An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$.

Y. Bugeaud P. Corvaja U. Zannier

It is a known amusing elementary problem to prove that, *if $a^n - 1$ divides $b^n - 1$ for every large positive integer n, then b is a power of a.* (Here a, b are integers greater than 1.)

This is a particular case of the so-called *Hadamard Quotient* theorem, concerning arbitrary recurrent sequences in place of $\{a^n - 1\}$ and $\{b^n - 1\}$ (see [vdP1]). The general case was proved by A.J. van der Poorten [vdP2] by quite ingenuous arguments of p-adic nature and rather complicated auxiliary constructions. Nevertheless, the simple case under consideration (as well as the cases where the recurrences admit a *dominant root*), is capable of an elementary solution, obtained after expansion of the fraction $(b^n - 1)/(a^n - 1)$ by geometric series. Still another solution may be obtained using ideas from Algebraic Number Theory (e.g., if b is not of the form $a^j c^2$, we may find primes p such that $1 = \left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right)$ and then it suffices to take $n = (p-1)/2$ to obtain a contradiction).

Anyway, none of these arguments leads to the stronger assertion which results by assuming only that $a^n - 1$ divides $b^n - 1$ just for an infinite set of integers n.

Such a theorem was achieved in [CZ, Thm. 1], actually in greater generality, by using deep tools from Diophantine Approximation.

These assertions may be considered as "exponential function" analogues of the well-known fact that if infinitely many values $f(n)$ divide $g(n)$, for polynomials f, g, then g/f is a polynomial.

It is the object of the present note to remark that the same techniques enable one to obtain a more explicit result, bounding the cancellation in the fraction $(b^n - 1)/(a^n - 1)$, which is represented by the G.C.D. of $a^n - 1$ and $b^n - 1$. In fact, we shall prove the following

Theorem. *Let a, b be multiplicatively independent integers ≥ 2, and let $\epsilon > 0$. Then, provided n is sufficiently large, we have*

$$\text{G.C.D.}(a^n - 1, b^n - 1) < \exp(\epsilon n).$$

The proof will proceed by producing the lower bound $a^{(1-\epsilon)n}$ for the denominator of $(b^n - 1)/(a^n - 1)$, which is equivalent to the theorem.

Remarks. (1) As an immediate corollary, one obtains that $\text{G.C.D.}(a^n - 1, b^n - 1) \ll a^{\frac{n}{2}}$ for large n, provided b is not a power of a. In fact, if a and b are multiplicative independent, then the theorem gives a sharper bound; otherwise one can write $a = c^r, b = c^s$ for an integer $c \geq 2$ and relatively prime integers r, s, where $r \geq 2$ if b is not a power of a. In this case write $a^n - 1 = (c^n - 1)(c^{(r-1)n} + \ldots + c^n + 1)$, $b^n - 1 = (c^n - 1)(c^{(s-1)n} + \ldots + c^n + 1)$. The G.C.D. of the second factors can be bounded by a constant independent of n since the polynomials $\frac{X^r - 1}{X - 1}$ and $\frac{X^s - 1}{X - 1}$ are relatively prime. Therefore $\text{G.C.D.}(a^n - 1, b^n - 1) \ll c^n - 1$, and the claim follows since $r \geq 2$. The number $1/2$ in the exponent is best-possible, in view of the examples $a = c^2$, $b = c^s$, for odd s.

(2) As to lower bounds, by taking $n = p - 1$, where p is a prime congruent to 1 modulo several $\ell - 1$, for ℓ a prime, we see that our G.C.D. is not $O(n)$. (By quantifying this argument, one actually finds that the G.C.D. is not even $O(n^c)$, no matter c, provided standard conjectures on prime numbers are true.)

(3) It seems to us that hardly one can obtain nontrivial estimates of the form $\text{G.C.D.}(a^n - 1, b^n - 1) < a^{\delta n}$ with $\delta < 1$ (valid for all large integers), by purely arithmetical methods.

(4) As in [CZ], we may work with more general power sums a_n, b_n, in place of $a^n - 1, b^n - 1$, provided a_n admits a *dominant root*. The conclusion will be that, unless a_n divides b_n in the ring of power sums, for large n we have $\text{G.C.D.}(a_n, b_n) < |a_n|^c$, for a $c < 1$ (depending on the data). Also, one can obtain the same estimate of the Theorem for $\text{G.C.D.}(a^n - l, b_n)$, by imposing certain natural necessary conditions on the data a, l, b_n.

(5) Due to the ineffectivity of the auxiliary results from Diophantine Approximation needed in the proof below, our method does not allow to compute an integer $n_0 = n_0(a, b, \epsilon)$ such that our inequality holds for $n > n_0$.

Proof of Theorem. We write, for a positive integer j,

$$z_j(n) = \frac{b^{jn} - 1}{a^n - 1} = \frac{c_{j,n}}{d_n},$$

where $c_{j,n}, d_n$ are positive integers. Since $b^n - 1$ divides $b^{jn} - 1$ for all positive integers j, n, we may choose d_n to be the denominator of $z_1(n)$.

We now assume that $\epsilon > 0$ is given and that $d_n \le a^{(1-\epsilon)n}$ for all n in an infinite set $\mathcal{N}$ of natural numbers. We shall eventually derive a contradiction which, as we have observed, will prove the theorem.

Fix an integer $h > 0$ and observe the approximation

$$\frac{1}{a^n - 1} = \frac{1}{a^n(1 - a^{-n})} = \frac{1}{a^n}\sum_{r=0}^{\infty}\frac{1}{a^{rn}} = \sum_{r=1}^{h}\frac{1}{a^{rn}} + O(a^{-(h+1)n}).$$

For a given positive integer j we thus obtain, on multiplying by $b^{jn} - 1$,

$$\left| z_j(n) - \sum_{s=1}^{h}\frac{1}{a^{sn}} + \sum_{r=1}^{h}(\frac{b^j}{a^r})^n \right| = O(b^{jn}a^{-(h+1)n}). \qquad (1)$$

As in [CZ], we shall apply the Schmidt Subspace Theorem, viewing the left side of (1) as a "small" linear form in the variables $z_j(n)$, b^{jn}/a^{rn}, $1/a^{sn}$. We shall consider several such linear forms, corresponding to various values of j.

In detail, we shall apply the following particular case of the Subspace Theorem, which we recall as a lemma. (For a proof see [S1,2].)

Lemma. *Let S be a finite set of absolute values of $\mathbf{Q}$, including ∞ (normalized so that $|p|_p = p^{-1}$) and let $N \in \mathbf{N}$. For $v \in S$, let $L_{1,v}, \ldots, L_{N,v}$ be linearly independent linear forms in N variables, with rational coefficients, and let $\delta > 0$. Then the solutions $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbf{Z}^N$ to the inequality*

$$\prod_{v \in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x})|_v < (\max|x_i|)^{-\delta}$$

are contained in finitely many proper subspaces of $\mathbf{Q}^N$.

Let us fix a second integer $k > 0$, which will represent the number of small linear forms arising from (1).

We shall apply the lemma with the following data: first, we let S consist of ∞ and the prime divisors of ab. Second, we put $N = hk + h + k$. For convenience we shall denote vectors in $\mathbf{Z}^N$ by writing

$$\mathbf{x} = (x_1, \ldots, x_N) = (z_1, \ldots, z_k, y_{01}, \ldots, y_{0h}, \ldots, y_{k1}, \ldots, y_{kh}).$$

In this notation, we choose linear forms with rational coefficients as follows. For $i = 1, \ldots, k$, we put

$$L_{i,\infty}(\mathbf{x}) = z_i + y_{01} + \ldots + y_{0h} - y_{i1} - \ldots - y_{ih},$$

while, for $(i, v) \notin \{(1, \infty), \ldots, (k, \infty)\}$ we put

$$L_{i,v}(\mathbf{x}) = x_i.$$

Observe that for each $v \in S$, the linear forms $L_{1,v}, \ldots, L_{n,v}$ are indeed linearly independent.

For a given integer $n \in \mathcal{N}$, we also set

$$\mathbf{x} = d_n a^{hn}\left(z_1(n), \ldots, z_k(n), a^{-n}, \ldots, a^{-hn}, (ba^{-1})^n, \ldots, (ba^{-h})^n, \ldots, (b^k a^{-1})^n, \ldots, (b^k a^{-h})^n\right).$$

Note that $\mathbf{x} \in \mathbf{Z}^N$. In order to apply the lemma, we shall estimate the double product $\prod_{v \in S}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x})|_v$.

We observe at once that for $i > k$ we have $\prod_{v \in S} |L_{i,v}(\mathbf{x})|_v \le d_n$: in fact, for each $i > k$, we have that $L_{i,v}(\mathbf{x})$ equals the coordinate x_i, which is of the form $d_n w_i$, where w_i is an S-unit (actually a product of powers of a and b). The assertion thus follows from the product formula $\prod_{v \in S} |w_i|_v = 1$ and from $\prod_{v \in S} |d_n|_v \le |d_n|_\infty = d_n$.

Therefore we find that

$$\prod_{v \in S} \prod_{i=1}^{N} |L_{i,v}(\mathbf{x})|_v \le d_n^{N-k} \prod_{v \in S} \prod_{i=1}^{k} |L_{i,v}(\mathbf{x})|_v = d_n^{N-k} \left(\prod_{i=1}^{k} |L_{i,\infty}(\mathbf{x})| \right) \prod_{p|ab} \prod_{i=1}^{k} |x_i|_p. \tag{2}$$

Further, for $i \le k$ we have $x_i = d_n a^{hn} z_i(n) = c_{i,n} a^{hn}$, whence $\prod_{p|ab} |x_i|_p \le a^{-hn}$. Also, in view of (1), we have, again for $i \le k$, $|L_{i,\infty}(\mathbf{x})| = O(d_n b^{in} a^{-n})$. Plugging these estimates into (2), we finally obtain

$$\prod_{v \in S} \prod_{i=1}^{N} |L_{i,v}(\mathbf{x})|_v = O(d_n^{N-k} a^{-hkn} d_n^k b^{k^2 n} a^{-kn}) = O(d_n^N b^{k^2 n} a^{-hkn}). \tag{3}$$

Recall that we are assuming $n \in \mathcal{N}$, i.e. $d_n \le a^{(1-\epsilon)n}$. Hence equation (3) gives, after a few calculations

$$\prod_{v \in S} \prod_{i=1}^{N} |L_{i,v}(\mathbf{x})|_v = O\left(\left(b^{k^2} a^{h+k} a^{-\epsilon N} \right)^n \right).$$

(Note that the implied constants depend only on a, b, h, k, not on n.) We now choose, once and for all, the integer k so that $\epsilon k > 2$. With this choice we have $\epsilon N > 2h$, whence $a^{\epsilon N - h - k} > a^{h-k}$. This gives

$$\prod_{v \in S} \prod_{i=1}^{N} |L_{i,v}(\mathbf{x})|_v = O(b^{k^2 n} a^{kn} a^{-hn}).$$

We finally choose the integer h so that $a^h > 2b^{k^2} a^k$, thus finding the estimate

$$\prod_{v \in S} \prod_{i=1}^{N} |L_{i,v}(\mathbf{x})|_v = O(2^{-n}). \tag{4}$$

On the other hand, since in any case $d_n < a^n$, we easily see that $\max |x_i| < A^n$, where A depends on a, b, h, k, but not on n. By taking δ to be any positive number $< \log 2 / \log A$, we deduce from (4) that, provided $n \in \mathcal{N}$ is sufficiently large, we have

$$\prod_{v \in S} \prod_{i=1}^{N} |L_{i,v}(\mathbf{x})|_v < (\max |x_i|)^{-\delta}.$$

By the lemma we thus see that the vectors $\mathbf{x}$ in question lie in finitely many proper subspaces of $\mathbf{Q}^N$. Therefore, we may assume that for infinitely many $n \in \mathcal{N}$, the corresponding $\mathbf{x}$ lies in the hyperplane of equation $\zeta_1 Z_1 + \ldots + \zeta_k Z_k + \sum_{i,j} \alpha_{i,j} Y_{i,j} = 0$, where the pair (i,j) runs through $\{0, \ldots, k\} \times \{1, \ldots, h\}$ and where the coefficients are rational numbers, not all zero.

Substituting from the definition of $\mathbf{x}$, we get the equation

$$\zeta_1 \frac{b^n - 1}{a^n - 1} + \ldots + \zeta_k \frac{b^{kn} - 1}{a^n - 1} + \sum_{i,j} \alpha_{i,j} (\frac{b^i}{a^j})^n = 0, \tag{5}$$

valid for all integers n in an infinite set $\mathcal{A} \subset \mathbf{Z}$.

Now, we note that the functions $n \mapsto a^n$, $n \mapsto b^n$, for $n \in \mathcal{A}$, are algebraically independent over $\mathbf{C}$: in fact, take a nontrivial equation $\sum_{i,j=0}^{D} \gamma_{i,j} a^{in} b^{jn} = 0$, valid for all $n \in \mathcal{A}$. Since a, b are multiplicatively independent, the terms a^ib^j are pairwise distinct, whence there exists a unique largest term a^ib^j with nonzero coefficient. Letting $n\to\infty$ through the set $\mathcal{A}$, we obtain a contradiction.

In view of this fact, equation (5) gives an identity in $\mathbf{Q}(X,Y)$, namely

$$\zeta_1\frac{Y-1}{X-1}+\ldots+\zeta_k\frac{Y^k-1}{X-1}+\sum_{i,j}\alpha_{i,j}\frac{Y^i}{X^j}=0.$$

We may write this as $\frac{f(Y)}{X-1}+\frac{g(X,Y)}{X^h}=0$, where f,g are polynomials. Therefore $X-1$ divides $f(Y)$ in $\mathbf{Q}[X,Y]$, whence $f=0$, and so $g=0$. This means that all the involved coefficient vanish, a contradiction.

Remark. A similar proof gives the same bound of the Theorem for the quantity

$$G_n := \max_{m\le Tn} \text{G.C.D.}(a^n-1, b^m-1),$$

where T is any fixed positive number and n is large enough. We very briefly outline the necessary modifications. As above we arrive at some equation

$$\zeta_1\frac{b^m-1}{a^n-1}+\ldots+\zeta_k\frac{b^{km}-1}{a^n-1}+\sum_{i,j}\alpha_{i,j}\frac{b^{im}}{a^{jn}}=0$$

valid for infinitely many pairs (m,n). Unlike the above proof, the final step (i.e. to derive a contradiction from the displayed equation) needs nontrivial results from the theory of S-unit equations (results which are themselves usually derived as consequences of the Subspace Theorem). See [S2] for a relevant statement.

References

[CZ] P. Corvaja, U. Zannier - Diophantine equations with power sums and universal Hilbert sets, *Indagationes Math.*, **9** (1998), 317-332.

[vdP1] A.J. van der Poorten - Some facts that should be better known, especially about rational functions, in *Number Theory and Applications* (Banff, AB, 1988), 497-528, Kluwer Acad. Publ., Dordrecht, 1989.

[vdP2] A.J. van der Poorten - Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, *C. R. Acad. Sci. Paris*, t. 306, Série I (1988), 97-102.

[S1] W.M. Schmidt - *Diophantine Approximation*, Springer-Verlag LNM **785**, 1980.

[S2] W.M. Schmidt - *Diophantine Approximations and Diophantine Equations*, Springer-Verlag LNM **1467**, 1991.

Yann Bugeaud
Univ. L. Pasteur, Mathématiques
7, rue René Descartes
67084 STRASBOURG CEDEX (FRANCE)
bugeaud@math.u-strasbg.fr

Pietro Corvaja
Dipartimento di Mat. e Inf.
via delle Scienze, 206
33100 UDINE (ITALY)
corvaja@dimi.uniud.it

Umberto Zannier
I.U.A.V. - DCA
S. Croce, 191
30135 VENEZIA (ITALY)
zannier@iuav.it