Fibonacci numbers of the form $p^a \pm p^b$

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

April 19, 2004

Abstract

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

1 Introduction

Recall that 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 [4]. 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 [9]. For example, the only instance in which a product of consecutive terms in the Fibonacci sequence is a perfect power is the trivial case $F_1F_2 = 1$.

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, [8] for the case $q = 2$, or [3] for the case $x = 10$).

2 Main Result

In this note, we prove the following theorem.

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

[1]2000 *Mathematics Subject Classification.* Primary 11B39; Secondary 11D72.
[2]*Keywords*: Fibonacci numbers, diophantine equations.

From the above theorem, it follows that there are only finitely many Fibonacci numbers which are of the form $100\ldots010\ldots0$ in some prime base p.

We write p and q for prime numbers, and $c_1, c_2 \ldots$ for positive constants which are effectively computable. For a positive real number x we write $\log x$ for the natural logarithm of x. Finally, we use the Vinogradov symbols $\gg$ and $\ll$ with their usual meaning.

3 The Proof

We shall always assume that $a \geq b$. If $a = b$, we then get the equation $F_n = 2p^a$ (note that in the case of the equation $F_n = p^a - p^b$ the instance $a = b$ yields $n = 0$, which is not convenient), and one can infer (see [4, 11]) that this equation implies $n = 2, 6$. Since $F_2 = 1, F_6 = 8$, one gets the only solution $(n, p, a, b) = (6, 2, 2, 2)$, in the case of $a = b$. Hence, we assume that $a > b$. Consider first that $p = 2$. Since

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where $\alpha = \frac{(1+\sqrt{5})}{2}$ and $\beta = \frac{(1-\sqrt{5})}{2}$, it follows that the given equation is of the form

$$\frac{1}{\sqrt{5}}\alpha^n - \frac{1}{\sqrt{5}}\beta^n = 2^a \pm 2^b. \tag{1}$$

In this case, the above equation is an $\mathcal{S}$-unit equation in four terms which is nondegenerate (see [6]). Thus, it has only finitely many positive integer solutions (n, a, b). In fact, the main theorem of [6] shows that the above equation has at most $2\exp(2^{36} \cdot 3^{13})$ positive integer solutions (n, a, b).

It is not hard to see that all the solutions (n, a, b) of the above equation (1) are effectively computable. Indeed, first of all, from the above equation we get that $2^b || F_n$. By results from [7], it follows that $3|n$ and n is odd if $b = 1$, and $n = 2^{b-2}3m$ holds with some integer m coprime to 6 if $b \geq 3$ (the case $b = 2$ is impossible). Hence, $b \leq 2 + \log(n/3)/\log 2 < 2\log(2n)$. Assume now that n is large. In this case, we may rewrite equation (1) as

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

Since $b < 2\log(2n)$, the above inequality shows that $2^a \approx \frac{1}{\sqrt{5}}\alpha^n$, therefore $a \approx c_1 n$, where $c_1 = \frac{\log \alpha}{\log 2} \approx 0.69$. In particular, $n/2 < a < n$ holds for large values of n. Equation (2) now implies that

$$\left|(\sqrt{5})^{-1}\alpha^n 2^{-a} - 1\right| \leq 2^{-a+b+1}. \tag{3}$$

By a standard application of linear forms in logarithms (see [1]), it follows that the left hand side of the above inequality (3) exceeds $\exp(-c_2 \log n)$, where c_2 is some absolute constant. Hence, we get the inequality

$$-c_2 \log n < -a + b + 1,$$

therefore

$$a < c_2 \log n + b + 1 < c_2 \log n + 2\log(2n) + 1,$$

which together with the fact that $a > n/2$ implies that n is bounded by an effectively computable constant c_3.

The above argument can also be used to deal with any *fixed* prime number p. That is, an immediate application of results on $\mathcal{S}$-unit equations shows that if p is fixed, then the diophantine equation $F_n = p^a \pm p^b$ has only finitely many positive integer solutions (n, a, b), and the theory of linear forms in logarithms can be used to find an explicit upper bound on the largest such solution. So, from now on we shall assume that $p > p_0$, where p_0 is a constant to be determined later

We now write $n(p)$ for the *index of apparition of* p *in* $(F_n)_{n\ge 0}$ and $e(p)$ for the *exponent of apparition*; i.e., $p^{e(p)}||F_{n(p)}$ and p does not divide F_m for any $m < n(p)$. Since

$$F_m = \frac{\alpha^m - \beta^m}{\alpha - \beta},$$

we have

$$F_m = \prod_{1\le k<m} (\alpha - e^{\frac{2\pi i k}{m}}\beta).$$

We write

$$\Phi_m = \prod_{\substack{1\le k<m\\ \gcd(k,m)=1}} (\alpha - e^{\frac{2\pi i k}{m}}\beta).$$

By the principle of inclusion and exclusion

$$\Phi_m = \frac{(\alpha^m - \beta^m)}{\prod_{p|m}(\alpha^{\frac{m}{p}} - \beta^{\frac{m}{p}})} \cdot \frac{\prod_{\substack{p<q\\ pq|m}}(\alpha^{\frac{m}{pq}} - \beta^{\frac{m}{pq}})}{\prod_{\substack{p<q<r\\ pqr|m}}(\alpha^{\frac{m}{pqr}} - \beta^{\frac{m}{pqr}})} \cdots. \tag{4}$$

Using now the trivial fact that the inequalities

$$\alpha^\ell - \beta^\ell \ge \alpha^\ell - |\beta|^\ell = (\alpha - |\beta|)(\alpha^{\ell-1} + \alpha^{\ell-2}|\beta| + \cdots + |\beta|^{\ell-1}) \ge \alpha^{\ell-1}$$

and

$$\alpha^\ell - \beta^\ell < 2\alpha^\ell < \alpha^{\ell+2}$$

hold for every positive integer ℓ, we then get, by (4), that the inequalities

$$\Phi_m \ge \alpha^{(m - \sum_{p|m}\frac{m}{p} + \sum_{\substack{p<q\\ pq|m}}\frac{m}{pq} - \dots) - 3\cdot 2^{\omega(m)-1}} = \alpha^{\phi(m) - 3\cdot 2^{\omega(m)-1}} \tag{5}$$

and

$$\Phi_m \le \alpha^{(m - \sum_{p|m}\frac{m}{p} + \sum_{\substack{p<q\\ pq|m}}\frac{m}{pq} - \dots) + 3\cdot 2^{\omega(m)-1}} = \alpha^{\phi(m) + 3\cdot 2^{\omega(m)-1}} \tag{6}$$

hold, where we use $\phi(m)$ and $\omega(m)$ to denote the Euler function of m and the number of distinct prime factors of m, respectively.

We now note that by the definition of the order of apparition, we have that $p^{e(b)}|\Phi_{n(p)}$, $n(p)|n$ and $e(p) \le b$. Moreover, since $p^b||F_n$, it follows easily that $n = n(p)p^{b-e(p)}m$, where $m \ge 1$ is coprime to p. We also record that since $p^a \pm p^b$ is always even, it follows that $3|n$.

Our next goal is to show that if n is large and $p > p_0$, then the inequality

$$\frac{b}{a} < \frac{3}{4} \tag{7}$$

holds.

With the above notations, we have

$$p^{a-b} \pm 1 = \frac{F_n}{p^b} = \frac{F_{n(p)p^{b-e(p)}m}}{p^{b-e(p)}F_{n(p)}} \cdot \frac{F_{n(p)}}{p^{e(p)}}.$$

Assume first that $(m-1)+(b-e(p))>0$. In this case,

$$p^{a-b}\pm 1 \ge \frac{F_{n(p)p^{b-e(p)}m}}{p^{b-e(p)}F_{n(p)}} \ge \alpha^{n(p)p^{b-e(p)}m-n(p)-2-(b-e(p))\frac{\log p}{\log \alpha}},$$

where we used the known fact that the inequality $\alpha^{\ell-2}<F_\ell<\alpha^\ell$ holds for all $\ell\ge 1$. It is now easy to see that the inequality

$$n(p)p^{b-e(p)}m-n(p)-2-(b-e(p))\frac{\log p}{\log \alpha}\ge \frac{n(p)}{2}$$

holds whenever $(m-1)+(b-e(p))>0$ provided that $p>p_0$. Indeed, if $b-e(p)>0$, we then write $x=b-e(p)$, and rewrite the above inequality as

$$n(p)(p^x m-1.5)>2+x\frac{\log p}{\log \alpha}.$$

Since $n(p)\ge 1$ and $m\ge 1$, the above inequality is implied by

$$p^x>3.5+x\frac{\log p}{\log \alpha}, \tag{8}$$

and this inequality clearly holds for all $x\ge 1$ provided that $p\ge p_0$. To compute p_0, we first take it to be such that the function

$$x\longmapsto p^x-3.5-x\frac{\log p}{\log \alpha}$$

is increasing for $x\ge 1$. The derivative of this function is

$$(\log p)\left(p^x-\frac{1}{\log \alpha}\right)\ge(\log p)\left(p-\frac{1}{\log \alpha}\right)$$

and this last expression is always positive is $p\ge 3$. Thus, if $p\ge 3$, then inequality (8) will hold for all $x\ge 1$ provided that it holds at $x=1$, and this last inequality holds whenever $p>8$. Thus, we may take $p_0\ge 11$.

If on the other hand $b-e(p)=0$, but $m\ge 2$, then the above inequality just becomes

$$n(p)>2+n(p)/2,$$

which is equivalent to $n(p)\ge 4$, which holds whenever $p>F_4=3$. This shows that we can take $p_0=11$.

Thus, if $(m-1)+(b-e(p))>0$, we have proved that

$$p^{a-b}\pm 1\ge \alpha^{\frac{n(p)}{2}}>\sqrt{F_{n(p)}}\ge p^{\frac{b}{2}},$$

which shows that $b<2(a-b)+\varepsilon$ holds with any $\varepsilon>0$ provided that a is large enough. Choosing n to be large enough and $\varepsilon=1$, we get that $b<2(a-b)+1\le 3(a-b)$, therefore $4b<3a$. This gives $b/a<3/4$, which proves inequality (7) in this case.

From now on, we assume that $n(p)=n$. In this case, $e(p)=b$, and we get, by inequality (6),

$$p^{a-b}\pm 1=\frac{F_n}{p^b}\ge\frac{F_n}{\Phi_n}\ge \alpha^{n-\phi(n)-2-3\cdot 2^{\omega(n)-1}}.$$

Thus,

$$p^{a-b} \pm 1 \geq \alpha^{n-\phi(n)-2-3\cdot 2^{\omega(n)-1}},$$

therefore the inequality

$$p^{a-b} > \alpha^{n-\phi(n)-2-3\cdot 2^{\omega(n)-1}} - 1 > \alpha^{n-\phi(n)-3-3\cdot 2^{\omega(n)-1}} \tag{9}$$

holds for large n, while

$$p^b \leq \Phi_n \leq \alpha^{\phi(n)+3\cdot 2^{\omega(n)-1}}. \tag{10}$$

Since $3|n$, we get that

$$\frac{\phi(n)}{n} = \prod_{q|n} \frac{q-1}{q} \leq \frac{2}{3}, \tag{11}$$

therefore $(n-\phi(n)) \geq \phi(n)/2$. Since $3 \cdot 2^{\omega(n)-1} < 3\,\tau(n) \leq n^{\varepsilon}$ holds for all $\varepsilon > 0$ and for all large enough values of n (here, $\tau(n)$ is the number of divisors of n), while $\phi(n) \gg n/\log\log n$ holds for all $n > e^e$, we easily get that the above inequality (11) implies that

$$n - \phi(n) - 3 - 3 \cdot 2^{\omega(n)-1} > \frac{1}{3}\left(\phi(n) + 3 \cdot 2^{\omega(n)-1}\right) \tag{12}$$

holds for large values of n. Comparing (12), (9) and (10), we get the inequality

$$(a-b) > \frac{b}{3},$$

leading to $b/a < 3/4$, which proves inequality (7) in this case as well.

We now rewrite our diophantine equation as

$$\left|\frac{1}{\sqrt{5}}\alpha^n - p^a\right| = \left|\frac{1}{\sqrt{5}}\beta^n \pm p^b\right| < 2p^b < 2\left(p^a\right)^{3/4}.$$

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

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

holds for large values of n. An argument of Shorey and Stewart [12] based on lower bounds for linear forms in logarithms, now shows that there exists an absolute constant c_4 such that $a < c_4$. 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

$$F_n = X^a \pm X^b, \tag{13}$$

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

We recall that in [10], 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 $X^a \pm X^b$, where $a > b$, does not have this property.

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

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

where $(L_n)_{n\geq 0}$ is the companion Lucas sequence given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$, we get the equation

$$L_n^2 = f(X),$$

where $f(X) = 5(X^a + \varepsilon X^b)^2 \pm 4$, where $\varepsilon \in \{\pm 1\}$. By a well-known result of Siegel, the diophantine equation $Y^2 = f(X)$ 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 $f'(x) = 10(x^a + \varepsilon x^b)x^{b-1}(ax^{a-b} + \varepsilon b)$, 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

$$\mp 4 = 5x^{2b}(x^{a-b} + \varepsilon)^2 = 5x^{2b}\left(\frac{\varepsilon(a-b)}{a}\right)^2,$$

which leads to

$$\left(\frac{\mp 4}{5}\right) \cdot \left(\frac{a}{\varepsilon(a-b)}\right)^2 = \left(\frac{-\varepsilon b}{a}\right)^{\frac{2b}{a-b}} \cdot \zeta^{2b}.$$

Taking absolute values and then squareroots of both sides of the above identity we get

$$\frac{2}{\sqrt{5}} \cdot \left(\frac{a}{a-b}\right) = \left(\frac{b}{a}\right)^{\frac{b}{a-b}}. \tag{14}$$

From homogeneity of the expression, we may assume that in the previous equation a, b are coprime. Further, we rewrite (14) as

$$2^{a-b}a^a = (a-b)^{a-b}\, b^b\, 5^{(a-b)/2},$$

which implies that a, b have the same parity and $a - b \geq 2$. Moreover, 5 divides a. By simple divisibility considerations, we derive that 5 divides either b or $a-b$. That is a contradiction with the assumption that $(a, b) = 1$. Hence, our polynomial $f(X)$ has only simple roots, which, via Siegel's Theorem, shows that equation (13) has only finitely many integer solutions (n, X) whenever $b < a$ are fixed positive integers.

Theorem 1 is therefore completely proved. $\square$

4 Comments

Recall that if r and s are coprime integers with $rs \neq 0,\ \Delta = r^2 + 4s \neq 0$ and such that the roots $\gamma,\ \delta$ of the quadratic equation

$$x^2 - rx - s = 0$$

have the property that γ/δ is not a root of 1, then the sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ of general terms

$$u_n = \frac{\gamma^n - \delta^n}{\gamma - \delta} \qquad \text{and} \qquad v_n = \gamma^n + \delta^n$$

are called *Lucas sequences of the first and second kind*, respectively.

Arguments similar to the ones used in this paper combined with standard arguments from the theory of linear forms in logarithms of algebraic numbers (see [13]) lead to the following generalization of Theorem 1.

Theorem 2. *Let $(w_n)_{n\geq 0}$ be a Lucas sequence of the first or second kind, respectively. Assume further that $\Delta > 0$. Then the diophantine equation $w_n = p^a \pm p^b$ has only finitely many positive integer solutions (n, p, a, b) with p a prime number and* $\max\{a, b\} \geq 2$.

A similar result as the one above holds with the Lucas sequence $(w_n)_{n\geq 0}$ replaced by a classical Lehmer sequence, for the definition of which we refer the reader to the papers [2].

Note that our Theorem 2 above does not cover the case in which $\Delta < 0$. We would like to propose this case as an open problem.

Problem. *Let $(u_n)_{n\geq 0}$ be a Lucas sequence with complex conjugate roots. Prove that the diophantine equation $u_n = p^a \pm p^b$ has only finitely many positive integer solutions (n, p, a, b) with p a prime number and* $\max\{a, b\} \geq 2$.

Finally, it would be nice to remove the condition that *p is a prime number* from the statements of Theorems 1 and 2. However, we have no idea how to approach such problems, although it is likely that one may be able to use the ABC conjecture to establish conditional proofs of such statement.

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] A. Baker and G. Wüstholz, 'Logarithmic forms and group varieties', *J. reine angew. Math.* **442** (1993), 19–62.

[2] Yu. Bilu, G. Hanrot and P. M. Voutier, 'Existence of primitive divisors of Lucas and Lehmer numbers', *J. reine angew. Math.* **539** (2001), 75–122.

[3] Y. Bugeaud and M. Mignotte, 'On integers with identical digits,' *Mathematika* **46** (1999), 411–417.

[4] Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential diophantine equations I. Fibonacci and Lucas powers', *Preprint*, 2003.

[5] R. D. Carmichael, 'On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$', *Ann. Math.* (2) **15** (1913), 30–70.

[6] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, 'Linear equations in variables which lie in a multiplicative group', *Ann. Math.* **155** (2002), 1–30.

[7] E. Jacobson, 'Distribution of the Fibonacci numbers mod 2^k', *Fibonacci Quart.* **30** (1992), 211 – 215.

[8] 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.

[9] F. Luca and T. N. Shorey, 'Diophantine equations with products of consecutive terms in Lucas sequences', *Preprint*, 2003.

[10] I. Nemes and A. Pethő, 'Polynomial values in linear recurrences. II', *J. Number Theory* **24** (1986), 47–53.

[11] A. Pethő, 'Perfect powers in second order linear recurrences', *J. Number Theory* **15** (1982), 5–13.

[12] T. N. Shorey and C. L. Stewart, 'Pure powers in recurrence sequences and some related diophantine equations', *J. Number Theory* **27** (1987), 324–352.

[13] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, 1986.