let w be a prime dividing $\frac{x^{P^v}-1}{x-1}$. Then we get $x^{P^v}\equiv 1 \pmod w$ and $\frac{x^n-1}{x^{P^v}-1}\equiv m \pmod w$. If w also divides $\frac{x^n-1}{x^{P^v}-1}$, then w is a prime factor of m, hence is less than m. Thus, we infer from $x^{P^v}\equiv 1 \pmod w$ that $x\equiv 1 \pmod w$ and, since w divides $1+x+\dots+x^{P^v-1}$, we get $P^v\equiv 0 \pmod w$, a contradiction. We have proved that $\frac{x^n-1}{x^{P^v}-1}$ and $\frac{x^{P^v}-1}{x-1}$ are coprime integers. Hence, (3) follows from (2). We then deduce from (3) that for all $i\in S$, we have $x^{P^v}\equiv 1 \pmod{p_i}$, and the proof of the lemma is complete. □

Lemma 2. *Let p be a prime number and let $v\ge 2$ be an integer. Then we have*

$$\gcd\left(\frac{x^{p^v}-1}{x^{p^{v-1}}-1},\frac{x^p-1}{x-1}\right)=p \text{ or } 1,$$

according as $x\equiv 1 \pmod p$ or not.

Proof : This lemma belongs to the folklore, but we prefer recalling its proof. Let q be a prime number dividing $\frac{x^p-1}{x-1}$. We have $x^p\equiv 1 \pmod q$ and $1+x^{p^{v-1}}+x^{2p^{v-1}}+\dots+x^{(p-1)p^{v-1}}\equiv p \pmod q$, thus $\gcd\bigl(\frac{x^{p^v}-1}{x^{p^{v-1}}-1},\frac{x^p-1}{x-1}\bigr)=1$ if $q\ne p$. Further, we observe that $\frac{x^p-1}{x-1}\equiv p \pmod{p^2}$, and the proof is complete. □

4. Proof

We shall explain our method by treating exhaustively (1) with $x=100$ and $2\le a\le 99$. Thus, we consider the equation

$$a\,\frac{100^n-1}{100-1}=y^q, \tag{4}$$

in the integers $2 \leq a \leq 99$, $n \geq 3$, $y \geq 2$ and $q \geq 2$, with q prime. Further, there is no restriction in assuming that a is q-th power free, and we easily see that a is odd and not divisible by 5, otherwise (4) cannot be satisfied.

The general strategy of our proof consists in finding a prime number Q which divides $a(100^n - 1)/(100 - 1)$ and such that Q^2 does not, hence (4) cannot be satisfied.

Suppose first that $a \in \{2, \dots, 99\}$ is prime and apply Lemma 1 to (4). In view of Proposition 1, the equation

$$\frac{100^n - 1}{100 - 1} = y^q$$

has no solution (y, n, q) with $n \geq 2$ and $q \geq 2$. Thus, we deduce that the set S occurring in the statement of Lemma 1 is equal to $\{a\}$ and we infer that, if (a, y, n, q) satisfies (4), then n is a power of a prime and $\mathrm{ord}_a(100)$ is equal to 1 or to a power of a prime. Hence, only the following 15 values of a remain possible :

a	3	7	11	13	17	19	23	37	41	47	53	59	73	79	83
$\mathrm{ord}_a(100)$	1	3	1	3	8	9	11	3	5	23	13	29	4	13	41

If $\mathrm{ord}_a(100) = 1$, then n has to be a power of a, since otherwise a divides y^q and a^2 does not. For the other values of a, we observe that n must be a power of the prime divisor V of $\mathrm{ord}_a(100)$ and we proceed as follows, setting $V = a$ if $\mathrm{ord}_a(100) = 1$. First, if $V = 2$, we observe that

$$101 \| \frac{100^2 - 1}{100 - 1}$$

and

$$101 \nmid \frac{100^{2^v} - 1}{100^2 - 1}, \quad v \geq 2,$$

by Lemma 2. Thus (4) cannot be satisfied. For the remaining cases, we check that $100^V - 1$ has a prime divisor Q with $Q \notin \{3, 11, a, V\}$ and such that Q^2 does not divide $100^V - 1$. Hence, by Lemma 2, Q divides $a\,(100^n - 1)/(100 - 1)$ and Q^2 does not : equation (4) cannot be satisfied. The following values of Q are suitable.

a	3	7	11	13	19	23	37	41	47	53	59	79	83
Q	7	13	23	7	7	4093	7	271	139	79	3191	53	1231

By exactly the same argument, we deduce that a cannot be a power of a prime. If now a is composed by two distinct primes p_1 and p_2, we argue again as above, however, we have to assume that $Q \notin \{3, 11, p_1, p_2, V\}$. We easily check that this can be done : it suffices to choose $Q = 37$ if $p_1 = 7$ and $p_2 = 13$.

For $x = 1000$, we proceed exactly as above, and we check that for a few number of primes a we have that $\mathrm{ord}_a(1000)$ is prime or is a power of a prime. For example, $\mathrm{ord}_a(1000)$ is a power of 2 only for

$$a \in \{7, 11, 13, 17, 73, 97, 101, 137, 193, 257, 353, 449, 641, 769\}.$$

To conclude, we check that the prime 9901 exactly divides $1000^4 - 1$.

However, a computational problem occurs when

$$a \in S = \{173, 277, 283, 359, 439, 479, 643, 853\},$$

in which case we, respectively, have $\mathrm{ord}_a(1000) = 43, 23, 47, 179, 73, 239, 107, 71$. Using PARI, we see that in each of these cases $a \| 1000^{\mathrm{ord}_a(1000)} - 1$, but, since the latter number is far too large, we are unable to find another prime factor of $(1000^{\mathrm{ord}_a(1000)} - 1)/(1000 - 1)$. We deduce from (1) that we necessarily have $q = 2$. To exclude this possibility, it suffices, by Lemma 2, to check that neither $a \times (1000^{\mathrm{ord}_a(1000)} - 1)/(1000 - 1)$ nor $a \times \mathrm{ord}_a(1000) \times (1000^{\mathrm{ord}_a(1000)} - 1)/(1000 - 1)$ is a square. This verification takes only a few seconds, and we are done. We observe that the same problem occurs for several values of x less than 100, and we solve it as explained above, considering $a \times (x^{\mathrm{ord}_a(x)} - 1)/(x - 1)$ and $a \times \mathrm{ord}_a(x) \times (x^{\mathrm{ord}_a(x)} - 1)/(x - 1)$. However, when $\mathrm{ord}_a(x) = 1$ and when we are unable to find a suitable prime factor of $x^{\mathrm{ord}_a(x)} - 1$, we have to check that neither $(x^{\mathrm{ord}_a(x)} - 1)/(x - 1)$ nor $a \times (x^{\mathrm{ord}_a(x)} - 1)/(x - 1)$ is a square. □

Acknowledgement. The author would like to thank the referee for his careful reading of the text and his numerous remarks.

References

[1] Bugeaud, Y., Linear forms in p-adic logarithms and the Diophantine equation $(x^n - 1)/(x - 1) = y^q$. Math. Proc. Cambridge Philos. Soc. To appear.

[2] Bugeaud, Y., Mignotte, M., On integers with identical digits. Mathematika. To appear.

[3] Bugeaud, Y., Mignotte, M., Sur l'équation diophantienne $(x^n - 1)/(x - 1) = y^q$, *II*. C. R. Acad. Sci. Paris Sér. I 328 (1999), 741–744.

[4] Bugeaud, Y., Mignotte, M., Roy, Y., On the diophantine equation $(x^n - 1)/(x - 1) = y^q$. Pacific J. Math. To appear.

[5] Inkeri, K., On the Diophantine equation $a(x^n - 1)/(x - 1) = y^m$. Acta Arith. 21 (1972), 299–311.

[6] Oblàth, R., Une propriété des puissances parfaites. Mathesis 65 (1956), 356–364.