SHORT COMMUNICATIONS

Arab J. Math. Sc.
Volume 7, Number 1, June 2001
pp. 67-71

ON THE DIOPHANTINE EQUATION $x^2 + 2^k = y^n$ II

S.A. ARIF AND FADWA S. ABU MURIEFAH

ABSTRACT. In [1], the authors made a conjecture that the diophantine equation $x^2+2^k = y^n$ where x, y, k, n are positive integers with n≥ 3 has exactly two families of solutions when k is even. In this paper this conjecture is proved.

1. INTRODUCTION

In 1992 Cohn [3] proved that the diophantine equation $x^2 + 2^k = y^n$ where $n \geq 3$ and k odd integer has exactly three families of solutions in positive integers x and y. When $k = 1$, the title equation was first solved by T. Nagell [6], and recently B. Sury [9] has given an elementary proof that this equation has no solution. The same problem with k even was considered later on by Arif and Abu Muriefah [1] and Cohn [4], and appeared to be of rather greater difficulty. In [1] authors made the following conjecture:
The diphantine equation

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

has exactly two families of solutions given by

$$x = 2^m, y^n = 2^{2m+1}, \qquad \text{for all } m \geq 1$$

and

$$x = 11.2^{3M}, \quad y = 5.2^{2M}, \quad n = 3, \text{for } m = 3M + 1.$$

1991 *Mathematics Subject Classification.* 11D41

In this paper we shall prove this conjecture. When $m = 1$, the conjecture is true by the result of [7]. It is also proved in [1] that equation (1) has no solution when n is even and $m > 1$. So we can suppose that n is an odd integer.

We start by the usual method of factorizing in the fields $Q(i)$, and then we use a recent result of Bilu, Hanrot and Voutier [2] about primitive divisors of Lucas numbers. We start by giving some important definitions and the result proved in [2].

Definitions. A *Lucas pair* is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero co-prime rational integers and $\frac{\alpha}{\beta}$ is not a root of unity. Given a Lucas pair (α, β) one defines the corresponding *sequence* of Lucas numbers by

$$u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \ n \geq 0.$$

A prime number p is a primitive divisor of $u_n(\alpha, \beta)$ if p divides u_n but does not divide $(\alpha - \beta)^2 u_1 u_2 \ldots u_{n-1}$.

Result (Theorem 1.4 of [2]). For $n > 30$, the nth term of any Lucas sequences has a primitive divisor.

For $5 \leq n \leq 30$ all values of pairs have been listed for which the nth term of Lucas sequences has no primitive divisors.

We first prove the following theorem.

Theorem 1. *If x, y and n are odd integers, then the diophantine equation (1) has a unique solution given by $x = 11, y = 5, n = 3$ and $m = 1$.*

Proof. It is enough to prove the result for $n = p$ an odd prime. Factoring equation (1) in $Q(i)$, we get

$$(x + 2^m i)(x - 2^m i) = y^p$$

Since the factors on the left hand side are relatively prime and any unit of $Q(i)$ is a p-th power, we can write

$$x + 2^m i = (a + bi)^p \tag{2}$$

where a and b are rational integers and $y = a^2 + b^2$. Since y is odd, a and b are of opposite parity. Let $\alpha = a + bi$ and $\bar{\alpha} = a - bi$. Then from (2) we get

$$\frac{\alpha^p - \bar{\alpha}^p}{\alpha - \bar{\alpha}} = \frac{2^m}{b}$$

Since the left hand side is an algebraic integer, this implies that $b | 2^m$, hence b is a power of 2, hence a is odd. It is easy to check that $\bar{\alpha}/\alpha$ is not a root of unity because it is never equal to ± 1 or $\pm i$. Also gcd $(\alpha + \bar{\alpha}, \alpha\bar{\alpha}) = \gcd(2a, a^2 + 2^{2m}) = 1$, so

$$u_t = \frac{\alpha' - \bar{\alpha}^t}{\alpha - \bar{\alpha}}, \; t \geq 0$$

is a Lucas sequence . Since 2 divides $(\alpha - \bar{\alpha})^2$, therefore by definition 2 is not a primitive divisor. Using Theorem 1.4 of [2] we get $p \leq 30$, and by checking the tables of [2] we see that only $p = 3$ and $m = 1$ is possible. So equation (1) becomes $x^2 + 4 = y3$ which has only one solution in x odd as $x = 11, y = 5$, [7]. This completes the proof of Theorem 1.

Proof of conjecture. From Theorem 1, it is sufficient to consider that x is even, so let

$$x = 2^\mu X, \qquad y = 2^\gamma Y \qquad \text{where } \mu > 0, \gamma > 0$$

and X, Y are odd integers. From (1) we obtain

$$2^{2\mu} X^2 + 2^{2m} = 2^{ny} Y^n \tag{3}$$

and therefore of three powers of $2, 2\mu, 2m$, and $n\gamma$ which occur here, two must be equal and the third is greater. Thus we have three cases

1. $2\mu > 2m = n\gamma$, then from (3) we get

$$(2^{\mu - m} X)^2 + 1 = Y^n$$

and this equation is known to have no solutions [5].

2. $n\gamma > 2\mu = 2m$, then from (3), we get

$$X^2 + 1 = 2^{n\gamma - 2\mu} Y^n \tag{4}$$

Considering modulo 8, we get $n\gamma - 2\mu = 1$ and so (4) becomes.

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

which has been proved to have only one $X = Y = 1, [8]$, so that

$$x = 2^m \text{ and } y^n = 2^{2m+1}$$

3. $2m > 2\mu = n\gamma$, then

$$X^2 + 2^{2(m-\mu)} = Y^n$$

which by Theorem 1 has no solution in X odd as $X = 11, Y = 5, n = 3$ and $m - \mu = 1$ and accordingly $n\gamma = 2\mu$ implies $3|\mu$, so

$$X = 11.2^{3M}, \qquad y = 5.2^{2M}, \qquad n = 3 \quad \text{for} \quad m = 3M + 1.$$

This completes the proof of the conjecture.

REFERENCES

1. S.Akhtar Arif and Fadwa S. Abu Muriefah, *On The Diophantine Equation $x^2 + 2^k = y^n$*. Internat. J. Math. and Math. Sci. **20**(2)(1997), 299-304.

2. Yu Bilu, G. Hanrot and P.M. Voutier, *Existence of primitive divisors of lucas and Lehmer numbers.* J. Reine Angew. Math (to appear).

3. J.H.E. Cohn, *The diophantine equation $x^2 + 2^k = y^n$* Arch. Math (Basel) **59**(4)(1992), 341-344.

4. .J.H.E. Cohn. *The diophantine equation $x^2 + 2^k = y^n$ II*, Internat. J.Math. and Math. Sci. **22**(3) (1999), 459-462.

5. V.A. Lebesgue, *Sur 1' impossibilite en nombres entiers de l'équation* $x^m = y^2 + 1$. Nouv. Anna. Des Math **9**(1850), 178-181.

6. T. Nagell, *Verallegemeinerung eines Fermatschen Satzes*, Arch. Math. **5**(1954), 153-159.

7. T. Nagell, . *Contributions to the theory of a category of diophantine equations of second degree with two unknowns,* Nova Acta Soc. Sci., Upsal. Ser 4, **16**(2)(1955), 1-38.

8. C. Stormer, *L'équation m arctan* $1/x + n$ *arctan* $1/y = k\pi/4$. Bull. Soc. Math. France **26**(1899), 160-170.

9. B. Sury, *On the diophantine equation* $x^2+2 = y^n$, Arch. Math. **74**(2000), 350-355.

DEPARTMENT OF MATHEMATICS, GIRLS COLLEGE OF EDUCATION RIYADH, SAUDI ARABIA

e-mail: abumuriefah@yahoo.com

Date received March 24, 2001.