#A11 INTEGERS 12 (2012)

FIBONACCI VARIATIONS OF A CONJECTURE OF POLIGNAC

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

Received: 9/17/10, Revised: 6/16/11, Accepted: 1/12/12, Published: 1/13/12

Abstract

In 1849, Alphonse de Polignac conjectured that every odd positive integer can be written in the form $2^n + p$, for some integer $n \geq 0$ and some prime p. In 1950, Erdős constructed infinitely many counterexamples to Polignac's conjecture. In this article, we show 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 is a Fibonacci number, and p is a prime.

1. Introduction

In 1849, Alphonse de Polignac [3] conjectured that every odd positive integer can be written in the form $2^n + p$ for some integer $n \geq 0$ and some prime p. Shortly after making this conjecture, Polignac himself found several counterexamples, and about a hundred years earlier, Euler indicated the counterexample 959 in a letter to Christian Goldbach [7]. In 1950, Erdős [5] constructed infinitely many counterexamples to Polignac's conjecture.

Recall that the Fibonacci sequence $\{F_n\}_{n=1}^{\infty}$ is defined as $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$. We are interested here in two variations of the conjecture of Polignac, which involve the Fibonacci numbers. In particular, given any positive integer k, we ask:

1. Can k be written in the form $F_n + p$, where F_n is a Fibonacci number, and p is a prime?

2. Can k be written in the form $F_n - p$, where F_n is a Fibonacci number, and p is a prime?

For a fixed k, Question 1 is a finite problem. One needs only to check the primes and Fibonacci numbers up to k. In fact, it is easy to find examples of positive integers that cannot be written in the form $F_n + p$. The first few are: 35, 119, 125 and 177. (Note, we allow $F_0 = 0$ to be used here.) However, whether there are infinitely many such exceptions is another issue.

Question 2 is more open-ended, and hence more difficult, since there is no bound on either the Fibonacci number or the prime required in the decomposition of k. For example, the first Fibonacci number for which $F_n - 155$ is prime is F_{954}. A simple computer search for a single value of k that cannot be written in the form $F_n - p$ produced none before running out of memory. So, finding a counterexample to the conjecture that every positive integer k can be written in the form $F_n - p$ is a more monumental task.

In this article, we show that Question 2 also has a negative answer. In fact, we prove that there exist infinitely many positive integers that cannot be written in either of the forms $F_n - p$ or $F_n + p$, which provides infinitely many negative answers to both Question 1. and Question 2. simultaneously.

2. Preliminaries

The following definitions are standard and can be found, along with related information, in [2, 6, 13].

Definition 1. Let α and β be algebraic integers, where $\alpha + \beta$ and $\alpha\beta$ are nonzero relatively prime rational integers, and α/β is not a root of unity. For $n \geq 0$, we can then define a sequence of rational integers

$$U_n(\alpha, \beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

The pair (α, β) is called a *Lucas pair*, and the corresponding sequence U_n is known as a *Lucas sequence* of the first kind.

Definition 2. Let $U_n = U_n(\alpha, \beta)$ be a Lucas sequence. We define a *primitive (prime) divisor* of U_n to be a prime p such that both of the following hold:

- $U_n \equiv 0 \pmod{p}$,
- $(\alpha - \beta)^2 U_1 U_2 \cdots U_{n-1} \not\equiv 0 \pmod{p}$.

Polignac's conjecture is related to the Lucas sequence $U_n(2, 1)$ as $2^n = U_n(2, 1) + 1$. We are concerned in this article with the Fibonacci sequence, which is the Lucas sequence $U_n((1 + \sqrt{5})/2, (1 - \sqrt{5})/2)$. Helpful in the resolution of Polignac's conjecture, and also the problem of concern in this article, is the well-known fact that any Lucas sequence U_n is periodic modulo every prime [12]. A proof that $\{F_n\}$ is periodic can be found in [11], and a more general discussion with more references can be found in [6].

Definition 3. Let U_n be a Lucas sequence of the first kind, and let p be a prime. Then the *period* of U_n modulo p is the least positive integer m such that $U_m \equiv 0 \pmod{p}$. If U_n is the Fibonacci sequence, we let $\mathrm{Per}_F(p)$ denote the period of $\{F_n\}$ modulo p.

Remark 4. The periods of $\{F_n\}$ modulo z, where z is a positive integer, are sometimes referred to as the *Pisano periods* [9].

The following concept is due to Erdős [5].

Definition 5. A *(finite) covering system*, or simply a *covering*, of the integers is a system of congruences $n \equiv r_i \pmod{m_i}$, with $1 \leq i \leq t$, such that every integer n satisfies at least one of the congruences. To avoid a trivial situation, we require $m_i > 1$ for all i.

Many applications of coverings require an associated set of primes, where each of these primes corresponds in some way to a particular modulus in the covering. It will be convenient throughout this article to represent a covering and the associated set of primes using a set $\mathcal{C}$ of ordered triples (r_i, m_i, p_i), where $n \equiv r_i \pmod{m_i}$ is a congruence in the covering and p_i is the corresponding prime. The exact correspondence needed in this article is described in the proof of Theorem 6. Abusing notation slightly, we refer to $\mathcal{C}$ as a "covering".

As mentioned before, Erdős [5] found infinitely many counterexamples to Polignac's conjecture. In fact, he constructed an infinite arithmetic progression of integers k such that $k - 2^n$ is never prime for all $n \geq 1$. To accomplish this task, he used the covering

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

and he exploited the fact that the sequence $U_n(2, 1)$ is periodic modulo p_i, with period m_i. This method gives rise to a system of linear congruences in the variable k, which can be solved using the Chinese remainder theorem. For example, using the triple $(1, 4, 5)$ in $\mathcal{C}$, we want $k - 2^n \equiv 0 \pmod 5$ when $n \equiv 1 \pmod 4$. But $k - 2^n \equiv k - 2 \pmod 5$, when $n \equiv 1 \pmod 4$, which tells us that $k - 2^n$ is divisible by 5 if $k \equiv 2 \pmod 5$. Continuing in this manner gives us the system

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

Since we require that k be odd, we add the congruence $k \equiv 1 \pmod 2$ to our system, and using the Chinese remainder theorem, we get the solution $k \equiv 7629217 \pmod{11184810}$.

Note that Erdős did not use the modulus 6 in his covering. One of the reasons to avoid the modulus 6 is the fact that there does not exist a prime p such that $U_n(2, 1)$ has period 6 modulo p. If such a prime p exists, it must divide $U_6(2, 1) = 63$. But it is easy to check that $U_n(2, 1)$ has period 2 modulo 3, and period 3 modulo 7.

In fact, this result is a direct consequence of Bang's theorem [1], which states that $U_n(2,1)$ has a primitive divisor for all $n \neq 1, 6$. However, keep in mind that the modulus 6 could be used to build a covering, with corresponding prime 3 or 7, provided that either 2 or 3, respectively, is not used as a modulus. So, as long as we are able to find a covering with a corresponding list of distinct primes p_i, one for each modulus m_i, such that the $U_n(2,1)$ is periodic with respect to m_i in the sense that the actual period of $U_n(2,1)$ modulo p_i divides m_i, we can construct infinitely many counterexamples to Polignac's conjecture. For example, if we decide to use the modulus 6 and not the modulus 3, then we can use the covering

$$\{(1,2,3),(2,4,5),(0,6,7),(0,8,17),(1,9,73),(8,12,13),(4,18,19),(4,24,241)\},$$

which gives the solution $k \equiv 12161672909 \pmod{15513331470}$. Thus, the use of primitive divisors is not essential in finding a solution to this problem. However, we see that not using primitive divisors in this situation can make the construction of the covering more difficult, and can also increase the number of congruences needed in the covering. In this example, the smallest solution for k increases as well.

Unlike the sequence $U_n(2,1)$, the question of periodicity is not as straightforward in $\{F_n\}$. For example, if p is a primitive divisor of $U_m(2,1)$, then elementary group theory shows that $U_m(2,1)$ has period m modulo p. However, if p is a primitive divisor of F_m, then [10]

$$\mathrm{Per}_F(p) = \begin{cases} m & \text{if } m \equiv 0 \pmod 2 \text{ and } m \not\equiv 0 \pmod 4 \\ 2m & \text{if } m \equiv 0 \pmod 4 \\ 4m & \text{if } m \equiv 1 \pmod 2 \text{ and } n > 1. \end{cases} \tag{1}$$

This added complexity, along with the fact that certain Fibonacci numbers have no primitive divisors, makes the use of primitive divisors to answer the questions posed in this article more complicated than in the solution to Polignac's conjecture. But just as in the solution to Polignac's conjecture, the issue of periodicity is the real key to solving the problem here.

Although the formula given in (1) gives $\mathrm{Per}_F(p)$ in terms of m, when p is a primitive divisor of F_m, a more satisfying formula for $\mathrm{Per}_F(p)$ in terms of only p is still unknown. Still more complications and nuances arise in the theory of the Pisano periods, and the interested reader should see [4, 10, 11, 12].

3. The Main Result

The main result of this article is:

Theorem 6. *There exist infinitely positive integers k, such that k cannot be written in either of the forms $F_n + p$ or $F_n - p$, where F_n is a Fibonacci number and p is a prime.*

Proof. We wish to build a covering $\mathcal{C} = \{(r_i, m_i, p_i)\}$, where the actual covering is the set of congruences $\{n \equiv r_i \pmod{m_i}\}$, and for each congruence in the covering, the corresponding prime p_i is such that $\{F_n\}$ has period m_i modulo p_i. In other words, $F_n \equiv F_{r_i} \pmod{p_i}$ when $n \equiv r_i \pmod{m_i}$. The fact that $\{F_n\}$ is periodic modulo every prime [6, 11, 12] is helpful in the construction of the covering. However, it is still somewhat tricky to construct a suitable covering since the period of $\{F_n\}$ modulo the prime $p > 2$ is always even [11], and not every even number is a period; for example, $\{F_n\}$ does not have period 2 or 4 modulo any prime. Another complication arises from the fact that there is no known formula for the period of $\{F_n\}$ modulo an arbitrary prime.

Our general strategy is to first choose a number L that will be the least common multiple of our moduli. Then we examine the divisors d of L, one at a time, and search for primes p such that $\{F_n\}$ has period d modulo p. If we find such a prime p, then we let d be a modulus in our covering with corresponding prime p. If we are fortunate, we find more than one such prime for a particular divisor d of L, and we get to use d as a modulus multiple times, once for each of these primes. Each time we add a new modulus, we use a greedy algorithm to find corresponding residues to attempt to build a covering. We continue until we find a covering or until we exhaust all divisors of L. If we exhaust all divisors of L, and the method has failed to produce a covering, we increase our initial value of L to include more divisors, and we repeat the process. After many computations, we were successful at $L = 453600$ with largest modulus 1134, used four times. It seems unlikely that such a covering could be constructed without the aid of a computer. We made use of both MAGMA and Maple to assist us in the construction.

The covering $\mathcal{C}$ we use here contains 133 triples (r_i, m_i, p_i), and as far as the author knows, this covering is the first covering to appear in the literature such that all moduli are periods of the Fibonacci numbers modulo some prime. Recently, the covering $\mathcal{C}$ has been used to prove that there exist infinitely many positive integers k such that $k \cdot (F_n + 5) + 1$ is composite for all integers $n \geq 1$ [8].

The covering is:

$$\begin{aligned}\mathcal{C} = \{&(0,3,2),(0,8,3),(1,10,11),(6,14,29),(6,16,7),(5,18,19),\\ &(3,20,5),(2,28,13),(19,30,31),(12,32,47),(29,36,17),\\ &(27,40,41),(22,42,211),(20,48,23),(5,50,101),(45,50,151),\\ &(35,54,5779),(18,56,281),(37,60,61),(0,70,71),(12,70,911),\\ &(47,72,107),(14,80,2161),(10,84,421),(89,90,181),(85,90,541),\\ &(92,96,1103),(13,100,3001),(53,108,53),(17,108,109),\\ &(42,112,14503),(7,120,2521),(40,126,1009),(124,126,31249),\\ &(42,140,141961),(100,144,103681),(85,150,12301),(115,150,18451),\\ &(78,160,1601),(46,160,3041),(50,162,3079),(140,162,62650261),\\ &(122,168,83),(50,168,1427),(73,180,109441),(75,200,401),\end{aligned}$$

$(175, 200, 570601), (110, 210, 21211), (196, 210, 767131),$
$(4, 216, 11128427), (158, 224, 10745088481), (193, 240, 241),$
$(133, 240, 20641), (82, 252, 35239681), (29, 270, 271), (17, 270, 811),$
$(119, 270, 42391), (209, 270, 119611), (154, 280, 12317523121),$
$(28, 288, 10749957121), (25, 300, 230686501), (124, 324, 2269),$
$(232, 324, 4373), (148, 324, 19441), (26, 336, 167), (206, 336, 65740583),$
$(98, 350, 54601), (168, 350, 560701), (28, 350, 7517651),$
$(238, 350, 51636551), (133, 360, 10783342081), (88, 378, 379),$
$(130, 378, 85429), (214, 378, 912871), (52, 378, 1258740001),$
$(393, 400, 9125201), (153, 400, 5738108801), (278, 420, 8288823481),$
$(292, 432, 6263), (196, 432, 177962167367), (215, 450, 221401),$
$(35, 450, 15608701), (335, 450, 3467131047901),$
$(446, 480, 23735900452321), (268, 504, 1461601), (436, 504, 764940961),$
$(107, 540, 1114769954367361), (306, 560, 118021448662479038881),$
$(73, 600, 601), (433, 600, 87129547172401), (92, 630, 631),$
$(476, 630, 1051224514831), (260, 630, 1983000765501001),$
$(340, 648, 1828620361), (364, 648, 6782976947987),$
$(638, 672, 115613939510481515041), (658, 700, 701),$
$(474, 700, 17231203730201189308301), (13, 720, 8641),$
$(515, 720, 13373763765986881), (700, 756, 38933),$
$(472, 756, 955921950316735037), (715, 800, 124001), (315, 800, 6996001),$
$(782, 800, 3160438834174817356001), (742, 810, 1621), (94, 810, 4861),$
$(580, 810, 21871), (418, 810, 33211), (256, 810, 31603957 81),$
$(34, 810, 7654861102843433881), (194, 840, 721561),$
$(266, 840, 140207234004601), (508, 864, 3023), (412, 864, 19009),$
$(14, 864, 447901921), (686, 864, 48265838239823),$
$(242, 900, 11981661982050957053616001), (46, 1008, 503),$
$(494, 1008, 4322424761927), (830, 1008, 571385160581761),$
$(302, 1050, 1051), (722, 1050, 9346455940780547345401),$
$(512, 1050, 14734291702642871390242051), (590, 1080, 12315241),$
$(950, 1080, 100873547420073756574681), (942, 1120, 6135922241),$
$(270, 1120, 164154312001), (750, 1120, 13264519466034652481),$
$(428, 1134, 89511254659), (680, 1134, 1643223059479),$
$(806, 1134, 68853479653802041437170359),$
$(1058, 1134, 5087394106095783259)\}.$

Then, we use the Chinese remainder theorem to find infinitely many positive integers k that satisfy the system of congruences $k \equiv F_{r_i} \pmod{p_i}$, for $1 \leq i \leq 133$. Thus, for any solution k, and any positive integer n, we have that both $F_n - k$ and $k - F_n$ are multiples of p_i for some i. Hence, if either $F_n - k$ or $k - F_n$ is prime, then it follows that $F_n - k = p_i$ or $k - F_n = p_i$ for some i. However, this is impossible

for infinitely many sufficiently large values of k.

The smallest positive value of k produced here by this procedure has 950 digits. Denote this value of k as $\mathcal{K}$. Since $F_{4547} < \mathcal{K} - p_i < \mathcal{K} + p_i < F_{4548}$ for each p_i in $\mathcal{C}$, we see that indeed $\mathcal{K}$ cannot be written in either the form $F_n - p$ or $F_n + p$, for some prime p. Next we consider values of $k > \mathcal{K}$. Observe that all of these values are of the form $\mathcal{K} + zP$, where $P = \prod_{i=1}^{133} p_i$, and z is a positive integer. When $n \geq 4553$, we have that $F_{n+1} - F_n \geq 4P$, so that there exists a positive integer z such that $F_n < \mathcal{K} + zP < F_{n+1}$, with $F_{n+1} - (\mathcal{K} + zP) > P > p_i$ and $\mathcal{K} + zP - F_n > P > p_i$ for all p_i in $\mathcal{C}$. Thus, there are infinitely many positive integers that also satisfy the conditions of the theorem. This fact is illustrated by the following data, which was generated by computer:

$$\begin{aligned} F_{4547} < \mathcal{K} &< F_{4548} \\ &< F_{4549} < \mathcal{K} + P \\ &< F_{4550} < \mathcal{K} + 2P \\ &< F_{4551} < \mathcal{K} + 3P < \mathcal{K} + 4P \\ &< F_{4552} < \mathcal{K} + 5P < \mathcal{K} + 6P < \mathcal{K} + 7P < \mathcal{K} + 8P \\ &< F_{4553} < \mathcal{K} + 9P < \cdots < \mathcal{K} + 13P \\ &< F_{4554} < \mathcal{K} + 14P < \cdots < \mathcal{K} + 22P \\ &< F_{4555} < \mathcal{K} + 23P < \cdots < \mathcal{K} + 37P \\ &< F_{4556} \cdots\cdots \end{aligned}$$

Hence, there are infinitely many positive integers, namely $k = \mathcal{K} + zP$, where z is a positive integer, that have the property that for all positive integers n, both $F_n - k$ and $k - F_n$ are divisible by at least one of the 133 primes p_i in $\mathcal{C}$, and $|F_n - k| > p_i$ for all primes p_i in $\mathcal{C}$. Therefore, k cannot be written in the form $F_n + p$ or $F_n - p$, where F_n is a Fibonacci number and p is a prime. Theorem 6 follows. □

Remark 7. I will gladly email any interested reader the values of $\mathcal{K}$ and P, and the list of residues, moduli and primes in the covering $\mathcal{C}$ formatted for use in Maple.

4. Some Open Questions

In this section, we ask some questions for future investigations.

Question 8. All values of k that satisfy the conditions of Theorem 6 found here are even. Are there infinitely many odd values of k that satisfy the conditions of Theorem 6?

Question 9. Is $\mathcal{K}$ the smallest value of k that satisfies the conditions of Theorem 6?

Question 10. For a fixed positive integer $m \geq 2$, are there infinitely many values of k such that k^m satisfies the conditions of Theorem 6?

Question 11. Are there consecutive values of k that satisfy the conditions of Theorem 6?

Acknowledgements The author thanks the referee for the many valuable suggestions.

References

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

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

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

[4] Amos Ehrlich, *On the periods of the Fibonacci sequence modulo M*, Fibonacci Quarterly, 27 (1989), pp. 11-13.

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

[6] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, **104**, American Mathematical Society, (2003).

[7] P.-H. Fuss, *Correspondance Mathématique et Physique de Quelques Célèbres Géomètres du XVIII Ème Siècle*, **I, II**, Johnson Reprint, New York, 1968.

[8] L. Jones, *Using Lucas sequences to generalize a theorem of Sierpiński*, Acta Arithmetica (to appear)

[9] Pisano Period, `http://en.wikipedia.org/wiki/Pisano_period`.

[10] John Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly 1 (1963) 37–45.

[11] D. D. Wall, *Fibonacci series modulo m*, American Mathematical Monthly, 67 (1960), 525-532.

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

[13] Hugh C. Williams, *Édouard Lucas and Primality Testing*, **22**, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley-Interscience, (1998).