Publ. Math. Debrecen
67/1-2 (2005), 103–113

Members of binary recurrences on lines of the Pascal triangle

By FLORIAN LUCA (Morelia) and FRANCESCO PAPPALARDI (Roma)

Abstract. In this paper, we look at a diophantine equation of the form $u_n = \binom{x}{y}$, where $(u_n)_{n\geq 0}$ is a binary recurrent sequence of integers. We show that if the pair of integers (x, y) belongs to a fixed line of the Pascal triangle, then the above equation has only finitely many positive integer solutions (n, x, y).

A *binary recurrent sequence* of integers $(u_n)_{n\geq 0}$ has $u_0, u_1 \in \mathbb{Z}$ and satisfies the recurrence

$$u_{n+2} = ru_{n+1} + su_n \tag{1}$$

for all $n \geq 0$, where r and s are some fixed nonzero integers such that the quadratic equation

$$\lambda^2 - r\lambda - s = 0$$

has two distinct nonzero roots α and β. In this case, the formula

$$u_n = c\alpha^n + d\beta^n \tag{2}$$

holds for all $n \geq 0$, with some constants c and d which can be computed in terms of u_0, u_1, α and β, and they belong to the field $\mathbb{K} := \mathbb{Q}[\alpha]$.

The sequence $(u_n)_{n\geq 0}$ is called *nondegenerate* if $cd \neq 0$ and α/β is not a root of 1. When $u_0 = 0,\ u_1 = 1$ the sequence is called a *Lucas sequence*.

Mathematics Subject Classification: 11B39, 11D72.
Key words and phrases: binary recurrences, binomial coefficients.

In order to keep the presentation of the paper simple, we shall assume that the polynomial $X^2 - rX - s$ is reducible over $\mathbb{Q}$. In this case, $a := \alpha$ and $b := \beta$ are nonzero integers, and therefore

$$u_n = ca^n + db^n \tag{3}$$

holds for all nonnegative integers n. Here, c and d are rational numbers. The fact that $(u_n)_{n\geq 0}$ is nondegenerate is equivalent to the fact that $a \neq \pm b$, and that $abcd \neq 0$.

In this note, we investigate a particular instance of the diophantine equation

$$u_n = \binom{m}{k}. \tag{4}$$

Other particular instances of equation (4) above have been investigated in [3] (with a Lucas sequence $(u_n)_{n\geq 0}$ and k either fixed or a prime number) and in [9] (for $k = 3$). We set forward the following:

Conjecture. *Equation* (4) *has only finitely many solutions* (n, m, k) *with* $4 \leq k \leq m/2$.

In this note, we fix a line $\mathcal{L}$ in the Cartesian plane $\mathbb{R}^2$ (where $\mathbb{R}$ stands for the real numbers) and we look at the diophantine equation

$$|u_n| = \binom{x}{y} \quad \text{for } (x, y) \in \mathcal{L}. \tag{5}$$

Our main purpose is to decide whether equation (5) above has only finitely or infinitely many positive integer solutions (n, x, y) with $(x, y) \in \mathcal{L}$.

First of all, note that if $\mathcal{L}$ is the x axis; i.e., the equation of $\mathcal{L}$ is $y = 0$, then equation (5) has infinitely many solutions (n, x) if there exists n_0 such that $|u_{n_0}| = 1$, and none otherwise. If the equation of $\mathcal{L}$ is $y = 1$, then equation (5) has again infinitely many solutions (n, x). Finally, if $\mathcal{L}$ is a vertical line of equation $y = k$ for some integer $k \geq 2$, then equation (5) is of the type

$$u_n = \frac{1}{k!} \cdot x(x-1) \cdot \ldots \cdot (x-k+1), \tag{6}$$

in positive integers (n, x). Note that the right hand side of equation (6) above is a polynomial in x. In this case, one can use the methods of

Corvaja and Zannier from [2] to show that equation (6) above has only finitely many solutions (n, x) when $k \geq 4$ and that the same is true when $k \in \{2, 3\}$ with finitely many exceptional parametric families of quadruples (a, b, c, d), all explicitly computable (see, for example, [3] and [7]).

In what follows, we will consider only the more interesting case, namely when $\mathcal{L}$ is not vertical. If $\mathcal{L}$ has negative slope, then $\mathcal{L}$ contains only finitely many pairs of positive integers (x, y), and therefore equation (5) has at most finitely many solutions. Thus, we may assume that $\mathcal{L}$ has positive slope, and since

$$\binom{x}{y} = 0 \quad \text{when } y > x,$$

we may assume that the slope of $\mathcal{L}$ is $\lambda \leq 1$. Finally, since

$$\binom{x}{y} = \binom{x}{x-y},$$

and since the points $(x, x-y)$ for $(x, y) \in \mathcal{L}$ form a line $\mathcal{L}_1$ of slope λ_1 and such that

$$\lambda + \lambda_1 = \frac{y}{x} + \frac{x-y}{x} = 1,$$

it follows that we may assume, up to interchanging $\mathcal{L}$ with $\mathcal{L}_1$ if needed, that $0 < \lambda \leq 1/2$.

We have the following theorem.

Theorem. *Let $\mathcal{L}$ be a line in the Cartesian $\mathbb{R}^2$ plane of slope $0 < \lambda \leq 1/2$. Then the diophantine equation*

$$|u_n| = \binom{x}{y} \quad (x, y) \in \mathcal{L}, \tag{7}$$

admits only finitely many positive integer solutions (n, x, y), with $(x, y) \in \mathcal{L}$.

We make a few remarks before proceeding to the proof of our theorem. The first remark is that our proof is completely effective, in the sense that all positive integer solutions (n, x, y) of equation (7) can be computed in terms of the data $(u_n)_{n \geq 0}$ and $\mathcal{L}$.

Secondly, the same theorem as above holds if we perturb the right hand side of (7) by a multiplicative factor which is a rational number

whose naïve height is at most polynomial in $\max\{x, y\}$. For example, the same argument as in the proof of our theorem shows that the equation

$$|u_n| = \frac{1}{m+1}\binom{2m}{m}$$

has only finitely many positive integer solutions (n, m). In particular, a nondegenerate binary recurrent sequence with integral roots contains only finitely many *Catalan numbers*. The above equation for the sequence of the Fibonacci numbers $(F_n)_{n\geq 0}$ given by $F_0 = 0,\ F_1 = 1$ which satisfies recurrence (1) with $(r, s) = (1, 1)$ has been considered in [8], where it is shown that its largest solution is $F_5 = \frac{1}{3+1}\binom{6}{3}$.

Finally, we remark that the above theorem holds *for all* nondegenerate binary recurrent sequences $(u_n)_{n\geq 0}$, and not only for those whose *roots* are integers. A proof of this more general result can be obtained by following the argument of the present proof of our theorem together with a few minor modifications, such as an extension of the lemma below to quadratic number fields, together with the properties of primitive divisors of sequences $(u_n)_{\geq 0}$ given by formula (2) and for which c/d and α/β are multiplicatively independent (see [6], for example). We have chosen to formulate and prove our main result in this more particular form just in order to keep the presentation of the paper simple.

Throughout the following proof, we use the Vinogradov symbols $\gg$ and $\ll$ and the Landau symbols O and o with their usual meanings. We shall also use $c_1,\ c_2\ \ldots$ for computable constants which are either absolute or depend on the initial data and which are labeled increasingly throughout the proof.

Proof of the Theorem. By replacing the binary recurrence $(u_n)_{n\geq 0}$ by the two subsequences $(u_{2n})_{n\geq 0}$ and $(u_{2n+1})_{n\geq 0}$, it follows that we may assume that both a and b are positive. We may also assume that $\mathcal{L}$ contains at least two points (x_1, y_1) and (x_2, y_2) with positive integer coordinates, for otherwise there is nothing to prove. In this case, the equation of $\mathcal{L}$ is of the form

$$x = \frac{ey + f_1}{g}, \tag{8}$$

where $e \geq 2g$ (because of the overriding assumption on the slope) are positive integers and f_1 is some integer. Since $\mathcal{L}$ contains at least two points (x, y) with positive integer coordinates, there exists an integer h such that if $y \equiv h \pmod{g}$, then $ey + f_1 \equiv 0 \pmod{g}$. Thus, with $y := gm + h$, we have

$$\begin{aligned} x &= \frac{ey + f_1}{g} = \frac{e(gm + h) + f_1}{g} = em + \frac{eh + f_1}{g} \\ &= em + f, \end{aligned} \tag{9}$$

where we write $f := (eh + f_1)/g \in \mathbb{Z}$. The class h modulo g above may not be uniquely determined, but all integer points (x, y) in $\mathcal{L}$ arise in this way; i.e., have the property that $y \equiv h \pmod{g}$ holds with some h such that $eh + f_1$ is a multiple of g. Note that if e and g are coprime, then the class of h modulo g is uniquely determined.

We now assume that equation (7) has infinitely many positive integer solutions (n, x, y) with $(x, y) \in \mathcal{L}$. Since h can take only finitely many values, we may assume that h, hence, f too, are fixed. In this case,

$$\begin{aligned} \binom{x}{y} &= \binom{em + f}{gm + h} \\ &= \frac{1}{(gm + h)!}(em + f)(em + f - 1) \cdot \ldots \cdot ((e - g)m + (f - h + 1)). \end{aligned} \tag{10}$$

Let $c_1 := e - g$ and $c_2 := e$. Note that there exists a constant c_3 such that for large m, all prime numbers p in the interval $[c_1 m, c_2 m]$ divide the integer shown at (10) with at most c_3 exceptions (this is because $e - g \geq g$).

At this point, we recall the Chebotarev Density Theorem (see for example [4]) that in a weak form can be stated as follows:

Chebotarev Density Theorem. *Let $\mathbb{L}/\mathbb{Q}$ be a Galois extension and let $\mathcal{C} \subset \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ be a union of conjugation classes. Then the set of rational primes p for which the Artin symbol $\sigma_p \in \mathcal{C}$ has natural density $\#\mathcal{C}/[\mathbb{L} : \mathbb{Q}]$.*

We recall that, with the notation of the above theorem, the Artin symbol σ_p of a rational prime p which is unramified in $\mathbb{L}/\mathbb{Q}$ is defined as

the set of the elements of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ that map into the Frobenius element over some residue field at p.

Using the above form of the Chebotarev Density Theorem, we prove the following Lemma:

Lemma. *Let γ and δ be fixed nonzero rational numbers and c_1, c_2, c_3 positive real numbers with $c_1 < c_2$. Assume that there exists a sequence $(x_k)_{k\ge 0}$ of real numbers diverging to infinity such that for each $k \ge 0$, the congruence $\gamma^y \equiv \delta \pmod p$ admits a solution $y := y_p$ for all prime numbers p in the interval $\mathcal{I}_k := [c_1 x_k, c_2 x_k]$ with at most c_3 exceptions. Then γ and δ are multiplicatively dependent.*

A criterion due to Dedekind states that given $\alpha \in \mathbb{Q}^*$ and a prime p that does not divide either the numerator or the denominator of α, a rational prime l verifies the two congruences

$$\begin{cases} p \equiv 1 \pmod l; \\ \alpha^{\frac{p-1}{l}} \equiv 1 \pmod p, \end{cases}$$

(i.e. $l \mid [\mathbb{F}_p^* : \langle \alpha \pmod p \rangle]$) if and only if the prime p splits completely as the product of degree one prime ideals in $\mathbb{Q}[\zeta_l, \alpha^{1/l}]/\mathbb{Q}$, where $\zeta_l = e^{2\pi i/l}$. This is also equivalent to the property that the Artin symbol σ_p is the conjugation class of the identity element in $\mathrm{Gal}(\mathbb{Q}[\zeta_l, \alpha^{1/l}]/\mathbb{Q})$.

Proof of the Lemma. Assume that γ and δ are multiplicatively independent and consider the Galois extension of $\mathbb{Q}$

$$\mathbb{L} = \mathbb{Q}(\zeta_l, \gamma^{1/l}, \delta^{1/l}),$$

where $\zeta_l = e^{2\pi i/l}$. We claim that we can choose the odd prime l in such a way that

$$\#\,\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\zeta_l)) = [\mathbb{L} : \mathbb{Q}(\zeta_l)] = l^2.$$

Indeed from Kummer Theory (see Lang [5], Theorem 13 on page 219), we know that if $\Gamma \subset \mathbb{Q}^*$ is the multiplicative group generated by γ and δ, then

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\zeta_l)) \cong \Gamma\mathbb{Q}^{*l}/\mathbb{Q}^{*l} \cong \Gamma/\Gamma \cap \mathbb{Q}^{*l}.$$

So it is enough to choose any odd l such that $\Gamma \cap \mathbb{Q}^{*l} = \Gamma^l$.

Next consider the subset $\mathcal{C}$ of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ of those elements σ that satisfy the following two conditions

$$\begin{cases} \sigma\mid_{\mathbb{Q}(\zeta_l,\gamma^{1/l})} = \mathrm{Id}; \\ \sigma\mid_{\mathbb{Q}(\zeta_l,\delta^{1/l})} \neq \mathrm{Id}. \end{cases}$$

It is clear that $\mathcal{C}$ closed under conjugation and it is a proper subset of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.

The Chebotarev Density Theorem assures that the set of primes p for which the Artin symbol $\sigma_p \in \mathcal{C}$ has positive density.

Furthermore, $\sigma_p \in \mathcal{C}$ is equivalent to

$$\begin{cases} p \equiv 1 \pmod{l}; \\ \gamma^{\frac{p-1}{l}} \equiv 1 \pmod{p}; \\ \delta^{\frac{p-1}{l}} \not\equiv 1 \pmod{p}. \end{cases}$$

If k is large enough, there exist more than c_3 primes $p_0 \in \mathcal{I}_k$ with $\sigma_{p_0} \in \mathcal{C}$.

By construction, $l \equiv 1 \pmod{p_0}$, l divides the index $[\mathbb{F}_{p_0}^* : \langle \gamma \pmod{p_0}\rangle]$, but l does not divide the index $[\mathbb{F}_{p_0}^* : \langle \delta \pmod{p_0}\rangle]$. Hence, $\langle \delta \pmod{p_0}\rangle$ is not contained in $\langle \gamma \pmod{p_0}\rangle$ and the congruence $\gamma^y \equiv \delta \pmod{p_0}$ cannot hold for any y. This concludes the proof of the Lemma.

We now return to the proof of our theorem.

We note that whenever

$$|u_n| = \binom{x}{y} \tag{11}$$

holds with the binomial coefficient appearing in (11) above being the one shown in (10), we have that $p \mid u_n$ for all $p \in [c_1 m, c_2 m]$ with at most c_3 exceptions provided that m is large enough. In turn, when m is large, say larger than the maximum of $|a|$, $|b|$, and the denominators of c and d, the above congruence implies that

$$\gamma^n \equiv \delta \pmod{p} \tag{12}$$

holds with $\gamma := a/b$ and $\delta := -d/c$. Thus, assuming that equation (7) has infinitely many solutions, we get that equation (12) admits a solution

n for all primes $p \in [c_1 m, c_2 m]$ except possibly at most c_3 of those, and that this holds for infinitely many positive integers m. With the Lemma, we get that $-c/d$ and a/b are multiplicatively dependent. Thus, there exists a rational number ρ and integers u and v such that $-c/d = \pm\rho^u$ and $a/b = \rho^v$. We may certainly assume that $a > b$; hence $\rho > 1$, therefore that $v > 0$. Writing $\rho := a_1/b_1$, where a_1 and b_1 are coprime and $b_1 > 0$, we get

$$\begin{aligned} u_n &= -db^n \left(\left(\frac{-c}{d} \right) \cdot \left(\frac{a}{b} \right)^n - 1 \right) \\ &= \mp \frac{d}{b_1^u} \cdot \left(\frac{b}{b_1^v} \right)^n \cdot (a_1^{nv+u} \mp b_1^{nv+u}), \end{aligned} \tag{13}$$

and it is is easy to see from (13) together with the fact that u_n is an integer for all $n \geq 0$, that there must exist a rational number $d_1 > 0$, and an integer $a_2 \geq 1$, such that

$$|u_n| = d_1 a_2^n |a_1^{nv+u} \mp b_1^{nv+u}|.$$

Thus, it remains to investigate the diophantine equation

$$d_1 a_2^n |a_1^{nv+u} \mp b_1^{nv+u}| = \binom{em+f}{gm+h}.$$

We first use size arguments. By Stirling's formula, it follows easily that

$$\binom{em+f}{gm+h} = \exp\left(m(1+o(1)) \left(e \log e - g \log g - (e-g) \log(e-g) \right) \right),$$

and therefore we can say that the inequalities

$$c_4 m \leq \log \binom{em+f}{gm+h} \leq c_5 m$$

hold with some computable constants c_4 and c_5 and for all sufficiently large m. On the other hand, it is clear that the inequalities

$$c_6 n \leq \log\Big(d_1 a_2^n |a_1^{nv+u} \mp b_1^{nv+u}| \Big) \leq c_7 n$$

hold for all sufficiently large n with some computable positive constants c_6 and c_7. Thus, it follows that both inequalities

$$n \leq c_8 m \quad \text{and} \quad m \leq c_9 n$$

hold for large m and n with some computable positive constants c_8 and c_9.

Let $n_1 := nv + u$. We may assume that $n_1 > 12$. We treat only the case in which $|u_n| = d_1 a_2^n |a_1^{n_1} - b_1^{n_1}|$ as the case of the $+$ sign is entirely similar. From the divisibility properties of the sequence $a_1^{n_1} - b_1^{n_1}$, it follows that for large n_1, there exist prime factors p of it which are congruent to 1 modulo n_1. In fact, from a result from CARMICHAEL's paper [1], we know that if we write

$$a_1^{n_1} - b_1^{n_1} = M = \prod_{p^{\alpha_p} \| M} p^{\alpha_p},$$

then

$$\prod_{\substack{p^{\alpha_p} \| M \\ p \equiv 1 \,(\mathrm{mod}\, n_1)}} p^{\alpha_p} \geq \frac{1}{n_1} \prod_{\substack{1 \leq k \leq n_1 \\ \gcd(k, n_1) = 1}} (a_1 - e^{\frac{2\pi i k}{n_1}} b_1)$$

$$\geq \exp\bigl(c_{10}\bigl(\phi(n_1) - \tau(n_1) - \log n_1\bigr)\bigr),$$

where c_{10} can be taken to be $\max(\log|a_1|, \log|b_1|)$ and $\phi(n_1)$ and $\tau(n_1)$ are the Euler function and the number of divisors of n_1, respectively. For large n, the inequalities

$$\phi(n_1) - \tau(n_1) - \log n_1 \gg \frac{n_1}{\log\log n_1}$$

$$\gg \frac{n}{\log\log n} \gg \frac{m}{\log\log m}$$

hold, and therefore we can say that the inequality

$$\prod_{\substack{p^{\alpha_p} \| M \\ p \equiv 1 \,(\mathrm{mod}\, n_1)}} p^{\alpha_p} \geq \exp\left(\frac{c_{11} m}{\log\log m}\right) \tag{14}$$

holds for large values of n with some appropriate positive constant c_{11}.

Let t be the number of prime factors $p \equiv 1 \pmod{n_1}$ of the number M. Every such prime is of the form $1 + \ell n_1$ for some ℓ. Since this prime must also divide $(em+f)!$, and $n_1 \gg n \gg m$, it follows that $\ell \ll 1$. In particular, $t \ll 1$. The same argument shows that $\alpha_p \ll 1$ holds for each one of these primes, therefore the inequality

$$\sum_{\substack{p^{\alpha_p} \| M \\ p \equiv 1 \,(\mathrm{mod}\, n_1)}} \alpha_p \leq c_{12}$$

holds with some appropriate positive constant c_{12}. In particular,

$$\prod_{\substack{p^{\alpha_p} \| M \\ p \equiv 1 \,(\mathrm{mod}\, n_1)}} p^{\alpha_p} \le (em+f)^{c_{12}}. \tag{15}$$

Comparing (14) with (15), we get

$$(em+f)^{c_{12}} \ge \exp\left(\frac{c_{11} m}{\log\log m}\right),$$

which is equivalent to

$$c_{12} \log(em+f) \ge \frac{c_{11} m}{\log\log m},$$

which certainly can have only finitely many positive integer solutions m.

This contradiction completes the proof of the Theorem.

Acknowledgements. We thank the anonymous referee for suggestions which improved the presentation of this paper. This work was done when the first author visited the Department of Mathematics at the Università Roma Tre in August 2003. The project was funded under the Italian Mexican Agreement of Scientific and Technological cooperation 2003–2005: *Kleinian Groups and Egyptian Fractions*.

References

[1] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. Math.* (2) **15** (1913), 30–70.

[2] P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Math. (N.S.)* **9**, no. 3 (1998), 317–332.

[3] A. Flammenkamp and F. Luca, Binomial coefficients and Lucas sequences, *J. Number Theory* **93**, no. 2 (2002), 246–284.

[4] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem, Algebraic number fields: L-functions and Galois properties, Proc. Sympos., Univ. Durham, Durham, 1975, *Academic Press*, *London*, 1977, 409–464.

[5] S. Lang, Algebra, Second edition, *Addison-Wesley Publishing Company*, Advanced Book Program, *Reading*, *MA*, 1984.

[6] F. Luca, Arithmetic properties of members of a binary recurrent sequence, *Acta Arith.* **109**, no. 1 (2003), 81–107.

[7] F. Luca, Fibonacci numbers, Lucas numbers, and orders of finite simple groups, *JP Journal of Algebra and Number Theory* **4**, no. 1 (2004), 23–54.

[8] F. Luca, Proposed Problem H-599, Advanced Problem Section, *Fibonacci Quart* **41**, no. 3 (2003), *Solution in Fibonacci Quart.* **42**, no. 3 (2004).

[9] L. Szalay, On the resolution of the equations $U_n = \binom{x}{3}$ and $V_n = \binom{x}{3}$, *Fibonacci Quart* **40**, no. 1 (9–12).

FLORIAN LUCA
MATHEMATICAL INSTITUTE
UNAM
AP. POSTAL 61-3 (XANGARI) CP 58 089
MORELIA, MICHOACÁN
MEXICO

E-mail: fluca@matmor.unam.mx

FRANCESCO PAPPALARDI
DIPARTAMENTO DI MATEMATICA
UNIVERSITÀ ROMA TRE
LAGO S.L. MURIALDO 1, ROMA 00146
ITALY

E-mail: pappa@mat.uniroma3.it

(Received September 23, 2003; revised May 28, 2004)