DISTINCT PRODUCTS IN LUCAS SEQUENCES – ON A PROBLEM OF KIMBERLING

MÁRTON SZIKSZAI

Abstract. Consider the Diophantine equation

$$A\prod_{i\in I} u_i^{\alpha_i} = B\prod_{j\in J} u_j^{\beta_j}$$

in unknown non-empty disjoint subsets of natural numbers I, J and positive integer exponents α_i, β_j, where $u = (u_n)_{n=0}^{\infty}$ is a Lucas sequence and A, B are given integers. We derive effective upper bounds on $\max I$ and $\max J$ and present a method to effectively enumerate all solutions when u is given. As an application we solve a partial case of a problem of Kimberling on distinct products.

1. Introduction

Let I and J be non-empty disjoint subsets of natural numbers. A sequence of integers $s = (s_n)_{n=0}^{\infty}$ is said to have the distinct product property with respect to I and J if

$$\prod_{i\in I} s_i \neq \prod_{j\in J} s_j. \tag{1}$$

It is easy to see that there are sequences which satisfy (1) to some measure: the sequence of prime numbers does for any choice of I and J, the sequence of Fibonacci numbers also, except for the trivial case $F_1 = F_2$ (see question 238505 on `mathoverflow.net` [8]), while geometric progressions can either have or fail to have it on infinitely many occasions. At the 17th International Conference on Fibonacci Numbers and Their Applications, Kimberling [4] discussed a few specific binary linear recurrences where the property has already been described completely. Further, he challenged the audience to investigate other examples. Observe that for a given sequence we can translate (1) to the Diophantine equation

$$\prod_{i\in I} s_i = \prod_{j\in J} s_j \tag{2}$$

in unknowns I and J. There is a natural one-to-one correspondence between solutions to (2) and the choices of I and J for which (1) does not hold.

In this short paper, we address a more general distinct product property in Lucas sequences. We do so by allowing powers of terms and constant multipliers on both sides of (2). Let P and Q be non-zero coprime integers such that the quotient of the roots α and β of the polynomial

$$x^2 - Px + Q$$

is never a root of unity. The sequence $u = (u_n)_{n=0}^{\infty}$ defined by

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

Research was supported by the Hungarian Academy of Sciences.

is called the Lucas sequence corresponding to the pair (P, Q). They form a specific and important class of non-degenerate binary linear recurrence sequences. One has initial terms $u_0 = 0, u_1 = 1$ and a recurrence relation of the form

$$u_{n+2} = Pu_{n+1} - Qu_n \qquad (n \geq 0). \tag{3}$$

These sequences were introduced and studied extensively by Lucas [6] and can be thought of as a natural generalization of the Fibonacci sequence preserving the most important arithmetic properties of it. As mentioned we consider an equation more general than (2) for them. That is, we deal with

$$A \prod_{i \in I} u_i^{\alpha_i} = B \prod_{j \in J} u_j^{\beta_j} \tag{4}$$

in unknown non-empty disjoint subsets of natural numbers I, J and unknown positive integer exponents α_i, β_j, where A, B are fixed non-zero coprime integers. Since we can always eliminate common factors of A and B, the latter assumption can be used without losing generality. Our main result is as follows.

Theorem 1.1. *Let $u = (u_n)_{n=0}^{\infty}$ be the Lucas sequence corresponding to the pair (P, Q). If $\gcd(AB, Q) \neq 1$, then equation (4) has no solutions. Otherwise, we have*

$$\max I \leq \max\{L(B) - \epsilon(L(B)), 30\}, \qquad \max J \leq \max\{L(A) - \epsilon(L(A)), 30\}, \tag{5}$$

where $L(x)$ stands for the greatest prime factor of the non-zero integer x and

$$\epsilon(x) = \left(\frac{P^2 + 4Q}{L(x)}\right)$$

with $\left(\frac{P^2+4Q}{L(x)}\right)$ being the Legendre symbol. Further, for a fixed pair (P, Q), all solutions can be effectively computed.

Remark 1.2. *A natural question would concern the problem of improving the bounds in (5). Already at this point we emphasize that it is not possible in general, nevertheless we discuss the matter in detail in Section 3.*

As an application of Theorem 1.1 we solve the distinct product problem in Lucas sequences. To simplify our corresponding statement we consider the equation

$$\pm \prod_{i \in I} s_i = \prod_{j \in J} s_j \tag{6}$$

in place of (2). For any sequence $s = (s_n)_{n=0}^{\infty}$ we set

$$S_{\pm 1} = \{n : s_n \neq \pm 1\}.$$

We call a solution (I, J) of (6) minimal, if $I \cap S_{\pm 1} = J \cap S_{\pm 1} = \emptyset$.

Corollary 1.3. *Let $u = (u_n)_{n=0}^{\infty}$ be the Lucas sequence corresponding to the pair (P, Q). Then all minimal solutions of (6) are listed in Table 1.3.*

It is clear that if $S_{\pm 1}$ is known, then one can easily go between solutions of (2) and (6) by inclusion and exclusion and can also construct the "trivial" solutions, when both sides are ± 1. Since $S_{\pm 1}$ has already been obtained for all Lucas sequences (see [3]), we have that Corollary 1.3 yields a description of the distinct product property.

In the proofs, we combine results on the rank of apparition of primes and primitive prime divisors in Lucas sequences. This is enough to obtain the bounds in (5) and to provide an effective, yet impractical, way to solve (4) when (P, Q) are given. In Corollary 1.3, these

TABLE 1

(P,Q)	(I,J) *(or* (J,I) *due to symmetry)*
$(\pm 1,2)$	$(\{6,9\},\{18\}),(\{4,6,8\},\{12\}),(\{4\},\{8\})$
$(\pm 1,3)$	$(\{3,4,6\},\{12\})$
$(\pm 1,4)$	$(\{4,6\},\{12\})$
$(\pm 2,3)$	$(\{2,5\},\{10\})$
$(P,(P^2-1)/2),\ P\equiv 1 \pmod 2,\ P\neq\pm 1$	$(\{2\},\{4\})$
$(P,(P^2-1)/3),\ P\not\equiv 0 \pmod 3,\ P\neq\pm 1,\pm 2$	$(\{2,3\},\{6\})$

pairs are variables and hence the proof involves a more careful application of these tools with some additional treatment of "small" cases based on factorization properties and divisibility arguments. Finally, we make remarks about possible improvements on both the bounds in (5) and on the naive algorithm we construct in the proof of Theorem 1.1.

2. Proofs of the Results

We start off by listing the important facts on prime divisors in Lucas sequences that we rely on in the proofs. First, we need to introduce a few notions. Let p be a prime. The rank of apparition of p in the Lucas sequence $u=(u_n)_{n=0}^{\infty}$ is the smallest positive integer $r(p)$ such that $p \mid u_{r(p)}$. Further, p is said to be a primitive divisor of some term u_n if $p \mid u_n$, but $p \nmid u_m$ for every positive $m<n$. Now we are ready to make precise statements. The first one is a classical result, frequently referred to as the "law of apparition" or in a more fitting translation the "law of appearance".

Lemma 2.1. *Let $u=(u_n)_{n=0}^{\infty}$ be a Lucas sequence corresponding to the pair (P,Q) and let p be a prime. If $p \mid Q$, then p does not divide any u_n with positive n. Otherwise, if p is odd, we have*

$$r(p) \mid p-\epsilon(p)\ .$$

Further, if $2 \nmid Q$ then

$$r(2)=\begin{cases}2, & \text{if } 2 \mid P,\\ 3, & \text{if } 2 \nmid PQ.\end{cases}$$

Proof. The proof is by simple induction and divisibility arguments and can be found in numerous papers and textbooks, for instance, in Section 2.4 of the book of Ribenboim [7]. □

The second result is the celebrated theorem of Bilu, Hanrot, and Voutier [1] which extends the famous theorem of Carmichael [2] on primitive prime divisors of Fibonacci numbers to arbitrary Lucas sequences.

Lemma 2.2. *Let $u=(u_n)_{n=0}^{\infty}$ be a Lucas sequence. For $n>30$ every u_n has a primitive prime divisor.*

Proof. This is just a reformulation of the main result in [1] for the case of Lucas sequences. □

Remark 2.3. *Theorem C and 1.3 together with Tables 1 and 3 in* [1] *give a stronger result by listing all occurrences when a term may fail to admit a primitive prime divisor. However, to keep the lemma's statement simple we use this form and refer to the paper when the more specific version is useful.*

We continue with the proof of our main result.

Proof of Theorem 1.1. First, assume that $\gcd(AB, Q) \neq 1$. Then there exists a prime $p \mid \gcd(AB, Q)$ and hence by Lemma 2.1 there is no term in the sequence which is divisible by p. Since $\gcd(A, B) = 1$, we have that p divides only one side of (4) and there can be no solution.

In what follows, $\gcd(AB, Q) = 1$ and for later use we set $\max I = n, \max J = m$. Suppose that there is a solution to (4). At this point we split the proof into several parts.

Case 1. $30 < m$ and $n < m$. Lemma 2.2 implies that there is an odd primitive prime factor $p \mid u_m$. Since $n < m$, we have $p \mid B$. By definition p divides $u_{r(p)}$, but p is a primitive factor and hence we get the sequence of inequalities $n < m \leq r(p) \leq p - \epsilon(p) \leq L(B) - \epsilon(L(B))$.

Case 2. $30 < n$, $m < n$. The same way we derive $m < n \leq L(A) - \epsilon(L(A))$.

Case 3. $m, n \leq 30$. In this case, both m and n are bounded already.

It remains to show that for a given pair (P, Q) we can find all the solutions effectively. Indeed, if the sequence is fixed we can generate all of its terms up to the bounds in (5). For each possible choice of I and J the fundamental theorem of arithmetic changes (4) into an exponential Diophantine equation

$$\prod_{i \in I} p_{i1}^{\alpha_{i1}} p_{i2}^{\alpha_{i2}} \dots p_{in_i}^{\alpha_{in_i}} = \prod_{j \in J} q_{j1}^{\beta_{j1}} q_{j2}^{\beta_{j2}} \dots q_{jm_j}^{\beta_{jm_j}}, \tag{7}$$

where all p_{is} and q_{jt} are known primes. Expanding the product and collecting the same bases simplifies (7) to

$$p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k} = q_1^{\delta_1} q_2^{\delta_2} \dots q_l^{\delta_l}$$

with positive unknown exponents, where each γ_i and δ_j are linear functions of the exponents in (7). Thus all solutions can be found or parametrized (in case there are infinitely many) using elementary linear algebra. This provides the desired method and finishes the proof. □

We are left to prove Corollary 1.3. Since we have to solve (4) in the specific form of (6), we have an easier task on one hand. On the other, P and Q are now variables and for a complete solution some additional reasoning is also needed. At one point we use the fact that Lucas sequences are strong divisibility sequences.

Lemma 2.4. *Let $u = (u_n)_{n=0}^{\infty}$ be a Lucas sequence. Then for every positive m and n we have* $\gcd(u_m, u_n) = u_{\gcd(m,n)}$.

Proof. This result is also classical and was proven by Lucas [6]. It can be found in [7] also. □

Proof of Corollary 1.3. Let $u = (u_n)_{n=0}^{\infty}$ be a Lucas sequence corresponding to the pair (P, Q) and consider equation (6). Since this is just a very specific case of equation (4) with $A, B = \pm 1$ and $\alpha_i = \beta_j = 1$ for i, j, we can apply (5) to bound $\max I$ and $\max J$. In fact, we get

$$\max I, \max J \leq 30.$$

The equation is symmetric so we can assume that $\max I < \max J$. Set $\max J = m$. We split the proof into three parts.

Case 1. $m = 9, 11,\ 14 \leq m \leq 17,\ 19 \leq m \leq 29$. Using Theorem C in [1] we find that u_m does have a primitive divisor. By comparing prime factors on both sides of the equation we get that there is no solution in this case.

Case 2. $m = 5, 7, 8, 10, 12, 13, 18, 30$. Looking at Tables 1 and 3 in [1] we see there are just a few pairs (P, Q) to consider. We can extract them using the identities

$$P = a, \qquad Q = \frac{a^2 - b}{4}$$

and solve (6) by trial and error quickly.

Case 3. $m = 2, 3, 4, 6$. Observe that if Case 2 has been done then one finds that either $u_5 = \pm 1$ or has a primitive divisor. In the latter case, we use Lemma 2.4 to see that $\gcd(u_5, u_2u_3u_4u_6) = 1$ and hence there is no solution to (6), while in the former setting, we simply cancel u_5. Now we apply (3) and write u_2, u_3, u_4, u_6 as polynomials in P and Q and consider the equations for every I and J. In most cases, these are trivial and either can be solved quickly or there is no solution. However, some non-evident ones also arise and these happen when $m = 6$ and $n = 4$. We give details in a single case, the others can be solved similarly. Let $I = \{4\}$ and $J = \{6\}$. We have to solve

$$P^3 - 2PQ = P^5 - 4P^3Q + 3PQ^2.$$

Canceling P and factoring the right-hand side we get

$$P^2 - 2Q = (P^2 - 3Q)(P^2 - Q).$$

If there is a prime $p \mid P^2 - 2Q$, then a simple divisibility argument shows that $p \mid Q$. But $p \mid Q$ implies $p \nmid u_n$ for every $n \geq 1$ which contradicts the existence of such a prime (one can arrive at the same conclusion by checking the coprimality condition as well). Hence, $P^2 - 2Q = \pm 1$ is what remains to be checked. This gives

$$\pm 1 = (\pm 1 - Q)(\pm 1 + Q).$$

Solving it for Q shows that this is not a possibility either and hence there are no such solutions. □

3. Closing Remarks

We have the following natural question: can we improve the bounds (5) in Theorem 1.1? The answer is negative in general with the reason behind being that $r(p) = p - \epsilon(p)$ can occur and we cannot do better than $L(A) - \epsilon(L(A))$ or $L(B) - \epsilon(L(B))$. However a result of Kiss and Phong [5] shows that the ratio $(p - \epsilon(p))/r(p)$ is unbounded and that there exists a constant C, depending only on P and Q, such that

$$\frac{p - \epsilon(p)}{r(p)} \leq C \frac{p}{\log p}.$$

Hence, as the prime p gets larger we expect $r(p)$ to be a smaller factor of $p - \epsilon(p)$. In fact, for a given sequence, we may compute $r(p)$ for every $p \mid AB$ by looking at factors of $p - \epsilon(p)$ and replace (5) with

$$\max I \leq \max\{\max_{p|B} r(p), 30\}, \qquad \max J \leq \max\{\max_{p|A} r(p), 30\}.$$

We close with a short discussion on the naive method presented in the proof of Theorem 1.1. While being impractical due to the factorization involved, several improvements are possible. Since the way we described it was enough to prove Corollary 1.3 and we lack applications beside the distinct product property, we do not give much detail.

A specific case. We expect that if $A, B \in \{\pm 1\}$, then (4) can be completely solved with (P, Q) as variables making Corollary 1.3 more general. Observe that the proof of Corollary 1.3 applies in **Case 1** and **Case 2** with the latter involving only finitely many pairs (P, Q) for which the method of Theorem 1.1 works. Further, in **Case 3** we expect similar results. Nevertheless, things may need further work, since we use the factorization properties to cancel out terms entirely which is not possible for differing exponents. We do not prove or disprove the claim for the reasons mentioned before.

Reducing the bounds for small A and B. We can use the the stronger form of Lemma 2.2 as in [1] to reduce (5) to $\max I \leq \max\{L(B) - \epsilon(L(B)), 7\}$ and $\max J \leq \max\{L(A) -$

$\epsilon(L(A)), 7\}$ in almost every case. This way we get an improvement on (5), when A and B have prime factors up to 29 only.

Restrictions on I and J. Assume that one of A and B, let say A, is ± 1. If $L(B) \leq 30$, then we have relatively low bounds for $\max I$ and $\max J$ and can use the method. Hence suppose that $L(B) > 30$ and take an index n with $15 < n \leq \max I = L(B) + 1$. Obviously, n cannot have a multiple in J, since $\max J \leq 30$ and I, J are disjoint. Thus for every such n, if u_n has a primitive divisor (always has, if $(P, Q) \neq (\pm 1, 2)$), then it must divide B, otherwise Lemma 2.4 gives a contradiction by comparing the prime factors on both sides. This puts restrictions on the possible elements of I. This idea can be realized when $A \neq \pm 1$ as well, but one has to be more careful about how $\max I$ and $\max J$ relate to each other.

Acknowledgement

The author is grateful to the anonymous referee for his/her comments and suggestions which helped to improve the paper.

References

[1] Y. Bilu, G. Hanrot, and P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte)*, J. Reine Angew. Math., **539** (2001), 75–122.
[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math., (2) **15.1–4** (1913), 30–70.
[3] L. Hajdu and M. Szikszai, *On the GCD-s of k consecutive terms of Lucas sequences*, J. Number Theory, **132** (2012), 3056–3069.
[4] C. Kimberling, *Problem proposals*, Proceedings of the Seventeenth International Conference on Fibonacci Numbers and Their Applications, **55.5** (2017), 213-221.
[5] P. Kiss and B. M. Phong, *On a function concerning second order recurrences*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math., **21** (1978), 119–122.
[6] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–240 and 289–321.
[7] P. Ribenboim, *Little Book of Bigger Primes*, Second edition, Springer-Verlag, New York, 2004.
[8] `http://mathoverflow.net/questions/238505/distinctness-of-products-of-fibonacci-numbers`.

MSC2010: 11D61, 11B39

Institute of Mathematics, University of Debrecen, P.O. Box 400, H-4002 Debrecen, Hungary and MTA-DE Research Group "Equations Functions and Curves", Hungarian Academy of Sciences and University of Debrecen

E-mail address: `szikszai.marton@science.unideb.hu`