

## ON THE DIOPHANTINE EQUATION $x^2 = 4q^m - 4q^n + 1$

FLORIAN LUCA

(Communicated by David E. Rohrlich)

ABSTRACT. In this note, we find all positive integer solutions  $(x, q, m, n)$  of the diophantine equation from the title with  $q$  a prime power.

In this note, we study the diophantine equation

$$(1) \quad x^2 = 4q^m - 4q^n + 1$$

in integer unknowns  $(x, q, m, n)$ , with  $x > 0$ ,  $m \geq n \geq 0$ ,  $(m, n) \neq (1, 0)$ , and  $q$  a prime power. We exclude the pair  $(m, n) = (1, 0)$ , because in this case equation (1) reduces to

$$(2) \quad q = \frac{x^2 + 3}{4}.$$

Since  $x$  is odd, we may write  $x = 2t + 1$  for some positive integer  $t$ , and we get that equation (2) is equivalent to finding all solutions of the diophantine equation

$$(3) \quad q = t^2 + t + 1,$$

where  $t$  is a positive integer and  $q$  is a prime. It is not known if equation (3) has infinitely many solutions, although there is a conjecture which asserts that equation (3) does admit infinitely many solutions.

When  $n = 1$  and  $q = 2$ , equation (1) reduces to

$$(4) \quad x^2 = 2^{m+2} - 7,$$

which is a famous diophantine equation due to Ramanujan and first solved by Nagell. When  $n = 1$ , all solutions of equation (1) with  $q$  an odd prime have been found by Skinner in [4], and the general case in which  $q$  is an odd prime power has been settled by Mignotte and Pethő in [3]. We also recall that all the solutions of the analogous diophantine equation

$$(5) \quad x^2 = 4q^m + 4q^n + 1$$

where found, for  $n = 1$  and  $n = 2$ , by Tzanakis de Wolfskill in [5], and for general  $n$ , by Mao Hua Le in [2].

First of all, let us notice that we may assume that  $m$  and  $n$  are coprime if  $n > 0$ . Indeed, for if  $m$  and  $n$  are not coprime, then we may write  $d := \gcd(m, n)$ ,  $q_1 := q^d$ ,  $m_1 := m/d$ , and  $n_1 := n/d$ , and rewrite equation (1) as

$$(6) \quad x^2 = 4q_1^{m_1} - 4q_1^{n_1} + 1,$$

---

Received by the editors September 28, 2001.

2000 *Mathematics Subject Classification*. Primary 11D61, 11D72.

©2002 American Mathematical Society

which is an equation of the same type as equation (1), but now the new exponents  $m_1$  and  $n_1$  are coprime. We also notice that equation (1) has the solutions  $m = n$ ,  $x = 1$ , and  $m = 2n$ ,  $x = 2q^n - 1$  for all  $n \geq 0$ . We shall refer to such solutions as *trivial*. Our main result in this note is the complete determination of all the non-trivial solutions of equation (1) with  $(m, n) \neq (1, 0)$  and  $q$  a prime power.

**Theorem.** *The only non-trivial solutions of equation (1) with  $q$  a prime power and  $m > n \geq 0$  but  $(m, n) \neq (1, 0)$  are*

$$(7) \quad (x, q, m, n) = (37, 7, 3, 0), (5, 2, 3, 1), (11, 2, 5, 1), \\ (181, 2, 13, 1), (31, 3, 5, 1), (559, 5, 7, 1).$$

*Proof of the Theorem.* We first treat the case  $n = 0$ . In this case, equation (1) reduces to

$$(8) \quad x^2 = 4q^m - 3,$$

with  $m \geq 2$ . Notice that  $m$  is odd, for if  $m$  is even, then  $4q^m = ((2q)^{m/2})^2$  is a perfect square, but the only perfect squares which differ by 3 are 1 and 4, which leads to  $x = 1$  and  $q = 1$ , which is not a convenient solution. Now let  $p \geq 3$  be any prime divisor of  $m$ . We may replace  $m$  by  $p$  and  $q$  by  $q^{m/p}$  and therefore analyze the equation

$$(9) \quad x^2 = 4q^p - 3.$$

When  $p = 3$ , with  $X := q$  and  $Y := x$ , we get the elliptic curve

$$(10) \quad Y^2 = 4X^3 - 3.$$

We used SIMATH to conclude that the only integer solutions of this equation are  $(X, Y) = (1, 1)$  and  $(7, 37)$ . Thus, we get the solution  $(x, q, m, n) = (37, 7, 3, 0)$  of equation (1). When  $p \geq 5$ , we rewrite equation (9) as

$$(11) \quad q^p = \frac{x^2 + 3}{4} = \left(\frac{x + i\sqrt{3}}{2}\right)\left(\frac{x - i\sqrt{3}}{2}\right).$$

It is easy to see from (9) that  $q$  is coprime to 3, therefore the two algebraic integers appearing in the right-hand side of equation (11) are coprime in the ring of algebraic integers of  $\mathbf{Q}[i\sqrt{3}]$ . Since the ring of algebraic integers  $\mathbf{Z}[\frac{1+i\sqrt{3}}{2}]$  of  $\mathbf{Q}[i\sqrt{3}]$  is euclidian, it follows that there exist two integers  $a$  and  $b$  with  $a \equiv b \pmod{2}$ , and a unit  $\zeta$  in  $\mathbf{Z}[\frac{1+i\sqrt{3}}{2}]$ , such that

$$(12) \quad \frac{x + i\sqrt{3}}{2} = \zeta z^p$$

where

$$(13) \quad z = \frac{a + i\sqrt{3}b}{2}.$$

Notice that  $x > 1$ , therefore  $z$  is not a root of unity. Since  $p \geq 5$  and all the units of  $\mathbf{Z}[\frac{1+i\sqrt{3}}{2}]$  are torsioned of order dividing 6, it follows that, up to a substitution, we may assume that  $\zeta = 1$  in formula (12). Eliminating  $x$  from (12) we get

$$(14) \quad i\sqrt{3} = z^p - \bar{z}^p.$$

But  $z - \bar{z} = bi\sqrt{3}$  and

$$\frac{z^p - \bar{z}^p}{z - \bar{z}} \in \mathbf{Z}.$$

Thus, it follows that  $b = \pm 1$  and

$$(15) \quad \frac{z^p - \bar{z}^p}{z - \bar{z}} = \pm 1.$$

For any integer  $k \geq 0$  let

$$(16) \quad u_k := \frac{z^k - \bar{z}^k}{z - \bar{z}}.$$

Then  $(u_k)_{k \geq 0}$  is a Lucas sequence of the first kind, and equation (15) is equivalent to  $u_k = \pm 1$ . However, it is well known that, in general, the  $k$ th term of a Lucas sequence has a *primitive divisor*. That is, for  $k \neq 1, 2, 3, 6$ , there exists, with a few exceptions, a prime number  $P \equiv \pm 1 \pmod{k}$  such that  $P \mid u_k$ . Equation (15) now tells us that  $u_p$  has no primitive divisor. The members of Lucas sequences with no primitive divisors have recently been completely classified by Bilu, Hanrot and Voutier in [1]. In particular, from the result in [1], we know that if  $p \geq 5$  is a prime, then  $u_p$  has primitive divisors except for  $p = 5, 7, 13$ , and a few exceptional values of  $z$ , which are listed in Table 1 in [1]. None of the exceptional Lucas terms from Table 1 in [1] leads to a value of  $z \in \mathbf{Q}[i\sqrt{3}]$ . Thus, there is no solution of equation (8) with  $x > 1$  and  $m > 3$ . This concludes the analysis for the case  $n = 0$ .

From now on, we assume that  $n > 0$ . All the solutions of equation (1) with  $n = 1$  were found by Mignotte and Pethő in [3], and these solutions are listed in formula (7). Thus, from now on we assume that  $n \geq 2$ ,  $m > n$ , and  $m$  and  $n$  are coprime.

We start by writing

$$(17) \quad 4q^n - 1 = Dw^2,$$

where  $D \geq 1$  is square-free. We first show that  $D > 3$ . Clearly,  $D \neq 1$  because  $-1$  is not a quadratic residue modulo 4. Assume now that  $D = 3$ . Since  $-1$  is not a quadratic residue modulo 3, it follows that  $n$  is odd. Let  $p$  be a prime divisor of  $n$ . By writing  $q_1 := q^{n/p}$ , it follows that we need to investigate the equation

$$(18) \quad 4q_1^p - 1 = 3w^2,$$

where  $q_1$  is a prime power and  $p \geq 3$  is prime. When  $p = 3$ , with the substitution  $X := q_1$  and  $Y := w$ , we get the elliptic curve

$$(19) \quad 3Y^2 = 4X^3 - 1.$$

We used SIMATH to conclude that the only integer solution of (19) is  $(X, Y) = (1, 1)$ . Thus, there is no solution  $(q_1, w)$  of equation (18) for  $p = 3$ . Assume now that  $p \geq 5$  and rewrite (18) as

$$(20) \quad q_1^p = \frac{1 + 3w^2}{4} = \left(\frac{1 + i\sqrt{3}w}{2}\right)\left(\frac{1 - i\sqrt{3}w}{2}\right).$$

We now use an argument similar to one employed above, to conclude that equation (20) implies the existence of an algebraic number  $z \in \mathbf{Z}[\frac{1+i\sqrt{3}}{2}]$  such that

$$(21) \quad q = z\bar{z}$$

and

$$(22) \quad \frac{1 + i\sqrt{3}w}{2} = z^p.$$

Notice that  $w > 1$  so  $z$  is not a root of unity. From equation (22) we get

$$(23) \quad 1 = z^p + \bar{z}^p = \frac{z^{2p} - \bar{z}^{2p}}{z^p - \bar{z}^p} = \frac{u_{2p}}{u_p}.$$

The numbers  $u_{2p}$  and  $u_p$  appearing in formula (23) are the same as the ones shown in (16). Thus, from (23), we get that  $u_{2p} = u_p$ , which implies that  $u_{2p}$  has no primitive divisor. We again use Table 1 in [1] to conclude that the only possible case is  $p := 5$  and  $z := \frac{5+i\sqrt{3}}{2}$ , but for this choice of  $p$  and  $z$  the relation  $u_5 = u_{10}$  does not hold (in fact,  $u_{10}/u_5 = -25$  in this case). Thus, the conclusion of this argument is that if  $n \geq 2$ , then  $D > 3$ .

Now let  $q := p^f$ , where  $p$  is a prime and  $f \geq 1$ . Notice that  $D \equiv 3 \pmod{4}$  so that  $-D$  is the discriminant of the quadratic field  $\mathbf{K} := \mathbf{Q}[i\sqrt{D}]$ . Moreover,  $p$  splits in  $\mathbf{K}$ . Indeed, if  $p$  is odd, then

$$(24) \quad \left(\frac{-D}{p}\right) = \left(\frac{-Dw^2}{p}\right) = \left(\frac{1-4q^n}{p}\right) = \left(\frac{1}{p}\right) = 1.$$

In the above computation, for an integer  $a$ , we used  $\left(\frac{a}{p}\right)$  to denote the Legendre symbol of  $a$  with respect to  $p$ . If  $p = 2$ , then equation (17) implies that  $D \equiv 7 \pmod{8}$ , therefore  $-D \equiv 1 \pmod{8}$ , so 2 splits in  $\mathbf{K}$ . Write  $(p) = \pi\bar{\pi}$ , where  $\pi$  is a prime ideal. From equation (17), we get

$$(25) \quad p^{fn} = q^n = \frac{1 + Dw^2}{4} = \left(\frac{1 + i\sqrt{D}w}{2}\right)\left(\frac{1 - i\sqrt{D}w}{2}\right).$$

If we rewrite (25) in terms of ideals in  $\mathbf{K}$ , we get

$$(26) \quad \pi^{fn} \cdot \bar{\pi}^{fn} = \left[\frac{1 + i\sqrt{D}w}{2}\right] \cdot \left[\frac{1 - i\sqrt{D}w}{2}\right].$$

It is easy to check that the two ideals appearing in the right-hand side of equation (26) are coprime (indeed, the sum of their generators is 1). From the unique factorization property for ideals, it follows that, up to interchanging  $\pi$  by  $\bar{\pi}$ , the equality

$$(27) \quad \pi^{fn} = \left[\frac{1 + i\sqrt{D}w}{2}\right]$$

must hold. Let  $o(\pi)$  be the order of the ideal class of  $\pi$  in the ideal class group  $C_{\mathbf{K}}$  of  $\mathbf{K}$ . Since  $\pi^{fn}$  is principal, it follows that  $o(\pi)$  divides  $nf$ .

We now return to equation (1) and write it as

$$(28) \quad 4q^m = x^2 + 4q^n - 1 = x^2 + Dw^2$$

or

$$(29) \quad q^m = \frac{x^2 + Dw^2}{4} = \left(\frac{x + i\sqrt{D}w}{2}\right)\left(\frac{x - i\sqrt{D}w}{2}\right).$$

We interpret (29) in terms of ideals by writing

$$(30) \quad \pi^{fm} \cdot \bar{\pi}^{fm} = \left[\frac{x + i\sqrt{D}w}{2}\right] \cdot \left[\frac{x - i\sqrt{D}w}{2}\right].$$

It is easy to check that the two ideals appearing in the right-hand side of (30) are coprime. Indeed, let  $\mathfrak{p}$  be a prime ideal dividing both  $\frac{x+i\sqrt{D}w}{2}$  and  $\frac{x-i\sqrt{D}w}{2}$ . Then  $\mathfrak{p}$  divides  $i\sqrt{D}w$ , therefore  $N_{\mathbf{K}}(\mathfrak{p}) \mid Dw^2$ . Thus,  $N_{\mathbf{K}}(\mathfrak{p})$  divides  $4q^n - 1$ . However, since  $\mathfrak{p}$  also divides  $q^m$ , we get  $N_{\mathbf{K}}(\mathfrak{p}) \mid q^{2m}$ . But obviously,  $4q^n - 1$  and  $q^m$  are

coprime. Thus, since the two ideals appearing in the right-hand side of equation (30) are coprime, it follows, by the unique factorization property for ideals, that, up to replacing  $w$  with  $-w$ , we have

$$(31) \quad \pi^{fm} = \left( \frac{x + i\sqrt{D}w}{2} \right).$$

In particular,  $\pi^{fm}$  is principal, which implies that  $o(\pi) \mid fm$ . Since  $o(\pi) \mid fn$  as well, and since  $m$  and  $n$  are coprime, it follows that  $o(\pi) \mid f$ . Hence,  $\pi^f$  is principal.

Now let  $a$  and  $b$  be two integers with  $a \equiv b \pmod{2}$  such that

$$(32) \quad z := \frac{a + i\sqrt{D}b}{2}$$

is a generator of  $\pi^f$ . We then get

$$[q] = [p^f] = \pi^f \bar{\pi}^f = [z] \cdot [\bar{z}],$$

therefore, from equation (26), we conclude that

$$(33) \quad [z^n] \cdot [\bar{z}^n] = [q^n] = \left[ \frac{1 + i\sqrt{D}w}{2} \right] \left[ \frac{1 - i\sqrt{D}w}{2} \right].$$

The two ideals appearing on the right-hand side of equation (33) are coprime and so are the two ideals appearing on the left-hand side. Since the ideals appearing on the left-hand side are prime powers, it follows, from the unique factorization property for ideals, that we may assume (up to replacing  $b$  by  $-b$ )

$$(34) \quad [z^n] = \left[ \frac{1 + i\sqrt{D}w}{2} \right].$$

Equation (34) together with the fact that  $D > 3$  (that is, the only units in  $\mathbf{K}$  are  $\pm 1$ ) implies that

$$(35) \quad \frac{1 + i\sqrt{D}w}{2} = \pm z^n.$$

Eliminating  $w$  from equation (35), we get

$$(36) \quad \pm 1 = z^n + \bar{z}^n = \frac{z^{2n} - \bar{z}^{2n}}{z^n - \bar{z}^n} = \frac{u_{2n}}{u_n},$$

where for a positive integer  $k$  the number  $u_k$  is given in formula (16). Thus, we again get that  $u_{2n}$  has no primitive divisors.

We first treat the case  $n \geq 3$ . If  $n = 3$ , then from formula (32) and equation (36) we get

$$\pm 1 = z^3 + \bar{z}^3 = \frac{a^3 - 3Dab^2}{4}$$

or

$$(37) \quad \pm 4 = a(a^2 - 3Db^2).$$

If  $a$  is even, then so is  $b$  (because  $a \equiv b \pmod{2}$ ), and in this case the right-hand side of (37) is a multiple of 8, which is impossible. Thus,  $a$  is an odd divisor of 4, therefore  $a = \pm 1$ . From equation (37) we now conclude that  $3Db^2 = \pm 3, \pm 5$ , which is obviously impossible.

Assume now that  $n \geq 4$ . In this case,  $2n \geq 8$  and  $u_{2n}$  has no primitive divisors. From Table 1 in [1], together with the fact that  $z$  is complex non-real and that  $D > 3$  is odd, it follows that the only possibilities are

$$\begin{aligned} n = 4 \text{ and } z &:= \frac{1 + i\sqrt{7}}{2}; \\ n = 5 \text{ and } z &:= \frac{5 + i\sqrt{47}}{2}; \\ n = 6 \text{ and } z &:= \frac{1 + i\sqrt{7}}{2}, \frac{1 + i\sqrt{11}}{2}, \frac{1 + i\sqrt{15}}{2}, \frac{1 + i\sqrt{19}}{2}; \text{ or} \\ n = 9 \text{ and } z &:= \frac{1 + i\sqrt{7}}{2}. \end{aligned}$$

Out of the above possibilities, only the first one, namely  $n = 4$  and  $z := \frac{1+i\sqrt{7}}{2}$ , satisfies equation (36). Thus,  $q = 2$ ,  $n = 4$ ,  $D = 7$ , and  $w = 3$ , and equation (29) can be rewritten as

$$(38) \quad 2^m = \left(\frac{x + 3i\sqrt{7}}{2}\right)\left(\frac{x - 3i\sqrt{7}}{2}\right).$$

From arguments similar to the ones previously employed, we get that, up to replacing  $x$  by  $-x$ , any solution  $(x, m)$  of the above equation (38) will satisfy

$$(39) \quad \frac{x + 3i\sqrt{7}}{2} = \pm z^m,$$

with  $z = \frac{1+i\sqrt{7}}{2}$ . Eliminating  $x$  from equation (39), we get

$$\pm 3i\sqrt{7} = z^m - \bar{z}^m$$

or

$$(40) \quad u_m = \pm 3,$$

where for a positive integer  $k$ , the number  $u_k$  is given by formula (16). From [1], we know that if  $m \geq 31$ , then  $u_m$  has a primitive divisor which is at least as large as  $m - 1 > 3$ . Thus,  $m \leq 30$ . We have computed all the terms  $u_m$  for  $m$  in the interval  $[5, 30]$  and only  $m = 4$  and  $m = 8$  satisfy (40), but they are not convenient, because we are searching for solutions of equation (1) with  $m$  and  $n$  coprime. Thus, the conclusion so far is that  $n \geq 3$  cannot hold.

Thus,  $n = 2$ . In particular,  $m \geq 3$  is odd. Equation (36) now tells us that

$$(41) \quad \pm 1 = z^2 + \bar{z}^2 = \frac{a^2 - Db^2}{2}.$$

Notice that equation (41) implies, in particular, that  $a^2$  and  $Db^2$  are coprime (recall that  $D$  is odd), and that  $a \neq \pm 1$ . Equation (35) now tells us that

$$(42) \quad \frac{1 + i\sqrt{D}w}{2} = \pm z^2 = \pm \left(\frac{a^2 - Db^2}{4} + \frac{i\sqrt{D}ab}{2}\right),$$

therefore

$$(43) \quad w = \pm ab.$$

We now return to equation (29) and write it under the form

$$(44) \quad z^m \cdot \bar{z}^m = q^m = \left(\frac{x + i\sqrt{D}w}{2}\right)\left(\frac{x - i\sqrt{D}w}{2}\right).$$

From arguments similar to the previous ones, we conclude that, up to replacing  $x$  by  $-x$ , we can write

$$(45) \quad \frac{x + i\sqrt{D}w}{2} = \pm z^m,$$

and now by eliminating  $x$  from equation (45), we get

$$(46) \quad \pm i\sqrt{D}ab = \pm i\sqrt{D}w = z^m - \bar{z}^m.$$

By applying the binomial formula in equation (46), we get that

$$(47) \quad \pm ab = \frac{b}{2^{m-1}}(ma^{m-1} - \dots + (-1)^{(m-1)/2}D^{(m-1)/2}b^{m-1}).$$

From equation (47), we conclude right away that  $a \mid D^{(m-1)/2}b^{m-1}$ . Since  $a^2$  and  $Db^2$  are coprime, it follows that  $a = \pm 1$ , which, as we have already seen, is impossible.

So, it follows that equation (1) has no non-trivial solutions with  $n > 1$  and  $\gcd(m, n) = 1$ .

The Theorem is therefore proved.  $\square$

*Remark.* The method used in this paper can be employed to find, for a given odd integer  $k$ , all solutions of the diophantine equation

$$(48) \quad x^2 = 4q^m - 4q^n + k^2,$$

with  $m \geq n \geq 0$ ,  $(m, n) \neq (1, 0)$  and  $q$  a prime power. The case treated here is, of course,  $k = 1$ . We do not give further details.

#### ACKNOWLEDGEMENTS

This work was done when I visited the Tata Institute for Fundamental Sciences in Mumbai, India in Summer 2001. I would like to thank the Institute for its hospitality, Professor T.N. Shorey for his advice and the Third World Academy of Sciences for their support.

#### REFERENCES

- [1] Y. Bilu, G. Hanrot, P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75-122. MR **2002j**:11027
- [2] M. H. Le, *The diophantine equation  $x^2 = 4q^m + 4q^n + 1$* , Proc. Amer. Math. Soc. **106** no. 3 (1989), 599-604. MR **90b**:11024
- [3] M. Mignotte, A. Pethő, *On the diophantine equation  $x^p - x = y^q - y$* , Publ. Math. **43** no. 1 (1999), 207-216. MR **2000d**:11044
- [4] C. Skinner, *The diophantine equation  $x^2 = 4q^n - 4q + 1$* , Pacific J. of Math. **139** no. 2 (1989), 303-309. MR **90g**:11039
- [5] N. Tzanakis, J. Wolfskill, *The diophantine equation  $x^2 = 4q^{a/2} + 4q + 1$ , with an application to coding theory*, J. Number Theory **26** no. 1 (1987), 96-116. MR **88g**:11009

INSTITUTO DE MATEMÁTICAS UNAM, AP. POSTAL 61-3 (XANGARI), CP 58 089, MORELIA, MICHOACÁN, MEXICO

*E-mail address:* `fluca@matmor.unam.mx`