Ka-Lam Kueh, On the Diophantine equation $x^2 + c^{2m} = y^n$,
Чебышевский сб., 2001, том 1, выпуск 1, 95–97

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 1 (2001)

Труды IV Международной конференции
«Современные проблемы теории чисел и ее приложения»

ON THE DIOPHANTINE EQUATION $x^2 + c^{2m} = y^n$

KA-LAM KUEH (Taiwan)

maklk@ccvax.sinica.edu.tw

In this note we apply existence of primitive divisors of Lucas numbers to the investigation of the diophantine equation of the title.

Florian Lucas [5] using the results of Yu. Bilu, G. Hanrot and P. M. Voutier [3] proved that diophantine equation

$$x^2 + 3^{2m} = y^n,\ (3, x) = 1,\ n \geqslant 3$$

in positive integers has only solution $(x, y, m, n) = (46, 13, 2, 3)$ and thus proved a conjecture of [1]. The same argument with a result of [2] gives complete solution of the equation

$$x^2 + 2^{2m} = y^n,\ (2, x) = 1,\ n \geqslant 3$$

namely, the latter equation in positive integers has a unique solution $(x, y, m, n) = (11, 5, 1, 3)$.

In this note we consider in the positive integers the diophantine equation

$$x^2 + c^{2m} = y^n,\ (x, c) = 1,\ n \geqslant 3. \qquad (1)$$

with a fixed c.

Theorem 1. *If in (1) n is an odd number $\geqslant 5$, then there exists an odd prime p such that $p \mid c$ and $p \equiv (-1)^{\frac{p-1}{2}} \pmod{n}$.*

Theorem 2. *If in (1) c is a prime then either $n = 4$ or $n = 8$, $m = 1$, $c = 239, x = 28560, y = 13$ or n is an odd number.*

Remark. If c is a given prime then from theorems 1, 2 it follows a few possibility for the values of n. For these possible values of n equation (1) for many cases can be investigated by methods of works [1, 2, 4] or by some other way.

Proof of theorem 1. From $(x, c) = 1$ it follows that $x^2 + c^{2m} \not\equiv 0 \pmod 4$ and therefore x, c are integers with different evenness. It means that the numbers

$x + c^m\sqrt{-1}$ and $x - c^m\sqrt{-1}$ are relatively primes as integers in the field $Q(\sqrt{-1})$ which has unique prime factorization. Hence, from

$$(x + c^m\sqrt{-1})(x - c^m\sqrt{-1}) = y^n$$

and oddness n we have

$$x + c^m\sqrt{-1} = (a + b\sqrt{-1})^n \tag{2}$$

where a, b are rational integers of different evenness, $y = a^2 + b^2$. Considering imaginary part of this relation, we see that $b \mid c^m$.

Put $\alpha = a + b\sqrt{-1}$, $\beta = a - b\sqrt{-1}$ and $u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$. Since $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational integers, α/β is not a root of unity (since, for example, a, b are different evenness) then sequence u_k is a Lucas sequence. By the results of [3] for all $k > 30$, u_k has a primitive divisor. As to $5 \leqslant k \leqslant 30, k \neq 6$ all Lucas numbers without primitive divisor are listed in Theorem C of [3]. No one of such numbers is of the form $a + b\sqrt{-1}$. Therefore u_n has a primitive divisor.

Let prime p be the primitive divisor of u_n. From (2) it follows $c^m = bu_n$. Hence $p \mid c$. According to definition of primitive divisor p does not divide even number $(\alpha - \beta)^2 u_1 \ldots u_{n-1}$, i. e. $p > 2$. Therefore it remains to prove that $p \equiv 1 \pmod{n}$ if $p \equiv 1 \pmod{4}$ and $p \equiv -1 \pmod{n}$ if $p \equiv 3 \pmod{4}$. Also note that $(b, p) = 1$ which is important.

For rational integers X, Y, Z, T we will write that $X + Y\sqrt{-1} \equiv Z + T\sqrt{-1} \pmod{p}$ if $X - Z$ and $Y - T$ are divided by p. In this notation the fact that u_n is divided by p can be written as

$$(a + b\sqrt{-1})^n \equiv (a - b\sqrt{-1})^n \pmod{p}. \tag{3}$$

Two cases are possible:

Case 1.) $p \equiv 1 \pmod{4}$.

Since $(a \pm b\sqrt{-1})^p \equiv a \pm b\sqrt{-1} \pmod{p}$ and $(a^2 + b^2, p) = 1$, then is $(a \pm b\sqrt{-1})^{p-1} \equiv 1 \pmod{p}$. Therefore if $p - 1 \equiv r \pmod{n}, 0 \leqslant r \leqslant n - 1$, then using (3) we have $(a + b\sqrt{-1})^r - (a - b\sqrt{-1})^r \equiv 0 \pmod{p}$. Hence if $r \neq 0$ then $u_r \equiv 0 \pmod{p}$. It contradicts that p does not divide $(\alpha - \beta)^2 u_1 \ldots u_{n-1}$. Thus $r = 0$ and in this case the theorem is proved.

Case 2. $p \equiv 3 \pmod{4}$.

Since $(a \pm b\sqrt{-1})^p \equiv a \mp b\sqrt{-1} \pmod{p}$ there is

$$(a \pm b\sqrt{-1})^{p+1} \equiv a^2 + b^2 \pmod{p}.$$

Hence

$$(a + b\sqrt{-1})^{p+1} \equiv (a - b\sqrt{-1})^{p+1} \pmod{p}. \tag{4}$$

Let $p + 1 \equiv r \pmod{n}, 0 \leqslant r \leqslant n - 1$. From (3), (4) it follows that $(a + b\sqrt{-1})^r - (a - b\sqrt{-1})^r \equiv 0 \pmod{p}$. As in CASE 1 we conclude that $r = 0$.

Theorem 1 is proved.

Proof of theorem 2. Let $n = 2k, k \geqslant 3$ and (1) takes place. Then $c \neq 2$ due to [2]. Hence c is an odd prime. From

$$(y^k - x)(y^k + x) = c^{2m}$$

and $(x, c) = 1$ we deduce that

$$y^k - x = 1,\ y^k + x = c^{2m}.$$

Therefore

$$c^{2m} + 1 = 2y^k.$$

If k has an odd prime divisor then it contradicts to [6] that $u^2 + 1 = 2v^k$ is not possible in positive integers $u > 1, v$ and $k \geqslant 3$. Otherwise by [7] the equation

$$u^2 - 2v^4 = -1$$

has only solutions (1,1) and (239,13). Thus we have proved theorem 2.

Corallary 1. *For $c = 5$ Eq. (1) has no solutions in the positive integers.*

Corallary 2. *For $c = 7$ Eq. (1) has only solutions*
$(x, y, m, n) = (524, 65, 1, 3)$ *and* $(x, y, m, n) = (24, 5, 1, 4)$.

REFERENCES

[1] Arif S. A., Muriefah S. A. On a diophantine equation. Bull. Austral. Math. Soc. V. 57(1998). P. 189-198.

[2] Arif S. A., Muriefah S. A. On the diophantine equation $x^2 + 2^k = y^n$. Int. J. Math. Math. Sci. V. 20(1997). P. 299-304.

[3] Bilu Yu., Hanrot G. , Voutier P. M. Existence of primitive divisors of Lucas and Lehmer numbers. J. reine angew. Math. (to appear).

[4] Cohn J. H. E. The diophantine equation $x^2 + 2^k = y^n$. Int. J. Math. Math. Sci. V. 22(1999). P. 459-462.

[5] Luca F. On a diophantine equation. Bull. Austral. Math. Soc. V. 61(2000). P. 241-246.

[6] Störmer M. C. Solution compléte en nombres entries de l'équation $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$, Bull. Soc. Math. France. V. 27(1899). P. 160-170.

[7] Ljunggren W. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. Norske Vid. Akad. Oslo. V. 51. (1942).

Institute of Mathematics, Academia Sinica, Taipei, Taiwan.
Received 5.11.2001.