CONGRUENCE RELATIONS FROM BINET FORMS

RUSSELL EULER AND JAWAD SADEK

Abstract. We apply techniques from modular arithmetic directly to the Binet forms for Fibonacci, Lucas, and Pell numbers. We illustrate the usefulness of these techniques by deriving new results and simplifying some proofs for well-known results.

1. Introduction

In this paper, we will give simple proofs of some known results involving Fibonacci, Lucas and Pell numbers. We will also derive some new results involving these numbers. These proofs and derivations will rely directly on the well-known Binet formulas for these numbers and on the properties of congruence modulo p, where p will denote an odd prime unless otherwise stated. To the best of our knowledge, the techniques are new in the sense that they have not been used in this context. In addition, these techniques simplify the proofs of many well-known identities, and generate a myriad of new identities and relationships. The examples we will give underscore the power of the overriding techniques. We start with the theoretical basis for our methods.

Recall that the Binet formulas for the Lucas, Fibonacci, and Pell numbers are given by

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n, \tag{1.1}$$

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right], \tag{1.2}$$

and

$$P_n = \frac{1}{2\sqrt{2}}\left[\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n\right], \tag{1.3}$$

respectively. To apply congruence properties to these formulas, one has to overcome two potential problems: division by a positive integer and taking the square roots of 5 and 2.

First, since p is assumed to be an odd prime, the elements of $Z[p]$ form a field under multiplication and addition modulo p, and so every nonzero element in $Z[p]$ has a multiplicative inverse. Hence $\frac{1}{a}$, where a is a positive integer, is well-defined. For instance, since $2 \times 4 \equiv 1 \pmod 7$, $\frac{1}{2} \equiv 4 \pmod 7$.

Secondly, for the expressions $\sqrt{5}$ and $\sqrt{2}$ to be meaningful in the field $Z[p]$, the congruences $x^2 \equiv 5 \pmod p$ and $x^2 \equiv 2 \pmod p$ must have solutions. This is to say that 5 and 2 are quadratic residues modulo p. To investigate when 5 and 2 are quadratic residues modulo p we appeal to the Euler criterion [4, p. 142–43], that states *if $gcd(m, p) = 1$, then m is a quadratic residue modulo p if and only if* $m^{\frac{(p-1)}{2}} \equiv 1 \pmod p$. We will give necessary and sufficient conditions on p for the square roots of 5 and 2 to exist modulo p.

Finally, we recall, in this context, the Legendre symbol, (m/p), which is defined by $(m/p) = +1$ if both m is not congruent to $0 \pmod p$ and m is a quadratic residue mod p; $(m/p) = -1$ otherwise.

2. Application to Pell Numbers

The Pell numbers are defined recursively by $P_0 = 0$, $P_1 = 1$, and $P_{n+2} = 2P_{n+1} + P_n$ for all $n \geq 0$. The Binet formula for the Pell numbers is given in (1.3). It is desirable for 2 to be congruent to a square modulo p. It is well-known [3, p. 142], that $(2/p) = 1$ if and only if $p \equiv 1$ or $7 \pmod 8$ and so

$$x^2 \equiv 2 \pmod p \tag{2.1}$$

will have a solution. Let r be a least residue satisfying (2.1). Then, from (1.3),

$$P_n \equiv \frac{1}{2r}\left[(1+r)^n - (1-r)^n\right] \pmod p.$$

Furthermore, we desire $\frac{1}{2r} \equiv y \pmod p$ or some integer y. That is,

$$2ry \equiv 1 \pmod p. \tag{2.2}$$

Since $(2r, p) = 1$, (2.2) will have a solution, say s. Therefore,

$$P_n \equiv s\left[(1+r)^n - (1-r)^n\right] \pmod p. \tag{2.3}$$

Many interesting results can be obtained from (2.3) using specific values for p. Some values of p that could be used are 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, and 103. As an illustration of our techniques, we offer the following examples.

Example 1. *7 divides $P_n + P_{n+2k} + P_{n+4k}$ for all $n \geq 0$ if and only if $k = 3j + 1$ or $k = 3j + 2$.*

First notice that (1.3) can be written as

$$P_n \equiv \left[(-1)^n 2^n - 4^n\right] \pmod 7 \tag{2.4}$$

since $2 \equiv 9 \pmod 7$ and $\frac{1}{6} \equiv -1 \pmod 7$. Therefore,

$$\begin{aligned}
P_n + P_{n+2k} + P_{n+4k} &\equiv \Big[(-1)^n 2^n - 4^n + (-1)^{n+2k} 2^{n+2k} - 4^{n+2k} \\
&\qquad + (-1)^{n+4k} 2^{n+4k} - 4^{n+4k}\Big] \pmod 7 \\
&\equiv \Big[(-1)^n 2^n (1 + 2^{2k} + 2^{4k}) - 4^n (1 + 4^{2k} + 4^{4k})\Big] \pmod 7 \\
&\equiv \Big[(-1)^n 2^n (1 + 2^{2k} + (2^4)^k) - 2^{2n} (1 + (4^2)^k + (4^4)^k)\Big] \pmod 7 \\
&\equiv \Big[(-1)^n 2^n (1 + 2^{2k} + 2^k) - 2^{2n} (1 + 2^k + 2^{2k})\Big] \pmod 7 \\
&\equiv \Big[\left((-1)^n 2^n - 2^{2n}\right)\Big(1 + 2^k + 2^{2k}\Big)\Big] \pmod 7 \\
&\equiv 0 \pmod 7
\end{aligned}$$

for all $n \geq 0$ if and only if $1 + 2^k + 2^{2k} \equiv 0 \pmod 7$.

If $k = 3j$, then $1 + 2^k + 2^{2k} \equiv 3 \pmod 7$. If $k = 3j + 1$, then

$$\begin{aligned}
1 + 2^k + 2^{2k} &\equiv \left(1 + 2(8)^j + 4(64)^j\right) \pmod 7 \\
&\equiv (1 + 2 + 4) \pmod 7 \\
&\equiv 0 \pmod 7.
\end{aligned}$$

Similarly, if $k = 3j + 2$, then $1 + 2^k + 2^{2k} \equiv 0 \pmod 7$. The desired follows.

Example 2. We will now use (2.4) to derive another result involving Pell numbers. Since

$$\begin{aligned} P_n &\equiv [(-1)^n 2^n - 4^n] \pmod 7 \\ &\equiv [(-1)^n 2^n - (-3)^n] \pmod 7 \\ &\equiv (-1)^n [2^n - 3^n] \pmod 7 \\ &\equiv -(-1)^n [3^n - 2^n] \pmod 7, \end{aligned}$$

it follows

$$\begin{aligned} P_{6n+k} &\equiv -(-1)^{6n+k} \left[(3^6)^n 3^k - (2^6)^n 2^k\right] \pmod 7 \\ &\equiv -(-1)^k \left[(3^k - 2^k)\right] \pmod 7 \\ &\equiv P_k \pmod 7. \end{aligned}$$

In particular, for $k = 0$, 7 divides P_{6n} for all $n \geq 0$.

Example 3. For additional results, we will consider (1.3) working modulo 17. Since $2 \equiv 36 \pmod{17}$ and $\frac{1}{12} \equiv 10 \pmod{17}$,

$$\begin{aligned} P_n &\equiv \frac{1}{2\sqrt{36}} \left[\left(1 + \sqrt{36}\right)^n - \left(1 - \sqrt{36}\right)^n\right] \pmod{17} \\ &\equiv 10 \left[7^n + (-1)^{n+1} 5^n\right] \quad (\text{mod } 1)7. \end{aligned}$$

So,

$$\begin{aligned} P_{8n} &\equiv 10 \left[(7^8)^n - (5^8)^n\right] \pmod{17} \\ &\equiv 10 [16^n - 16^n] \pmod{17} \\ &\equiv 0 \pmod{17}. \end{aligned}$$

Therefore, 17 divides P_{8n} for all $n \geq 0$.

When working with the Binet formula for either the Fibonacci or Lucas numbers, it is desirable for 5 to be congruent to a square modulo p. We have the following lemma.

Lemma 2.1. *Let p be an odd prime. Then $x^2 \equiv 5 \pmod p$ has a solution if and only if $p = 5$ or $p \equiv \pm 1 \pmod{10}$.*

Proof. The case $p = 5$ is trivial. Let p be an odd prime different from 5. Then, p can be of the form $p = 10k \pm 1$ or $p = 10k \pm 3$ only. Let $p = 10k \pm 1$. Using *the quadratic reciprocity law*, we may write $(5/p) = ((10k \pm 1)/5)\,(-1)^{\frac{5-1}{2}\frac{p-1}{2}} = (\pm 1/5) = (\pm 1)^{p-1} = 1$ and so

$$u^2 \equiv 5 \pmod p \tag{2.5}$$

will have a solution. Now, if $p \equiv \pm 3 \quad (\text{mod } 1)0$, then, by a similar argument, we obtain $(5/p) = -1$ and so (2.5) will have no solutions. The desired follows. □

Let t be a least residue satisfying (2.5). Then, from (1.1),

$$L_n \equiv \left[\left(\frac{1+t}{2}\right)^n + \left(\frac{1-t}{2}\right)^n\right] \pmod p.$$

We want $\frac{1}{2} \equiv \nu \pmod p$ for some integer ν. So,

$$2\nu \equiv 1 \pmod p. \tag{2.6}$$

Since $(2,p)=1$, (2.6) will have a solution. Hence,

$$L_n \equiv \nu^n\left[(1+t)^n+(1-t)^n\right] \pmod{p}. \tag{2.7}$$

Similarly,

$$F_n \equiv \frac{\nu^n}{t}\left[(1+t)^n-(1-t)^n\right] \pmod{p}. \tag{2.8}$$

Now the factor $\frac{1}{t}$ in (2.8) can be replaced with some integer w since $\frac{1}{t} \equiv w \pmod{p}$ will have a solution. Some values of p that could be used in (2.7) or (2.8) include 5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 101, and 109.

3. Application to Lucas Numbers

We illustrate by the following two examples.

Example 1. In [2], the following question is asked: "Are there any Lucas numbers ending in a zero?" The answer is 'no' and the author's proof relies on applying the Binomial Theorem to the Binet formula (1.1). For our more elementary proof, since $5 \equiv 0 \pmod{5}$ and $\frac{1}{2} \equiv 3 \pmod{5}$ identity (1.1) becomes

$$L_n \equiv 2\cdot 3^n \pmod{5}.$$

This congruence implies that 5 does not divide L_n for all integers n. So, no Lucas number can have 0 as a units digit.

Example 2. The following two congruences were proposed in [1]:

$$L_n \equiv (30^n+50^n) \pmod{79}$$

and

$$L_n \equiv (10^n+80^n) \pmod{89}.$$

We offer the following simple argument for a more general result inspired by Seiffert's generalization in [1].

Lemma 3.1. *If $p+q-1$ is an odd prime such that $pq \equiv -1 \pmod{(p+q-1)}$, and $p+q-1 \equiv \pm 1 \pmod{10}$, then $p \equiv \frac{1\pm\sqrt{5}}{2} \pmod{(p+q-1)}$ and $q \equiv \frac{1\pm\sqrt{5}}{2} \pmod{(p+q-1)}$.*

Proof. Since $pq \equiv -1 \pmod{(p+q-1)}$ and $p(p-1) \equiv -pq \pmod{(p+q-1)}$, $p^2-p-1 = p(p-1)-1 \equiv -pq-1 \equiv 0 \pmod{(p+q-1)}$. Similarly, $q^2-q-1 \equiv 0 \pmod{(p+q-1)}$. Under the assumed conditions on p and q and using Lemma 2.1, $\sqrt{5} \pmod{(p+q-1)}$ exists and $\frac{1}{2}$ is well-defined. Thus, using the quadratic formula, these two equations have the desired solutions. □

Now it follows from (1.1) and Lemma 3.1 that $L_n \equiv (p^n+q^n) \pmod{(p+q-1)}$. Letting $p=30$, $q=50$, and $p=10$, $q=80$, we obtain the first and second congruence, respectively, from Bruckman's result. In fact, using the above formulas for p and q, one can obtain infinitely many similar congruences. For instance, $L_n \equiv (26^n+34^n) \pmod{59}$, $L_n \equiv (6^n+24^n) \pmod{29}$, $L_n \equiv (15^n+5^n) \pmod{19}$, just to name a few. Also, Lemma 3.1 gives similar identities involving Fibonacci numbers. This will be given in the next section.

4. Application to Fibonacci Numbers

To illustrate these techniques for congruences involving Fibonacci numbers, consider the following alternative proof of the known congruence

Example 1. $F_{n+1}5^n + F_n 5^{n+1} \equiv 1 \pmod{29}$.

Proof. Since $5 \equiv 121 \pmod{29}$,

$$\begin{aligned} F_n &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \\ &\equiv \frac{1}{11}\left[\left(\frac{1+11}{2}\right)^n - \left(\frac{1-11}{2}\right)^n\right] \pmod{29} \\ &\equiv \frac{1}{11}\left[6^n - (-5)^n\right] \pmod{29}. \end{aligned}$$

However, $\frac{1}{11} \equiv 8 \pmod{29}$. So,

$$F_n \equiv 8\left[6^n - (-5)^n\right] \pmod{29}. \tag{4.1}$$

In addition to being intrinsically interesting, (4.1) can be used to complete the elementary proof as follows.

$$\begin{aligned} F_{n+1}5^n + F_n 5^{n+1} &\equiv \left(8\left[6^{n+1} - (-5)^{n+1}\right]5^n + 8\left[6^n - (-5)^n\right]5^{n+1}\right) \pmod{29} \\ &\equiv 8\left[6\cdot 30^n + 5\cdot 30^n - (-5)^{n+1}5^n - (-5)^n 5^{n+1}\right] \pmod{29} \\ &\equiv 8\left[11\cdot 30^n + (-1)^n 5^{2n+1} - (-1)^n 5^{2n+1}\right] \pmod{29} \\ &\equiv 8\left[11 + (-1)^n(1-1)5^{2n+1}\right] \pmod{29} \\ &\equiv 88 \pmod{29} \\ &\equiv 1 \pmod{29}. \end{aligned}$$

□

Now we give additional congruence relations similar to Bruckman's in [1] that involve Fibonacci numbers. In fact, we have the following result.

Example 2. If $p+q-1$ is an odd prime, $pq \equiv -1 \pmod{(p+q-1)}$, and $p+q-1 \equiv \pm 1 \pmod{10}$, then $F_n \equiv \frac{1}{\sqrt{5}}(p^n - q^n) \pmod{(p+q-1)}$.

Proof. This follows from (1.2) and Lemma 3.1. □

Some identities that follow from this are $F_n \equiv 8\,(6^n - 24^n) \pmod{29}$, $F_n \equiv 37(26^n - 34^n) \pmod{59}$, etc.

5. Extension to Nonprime Moduli

Let $p = m_1 m_2 \cdots m_k$, where $(m_i, m_j) = 1$ for $i \neq j$. It is known [3, p. 117], that $x^2 \equiv a \pmod{p}$ is solvable if and only if $x^2 \equiv a \pmod{m_i}$ is solvable for $1 \le i \le k$. Also, the linear congruence $ax \equiv b \pmod{p}$ is solvable if and only if d divides b, where $d = (a,p)$. Taking these results into account, the two problems that one encounters when applying the above modular arithmetic techniques to the Binet formulas can be resolved. Therefore, it is possible to extend these techniques to cover some nonprimes. As an illustration, we give a more precise result than Seiffert's result in [1].

Lemma 5.1. *Let $m = 5^c p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, where the p_i's are distinct primes of the form $p_i = 10k_i \pm 1$, $c = 0$ or 1, and c_i is a non-negative integer for $1 \le i \le r$. Then $p \equiv \frac{1+\sqrt{5}}{2} \pmod{m}$ and $q \equiv \frac{1-\sqrt{5}}{2} \pmod{m}$ are defined and $L_n \equiv (p^n + q^n) \pmod{m}$. In addition, if $\frac{1}{\sqrt{5}} \pmod{p_i}$ is defined for $1 \le i \le r$, then $F_n \equiv \frac{1}{\sqrt{5}}(p^n - q^n) \pmod{m}$.*

Proof. The proof follows from the Binet formulas (1.1) and (1.2), Lemma 2.1, the discussion in the beginning of this section, and the fact that if $(a, p_i) = 1$, then $x^2 \equiv a \pmod{p_i^{c_i}}$ is solvable if and only if $x^2 \equiv \pmod{p_i}$ is solvable. □

As an example we offer the following result for Lucas numbers when $p = 95 = 5 \times 19$. By Lemma 2.1, the congruences $x^2 \equiv 5 \pmod{5}$, and $x^2 \equiv 5 \pmod{19}$ are solvable. Thus $x^2 \equiv 5 \pmod{95}$ is solvable. Also, since $(2, 95) = 1$, the congruence $2x \equiv 1 \pmod{95}$ is solvable. Using (1.1) and similar calculations done in the previous sections, one can show that $L_n \equiv (53^n + 43^n) \pmod{95}$. Notice here that $\sqrt{5} \equiv 10 \pmod{95}$. Since $(10, 95) = 5$ and 5 does not divide 1, the congruence $10t \equiv 1 \pmod{95}$ will have no solutions. Therefore there does not exist a similar identity for the Fibonacci numbers when $m = 95$. But we can give the following result for Fibonacci numbers when $p = 209 = 11 \times 19$, for instance. The congruence $x^2 \equiv 5 \pmod{209}$ has a solution $x \equiv 29 \pmod{209}$. Also $\frac{1}{\sqrt{5}} \equiv \frac{1}{29} \equiv 173 \pmod{209}$. It follows that $F_n \equiv 173\,(15^n - 195^n) \equiv 36(-15^n + (-1)^n 14^n) \pmod{209}$.

Remarks. First, the conditions $pq \equiv -1 \pmod{(p+q-1)}$ and $p + q \neq 1$ from Seiffert's result in [1] ensure that the conditions of Lemma 5.1 are satisfied. In fact, one can show that m is odd. Because if $m = 2k$ for some integer k, then, since $pq = am - 1$ for some integer a, $pq = 2ak - 1$, an odd number. Thus p and q must be both odd and so $p + q$ is even. However, $m = p + q - 1 = 2k$ implies $p + q = 2k + 1$, an odd number. This is a contradiction. Also, if we let $m = p + q - 1$, then the condition $pq \equiv -1 \pmod{m}$ implies $p^2 - p - 1 \equiv 0 \pmod{m}$ (see proof of Lemma 3.1). Now the assumption that a solution to this quadratic exists implies the existence of $\sqrt{5} \pmod{m}$.

Secondly, simple arithmetic implies the integer m in Lemma 5.1 has to be of the form $10k \pm 1$ or $10k \pm 5$ for some integer k.

6. Acknowledgement

The authors thank the anonymous referee for detailed comments that led us to generalizing some of the results and improved the presentation of this paper.

References

[1] P. S. Bruckman, *Problem B-996*, The Fibonacci Quarterly, **44.1** (2006), 87.
[2] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley-Interscience, New York, 2001.
[3] C. T. Long, *Elementary Introduction to Number Theory*, Third Edition, Waveland Press, 1995.
[4] B. M. Stewart, *Theory of Numbers*, Second Edition, The Macmillan Company, New York, 1964.

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 Statiatics, Northwest Missouri State University, Maryville, MO 64468
E-mail address: jawads@nwmissouri.edu