DIOPHANTINE TRIPLES AND REDUCED QUADRUPLES WITH THE LUCAS SEQUENCE OF RECURRENCE
$$u_n = Au_{n-1} - u_{n-2}$$

Nurettin Irmak and László Szalay

University of Niğde, Turkey and University of West Hungary, Hungary

Abstract. In this study, we show that there is no positive integer triple $\{a, b, c\}$ such that all of $ab+1$, $ac+1$ and $bc+1$ are in the sequence $\{u_n\}_{n\geq 0}$ satisfies the recurrence $u_n = Au_{n-1} - u_{n-2}$ with the initial values $u_0 = 0$, $u_1 = 1$. Further, we investigate the analogous question for the quadruples $\{a, b, c, d\}$ with $abc + 1 = u_x$, $bcd + 1 = u_y$, $cda + 1 = u_z$ and $dab + 1 = u_t$, and deduce the non-existence of such quadruples.

1. Introduction

A Diophantine m-tuple is a set $\{a_1, a_2, \ldots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a square for all $1 \leq i < j \leq m$. This problem and its variations have a rich history. Diophantus investigated first, although rational quadruples, and found the set $\{1/16, 33/16, 68/16, 105/16\}$. Fermat was the first who could give an integer quadruple, namely the set $\{1, 3, 8, 120\}$.

It is widely known that infinitely many integer Diophantine quadruples exist. For instance, Hoggatt and Bergum ([5]) proved that for any positive integer k, the set

$$\{F_{2k}, \; F_{2k+2}, \; F_{2k+4}, \; 4F_{2k+1}F_{2k+2}F_{2k+3}\}$$

is always quadruple. A widely believed conjecture states that no quintuple exists. The famous theorem of Dujella ([3]) states that there are only finitely many quintuples.

A variant of the problem is obtained if one replaces the squares by the terms of a given binary recurrence. For details, see the articles [1, 4, 6, 7].

The first cited paper investigates a general case and provides sufficient and necessary conditions to have only finitely diophantine triples with terms of the binary recurrent sequence. But the arguments in [4] give no hint how to find the triples themselves. The other papers describe methods to determine all Diophantine triples for Fibonacci, Lucas and balancing numbers, respectively.

In this paper, we follow the treatment of the above results, but there is an essential difference, namely the binary recurrence we investigate here contains a positive integer parameter A. Therefore, we must include new, additional ideas in order to prove our theorems.

Assume that A is a given positive integer. Define the sequence $\{u_n\}$ by

$$u_n = Au_{n-1} - u_{n-2}$$

with the initial conditions $u_0 = 0$, $u_1 = 1$. The Binet formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

gives u_n explicitly, where $\alpha = (A + \sqrt{A^2 - 4})/2$ and $\beta = (A - \sqrt{A^2 - 4})/2$. Obviously, $\alpha + \beta = A$ and $\alpha\beta = 1$. Further the condition $A \geq 3$ entails that the zeros of the characteristic polynomial $x^2 - Ax + 1$ are real, have $\alpha > 1$ and $\beta \in (0, 1)$ and moreover α increases and β decreases when A increases. We define $\{v_n\}_{n \geq 0}$ as the associated sequence of $\{u_n\}_{n \geq 0}$. The recurrence relation for $\{u_n\}_{n \geq 0}$ and $\{v_n\}_{n \geq 0}$ coincide, but the initial conditions in the second case are $v_0 = 2$ and $v_1 = A$. It is well-known that

$$v_n = \alpha^n + \beta^n.$$

The main results of this work are the following.

THEOREM 1.1. *Suppose that $A \neq 2$ is a positive integer. Then there do not exist integers $1 \leq a < b < c$ such that*

(1.1)
$$
\begin{aligned}
ab + 1 &= u_x, \\
ac + 1 &= u_y, \\
bc + 1 &= u_z
\end{aligned}
$$

hold with the natural numbers $1 \leq x < y < z$.

Note that $A = 2$ gives that the sequence $\{u_n\}_{n \geq 0}$ is the sequence of all natural numbers and in this case, trivially, system (1.1) is satisfied by arbitrary a, b and c. Clearly, it will also be true for (1.2).

THEOREM 1.2. *If $A \neq 2$ is a positive integer then the system*

(1.2)
$$
\begin{aligned}
abc + 1 &= u_x, \\
bcd + 1 &= u_y, \\
cda + 1 &= u_z, \\
dab + 1 &= u_t
\end{aligned}
$$

is not solvable in the integers $1 \leq a < b < c < d$ and $1 \leq x < t < z < y$.

Observe, that although the last three equations of (1.2) would generalize system (1.1) by one more unknown d, here we have the additional equation $abc + 1 = u_x$.

Note that the case $A = 1$ provides the periodic sequence

$$u_n = 0, 1, 1, 0, -1, -1, \ldots.$$

Hence, neither (1.1) nor (1.2) cannot be fulfilled with $A = 1$. Thus, in the sequel, we assume $A \geq 3$.

In the next part, we gather the auxiliary results which are needed in the proofs of the theorems.

2. Preliminary Results

LEMMA 2.1. *Assume that n and m are arbitrary non-negative integers. Then the following identities hold.*

(1) $\gcd(u_n, u_m) = u_{\gcd(n,m)}$,
(2) $\gcd(u_n, v_m) = 1$ *or* 2 *or* $v_{\gcd(n,m)}$, *especially* $\gcd(u_n, v_n) = 1$ *or* 2,
(3) $(u_n - 1)(u_n + 1) = u_{n-1}u_{n+1}$,
(4) $u_{2n+1} - 1 = u_n v_{n+1}$,
(5) $2u_{n+m} = u_n v_m + v_n u_m$.

PROOF. The first two identities are known from [2]. Paper [9] contains (3), the remaining identities can be proved by using Binet formula. For instance,

$$
\begin{aligned}
u_n v_{n+1} &= \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) \left(\alpha^{n+1} + \beta^{n+1} \right) \\
&= \frac{\alpha^{2n+1} - \beta^{2n+1}}{\alpha - \beta} - (\alpha\beta)^n = u_{2n+1} - 1.
\end{aligned}
$$

□

LEMMA 2.2. *Suppose that $A \geq 3$. Then for all integers $n \geq 3$, the inequalities*

(2.1) $$\alpha^{n-1} < u_n < \alpha^{n-0.83}$$

and

(2.2) $$\alpha^n < v_n < \alpha^{n+0.004}$$

hold.

PROOF. Using the Binet formula of the sequence $\{u_n\}_{n \geq 0}$, we obtain

(2.3) $$\alpha^{n-1} < \frac{\alpha^n - \beta^n}{\alpha - \beta} = u_n = \frac{\alpha^n}{\alpha - \beta} \left(1 - \left(\frac{\beta}{\alpha} \right)^n \right) < \alpha^{n - \log_\alpha(\alpha - \beta)}.$$

To justify the right hand side, we show that the function

$$f(\alpha) = \log_\alpha \left(\alpha - \frac{1}{\alpha} \right) = \frac{\log(\alpha^2 - 1)}{\log \alpha} - 1$$

is strictly increasing for $\alpha > 1$. Indeed, $f'(\alpha) > 0$ is a consequence of the arguments

$$(\alpha^2 - 1) \log(\alpha^2 - 1) < (\alpha^2 - 1) \log \alpha^2 < 2\alpha^2 \log \alpha.$$

Replacing α by the worst case $(3 + \sqrt{5})/2$ (it corresponds to the smallest possibility for A which is $A = 3$) in the exponent of the rightmost term of (2.3), it leads to $u_n < \alpha^{n-0.83}$.

The lower bound in (2.2) for v_n is trivial. To have an upper bound, we evaluate

$$v_n \leq \alpha^n \left(1 + \frac{1}{\alpha^6} \right) < 1.0032 \cdot \alpha^n < \alpha^{n+0.004}.$$

□

REMARK 2.3. Since the estimate of the right hand side of (2.1) does not depend on the condition $n \geq 3$, we conclude that it remains valid for any $n \in \mathbb{N}$. A similar observation is true for the left hand side of (2.2).

LEMMA 2.4. *Suppose $A \geq 3$. Then $\log_\alpha(2(A^2 - 2)) < 3.1$.*

PROOF. Let $g(\alpha) = \log(\alpha + 1/\alpha)/\log \alpha$ and $h(\alpha) = \log_\alpha(2)$. It is easy to see that the functions $g(\alpha)$ and $h(\alpha)$ are strictly decreasing when $\alpha > 1$. Thus, the largest possible value $\alpha = (3 + \sqrt{5})/2$ belonging to the case $A = 3$, together with

$$\log_\alpha(A^2 - 2) < 2\log_\alpha A = 2g(\alpha)$$

shows the statement.   □

LEMMA 2.5. *Assume that $n \geq 3$ and $A \geq 3$ are integers. Then*

$$\gcd(u_n - 1, u_{n-2} - 1) \leq 2(A^2 - 2).$$

PROOF. Put $g = \gcd(u_n - 1, u_{n-2} - 1)$. The recurrence relation of the sequence $\{u_n\}_{n \geq 0}$, together with Lemma 2.1 (1) and (3) yields

$$\begin{aligned} g &= \gcd(u_n - 1, u_n - u_{n-2}) \leq \gcd(u_{n-1}u_{n+1}, u_n - u_{n-2}) \\ &\leq \gcd(u_{n-1}, Au_{n-1} - 2u_{n-2}) \gcd(u_{n+1}, 2u_n - Au_{n-1}) \\ &\leq 2\gcd(u_{n+1}, (2 - A^2)u_n + Au_{n+1}) \leq 2(A^2 - 2). \end{aligned}$$

□

LEMMA 2.6. *Any integer $n \geq 2$ satisfies*

$$\gcd(u_{2n-3} - 1, u_n - 1) < \alpha^{5.7}.$$

PROOF. Similarly to the previous lemma, put $g = \gcd(u_{2n-3} - 1, u_n - 1)$ and apply (4) of Lemma 2.1. It implies

$$
\begin{aligned}
g &= \gcd(u_{n-2}v_{n-1}, u_{n-1}u_{n+1}) \\
&\leq \gcd(u_{n-2}, u_{n-1})\gcd(u_{n-2}, u_{n+1})\gcd(v_{n-1}, u_{n-1})\gcd(v_{n-1}, u_{n+1}).
\end{aligned}
$$

By (5) of Lemma 2.1, we have $2u_{n+1} = u_{n-1}v_2 + v_{n-1}u_2$, which together with (1) and (2) of Lemma 2.1 yields

$$
g \leq 2u_3 \gcd(v_{n-1}, u_{n-1}v_2 + u_2v_{n-1}) \leq 4u_3v_2 < \alpha^{5.7}.
$$

□

LEMMA 2.7. *Any integer $n \geq 2$ satisfies*

$$
\gcd(u_{2n-2} - 1, u_n - 1) < \alpha^{6.4}.
$$

PROOF. Put $g = \gcd(u_{2n-2} - 1, u_n - 1)$.

$$
\begin{aligned}
g &= \gcd(u_{2n-1}u_{2n-3}, u_{n-1}u_{n+1}) \\
&\leq \gcd(u_{2n-1}, u_{n-1})\gcd(u_{2n-1}, u_{n+1}) \\
&\quad \times \gcd(u_{2n-3}, u_{n-1})\gcd(u_{2n-3}, u_{n+1}) \\
&\leq u_1^2 u_3 u_5 < \alpha^{6.4}.
\end{aligned}
$$

□

LEMMA 2.8. *All positive solutions of (1.1) satisfy $z \leq 2y - 1$.*

PROOF. Considering the last two equations of system (1.1) we have

$$
c \mid \gcd(u_y - 1, u_z - 1).
$$

Moreover $u_z = bc + 1 < c^2$, therefore $\sqrt{u_z} < c$ holds. By (2.1), we obtain

$$
\sqrt{\alpha^{z-1}} < \sqrt{u_z} < c < u_y < \alpha^{y-0.83},
$$

which implies $z < 2y - 0.66$, so $z \leq 2y - 1$. □

LEMMA 2.9. *The solutions to system (1.2) satisfy the inequality $y \leq 2z - 1$.*

PROOF. Clearly, $u_y = bcd + 1 < (cd)^2$, so $\sqrt{u_y} < cd$. From (1.2), we deduce that

$$
cd \mid \gcd(u_y - 1, u_z - 1).
$$

By Lemma 2.2,

$$
\sqrt{\alpha^{y-1}} < \sqrt{u_y} < cd < u_z < \alpha^{z-0.83},
$$

which leads to $y \leq 2z - 1$. □

3. PROOF OF THEOREM 2

Suppose that $A \geq 3$. Further suppose $1 \leq a < b < c$ and that $1 \leq x < y < z$ satisfy (1.1). Then, $1 \cdot 2 + 1 \leq ab + 1 = u_x$ implies $x \geq 2$. Now we distinguish two cases.

CASE 1. $z \leq 138$.

Firstly, we find upper bound for the coefficient A of the sequence $\{u_n\}_{n \geq 0}$.

LEMMA 3.1. *If $z \leq 138$ and there exist a solution of (1.1) then $A \leq A_0$ with a suitable $A_0 \in \mathbb{N}^+$.*

PROOF. Clearly, the terms of the sequence $\{u_n\}$ are monic polynomials in A with $\deg(u_n(A)) = n - 1$ $(n \geq 1)$, the first few terms are $u_0(A) = 0$, $u_1(A) = 1$ and

$$u_2(A) = A, \quad u_3(A) = A^2 - 1, \quad u_4(A) = A^3 - 2A, \quad \dots .$$

If $2 \leq x < y < z \leq 138$ and $1 \leq a < b < c$ satisfy (1.1) then

$$a = \sqrt{\frac{(u_x(A) - 1)(u_y(A) - 1)}{u_z(A) - 1}}$$

must be necessarily integer for some A. Since $u_z(A)$ is monic, then by polynomial division, there uniquely exist polynomials $q(A) \in \mathbb{Z}[A]$ and $r(A) \in \mathbb{Z}[A]$ such that

$$(u_x(A) - 1)(u_y(A) - 1) = q(A) \cdot (u_z(A) - 1) + r(A),$$

where $\deg(r(A)) < \deg(u_z(A))$.

Checking the eligible possibilities for x, y and z by computer, $r(A)$ is never the constant zero polynomial. Hence,

(3.1) $$\frac{(u_x(A) - 1)(u_y(A) - 1)}{u_z(A) - 1} = q(A) + \frac{r(A)}{u_z(A) - 1}$$

follows. Again a computer verification shows that there is no positive integer $A \geq 3$ satisfying the equation $r(A) = 0$ with the condition $z \leq 138$. Thus the fraction $r(A)/(u_z(A) - 1)$ never disappears on the right hand side of (3.1).

If for some A the left hand side of the equation (3.1) is integer, then by $q(A) \in \mathbb{N}$, we deduce that

$$\frac{r(A)}{u_z(A) - 1}$$

is so. But $\deg(r(A)) < \deg(u_z(A))$, so A cannot be large since

$$\lim_{A \to \infty} \frac{r(A)}{u_z(A) - 1} = 0.$$

Consequently, $|r(A)| \geq u_z(A) - 1$ must hold, which proves $A \leq A_0$ with some positive integer A_0. To obtain the exact upper bound, we run a computer

search with the conditions $2 \le x < y < z \le 138$, and we found that $A_0 = 2$.

□

Then, by Lemma 3.1 we obtain immediately that there is no solution to the system (1.1) in the first case.

CASE 2. $z > 138$.

Put $P = \gcd(u_z - 1, u_y - 1)$. By (1) and (3) of Lemma 2.1, we have

$$
\begin{aligned}
P &= \gcd(u_{z-1}u_{z+1}, u_{y-1}u_{y+1}) \\
&\le \prod_{i,j \in \{\pm 1\}} \gcd(u_{z-i}, u_{y-j}) = \prod_{i,j \in \{\pm 1\}} u_{\gcd(z-i, y-j)}.
\end{aligned}
\tag{3.2}
$$

Let us say that $\gcd(z-i, y-j) = \frac{z-i}{t_{ij}}$ for some positive integer t_{ij}.

Suppose that $t_{ij} \ge 8$ holds for all pairs $(i,j) \in \{\pm 1\}^2$. Then Lemma 2.2 implies that

$$
\alpha^{\frac{z-1}{2}} < \sqrt{u_z} < c \le P \le u_{\frac{z-1}{8}}^2 u_{\frac{z+1}{8}}^2 < \alpha^{4\left(\frac{z+1}{8} - 0.83\right)}.
\tag{3.3}
$$

If we compare the exponents of α in (3.3), we arrive at a contradiction.

In what follows, we assume that $t_{ij} \le 7$ holds for some pair. Let k denote this t_{ij}. Further suppose that

$$
\frac{z-i}{k} = \frac{y-j}{\ell}
$$

holds for a suitable positive integer ℓ coprime to k.

Suppose for the moment that $\ell > k$. Then $z - i < y - j$ implies $z = y + 1$ via $y < z$. Thus,

$$
\begin{aligned}
P &= \gcd(u_y - 1, u_{y+1} - 1) = \gcd(u_{y+1}u_{y-1}, u_y u_{y+2}) \\
&= \gcd(u_{y-1}, u_{y+2}) \le u_3 < \alpha^{2.2}.
\end{aligned}
$$

Hence, by the first part of (3.3), we have

$$
\alpha^{\frac{z-1}{2}} < \alpha^{2.2},
$$

which leads to the contradiction $z < 5.4$.

Assume now that $\ell = k$. Necessarily we have $k = \ell = 1$. Since $z - i = y - j$, we obtain $z = y + 2$. By Lemma 2.5,

$$
\alpha^{\frac{z-1}{2}} < \sqrt{u_z} < c \le P = \gcd(u_z - 1, u_{z-2} - 1) < 2(A^2 - 2).
$$

Using Lemma 2.4, we obtain a contradiction again from

$$
z < 2 \log_\alpha \left(2(A^2 - 2)\right) + 1 < 7.2.
$$

In the sequel, we assume $\ell < k$. First we analyze the case when $2 \le k/\ell$. Here,

$$
z = \frac{k}{\ell}(y - j) + i \ge 2(y - 1) - 1 = 2y - 3,
$$

which, together with Lemma 2.8 implies the following three possibilities.

- When $z = 2y - 1$ holds, then we have

$$\alpha^{y-1.17} = \frac{\alpha^{2y-2}}{\alpha^{y-0.83}} < \frac{u_{2y-1}}{u_y} = \frac{bc+1}{ac+1} < \frac{b}{a}.$$

  Subsequently,

$$a^2 \alpha^{y-1.17} < ab = u_x - 1 < u_x < \alpha^{x-0.83}$$

  holds according to Remark 2.3. Thus,

$$a^2 < \alpha^{x-y+0.34} \le \alpha^{-0.66}$$

  again a contradiction.

- Assume that $z = 2y - 2$. Then, by Lemma 2.7, it follows that

$$\alpha^{\frac{z-1}{2}} < P = \gcd(u_y - 1, u_{2y-2} - 1) < \alpha^{6.4},$$

  which is not possible since $z \ge 139$.

- If $z = 2y - 3$ then, according to Lemma 2.6,

$$\alpha^{\frac{z-1}{2}} < P = \gcd(u_y - 1, u_{2y-3} - 1) < \alpha^{5.7}$$

  holds, which is obviously impossible.

Finally assume that $k/\ell < 2$. Note that this condition implies $k \ge 3$. Taking any pair $(i_0, j_0) \ne (i, j)$, we have

$$z - i_0 = \frac{k}{\ell}(y - j) + i - i_0.$$

Now the main goal is to calculate the best upper bound for $P_0 = \gcd(z - i_0, y - j_0)$. Starting with

$$\begin{aligned} P_0 &= \gcd\left(\frac{k}{\ell}(y - j) + i - i_0, y - j_0\right) \\ &\le \gcd(k(y - j) + \ell(i - i_0), k(y - j_0)) = |k(j_0 - j) + \ell(i - i_0)|, \end{aligned}$$

we need to consider the last expression. The three cases

(3.4) $j \ne j_0,\ i \ne i_0,$ $j \ne j_0,\ i = i_0,$ $j = j_0,\ i \ne i_0,$

give $2(k + \ell)$, $2k$, 2ℓ, respectively. Then, using the inequality (3.2), we get

$$\begin{aligned} \alpha^{\frac{z-1}{2}} \le P &= \gcd(u_y - 1, u_z - 1) < \prod_{i,j \in \{\pm 1\}} u_{\gcd(z-i, y-j)} \\ &\le \alpha^{\frac{z+1}{k} + 2(k+\ell) + 2k + 2\ell - 4 \cdot 0.83}. \end{aligned}$$

Going through the eligible pairs

(3.5) $(k, \ell) = (3, 2),\ (4, 3),\ (5, 3),\ (5, 4),\ (6, 5),\ (7, 4),\ (7, 5),\ (7, 6),$

the previous argument provides the upper bounds

$$z < 105.1,\ 101.8,\ 98,\ 111.3,\ 124.1,\ 115.8,\ 127,\ 138.2,$$

respectively. The assertion of the second part of the proof contradicts any of these upper bounds. Thus, the proof of Theorem 2 is complete.

4. The proof of Theorem 3

Apart from the second equation, system (1.2) turns to a triple if we take $a = 1$. Therefore, we may suppose that $2 \leq a < b < c < d$ and with $1 \leq x < z < v < y$ they satisfy system (1.2). Since $2 \times 3 \times 4 + 1 \leq abc + 1 = u_x$, then $2 \leq x < t < z < y$ hold. We again split the proof into two parts.

Case 3. $y \leq 138$.

Repeating the treatment of Lemma 3.1 we prove the impossibility of the existence of quadruples satisfies (1.2) with $y \leq 138$.

Lemma 4.1. *System (1.2) has no solution with $A \geq 3$ and $y \leq 138$.*

Proof. We follow the approach of the proof of Lemma 3.1. Considering the integer

$$a = \sqrt[3]{\frac{(u_x(A) - 1)(u_t(A) - 1)(u_z(A) - 1)}{(u_y(A) - 1)^2}},$$

and the polynomial division

$$(u_x(A) - 1)(u_t(A) - 1)(u_z(A) - 1) = q(A)(u_y(A) - 1)^2 + r(A),$$

we find $A \leq 2$ under the assumption $y \leq 138$.

Case 4. $y > 138$.

The results of Lemma 2.8 and 2.9 coincide if we change the roles of y and z. Since only the two largest variables (y and z) are used in the second part of the proof of Theorem 1.1, we can make a step by step copy of that to show the remaining part of Theorem 1.2. The only difference is to consider here cd instead of c:

$$\sqrt{u_y} < cd \leq \gcd(u_y - 1,\ u_z - 1) \leq \prod_{i,j \in \{\pm 1\}} u_{\gcd(y-i, z-j)}.$$

Therefore the proof is complete.   □

References

[1] M. Alp, N. Irmak and L. Szalay, *Balancing Diophantine Triples,* Acta Univ. Sapientiae **4** (2012), 11–19.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$,* Ann. of Math. (2) **15** (1913/14), 30–48.

[3] A. Dujella, *There are only finitely many Diophantine quintuples,* J. Reine Angew. Math. **566** (2004), 183–214.

[4] C. Fuchs, F. Luca and L. Szalay, *Diophantine triples with values in binary recurrences,* Ann. Scuola Norm. Sup. Pisa. Cl. Sci. III **5** (2008), 579–608.

[5] V. E. Hoggat and G. E. Bergum, *A problem of Fermat and Fibonacci sequence,* Fibonacci Quart. **15** (1977), 323–330.

[6] F. Luca and L. Szalay, *Fibonacci Diophantine triples,* Glas. Mat. Ser. III **43(63)** (2008), 253–264.

[7] F. Luca and L. Szalay, *Lucas Diophantine triples,* INTEGERS **9** (2009), 441–457.

[8] G. K. Panda and S. S. Rout, *A Class of recurrent sequences exhibiting some exciting properties of balancing numbers,* World Acad. of Sci., Eng. and Tech. **61** (2012), 164–166.

[9] L. Szalay, *Diophantine equations with binary recurrences associated to Brocard-Ramanujan problem,* Portugal. Math. **69** (2012), 213–220.

N. Irmak
Mathematics Department, Art and Science Faculty
University of Niğde
51240 Niğde
Turkey
E-mail: `nirmak@nigde.edu.tr, irmaknurettin@gmail.com`

L. Szalay
Institute of Mathematics
University of West Hungary
H-9400 Sopron
Hungary
E-mail: `laszlo.szalay@emk.nyme.hu`