GLASNIK MATEMATIČKI
Vol. 42(62)(2007), 281 – 289

ON A DIOPHANTINE EQUATION RELATED TO A CONJECTURE OF ERDÖS AND GRAHAM

F. Luca and P. G. Walsh
UNAM, Mexico and University of Ottawa, Canada

Abstract. A particular case of a conjecture of Erdös and Graham, which concerns the number of integer points on a family of quartic curves, is investigated. An absolute bound for the number of such integer points is obtained.

1. Introduction

In [3], Erdös and Graham posed a conjecture concerning the product of blocks of consecutive integers. Specifically, for fixed positive positive integers $k \geq 2$ and $l \geq 4$, the assertion states that the equation

$$y^2 = \prod_{i=1}^{k} (x_i)_l \tag{1}$$

has at most finitely many solutions in positive integers $(y, x_1, \ldots, x_k)$ which satisfy the conditions

$$0 < x_1 < \cdots < x_k, \quad x_i + l \leq x_{i+1}, \quad i = 1, \ldots, k,$$

and with $(x)_l$ defined as

$$(x)_l = (x+1)(x+2)\cdots(x+l).$$

Recently, Ulas [11] has shown that this statement is false when either $k = l = 4$, or $k \geq 6$ and $l = 4$. In the same paper, Ulas states a conjecture that for any integer $l \geq 4$, there is an integer $k_0 = k_0(l)$ with the property that if $k \geq k_0$, equation (1) has infinitely many integer solutions.

2000 *Mathematics Subject Classification.* 11D25.

Key words and phrases. Linear recurrence, elliptic curve, Diophantine equation.

The second author gratefully acknowledges support from The Natural Sciences and Engineering Research Council of Canada.

In the present paper, we consider the particular pair of values $(k, l) = (2, 4)$. In this case, it follows from the identity

$$(x-1)x(x+1)(x+2) = (x^2+x-1)^2 - 1$$

that a positive integer solution to (1) corresponds to two integer points (x, y), with positive coordinates, on a quartic curve of the form

$$(x^2+x-1)^2 - dy^2 = 1$$

for some squarefree integer $d > 1$.

For a squarefree integer $d > 1$, let $(X, Y) = (T, U)$ denote the minimal solution of the Pell equation $X^2 - dY^2 = 1$, and for $i \geq 1$, let

$$T_i + U_i\sqrt{d} = (T + U\sqrt{d})^i.$$

The problem we consider here, for a given squarefree integer $d > 1$, is to determine an absolute upper bound for the number of solutions in positive integers (i, x) to the equation

$$T_i = x^2 + x - 1. \tag{2}$$

Problems of this type have a long history, with many fundamental results. For instance, the combined work of Ljunggren [5] and Cohn [2] completely solved the equation $T_i = x^2$, in which it was shown that equation (2) implies that either $i = 1$ or $i = 2$, and that a solution exists for both $i = 1, 2$ only when $d = 1785$. More general results on polynomial values in linear recurrence sequences have been proved by Nemes and Pethö [9], and also by Shorey and Stewart [10].

Extensive computation on equation (2) indicates that the following is likely true.

CONJECTURE. *The equation $T_i = x^2 + x - 1$ implies that either $i = 1$ or $i = 2$, and a solution exists for both $i = 1, 2$ only when $d = 39270$.*

Evidently, the conjecture of Erdös and Graham, for the particular case $(k, l) = (2, 4)$, is a consequence of this conjecture. Unfortunately, we are unable to prove such a sharp result. However, we are able to obtain the following absolute upper bound for the number of solutions to (2). In what follows, $d > 1$ represents a squarefree positive integer.

THEOREM. *There is a computable constant C_1 such that for $d > C_1$, there are at most two positive integer solutions (i, x) to equation $T_i = x^2 + x - 1$. For all remaining d, there are at most three positive integer solutions (i, x) to the equation $T_i = x^2 + x - 1$.*

This theorem comes very close to proving the Erdös-Graham conjecture for the pair of values $(k, l) = (2, 4)$. What is still needed in order to solve this case of the conjecture is a proof that there are only finitely many d for which equation (2) is solvable for both an even index i_1 and an odd index i_2.

2. Proof

In the proof of the theorem, for any given squarefree integer d, it will be shown that there is at most one even index i, and at most two odd indices i, for which equation (2) is solvable. Also, for $d > C_1$, it will be shown that there is at most one odd index i for which equation (2) is solvable.

We begin by dealing with the case that the index i is even. Assume that

$$T_{2i} = x^2 + x - 1$$

for some integer x. The identity $T_{2i} = 2T_i^2 - 1$ implies that

$$2T_i^2 = x(x+1).$$

Therefore, there are positive integers u, v for which either

$$x = u^2, x+1 = 2v^2, T_i = uv$$

or

$$x = 2v^2, x+1 = u^2, T_i = uv.$$

We see that $u^2 - 2v^2 = \pm 1$, and so upon putting $\alpha = u + v\sqrt{2}$, we deduce that

$$\alpha^2 = (u^2 + 2v^2) + T_i\sqrt{8}$$

is a unit. In other words, $(X, Y, Z) = (u^2 + 2v^2, T_i, U_i)$ is a solution to the system of simultaneous Pell equations

$$X^2 - 8Y^2 = 1,\ Y^2 - dZ^2 = 1.$$

Such a system has recently been shown by Yuan [12] to have at most one solution in positive integers (X, Y, Z), which in turn implies that the equation $T_{2i} = x^2 + x - 1$ has at most one solution.

We now consider the equation

$$T_{2i+1} = x^2 + x - 1. \tag{3}$$

The following lemma provides the starting point for our analysis.

Lemma 2.1. *Let $d > 1$ be a squarefree integer, and let $\epsilon_d = T + U\sqrt{d}$ denote the minimal unit (> 1) of norm 1 in $\mathbf{Z}(\sqrt{d})$. Then*

$$\epsilon_d = \tau^2,$$

where

$$\tau = \frac{a\sqrt{r} + b\sqrt{s}}{\sqrt{c}},$$

$c \in \{1, 2\}$, $d = rs$, $r > 1$ not a square, and $a^2 r - b^2 s = c$.

Proof. This is well known, for example see Nagell [7]. ∎

REMARK 2.2. We note that all solutions to $a^2r-b^2s=c$ arise from taking odd powers of τ. In particular, if

$$\tau^{2i+1}=\frac{a_{2i+1}\sqrt{r}+b_{2i+1}\sqrt{s}}{\sqrt{c}},$$

then all solutions to $a^2r-b^2s=c$ are given by $a=a_{2i+1}, b=b_{2i+1}$. We also remark that for all $i\geq 0$, the highest power of 2 dividing a_{2i+1} (resp. b_{2i+1}) is the same as the highest power of 2 dividing a_1 (resp. b_1). This fact will be used in the arguments presented below.

In our situation, namely equation (3), we see that since T_{2i+1} is odd, T_1 is also odd, and hence the value of c in the lemma is necessarily equal to 1.

With τ as in the lemma, let

$$\tau^{2i+1}=a_{2i+1}\sqrt{r}+b_{2i+1}\sqrt{s}.$$

It is readily checked that

$$T_{2i+1}=2ra_{2i+1}^2-1,$$

from which equation (3) implies that

$$2ra_{2i+1}^2=x(x+1).$$

It follows that there are positive integers m,n,u,v for which

$$x+1=mu^2, x=nv^2, mn=2r, a_{2i+1}=uv.$$

Let $\alpha=u\sqrt{m}+v\sqrt{n}$, then

$$\alpha^2=(2u^2m-1)+a_{2i+1}\sqrt{8r}$$

is a unit. Putting $(X,Y,Z)=(2u^2m-1,a_{2i+1},b_{2i+1})$, it follows that (X,Y,Z) is a solution to the system of simultaneous Pell-type equations

$$X^2-8rY^2=1,\ rY^2-sZ^2=1. \tag{4}$$

We must now deal with two subcases separately, depending on whether X, in (4), is divisible by 3 or not. We make an important remark here. We claim that if there is a solution (X_0,Y_0,Z_0) to (4) with 3 dividing X_0, then 3 divides X for all solutions to (4). The reason is as follows. Assume that 3 divides such an integer X_0, where (X_0,Y_0,Z_0) is a solution to (4). Then by the properties of solutions to Pell equations (for example see [4]), $X_0+Y_0\sqrt{8r}$ is an odd power of the fundamental solution to $X^2-8rY^2=1$. Conversely, 3 divides X_1 for any solution $X_1+Y_1\sqrt{8r}$ to $X^2-8rY^2=1$ which is an odd power of the fundamental solution. Now let (X_1,Y_1,Z_1) be any solution to (4). Now, by the remark after the lemma above, the highest power of 2 dividing Y_1 is the same as the highest power of two dividing Y_0, and so using the binomial theorem, it is easily deduced that $X_1+Y_1\sqrt{8r}$ is an odd power of the fundamental solution to $X^2-8rY^2=1$. Therefore, 3 divides X_1.

We first deal with the subcase that 3 divides X for all solutions (X, Y, Z) to the system of equations in (4). The two equations in (4) imply that

$$8rY^2 = X^2 - 1 = 8(sZ^2 + 1),$$

from which it follows that

$$X^2 - 9 = 8sZ^2.$$

Since s is squarefree, it follows that 3 divides Z. Putting $x = X/3, y = Y, z = Z/3$, we obtain the system of Pell equations

$$x^2 - 8sz^2 = 1,\ ry^2 - 9sz^2 = 1. \tag{5}$$

We remark that this system is equivalent to the system of equations

$$x^2 - 8sz^2 = 1,\ 9x^2 - 8ry^2 = 1. \tag{6}$$

We will assume that $r > 1$, for otherwise the desired result is a consequence of the main result in [12]. With $r > 1$ and squarefree, all solutions (y, z) to $ry^2 - 9sz^2 = 1$ arise from a positive odd power of a minimal solution. A consequence of this fact is that if (y_0, z_0) is the minimal solution to $ry^2 - 9sz^2 = 1$, and 2^{a_0} and 2^{b_0} properly divide y_0 and z_0 respectively, then these same powers of 2 properly divide y and z, respectively, for any integer solution to $ry^2 - 9sz^2 = 1$. This fact implies that the powers of 2 that divide x, y, and z, for any solution to equation (5), remain constant. With this in mind, we appeal to Lemma 2.1, and deduce that if (x_1, y_1, z_1) is a solution to the system of equation in (6), then there are unique squarefree positive integers m_1, m_2, m_3 (i.e. independent of the particular solution to the system in (6)), and integers u_1, u_2, u_3 for which $(x-1)/2 = m_1u_1^2$, $(3x-1)/2 = m_2u_2^2$, and $(3x+1)/2 = m_3u_3^2$. It follows that $3(x-1)/2 = 3m_1u_1^2$, $(3x-1)/2 = m_2u_2^2$, and $(3x+1)/2 = m_3u_3^2$ are three consecutive integers of fixed quadratic type in their factorizations. It follows from the main result of [1] that there can be only one solution to such a system of equations, and consequently, the system of equations in (5) has at most one solution.

We now deal with the case that 3 does not divide x for all solutions (x, y, z) to the system of equations (4). Firstly, as noted already, all solutions (x, y, z) to (4) have the property that the highest power of 2 dividing y is constant. This implies that among all solutions to (4), the highest power of 2 dividing the power of the fundamental solution, $t + u\sqrt{8r}$ say, of the Pell equation $X^2 - 8rY^2 = 1$ which equals $x + y\sqrt{8r}$ is also constant. This forces there to be a unique factorization $2r = r_1r_2$ for which

$$(x-1)/2 = r_1u_1^2,\ (x+1)/2 = r_2u_2^2,$$

for some integers u_1, u_2, as x ranges over all solutions (x, y, z) to equation (4).

As in the previous subcase, we see that x and z are related by

$$x^2 - 9 = 8sz^2,$$

where in this case we know that $(x, 6) = 1$. Therefore, there are positive integers A, B, u, v for which

$$(x-3)/2 = Au^2,\ (x+3)/2 = Bv^2,$$

where $AB = 2s$, $Z = uv$, and $Bv^2 - Au^2 = 3$.

The desired result is now a consequence of the following lemma.

LEMMA 2.3. *Let $D > 1$ be a squarefree integer, then there exist at most two factorizations $D = AB$, $1 \leq A < B \leq D$ for which the equation $BX^2 - AY^2 = 3$ is solvable in positive integers X, Y.*

PROOF. Let $\epsilon_D = T + U\sqrt{D}$ denote the minimal solution to the Pell equation $X^2 - DY^2 = 1$. Let $D = A_1B_1$ be a fixed factorization of D with the above properties, and let A_2B_2 denote any other factorization of D with the above properties. We will show that there is only one possibility for A_2, B_2. Let X_1, Y_1, X_2, Y_2 denote corresponding integer solutions to $B_iX_i^2 - A_iY_i^2 = 3$, and for $i = 1, 2$ put

$$\alpha_i = X_i\sqrt{B_i} + Y_i\sqrt{A_i}$$

and

$$\beta_i = \alpha_i^2 = V_i + W_i\sqrt{D}.$$

By mimicking the proof of Theorem 110 on p.208 of [8], we find that, up to sign,

$$\beta_2 = \epsilon_D^t\beta_1, \tag{7}$$

for some integer t. If t is even, then it is trivial to check that $B_1 = B_2$ and $A_1 = A_2$. Therefore, assume that t is odd. Let $\tau = a\sqrt{R} + b\sqrt{S}$ be as described in Lemma 2.1, that is, $\tau^2 = \epsilon_D$. We will prove the lemma only in the case that the value $c = 1$, as this is the only case required in the application of this lemma, and the proof for the case $c = 2$ is very similar. It follows from (7) that

$$\alpha_2 = \tau^t\alpha_1.$$

Therefore, since A_1, A_2, B_1, B_2, R, S are all squarefree, it is not difficult to check that

$$B_2 = B_1R/(B_1, R)^2,\ A_2 = B_1S/(B_1, S)^2.$$

In other words, B_2 and A_2 are completely determined once D and B_1, A_1 are fixed. $\square$

Returning to the proof of the main theorem, we see that

$$(x-3)/2 = Au^2, (x-1)/2 = r_1u_1^2, (x+1)/2 = r_2u_2^2$$

are three consecutive integers with prescribed quadratic type in terms of their factorizations. By a theorem of Bennett in [1], for each fixed triple (A, r_1, r_2) there is at most one solution in integers (u, u_1, u_2). As argued above, for fixed r, s as in (4), there is only one choice for r_1, one choice for r_2, and two choices for A. Since r and s are completely determined by d, it follows that for a fixed d in the statement of the theorem, there are at most two odd indices i for which T_i is of the form x^2+x-1.

To complete the proof of the theorem, we must show that for d sufficiently large, there is at most one odd index i for which equation (2) holds. As noted earlier, an integer solution to equation (2) leads to a factorization $d=rs$, and positive integers x, y, z satisfying equation (4). We remark that if $r=1$, then the main result of [12] shows that (4) has at most one solution, thus we may assume that r is a squarefree positive integer greater than 1.

Assume that equation (4) is solvable in positive integers, and let x_1, y_1, z_1 denote the smallest such solution. Let x_2, y_2, z_2 denote another solution to (4) in positive integers. Standard arguments, similar to those given in [12, Lemma 2.1-2.3], and using the fact that $r>1$ and squarefree, show that $x_2/x_1, y_2/y_1, z_2/z_1$ are all odd integers. Let $m=ry_1^2$ and put

$$\alpha=\sqrt{m}+\sqrt{m-1}, \quad \beta=\sqrt{8m+1}+\sqrt{8m}.$$

It follows that there are odd positive integers $t>1$ and $s>1$ for which

$$y_2\sqrt{r}+z_2\sqrt{s}=\alpha^t, \quad x_2+y_2\sqrt{8r}=\beta^s.$$

It follows that

$$y_2/y_1=\frac{\alpha^t+\alpha^{-t}}{\alpha+\alpha^{-1}}=\frac{\beta^s-\beta^{-s}}{\beta-\beta^{-1}}, \tag{8}$$

and as $\alpha+\alpha^{-1}=2\sqrt{m}$ and $\beta-\beta^{-1}=4\sqrt{2m}$, it is readily deduced that $t>s$.

Furthermore, it is easy to prove by induction that for s, t odd, the coefficient of $\sqrt{m}$ in α^t is congruent to $(-1)^{(t-1)/2}t$ modulo m, and the coefficient of $\sqrt{8m}$ in β^s is congruent to s modulo m. Therefore, since this coefficient is precisely y_2/y_1, we have that

$$y_2/y_1\equiv(-1)^{(t-1)/2}t\equiv s \pmod{m},$$

and hence that m divides $t\pm s$. Consequently, the fact that $t>s$ implies that $t>(m+1)/2$.

Now using equation (8) again, we deduce that

$$\frac{\beta^s}{2\sqrt{2}\alpha^t}-1=\frac{\beta^{-s}+2\sqrt{2}\alpha^{-t}}{2\sqrt{2}\alpha^t}<\frac{1}{\alpha^t}.$$

Define $z=s\log\beta-t\log\alpha-\log(2\sqrt{2})$, then $z>0$ by the above, and moreover, since $e^z-1>z$, we find that

$$0<s\log\beta-t\log\alpha-\log(2\sqrt{2})<\alpha^{-t}.$$

Quantitative results on estimates for linear forms in three logarithms of algebraic numbers (for example see [6]), show that

$$z>\exp(-c_1\log H(\alpha)\log H(\beta)\log t), \tag{9}$$

where c_1 is an absolute positive constant, and $H(\alpha) \geq 3, H(\beta) \geq 3$ are upper bounds for the height of the minimal polynomials of α and β respectively. These polynomials are given explicitly by

$$(X^2 - 1)^2 = 4mX \text{ and } (X^2 + 1)^2 = 4(4m + 1)X,$$

and hence we see that $H(\alpha) = H(\beta) = 4(4m + 1)$. Therefore, equation (9) shows that

$$t \log \alpha \leq -\log z \leq c_1 (\log(4(4m + 1)))^2 \log t.$$

Using the fact that $t \geq (m + 1)/2$, and the definition of α, it follows that m is absolutely bounded. Since both r and s are bounded by m, we see that $d = rs$ is also absolutely bounded.

References

[1] M.A. Bennett, *On consecutive integers of the form* ax^2, by^2, cz^2, Acta Arith. **88** (1999), 363-370.

[2] J.H.E. Cohn, *The Diophantine equation* $x^4 - Dy^2 = 1$ *II*, Acta Arith. **78** (1997), 401-403.

[3] P. Erdös and R.L. Graham, Old and New Problems and Results in Combinatorial Number Theory, Monograph Enseign. Math. **28**, Geneva, 1980.

[4] D.H. Lehmer, *An extended theory of Lucas functions*, Ann. Math. **31** (1930), 419-448.

[5] W. Ljunggren, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturv. **45** (1942), 61-70.

[6] E.M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Math. **64** (2000), 1217-1269.

[7] T. Nagell, *On a special class of Diophantine equations of the second degree,* Ark. Math. **3** (1954), 51-65.

[8] T. Nagell, Introduction to Number Theory (2nd ed.), Chelsea, New York, 1964.

[9] I. Nemes and A. Pethö, *Polynomial values in linear recurrences II*, J. Number Theory **24** (1986), 47-53.

[10] T.N. Shorey and C.L. Stewart, *On the diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$ *and pure powers in recurrence sequences*, Math. Scand. **52** (1983), 24-36.

[11] M. Ulas, *On products of disjoint blocks of consecutive integers*, L'Enseignement Math. **51** (2005), 331-334.

[12] P. Yuan, *On the number of solutions of* $x^2 - 4m(m + 1)y^2 = y^2 - bz^2 = 1$, Proc. A.M.S. **132** (2004), 1561-1566.

F. Luca
Instituto de Matemáticas UNAM
Campus Morelia
Ap. Postal 61-3 Xangari
CP 58 089
Morelia, Michoacan
México
E-mail: fluca@matmor.unam.mx

P. G. Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario
Canada K1N 6N5
E-mail: gwalsh@mathstat.uottawa.ca

Received: 5.3.1007.