Publ. Math. Debrecen
82/2 (2013), 373–378
DOI: 10.5486/PMD.2013.5328

On the Diophantine equation $cy^l = \frac{x^p-1}{x-1}$

By MOHAMMAD SADEK (Cairo)

Abstract. Let p, c be distinct odd primes, and $l \geq 2$ an integer. We find sufficient conditions for the Diophantine equation

$$cy^l = \Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

not to have integer solutions.

1. Introduction

The solutions of the Nagell–Ljunggren equation $y^q = \frac{x^n-1}{x-1}$, where $q, n \geq 2$ are integers, have been the source for many conjectures. One of these is the following:

Conjecture 1.1. *The only solutions to the Diophantine equation $y^q = \frac{x^n-1}{x-1}$ in integers $x, y > 1$, $n > 2$, $q \geq 2$ are given by*

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

The above conjecture has been solved completely for $q = 2$. Furthermore, it has been proved if one of the following assumptions holds:

$$3 \mid n, \text{ or } 4 \mid n, \text{ or } q = 3 \text{ and } n \not\equiv 5 \mod 6.$$

Mathematics Subject Classification: 11D61.
Key words and phrases: Diophantine equations, Ljunggren–Nagell equation, cyclotomic polynomials.

We moreover know that the Nagell–Ljunggren equation has no solutions with x square. The main tools used to attack this Diophantine equation are effective Diophantine approximation, linear forms in p-adic logarithms, and Cyclotomic fields theory. For these results and more see [1], [5] and [6].

In [3] the Diophantine equation $y^l = c\frac{x^n-1}{x-1}$ has been treated. A complete list of such Diophantine equations with integer solutions has been given, under the condition that $1 \le c \le x \le 100$. A more general equation $a\frac{x^n-1}{x-1} = cy^l$ where $ac > 1$ has been considered in [7]. Our interest in the latter equation is when $a = 1$.

In this note we will be concerned with the Diophantine equation $cy^l = \frac{x^p-1}{x-1}$, where c, p are distinct odd primes and $l \ge 2$. We exhibit the existence of an infinite set of triples (p, c, l) for which the mentioned Diophantine equation has no integer solutions. For example, this infinite set contains the set of triples (p, c, l) where the Legendre symbol $\left(\frac{c}{p}\right) = -1$ and l is even.

The key idea is exploiting the following identity satisfied by the cyclotomic polynomial $\Phi_p(x) = \frac{x^p-1}{x-1}$

$$4\Phi_p(x) = A_p(x)^2 - (-1)^{(p-1)/2} p B_p(x)^2,$$

where $A_p(x), B_p(x) \in \mathbb{Z}[x]$. This identity goes back to Gauss, nevertheless the formulae describing $A_p(x)$ and $B_p(x)$ were given recently in [2]. Using this identity we show that the existence of an integer solution to the equation in question implies the existence of a proper integer solution to some auxiliary Diophantine equation.

2. Factorization of cyclotomic polynomials

For an odd square-free integer $n > 1$, and $|x| \le 1$ define

$$f_n(x) = \sum_{j=1}^{\infty} \left(\frac{j}{n}\right) \frac{x^j}{j},$$

where $\left(\frac{j}{n}\right)$ is the Jacobi symbol of j mod n. We state Theorem 1 of [2].

Theorem 2.1. *Let $n > 3$ be an odd square-free integer. Consider the Gauss's identity $4\Phi_n(x) = A_n(x)^2 - (-1)^{(n-1)/2} n B_n(x)^2$, where $A_n(x), B_n(x) \in \mathbb{Z}[x]$. If $n \equiv 1 \mod 4$, then*

$$A_n(x) = 2\sqrt{\Phi_n(x)} \cosh\left(\frac{\sqrt{n}}{2} f_n(x)\right), \quad B_n(x) = 2\sqrt{\frac{\Phi_n(x)}{n}} \sinh\left(\frac{\sqrt{n}}{2} f_n(x)\right).$$

If $n \equiv 3$ mod 4, then

$$A_n(x) = 2\sqrt{\Phi_n(x)}\cos\left(\frac{\sqrt{n}}{2}f_n(x)\right), \quad B_n(x) = 2\sqrt{\frac{\Phi_n(x)}{n}}\sin\left(\frac{\sqrt{n}}{2}f_n(x)\right).$$

3. An auxiliary Diophantine equation

The results of this section are motivated by Proposition 8.1 of [4].

By a proper solution (x_0, y_0, z_0) to the Diophantine equation $ax^p+by^q = cz^r$, we mean three integers x_0, y_0, z_0 such that $ax_0^p+by_0^q = cz_0^r$ and $\gcd(x_0, y_0, z_0) = 1$.

We state the following result on local solutions to $cy^l = x^2 \pm pz^2$ where c, p are distinct odd primes and $l \geq 2$.

Proposition 3.1. *There are proper local solutions to*

$$\alpha^2 cy^l = x^2 \pm pz^2, \quad \alpha \in \{1, 2\},$$

at every prime if and only if the Legendre symbol $\left(\frac{\mp p}{c}\right) = 1$*; and, when l is even we have* $\left(\frac{c}{p}\right) = 1$.

Proof. The given conditions are clearly necessary. Now we need to prove they are sufficient. We use the fact that if $q \nmid 2cp$, then there are q-adic integer solutions to $x^2 \pm pz^2 = \alpha^2 c$, so take $(x, 1, z)$. For the prime c, since $\left(\frac{\mp p}{c}\right) = 1$, there are c-adic integer solutions to $x^2 = \mp p$, so take $(x, 0, 1)$. For the prime p, if l is odd, take $(\alpha c^{(l+1)/2}, c, 0)$; if l is even, hence $\left(\frac{c}{p}\right) = 1$, then there is a p-adic integer satisfying $x^2 = \alpha^2 c$, and we take $(x, 1, 0)$. For the prime 2, the equation becomes $x^2 - z^2 = \alpha^2 y^l$, so we can lift the solution $(1, 0, 1)$ mod 2 to a 2-adic integer solution. □

Proposition 3.2. *Let p, c be distinct odd primes, and $l \geq 2$ be an integer. Set $\delta = (-1)^{(p-1)/2}$. If the Diophantine equation*

$$\alpha^2 cy^l = x^2 - \delta pz^2, \quad \alpha \in \{1, 2\},$$

has a proper solution with y being odd and $\gcd(x, y) = 1$, then there exist coprime ideals I, J in $\mathbb{Q}(\sqrt{\delta p})$ with $IJ = (\alpha^2 c)$, whose ideal classes are l-th powers inside the class group of $\mathbb{Q}(\sqrt{\delta p})$.

Proof. Suppose (x, y, z) is a proper solution to $\alpha^2 cy^l = x^2 - \delta pz^2$ where y is odd and $\gcd(x, z) = 1$. Now considering the latter as ideal equation, we have

$$(\alpha^2 c)(y)^l = \left(x - \sqrt{\delta p}\, z\right)\left(x + \sqrt{\delta p}\, z\right).$$

Now the ideal $\mathfrak{a} = \left(x - \sqrt{\delta p}\, z, x + \sqrt{\delta p}\, z\right) \mid \left(2x, 2\sqrt{\delta p}, \alpha^2 cy^l\right) = (2, \alpha)$.

1) If $\alpha = 1$, then

$$\left(x - \sqrt{\delta p}\, z\right) = IL_1^l, \ \left(x + \sqrt{\delta p}\, z\right) = JL_2^l,$$

where $IJ = (c)$ and $L_1L_2 = (y)$. This implies that the ideal classes of I and J are both l-th powers inside the class group of $\mathbb{Q}(\sqrt{\delta p}\,)$.

2) If $\alpha = 2$, then both x, z are odd. This will yield a contradiction when $p \equiv \pm 1 \mod 8$. This follows from the fact that $4cy^l = x^2 - \delta p z^2 \equiv 0 \mod 8$ when $p \equiv \pm 1 \mod 8$.
When $p \equiv \pm 5 \mod 8$, the ideal (2) is prime inside $\mathbb{Q}(\sqrt{\delta p}\,)$ because $\delta p \equiv 5 \mod 8$. If $\mathfrak{a} = (2)$, then $2 \mid (x - \sqrt{\delta p} z)$ which implies that $2 \mid x, z$, a contradiction. Thus $\mathfrak{a} = 1$, and we argue like in the first case. □

4. The equation $cy^l = \frac{x^p - 1}{x - 1}$

We start by stating the following elementary lemma.

Lemma 4.1. *Let $a \in \mathbb{Z}$ and p be an odd prime.*

i) $\Phi_p(a)$ *is odd.*

ii) *Set* $d = \gcd(A_p(a), B_p(a))$. *Then* $d \in \{1, 2\}$. *If* $p \equiv \pm 1 \mod 8$, *then* $d = 2$.

Proof. i) Since $\Phi_p(a) \equiv 1 \mod a$, hence if a is even, $\Phi_p(a)$ is odd. If a is odd, then $\Phi_p(a) \equiv \Phi(1) = p \mod 2$.

ii) Assume that $q \mid d$, where $q > 1$ is an odd prime. We will write $\tilde{a}$ for the reduction of $a \mod q$.

If $q \neq p$, then $(x - \tilde{a}) \mid A_p(x),\ B_p(x) \mod q$ because $q \mid A_p(a)$ and $B_p(a)$. Hence $(x - \tilde{a})^2 \mid \Phi_p(x) \mod q$. The latter statement contradicts the fact that $x^p - 1$ has no multiple factors mod q when $\gcd(q, p) = 1$.

If $q = p$, then $p^2 \mid \Phi_p(a)$. In particular $\tilde{a}^p \equiv 1 \mod p$. Fermat's Little Theorem yields that there is a $\lambda \in \mathbb{Z}$ such that $a = 1 + \lambda p$. So

$$\Phi_p(a) = \sum_{i=0}^{p-1} a^i = \sum_{i=0}^{p-1} (1 + \lambda p)^i \equiv p + \lambda p \sum_{i=0}^{p-1} i \equiv p \mod p^2,$$

which contradicts that $p^2 \mid \Phi_p(a)$. We conclude that $d \mid 2$.

Now we assume $p \equiv \pm 1$ mod 8. Assume on the contrary that $2 \nmid d$. This implies that both $A_p(a)$ and $B_p(a)$ are odd as $4 \mid A_p^2(a) - (-1)^{(p-1)/2} p B_p^2(a)$. A direct calculation shows that if $A_p(a)$, $B_p(a)$ are both odd, then

$$4\Phi_p(a) = A_p^2(a) - (-1)^{(p-1)/2} p B_p^2(a) \equiv 1 - (-1)^{(p-1)/2} p \equiv 0 \mod 8,$$

which contradicts (i). □

Corollary 4.2. *Let p, c be distinct odd primes. Let $l \geq 2$ be an integer. Assume that (a, b) is an integer solution to the Diophantine equation $cy^l = \Phi_p(x)$. Then there exists an integer solution (x, y, z), where $\gcd(x, z) = 1$ and y is odd, to a Diophantine equation of the form*

$$\alpha^2 cy^l = x^2 - (-1)^{(p-1)/2} pz^2, \quad \alpha \in \{1, 2\}.$$

In the case $p \equiv \pm 1 \mod 8$, one has $\alpha = 1$.

Proof. One has $4c\,b^l = 4\Phi_p(a) = A_p(a)^2 - (-1)^{(p-1)/2} pB_p(a)^2$, where $A_p(x), B_p(x) \in \mathbb{Z}[x]$ and $d = \gcd(A_p(a), B_p(a)) \mid 2$, Lemma 4.1. If $d = 1$, then $(A_p(a), b, B_p(a))$ is a proper solution to $4cy^l = x^2 - (-1)^{(p-1)/2} z^2$. If $d = 2$, then $(A_p(a)/2, b, B_p(a)/2)$ is a proper solution to $cy^l = x^2 - (-1)^{(p-1)/2} z^2$. Observe that if $p \equiv \pm 1 \mod 8$, then $d = 2$, Lemma 4.1 (ii). $\square$

Now we state our main result which says that there is an infinite number of triples (c, p, l) such that $cy^l = \Phi_p(x)$ has no integer solution.

Theorem 4.3. *Let p, c be distinct odd primes, and $l \geq 2$ an integer. Set $\delta = (-1)^{(p-1)/2}$. If the triple (p, c, l) satisfies one of the following conditions:*

i) $\left(\frac{\delta p}{c}\right) = -1$;

ii) $\left(\frac{c}{p}\right) = -1$, *and l is even;*

iii) *There exist no ideals I, J whose ideal classes are l-th powers in the class group of $\mathbb{Q}(\sqrt{\delta p})$ and satisfy $(\alpha^2 c) = IJ$, where*

$$\alpha \in \begin{cases} \{1\} & \text{if } p \equiv \pm 1 \mod 8 \\ \{1, 2\} & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$$

then the Diophantine equation

$$cy^l = \Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

has no integer solutions.

Proof. Assume on the contrary that there exists a proper integer solution to $cy^l = \Phi_p(x)$. This implies the existence of a proper integer solution to $\alpha^2 cy^l = x^2 - \delta pz^2$, see Corollary 4.2. Hence we have a contradiction in (i) and (ii), see Proposition 3.1. Furthermore one has a contradiction in case (iii) obtained using Proposition 3.2. $\square$

Parts (i) and (ii) of the above theorem provide an infinite family of Diophantine equations with no integer solutions. For example

$$13y^{2l} = \Phi_{137}(x) = x^{136} + \cdots + x + 1$$

has no integer solutions because $\left(\frac{13}{137}\right) = -1$.

In the following example we show that (iii) of Theorem 4.3 can be used to find explicit triples (c, l, p) such that the Diophantine equation $cy^l = \Phi_p(x)$ has no integer solutions.

Example 4.4. The Diophantine equation

$$3y^{5k} = \Phi_{47}(x) = x^{46} + x^{45} + \cdots + x + 1, \quad k \geq 1,$$

has no integer solutions. We have $47 \equiv -1 \mod 8$ and $(3) = \mathfrak{p}\mathfrak{p}'$ in the ring of integers of $\mathbb{Q}(\sqrt{-47})$. The class number of $\mathbb{Q}(\sqrt{-47})$ is 5. The ideal class $[\mathfrak{p}]$ of $\mathfrak{p}$ can not be a fifth power inside the ideal class group of $\mathbb{Q}(\sqrt{-47})$ because $[\mathfrak{p}]$ generates the ideal class group.

References

[1] Y. Begeaud, M. Mignotte, Y. Roy and T. Shorey, The equation $\frac{x^n-1}{x-1} = y^q$ has no solution with x square, *Math. Proc. Camb. Phil. Soc.* (*to appear*).

[2] R. Brent, On computing factors of cyclotomic polynomials, *Math. Comp.* **61**(203) (1993), 131–149.

[3] Y. Bugeaud, On the Diophantine equation $a\frac{x^n-1}{x-1} = y^q$, in: *Number Theory conference held in Turku, De Gruyter*, 19–24, 2001.

[4] Henri Darmon and Andrew Granville, On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$, *Bull. London Math. Soc.* **27** (1995), 513–543.

[5] P. Mihailescu, Class number conditions for the diagonal case of of the equation of Nagell–Ljunggren, *preprint.*

[6] P. Mihailescu, New bounds and conditions for the equation of Nagell-Ljunggren, *J. Number Theory* **124**(2) (2007), 380–395.

[7] T. N. Shorey, The equation $a\frac{x^n-1}{x-1} = by^q$ with $ab > 1$, Number Theory in Progress, Vol. 1, *Walter de Gruyter, Berlin*, 1999.

MOHAMMAD SADEK
DEPARTMENT OF MATHEMATICS
AND ACTUARIAL SCIENCES
AMERICAN UNIVERSITY IN CAIRO

E-mail: mmsadek@aucegypt.edu

(Received September 9, 2011; revised May 9, 2012)