ON THE DIOPHANTINE EQUATION $x^2 + 7^{2k} = y^n$

Florian Luca
Instituto de Matemáticas UNAM, Campus Morelia Apartado Postal 27-3 (Xangari),
C.P. 58089, Morelia, Michoacán, Mexico
e-mail: fluca@matmor.unam.mx

Alain Togbé
Mathematics Department, Purdue University North Central, 1401 S, U.S. 421, Westville IN 46391
e-mail: atogbe@pnc.edu

(Submitted January 2007)

ABSTRACT

In this note, we find all the solutions of the Diophantine equation $x^2 + 7^{2k} = y^n$, $x \geq 1$, $y \geq 1$, $k \in \mathbb{N}, n \geq 3$.

1. INTRODUCTION

The history of the Diophantine equation

$$x^2 + C = y^n, \;\; x \geq 1, \;\; y \geq 1, \;\; n \geq 3,$$

is very rich. In 1850, Lebesgue [13] was the first to obtain a non-trivial result. He proved that the above equation has no solutions when $C = 1$. In 1965, Chao Ko [10] proved that the only solution of the above equation with $C = -1$ is $x = 3$, $y = 2$. J. H. E. Cohn [9] solved the above equation for several values of the parameter C in the range $1 \leq C \leq 100$. A couple of the remaining values of C in the above range were covered by Mignotte and De Weger in]17], and the rest in the recent paper [6]. See also [7].

Recently, several authors become interested in the case when C is positive and only the prime factors of C are specified. For example, the case when $C = p^k$, where p is a prime number, was dealt with in [1] and [12] for $p = 2$, in [2], [3] and [14] for $p = 3$, in [18] for $p = 5$ and k odd. Partial results for a general prime p appear in [4] and [11]. All the solutions when x and y are coprime and $C = 2^a \cdot 3^b$ were found in [15]. See also the recent survey [19].

Here, we consider the case $p = 7$ and the following equation

$$x^2 + 7^{2k} = y^n, \;\; x \geq 1, \;\; y \geq 1, \;\; k \geq 1, \;\; n \geq 3. \tag{1.1}$$

Our main result is the following.

Theorem 1.1: *All solutions of equation* (1.1) *are:*
$n = 3$ $\quad (x, y, k) = (524 \cdot 7^{3\lambda}, 65 \cdot 7^{2\lambda}, 1 + 3\lambda)$,
$n = 4$ $\quad (x, y, k) = (24 \cdot 7^{2\lambda}, 5 \cdot 7^{\lambda}, 1 + 2\lambda)$, *where* $\lambda \geq 0$ *is any integer.*

2. REDUCTION TO PRIMITIVE SOLUTIONS

Here, we show that it suffices to study equation (1.1) when $\gcd(x, y) = 1$. We call such solutions *primitive*. Assume that (x, y, k, n) is a non-primitive solution. Then $7 \mid x$. Write

$x = 7^a x_1$ with $a \geq 1$ and $7 \nmid x_1$. Clearly $7 \mid y$ so we may write $y = 7^b y_1$ with some $b \geq 1$ and $7 \nmid y_1$. So equation (1.1) becomes

$$7^{2a} x_1^2 + 7^{2k} = 7^{nb} y_1^n. \tag{2.1}$$

By looking at the exponents of 7 and keeping in mind -1 is not a quadratic residue modulo 7, we have that either $2k = nb \leq 2a$ or $2a = nb < 2k$. The first instance leads to

$$X^2 + 1 = Y^n,$$

where $X = 7^{a-k} x_1$ and $Y = y_1$, which has no solution by Lebesgue's result, while the second instance leads to

$$X^2 + 7^{2k_1} = Y^n,$$

where $X = x_1,\ Y = y_1$ and $2k_1 = 2k - 2a = 2k - nb$. Note that (X, Y, k_1, n) is a solution of the original equation (1.1) which is furthermore primitive. Assume that we have showed that the only primitive solutions of equation (1.1) are $(x, y, k, n) = (524, 65, 1, 3)$ and $(24, 5, 1, 4)$. If $(x_1, y_1, k_1, n) = (524, 65, 1, 3)$, then $2k = 2 + 2a = 2 + 3b$, which shows that $a = 3\lambda$ and $b = 2\lambda$ for some positive integer λ. Hence, $(x, y, k, n) = (7^a x_1, 7^b y_1, 1 + 3\lambda, 3) = (524 \cdot 7^{3\lambda}, 65 \cdot 7^{2\lambda}, 1 + 3\lambda, 3)$. If on the other hand $(x_1, y_1, k, n) = (24, 5, 1, 4)$, then $2k = 2 + 2a = 2 + 4b$, therefore $b = \lambda$ and $a = 2\lambda$. Thus, $(x, y, k, n) = (24 \cdot 7^{2\lambda}, 5 \cdot 7^{\lambda}, 1 + 2\lambda, 4)$.

It remains to prove that the only primitive solutions are indeed $(x, y, k, n) = (524, 65, 1, 3)$ and $(24, 5, 1, 4)$.

3. THE CASE WHEN $n = 3$

Here, we obtain the following result.

Lemma 3.1: *The only primitive solution of* (1.1) *with* $n = 3$ *is* $(x, y, k) = (524, 65, 1)$.

Proof: We factor our equation in $\mathbb{Z}[i]$ obtaining

$$\left(x + i7^k\right)\left(x - i7^k\right) = y^3. \tag{3.1}$$

Since x and y are coprime and $7^{2k} \equiv 1 \pmod 4$, we get that x is even (otherwise $x^2 + 7^{2k}$ is a multiple of 2 but not of 4). This implies that $x + 7^k i$ and $x - 7^k i$ are coprime in $\mathbb{Z}[i]$ which is a UFD. Since $n = 3$ and the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$ of multiplicative orders dividing 4 (hence, coprime to 3), we get that the relations

$$\begin{cases} x + i7^k = (u + iv)^3 \\ x - i7^k = (u - iv)^3 \end{cases} \tag{3.2}$$

hold with some integers u and v. Eliminating x from the two equations (3.2), we get

$$2i7^k = (u + iv)^3 - (u - iv)^3, \tag{3.3}$$

which is the same as $7^k = v(3u^2 - v^2)$. Note that u and v are coprime since otherwise any prime factor common to both u and v will also divide both x and y which is impossible. The only possibilities are therefore $v = \pm 1$ or $v = \pm 7^k$, which lead to the equations

$$3u^2 = 1 \pm 7^k, \tag{3.4}$$

$$3u^2 = \pm 1 + 7^{2k}, \tag{3.5}$$

respectively. The first equation is impossible because if the sign is $-$, then the right hand side is negative while the right hand side is positive, while if the sign is $+$, then the right hand side is congruent to 2 modulo 3 while the left hand side is divisible by 3. For the second equation, considerations modulo 3 show that the sign must be -1. Thus, $(7^k)^2 - 3u^2 = 1$. The Pell equation $X^2 - 3Y^2 = \pm 1$ has the smallest solution $(X_1, Y_1) = (2, 1)$ and the second solution is $(X_2, Y_2) = (7, 4)$. The sequence $(X_m)_{m \geq 1}$ is a Lucas sequence of the second type. By the Primitive Divisor Theorem of Carmichael [8], it follows that if $m > 12$, then X_m has a prime factor $p \equiv \pm 1 \pmod{m}$. In particular, X_m cannot be a power of 7 if $m > 12$. One can now check by hand that the only $m \leq 12$ such that X_m is a power of 7 is $m = 2$. This leads to the solution $u = 4,\ v = \pm 7,\ k = 1$, therefore to $(x, y, k) = (524, 65, 1)$.

At this point, we consider it worthwhile to point out that in fact, all solutions of equations (3.4) and (3.5) have been computed by De Weger in his Ph.D. thesis [20]. Namely, we multiply each of the two equations by 3 to get an equation of the form $Z^2 = X + Y$, where both X and Y are S-units for the set of primes $\{2, 3, 5, 7\}$ (i.e., are integers whose prime factors lie in the above set) and such that $\gcd(X, Y)$ is square-free. But all such solutions appear in Table 1, pages 171–174 in [20]. A careful analysis of that table reveals that the only solutions when X and Y are ± 3 and $\pm 3 \cdot 7^\alpha$ for some positive integer α are the ones mentioned above.

This completes the proof of Lemma 3.1. □

4. THE CASE WHEN $n = 4$

We have the following result.

Lemma 4.1: *The only primitive solution of equation* (1.1) *with* $n = 4$ *is* $(x, y, k) = (24, 5, 1)$.

Proof: Now we rewrite equation (1.1) as

$$7^{2k} = \left(y^2 + x\right)\left(y^2 - x\right). \tag{4.1}$$

Since x is even and y is odd, we have that $y^2 + x$ and $y^2 - x$ are coprime. Thus,

$$\begin{cases} y^2 - x &= 1, \\ y^2 + x &= 7^{2k}, \end{cases} \tag{4.2}$$

which leads to

$$\left(7^k\right)^2 - 2y^2 = -1. \tag{4.3}$$

The above equation can be handled in two ways. The first way is to notice that the above equation gives a solution (X, Y) to the Pell equation $X^2 - 2Y^2 = \pm 1$ with $X = 7^k$. The first solution of the above equation is $(X_1, Y_1) = (1, 1)$. Further, $X_2 = 3$ and $X_3 = 7$. By checking X_m for all $m \leq 12$ and invoking the Primitive Divisor Theorem as we did in the case $n = 3$, we get that the only m such that $X_m = 7^k$ is $m = 3$ which gives $k = 1$. This leads to $y = 5$ and $x = 24$, which is the desired solution. The second way is to rewrite it as

$$Z^2 := (2y)^2 = 2 \cdot 7^{2k} + 2 := X + Y,$$

and invoke again De Weger's table. This concludes the proof. $\square$

5. THE REMAINING CASES

If (x, y, k, n) is a primitive solution to our original equation (1.1) and $d > 2$ is a divisor of n, then $(x, y^{n/d}, k, d)$ is also a primitive solution of (1.1). The cases when $d = 3$ or $d = 4$ have been handled by the results from Sections 3 and 4. Since $n \geq 3$ is coprime to 3 and not a multiple of 4, it follows that there exists a prime $p \geq 5$ dividing n. We may certainly replace n by this prime, and hence assume that $n = p \geq 5$ is prime. We look again at the equation

$$(x + i7^k)(x - i7^k) = y^p.$$

Since x is even and y is odd, we get that $x + 7^k i$ and $x - 7^k i$ are coprime in $\mathbb{Z}[i]$. Since p is odd and the units of $\mathbb{Z}[i]$ have orders dividing 4, we get that there exist integers u and v such that if we put $\alpha = u + iv$, then

$$\begin{cases} x + i7^k = \alpha^p; \\ x - i7^k = \overline{\alpha}^p. \end{cases} \tag{5.1}$$

The above equations lead to

$$\frac{7^k}{v} = \frac{\alpha^p - \bar{\alpha}^p}{\alpha - \bar{\alpha}} \in \mathbb{Z}.$$

The sequence $\{u_n\}_{n\geq 0}$ of general term $u_n = (\alpha^n - \bar{\alpha}^n)/(\alpha - \bar{\alpha})$ for all $n \geq 0$ is a Lucas sequence of integers. By the extension of the Primitive Divisor Theorem of Carmichael to Lucas sequences with complex conjugated roots by Bilu, Hanrot and Voutier [5], we know that if $p > 30$ is a prime, then u_p must have a prime factor $q \equiv \pm 1 \pmod{p}$. In particular, u_p cannot be a power of 7 for such primes p. When $p \in [5, 29]$, since u_p is a power of 7, we get that u_p is lacking primitive divisors. There are only finitely many possibilities for the pair (p, u_p) and all such instances appear in Table 1 in the paper [5]. A quick inspection of that table reveals that there exists no *defective* (i.e., without primitive divisors) Lucas number u_p whose roots α and $\overline{\alpha}$ are in $\mathbb{Z}[i]$. Thus, there are no more primitive solutions to our original equation.

ACKNOWLEDGMENTS

We thank the referee for comments which improved the quality of the paper. Work by the first author was done while he visited the Mathematics and Statistics Department of the Williams College. He thanks this Institution for its hospitality. The second author was partially supported by Purdue University North Central.

REFERENCES

[1] S. A. Arif and F. S. A. Muriefah. "On the Diophantine Equation $x^2 + 2^k = y^n$." *Internat. J. Math. Math. Sci.* **20.2** (1997): 299–304.

[2] S. A. Arif and F. S. A. Muriefah. "The Diophantine Equation $x^2 + 3^m = y^n$." *Internat. J. Math. Math. Sci.* **21** (1998): 619–620.

[3] S. A. Arief and F. S. A. Muriefah. "On a Diophantine Equation." *Bull. Austral. Math. Soc.* **57** (1998): 189–198.

[4] S. A. Arif and F. S. A. Muriefah. "On the Diophantine equation $x^2 + q^{2k+1} = y^n$." *J. Number Theory* **95.1** (2002): 95–100.

[5] Yu. Bilu, G. Hanrot and P. M. Voutier. "Existence of Primitive Divisors of Lucas and Lehmer Numbers. With an appendix by M. Mignotte." *J. Reine Angew. Math.* **539** (2001): 75–122.

[6] Y. Bugeaud, M. Mignotte and S. Siksek. "Classical and Modular Approaches to Exponential Diophantine Equations. II. The Lebesgue-Nagell Equation." *Compos. Math.* **142.1** (2006): 31–62.

[7] Y. Bugeaud and T. N. Shorey. "On the Number of Solutions of the Generalized Ramanujan-Nagell Equation." *J. Reine Angew. Math.* **539** (2001): 55–74.

[8] R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \beta^n$." *Ann. Math.* **15** (1913): 30–70.

[9] J. H. E. Cohn. "The Diophantine Equation $x^2 + c = y^n$." *Acta Arith.* **65** (1993): 367–381.

[10] C. Ko. "On the Diophantine Equation $x^2 = y^n + 1$, $xy \neq 0$." *Sci. Sinica* **14** (1965): 457–460.

[11] M. Le. "An Exponential Diophantine Equation." *Bull. Austral. Math. Soc.* **64.1** (2001): 99–105.

[12] M. Le. "On Cohn's Conjecture Concerning the Diophantine Equation $x^2 + 2^m = y^n$." *Arch. Math.* (Basel) **78.1** (2002): 26–35.

[13] V. A. Lebesgue. "Sur l'Impossibilité en Nombres Entiers de l'Équation $x^m = y^2 + 1$." *Nouv. Annal. des Math.* **9** (1850): 178–181.

[14] F. Luca. "On a Diophantine Equation." *Bull. Austral. Math. Soc.* **61** (2000): 241–246.

[15] F. Luca. "On the Equation $x^2 + 2^a 3^b = y^n$." *Int. J. Math. Math. Sci.* **29.4** (2002): 239–244.

[16] F. Luca and A. Togbé. "On the Diophantine Equation $x^2 + 2^a 5^b = y^n$." *Internat. J. Number Theory*, to appear.

[17] M. Mignotte and B. M. M. de Weger. "On the Diophantine Equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$." *Glasgow Math. J.* **38.1** (1996): 77–85.

[18] F. S. A. Muriefah and S. A. Arif. "The Diophantine Equation $x^2 + 5^{2k+1} = y^n$." *Indian J. Pure Appl. Math.* **30.3** (1999): 229–231.

[19] F. S. A. Muriefah and Y. Bugeaud. "The Diophantine Equation $x^2 + c = y^2$: A Brief Overview." *Rev. Colombiana Math.*, to appear.

[20] B. M. M. de Weger, *Algorithms for Diophantine Equations,* CWI Tract **65**, CWI Amsterdam, 1989.

AMS Classification Numbers: 11D61, 11Y50

✠ ✠ ✠