Fibonacci numbers that are not sums of two prime powers

Florian Luca[1] and *Pantelimon Stănică*[2]

[1] IMATE, UNAM, Ap. Postal 61-3 (Xangari), CP. 58 089
Morelia, Michoacán, Mexico; e-mail: fluca@matmor.unam.mx
[2] Auburn University Montgomery, Department of Mathematics,
Montgomery, AL 36124-4023, USA; e-mail: pstanica@mail.aum.edu

May 09, 2004

Abstract

In this paper, we construct an infinite arithmetic progression $\mathcal{A}$ of positive integers n such that if $n \in \mathcal{A}$, then the nth Fibonacci number is not a sum of two prime powers.

1 Introduction

In 1849, A. de Polignac [7] asked if every odd positive integer can be represented as the sum of a power of 2 and a prime (or 1). Euler did note that 959 was not of this form. Romanoff [8] used the Brun sieve to show that a positive proportion of integers are representable in this way. Later, van der Corput [2] showed that a positive proportion of integers are not representable in this way by using covering congruences. With the same method as van der Corput's, Erdős [3] constructed a residue class of odd numbers which contains no integers of the above form. Extending Erdős's argument, Cohen and Selfridge [1] constructed a 26 digit number which is neither the sum nor the difference of two prime powers. Inspired by their work, Z.W. Sun (see [9]) constructed a residue class of odd integers consisting exclusively of numbers not of the form $\pm p^a \pm q^b$ with some primes p and q and some nonnegative integers a and b. We mention that Erdős asked if there exist infinitely many positive integers which are not representable as a sum or difference of two powers (see [5]) and a partial result can be found in [6].

In this paper, we show that there exist infinitely many positive integers which are not of the form $p^a + q^b$ with primes p and q and nonnegative integers a and b and which further can be chosen to be members of the Fibonacci sequence $(F_n)_{n\geq 0}$ given by $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$.

In what follows, we use the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings. We recall that given two functions A and B of the real variable x, the notations $A \ll B$ and $B \gg A$ are equivalent to the fact that the inequality $|A(x)| \leq cB(x)$ holds with some positive constant c and for all sufficiently large real numbers x.

[1]2000 *Mathematics Subject Classification.* Primary 11B39; Secondary 11B25, 11B50, 11P32.
[2]*Keywords*: Fibonacci numbers, arithmetic progressions, covering system of congruences.

2 The Result

Our main result is the following.

Theorem 1. *There exists a positive integer n_0 such that if $n > n_0$ and*

$$n \equiv 1807873 \pmod{3543120}$$

then $F_n \neq p^a + q^b$ with p, q prime numbers and a, b nonnegative integers.

We use the same method employed in [2, 3, 9]. However, there are additional difficulties which arise because we want our numbers to belong to the Fibonacci sequence.

Let us quickly recall how one can create a residue class of odd integers most of which are not sums of two powers. Well, assume that n is odd and a sum of two powers, say $p^a + q^b$. Since n is odd, it follows that one of p and q, say p equals 2. Suppose now that we are given a finite set of triples $(a_i, b_i, p_i)_{i=1}^s$ where a_i and b_i are nonnegative integers and p_i are distinct primes such that the following hold:

(i) For every $a \in \mathbb{Z}$ there exists $i \in \{1, \ldots, s\}$ such that $a \equiv a_i \pmod{b_i}$.

(ii) $p_i \mid (2^{b_i} - 1)$ holds for all $i = 1, \ldots, s$.

We may then choose n to belong to the arithmetic progression given by $n \equiv 2^{a_i} \pmod{p_i}$. Since the p_i's are distinct primes, the above system admits a unique solution modulo $p_1 \ldots p_s$ by the Chinese Remainder Lemma. Let $\mathcal{A}$ be this progression. Assume that n is sufficiently large in the above progression $\mathcal{A}$ and that $n = 2^a + q^b$ holds with some prime number q. By (i) above, there exists $i \in \{1, \ldots, s\}$ such that $a \equiv a_i \pmod{b_i}$. By (ii) above, $2^a \equiv 2^{a_i} \pmod{p_i}$. However, $n \equiv 2^{a_i} \pmod{p_i}$, and therefore $n \equiv 2^a \pmod{p_i}$. Hence, $p_i \mid (n - 2^a)$. However, $n - 2^a = q^b$. Since q is prime, it follows that $p_i = q$. Now let X be a very large positive real number. The number of positive integers $n \leq X$ which belong to $\mathcal{A}$ is $\gg X$. However, the number of positive integers of the form $2^a + q^b$ with $q \in \{p_1, \ldots, p_s\}$ and which are $\leq X$ is $\ll \log^2 X$. This shows that most numbers in $\mathcal{A}$ are not of the form $p^a + q^b$.

We now modify the above construction in order to insure that our numbers can be chosen from the Fibonacci sequence. Let k be a positive integer. It is known that $(F_n)_{n \geq 0}$ is periodic modulo k. We write $h(k)$ to denote this period. Moreover, for integers f and k we write $\mathcal{A}(f, k)$ for the set of residue classes n modulo $h(k)$ such that $F_n \equiv f \pmod{k}$.

Assume now that $(a_i, b_i, p_i)_{i=1}^s$ is a finite set of triples of nonnegative integers a_i and b_i and distinct odd primes p_i for $i = 1, \ldots, s$ which fulfill the following conditions:

(i) For every $a \in \mathbb{Z}$ there exists $i \in \{1, \ldots, s\}$ such that $a \equiv a_i \pmod{b_i}$.

(ii) $p_i \mid (2^{b_i} - 1)$ holds for all $i = 1, \ldots, s$.

(iii) The set

$$\bigcap_{i=1}^{s} \mathcal{A}(2^{a_i}, p_i) \neq \emptyset.$$

Moreover, if there exists $i \in \{1, \ldots, s\}$ such that $3 \mid h(p_i)$, then we shall assume that the above intersection contains a class coprime to 3.

Let x be an element of the set $\bigcap_{i=1}^{s} \mathcal{A}(2^{a_i}, p_i)$. Note that x is defined only modulo $M = \text{lcm}[h(p_1), \ldots, h(p_s)]$. Moreover, if $3 \mid M$, then x is not a multiple of 3. If M is not a multiple of 3 we replace M by $3M$ and x by the solution of the system of congruences $x \pmod{M}$ and $1 \pmod{3}$. Assume now that $n \equiv x \pmod{M}$ and that $F_n = p^a + q^b$ holds with some primes p and q and nonnegative integers a and b. It then follows that F_n is an odd integer, because the only even Fibonacci numbers are those whose indices are multiples of 3. Since F_n is odd, it follows that one of p and q, say p is 2. By (i) above, there exists $i \in \{1, \ldots, s\}$ such that $a \equiv a_i \pmod{b_i}$. By (ii) above, it follows that $2^a \equiv 2^{a_i} \pmod{p_i}$. By the choice of n, we have that $F_n \equiv 2^{a_i} \pmod{p_i}$. Thus, $F_n \equiv 2^a \pmod{p_i}$. In particular, $p_i \mid (F_n - 2^a)$. However, since $F_n - 2^a = q^b$, it follows that $q = p_i$. Thus, $q \in \{p_1, \ldots, p_s\}$. We now get that $F_n = 2^a + p_i^b$ for some $i = 1, \ldots, s$. Since $F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$, where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, we may apply a well-known result from the theory of $\mathcal{S}$-unit equations (see [4]) to conclude that such an equation can have only finitely many solutions (n, a, b). Thus, there exists n_0 with the property that if $n > n_0$ and $n \equiv x \pmod{M}$, then F_n is not of the form $p^a + q^b$ with primes p and q and nonnegative integers a and b.

In order to finish the proof of the Theorem, it suffices to find a finite set of triples $(a_i, b_i, p_i)_{i=1}^{s}$ fulfilling (i)–(iii) above.

We first note that by taking $s = 7$ and

$$((a_1, b_1), \ldots, (a_7, b_7)) = ((0,2),\ (0,3),\ (3,4),\ (1,12),\ (5,36),\ (17,36),\ (29,36))$$

we get that (i) above is fulfilled. Indeed, every integer is congruent either to $0 \pmod{2}$ or to $0 \pmod{3}$ or to $3 \pmod{4}$ or to $1 \pmod{12}$ or to $5 \pmod{12}$, and in this last case it is congruent to either 5, 17 or 29 modulo 36. We now take $(p_1, \ldots, p_7) = (3, 7, 5, 13, 19, 37, 73)$ and note that condition (ii) above is fulfilled. It is easy to check that $(h(p_1), \ldots, h(p_7)) = (8, 16, 20, 28, 18, 76, 148)$. Finally, it is easy to see that

$$\begin{aligned}
\mathcal{A}(2^{a_1}, p_1) &= \mathcal{A}(2^0, 3) = \{1, 2, 7\} \pmod{8}, \\
\mathcal{A}(2^{a_2}, p_2) &= \mathcal{A}(2^0, 7) = \{1, 2, 6, 15\} \pmod{16}, \\
\mathcal{A}(2^{a_3}, p_3) &= \mathcal{A}(2^3, 5) = \{4, 6, 7, 13\} \pmod{20}, \\
\mathcal{A}(2^{a_4}, p_4) &= \mathcal{A}(2^1, 13) = \{3, 25\} \pmod{28}, \\
\mathcal{A}(2^{a_5}, p_5) &= \mathcal{A}(2^5, 19) = \{7, 11\} \pmod{18}, \\
\mathcal{A}(2^{a_6}, p_6) &= \mathcal{A}(2^{17}, 37) = \{10, 15, 28, 61\} \pmod{76}, \\
\mathcal{A}(2^{a_7}, p_7) &= \mathcal{A}(2^{29}, 73) = \{53, 95\} \pmod{148},
\end{aligned}$$

One now checks that the system of congruences $x \equiv 1 \pmod{8}$, $x \equiv 1 \pmod{16}$, $x \equiv 13 \pmod{20}$, $x \equiv 25 \pmod{28}$, $x \equiv 7 \pmod{18}$, $x \equiv 61 \pmod{76}$ and $x \equiv 53 \pmod{148}$ has a positive integer solution x. In fact, the above system is equivalent to the system of congruences $x \equiv 1 \pmod{16}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{7}$, $x \equiv 7 \pmod{9}$, $x \equiv 4 \pmod{19}$ and $x \equiv 16 \pmod{37}$. Solving this system, we get $x \equiv 1807873 \pmod{3543120}$, which, together with the above arguments completes the proof of Theorem 1.

We would like to conclude by offering the following problem.

Problem. *Find an arithmetic progression of positive integers* $A \pmod{B}$ *such that if* $n > n_0$ *satisfies* $n \equiv A \pmod{B}$, *then* $F_n \neq \pm p^a \pm q^b$ *for any primes* p, q *and nonnegative integers* a, b.

Acknowledgments. This work was done during a visit of F. L. at the Mathematics Department of the Auburn University at Montgomery. He thanks the people of this department for their warm hospitality.

References

[1] F. Cohen and J. L. Selfridge, 'Not every number is the sum or difference of two prime powers', *Math. Comp.* **29** (1975), 79–81.

[2] J. G. van der Corput, 'On de Polignac's conjecture', *Simon Stevin* **27** (1950), 99–105.

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

[4] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, 'S-unit equations and their applications', in *New advances in transcendence theory* (Durham, 1986), 110–174, Cambridge Univ. Press, Cambridge, 1988.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1994.

[6] F. Luca, 'On numbers which are not a sum or a difference of two powers', *Mathematika*, to appear.

[7] A. de Polignac, 'Recherches nouvelles sur les nombres premiers', *C.R. Acad. Sci. Paris Math.* **29** (1949), 397–401, 738–739.

[8] N. P. Romanoff, 'Über einige Sätze der additiven Zahlentheorie', *Math. Ann.* **57** (1934), 668–678.

[9] Z. W. Sun, 'On integers not of the form $\pm p^a \pm q^b$', *Proc. Amer. Math. Soc.* **128** (2000), 997–1002.