Bull. Math. Soc. Sci. Math. Roumanie
Tome 57(105) No. 4, 2014, 409–413

Equations with arithmetic functions of Pell numbers

by
[1]Florian Luca, [2]Pantelimon Stănică

Abstract

Here, we prove some diophantine results about the Euler function of Pell numbers and their Pell–Lucas companion sequence. For example, if the Euler function of the nth Pell number P_n or Pell–Lucas companion number Q_n is a power of 2, then $n \le 8$.

Key Words: Euler function, Pell numbers.
2010 Mathematics Subject Classification: Primary 11B39, Secondary 11A25.

1 Introduction

Let $\alpha = 1 + \sqrt{2}$ and $\beta = 1 - \sqrt{2}$ be the two roots of the quadratic equation $x^2 - 2x - 1 = 0$. Let $(P_n)_{n \ge 0}$ and $(Q_n)_{n \ge 0}$ be the Pell sequence and its companion of general terms

$$P_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{and} \qquad Q_n = \alpha^n + \beta^n$$

for all $n \ge 0$.

Let $\phi(m)$ and $\sigma(m)$ be the Euler function and the sum of divisors function of the positive integer m.

In this paper, we prove the following result.

Theorem 1. *The following statements hold:*

(i) The only nonnegative integer solutions of the equation $\phi(P_n) = 2^m$ are $(n, m) \in \{(1, 0), (2, 0), (3, 2), (4, 2), (8, 7)\}$. If $n > 1, t > 1$, the only nonnegative integer solutions to $\phi(P_n^t) = 2^m$ are $(n, t, m) = (2, t, t - 1), t \ge 2$.

(ii) The only nonnegative integer solutions of the equation $\phi(Q_n) = 2^m$ are $(n, m) \in \{(1, 0), (2, 1), (4, 4)\}$. If $n > 1, t > 1$, then there are no nonnegative solutions to $\phi(Q_n^t) = 2^m$.

(iii) The only nonnegative integer solutions of the equation $\sigma(P_n^t) = 2^m$ *are* $(n, t, m) = (1, t, 0)$, $t \geq 1$.

(iv) The equation $\sigma(Q_n^t) = 2^m$ *does not have nonnegative integer solutions* (n, t, m), $t \geq 1$.

Before proceeding further, we mention that several other Diophantine equations with binary recurrences have been studied previously. For example, the above Diophantine equations with the numbers P_n and Q_n replaced by the Fibonacci and Lucas numbers F_n and L_n were studied in [4]. In [5], it was shown that the largest Fibonacci number whose Euler function is a rep-digit; i.e., a number whose decimal representation consists of a string of the same repeating digit $d \in \{1, 2, \ldots, 9\}$, is $\phi(F_{11}) = 88$. In [6], it was shown that there are no rep-digits with two or more digits which are multiply perfect, namely numbers who divide the sum of their divisors.

We record a corollary of our theorem.

Corollary 1. *A polygon with* P_n*, respectively,* Q_n *sides can be constructed with a ruler and compass if and only if* $n \in \{1, 2, 3, 4, 8\}$*, respectively,* $n \in \{1, 2, 4\}$.

Proof. Recall that by a theorem of Gauss, the regular polygon with $m \geq 3$ sides can be constructed with the ruler and the compass if and only if $\phi(m)$ is a power of 2. By our theorem, we infer the corollary. □

A lot of research promoted by Erdős and his collaborators has been devoted on investigating the intersections of ranges of various arithmetic functions. We added into the mix the binary recurrences. One of the reasons why we consider such problems interesting is that on the one hand Euler's phi-function and the sum of divisors function are multiplicative so they behave well with respect to multiplicative properties of the integers while a linearly recurrent sequence displays an additive pattern. It is the intersection between the multiplicative and additive structures that makes such questions interesting. Of course, it would be desirable to completely describe the image of an arbitrary arithmetical function acting on a second, or higher-order linearly recurrent sequence, but that problem seems hopelessly difficult.

One the ingredients of our proof is the notion of a primitive divisor for the sequences $\{P_n\}_{n\geq 1}$ and $\{Q_n\}_{n\geq 1}$. A primitive divisor of P_n (or Q_n) is a prime factor of P_n (or Q_n) which does not divide P_m (or Q_m) for any $1 \leq m < n$. Such a primitive divisor always exists for all $n \geq 13$, by a celebrated result of Carmichael of 1913 ([2]). See also [1] for the most general result concerning primitive divisors of Lucas sequences.

2 The Proof

If s is a positive integer such that $\phi(s)$ is a power of 2, then s has the form $s = 2^a p_1 \ldots p_\ell$, where $a \geq 0$ and $p_1, \ldots, p_\ell$ are distinct Fermat primes. For more information on Fermat numbers, see [3]. Further, if $d \mid s$, then also $\phi(d)$ is a power of 2.

So, for the Pell sequence, we first check that $\phi(P_{2^k})$ is a power of 2 for $k = 0, 1, 2, 3$ but not for $k = 4$. We also check that $\phi(P_3)$ is a power of 2 but $\phi(P_9)$ is not. Suppose now that $p > 3$ is some prime and that $\phi(P_p) = 2^k$. Since P_p is odd and coprime to 3 and 5, it follows that $P_p = p_1 \cdots p_\ell$, where $p_i = 2^{2^{b_i}} + 1$ for some $2 \leq b_1 < \cdots < b_\ell$. Since $p_i \equiv 1 \pmod 8$, it follows that $(8|p_i) = 1$ for $i = 1, \ldots, \ell$. Here and in what follows, for an odd prime p and an integer a we use $(a|p)$ for the Legendre symbol. Since p_i is a prime factor of P_p and the discriminant $\Delta = (\alpha - \beta)^2 = 8$ of the Pell sequence is a quadratic residue modulo p_i, it follows that $p_i \equiv 1 \pmod p$. However, this is false since $p_i - 1$ is a power of 2. This shows that if $\phi(P_n)$ is a power of 2, then $n \mid 24$, and we get the solutions from the first claim of (i). Certainly, if $t > 1$ and $\phi(P_n^t) = 2^m$, then we must have $P_n^t = 2^a p_1 \ldots p_\ell$ (for some integer a, and odd primes $p_1, \ldots, p_\ell$), which implies that, in fact, $\ell = 0$ and $P_n^t = 2^a$, and the previous argument can also be used, obtaining the second claim of (i).

We now look at $\phi(Q_n)$ being a power of 2. Note that

$$Q_{2^k} = \alpha^{2^k} + \beta^{2^k} = 2 \sum_{\substack{0 \le i \le 2^k \\ i \equiv 0 \pmod 2}} \binom{2^n}{i} 2^{i/2}.$$

Further, for even $i \in \{1, \ldots, 2^k\}$, we have

$$\begin{aligned}
\nu_2\left(\binom{2^k}{i} 2^{i/2}\right) &= \nu_2\left(\frac{2^k(2^k-1)\cdots(2^k-(i-1))}{i!}\right) + i/2 \\
&= k + \nu_2\left(\frac{(i-1)!}{i!}\right) + i/2 \\
&= k + i/2 - \nu_2(i),
\end{aligned}$$

where $\nu_2(m)$ is the exponent of 2 in the factorization of the positive integers m. Since $i/2 \ge \nu_2(i)$ for all even positive integers i, we get that

$$Q_{2^k}/2 \equiv 1 \pmod{2^k}. \tag{2.1}$$

To compute the exact exponent of 2 in $Q_{2^k}/2 - 1$, we proceed as follows. Suppose that $k \ge 2$. Then

$$\begin{aligned}
Q_{2^k}/2 - 1 &= \frac{\alpha^{2^k} + \beta^{2^k}}{2} - 1 = \frac{\alpha^{2^k} + \beta^{2^k} - 2}{2} = \frac{1}{2}\left(\alpha^{2^{k-1}} - \beta^{2^{k-1}}\right)^2 \\
&= \frac{1}{2}(\alpha - \beta)^2(\alpha + \beta)^2(\alpha^2 + \beta^2)^2 \cdots (\alpha^{2^{k-2}} + \beta^{2^{k-2}})^2 \\
&= 4Q_1^2 Q_2^2 \cdots Q_{2^{k-2}}^2.
\end{aligned}$$

From (2.1), we get that $\nu_2(Q_{2^j}) = 1$ for all $j \ge 0$. Hence, $\nu_2(Q_{2^k}/2 - 1) = 2k$ for $k \ge 2$. Obviously, for $k = 1$ we get that $\nu_2(Q_2/2 - 1) = 1$.

We now check that $\phi(Q_2)$ and $\phi(Q_4)$ are powers of 2 and that $\phi(Q_{2^k})$ is not a power of 2 for $k \in \{3, 4\}$. Suppose that $\phi(Q_{2^k})$ is a power of 2 for some $k \ge 5$. Write

$$Q_{2^k}/2 = (2^{2^{b_1}} + 1) \cdots (2^{2^{b_\ell}} + 1)$$

for some $2 \le b_1 < \cdots < b_\ell$ such that $p_i = 2^{2^{b_i}} + 1$ is prime for all $i = 1, \ldots, \ell$. Then $2^{b_1} = \nu_2(Q_{2^k}/2 - 1) = 2k$. Further, for $j \ge 2$, we use (2.1) to write $Q_{2^j} = 2(1 + 2^{2j}\alpha_j)$ for some odd integer α_j. Then

$$Q_{2^k}/2 - 1 = 2^{2k} 3^2 \cdot 17^2 (1 + 2^6\alpha_3)^2 \cdots (1 + 2^{2(k-2)}\alpha_{k-2})^2.$$

On the other hand,

$$Q_{2^k}/2 - 1 = 2^{2^{b_1}} + 2^{2^{b_2}} + \text{higher powers of } 2.$$

Thus, we get

$$3^2 \cdot 17^2 (1 + 2^6 \alpha_3)^2 \cdots (1 + 2^{2(k-2)} \alpha_{k-2})^2 = 1 + 2^{2^{b_2} - 2^{b_1}} + \text{higher powers of } 2.$$

The left hand side above is congruent to 9 modulo 16. This gives that $2^{b_2} - 2^{b_1} = 3$, and its only solution is $b_1 = 0,\ b_2 = 1$. Thus, $p_1 = 3$ and this is impossible because 3 cannot divide Q_{2^k} for some $k \geq 5$. Thus, if $\phi(Q_n)$ is a power of 2, we deduce that $n = 2^a m$, where $a \in \{0, 1, 2\}$ and m is odd. Let us show that $m = 1$. Assume that this is not so. Fix a. Let p be some prime factor of m. Then $\phi(Q_{2^a p})$ is also a power of 2. Let $q = 2^{2^b} + 1$ be any primitive prime factor of $Q_{2^a p}$. Then q is not 3 or 5, so, in particular, $q \equiv 1 \pmod 8$. Thus, $(8|q) = 1$, showing that $q \mid P_{q-1}$. Since also $q \mid Q_{2^a p} \mid P_{2^{a+1} p} \mid P_{8p}$, we get that $q \mid \gcd(P_{q-1}, P_{8p})$. Since $q - 1$ is a power of 2, we get that $q \mid P_8$, so that $q \in \{3, 17\}$, which is impossible because we chose q to be primitive for $Q_{2^a p}$. This shows that there is no number of the form $Q_{2^a p}$ for some $a \in \{0, 1, 2\}$ and odd prime p whose Euler function is a power of 2. This takes care of the first part of (ii). Certainly, if $t > 1$ and $\phi(Q_n^t) = 2^m$, since, then, we must have $Q_n^t = 2^a p_1 \dots p_\ell$, it follows that $Q_n^t = 2^a$, and we can use the previous argument, which shows the second part of (ii).

We now move on to the σ function. Using a similar reasoning as before, we can assume $t = 1$. If $\sigma(s)$ is a power of 2, then $s = p_1 \cdots p_\ell$, where $p_i = 2^{q_i} - 1$ are distinct Mersenne primes for $i = 1, \dots, \ell$. In particular, s is odd. Further, if $d \mid s$, then also $\sigma(d)$ is a power of 2. So, assume that P_n has the property that the sum of its divisors is a power of 2. Then n is odd. Let p be some prime factor of n. Then the sum of divisors of P_p is a power of 2. Write

$$P_p = p_1 \cdots p_\ell, \tag{2.2}$$

where $p_i = 2^{q_i} - 1$ are Mersenne primes with $q_1 < \cdots < q_\ell$. Clearly, $q_1 > 2$, because 3 does not divide P_p for any prime index p. Since $p_i \equiv 7 \pmod 8$, it follows that $(8|p_i) = 1$. Thus, $p_i \equiv 1 \pmod p$. In particular, $p \mid 2^{q_1} - 2 = 2(2^{(q_1-1)/2} - 1)(2^{(q_1-1)/2} + 1)$. Thus, $2^{(q_1-1)/2} + 1 \geq p$. Reducing P_n modulo 8 we discover that its period is $0, 1, 2, 5, 4, 5, 2, 1$ of length 8. Since $P_p \equiv (-1)^\ell \pmod 8$ from formula (2.2), and there is no Pell number P_n congruent to 7 modulo 8, we get that ℓ is even. Hence,

$$P_p = 1 - 2^{q_1} + \text{higher powers of } 2.$$

We thus get that $q_1 = \nu_2(P_p - 1)$. One checks that $P_p - 1 = P_{(p-1)/2} Q_{(p+1)/2}$ or $P_{(p+1)/2} Q_{(p-1)/2}$ according to the residue class of p modulo 4. Furthermore, $\nu_2(Q_m) = 1$ for all positive integers m, whereas $\nu_2(P_m) = \nu_2(m)$. Thus, we get that $q_1 = \nu_2(P_p - 1) \leq 1 + \max\{\nu_2((p-1)/2), \nu_2((p+1)/2)\}$, giving that

$$2^{q_1} \leq p + 1 \leq 2^{(q_1-1)/2} + 2.$$

The above inequality fails for all primes $q_1 \geq 3$. Thus, the only n such that $\sigma(P_n)$ is a power of 2 is $n = 1$. This takes care of (iii). Finally, (iv) follows from the fact that Q_n is even for all n, so $\sigma(Q_n)$ cannot be a power of 2.

Acknowledgement. This paper was written during a visit of F. L. at the Applied Mathematics Department of Naval Postgraduate School in December, 2012. During the preparation of this paper, F. L. was supported in part by Project PAPIIT IN104512 (UNAM), VSP N62909-12-1-4046 (Department of the US Navy, ONR–Global) and a Marcos Moshinsky fellowship.

References

[1] Y. Bilu, G. Hanrot, P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122. With an appendix by M. Mignotte.

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

[3] M. Křížek, F. Luca, L. Somer, 17 *lectures on Fermat numbers. From number theory to geometry. With a foreword by Alena Šolcová*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 9. Springer-Verlag, New York, 2001.

[4] F. Luca, Equations involving arithmetic functions of Fibonacci numbers, *Fibonacci Quart.* **38** (2000), 49–55.

[5] F. Luca and M. Mignotte, $\phi(F_{11}) = 88$, *Divulg. Mat.* **14** (2006), 101–106.

[6] F. Luca and P. Pollack, Multiperfect numbers with identical digits, *J. Number Theory* **131** (2011), 260–284.

Received: 10.01.2013
Accepted: 19.04.2014

[1] Mathematical Institute, UNAM Juriquilla
Juriquilla, 76230 Santiago de Querétaro
Querétaro de Arteaga, México
and
School of Mathematics
University of the Witwatersrand
P. O. Box Wits 2050, South Africa
E-mail: `fluca@matmor.unam.mx`

[2] Applied Mathematics Department
Naval Postgraduate School
Monterey, CA 93943, USA
E-mail: `pstanica@nps.edu`