A PROBLEM RELATED TO A CONJECTURE OF POLIGNAC

Kellie Bresz
Department of Mathematics, Shippensburg University, Pennsylvania,

Lenny Jones
Department of Mathematics, Shippensburg University, Pennsylvania,
lkjone@ship.edu

Alicia Lamarche
Department of Mathematics, University of South Carolina, South Carolina
alicial@math.sc.edu

Maria Markovich
Department of Mathematics, University of South Carolina, South Carolina
mariaem@math.sc.edu

Received: 7/21/15, Accepted: 6/3/16, Published: 6/10/16

Abstract

In 1849, Polignac conjectured that every odd positive integer is of the form $2^n + p$ for some integer $n \geq 0$ and prime p. Then, in 1950, Erdős provided infinitely many counterexamples to Polignac's conjecture. More recently, in 2012 the second author showed that there are infinitely many positive integers that are not of the form F_n+p or $F_n - p$, where F_n denotes the nth Fibonacci number and p is a prime. In this article, we consider a fusion of these problems and show that there exist infinitely many positive integers which cannot be written as $2^n+F_n \pm p$. Additionally, we look at various results which follow from the main theorem concerning the construction of composite sequences.

1. Introduction

In 1849, Polignac [6] conjectured that every odd positive integer larger than 3 can be written in the form $2^n + p$, for some integer $n \geq 1$ and prime p. This conjecture is easily seen to be false; the smallest counterexample is 127, as Polignac himself discovered soon after making the conjecture. Coincidentally, the counterexample of 959 was found by Euler about a hundred years earlier. Much later, in 1950, Erdős [2] produced infinitely many counterexamples to this conjecture.

More recently, in 2012 the second author [5] showed that there exist infinitely many positive integers that cannot be written in either of the forms F_n+p or F_n-p, where F_n denotes the nth Fibonacci number and p is a prime. In 2014, Ismailescu and Shim [4] extended this work to show that there exist infinitely many positive integers that are not of the form $\epsilon_1 F_n + \epsilon_2 p$, where $\epsilon_i \in \{-1, 1\}$. In this paper, we investigate a fusion of these problems by generating infinitely many counterexamples to the following conjecture.

> Every positive integer can be written in the form $2^n + F_n \pm p$ for some integer $n \geq 0$, where F_n denotes the nth Fibonacci number and p is a prime.

Interestingly, unlike the original conjecture of Polignac, finding counterexamples to this statement is very much a nontrivial task. While a search using Maple produced multiple possible counterexamples, such as 1099, 1231, and 3157, the methods used in this article do not lend themselves to showing that these particular numbers cannot be written as $2^n + F_n \pm p$.

2. Preliminaries

This section contains concepts that will be useful in proving the main theorem.

Definition 2.1. Let $a > 1$ be an integer. A prime divisor p of $a^n - 1$ is called a *primitive divisor* of $a^n - 1$ if $a^m \not\equiv 1 \pmod{p}$ for all positive integers $m < n$.

The following theorem is due to Bang [1].

Theorem 2.2. *Let a and n be positive integers with $a \geq 2$. Then $a^n - 1$ has a primitive divisor with the following exceptions:*

- $a = 2$ *and* $n = 6$
- $a + 1$ *is a power of 2 and* $n = 2$

The next concept, which plays an important role in the proof of the main theorem, is due to Erdős [2].

Definition 2.3. A *(finite) covering system* of the integers is a system of congruences $n \equiv r_i \pmod{m_i}$, with $1 \leq i \leq t$ and $m_i > 1$ such that every integer n satisfies at least one of the congruences.

Throughout this article we represent a covering system $\mathcal{C}$ as a set of ordered triples (r_i, m_i, p_i), where $n \equiv r_i \pmod{m_i}$ is a congruence in the covering system and p_i is a prime corresponding to the modulus in the particular congruence. The relationship between p_i and m_i is further explained in the proof of the main theorem.

Using the concept of a covering system, Erdős was able to construct an arithmetic progression of integers k such that $k - 2^n$ is composite for all $n \geq 1$, thus providing infinitely many counterexamples to Polignac's conjecture. To do so, the following covering system was used.

$$\mathcal{C} = \{(0,2,3),(0,3,7),(1,4,5),(3,8,17),(7,12,13),(23,24,241)\}.$$

To construct such a covering system, Erdős took advantage of the periodicity of 2^n modulo p_i, which has period m_i. The next step in constructing counterexamples to Polignac's conjecture is to use the covering $\mathcal{C}$ to form a system of linear congruences for k. As an example of this, we consider the ordered triple $(0,3,7)$ in $\mathcal{C}$. We want $k - 2^n \equiv 0 \pmod 7$ when $n \equiv 0 \pmod 3$. Notice that when $n \equiv 0 \pmod 3$, we have $k - 2^n \equiv k - 1 \pmod 7$, which means that $k - 2^n$ is divisible by 7 if $k \equiv 1 \pmod 7$. Continuing to do this for each ordered triple in the covering, we get the following system of congruences for k.

$$\begin{array}{lll} k \equiv 1 \pmod 3, & k \equiv 1 \pmod 7, & k \equiv 2 \pmod 5, \\ k \equiv 8 \pmod{17}, & k \equiv 11 \pmod{13}, & k \equiv 121 \pmod{241}. \end{array}$$

To ensure that k is odd, we add $k \equiv 1 \pmod 2$ to the system of congruences. Using the Chinese remainder theorem gives the solution $k \equiv 7629217 \pmod{11184810}$.

Consider the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. In [5], the second author was interested in showing that there exist infinitely many positive integers k which are not of the form $F_n + p$ or $F_n - p$, where F_n denotes the nth Fibonacci number and p is a prime. Jones' approach also makes use of a covering argument, exploiting the periodicity of $\{F_n\}$ modulo an arbitrary prime to build a covering system. It is well known that the Fibonacci sequence is periodic modulo any positive integer $m \geq 2$ [7], and throughout this article we denote this period by $\pi(m)$. For each congruence (r_i, m_i, p_i) in the covering, m_i and p_i are chosen such that $\{F_n\}$ modulo p_i has period m_i. The resulting covering system contains 133 congruences, each of which makes use of a unique prime. The smallest positive value of k produced by this covering has 950 digits.

Recently, in 2014 Ismailescu and Shim [4] improved upon this covering in terms of size by not requiring that each congruence has a unique corresponding prime. By loosening this restriction, they were able to drastically decrease the least common multiple of the moduli from 453600 to 144. Their covering system follows.

$$\begin{aligned} \mathcal{C} = \quad & \{(1,3,2),(2,3,2),(0,4,3),(7,16,7),(9,16,7),(10,16,7),(14,16,7), \\ & (3,18,19),(8,18,19),(15,18,19),(0,36,17),(9,36,17),(18,36,17), \\ & (27,36,17),(6,48,23),(18,48,23)\}. \end{aligned}$$

With these results in mind, we proceed to the main theorem of the article.

3. Main Theorem

The statement and proof of the main result follows.

Theorem 3.1. *There exist infinitely many positive integers k which cannot be written in the form $2^n + F_n \pm p$, where p is a prime.*

Proof. Ultimately, our goal is to build a covering $\mathcal{C}$ containing congruences $n \equiv r_i \pmod{m_i}$ with corresponding primes p_i which are chosen such that the following conditions are satisfied:

1. p_i divides $2^{m_i} - 1$,
2. m_i is a multiple of $\pi(p_i)$.

Requiring these conditions on m_i and p_i allows us to form a system of congruences for k, where $k \equiv 2^{r_i} + F_{r_i} \pmod{p_i}$, and solving this system gives us an infinite arithmetic progression of positive integers which cannot be written as $2^n + F_n \pm p$.

Building a covering based upon implementing each of these conditions separately is handled in [2] and [5] respectively. Due to Theorem 2.2, when $m_i \notin \{1, 6\}$ condition (1) alone does not present any difficulties in finding appropriate m_i and p_i to use in the covering. However, as mentioned in [5], condition (2) gives rise to complications. Although $\{F_n\}$ is periodic modulo any prime [3, 7, 8], the period of $\{F_n\}$ modulo $p > 2$ is always even [7], and not every even number appears as a period. Additionally, given an arbitrary prime p, there is no known formula for $\pi(p)$.

To begin building our covering, we first choose an integer L to be the least common multiple of the moduli in $\mathcal{C}$. Then we examine each of the divisors d of L checking that d is a multiple of $\pi(p)$, and if this is the case we also check that p divides $2^d - 1$. As d becomes large this task becomes increasingly computationally difficult, so many of the moduli and corresponding primes were chosen such that $d = p_i - 1$. This way, Fermat's little theorem allows us to avoid having to check divisibility of $2^d - 1$ by the desired prime. Once a list of possible moduli with corresponding primes is generated, we go back through the list and attempt to build a covering by choosing residues. For purposes of reusing $\mathcal{C}$ in the proofs of Theorems 4.1 and 4.2, we require the additional condition that $2^{r_i} + F_{r_i} \not\equiv 0 \pmod{p_i}$. Oftentimes, such as in [5], this process is carried out by a greedy algorithm. In this case, a majority of the construction can be done by hand, with Maple being used to perform large or repetitious computations. If, after going through the list of divisors of L, we are left with a system of congruences that does not form a covering system, we increase L and then repeat the process.

To better convey the method in which $\mathcal{C}$ was constructed, we consider the following example. By generating a list of $\pi(p)$ for various primes p, we see that $\pi(3) = 8$, and that $3 \mid 2^8 - 1$, making the ordered triple $(r_i, 8, 3)$ a candidate for a congruence in $\mathcal{C}$. To choose the residue(s) r_i, we examine $\{F_n\}$ modulo 3.

index n	0	1	2	3	4	5	6	7	8
$\{F_n\} \pmod 3$	0	1	1	2	0	2	2	1	0
$2^n \pmod 3$	1	2	1	2	1	2	1	2	1

Notice that $F_0 \equiv F_4 \equiv F_8 \equiv 0 \pmod 3$. From this, we see that it may be possible to use $(0, 8, 3)$ and $(4, 8, 3)$, or equivalently $(0, 4, 3)$, in $\mathcal{C}$. Additionally, $F_3 \equiv F_5 \equiv 2 \pmod 3$, so it may also be possible to use $(3, 8, 3)$ and $(5, 8, 3)$ in $\mathcal{C}$. We are not limited to using a single congruence modulo m_i so long as the congruence for k is the same for each r_i used. With this in mind, we compute the congruences for k for each of the candidate residues. For example, we see that all three of the ordered triples $(0, 4, 3)$, $(3, 8, 3)$ and $(5, 8, 3)$ can be used in $\mathcal{C}$, since they all give rise to the single consistent congruence $k \equiv 1 \pmod 3$.

The final covering

$$\begin{aligned}\mathcal{C} = \quad & \{(1,3,2),(2,3,2),(0,4,3),(3,8,3),(5,8,3),(2,10,11),(9,18,19),\\ & (15,18,19),(9,20,5),(14,20,5),(3,30,31),(6,30,31),(18,40,41),(33,48,7),\\ & (6,48,7),(21,60,61),(30,60,61),(39,72,17),(165,180,181),\\ & (57,240,241),(78,240,241)\}\end{aligned}$$

contains 21 ordered triples, with $L = 720$.

Next, we use the Chinese remainder theorem to find infinitely many positive integers k that satisfy the following system of 12 congruences for k:

$$\begin{array}{lll} k \equiv 1 \pmod 2 & k \equiv 1 \pmod 3 & k \equiv 5 \pmod{11} \\ k \equiv 14 \pmod{19} & k \equiv 1 \pmod 5 & k \equiv 10 \pmod{31} \\ k \equiv 32 \pmod{41} & k \equiv 2 \pmod 7 & k \equiv 60 \pmod{61} \\ k \equiv 11 \pmod{17} & k \equiv 93 \pmod{181} & k \equiv 203 \pmod{241} \end{array}$$

In solving this system, we obtain $k \equiv 2421152702567461 \pmod{\mathcal{P}}$, where $\mathcal{P}$ is the product of the primes in

$$\mathfrak{P} = \{2, 3, 5, 7, 11, 17, 19, 31, 41, 61, 181, 241\}.$$

By construction, for any solution k and positive integer n, we have that $|2^n + F_n - k|$ is composite unless $|2^n + F_n - k| = q$ for some prime $q \in \mathfrak{P}$. To see that this does not occur, we first consider the smallest positive solution generated: $k_0 = 2421152702567461$. Observe that

$$2^{51} + F_{51} \leq k_0 - q < k_0 + q \leq 2^{52} + F_{52}$$

for each $q \in \mathfrak{P}$, so that k_0 cannot be written in either the form $2^n + F_n + p$ or $2^n + F_n - p$ for some prime p.

For values of $k > k_0$, notice that for $n \geq 54$, there exists a positive integer z such that

$$2^n + F_n < k_0 + z\mathcal{P} < 2^{n+1} + F_{n+1},$$

with $2^{n+1}+F_{n+1}-(k_0+z\mathcal{P}) > \mathcal{P}$ and $k+z\mathcal{P}-(2^n+F_n) > \mathcal{P}$, so that $|2^n+F_n-k| > q$ for each prime $q \in \mathfrak{P}$. Thus, we conclude that there exist infinitely many integers of the form $k = k_0 + z\mathcal{P}$ which cannot be written as $2^n + F_n + p$ or $2^n + F_n - p$ for some prime p. □

Remark 3.2. We note that the covering $\mathcal{C}$ used in the proof of Theorem 3.1 can also be used to show the main result in [5].

4. Composite Sequences

In this section, we consider results that follow from the main theorem.

Theorem 4.1. *There exist infinitely many positive integers k such that*

$$k\left(2^n + F_n\right) + 1$$

is composite for all integers $n \geq 0$.

Proof. Using the same covering system $\mathcal{C}$ as in Theorem 3.1 the proof of this becomes straightforward. To create the system of congruences for k, we see that

$$k \equiv \frac{-1}{2^{r_i} + F_{r_i}} \pmod{p_i}.$$

As mentioned in the proof of Theorem 3.1, $\mathcal{C}$ was constructed so that $2^{r_i} + F_{r_i} \not\equiv 0 \pmod{p_i}$ for each $p_i \in \mathfrak{P}$, so we do not encounter any problems with divisions by zero. Solving for k using each ordered triple in $\mathcal{C}$, we have the following system of congruences.

$$\begin{array}{lll}
k \equiv 1 \pmod{2}, & k \equiv 2 \pmod{3}, & k \equiv 2 \pmod{11}, \\
k \equiv 4 \pmod{19}, & k \equiv 4 \pmod{5}, & k \equiv 3 \pmod{31}, \\
k \equiv 32 \pmod{41}, & k \equiv 3 \pmod{7}, & k \equiv 1 \pmod{61}, \\
k \equiv 3 \pmod{17}, & k \equiv 72 \pmod{181}, & k \equiv 222 \pmod{241}.
\end{array}$$

Finally, using the Chinese remainder theorem, we obtain the following solution:

$$k \equiv 1871144509511609 \pmod{\mathcal{P}},$$

where, as before, $\mathcal{P}$ is the product of the primes in

$$\mathfrak{P} = \{2, 3, 5, 7, 11, 17, 19, 31, 41, 61, 181, 241\}.$$

□

Theorem 4.2. *There exist infinitely many positive integers k such that*

$$k\left(2^n + F_n\right) - 1$$

is composite for all integers $n \geq 0$.

Proof. Again, we use the same covering $\mathcal{C}$, and solve $k \equiv \frac{1}{2^{r_i}+F_{r_i}} \pmod{p_i}$ for each congruence in $\mathcal{C}$ to create the following system of congruences for k:

$$\begin{array}{lll}
k \equiv 1 \pmod{2}, & k \equiv 1 \pmod{3}, & k \equiv 9 \pmod{11}, \\
k \equiv 15 \pmod{19}, & k \equiv 1 \pmod{5}, & k \equiv 28 \pmod{31}, \\
k \equiv 9 \pmod{41}, & k \equiv 4 \pmod{7}, & k \equiv 60 \pmod{61}, \\
k \equiv 14 \pmod{17}, & k \equiv 109 \pmod{181}, & k \equiv 19 \pmod{241}.
\end{array}$$

Just as before, using the Chinese remainder theorem we obtain the following solution for k:

$$k \equiv 652252042102021 \pmod{\mathcal{P}}. \qquad \square$$

We call a sequence *trivially composite* when every term of the sequence is divisible by the same prime p. We show that there are no trivially composite sequences of the form $\{k\left(2^n + F_n\right) + 1\}_{n=0}^{\infty}$, where k is a fixed positive integer.

Theorem 4.3. *There does not exist a positive integer k such that the sequence*

$$\{k\left(2^n + F_n\right) + 1\}_{n=0}^{\infty}$$

is trivially composite.

Proof. Suppose, by way of contradiction, that there exists a positive integer k and a prime p such that $k(2^n + F_n) + 1 \equiv 0 \pmod{p}$ for all nonnegative integers n. When $n = 0$, we have

$$k(1 + 0) + 1 \equiv 0 \pmod{p} \text{ so } k \equiv -1 \pmod{p}. \tag{4.1}$$

When $n = 1$, we see that $3k \equiv -1 \pmod{p}$. From (4.1), we must have that $-3 \equiv -1 \pmod{p}$, which is only true when $p = 2$.

Finally, when $n = 3$ we have that $10k \equiv -1 \pmod{p}$, which implies that $-10 \equiv -1 \pmod{p}$, contradicting the fact that $p = 2$. $\square$

5. Unanswered Questions

Question 5.1. Do there exist infinitely many positive integers k such that $k^2(2^n + F_n) + 1$ is composite for all integers $n \geq 0$?

Question 5.2. Let $b > 2$ be an integer. Do there exist infinitely many positive integers k such that $k(b^n + F_n) + 1$ is composite for all integers $n \geq 0$?

In practice, given an explicit value for b, it seems possible to build a covering system to solve the problem at hand, following an argument very similar to that of Theorem 4.1. However, the problem of showing this for all b appears to be much more difficult.

Acknowledgements The authors thank the referee for the very careful reading of the manuscript, and for the good suggestions.

References

[1] A.S. Bang, Taltheoretiske Undersogelser, *Tidsskrift for Mat.* **5** (1886), 70–80, 130–137.

[2] P. Erdős, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* (1950), 113–123.

[3] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Amer. Math. Soc., (2003).

[4] D. Ismailescu and P. Shim, On numbers that cannot be expressed as a plus-minus weighted sum of a Fibonacci number and a prime, *Integers* **14** (2014), #A65.

[5] L. Jones, Fibonacci variations of a conjecture of Polignac, *Integers* **12** (2012), #A11.

[6] A. de Polignac, Recherches nouvelles sur les nombres premiers, *C.R. Acad. Sci. Paris Math.* **29** (1849) 397–401, 738–739.

[7] D.D Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525–532.

[8] M. Ward, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.* **35**, no. 3 (1933), 600–628.