The Nagell–Ljunggren equation via Runge's method

Michael A. Bennett · Aaron Levin

Abstract The Diophantine equation $\frac{x^n-1}{x-1} = y^q$ has four known solutions in integers x, y, q and n with $|x|, |y|, q > 1$ and $n > 2$. Whilst we expect that there are, in fact, no more solutions, such a result is well beyond current technology. In this paper, we prove that if (x, y, n, q) is a solution to this equation, then n has three or fewer prime divisors, counted with multiplicity. This improves a result of Bugeaud and Mihăilescu.

Keywords Nagell–Ljunggren equation · Runge's method

Mathematics Subject Classification   11D61

1 Introduction

The *Nagell–Ljunggren equation*

$$\frac{x^n - 1}{x - 1} = y^q, \quad \text{in integers} |x| > 1, |y| > 1, n > 2, q \geq 2 \tag{1}$$

arises in a wide variety of contexts, ranging from group theory [8] to irrationality criteria [14]; for an excellent survey, the reader is directed to Bugeaud and Mignotte [4].

Communicated by U. Zannier.

M. A. Bennett (✉)
Department of Mathematics, University of British Columbia, Vancouver, BC, Canada
e-mail: bennett@math.ubc.ca

A. Levin
Department of Mathematics, Michigan State University, East Lansing, MI, USA
e-mail: adlevin@math.msu.edu

Equation (1) attracted attention initially due to its connection to Catalan's conjecture and the corresponding Diophantine equation

$$x^n - y^q = 1. \tag{2}$$

Whilst Catalan's conjecture was proven by Mihăilescu [11] in 2004, the Nagell–Ljunggren equation has, in a certain sense, outlived its more illustrious cousin, in that it remains unknown to date whether the number of solutions to (1) in the four variables x, y, n and q is finite. Indeed, such a conclusion is beyond current technology even in the restricted case where $n = q$. Equation (1) does have precisely four known solutions:

$$(\mathcal{NL}) \quad \frac{3^5 - 1}{3 - 1} = 11^2, \quad \frac{7^4 - 1}{7 - 1} = 20^2, \quad \frac{18^3 - 1}{18 - 1} = 7^3 \quad \text{and} \quad \frac{(-19)^3 - 1}{(-19) - 1} = 7^3$$

and there is an impressively large literature providing constraints upon any hitherto unknown ones. In particular, combining results from [5,6,9,11–13], we have

Proposition 1 *If (x, y, n, q) is a solution of Eq. (1) not in $(\mathcal{NL})$, then*

- *$q \geq 3$ is odd,*
- *The least prime divisor p of n satisfies $p \geq 5$,*
- *$|x| \geq 10^4$ and x has a prime divisor $p \equiv 1 \pmod{q}$.*

We can in fact say rather more if we additionally assume that x is positive, improving the lower bounds on both $|x|$ and the least prime divisor of n in this case (see [2,3]); though similar arguments can be applied to negative values of x to sharpen Proposition 1, we will not have need of such a result here.

One feature distinguishing Eq. (1) from (2) is that the reduction to the case where n is prime is without loss of generality in (2), but not in (1). That being said, there is some degree of control over how composite the exponent n can be. Specifically, writing $\omega(n)$ for the number of distinct prime divisors of n, an argument of Shorey [15], together with the results of [1], implies that $\omega(n) \leq q - 2$ (for x both positive and negative, though this is stated in [15] only for the former). In [7], Bugeaud and Mihăilescu sharpened this substantially, proving that if (x, y, n, q) is a solution to (1), with $x > 1$, then necessarily

$$\omega(n) \leq \Omega(n) \leq 4,$$

where $\Omega(n)$ is the total number of prime divisors of n, counted with multiplicity. Our main result is the following improvement of this:

Theorem 1 *If (x, y, n, q) is a solution of (1), then $\omega(n) \leq \Omega(n) \leq 3$.*

The proof of this theorem relies upon a careful application of the classical method of Runge to an equation of the shape $f(x) = g(y)$, where f and g are polynomials with integer coefficients. The result of Bugeaud and Mihăilescu [7] depends fundamentally upon earlier work of Mihăilescu [10], which one might view, in part, as an application of Runge's method over cyclotomic fields. The proof of the crucial inequality from [10], given in Theorem 2 of that paper, uses tools from cyclotomic field theory and

techniques developed in the proof of Catalan's conjecture. What we prove, in an essentially elementary fashion and independent of the results of [10], is that solutions to (1) necessarily satisfy $\omega(n) \leq \Omega(n) \leq 3$, with the possible exception of the special case where $(n, q) = (p^5, 5)$ and $p \mid x - 1$, for p prime. We eliminate this remaining exceptional case by appealing to [10].

Our main tools in proving Theorem 1 are the following pair of results.

Theorem 2 *Suppose that q, r, s, x, y and z are integers with q prime and $3 \leq r < s$, such that*

$$y^q = \frac{x^r - 1}{x - 1} \tag{3}$$

and

$$z^q = \frac{x^s - 1}{x - 1}. \tag{4}$$

Then

$$|x| < 4 \max\left\{1, \frac{s}{qr}\right\} q^{r-1+\frac{s-r}{q-1}}. \tag{5}$$

Theorem 3 *Suppose that integers x, y, z and u and odd primes p and q satisfy*

$$py^q = \frac{x^p - 1}{x - 1},$$

$$p^2 z^q = \frac{x^{p^2} - 1}{x - 1}$$

and

$$p^3 u^q = \frac{x^{p^3} - 1}{x - 1}.$$

Then

$$|x| < 17 \, p^3 \left(\max\left\{1, \frac{p}{q}\right\}\right)^3 q^{p^2 + p - 2 + (p^3 - 1)/(q-1)}. \tag{6}$$

2 Preliminaries

Before proceeding with the proof of Theorem 1, we require a pair of lemmata of a combinatorial nature. Given solutions to (1), these will enable us to deduce the existence of simultaneous solutions to a number of related equations. The first is a result of Shorey [15, Lemma 7]. For a positive integer n, let $Q_n = \phi(G(n))$, where $G(n)$ is the square-free part of n and ϕ is Euler's function.

Lemma 1 *Let (x, y, n, q) be a solution of (1) with n odd. If the divisor D of n satisfies $(D, n/D) = (D, Q_{n/D}) = 1$, then there exist integers y_1 and y_2, with $y_1 y_2 = y$,*

$$y_1^q = \frac{(x^D)^{n/D} - 1}{x^D - 1} \quad \text{and} \quad y_2^q = \frac{x^D - 1}{x - 1}.$$

We use this to prove the following

Lemma 2 *Let (x, y, n, q) be a solution of* (1) *with n odd and write*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

where the α_i are positive integers and the p_i are primes with

$$p_1 < p_2 < \cdots < p_k.$$

Then, for each $1 \leq s \leq k$ and $0 \leq t \leq \alpha_s - 1$, writing

$$M_{s,t} = p_s^t \, p_{s+1}^{\alpha_{s+1}} \cdots p_k^{\alpha_k},$$

there exists an integer $y_{s,t}$ and $\delta_s \in \{0, 1\}$ such that we have

$$\frac{x^{p_s M_{s,t}} - 1}{x^{M_{s,t}} - 1} = p_s^{\delta_s} \, y_{s,t}^q. \tag{7}$$

If $\delta_s = 1$, then $q \mid \alpha_s$.

Proof Observe that, by assumption,

$$\prod_{s=1}^{k} \prod_{t=0}^{\alpha_s - 1} \frac{x^{p_s M_{s,t}} - 1}{x^{M_{s,t}} - 1} = y^q. \tag{8}$$

Let us suppose first that $k = 1$. Since, given integers $|z| > 1$ and $m \geq 1$, we have that

$$\gcd\left(\frac{z^m - 1}{z - 1}, z - 1\right) \quad \text{divides} \quad m,$$

it follows, writing $X = x^{M_{1,t}} = x^{p_1^t}$ for $t \in \{0, 1, \ldots, \alpha_1 - 1\}$, that

$$\gcd\left(\frac{X^{p_1} - 1}{X - 1}, X - 1\right) \in \{1, p_1\}.$$

Moreover, if $X \equiv 1 \pmod{p_1}$, say $X - 1 = p_1 a$ with a an integer, then

$$
\begin{aligned}
X^{p_1 - 1} + X^{p_1 - 2} + \cdots + 1 &= (1 + p_1 a)^{p_1 - 1} + (1 + p_1 a)^{p_1 - 2} + \cdots + 1 \\
&\equiv p_1 + \textstyle\sum_{i=1}^{p_1 - 1} i p_1 a \pmod{p_1^2} \\
&\equiv p_1 + a(p_1 - 1) p_1^2/2 \equiv p_1 \pmod{p_1^2},
\end{aligned}
$$

and, in particular, repeatedly applying Fermat's Little Theorem, we have

$$\operatorname{ord}_{p_1}\left(\frac{x^{p_1^{t+1}} - 1}{x^{p_1^t} - 1}\right) = \begin{cases} 1 & \text{if } x \equiv 1 \pmod{p_1} \\ 0 & \text{otherwise,} \end{cases}$$

for each $0 \le t \le \alpha_1 - 1$. There thus exist integers y_t, again for $0 \le t \le \alpha_1 - 1$, such that

$$\frac{x^{p_1^{t+1}} - 1}{x^{p_1^t} - 1} = p_1^{\delta} y_t^q,$$

where

$$\delta = \begin{cases} 1 & \text{if } x \equiv 1 \pmod{p_1} \\ 0 & \text{otherwise.} \end{cases}$$

Since, from (8), we have

$$\alpha_1 \delta = \text{ord}_{p_1} \prod_{t=0}^{\alpha_1 - 1} \frac{x^{p_1^{t+1}} - 1}{x^{p_1^t} - 1} = q \, \text{ord}_{p_1} y \equiv 0 \pmod{q},$$

the desired result follows.

Suppose now that the stated conclusion is true for solutions to (1) with $\omega(n) = k - 1$, where $k \ge 2$. Assuming that (x, y, n, q) is a solution of (1) with n odd and $\omega(n) = k$, say,

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

we may thus apply Lemma 1 with $D = n/p_1^{\alpha_1}$ to deduce the existence of integers Z and W such that

$$\frac{X - 1}{x - 1} = Z^q \quad \text{and} \quad \frac{X^{p_1^{\alpha_1}} - 1}{X - 1} = W^q, \tag{9}$$

where $X = x^{n/p_1^{\alpha_1}}$. As previously, we find that

$$q \, \text{ord}_{p_1} W = \text{ord}_{p_1} \prod_{t=0}^{\alpha_1 - 1} \frac{X^{p_1^{t+1}} - 1}{X^{p_1^t} - 1} = \begin{cases} \alpha_1 & \text{if } X \equiv 1 \pmod{p_1} \\ 0 & \text{otherwise,} \end{cases}$$

whereby we have (7) for $s = 1$. Applying our inductive hypothesis to the first equation in (9) (where we have $\omega(n/p_1^{\alpha_1}) = k - 1$), we conclude as desired. $\square$

3 Proof of Theorem 2

The idea of the proof is to apply Runge's method to an appropriate curve. The classical Runge's method is used to bound integer points on superelliptic curves of the form $y^q = f(x)$, where f is a monic polynomial with integer coefficients and $q \mid \deg f$. In order to construct a situation where this version of Runge's method applies, we will consider a product of powers of $\frac{x^r - 1}{x - 1}$ and $\frac{x^s - 1}{x - 1}$ to obtain a polynomial f of degree divisible by q and then examine integer solutions to $w^q = f(x)$.

Let q, r, s, x, y, z be an integer solution to Eqs. (3) and (4), as in the statement of the theorem. We may assume throughout that $|x| > 2$. Note that the main result of Bennett [1] implies that the Diophantine equation

$$x^t X^q - (x-1)Y^q = 1$$

has, if $t = 1$, precisely the solution $X = Y = 1$ in nonzero integers X and Y, and, for a fixed positive integer $2 \leq t \leq q - 1$, at most a single nonzero solution X, Y. Choosing integers $0 \leq r_0, s_0 < q$ such that $r \equiv r_0 \pmod{q}$ and $s \equiv s_0 \pmod{q}$ and rewriting (3) and (4) as

$$x^{r_0} \left(x^{(r-r_0)/q}\right)^q - (x-1)y^q = 1 \quad \text{and} \quad x^{s_0} \left(x^{(s-s_0)/q}\right)^q - (x-1)z^q = 1,$$

we may thus conclude that $1, r$ and s are pairwise incongruent modulo q (whereby, since Proposition 1 implies that $\gcd(rs, 3) = 1$, we may assume that $q \geq 5$). In particular, since $r \not\equiv 1 \pmod{q}$ and $s \not\equiv 1 \pmod{q}$, we may define an integer a with $0 < a < q$, via

$$a \equiv -(r-1)^{-1}(s-1) \pmod{q}.$$

Since $r \not\equiv s \pmod{q}$, it follows that $a \neq q - 1$, whence $1 \leq a \leq q - 2$. Let us now define

$$N = a(r-1) + s - 1,$$

so that

$$N \equiv -(r-1)^{-1}(s-1)(r-1) + (s-1) \equiv 0 \pmod{q},$$

whereby N/q is an integer.

We consider the equation

$$w^q = \left(\frac{x^r - 1}{x-1}\right)^a \left(\frac{x^s - 1}{x-1}\right), \tag{10}$$

where now Runge's condition is satisfied. This equation has the integer solution $(w, x) = (y^a z, x)$. Consider the Laurent series expansion

$$\left[\left(\tfrac{x^r-1}{x-1}\right)^a \left(\tfrac{x^s-1}{x-1}\right)\right]^{\frac{1}{q}} = (x^r - 1)^{a/q}(x^s - 1)^{1/q}(x-1)^{(-a-1)/q}$$

$$= x^{N/q}\left(1 - \tfrac{1}{x^r}\right)^{a/q}\left(1 - \tfrac{1}{x^s}\right)^{1/q}\left(1 - \tfrac{1}{x}\right)^{(-a-1)/q}.$$

Expanding

$$\left(1 - \frac{1}{x^r}\right)^{a/q} = \sum_{i=0}^{\infty} (-1)^i \binom{a/q}{i} x^{-ri}$$

and similarly for $\left(1 - \frac{1}{x^s}\right)^{1/q}$ and $\left(1 - \frac{1}{x}\right)^{(-a-1)/q}$, we may write

$$\left[\left(\frac{x^r - 1}{x - 1}\right)^a \left(\frac{x^s - 1}{x - 1}\right)\right]^{\frac{1}{q}} = x^{N/q} \sum_{n=0}^{\infty} a_n x^{-n},$$

where

$$a_n = \sum_{ri+sj+k=n,\ i,j,k \geq 0} \binom{a/q}{i} \binom{1/q}{j} \binom{-(a+1)/q}{k} (-1)^{i+j+k}.$$

Note that the series converges if $|x| > 1$. It follows that, for any solution (w, x) of (10) with $|x| > 1$,

$$w = \zeta x^{N/q} \sum_{n=0}^{\infty} a_n x^{-n},$$

for some qth root of unity ζ. In our case, w and x are both real, so we must have

$$w = \pm x^{N/q} \sum_{n=0}^{\infty} a_n x^{-n}. \tag{11}$$

Before we proceed further, we need to understand the coefficients a_n somewhat better.

Lemma 3 *Let n be a nonnegative integer. Then we have*

$$ord_q a_n = -n - ord_q(n!), \tag{12}$$

$$q^{n + \left[\frac{n}{q-1}\right]} a_n \text{ is an integer}, \tag{13}$$

and

$$|a_n| \leq ([n/r] + 1)([n/s] + 1). \tag{14}$$

Proof If l is a nonnegative integer and m is an integer, coprime to a given prime q, then we have

$$ord_q \binom{m/q}{l} = -l - ord_q(l!).$$

Let $n \geq 0$ and suppose that i, j and k are nonnegative integers for which $ri + sj + k = n$. We thus have

$$ord_q \left(\binom{a/q}{i} \binom{1/q}{j} \binom{-(a+1)/q}{k}\right) = -i - j - k - ord_q(i!j!k!).$$

It follows, if i and j are nonnegative integers, not both zero, that

$$-\mathrm{ord}_q \binom{-(a+1)/q}{n} + \mathrm{ord}_q \left(\binom{a/q}{i} \binom{1/q}{j} \binom{-(a+1)/q}{k} \right)$$

$$= (r-1)i + (s-1)j + \mathrm{ord}_q \left(\frac{(ri+sj+k)!}{i!j!k!} \right) \geq r-1,$$

since $\frac{(ri+sj+k)!}{i!j!k!}$ is an integer. We thus have

$$\mathrm{ord}_q a_n = \mathrm{ord}_q \left(\binom{-(a+1)/q}{n} (-1)^n \right) = -n - \mathrm{ord}_q(n!),$$

whereby $q^{n+\mathrm{ord}_q(n!)} a_n$ is an integer. Statement (13) follows upon observing that

$$\mathrm{ord}_q(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{q^k} \right] \leq \left[\frac{n}{q-1} \right].$$

To prove inequality (14), recall that $1 \leq a \leq q-2$ and apply the easy fact that $|c| \leq q$ implies $\left| \binom{c/q}{i} \right| \leq 1$ for all $i \geq 0$.   □

Let us now define

$$P(x) = q^{N/q + \left[\frac{N}{q(q-1)} \right]} x^{N/q} \sum_{n=0}^{N/q} a_n x^{-n}.$$

Note that, by Lemma 3, $P(x)$ is a polynomial with integer coefficients and, since $\mathrm{ord}_q a_{n+1} < \mathrm{ord}_q a_n \leq 0$ for all n,

$$q^{N/q + \left[\frac{N}{q(q-1)} \right]} w \mp P(x) \neq 0.$$

Let $m = N/q + 1$. Then from our definitions, Lemma 3 and (11),

$$\left| q^{N/q + \left[\frac{N}{q(q-1)} \right]} w \mp P(x) \right| = q^{N/q + \left[\frac{N}{q(q-1)} \right]} \left| x^{N/q} \sum_{n=m}^{\infty} a_n x^{-n} \right|$$

$$\leq q^{N/(q-1)} |x|^{N/q} \sum_{n=m}^{\infty} ([n/r]+1)([n/s]+1)|x|^{-n}.$$

Since we have that

$$\frac{([(n+1)/r]+1)([(n+1)/s]+1)}{([n/r]+1)([n/s]+1)} \leq 3,$$

for $n \geq m \geq 2$ and $s > r \geq 3$, where the inequality is sharp (corresponding to $(r,s,n) = (r, 2r, 2r-1)$), it follows that the positive integer

$$\left| q^{N/q+\left[\frac{N}{q(q-1)}\right]} w \mp P(x) \right|$$

is bounded above by

$$q^{N/(q-1)}([m/r]+1)([m/s]+1)|x|^{-1} \sum_{n=0}^{\infty} 3^n |x|^{-n}$$

$$= q^{N/(q-1)}([m/r]+1)([m/s]+1)\frac{1}{|x|-3}$$

and hence

$$|x| < 3 + q^{N/(q-1)}([m/r]+1)([m/s]+1).$$

From

$$N = a(r-1)+s-1 \le (q-2)(r-1)+s-1,$$

we find that

$$\frac{m}{r} < 1 + \frac{s}{qr} \quad \text{and} \quad \frac{m}{s} < 1,$$

whereby the result follows.

4 Proof of Theorem 3

Let x, y, z, u, p and q be as in the statement of Theorem 3. We choose a and b to be the smallest nonnegative integers satisfying

$$a \equiv 2p+1 \pmod{q} \quad \text{and} \quad b \equiv -p-2 \pmod{q}.$$

Then we have, writing $N = a(p-1)+b(p^2-1)+(p^3-1)$, that

$$N \equiv a+2b+3 \equiv 0 \pmod{q}$$

and hence

$$\left(\frac{x^p-1}{x-1}\right)^a \left(\frac{x^{p^2}-1}{x-1}\right)^b \left(\frac{x^{p^3}-1}{x-1}\right) = w^q, \tag{15}$$

for some integer w, where the left hand side is a polynomial in x with degree divisible by q. We have

$$\left[\left(\frac{x^p-1}{x-1}\right)^a \left(\frac{x^{p^2}-1}{x-1}\right)^b \left(\frac{x^{p^3}-1}{x-1}\right)\right]^{\frac{1}{q}}$$

$$= (x^p-1)^{a/q}(x^{p^2}-1)^{b/q}(x^{p^3}-1)^{1/q}(x-1)^{(-a-b-1)/q}$$

$$= x^{N/q}\left(1-\frac{1}{x^p}\right)^{a/q}\left(1-\frac{1}{x^{p^2}}\right)^{b/q}\left(1-\frac{1}{x^{p^3}}\right)^{1/q}\left(1-\frac{1}{x}\right)^{(-a-b-1)/q}$$

$$= x^{N/q}\sum_{n=0}^{\infty} b_n x^{-n},$$

where $\sum_{n=0}^{\infty} b_n x^{-n}$ is the product of the four series

$$\sum_{i=0}^{\infty} (-1)^i \binom{a/q}{i} x^{-pi}, \quad \sum_{j=0}^{\infty} (-1)^j \binom{b/q}{j} x^{-p^2 j}, \quad \sum_{k=0}^{\infty} (-1)^k \binom{1/q}{k} x^{-p^3 k}$$

and

$$\sum_{l=0}^{\infty} (-1)^l \binom{-(a+b+1)/q}{l} x^{-l}.$$

We may thus write

$$b_n = \sum \binom{a/q}{i} \binom{b/q}{j} \binom{1/q}{k} \binom{-(a+b+1)/q}{l} (-1)^{i+j+k+l},$$

where the sum is over nonnegative integers i, j, k and l for which

$$pi + p^2 j + p^3 k + l = n.$$

Note here that we have $0 \le a, b \le q - 1$, so that $a + b + 1 \le 2q - 1$. It follows that

$$\left| \binom{-(a+b+1)/q}{l} \right| < l + 1$$

and hence

$$|b_n| < \left(\left[\frac{n}{p} \right] + 1 \right) \left(\left[\frac{n}{p^2} \right] + 1 \right) \left(\left[\frac{n}{p^3} \right] + 1 \right) (n + 1). \tag{16}$$

The series $\sum_{n=0}^{\infty} b_n x^{-n}$ thus converges if $|x| > 1$ and hence, for any real solution (w, x) of (15) with $|x| > 1$, we can write

$$w = \pm x^{N/q} \sum_{n=0}^{\infty} b_n x^{-n}.$$

Arguing as in the proof of Lemma 3, we find that

$$\text{ord}_q \left(\binom{a/q}{i} \binom{b/q}{j} \binom{1/q}{k} \binom{-(a+b+1)/q}{l} \right)$$
$$\ge -i - j - k - l - \text{ord}_q (i! j! k! l!).$$

We assume now that $q \nmid (a + b + 1)$ (or equivalently, $p \ne q$). It will be clear from our argument that one obtains even stronger bounds when $q \mid (a + b + 1)$ (note that in this case, $(x^p - 1)^a (x^{p^2} - 1)^b (x^{p^3} - 1)$ is a perfect qth power). Then, assuming q fails to divide $a + b + 1$, after a little work, we conclude that

$$\text{ord}_q b_n = \text{ord}_q \binom{-(a+b+1)/q}{n} = -n - \text{ord}_q (n!),$$

whence $b_n \neq 0$ for each n and $q^{n+\mathrm{ord}_q(n!)} b_n$ is an integer. We thus have $q^{n+\left[\frac{n}{q-1}\right]} b_n$ integral, for each $n \geq 0$. Define

$$P(x) = q^{N/q+\left[\frac{N}{q(q-1)}\right]} x^{N/q} \sum_{n=0}^{N/q} b_n x^{-n}.$$

The polynomial $P(x)$ thus has integer coefficients and, since $\mathrm{ord}_q b_{n+1} < \mathrm{ord}_q b_n \leq 0$ for all n,

$$q^{N/q+\left[\frac{N}{q(q-1)}\right]} w \mp P(x) \neq 0.$$

Setting as before $m = N/q + 1$, we may conclude that

$$\left| q^{N/q+\left[\frac{N}{q(q-1)}\right]} w \mp P(x) \right| = q^{N/q+\left[\frac{N}{q(q-1)}\right]} \left| x^{N/q} \sum_{n=m}^{\infty} b_n x^{-n} \right|$$

is a positive integer. On the other hand, via (16), the right hand side here is bounded above by

$$q^{N/(q-1)} |x|^{N/q} \sum_{n=m}^{\infty} ([n/p] + 1)([n/p^2] + 1)([n/p^3] + 1)(n + 1)|x|^{-n}$$

which is in turn at most

$$q^{N/(q-1)}([m/p] + 1)([m/p^2] + 1)([m/p^3] + 1)(m + 1)|x|^{-1} \sum_{n=0}^{\infty} (7/2)^n |x|^{-n}.$$

Here, we have used that

$$\frac{([(n + 1)/p] + 1)([(n + 1)/p^2] + 1)([(n + 1)/p^3] + 1)(n + 2)}{([n/p] + 1)([n/p^2] + 1)([n/p^3] + 1)(n + 1)} \leq \frac{2240}{729} < 7/2,$$

with equality in the first of these inequalities corresponding to $(n, p) = (26, 3)$. It follows that

$$1 \leq q^{N/(q-1)}([m/p] + 1)([m/p^2] + 1)([m/p^3] + 1)(m + 1)\frac{1}{|x| - 7/2},$$

whereby

$$|x| < 7/2 + q^{N/(q-1)}([m/p] + 1)([m/p^2] + 1)([m/p^3] + 1)(m + 1).$$

If we now use the inequality

$$N \leq (q - 1)(p - 1) + (q - 1)(p^2 - 1) + p^3 - 1 = (q - 1)(p^2 + p - 2) + p^3 - 1,$$

we find that $m < p^3$ and

$$m < \begin{cases} 2p^2 + p - 1 & \text{if } q \geq p, \\ 2p^3/q - 1 & \text{if } q < p. \end{cases}$$

We conclude easily that

$$|x| < \frac{7}{2} + \frac{49}{3} p^3 \left(\max\left\{1, \frac{p}{q}\right\} \right)^3 q^{p^2 + p - 2 + (p^3 - 1)/(q-1)},$$

and the result follows.

5 Proof of Theorem 1

We now prove Theorem 1. Let (x, y, n, q) be a solution of (1) with n odd and $\Omega(n) \geq 4$. As in Lemma 2, we write

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

where the α_i are positive integers and the p_i are primes with

$$p_1 < p_2 < \cdots < p_k.$$

Note that $k = \omega(n)$, $\sum_{i=1}^{k} \alpha_i = \Omega(n)$, and that, by assumption, Eq. (8) holds.

Define δ_s as in Lemma 2, for $1 \leq s \leq k$. We begin by supposing that $\delta_s = 0$ for each value of s. Let us set

$$p = \begin{cases} p_1 & \text{if } \alpha_1 \geq 2, \\ p_2 & \text{if } \alpha_1 = 1, \end{cases}$$

and define the positive integer m via $n = m p_1 p$. From Lemma 2, we may find integers y_1 and y_2 for which

$$\frac{x^n - 1}{x^m - 1} = (y_1 y_2)^q \quad \text{and} \quad \frac{x^{mp} - 1}{x^m - 1} = y_2^q.$$

Applying Theorem 2 with $r = p$, $s = p_1 p$, and using the fact that $|x| \geq 2q + 1$, we thus have

$$2^m q^m < 4 \max\left\{1, \frac{p_1}{q}\right\} q^{p - 1 + \frac{p(p_1 - 1)}{q - 1}}.$$

Since $q \geq 3$, $p \geq p_1 \geq 5$ and $\Omega(n) \geq 4$ (whence $m \geq p^2$), it follows that

$$2^{p^2} q^{p^2} \leq 2^m q^m < p q^{p + \frac{p(p-1)}{q-1}}$$

and so

$$2^{p^2} q^{p(p-1)(q-2)/(q-1)} < p,$$

an immediate contradiction.

Next, let us suppose that $\delta_s = 1$ for at least one value of s. Choosing s to be the smallest such index, we thus have that $q \mid \alpha_s$ and, writing

$$X = x^\beta \quad \text{where} \quad \beta = \prod_{j>s} p_j^{\alpha_j},$$

and applying Lemma 2,

$$\frac{X^{p_s^{\alpha_s - i}} - 1}{X^{p_s^{\alpha_s - i - 1}} - 1} = p_s y_i^q, \quad \text{for } i = 0, 1, \ldots, \alpha_s - 1$$

and integers y_i. Setting $Z = X^{p_s^{\alpha_s - 3}}$, we may thus write

$$\frac{Z^{p_s^j} - 1}{Z - 1} = p_s^j z_j^q \quad \text{for } j = 1, 2, 3,$$

where the z_j are integers. Theorem 3 thus implies that

$$|Z| < 17 \, p_s^3 \left(\max \left\{ 1, \frac{p_s}{q} \right\} \right)^3 q^{p_s^2 + p_s - 2 + (p_s^3 - 1)/(q-1)}. \tag{17}$$

Since

$$|Z| \geq |x|^{p_s^{\alpha_s - 3}},$$

and Proposition 1 enables us to conclude that $|x| \geq 2q + 1$, we thus have

$$2^{p_s^{\alpha_s - 3}} q^{p_s^{\alpha_s - 3}} < 17 \, p_s^3 \left(\max \left\{ 1, \frac{p_s}{q} \right\} \right)^3 q^{p_s^2 + p_s - 2 + (p_s^3 - 1)/(q-1)}.$$

From $p_s \geq 5$ and the fact that $q \mid \alpha_s$, we reach an easy contradiction, at least provided either $q \geq 7$, or $q \in \{3, 5\}$ and $\alpha_s \neq q$. We may thus suppose that $(q, \alpha_s) = (3, 3)$ or $(5, 5)$ (whereby, from the fact that $\omega(n) \leq q - 2$, we have $k = 1$ and $k \leq 3$, respectively). We therefore have either $n = p^3$ for p prime (so that $\Omega(n) < 4$ as desired) or $(q, \alpha_s) = (5, 5)$. In the latter case, if $s < k$, then

$$|Z| = |x|^{\beta p_s^2} > |x|^{p_s^3} \geq 10^{4 p_s^3},$$

contradicting (17). We may thus assume that $s = k$. We will show that necessarily $k = 1$. Suppose otherwise. Then setting $X = x^{p_k^3}$ and applying Lemma 2, we thus have

$$\frac{X^{p_k} - 1}{X - 1} = p_k y_1^5,$$

$$\frac{X^{p_k^2} - 1}{X - 1} = p_k^2 y_2^5$$

and

$$\frac{X^{p_{k-1} p_k^2} - 1}{X - 1} = p_k^2 y_3^5,$$

for integers y_1, y_2 and y_3. We choose integers a and b, with $0 \le a, b \le 4$, such that

$$a(p_k - 1) + b(p_k^2 - 1) + p_{k-1} p_k^2 - 1 \equiv 0 \pmod 5$$

and

$$a + 2b + 2 \equiv 0 \pmod 5.$$

This is always possible as $\det \begin{pmatrix} p_k - 1 & p_k^2 - 1 \\ 1 & 2 \end{pmatrix} = -(p_k - 1)^2$ and $p_k \not\equiv 1 \pmod 5$ (say by combining the proof of Lemma 9 of [15] with Theorem 1.1 of [1]).

We now argue as in the proof of Theorem 3, considering the Laurent series expansion

$$\left[\left(\frac{X^{p_k} - 1}{X - 1} \right)^a \left(\frac{X^{p_k^2} - 1}{X - 1} \right)^b \left(\frac{X^{p_{k-1} p_k^2} - 1}{X - 1} \right) \right]^{1/5} = X^{N/5} \sum_{n=0}^{\infty} c_n X^{-n},$$

where now

$$N = a(p_k - 1) + b(p_k^2 - 1) + p_{k-1} p_k^2 - 1.$$

Here, we have

$$c_n = \sum \binom{a/5}{i} \binom{b/5}{j} \binom{1/5}{l} \binom{-(a+b+1)/5}{m} (-1)^{i+j+l+m},$$

where the sum is over nonnegative integers i, j, l and m with

$$p_k i + p_k^2 j + p_{k-1} p_k^2 l + m = n.$$

We note that $a + b + 1 \equiv 0 \pmod 5$ easily implies that either $p_k \equiv 0 \pmod 5$ or $p_{k-1} \equiv 1 \pmod 5$, both of which are impossible (the first, since $p_{k-1} \ge 5$, and the second, from using again Theorem 1.1 of [1]).

As previously,

$$\mathrm{ord}_5 c_n = -n - \mathrm{ord}_5(n!),$$

so that $5^{n+[\frac{n}{4}]}c_n$ is a nonzero integer for each $n \geq 0$, and

$$|c_n| < \left(\left[\frac{n}{p_k}\right]+1\right)\left(\left[\frac{n}{p_k^2}\right]+1\right)\left(\left[\frac{n}{p_{k-1}p_k^2}\right]+1\right)(n+1). \qquad (18)$$

We have that

$$w = p_k^{(a+2b+2)/5}y_1^a y_2^b y_3 = \pm X^{N/5}\sum_{n=0}^{\infty}c_n X^{-n}$$

and hence writing

$$P(X) = 5^{N/5+[N/20]}X^{N/5}\sum_{n=0}^{N/5}c_n X^{-n},$$

that $5^{N/5+[N/20]}w \mp P(X)$ is a nonzero integer. Defining $m = N/5+1$, we thus have

$$1 \leq 5^{N/4}|X|^{N/5}\sum_{n=m}^{\infty}([n/p_k]+1)([n/p_k^2]+1)([n/p_{k-1}p_k^2]+1)(n+1)|X|^{-n}.$$

Writing $T_n = ([n/p_k]+1)([n/p_k^2]+1)([n/p_{k-1}p_k^2]+1)(n+1)$,

$$T_{n+1}/T_n \leq 106{,}272/42{,}875 < 3,$$

provided $n \geq 3$ and $5 \leq p_{k-1} < p_k$ (with equality in the first inequality if $n = 244$, $p_{k-1} = 5$ and $p_k = 7$). We thus have that

$$1 \leq 5^{N/4}(m/p_k+1)(m/p_k^2+1)(m/p_{k-1}p_k^2+1)(m+1)|X|^{-1}\sum_{n=0}^{\infty}3^n|X|^{-n},$$

whence

$$|X| < 3 + 5^{N/4}(m/p_k+1)(m/p_k^2+1)(m/p_{k-1}p_k^2+1)(m+1).$$

Since

$$N \leq 4p_k + 4p_k^2 + p_{k-1}p_k^2 - 9 \leq 2p_k^3 - 5,$$

we have

$$|X| < 3 + 5^{\frac{1}{2}p_k^3}\left(\frac{2}{5}p_k^2+1\right)\left(\frac{2}{5}p_k+1\right)\cdot 3 \cdot \left(\frac{2}{5}p_k^3+1\right).$$

On the other hand,

$$|X| = |x|^{p_k^3} \geq 10^{4p_k^3},$$

a contradiction, since $p_k \geq 7$. Our conclusion is thus that

$$n = p^5 \text{ for } p \text{ prime}, q = 5 \text{ and } x \equiv 1 \pmod{p}. \tag{19}$$

To finish the proof of Theorem 1, it remains to treat case (19); we are currently unable to do so without appeal to the results of [10]. If we have a solution to

$$\frac{x^{p^5} - 1}{x - 1} = y^5$$

in integers x and y and prime p with $|x| > 1$ and $x \equiv 1 \pmod{p}$, then

$$\frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = p\, y_k^5$$

for integers y_k, $1 \leq k \leq 5$. Appealing to Theorem 2 of Mihăilescu [10] and the fact that $|x| > 10^4$, it follows that

$$10^{4p^4} < |x|^{p^4} < 5^{10p^2},$$

a contradiction which completes the proof of Theorem 1.

References

1. Bennett, M.A.: Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$. J. Reine Angew. Math. **535**, 1–49 (2001)
2. Bugeaud, Y., Hanrot, G., Mignotte, M.: Sur l'équation diophantienne $\frac{x^n - 1}{x - 1} = y^q$. III. Proc. London Math. Soc. **84**, 59–78 (2002)
3. Bugeaud, Y., Mignotte, M.: Sur l'équation diophantienne $\frac{x^n - 1}{x - 1} = y^q$, II. C. R. Acad. Sci. Paris Sr. I Math. **328**, 741–744 (1999)
4. Bugeaud, Y., Mignotte, M.: L'équation de Nagell–Ljunggren $\frac{x^n - 1}{x - 1} = y^q$. Enseign. Math. **48**, 147–168 (2002)
5. Bugeaud, Y., Mignotte, M., On the Diophantine equation $(x^n - 1), (x - 1) = y^q$ with negative x. Number theory for the millennium, I (Urbana, IL, : 145–151. A K Peters, Natick, MA, 2000) (2002)
6. Bugeaud, Y., Mignotte, M., Roy, Y.: On the Diophantine equation $(x^n - 1)/(x - 1) = y^q$. Pac. J. Math. **193**, 257–268 (2000)
7. Bugeaud, Y., Mihăilescu, P.: On the Nagell–Ljunggren equation $\frac{x^n - 1}{x - 1} = y^q$. Math. Scand. **101**, 177–183 (2007)
8. Guralnick, R.M.: Subgroups of prime power index in a simple group. J. Algebra **81**, 304–311 (1983)
9. Ljunggren, W.: Noen Setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$. Norsk. Mat. Tidsskr. **25**, 17–20 (1943)

10. Mihăilescu, P.: New bounds and conditions for the equation of Nagell–Ljunggren. J. Number Theory **124**(2), 380–395 (2007)
11. Mihăilescu, P.: Primary cyclotomic units and a proof of Catalan's conjecture. J. Reine Angew. Math. **572**, 167–195 (2004)
12. Nagell, T.: Des équations indéterminées $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$. Nordsk. Mat. Forenings Skr. **2** (1920)
13. Nagell, T.: Note sur l'équation indéterminée $(x^n - 1)/(x - 1) = y^q$. Norsk. Mat. Tidsskr. **2**, 75–78 (1920)
14. Sander, J.W.: Irrationality criteria for Mahler's numbers. J. Number Theory **52**, 145–156 (1995)
15. Shorey, T.N.: Perfect powers in values of certain polynomials at integer points. Math. Proc. Camb. Philos. Soc. **99**, 195–207 (1986)