How a simple question on the Fibonacci sequence lead the authors to a number-theroretical promenade

J.-P. Allouche
CNRS, IMJ-PRG
Sorbonne Université
4 Place Jussieu
F-75252 Paris Cedex 05 France
jean-paul.allouche@imj-prg.fr

G. Pirillo
Dipartimento di Matematica ed Informatica U. Dini
Università di Firenze
Viale Morgagni 67/A
50134 Firenze Italia
pirillo@math.unifi.it

L. Vannucci
Dipartimento di Statistica, Informatica e Applicazioni "G. Parenti"
Università di Firenze
Viale Morgagni 59
50134 Firenze Italia
luigi.vannucci@unifi.it

Abstract

The Fibonacci sequence $(F_n)_{n\geq 0}$ is defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Looking at one of the numerous properties of this well-known sequence of integers leads to a promenade in number theory. We ask several questions that either have already known answers, or else that provide –not necessarily new– open problems. En route, we find the set of integers that can be written as $b^2 + ab - a^2$ for some integers a, b: they can be characterized using the general theory of binary integer quadratic forms, but we offer an elementary proof of this characterization.

1 Introduction

Research in mathematics frequently involves asking questions on, e.g., generalizations of known results. Sometimes the questions appear to be not new, sometimes they are new; in all cases they can lead to rewarding answers, or they can be difficult and remain open problems. The history of someone's research, including success and failure, is rarely written down in published papers, with some notable exceptions, such as [5] where "*the authors are especially interested in highlighting some of the stances that mathematicians take in the middle of their work*", and the column *Trip to the proof* in the journal *Nieuw Archief voor Wiskunde.* We would like here to explain how, starting from a "simple" question, we tried to extend our investigations, arriving, after a promenade in number theory, to actual, "elementary looking", but sometimes still open, questions.

A large number of papers deal with the Fibonacci sequence $(F_n)_{n\geq 0}$,

$$(F_n)_{n\geq 0} = 0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ldots,$$

its numerous properties, and its many generalizations. Among these properties, let us recall the Simson-Cassini identity:

$$\forall n \geq 1, \quad F_{n+1}F_{n-1} - F_n^2 = (-1)^n. \tag{1}$$

One of us recently asked a "simple looking" question on this sequence, namely: *how to generalize the Simson-Cassini identity?* A first suggestion was to change the initial values of the Fibonacci sequence, and to define a sequence $(H_n)_{n\geq 0}$ by $H_0 = b$, $H_1 = a$, and $H_{n+2} = H_{n+1} + H_n$ for all $n \geq 0$, where a and b are two given integers. Several computer tests seemed to confirm that

$$\forall n \geq 1, \quad H_{n+1}H_{n-1} - H_n^2 = (-1)^{n+1}A(a,b) \tag{2}$$

where $A(a,b)$ only depends on a and b. Furthermore, experiments yielded $A(a,b) = b^2 + ab - a^2$. Of course, once stated, this identity can be proved, e.g., by induction on n. But we found it plausible that this general identity was already known. This was indeed the case, as indicated in the next section. We decided to continue looking at Identity (2): we found unexpected links that we would like to give here, as an example of how a simple question can lead to not-that-simple subjects and possibly complicated (sometimes even still unsolved) questions. Before continuing, we would make a remark on $A(a,b)$ and the Fibonacci numbers.

Remark 1.1 The quantity $A(a,b)$ was shown to be related to the Fibonacci numbers in the paper [16] where the author proposes his thesis that the incommensurability of the hypotenuse and another side of an isosceles right angle triangle was discovered by the Pythagorean School at almost the same time as the incommensurability of the diagonal and side of a regular pentagon (in other words the facts that $\sqrt{2}$ and $(1+\sqrt{5})/2$ are irrational were proved at about the same time). Furthermore, the author of [16] gives "*an argument that shows how the Fibonacci numbers and the Cassini identity appeared naturally during the development of the argument of the incommensurability*". In particular he proves that, when trying to make $|b(b+a)-a^2|$ (namely equal to 1) as small as possible (with a and b integers), the Fibonacci numbers will pop up as the increasing values of a. This actually gives a characterization of the Fibonacci numbers.

2 A paper by Y. Soykan

Trying to find Identity (2) in the literature, we came across a quite recent paper [19] where the author is interested in the "Generalized m-step Fibonacci numbers" $(V_n)_{n\geq 0}$ defined, for $m \geq 2$, for coefficients $r_1, r_2, \ldots, r_m$ (with $r_m \neq 0$), and for initial values $V_0, V_1, \ldots, V_{m-1}$, by the recurrence relation

$$\forall n \geq m, \quad V_n = \sum_{1\leq i\leq m} r_i V_{n-i}. \tag{3}$$

This sequence is extended to negative indices by the formula

$$V_{-n} = -\frac{r_{m-1}}{r_m}V_{-(n-1)} - \frac{r_{m-2}}{r_m}V_{-(n-2)} - \frac{r_{m-3}}{r_m}V_{-(n-3)} - \cdots \\ - \frac{r_1}{r_m}V_{-(n-(m-1))} + \frac{1}{r_m}V_{-(n-m)}$$

for $n = 1, 2, \ldots$, so that the recurrence relation in (3) now holds for all $n \in \mathbb{Z}$. Soykan gives a nice determinantal formula that subsumes several previous results including the generalization of Simson-Cassini's identity above. (Note that, as indicated in [19], a relation, more general than Identity (2), was already given in a paper of Horadam [12].) With the notation above, Soykan's result reads:

Theorem 2.1 (Soykan) *For $m \geq 2$, define $f(n)$ by*

$$f(n) = \begin{vmatrix} V_{n+m-1} & V_{n+m-2} & V_{n+m-3} & \cdots & V_{n+2} & V_{n+1} & V_n \\ V_{n+m-2} & V_{n+m-3} & V_{n+m-4} & \cdots & V_{n+1} & V_n & V_{n-1} \\ V_{n+m-3} & V_{n+m-4} & V_{n+m-5} & \cdots & V_n & V_{n-1} & V_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ V_{n+2} & V_{n+1} & V_n & \cdots & V_{n-m+5} & V_{n-m+4} & V_{n-m+3} \\ V_{n+1} & V_n & V_{n-1} & \cdots & V_{n-m+4} & V_{n-m+3} & V_{n-m+2} \\ V_n & V_{n-1} & V_{n-2} & \cdots & V_{n-m+3} & V_{n-m+2} & V_{n-m+1} \end{vmatrix}.$$

Then

$$f(n) = y(n) r_m^n f(0)$$

where $y(n) = 1$ if m is odd, and $y(n) = (-1)^n$ if m is even.

This first step shows that some subjects (typically studying the Fibonacci sequence) are both "dangerous" (i.e., the literature is so vast that most of the questions that one can imagine of have already been answered) and challenging (after all, new original results appear from time to time).

3 The set of values attained by the quantities $A(a,b)$

The next question that may come to mind is about $A(a,b) = b^2 + ab - a^2$ occurring in Identity (2), namely:

$$\textit{what is the set } \mathcal{S} = \{n,\ \exists a,b \text{ integers},\ n = A(a,b)\}\,?$$

A first approach shows that certain values of the integer n can never be of the form $A(a,b)$ with a and b integers: the reader can prove as an exercise that, e.g., no integer equal to twice an odd number can be written as $b^2 + ab - a^2$. Actually there is a necessary and sufficient condition for an integer to belong to the set $\mathcal{S}$:

Proposition 3.1 *An integer n belongs to the set $\mathcal{S}$ defined above if and only if all its prime factors congruent to 2 or 3 modulo 5 occur with even exponents in the decomposition of $|n| = \prod p_j^{a_j}$ with p_j prime and $a_j \geq 1$.*

Remark 3.2 We have $\mathcal{S} = \{0, \pm 1, \pm 4, \pm 5, \pm 9, \pm 11, \pm 16, \pm 19, \pm 20, \pm 25, \ldots\}$. The positive elements in $\mathcal{S}$ are $1, 4, 5, 9, 11, 16, 19, 20, 25, \ldots$, that is sequence A031363 in the OEIS [15]. Note that this sequence also occurs in physics for questions related to quasicrystals (see [1] and references therein).

Though Proposition 3.1 is a consequence of the classical theory of the representation of integers by binary integer quadratic forms, we offer an "elementary" proof in the Appendix at the end of this paper.

Remark 3.3 Given the geometric origin of the problem, one might consider that, in the expression $n = b^2 + ab - a^2$, the quantities a and b are lengths of the diagonal and side of a regular pentagon, hence are nonnegative. (We could say that the incommensurability of side and diagonal of the regular pentagon can also be expressed by saying that the binary quadratic form $b + ab - a^2$ cannot take the value 0, and therefore that the study of binary quadratic forms goes back to the Pythagoreans.) Thus $\mathcal{S}$ should be replaced with $\mathcal{S}_+ = \{n,\ \exists a,b \text{ nonnegative integers},\ n = A(a,b)\}$. The following lemma shows that we actually have $\mathcal{S}_+ = \mathcal{S}$.

Lemma 3.4 *An integer can be written $n = b^2 + ab - a^2$ with a, b integers, if and only if it can be written $n = b'^2 + a'b' - a'^2$ with a', b' nonnegative integers, in other words $\mathcal{S}_+ = \mathcal{S}$.*

Proof. It suffices to prove that $\mathcal{S} \subset \mathcal{S}_+$. First note that if $n = b^2 + ab - a^2$, then $-n = (-a)^2 + (-a)b - b^2$, hence we may suppose $n \geq 0$. So, let n be a nonnegative integer such that $0 \leq n = b^2 + ab - a^2$, with $a, b \in \mathbb{Z}$.

If a and b are both nonnegative or both nonpositive, then $0 \leq n = b^2 + ab - a^2 = |b|^2 + |a||b| - |a|^2$.

If $b < 0$ and $a \geq 0$, we can write $0 \leq n = b^2 + ab - a^2 = (-b)^2 + (-b)(a - b) - (a-b)^2$, where $(-b) > 0$ and clearly $a - b = a + (-b) \geq 0$.

If $a < 0$ and $b \geq 0$, we have $0 \leq n = b^2 + ab - a^2 \leq b^2 + ab = b(b+a)$, thus $b+a \geq 0$. Hence we can write $0 \leq n = b^2+ab-a^2 = (b+a)^2+(b+a)(-a)-(-a)^2$ with $(-a) > 0$ and $b + a \geq 0$. ☐

4 Pisot sequences

At this point, one of us remembered that something "related to Pisot numbers" had the same flavor as the Simpson-Cassini Identity, with inequalities instead of equalities. Indeed Boyd (see [2, 3]) studied the *Pisot sequences* introduced by Pisot [17] and defined by:

Let a_0, a_1 be two integers such that $a_1 \geq a_0 \geq 1$. Then $E(a_0, a_1)$ is the integer sequence $(a_n)_{n\geq 0}$ defined by $-1/2 < a_{n+2} - (a_{n+1})^2/a_n \leq 1/2$ for $n \geq 0$. This definition can also be written as $a_{n+2} = \lfloor a_{n+1}^2/a_n + 1/2 \rfloor$.

Note that generalized Pisot sequences $E_r(a_0, a_1)$ are defined in [4, 7] (also see the references therein), namely

Let r be a given real number. Let a_0, a_1 be two integers such that $a_1 > a_0 > 0$. The sequence of integers $E_r(a_0, a_1) = (a_n)_{n\geq 0}$ is defined by the nonlinear recurrence relation $a_{n+2} = \lfloor \frac{a_{n+1}^2}{a_n} + r \rfloor$.

The Fibonacci sequence is an example of a Pisot sequence. But Boyd [2, 3] proved that certain Pisot sequences satisfy no linear recurrence. He proposed several conjectures, among which we note: *is it true that, for almost all pairs (a_0, a_1), the sequence $E(a_0, a_1)$ satisfies no linear recurrence?* To the best of our knowledge this conjecture is still open. A recent interesting step torwards its proof was given in [7] with an automated procedure to check whether sequence $E(a_0, a_1)$ satisfies a linear recurrence for a given pair (a_0, a_1). The interest of this result is that it can happen that $E(a_0, a_1)$ satisfies a linear recurrence of higher order up to some large value of the index, but the recurrence breaks down eventually: the automated procedure detects such "fake" recurrences. The paper [7] also explains while these pseudo-recurrences (*Doppelgänger*) hold.

Our next question was to see whether Soykan's generalization of the Simson-Cassini Identity could provide a generalization of the Pisot sequences. Interestingly enough, a generalization of Pisot sequences is proposed in [7], where the sequence $(a_n)_{n\geq 0}$ is required to have the property that the determinant

$$\Delta_s = \begin{vmatrix} a_n & \cdots & a_{n+s} \\ a_{n+1} & \cdots & a_{n+s+1} \\ \vdots & \vdots & \vdots \\ a_{n+s} & \cdots & a_{n+2s} \end{vmatrix}$$

is “small” compared to a_n (of course this determinant is zero if $(a_n)_{n\geq 0}$ satisfies a linear recurrence of order s with constant coefficients). Note that this determinant is *precisely* $\pm f(N)$ where f is defined in Theorem 2.1 with $N = n+s$, $s = m-1$ (write rows and columns in reverse order).

5 More sequences and more number-theoretical allusions

Two more ideas or connections came to our mind. The first idea was whether one can imagine of an identity similar to (2), but with more terms. And indeed this had already been studied! For example, for the Fibonacci sequence $(F_n)_{n\geq 0}$, one has the Gelin-Cesàro Identity

$$\forall n \geq 2, \; F_{n-2}F_{n-1}F_{n+1}F_{n+2} - F_n^4 = -1.$$

According to [14] where other identities can be found, this identity dates back to 1880; it was stated by Gelin and proved by Cesàro. More references can be found in [19].

Last but not least, this tentative research lead us to discuss the famous *Somos sequences*. Recall that Somos-4 sequence $(a_n)_{n\geq 0}$ is defined by $a_0 = a_1 = a_2 = a_3 = 1$; and for $n \geq 4$,

$$a_n = (a_{n-1}a_{n-3} + a_{n-2}^2)/a_{n-4}.$$

The fact that a_n is rational for all n is clear, but what is surprising is that all the values of a_n are integers! More generally the Somos-k sequence is defined for $k \geq 1$ by $a_0 = a_1 = a_2 = \ldots = a_{k-1} = 1$, and for $n \geq k$,

$$a_n = \frac{1}{a_{n-k}} \sum_{j=1}^{\lfloor k/2 \rfloor} a_{n-j}a_{n-(k-j)}.$$

The Somos-2 and Somos-3 sequences are constant sequences equal to 1. Somos-k sequences have integer values for $k = 4, 5, 6, 7$ (see sequences A006720, A006721, A006722, A006723 in the OEIS [15]), but they do not give only integers for $k \geq 8$. The proofs are by no means easy (see, in particular, [13] and [8]). Note that these sequences and similar sequences are related to elliptic curves, elliptic divisibility sequences, cluster algebras, perfect matchings of certain bipartite planar graphs... For more on these sequences see, e.g., [9, 10] and the webpage [18]. We cannot end this paper without citing the nice paper [6], where the authors show how to construct Somos-like sequences, with non-linear recurrences: you know *in advance* that these sequences consist of integers only, but proving the statement directly without knowing the construction trick seems very difficult! (see, in particular, the Proposition on Page 857 of [6]).

6 Appendix

Proposition 3.1 is a consequence of the theory of binary integer quadratic forms. The purpose of this appendix is to give a self-contained elementary proof (using quadratic reciprocity) of this proposition, inspired by one of the proofs for characterizing the set of values attained by the sums of two integer squares (see, e.g., Section 20.4 of [11]). Let us quickly recall that the Legendre symbol is defined for p prime and x integer not congruent to 0 modulo p by

$$\left(\frac{x}{p}\right)_\ell = \begin{cases} +1 \text{ if } x \text{ is a quadratic residue modulo } p, \\ -1 \text{ otherwise.} \end{cases}$$

Also the famous Gauss "law of reciprocity" reads (see, e.g., [11, p. 76]):

If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)_\ell \left(\frac{q}{p}\right)_\ell = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof of Proposition 3.1. The proof is done in several steps corresponding to the Lemmas below. As we have seen that an integer n belongs to $\mathcal{S}$ if and only if $-n$ belongs to $\mathcal{S}$, we can suppose that $n \geq 0$.

First we prove that if n belongs to $\mathcal{S}$, then its prime factors congruent to 2 or 3 modulo 5 must appear with an even exponent in its decomposition: this is Lemma 6.1. Note that the condition on n is equivalent to saying that $n = m^2 \prod p_i$, for some integer m, where all p_i –if any– are distinct and are either 5 or congruent to 1 or 4 modulo 5.

Conversely suppose that $n = m^2 \prod p_i$, for some integer m, where all p_i –if any– are distinct and are either 5 or congruent to 1 or 4 modulo 5. In order to prove that n belongs to $\mathcal{S}$, we note that $\mathcal{S}$ is closed under multiplication (Lemma 6.2). Hence it suffices to prove that any square is in $\mathcal{S}$ (Lemma 6.3) and that 5 and any prime congruent to 1 or 4 modulo 5 belong to $\mathcal{S}$ (Lemma 6.4). □

In what follows, if p is a prime number, we let $v_p(n)$ denote the largest integer s such that p^s divides n ($v_p(n)$ is the p-adic valuation of n).

Lemma 6.1 *If $y^2 + xy - x^2$ is divisible by a prime p congruent to 2 or 3 modulo 5, then the largest power of this prime dividing $y^2 + xy - x^2$ must be even.*

Proof. We begin with the case where $p = 2$. Suppose that there exists an integer with odd 2-adic valuation and which can be written $y^2 + xy - x^2$ for some integers x, y. Let $\theta \geq 0$ be defined by

$$2\theta + 1 := \inf\{v_2(n);\ v_2(n) \text{ is odd and } \exists(x, y) \text{ with } n = y^2 + xy - x^2\}.$$

Let n be such that $n = y^2+xy-x^2$, for some integers x, y, and $v_2(n) = 2\theta+1$. In particular y^2+xy-x^2 is even. Since $y^2+xy-x^2 \equiv (1+x)(1+y)+1 \bmod 2$, we have that both x and y are even. Thus 4 divides n. This implies in particular $\theta \geq 1$. We then have $n/4 = (y/2)^2 + (x/2)(y/2) - (x/2)^2$ and $v_2(n/4) = 2\theta - 1$ which contradicts the definition of θ.

Now let p be a prime number congruent to 2 or 3 modulo 5 and different from 2. If there exists an integer with odd p-adic valuation that can be written as $y^2 + xy - y^2$ for some x, y, define $\mu \geq 0$ by

$$2\mu + 1 := \inf\{v_p(n);\ v_p(n) \text{ is odd and } \exists(x,y) \text{ with } n = y^2 + xy - x^2\}.$$

Let n be such that $n = y^2+xy-x^2$, for some integers x, y, and $v_p(n) = 2\mu+1$. In particular $y^2 + xy - x^2$ is divisible by p. Since 2 is invertible modulo p, we can write

$$0 \equiv y^2 + xy - x^2 \equiv \left(y + \frac{x}{2}\right)^2 - 5\left(\frac{x}{2}\right)^2 \bmod p$$

If $x/2$ is not congruent to 0 modulo p, this implies that

$$\left(\frac{y + \frac{x}{2}}{\frac{x}{2}}\right)^2 \equiv 5 \bmod p$$

which is impossible since 5 is not a square modulo p: namely using quadratic reciprocity we have $\left(\frac{5}{p}\right)_\ell \left(\frac{p}{5}\right)_\ell = (-1)^{\frac{p-1}{2}\frac{5-1}{2}} = 1$, hence $\left(\frac{5}{p}\right)_\ell = \left(\frac{p}{5}\right)_\ell$ and the squares modulo 5 are $0, 1, 4$. Hence $x/2$ is divisible by p, so is x. But y^2+xy-x^2 is divisible by p, thus y is divisible by p. This implies that n is divisible by p^2 (hence $\mu \geq 1$). Finally this gives $n/p^2 = (y/p)^2 + (x/p)(y/p) - (x/p)^2$. But $v_p(n/p^2) = 2\mu - 1$, which contradicts the definition of μ. □

Lemma 6.2 *The product of two integers belonging to $A(a, b)$ also belongs to $A(a, b)$.*

Proof. It suffices to use any of the three following identities

$$\begin{aligned}
(y^2 + xy - x^2)(b^2 + ab - a^2) &= (xb + yb - xa)^2 + (xb + yb - xa)(ay - bx) - (ay - bx)^2 \\
(y^2 + xy - x^2)(b^2 + ab - a^2) &= (ay + by - ax)^2 + (ay + by - ax)(xb - ya) - (xb - ya)^2 \\
(y^2 + xy - x^2)(b^2 + ab - a^2) &= (yb + xa)^2 + (bx + xa + ya)(yb + xa) - (bx + xa + ya)^2.
\end{aligned} \tag{4}$$

□

Lemma 6.3 *For any integer m we have that m^2 belongs to $\mathcal{S}$.*

Proof. Indeed we have $m^2 = y^2 + xy - x^2$ for $y = m$ and $x = 0$. □

Lemma 6.4 *If p is a prime equal to 5 or congruent to 1 or 4 modulo 5, then there exist integers x and y such that $p = y^2 + xy - x^2$.*

Proof. For $p = 5$, one writes $5 = 3^2 + 4 \times 3 - 4^2$. If p is a prime number congruent to j modulo 4 where $j \in \{1, 4\}$, let $u \in [1, p-1]$ such that $u^2 \equiv 5 \bmod p$ (law of reciprocity). Define $x = 2$ and $y = u - 1$. Then, clearly $u > 2$, hence $u^2 - 5 > 0$, and

$$y^2 + xy - x^2 = (u-1)^2 + 2(u-1) - 4 = u^2 - 5 \equiv 0 \bmod p.$$

Thus there exists $m > 0$ such that $y^2 + xy - x^2 = mp$; furthermore we have $mp = y^2 + xy - x^2 = u^2 - 5 \leq (p-1)^2 - 5 < (p-1)^2$ so that $mp < (p-1)^2$, hence $1 \leq m < p$. Let m_0 be the least integer in $[1, p-1]$ such that there exist $(x, y) \in \mathbb{N}^2$ with $y^2 + xy - x^2 = m_0 p$. If $m_0 = 1$ we are done. Otherwise, first note that m_0 cannot divide both x and y, because this would imply that m_0^2 divides $y^2 + xy - x^2 = m_0 p$ and hence that m_0 divides p which is impossible. Thus there exist integers c, d, x_1, y_1 such that $x = cm_0 + x_1$, $y = dm_0 + y_1$ with $|x_1| \leq m_0/2$, $|y_1| \leq m_0/2$ and $0 < y_1^2 + x_1 y_1 - x_1^2 \leq y_1^2 + x_1 y_1 \leq 2(m_0/2)^2 = m_0^2/2 < m_0^2$.
Now

$$y_1^2 + x_1 y_1 - x_1^2 = (y - dm_0)^2 + (x - cm_0)(y - dm_0) - (x - cm_0)^2 \equiv 0 \bmod m_0.$$

Thus there exists an integer m_1 such that $y_1^2 + x_1 y_1 - x_1^2 = m_1 m_0$. Furthermore $m_1 < m_0$ since $y_1^2 + x_1 y_1 - x_1^2 < m_0^2$. Now we write, using Lemma 6.2,

$$\begin{aligned} m_0^2 m_1 p &= (y^2 + xy - x^2)(y_1^2 + x_1 y_1 - x_1^2) \\ &= (xy_1 + yy_1 - xx_1)^2 + (xy_1 + yy_1 - xx_1)(x_1 y - y_1 x) - (x_1 y - y_1 x)^2 \\ &= (x_1 y + y_1 y - x_1 x)^2 + (x_1 y + y_1 y - x_1 x)(xy_1 - yx_1) - (xy_1 - yx_1)^2. \end{aligned}$$

But we have $x_1 \equiv x \bmod m_0$ and $y_1 \equiv y \bmod m_0$. This implies that both $xy_1 + yy_1 - xx_1$ and $x_1 y + y_1 y - x_1 x$ are congruent to $xy + y^2 - x^2$ hence to 0 modulo m_0, and that $(x_1 y - y_1 x)$ is congruent to $(xy - yx)$ hence to 0 modulo m_0. We thus have $xy_1 + yy_1 - xx_1 = m_0 Y$ and $x_1 y - y_1 x = m_0 X$ for some integers X and Y in $\mathbb{Z}$. Hence

$$m_0^2 m_1 p = m_0^2 Y^2 + m_0^2 XY - m_0^2 X^2$$

hence

$$m_1 p = Y^2 + XY - X^2$$

By Lemma 3.4 this implies that there exist two integers X' and Y' in $\mathbb{N}$ such that $m_1 p = (Y')^2 + X'Y' - (X')^2$, which contradicts the definition of m_0 since $m_1 < m_0$. $\square$

References

[1] M. Baake, Solution of the coincidence problem in dimensions $d \leq 4$, in *The Mathematics of Long-range Aperiodic Order (Waterloo, ON, 1995)*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 489, Kluwer Acad. Publ., Dordrecht, pp. 9–44, 1997.

[2] D. W. Boyd, Pisot sequences which satisfy no linear recurrence, *Acta Arith.* **24** (1977), 89–98.

[3] D. W. Boyd, Pisot sequences which satisfy no linear recurrence. II. *Acta Arith.* **48** (1987), 191–195.

[4] D. W. Boyd, Linear recurrence relations for some generalized Pisot sequences, in *Advances in Number Theory (Kingston ON, 1991)*, pp. 333–340, Oxford Univ. Press, New York, 1993. Updates from 1996 and 1999, available at `https://www.researchgate.net/profile/David_Boyd7/publication/262181133_Linear_recurrence_relations_for_some_generalized_Pisot_sequences_-_annotated_with_corrections_and_additions/links/00b7d536d49781037f000000`.

[5] J. Brillhart, P. Morton, A case study in mathematical research: the Golay-Rudin-Shapiro sequence, *Amer. Math. Monthly* **103** (1996), 854–869.

[6] S. B. Ekhad, D. Zeilberger, How to generate as many Somos-like miracles as you wish, *J. Difference Equ. Appl.* **20** (2014), 852–858.

[7] S. B. Ekhad, N. J. A. Sloane, D. Zeilberger, Automated proofs (or disproofs) of linear recurrences satisfied by Pisot sequences, Preprint (2016), available at `https://arxiv.org/abs/1609.05570`.

[8] S. Fomin, A. Zelevinsky, The Laurent phenomenon, *Adv. Appl. Math.* **28** (2002), 119–144.

[9] D. Gale, The strange and surprising saga of the Somos sequences, *Math. Intelligencer* **13**, no 1 (1991), 40–42

[10] D. Gale, Somos sequence update, *Math. Intelligencer* **13**, no 4 (1991), 49–50.

[11] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Fourth Edition, Oxford at the Clarendon Press, 1960.

[12] A. F. Horadam, Generating functions for powers of a certain generalised sequence of numbers, *Duke Math. J.* **32** (1965), 437–446.

[13] J. L. Malouf, An integer sequence from a rational recursion, *Discrete Math.* **110** (1992), 257–261.

[14] R. S. Melham, A Fibonacci Identity in the spirit of Simson and Gelin-Cesàro, *Fibonacci Quart.* **41** (2003), 14–143.

[15] *On-Line Encyclopedia of Integer Sequences*, founded by N. J. A. Sloane, electronically available at `http://oeis.org`.

[16] G. Pirillo, A characterization of Fibonacci numbers, *Chebyshevskiĭ Sb.* **19** (2018), 259–271, available at https://www.chebsbornik.ru/jour/article/view/475# .

[17] C. Pisot, La répartition modulo 1 et les nombres algébriques, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (2)* **7** (1938), 205–248.

[18] J. Propp, *The Somos Sequence Site*, http://faculty.uml.edu/jpropp/somos.html.

[19] Y. Soykan, Simson identity of generalized m-step Fibonacci numbers, *Int. J. Adv. Appl. Math. and Mech.* **7** (2019), 45–56, available at http://www.ijaamm.com/uploads/2/1/4/8/21481830/v7n2p4_45-56.pdf.