FIBONACCI NUMBERS OF THE FORM $p^a \pm p^b + 1$

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58180, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

Laszlo Szalay
Department of Mathematics and Statistics, University of West Hungary, 9400, Sopron, Bajcsi-Zs. út 4, Hungary
e-mail: laszalay@ktk.nyme.hu

(Submitted July 2004-Final Revision October 2006)

ABSTRACT

In this paper, we show that the diophantine equation $F_n = p^a \pm p^b + 1$ has only finitely manypositive integer solutions (n, p, a, b), where p is a prime number and $\max\{a, b\} \geq 2$.

1. INTRODUCTION

The Fibonacci sequence denoted by $(F_n)_{n\geq 0}$ is the sequence of integers given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$.

There are many papers in the literature which address diophantine equations involving Fibonacci numbers. A long standing problem asking whether 0, 1, 8 and 144 are the only perfect powers in the Fibonacci sequence was recently confirmed by Bugeaud, Mignotte and Siksek [2]. An extension of such a result to diophantine equations involving perfect powers in products of Fibonacci numbers whose indices form an arithmetic progression was obtained in [5]. For example, the only instance in which a product of consecutive terms in the Fibonacci sequence is a perfect power is the trivial case $F_1 F_2 = 1$.

In a different direction, there has been a lot of activity towards studying arithmetic properties of those positive integers n which admit nice representations in a fixed base $b > 1$. For example, finding all the perfect powers y^q which are *rep-units* in some integer base $x > 1$ (with $n \geq 3$ digits) reduces to the diophantine equation $y^q = \frac{x^n-1}{x-1}$. All solutions of this last diophantine equation are still not known, although particular instances of it have been dealt with (see, for example, [3] for the case $q = 2$, or [1] for the case $x = 10$). All solutions of the diophantine equation $x^2 = 2^a \pm 2^b + 1$ in positive integers (x, a, b) where found in [10], and the more general equation diophantine equation $x^2 = p^a \pm p^b + 1$ in positive integer unknowns (x, p, a, b) with p a prime number was treated in [4]. We mention a further result directly related to the problem treated in this paper. Let p be a fixed prime. Pethö and Tichy (see Theorem 2 in [8]), showed that there are only finitely many Fibonacci numbers of the form $F_n = p^a + p^b + p^c$ with integers $a > b > c \geq 0$; i.e., which have three digits of 1 in base p and the remaining digits equal to zero. Their proof can be generalized to allow for three term representations with digits 1 and some negative signs too. However, the proof of their result uses the finiteness of solutions of S-unit equations, and as such is ineffective.

Throughout this paper, we use the Landau symbols O and o as well as the Vinogradov symbols $\ll$, $\gg$, and $\asymp$ with their regular meanings and with the understanding that the constants (respectively the convergence) implied by them is effectively computable. We recall that $A \ll B$,$B \gg A$, and $A = O(B)$ are all equivalent to the fact that the inequality $|A| \leq cB$ holds with some positive constant c, and that $A \asymp B$ means that both $A \gg B$ and $A \ll B$

hold. For two positive integers u and v we use both $\gcd(u,v)$ and (u,v) for their greatest common divisor.

2. MAIN RESULT

In this note, we prove the following theorem.

Theorem 1: *The diophantine equation $F_n = p^a \pm p^b + 1$ admits only finitely many, effectively computable, positive integer solutions (n, p, a, b), where p is a prime number, $n > 2$ and $\max\{a, b\} \geq 2$.*

The proof of our Theorem follows closely the method of [6], where it was shown that the similar looking diophantine equation $F_n = p^a \pm p^b$ has only finitely many positive integer solutions (n, p, a, b) with p a prime number and $\max\{a, b\} \geq 2$.

3. PRELIMINARY RESULT

Let $(L_k)_{k\geq 0}$ be the Lucas sequence given by $L_0 = 2,\ L_1 = 1$, and $L_{k+2} = L_{k+1} + L_k$ for all $k \geq 0$. The following Lemma is instrumental for the proof of our main result Theorem 1.

Lemma 2: *Let $m \geq n$ be two nonnegative integers such that $m \equiv n \pmod 2$. Let $\delta \in \{\pm 1\}$ be 1 if $m \equiv n \pmod 4$ and -1 otherwise. Then,*

$$F_m - F_n = F_{(m-\delta n)/2} L_{(m+\delta n)/2}.$$

Proof: We write $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$. It is well-known that the formulae

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{and} \qquad L_n = \alpha^n + \beta^n$$

hold for all nonnegative integers n. Then,

$$F_{(m-\delta n)/2} L_{(m+\delta n)/2} = \frac{\left(\alpha^{(m-\delta n)/2} - \beta^{(m-\delta n)/2}\right)\left(\alpha^{(m+\delta n)/2} + \beta^{(m+\delta n)/2}\right)}{\alpha - \beta}$$

$$= \frac{(\alpha^m - \beta^m) + (\alpha\beta)^{(m-n)/2}\left(\alpha^{(1-\delta)n/2}\beta^{(1+\delta)n/2} - \alpha^{(1+\delta)n/2}\beta^{(1-\delta)n/2}\right)}{\alpha - \beta}.$$

When $m \equiv n \pmod 4$, we have that $\delta = 1$, $(m-n)/2$ is even, and since $\alpha\beta = -1$, we have that $(\alpha\beta)^{(m-n)/2} = 1$. Thus, the above formula becomes

$$F_{(m-n)/2} L_{(m+n)/2} = \frac{\alpha^m - \beta^m + (\beta^n - \alpha^n)}{\alpha - \beta} = F_m - F_n.$$

When $\delta = -1$, we have that $(m-n)/2$ is odd, and therefore $(\alpha\beta)^{(m-n)/2} = -1$. The above formula becomes

$$F_{(m+n)/2}L_{(m-n)/2} = \frac{\alpha^m - \beta^m - (\alpha^n - \beta^n)}{\alpha - \beta} = F_m - F_n,$$

which completes the proof of the lemma. $\square$

4. THE PROOF OF THEOREM 1

We write the diophantine equation

$$F_n = p^a \pm p^b + 1 \tag{1}$$

as

$$F_n - 1 = p^b(p^{a-b} \pm 1).$$

Since $F_1 = F_2 = 1$, it follows, by Lemma 2, that

$$F_{(n-\delta)/2}L_{(n+\delta)/2} = p^b(p^{a-b} \pm 1), \tag{2}$$

where $\delta = 1$ if $n \equiv 1 \pmod 4$, $\delta = -1$ if $n \equiv -1 \pmod 4$, $\delta = 2$ if $n \equiv 2 \pmod 4$ and $\delta = -2$ if $n \equiv 0 \pmod 4$. Since $n > 2$, it follows that the integer appearing in either side of equation (2) is nonzero, therefore the instance in which $a = b$ and the sign is -1 does not occur. We may assume that n is as large as we wish, since when n is fixed, equation (2) shows that both p^b and $p^{a-b} \pm 1$ are divisors of the fixed nonzero integer $F_{(n-\delta)/2}L_{(n+\delta)/2}$, thus there are only finitely many possibilities for p, a, and b, which are obviously effectively computable.

Since $F_{(n-\delta)/2} | F_{n-\delta}$, $L_{(n+\delta)/2} \mid F_{n+\delta}$, and $\gcd(F_u, F_v) = F_{(u,v)}$ holds for all positive integers u and v, we get that

$$\gcd\left(F_{(n-\delta)/2}, L_{(n+\delta)/2}\right) | \gcd\left(F_{n-\delta}, F_{n+\delta}\right) \mid F_{2|\delta|} \mid F_4.$$

It then follows that $\gcd\left(F_{(n-\delta)/2}, L_{(n+\delta)/2}\right) \mid 3$. Equation (2) now shows that $p^b \le 3L_{\lfloor n/2 \rfloor + 1}$. In particular, $p^b \ll \alpha^{n/2}$. From equation (2), we get that

$$p^{a-b} \ge \frac{p^{a-b}+1}{2} \ge \frac{F_n - 1}{2p^b} \ge \frac{F_n - 1}{6L_{\lfloor n/2 \rfloor + 1}} \gg \alpha^{n/2}.$$

In particular, $a > b$ if n is sufficiently large. We next show that there exists a computable constant c_1 such that $a < c_1$. We shall assume that a is large. Since

$$p^b \ll \alpha^{n/2} \qquad \text{and} \qquad p^{a-b} \gg \alpha^{n/2},$$

we get that $p^b \ll p^{a-b}$, therefore $a \ge 2b + O(1)$. We thus get that $b/a < 2/3$ if $a > c_2$, where c_2 is some effectively computable constant.

We now rewrite our diophantine equation (1) as

$$\left|\frac{1}{\sqrt{5}}\alpha^n - p^a\right| = \left|\frac{1}{\sqrt{5}}\beta^n \pm p^b + 1\right| < 3p^b < 3\left(p^a\right)^{2/3}.$$

The above inequality implies that p^a and $\frac{1}{\sqrt{5}}\alpha^n$ are very close one to another when n is large, and therefore the inequality

$$\left|\frac{1}{\sqrt{5}}\alpha^n - p^a\right| < \left(\max\left\{\frac{1}{\sqrt{5}}\alpha^n,\ p^a\right\}\right)^{3/4}$$

holds for large values of n. An argument of Shorey and Stewart (see [9]) based on lower bounds for linear forms in logarithms, now shows that there exists a computable absolute constant $c_3 > c_2$ such that $a < c_3$. Since $a > b$, we may assume that both a and b are fixed. We may now set $X = p$, and look at the more general equation

$$F_n = X^a \pm X^b + 1, \tag{3}$$

in integer unknowns (n, X) with n positive.

We recall that in [7], all polynomials $P(X) \in \mathbb{Q}[X]$ of degree ≥ 2 such that the diophantine equation $F_n = P(X)$ admits infinitely many integer solutions (n, X) have been completely classified. Such polynomials are related to the Chebyshev polynomials. Instead of applying the above result, we will just prove that a polynomial of the form $X^a \pm X^b + 1$, where $a > b > 0$, does not have this property.

Inserting the equation $F_n = X^a \pm X^b + 1$ into the well-known identity

$$L_n^2 = 5F_n^2 \pm 4,$$

we get the equation

$$Y^2 = f(X), \tag{4}$$

with $Y = L_n$ and $f(X) = 5(X^a + \varepsilon X^b + 1)^2 \pm 4$, where $\varepsilon \in \{\pm 1\}$. By a well-known result of Siegel, the diophantine equation (4) has only finitely many integer solutions (X, Y) provided that $f(X) \in \mathbb{Q}[X]$ has at least three simple roots. We now show that all roots of our polynomial $f(X)$ are simple (note that the degree of $f(X)$ is $2a \geq 4$). Indeed, if x is a double root of $f(x)$, then x satisfies both the equation $f(x) = 0$ and the equation $f'(x) = 0$. Since $f'(x) = 10(x^a + \varepsilon x^b + 1)x^{b-1}(ax^{a-b} + \varepsilon b)$, it follows easily that the only possibility is $ax^{a-b} + \varepsilon b = 0$. This gives $x = \zeta(-\varepsilon b/a)^{\frac{1}{(a-b)}}$, where ζ is some root of unity of order $a - b$. Inserting this into the equation $f(x) = 0$, we get

$$\frac{2\zeta_1}{\sqrt{5}} - 1 = x^b(x^{a-b} + \varepsilon) = x^b\left(\frac{\varepsilon(a-b)}{a}\right),$$

where ζ_1 is some root of unity of order 4, which leads to

$$\left(\frac{2\zeta_1}{\sqrt{5}} - 1\right)^{a-b} = \left(\frac{-\varepsilon b}{a}\right)^b \left(\frac{\varepsilon(a-b)}{a}\right)^{a-b}.$$

Squaring the above relation we get that $(2\zeta_1 - \sqrt{5})^{2(a-b)}$ is a rational number, which is impossible for $a > b$. Hence, our polynomial $f(X)$ has only simple roots, which, via Siegel's Theorem, shows that equation (3) has only finitely many integer solutions (n, X) whenever $b < a$ are fixed positive integers. The fact that these are effectively computable follows from the fact that all the integer solutions to hyperelliptic equations like (4) can be found in an effective way.

Theorem 1 is therefore completely proved. □

5. COMMENTS AND GENERALIZATIONS

Our result can be somewhat extended to a more general situation. Namely, let $(G_n)_{n\geq 0}$ be the sequence of integers given by $G_0 = 0$, $G_1 = 1$ and $G_{n+2} = uG_{n+1} + G_n$ for all $n \geq 0$, where $u \geq 1$ is an integer. One can show that the analogue of Lemma 2 holds for the Fibonacci sequence $(F_n)_{n\geq 0}$ replaced by the sequence $(G_n)_{n\geq 0}$, where now the role of the sequence $(L_n)_{\geq 0}$ is played by the sequence $(H_n)_{n\geq 0}$ given by $H_0 = 2$, $H_1 = u$ and $H_{n+2} = uH_{n+1} + H_n$ for all $n \geq 0$. By a completely similar method, one can now show that for each of $k = 1,\ 2$, the equation

$$G_n = p^a \pm p^b + G_k \qquad \text{with} \qquad n \equiv k \pmod 2$$

has only finitely many effectively computable solutions n. However, the beauty of the result for the case of the Fibonacci sequence comes from the fact that every positive integer n is either odd or even, but both F_1 and F_2 equal to 1, thus allowing us to conclude that equation (1) has only finitely many effectively computable solutions n independently of the parity of n.

ACKNOWLEDGMENTS

We thank the anonymous referee for pointing out a reference. This paper was written during a very enjoyable visit by the first author to University of West Hungary in Sopron; he wishes to express his thanks to that institution for the hospitality and support. The first author's research was also partly supported by grants SEP-CONACYT 37259-E and 37260-E.

REFERENCES

[1] Y. Bugeaud and M. Mignotte. "On Integers With Identical Digits." *Mathematika* **46** (1999): 411-417.

[2] Y. Bugeaud, M. Mignotte and S. Siksek. "Classical and Modular Approaches to Exponential Diophantine Equations I. Fibonacci and Lucas Powers." *Ann. of Math.* **163** (2006): 969-1018.

[3] W. Ljunggren. "Some Theorems on Indeterminate Equations of the Form $(x^n - 1)/(x - 1) = y^q$." (Norwegian) *Norsk Mat. Tidsskr.* **25** (1943): 17-20.

[4] F. Luca. "The Diophantine Equation $x^2 = p^a \pm p^b + 1$." *Acta Arith.* **112** (2004): 87-101.

[5] F. Luca and T. N. Shorey. "Diophantine Equations With Products of Consecutive Terms in Lucas Sequences." *J. Number Theory* **114** (2005): 298-311.

[6] F. Luca and P. Stănică. "Fibonacci Numbers of the Form $p^a \pm p^b$." *Proceedings of the eleventh International Conference on Fibonacci numbers and their Applications*, Braunschweig, July 2004, Editor W. Webb, Kluwer Acad. Publ., to appear.

[7] I. Nemes and A. Pethö. "Polynomial Values in Linear Recurrences. II." *J. Number Theory* **24** (1986): 47-53.
[8] A. Pethö and R. F. Tichy. "S-unit Equations, Linear Recurrences and Digit Expansions." *Publ. Math. Debrecen* **42** (1993): 145-154.
[9] T. N. Shorey and C. L. Stewart. "Pure Powers in Recurrence Sequences and Some Related Diophantine Equations." *J. Number Theory* **27** (1987): 324-352.
[10] L. Szalay. "The Equations $2^N \pm 2^M \pm 2^L = x^2$." *Indag Math.* **13** (2002): 131-142.

AMS Classification Numbers: 11B39, 11D72

✠ ✠ ✠