AN EXTENSION OF THE PERIODICITY OF AN EXTENDED FIBONACCI FAMILY

RUSSELL EULER AND JAWAD SADEK

ABSTRACT. The Fibonacci congruence $F_{\phi(m)+n} \equiv F_n \pmod{\frac{m}{d}}$ has been extended to Pell numbers, Lucas numbers, and Pell-Lucas numbers, where ϕ is the Euler phi-function, $m = a^2 - a - 1$, $d = (2a-1, m)$, $a \geq 2$ is an integer, and (x, y) denotes the greatest common divisor of the integers x and y. We prove that the generalization holds for a larger class of integers than the one containing the integers of the form $m = a^2 - a - 1$.

1. INTRODUCTION

Let a and λ be integers such that $a \geq 2$ and $\lambda > 0$. Let $m(a;\lambda) = a^2 - \lambda a - 1$. Unless it is needed for clarity, the dependence of $m(a;\lambda)$ on a will be suppressed and the notation m_λ will be used instead. Also, if N is a positive integer, then a prime of the form $Nk \pm 1$, where k is a positive integer, will be called $(Nk \pm 1)$-prime.

In [3] and [6], the authors show that if $m_1 = a^2 - a - 1$ and $d = (m_1, 2a-1)$, the greatest common divisor of m_1 and $2a - 1$, then

$$F_{\phi(m_1)+n} \equiv F_n \left(\text{mod } \frac{m_1}{d}\right), \tag{1.1}$$

where F_n is the nth Fibonacci number and ϕ is the Euler phi-function [1]. In [4], the author extends this congruence to Pell numbers, Lucas numbers, and Pell-Lucas numbers, denoted by P_n, L_n, and Q_n, respectively. In this article we show that the results in [3] and [4] are special cases of a more general form, say m, of m_λ. Precisely, if $c = 0$ or 1, we show that

$$F_{\phi(m_\lambda)+n} \equiv F_n \left(\text{mod } \frac{m}{d}\right), \tag{1.2}$$

where $d = (\lambda^2 + 4, m)$ and

$$m = 5^c M_1, \tag{1.3}$$

where M_1 has only $(10k \pm 1)$-primes in its factorization. Also,

$$P_{\phi(m)+n} \equiv P_n \left(\text{mod } \frac{m}{d}\right) \quad \text{and } Q_{\phi(m_\lambda)+n} \equiv Q_n \left(\text{mod } \frac{m}{d}\right),$$

and

$$m = 2^c M_2, \tag{1.4}$$

where M_2 has only $(8k \pm 1)$-primes in its factorization.

We show that $m_1 = a^2 - a - 1$ is of the form (1.3), whereas $m = 59$ or $m = 61$, for instance, is not of the form m_1 for any integer a. Similarly, $m_2 = a^2 - 2a - 1$ is of the form (1.4), and although $m = 41$ and $m = 49$ are of the form (1.4), neither are of the form m_2. Thus, our results hold for a larger class of the positive integers. Unless it is stated otherwise, throughout this paper j, k, k_i, p, p_i, r, and r_i will be nonnegative integers, h will denote an integer such that $0 \leq h \leq 9$ but $h \neq 3$, and $c = 0$ or 1.

2. Periodicity of Fibonacci and Pell Numbers

We note first that for nonnegative integers n, the recurrence relation defined by

$$g_{n+2} = \lambda g_{n+1} + g_n \tag{2.1}$$

with initial conditions

$$g_0 = A \quad \text{and} \quad g_1 = B$$

can be used to study the Fibonacci, Lucas, Pell, and Pell-Lucas numbers in a unified way. In particular, if A $= 0, B = \lambda = 1$, then $g_n = F_n$. If $A = 2$, $B = \lambda = 1$, then $g_n = L_n$. If $A = 0$, $B = 1$, and $\lambda = 2$, then $g_n = P_n$. If $A = B = \lambda = 2$, then $g_n = Q_n$.

Following the standard procedures for solving second-order homogeneous recurrence relations with constant coefficients [5], the Binet formula for the integer family $\{g_n\}$ defined by (2.1) is given by

$$g_n = \frac{1}{\sqrt{\lambda^2+4}}\left([B - Av]u^n - [B - Au]v^n\right), \tag{2.2}$$

where $u = \frac{1}{2}\left(\lambda + \sqrt{\lambda^2+4}\right), v = \frac{1}{2}\left(\lambda - \sqrt{\lambda^2+4}\right)$, and A and B are nonnegative integers.

To show that the value m_λ need not be restricted to the form $m_\lambda = a^2 - \lambda a - 1$, we prove the following lemmas.

Lemma 2.1. *The prime factorization of $m(a; 1)$ has at most one factor of 5. The prime factorization $m(a; 2)$ has at most one factor of 2.*

Proof. Since $a^2 \equiv 0, 1, 4 \pmod 5$, $m(a; 1) \equiv 0, 1, 4 \pmod 5$. We claim that 5 divides $m(a; 1)$ if and only if $a = 5j + 3$. This is so because the cases $a = 5j$, $5j + 1$, $5j + 2$, $5j + 4$ are congruent to $4, 4, 1, 1 \pmod 5$, respectively. Furthermore, for $a = 5j + 3$, $m(a; 1) = 5(5j^2 + 5j + 1)$. Since the factor $(5j^2 + 5j + 1) = 5j(j + 1) + 1$ is not a multiple of 5, the desired result follows. Similarly, $m(a; 2) \equiv 2, 6, 7 \pmod 8$. In each case where $m(a; 2)$ is even, it can be written as $4M' + 2$, where M' is a nonnegative integer. The second claim of the lemma follows. □

In the following lemma, $10k \pm 1$ and $8k \pm 1$ are not necessarily primes.

Lemma 2.2. *$m(a; 1) = 5^c(10k \pm 1)$ and $m(a; 2) = 2^c(8k \pm 1)$.*

Proof. In Lemma 2.1, we showed that $5 \mid m(a; 1)$ if and only if $a = 5k + 3$ and in that case, $m(a; 1) = 5(5j^2 + 5j + 1) = 5(10k + 1)$. If $5 \nmid m(a; 1)$, $a^2 \equiv 0, 1, 4, 5, 6, 9 \pmod{10}$, $m(a; 1) \equiv \pm 1 \pmod{10}$, and so the desired follows. For $m(a; 2)$, we let $a = 8k \pm k_i$ where $0 \le k_i \le 7$ and argue similarly. □

Lemma 2.3. *Let b be a positive integer. If $b \mid m(a; \lambda)$, then $b \mid m(a - b; \lambda)$.*

Proof.

$$\begin{aligned} m(a - b; \lambda) &= (a - b)^2 - \lambda(a - b) - 1 \\ &= a^2 - \lambda a - 1 + b(b - 2a + \lambda). \end{aligned}$$

The lemma now follows. □

Lemma 2.4. *If $m(a; \lambda)$ is not prime, then it has a factor smaller than a.*

Proof. Since $m(a; \lambda) = a^2 - \lambda a - 1 < a^2$, the lemma follows. □

Lemma 2.5. *If $5 \nmid m(a; 1)$, then $m(a; 1) = (10k \pm 1)^{r_1}$, where r_1 is odd. Also, if $2 \nmid m(a; 2)$ then $m(a; 2) = (8k_2 \pm 1)^{r_2}$, where r_2 is odd.*

Proof. Since $(a-2)^2 < m(a;2) < (a-1)^2 < m(a;1) < a^2$, $m(a;\lambda)$ cannot be the square of an integer for $\lambda = 1$ or $\lambda = 2$. Thus r_1 and r_2 must be odd. For $\lambda = 1$, since $m(a;1) = a^2 - a - 1 = a(a-1) - 1$ is odd, and $5 \nmid m(a;1)$, we need only to consider the factor $10k \pm 3$. Now $(10k \pm 3)^{r_1} = (10k \pm 3)^{2j+1} = ((10k \pm 3)^2)^j (10k \pm 3) = (10k' \pm 1)(10k \pm 3) = 10k'' \pm 3$. This contradicts Lemma 2.2, so $p = 10k \pm 1$. A similar argument takes care of the case where $\lambda = 2$. □

Lemma 2.6. *$m(a;1)$ is not of the form $(10k_1 \pm 3)(10k_2 \pm 3)$ and $m(a;2)$ is not of the form $(8k_1 \pm 3)(8k_2 \pm 3)$.*

Proof. Multiplying out $(10k_1 \pm 3)(10k_2 \pm h) = m(a;1)$ does not yield an expression of the form $5^c(10k \pm 1)$. This contradicts Lemma 2.2. Similarly, by simple multiplication, $m(a;2)$ is not of the form $(8k_1 \pm 3)(8k_2 \pm h)$. Now we argue the case where $\lambda = 1$ and $h = 3$. For $\lambda = 1$, assume that a is the first positive integer such that $10k \pm 3$ divides $m(a,1)$ and that $m(a;1) = (10k_1 \pm 3)(10k_2 \pm 3)$. By Lemma 2.4 we may assume that $10k_1 \pm 3$ is smaller than a. But by Lemma 2.3, $b = a - (10k \pm 3)$ would be a positive integer smaller than a that divides $m(a-b;1)$. However, a was assumed to be the smallest such number. Since by Lemma 2.5, the case $m(a;1) = (10k \pm 3)^r$ cannot occur, we have a contradiction. The case where $\lambda = 2$ and $h = 3$ is similar. □

Lemma 2.7. *$m(a;1)$ is not of the form $(10k_1 \pm 3)^2(10k_2 \pm 1)$ and $m(a;2)$ is not of the form $(8k_1 \pm 3)^2(8k_2 \pm 1))$.*

Proof. For $\lambda = 1$, $m(a;1) = (10k_1 \pm 3)^2(10k_2 \pm 1) = (10k_1 \pm 3)(10k' \pm 3)$. The desired result follows now from Lemma 2.6. Similarly, the result holds for $\lambda = 2$. □

Now we state our first result.

Theorem 2.8. *$m(a;1) = 5^c(10p_1 \pm 1)^{c_1}(10p_2 \pm 1)^{c_2} \cdots (10p_r \pm 1)^{c_r}$ and $m(a;2) = 2^c(8p_1 \pm 1)^{r_1}(8p_2 \pm 1)^{r_2} \cdots (8p_s \pm 1)^{r_s}$.*

Proof. By Lemmas 2.2 and 2.5 $m(a;1) = 5^c(10k \pm 1)$ and $m(a;1)$ are squares of some integers. Since $(10p \pm 3)^{2k+1} = 10p' \pm 3$, and $(10p \pm h)^r = 10p' \pm 1$, we only need to check the cases $(10k_1 \pm 3)^2(10k_2 \pm 1)$ and $(10k_1 \pm 3)(10k_2 \pm 3)$. The theorem follows now by Lemmas 2.6 and 2.7. The proof of $m(a;2)$ is similar. □

To prove that (1.1) holds for any m of the form (1.2), we need the following lemmas [2].

Lemma 2.9. *If m is of the form (1.3), then $x^2 \equiv 5 \pmod{m}$ has a solution.*

Lemma 2.10. *If $(2,p) = 1$, then $2x \equiv 1 \pmod{p}$ has a solution.*

Lemma 2.11. *If m is of the form (1.4), then $x^2 \equiv 2 \pmod{m}$ has a solution.*

For the rest of the paper we use the following notations. We let t_λ be a least residue satisfying $x^2 \equiv \lambda^2 + 4 \pmod{\frac{m}{d}}$, if it exists, ν the multiplicative inverse of $\frac{1}{2} \pmod{\frac{m}{d}}$, and w_λ be the multiplicative inverse $\frac{1}{t_\lambda}$, when it exists, of $t_\lambda \pmod{\frac{m}{d}}$ [1]. Now we prove our generalization of the results in [4].

Theorem 2.12. *Let $\frac{m}{d}$ be an odd integer with prime factorization $\frac{m}{d} = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$. Assume $(\lambda^2 + 4, \frac{m}{d}) = 1$ and $(d, \frac{m}{d}) = 1$. If $x^2 \equiv \lambda^2 + 4 \pmod{\frac{m}{d}}$ has a solution and $\frac{1}{t_\lambda} \pmod{\frac{m}{d}}$ exists, then $g_{\phi(m)+n} \equiv g_n \pmod{\frac{m}{d}}$.*

Proof. If the integer t_λ satisfies $(t_\lambda, \frac{m}{d}) = D > 1$, then $(t_\lambda^2, \frac{m}{d}) = (\lambda^2+4, \frac{m}{d}) \geq D > 1$. This contradicts the assumption of the theorem. Also, if $(\lambda \pm \sqrt{\lambda^2+4}, \frac{m}{d}) > 1$, then $\lambda \pm \sqrt{\lambda^2+4} = kp_i$, for some integers i and k. Squaring and factoring yield $2\lambda\left(\lambda \pm \sqrt{\lambda^2+4}\right) + 4 = k^2 p_i^2$. Thus, $2\lambda(kp_i) + 4 = k^2 p_i^2$ and so $p_i \mid 4$. Since $\frac{m}{d}$ is odd, we have a contradiction. Now we proceed using (2.2), the fact that $\phi(m) = \phi(\frac{m}{d})\phi(d)$, and Euler's Theorem.

$$\begin{aligned}
g_{\phi(m)+n} &= \frac{1}{\sqrt{\lambda^2+4}}\left([B-Av]\left\{\frac{\lambda+\sqrt{\lambda^2+4}}{2}\right\}^{\phi(m)+n} - [B-Au]\left\{\frac{\lambda-\sqrt{\lambda^2+4}}{2}\right\}^{\phi(m)+n}\right)\\
&\equiv \nu^{\phi(m)+n} w_\lambda \left([B-Av]\left\{(\lambda+t_\lambda)^{\phi(\frac{m}{d})}\right\}^{\phi(d)}[\lambda+t_\lambda]^n\right.\\
&\quad \left. - [B-Au]\left\{(\lambda-t_\lambda)^{\phi(\frac{m}{d})}\right\}^{\phi(d)}[\lambda-t_\lambda]^n\right)\left(\bmod \frac{m}{d}\right)\\
&\equiv \nu^n w_\lambda \left([B-Av]\{\lambda+t_\lambda\}^n - [B-Au]\{\lambda-t_\lambda\}^n\right)\left(\bmod \frac{m}{d}\right).
\end{aligned}$$

Similarly,

$$\begin{aligned}
g_n &= \frac{1}{\sqrt{\lambda^2+4}}\left([B-Av]\left\{\frac{\lambda+\sqrt{\lambda^2+4}}{2}\right\}^{n} - [B-Au]\left\{\frac{\lambda-\sqrt{\lambda^2+4}}{2}\right\}^{n}\right)\\
&\equiv \nu^n w_\lambda \left([B-Av]\{\lambda+t_\lambda\}^n - [B-Au]\{\lambda-t_\lambda\}^n\right)(\bmod \frac{m}{d}).
\end{aligned}$$

The theorem follows. ☐

Corollary 2.13. *If m is of the form* (1.3)*, then $F_{\phi(m)+n} \equiv F_n (mod\ \frac{m}{d})$.*

Proof. We take $\lambda = 1$, $g_0 = 0$, and $g_1 = 1$. By Lemmas 2.7 and 2.9, the congruences $x^2 \equiv 5 \pmod{\frac{m}{d}}$ and $2x \equiv 1 (\bmod \frac{m}{d})$ have integral solutions t_1 and ν, respectively. Since $(5, \frac{m}{5}) = 1, (1+t_1, \frac{m}{d}) = 1$. It follows from Lemma 2.2 and Theorem 2.12 that

$$F_{\phi(m)+n} \equiv F_n \left(\bmod \frac{m}{d}\right). \tag{2.3}$$

☐

Similarly, using Lemmas 2.2, 2.10, and 2.11, and Corollary 2.12 we get

$$P_{\phi(m)+n} \equiv P_n \left(\bmod \frac{m}{d}\right) \tag{2.4}$$

when m is of the form (1.4).

3. Periodicity of Lucas and Pell-Lucas Numbers

The following addition formulas are well-known [4]:

$$L_{m+n} = F_m L_{n-1} + F_{m+1} L_n, \qquad Q_{m+n} = P_m Q_{n-1} + P_{m+1} Q_n. \tag{3.1}$$

Theorem 3.1. *If m is of the form* (1.4) *and $d = (5, m)$, then $L_{\phi(m)+n} \equiv L_n$ (mod $\frac{m}{d}$).*

Proof. By (2.3), $F_{\phi(m)} \equiv F_0 \equiv 0 \left(\bmod \frac{m}{d}\right)$ and $F_{\phi(m)+1} \equiv F_1 \equiv 1 \left(\bmod \frac{m}{d}\right)$.

Thus, from (3.1),

$$\begin{aligned} L_{\phi(m)+n} &= F_{\phi(m)}L_{n-1} + F_{\phi(m)+1}L_n \\ &\equiv (0 + L_n) \pmod{\frac{m}{d}} \\ &\equiv L_n \pmod{\frac{m}{d}}. \end{aligned}$$

□

A similar theorem holds for the Pell-Lucas numbers Q_n. Precisely, $Q_{\phi(m)+n} \equiv Q_n \pmod{\frac{m}{d}}$, where m and d are as used in Theorem 3.1. In fact, by (2.4), $P_{\phi(m)} \equiv P_0 \equiv 0 \left(\bmod \frac{m}{d}\right)$ and $P_{\phi(m)+1} \equiv P_1 \equiv 1 \left(\bmod \frac{m}{d}\right)$. The result now follows from (3.1).

ACKNOWLEDGMENT

The authors thank the anonymous referee for detailed comments that improved the clarity and presentation of this paper.

References

[1] J. P. Dence and T. P. Dence, *Elements of the Theory of Numbers*, 1st Edition, Academic Press, New York, 1999.

[2] R. Euler and J. Sadek, *Congruence relations from Binet forms*, The Fibonacci Quarterly, **50.3** (2012), 246–251.

[3] A. R. Gugheri, *Periodicity of the Fibonacci sequence*, Mathematical Spectrum, **45** (2012/2013), 37–38.

[4] T. Koshy, *Abbas Rouholamini Gugheri's congruence for an extended Fibonacci family*, Mathematical Spectrum, **47** (2014/2015), 76–80.

[5] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley-Interscience, New York, 2001.

[6] H. Kwong, *Problem B-1122*, The Fibonacci Quarterly, **52.1** (2014), 82–83.

MSC2010: 11B39, 11B99

Department of Mathematics and Statistics, Northwest Missouri State University, Maryville, MO, 64468

E-mail address: reuler@nwmissouri.edu

Department of Mathematics and Statistics, Northwest Missouri State University, Maryville, MO, 64468

E-mail address: jawads@nwmissouri.edu