

Title	ON THE NAGELL-LJUNGGREN EQUATION (Analytic Number Theory : Distribution and Approximation of Arithmetic Objects)
Author(s)	Hirata-Kohno, Noriko; Kovacs-Coskun, Tunde; Miyazaki, Takafumi
Citation	数理解析研究所講究録 (2016), 2013: 60-67
Issue Date	2016-12
URL	http://hdl.handle.net/2433/231633
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

ON THE NAGELL-LJUNGGREN EQUATION

N. HIRATA-KOHNO, T. KOVÁCS AND T. MIYAZAKI

ABSTRACT. We show that there exists an effective upper bound for the solutions to the Nagell-Ljunggren equation of the form $\frac{x^m - 1}{x - 1} = y^q$ in 4 unknowns in integers $x > 1, y > 1, m > 2, q > 1$, when x is a cube of an integer. Our method relies on a refined estimate of linear forms in logarithms.

1. INTRODUCTION

It is a longstanding conjecture that the exponential Diophantine equation in four unknowns, so-called the Nagell-Ljunggren equation:

$$(1) \quad \frac{x^m - 1}{x - 1} = y^q \quad \text{in integers } x > 1, y > 1, m > 2, q > 1$$

has finitely many solutions (x, y, m, q) . Nagell and Ljunggren confirmed [12][15][16] that apart from

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

the equation (1) has no solution (x, y, m, q) if either one of the following conditions is satisfied:

- (i) $q = 2$, (ii) $3|m$, (iii) $4|m$, (iv) $q = 3$ and $m \not\equiv 5 \pmod{6}$.

It remains unknown to date whether the number of the solutions is finite or not, and there is no known solution other than those of (2). It is widely believed that there is no other solution. The problem requires us when it happens a perfect power of an integer to be written with all digits equal to 1 in base x . Shorey and Tijdeman [22] proved that the equation (1) has only finitely many solutions (x, y, m, q) if one of the following conditions is satisfied:

- (i) x is fixed, (ii) m has a fixed prime factor, (iii) y has a fixed prime factor. This assertion is effective.

It is mentioned by Shorey [20] that the *abc* conjecture implies the finiteness of the solutions to the equation (1).

Since the case $q = 2$ is solved, there is no loss of generality in assuming that q is an odd prime. The fact that there is no other solution with m even follows from the affirmative answer of Catalan's conjecture due to Mihăilescu [14]. Note that it is still an open problem to prove in general the equation (1) has only finitely many solutions of form (x, y, q, q) .

2000 *Mathematics Subject Classification.* 11G05, 11Y50.

Key words and phrases. Exponential Diophantine equation, the Nagell-Ljunggren equation.

The first author was supported partly by Grant-in-Aid for Scientific Research (C), JSPS, no. 26520208 and no. 15K04799. The second author was supported partly by the OTKA Grant, 100339 and by the JSPS, P12806. The third author was supported partly by Grant-in-Aid for JSPS Research Fellow, JSPS, no. 25-484.

Now we consider the Nagell-Ljunggren equation under the condition that x is a power. Bugeaud, Mignotte, Roy and Shorey [7] proved that the equation (1) has no solution whenever x is a square. Hirata-Kohno and Shorey [9] considered an analogous question when $x = z^\mu$ where $z > 1$, $\mu \geq 3$ and they showed that the equation (1) with $x = z^\mu$ with $q > 2(\mu - 1)(2\mu - 3)$ has only finitely many solutions effectively bounded depending only on μ .

In this paper, we show that the constant giving an upper bound for the height of the solutions, can be improved using a refinement of a lower bound for the linear forms in logarithms of form $|b_1 \log \alpha_1 + \dots + b_n \log \alpha_n|$.

Theorem 1.1 (Hirata-Kohno, Kovács and Miyazaki). *Let $z > 1$ be an integer. Assume $q \neq 5, 7, 11$. Then there exists an effectively computable absolute constant $C > 0$ satisfying the following statement. Suppose (x, y, m, q) is a solution to the equation (1) with $x = z^3$. Then we have $\max(x, y, m, q) \leq C$.*

We may derive the finiteness of the solutions to the equation (1) of Theorem 1.1 from [9], however, our new ingredient here for the proof is based on an advantage of the factor $\log E$ in [11] and [18] appeared in a lower bound for the linear forms in logarithms. We use a lower bound obtained by Bugeaud in [5] which is again precisely calculated by the third author.

Note that the result is due to Inkeri when $\mu = q = 3$ (Lemma 4, [10]). Bugeaud and Mignotte proved if $\mu = q$, there is no solution in (x, y, m, q) (Théorème 9, [6]), and this statement follows from a theorem of Bennett on the Thue equation [3] showing, when $a > b \geq 1$ and $n \geq 3$, that the equation

$$|ax^n - by^n| = 1$$

has at most 1 solution in positive integers (x, y) (indeed, if $\mu = q$, we suppose that there exists $z > 1, y > 1, q \leq 3, m \leq 3$ with $z^{qm} - 1 = (z^q - 1)y^q$, then consider the equation $z^q Z^q - (z^q - 1)Y^q = 1$ where Bennett's theorem can be applied to conclude the statement).

In 2007, Bugeaud and Mihăilescu showed $\omega(m) \leq 4$ if (x, y, m, q) is a solution to the equation (1) [8] and it was improved to $\omega(m) \leq 3$ by Bennett and Levin [4].

2. OUTLINE OF THE PROOF

Proposition 2.1 (Consequence of Lemma 2 of [9]). *The equation (1) with $x = z^3$ implies that either $\max(x, y, m, q)$ is bounded by a positive effective constant, or*

$$\frac{z^m - 1}{z - 1} = y_1^q, \quad \frac{z^{2m} + z^m + 1}{z^2 + z + 1} = y_2^q$$

where $y_1 > 1$ and $y_2 > 1$ are relatively prime integers such that $y_1 y_2 = y$.

The next lemma states approximations of certain algebraic numbers by rationals using Padé approximations found in [5] which is a precise statement of Shorey and Nesterenko [17]. This also improves Lemma 3 of [9].

Lemma 2.2. *Let A, B, K and n be positive integers such that $A > B, K < n, n \geq 3$ and $\omega = (B/A)^{1/n}$ is not a rational number. For $0 < \phi < 1$, put*

$$\delta = 1 + \frac{2 - \phi}{K}, \quad s = \frac{\delta}{1 - \phi},$$

$$u_1 = 40^{n(K+1)(s+1)/(Ks-1)}, u_2^{-1} = K2^{K+s+1}40^{n(K+1)}.$$

Assume that

$$A(A - B)^{-\delta} u_1^{-1} > 1.$$

Then

$$\left| \omega - \frac{p}{q} \right| > \frac{u_2}{Aq^{K(s+1)}}$$

for all integers p and q with $q > 0$.

Now we apply the lemma above to prove the statement whenever q is fixed. We show:

Proposition 2.3. *The equation (1) with $x = z^3$ and the condition $q \neq 5, 7, 11$ implies that $\max(x, y, m)$ is bounded by an effectively computable number depending only on q .*

The proposition 2.3 is proven as follows. Let us consider the equation (1) with $x = z^3$. Recall that Shorey and Tijdeman showed that the equation (1) has only finitely many solutions if either x is fixed or m has a fixed prime divisor. Then we may assume that $\min(m, z)$ exceeds a sufficiently large constant depending only on q . By Proposition 2.1, we may suppose $\frac{z^m - 1}{z - 1} = y_1^q$, $\frac{z^{2m} + z^m + 1}{z^2 + z + 1} = y_2^q$, namely $(z - 1)y_1^q = z^m - 1$, $(z^2 + z + 1)y_2^q = z^{2m} + z^m + 1$. thus $0 < (z^2 + z + 1)y_2^q - (z - 1)^2 y_1^{2q} \leq 3z^m$ which implies

$$(3) \quad 0 < \left| \left(\frac{(z - 1)^2}{z^2 + z + 1} \right)^{1/q} - \frac{y_2}{y_1^2} \right| < \frac{6z^m}{z^2 y_1^{2q}}$$

But Lemma 2.2 with $A = z^2 + z + 1$, $B = (z - 1)^2$ gives a contradiction against the upper bound above.

Now it remains to show that the equation (1) with $x = z^3$ implies that q is bounded. The proof uses a lower bound for the linear forms in logarithms.

The following result is a precise version of [11, Corollaire 3], whose advantage comes from the role of $\log E$ in a lower bound for the linear forms in logarithms.

Proposition 2.4. *Let X_1/Y_1 and X_2/Y_2 be multiplicatively independent rational numbers greater than the unity. Let b_1 and b_2 be positive integers. We consider the linear form*

$$\Lambda = b_2 \log(X_2/Y_2) - b_1 \log(X_1/Y_1).$$

Let A_1, A_2 be positive real numbers such that

$$\log A_i \geq \max\{\log x_i, 1\} \quad (i = 1, 2).$$

Let $E \geq 3$ be a real number such that

$$E \leq 1 + \min \left\{ \frac{\log A_1}{\log(X_1/Y_1)}, \frac{\log A_2}{\log(X_2/Y_2)} \right\}.$$

Assume that

$$E \leq \min\{A_1^{3/2}, A_2^{3/2}\}.$$

Then we have

$$\log |\Lambda| \geq -35.1(\log A_1)(\log A_2)(\log B)^2(\log E)^{-3},$$

where

$$\log B = \max \left\{ \log \left(\frac{b_1}{\log A_2} + \frac{b_2}{\log A_1} \right) + \log \log E + 0.47, 10 \log E \right\}.$$

Using this result, we show the following.

Corollary 2.5. *Let X_1/Y_1 and X_2/Y_2 be multiplicatively independent rational numbers greater than the unity. Assume that*

$$X_1 \geq 3, \quad X_2 \geq 3, \quad \frac{X_2}{Y_2} \leq \frac{4}{3}.$$

Let b_1 be a positive integer. We consider the linear form

$$A = \log(X_2/Y_2) - b_1 \log(X_1/Y_1).$$

Assume that $|A|$ is not zero and that

$$X_2/Y_2 > X_1/Y_1.$$

Define ε with $\varepsilon < 1$ by

$$\frac{X_2}{Y_2} = 1 + \frac{1}{X_2^{1-\varepsilon}}.$$

Then we have

$$\log |A| \geq -35.1 \frac{(\log X_1) \log X_2}{\min\{\log X_1, (1-\varepsilon) \log X_2\}} (\log b_1 + 10)^2.$$

Proof. We may take $(A_1, A_2) = (X_1, X_2)$. It suffices to show that we can take E such that

$$(4) \quad \log E = \min\{\log X_1, (1-\varepsilon) \log X_2\}.$$

Indeed, if so, since

$$\begin{aligned} & \log \left(\frac{b_1}{\log X_2} + \frac{1}{\log X_1} \right) + \log \log E \\ & \leq \log \left(\frac{b_1}{\log X_2} + \frac{1}{\log X_1} \right) + \log \log \min\{X_1, X_2\} \\ & \leq \log(b_1 + 1), \end{aligned}$$

we have

$$\begin{aligned} (\log B)^2 (\log E)^{-3} & \leq \max\{\log(b_1 + 1) + 0.47, 10 \log E\}^2 \cdot (\log E)^{-3} \\ & = \max \left\{ \frac{\log(b_1 + 1) + 0.47}{\log E}, 10 \right\}^2 \cdot (\log E)^{-1} \\ & \leq \max \left\{ \frac{\log(b_1 + 1) + 0.47}{\log 3}, 10 \right\}^2 \cdot (\log E)^{-1} \\ & \leq (\log b_1 + 10)^2 \cdot (\log E)^{-1}. \end{aligned}$$

Hence, Proposition 2.4 gives us the desired inequality. So, we define E by (4). We are left with checking that all required inequalities on E hold.

First, we show $E \geq 3$. For this, it suffices to check that $X_2^{1-\varepsilon} \geq 3$ holds. Since $X_2/Y_2 \leq 4/3$ by our assumption, we have

$$X_2^{\varepsilon-1} = X_2/Y_2 - 1 \leq 1/3.$$

Next, from the definition of ε , we have

$$\log(X_2/Y_2) = \log(1 + X_2^{\varepsilon-1}) < X_2^{\varepsilon-1},$$

and so

$$-\log \log(X_2/Y_2) > (1-\varepsilon) \log X_2 \geq \log E.$$

Since $X_1, X_2 \geq 3$ and $X_2/Y_2 > X_1/Y_1$, it follows from (4) that

$$1 + \min \left\{ \frac{\log X_1}{\log(X_1/Y_1)}, \frac{\log X_2}{\log(X_2/Y_2)} \right\} > \frac{\log 3}{\log(X_2/Y_2)} > E.$$

Finally, we can observe that (4) yields

$$\log \min\{X_1^{3/2}, X_2^{3/2}\} = (3/2) \log \min\{X_1, X_2\} > \log E.$$

This completes the proof. □

We now give an outline of the proof of Theorem 1.1.

Proof. Consider the following linear form in two logarithms:

$$A = \log \left(\frac{z^2 + z + 1}{(z-1)^2} \right) - q \log \left(\frac{y_1^2}{y_2} \right),$$

where positive integers y_1, y_2 satisfy

$$y_1^q = z^{m-1} + z^{m-2} + \cdots + z + 1, \quad y_2^q = \frac{z^{2m} + z^m + 1}{z^2 + z + 1}.$$

In our case, we may assume that

$$m \text{ is odd } > 1.$$

Set

$$(X_1, Y_1) = (y_1^2, y_2), \quad (X_2, Y_2) = (z^2 + z + 1, (z-1)^2), \quad b_1 = q.$$

Note that $X_1, X_2 \geq 3$ and

$$\frac{X_2}{Y_2} = \frac{z^2 + z + 1}{(z-1)^2} \leq \frac{4}{3} \quad (\Leftarrow z \geq 11).$$

(i) Put $(\gamma_1, \gamma_2) = (X_1/Y_1, X_2/Y_2)$. First, we show that $\gamma_2 > \gamma_1$. We already know

$$|A| = |\log \gamma_2 - q \log \gamma_1| < \frac{8\mu}{z^m} = \frac{24}{z^m}.$$

Then

$$\log \gamma_2 > q \log \gamma_1 - \frac{24}{z^m}.$$

Hence, since $q \geq 3$, it suffices to show

$$q \log \gamma_1 \geq \frac{36}{z^m}.$$

Observe that

$$\begin{aligned} \gamma_1^q &= \left(\frac{y_1^2}{y_2} \right)^q = \frac{y_1^{2q}}{y_2^q} = \frac{(z^{m-1} + z^{m-2} + \cdots + z + 1)^2 (z^2 + z + 1)}{z^{2m} + z^m + 1} \\ &> \frac{(z^{m-1} + 1)^2 z^2}{z^{2m} + z^m + 1} \\ &= \frac{z^{2m} + 2z^{m+1} + z^2}{z^{2m} + z^m + 1} \\ &= 1 + \frac{2z^{m+1} + z^2 - z^m - 1}{z^{2m} + z^m + 1} \\ &> 1 + \frac{1}{z^{m-1}}. \end{aligned}$$

Hence

$$q \log \gamma_1 > \log \left(1 + \frac{1}{z^{m-1}} \right) > \frac{0.95}{z^{m-1}} > \frac{36}{z^m} \quad (\Leftarrow z \geq 38).$$

- (ii) Next, we show that $X_1/Y_1, X_2/Y_2$ are multiplicative independent. Suppose the contrary. Then, we can find two co-prime positive integers k, l such that

$$(X_1/Y_1)^{qk} = (Y_2/X_2)^l,$$

that is,

$$\left(\frac{(z^{m-1} + z^{m-2} + \cdots + z + 1)^2 (z^2 + z + 1)}{z^{2m} + z^m + 1} \right)^k = \left(\frac{(z-1)^2}{z^2 + z + 1} \right)^l,$$

or

$$(5) \quad (z^2 + z + 1)^{k+l} (z^{m-1} + z^{m-2} + \cdots + z + 1)^{2k} = (z-1)^{2l} (z^{2m} + z^m + 1)^k.$$

Since m is odd, we easily see from (5) that

$$z \text{ is even.}$$

Since $m \geq 2$ and z is even, we have

$$\begin{aligned} (z^2 + z + 1)^{k+l} &\equiv (z+1)^{k+l} \equiv (k+l)z + 1 \pmod{2z}, \\ (z^{m-1} + z^{m-2} + \cdots + z + 1)^{2k} &\equiv (z+1)^{2k} \equiv 2kz + 1 \equiv 1 \pmod{2z}, \\ (z-1)^{2l} &\equiv (z^2 - 2z + 1)^l \equiv 1 \pmod{2z}, \\ (z^{2m} + z^m + 1)^k &\equiv 1 \pmod{2z}. \end{aligned}$$

It follows from (5) that

$$k + l \equiv 0 \pmod{2}.$$

This together with the fact $\gcd(k, l) = 1$ implies that

$$k \text{ is odd.}$$

Now, we reconsider (5). Since k is odd, we may conclude that the term

$$z^{2m} + z^m + 1 = \frac{z^{3m} - 1}{z^m - 1}$$

has to be a perfect square. But, this contradicts the result of Ljunggren [12].

(iii) We use Corollary 2.5. Noting that

$$\varepsilon = \frac{\log \left(\frac{3z(z^2+z+1)}{(z-1)^2} \right)}{\log(z^2+z+1)} (> 0.5),$$

we have

$$\begin{aligned} \log |A| &\geq -35.1 \max \left\{ \frac{1}{1-\varepsilon} \log X_1, \log X_2 \right\} (\log q + 10)^2 \\ &= -35.1 \max \left\{ \frac{2}{1-\varepsilon} \log y_1, \log(z^2+z+1) \right\} (\log q + 10)^2 \\ &\geq -35.1 \max \left\{ \frac{2}{q(1-\varepsilon)} \log \left(\frac{z^m-1}{z-1} \right), \log(z^2+z+1) \right\} (\log q + 10)^2 \\ &> -35.1 \max \left\{ \frac{2.1m}{q} \log z, 2.1 \log z \right\} (\log q + 10)^2 \\ &= -73.71(\log z) \max \{mq^{-1}, 1\} (\log q + 10)^2. \end{aligned}$$

On the other hand, we know

$$\log |A| < \log \left(\frac{24}{z^m} \right) = \log 24 - m \log z.$$

Combining this with the obtained lower bound for $\log |A|$, we have

$$\log 24 - m \log z > -73.71(\log z) \max \{mq^{-1}, 1\} (\log q + 10)^2,$$

or

$$m < 73.71 \max \{mq^{-1}, 1\} (\log q + 10)^2 + \frac{\log 24}{\log z}.$$

If $q \leq m$, then

$$q \left(1 - \frac{\log 24}{m \log z} \right) < 73.71(\log q + 10)^2,$$

which implies, say

$$q < 40,000.$$

If $q > m$, then

$$m < 73.71(\log q + 10)^2 + \frac{\log 24}{\log z}.$$

Since $z^m > y_1^q (= z^{m-1} + z^{m-2} + \dots + 1)$, we may replace the left-hand side above by

$$\frac{\log y_1}{\log z} q.$$

Then we have

$$\frac{\log y_1}{\log z} q < 73.71(\log q + 10)^2 + \frac{\log 24}{\log z}.$$

Hence,

$$q < 73.71 \frac{\log z}{\log y_1} (\log q + 10)^2 + \frac{\log 24}{\log y_1}.$$

So, we need an explicit upper estimate of z (or $\frac{\log z}{\log y_1}$) in terms of q , to bound q . But this is already done by Proposition 2.3. This completes the proof of our theorem. \square

REFERENCES

- [1] A. Baker, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, Quart. J. Math. Oxford, **15**, (1964), 375–383.
- [2] A. Baker, *Simultaneous rational approximations to certain algebraic numbers*, Proc. Cambridge Philos. Soc., **63**, (1967), 693–702.
- [3] M. A. Bennett, *Rational approximation to algebraic number of small height: The diophantine equation $|ax^n - by^n| = 1$* , J. Reine Angew. Math., **535**, (2001), 1–49.
- [4] M. A. Bennett and A. Levin, *The Nagell-Ljunggren equation via Runge's method*, Monatsh. Math., **177**, no. 1, (2015), 15–31.
- [5] Y. Bugeaud, *Linear forms in the logarithms of algebraic numbers close to 1 and applications to Diophantine equations*, In : Diophantine Equations, Tata Institute of Fundamental Research, Studies in Mathematics, Narosa Publishing House, 2008, 59–76.
- [6] Y. Bugeaud, M. Mignotte, *L'équation de Nagell-Ljunggren $(x^n - 1)/(x - 1) = y^q$* , L'Enseign. Math., **48** (2002), 147–168.
- [7] Y. Bugeaud, M. Mignotte, Y. Roy and T. N. Shorey, *The equation $(x^n - 1)/(x - 1) = y^q$ has no solution with x square*, Math. Proc. Cambridge Philos. Soc., **127**, (1999), 353–372.
- [8] Y. Bugeaud and P. Mihăilescu, *On the Nagell-Ljunggren equation $(x^n - 1)/(x - 1) = y^q$* , Math. Scand., **101**, (2007), 177–183.
- [9] N. Hirata-Kohno and T. N. Shorey, *On the Equation $(x^m - 1)/(x - 1) = y^q$ with x Power*, In: Analytic Number Theory, (ed. Y. Motohashi), London Math. Society Lecture Note Series, **247**, Cambridge Univ. Press, (1997), 119–125.
- [10] K. Inkeri, *On the diophantine the equation $(x^n - 1)/(x - 1) = y^m$* , Acta Arith., **21**, (1972), 299–311.
- [11] M. Laurent, M. Mignotte and Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory, **55**, (1995), 255–265.
- [12] W. Ljunggren, *Noen Setninger om ubestemte likninger av formen $\frac{x^n - 1}{x - 1} = y^q$* , Norsk. Mat. Tidsskr., **25**, (1943), 17–20.
- [13] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math., **572**, (2004), 167–195.
- [14] P. Mihăilescu, *New bounds and conditions for the equation of Nagell-Ljunggren*, J. Number Theory, **124**, (2007), 380–395.
- [15] T. Nagell, *Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$* , Norsk Mat. Forenings Skr. ser. 1 nr. 2 (1920), 14 pages.
- [16] T. Nagell, *Note sur l'équation indéterminée $\frac{x^n - 1}{x - 1} = y^q$* , Norsk. Mat. Tidsskr. 2 (1920), 75–78.
- [17] T. N. Shorey and Yu. Nesterenko, *Perfect powers in product of integers from a block of consecutive integers (II)*, Acta Arith., **76**, (1996), 191–198.
- [18] P. Philippon and M. Waldschmidt, *Formes linéaires de logarithmes sur les groupes algébriques commutatifs*, Illinois J. Math. **32**, (1988), 281–314.
- [19] T. N. Shorey, *On the equation $z^q = \frac{x^n - 1}{x - 1}$* , Indag. Math., **48**, (1986), 345–351.
- [20] T. N. Shorey, *Exponential Diophantine equations involving products of consecutive integers and related equations*, In: Number Theory, Hindustan Book Agency, (1999), 463–495.
- [21] T. N. Shorey and R. Tijdeman, *New Applications of Diophantine approximation to Diophantine equations*, Math. Scand., **39**, (1976), 5–18.
- [22] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Math., **87**, 1986, Cambridge Univ. Press.

Noriko Hirata-Kohno
Department of Math.
College of Science & Technology
Nihon University
Tokyo, Chiyoda
101-8308, Japan
hirata@math.cst.nihon-u.ac.jp

Tünde Kovács-Coskun
Donát Bánki Faculty
of Mechanical & Safety Engineering
Óbuda University
1081 Budapest
Hungary
kovacs.tunde@bgk.uni-obuda.hu

Takafumi Miyazaki
Faculty of Science & Technology
Div. of Pure and Applied Science
Gunma University
Tenjin-cho, Kiryu, Gunma
376-8518, Japan
tmiyazaki@gunma-u.ac.jp