Bull. Math. Soc. Sci. Math. Roumanie
Tome 57(105) No. 1, 2014, 35–43

A note on the Diophantine equation $(x^p - 1)/(x - 1) = p^e y^q$

by
Han Di and Guan Wenji

Abstract

Let p, q be odd primes, and let $e \in \{0, 1\}$. In this paper, using a lower bound for two logarithms in the complex case, we prove that if $p \equiv 3 \pmod 4$ and $q > 220p(\log p)^2$, then the equation $(x^p - 1)/(x - 1) = p^e y^q$ has no positive integer solution (x, y) with $\min\{x, y\} > 1$.

Key Words: Higher diophantine equation, Nagell-Ljunggren equation, Gel′fond-Baker method.
2010 Mathematics Subject Classification: Primary 11D41, Secondary 11D45.

1 Introduction

Let $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ be the sets of all integers, positive integers and rational numbers respectively. Let p, q be distinct odd primes, and let $e \in \{0, 1\}$. The equation

$$\frac{x^p - 1}{x - 1} = p^e y^q, x, y \in \mathbb{N}, \min\{x, y\} > 1 \tag{1.1}$$

is usually called the Nagell-Ljunggren equation. It is conjectured that (1.1) has no solution (x, y). This conjecture was proved for some special cases (see Problem D10 of [3] and its references). But, in general, the problem is far from solved.

In [2], Y. Bugeaud, G. Hanrot and M. Mignotte proved that if $p \not\equiv 1 \pmod 8$ and $q > 64000p(\log p)^2$, then (1.1) has no solution (x, y). In this paper, we give a substantial improvement of the constant for $p \equiv 3 \pmod 4$. More precisely, we prove the following result:

Theorem. If $p \equiv 3 \pmod 4$ and $q > 220p(\log p)^2$, then (1.1) has no solution (x, y).

2 Preliminaries

Let p be an odd prime. Further let $\zeta = e^{2\pi\sqrt{-1}/p}$, $m = (p - 1)/2$ and

$$S = \left\{ r \mid r \in \mathbb{N}, 1 \le r \le p - 1, \left(\frac{r}{p}\right) = 1 \right\},$$

$$\overline{S} = \left\{ \overline{r} \,|\overline{r} \in \mathbb{N}, 1 \leq \overline{r} \leq p-1, \left(\frac{\overline{r}}{p}\right) = -1 \right\}, \tag{2.1}$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol.

Lemma 2.1. ([1]). *Let a be a positive integer with $a > 1$. If $a \not\equiv 1 \pmod{p}$, then every prime divisor l of $(a^p-1)/(a-1)$ satisfies $l \equiv 1 \pmod{2p}$. If $a \equiv 1 \pmod{p}$, then $p \parallel (a^p-1)/(a-1)$ and every prime divisor l of $(a^p-1)/p(a-1)$ satisfies $l \equiv 1 \pmod{2p}$.*

Lemma 2.2. ([4, *Proposition 6.3.1 and Theorem 6.4.1*]). *For any integer k with $p \nmid k$, let*

$$G(k,p) = \sum_{i=0}^{p-1} \zeta^{ki^2}. \tag{2.2}$$

Then we have

$$G(k,p) = \left(\frac{k}{p}\right) \sqrt{(-1)^m p}.$$

Lemma 2.3. *If $p > 3$ and $p \equiv 3 \pmod 4$, then we have*

$$\frac{X^p-1}{X-1} = A^2(X) + pB^2(X), \tag{2.3}$$

where

$$A(X) = \sum_{i=0}^{m} \frac{a_i}{2} X^{m-i} \in \frac{1}{2}\mathbb{Z}[X],\ B(X) = \sum_{i=0}^{m} \frac{b_i}{2} X^{m-i} \in \frac{1}{2}\mathbb{Z}[X] \tag{2.4}$$

satisfy

$$A(X) + B(X)\sqrt{-p} = \prod_{r \in S} \left(X - \zeta^r\right),\ A(X) - B(X)\sqrt{-p} = \prod_{\overline{r} \in \overline{S}} \left(X - \zeta^{\overline{r}}\right) \tag{2.5}$$

and

$$a_0 = 2,\ a_m = -2,\ b_0 = b_m = 0,\ a_j = -a_{m-j},\ b_j = b_{m-j},\ j = 1,\ 2, \cdots, m-1. \tag{2.6}$$

Proof: This is the special case of Lemma 2 of [7] for $Y = 1$. □

Lemma 2.4. *If $p > 3$, $p \equiv 3 \pmod 4$ and X is an integer, then $A(X)$ and $B(X)$ are coprime integers.*

Proof: Since $p > 3$ and $p \equiv 3 \pmod 4$, m is an odd integer with $m > 1$. By Lemma 2.3, we see from (2.4) that

$$A(X) = (X^m - 1) + \sum_{j=1}^{(m-1)/2} \frac{a_j}{2}(X^{m-2j} - 1)X^j,$$

$$B(X) = \sum_{j=1}^{(m-1)/2} \frac{b_j}{2}(X^{m-2j}+1)X^j, \tag{2.7}$$

where a_j and b_j are integers for $j = 1, \cdots, (m-1)/2$. Since $(X^{m-2j} \pm 1)X^j$ is an even integer for any integer X, we see from (2.7) that $A(X)$ and $B(X)$ are integers.

Let $d = \gcd(A(X), B(X))$. Since $d^2 | (X^p - 1)/(X - 1)$ by (2.3), using Lemma 2.1, we have

$$\gcd(d, 2pX) = 1. \tag{2.8}$$

On the other hand, by (2.5), we get $X \equiv \zeta^r \pmod{d}$ and $X \equiv \zeta^{\bar{r}} \pmod{d}$, where $r \in S$ and $\bar{r} \in \bar{S}$. Since $r \neq \bar{r}$, it implies that the discriminant of $\mathbb{Q}(\zeta)$ is divisible by d, namely, $d| - p^{p-2}$. Therefore, by (2.8), we get $d = 1$. Thus, $A(X)$ and $B(X)$ are coprime integers. The lemma is proved. ∎

Lemma 2.5. *If* $p > 3$, $p \equiv 3 \pmod{4}$ *and* $X > 2p$, *then* $|B(X)| < X^{m-1}$.

Proof: Let

$$\prod_{r \in S}(X - \zeta^r) = X^m + \delta_1 X^{m-1} + \cdots + \delta_m. \tag{2.9}$$

By (2.4), (2.5) and (2.9), we have $\delta_m = -1$ and

$$\delta_k = \frac{1}{2}(a_k + b_k\sqrt{-p}),\ k = 1, \cdots, m-1. \tag{2.10}$$

Let

$$s_k = \sum_{r \in S} \zeta^{rk},\ k = 1, \cdots, m-1. \tag{2.11}$$

By Lemma 2.2, we see from (2.1), (2.2) and (2.11) that $1 + 2s_k = G(k, p)$ and

$$s_k = \frac{1}{2}\left(-1 + \left(\frac{k}{p}\right)\sqrt{-p}\right),\ k = 1, \cdots, m-1. \tag{2.12}$$

By the Newton formula between coefficients and roots of a polynomial, we get from (2.9) and (2.11) that

$$\delta_k = -\frac{1}{k}(s_k + \delta_1 s_{k-1} + \cdots + \delta_{k-1}s_1),\ k = 1, \cdots, m-1. \tag{2.13}$$

For $k = 1$, we have $\delta_1 = -s_1 = (1 - \sqrt{-p})/2$, and hence, $a_1 = 1$ and $b_1 = -1$ by (2.10). For $k > 1$, we now assume that

$$\max\{|a_j|, |b_j|\} \le p^{j-1},\ j = 1, \cdots, k-1. \tag{2.14}$$

By (2.10) and (2.12), we have

$$\begin{aligned} \delta_i s_{k-i} &= \tfrac{1}{4}\left(a_i + b_i\sqrt{-p}\right)\left(-1 + \left(\tfrac{k-i}{p}\right)\sqrt{-p}\right) \\ &= \tfrac{1}{4}\left(\left(-a_i - \left(\tfrac{k-i}{p}\right)b_i p\right) + \left(\left(\tfrac{k-i}{p}\right)a_i - b_i\right)\sqrt{-p}\right), \end{aligned} \tag{2.15}$$

$i = 1, \cdots, k-1$.
Therefore, by (2.10), (2.13) and (2.15), we get

$$2ka_k = 1 + \sum_{i=1}^{k-1} \left(-a_i - \left(\frac{k-i}{p} \right) b_i p \right), \ 2kb_k = \sum_{i=1}^{k-1} \left(\left(\frac{k-i}{p} \right) a_i - b_i \right). \tag{2.16}$$

Further, since $|\,((k-j)/p)\,| = 1$ for $j = 1, \cdots, k-1$, we obtain from (2.14) and (2.16) that

$$\begin{array}{l} |a_k| \le \frac{1}{2k} \left(1 + \sum\limits_{i=1}^{k-1} (|a_i| + |b_i| p) \right) \\ \le \frac{1}{2k} \left(1 + \left(1 + p + \cdots + p^{k-2} \right) + \left(p + p^2 + \cdots + p^{k-1} \right) \right) < p^{k-1}, \\ \\ |b_k| \le \frac{1}{2k} \left(1 + \sum\limits_{i=1}^{k-1} (|a_i| + |b_i|) \right) \\ \le \frac{1}{2k} \left(1 + 2 \left(1 + p + \cdots + p^{k-2} \right) \right) < p^{k-1}. \end{array} \tag{2.17}$$

By the inductive method, we find from (2.14) and (2.17) that

$$\max\{|a_k|, |b_k|\} \le p^{k-1}, \ k = 1, \cdots, m-1. \tag{2.18}$$

Thus, by (2.4), (2.6) and (2.18), if $X > 2p$, then

$$\begin{aligned} |B(X)| &\le \sum_{k=1}^{m-1} \frac{|b_k|}{2} X^{m-k} = X^{m-1} \sum_{k=1}^{m-1} \frac{|b_k|}{2X^{k-1}} \\ &\le X^{m-1} \sum_{k=1}^{m-1} \frac{p^{k-1}}{2(2p)^{k-1}} = X^{m-1} \sum_{k=1}^{m-1} \frac{1}{2^k} < X^{m-1}. \end{aligned}$$

The lemma is proved. □

Lemma 2.6. ([6, *Theorem* 3]) *Let* D, k *be positive integers such that* $D > 3, k > 1$ *and* $\gcd(k, 2D) = 1$. *Let* $h(-4D)$ *denote the class number of binary quadratic primitive forms of discriminant* $-4D$. *If* (X, Y, Z) *is a solution of the equation*

$$X^2 + DY^2 = k^Z, \quad X, Y, Z \in \mathbb{Z}, \ \gcd(X, Y) = 1, Z > 0, \tag{2.19}$$

then we have

$$Z = Z_1 t, \ t \in \mathbb{N}, \tag{2.20}$$

$$X + Y\sqrt{-D} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-D})^t, \lambda_1, \lambda_2 \in \{\pm 1\}, \tag{2.21}$$

where X_1, Y_1, Z_1 *are positive integers satisfying*

$$X_1^2 + DY_1^2 = k^{Z_1}, \gcd(X_1, Y_1) = 1, Z_1 \mid h(-4D). \tag{2.22}$$

Lemma 2.7. *For any odd prime p, we have $h(-4p) < p$.*

Proof: We can verify that the lemma holds for $p \le 17$. By Lemma 2 of [8], if $h(-4p) \ge p$, then

$$p \le h(-4p) < \frac{4}{\pi}\sqrt{p}\log(2e\sqrt{p}). \tag{2.23}$$

But, (2.23) is false for $p > 17$. Thus, the lemma is proved. □

Lemma 2.8. ([5, *Théorème* 3]) *Let α be a complex algebraic number such that $|\alpha| = 1$ and α is not a root of unity. Further let $h(\alpha)$ and $\log\alpha$ denote the absolute logarithmic height and the principal value of the logarithm of α respectively. Let $\Lambda = b_1\log\alpha - b_2\pi\sqrt{-1}$, where b_1, b_2 are positive integers. Then we have*

$$\log|\Lambda| \ge -8.87AH^2, \tag{2.24}$$

where

$$d = \frac{1}{2}[\mathbb{Q}(\alpha):\mathbb{Q}],\ A = \max\{20, 10.98|\log\alpha| + dh(\alpha)\},$$

$$H = \max\{17,\ \frac{\sqrt{d}}{10},\ d\log\left(\frac{b_1}{68.9} + \frac{b_2}{2A}\right) + 2.35d + 5.03\}. \tag{2.25}$$

Lemma 2.9. ([9, *Theorem* 1]) *If $q \ge (p-1)^2$, then (1.1) has no solution (x, y).*

3 Proof of Theorem

Let p, q be odd primes such that $p \equiv 3 \pmod 4$ and

$$q > 220p(\log p)^2. \tag{3.1}$$

Since $100p(\log p)^2 > (p-1)^2$ if $p < 8000$, by Lemma 2.9, the theorem holds for $p < 8000$. Therefore, it suffices to prove the theorem for

$$p > 8000. \tag{3.2}$$

We now assume that (1.1) has a solution (x, y). Then, by Lemma 2.1, we have $y \equiv 1 \pmod{2p}$ and

$$y \ge 2p + 1. \tag{3.3}$$

Further, since $q > p$ by (3.1), we get from (1.1) and (3.3) that $x^p > (x^p - 1)/(x-1) = p^e y^q \ge y^q > y^p \ge (2p+1)^p$. It implies that

$$x > 2p + 1. \tag{3.4}$$

We first consider the case that $e = 0$. Then, (1.1) can be written as

$$\frac{x^p - 1}{x - 1} = y^q. \tag{3.5}$$

Since $p > 3$ and $p \equiv 3 \pmod 4$, by Lemmas 2.3 and 2.4, we see from (3.5) that the equation

$$X^2 + pY^2 = y^Z,\ X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1, Z > 0 \tag{3.6}$$

has the solution

$$(X, Y, Z) = (A(x), B(x), q). \tag{3.7}$$

Since $e = 0$, by Lemma 2.1, we have $\gcd(y, 2p) = 1$. Therefore, applying Lemma 2.6 to (3.7), we get

$$q = Z_1 t,\ t \in \mathbb{N}, \tag{3.8}$$

$$A(x) + B(x)\sqrt{-p} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-p})^t,\ \lambda_1, \lambda_2 \in \{\pm 1\}, \tag{3.9}$$

where X_1, Y_1, Z_1 are positive integers satisfying

$$X_1^2 + pY_1^2 = y^{Z_1},\ \gcd(X_1, Y_1) = 1 \tag{3.10}$$

and

$$Z_1 \mid h(-4p). \tag{3.11}$$

Since q is an odd prime with $q > p$, by Lemma 2.7, we see from (3.8) and (3.11) that $Z_1 = 1$ and $t = q$. Therefore, by (3.9) and (3.10), we have

$$A(x) + B(x)\sqrt{-p} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-p})^q,\ \lambda_1, \lambda_2 \in \{\pm 1\}, \tag{3.12}$$

and

$$X_1^2 + pY_1^2 = y,\ \gcd(X_1, Y_1) = 1 \tag{3.13}$$

Let

$$\theta = X_1 + Y_1\sqrt{-p}\ , \overline{\theta} = X_1 - Y_1\sqrt{-p}. \tag{3.14}$$

By (3.12) and (3.14), we get

$$B(x) = \pm \frac{\theta^q - \overline{\theta}^q}{2\sqrt{-p}}\ . \tag{3.15}$$

Further let $\alpha = \theta/\overline{\theta}$. By (3.13) and (3.14), we have

$$|\theta| = |\overline{\theta}| = \sqrt{y} \tag{3.16}$$

and

$$y\alpha^2 - 2(X_1^2 - pY_1^2)\alpha + y = 0. \tag{3.17}$$

Therefore, we see from (3.3), (3.16) and (3.17) that α is a complex algebraic number such that $|\alpha| = 1, [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and α is not a root of unity.

By (3.15) and (3.16), we have

$$|B(x)| = \frac{|\overline{\theta}^q|}{2\sqrt{p}} |\alpha^q - 1| = \frac{y^{q/2}}{2\sqrt{p}} |\alpha^q - 1|. \tag{3.18}$$

Using Lemma 2.5, by (3.4), we have

$$|B(x)| < x^{(p-3)/2}\ . \tag{3.19}$$

On the other hand, by (3.5), we get $y^{q/2} > x^{(p-1)/2}$. Therefore, by (3.18) and (3.19), we obtain

$$\frac{2\sqrt{p}}{x} > |\alpha^q - 1|. \tag{3.20}$$

Using the maximum modulus principle, for any complex number z, we have either $|e^z - 1| \geq 1/2$ or $|e^z - 1| > 2|z - k\pi\sqrt{-1}|/\pi$ for some integers k. Therefore, by (3.20), we have either

$$\frac{2\sqrt{p}}{x} > \frac{1}{2} \tag{3.21}$$

or

$$\frac{\pi\sqrt{p}}{x} > |q\log\alpha - k\pi\sqrt{-1}|,\ k \in \mathbb{Z},\ |k| \leq q. \tag{3.22}$$

However, by (3.4), (3.21) is impossible. Thus, by (3.22), we get

$$\log(\pi\sqrt{p}) > \log x + \log|\Lambda|, \tag{3.23}$$

where

$$\Lambda = q\log\alpha - k\pi\sqrt{-1}. \tag{3.24}$$

Applying Lemma 2.8 to (3.24), Λ satisfies (2.24), where

$$A = \max\{20, 10.89|\log\alpha| + h(\alpha)\}, \tag{3.25}$$

$$H = \max\{17, \log\left(\frac{q}{68.9} + \frac{q}{2A}\right) + 7.38\}, \tag{3.26}$$

By (3.1), (3.2), (3.3), (3.16) and (3.17), we have $0 < |\log\alpha| \leq \pi, h(\alpha) = \log\sqrt{y}$, $40.69 < 10.98\pi + \log\sqrt{y}$ and $17 < 7.38 + \log(q/68.9)$. Hence, by (3.25) and (3.26), we get

$$6.20 < \log\sqrt{2p+1} \leq \log\sqrt{y} < A \leq 10.98\pi + \log\sqrt{y} \tag{3.27}$$

and

$$H \leq 7.38 + \log\left(\frac{q}{68.9} + \frac{q}{2A}\right) < 7.38 + \log\left(\frac{q}{68.9} + \frac{q}{81.38}\right) < 3.77 + \log q, \tag{3.28}$$

Since $x^p > (x^p - 1)/(x - 1) = y^q$, we have $p\log x > q\log y$. Substitute (2.24) into (3.23), we get

$$\log(\pi\sqrt{p}) + 8.87AH^2 > \log x > \frac{q}{p}\log y > 220(\log p)^2(\log y). \tag{3.29}$$

By (3.27), (3.28) and (3.29), we have

$$\frac{\log\pi + \frac{1}{2}\log p}{(\log p)^2(\log y)} + 8.87\left(\frac{10.98\pi + \frac{1}{2}\log y}{\log y}\right)\left(\frac{3.77 + \log q}{\log p}\right)^2 > 220. \tag{3.30}$$

By (3.2) and (3.3), we have

$$\frac{\log \pi + \frac{1}{2}\log p}{(\log p)^2(\log y)} < \frac{1}{(\log p)^2} < \frac{1}{(\log 8000)^2} < 0.02, \tag{3.31}$$

$$\frac{10.98\pi + \frac{1}{2}\log y}{\log y} = \frac{10.98\pi}{\log y} + \frac{1}{2} < \frac{10.98\pi}{\log 16000} + \frac{1}{2} < 4.07.$$

Using Lemma 2.9, we have $q < (p-1)^2$. It implies that

$$\frac{3.77 + \log q}{\log p} < \frac{3.77 + 2\log p}{\log p} < \frac{3.77}{\log 8000} + 2 < 2.42. \tag{3.32}$$

Thus, by (3.30), (3.31) and (3.32), we get $220 > 0.02 + 8.87 \times 4.07 \times (2.42)^2 > 220$, a contradiction.

We final consider the case that $e = 1$. Then, by Lemmas 2.3 and 2.4, we see from (1.1) and (2.3) that $p|A(x)$ and (3.6) has the solution.

$$(X, Y, Z) = \left(B(x), \frac{A(x)}{p}, q\right). \tag{3.33}$$

Therefore, by Lemmas 2.6 and 2.7, we get from (3.33)

$$|B(x)| = \frac{1}{2}|\theta^q + \overline{\theta}^q| = \frac{|\overline{\theta}^q|}{2}|\beta^q - 1| = \frac{y^{q/2}}{2}|\beta^q - 1|, \tag{3.34}$$

where $\beta = -\theta/\overline{\theta}, \theta$ and $\overline{\theta}$ are defined as in (3.14). Thus, using the same method as in the proof of the case that $e = 0$, we can deduce from (3.34) that (1.1) has no solution (x, y) for $e = 1$. The theorem is proved.

Acknowledgments

The authors would like to thank the referee for carefully examining this paper and providing a number of important comments.

References

[1] G. D. Birhoff, H. S. Vandiver, On the integral divisors of $a^n - b^n$, Ann. of Math. (2), 5 (1904), 173-180.

[2] Y. Bugeaud, G. Hanrot and M. Mignotte, Sur l′équation diophantienne $(x^n-1)/(x-1) = y^q$ III, Proc. London Math. Soc. 84 (2002), 59-78.

[3] R. K. Guy, Unsolved problems in number theory, 3rd ed., Springer Verlag, New York, 2004.

[4] K. Lreland and M. Rosen, A classical in introduction to modern number theory, Springer Verlag, New York, 1982.

[5] M. Laurent, M. Mignotte and Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d′interpolation J. Number Theory 55(1995), 285-321

[6] M. H. Le, Some exponential diophantine equations I: The equation $D_1x^2 - D_2y^2 = \lambda k^z$, J. Number Theory 55 (1995), 209-221.

[7] M. H. Le, On Cohn′s conjecture concerning the diophantine equation $x^2 + 2^m = y^n$, Arch. Math. 78 (2002), 26-35.

[8] M. H. Le, On the diophantine equation $y^x - x^y = z^2$, Rocky Mountain J. Math. 37 (2007), 1181-1185.

[9] P. Mihăilescu, New bounds and conditions for the equation of Nagell-Ljunggren, J. Number Theory 124 (2007), 380-395.

Received: 10.11.2012,

Revised: 11.07.2013,

Accepted: 02.08.2013.

Mathematical and Information Department
Weinan Teacher's University,
Weinan, Shaanxi, P.R.China
E-mail: `guanwenji-2003@yahoo.com.cn`

Department of Mathematics,
Northwest University,
Xi'an, Shaanxi, P.R.China
E-mail: `handi515@163.com`