GLASNIK MATEMATIČKI
Vol. 52(72)(2017), 221 – 234

ON DIOPHANTINE QUADRUPLES OF FIBONACCI NUMBERS

Yasutsugu Fujita and Florian Luca
Nihon University, Japan and University of the Witwatersrand, South Africa

Abstract. We show that there are only finitely many Diophantine quadruples, that is, sets of four positive integers $\{a_1, a_2, a_3, a_4\}$ such that $a_i a_j + 1$ is a square for all $1 \le i < j \le 4$, consisting of Fibonacci numbers.

1. Introduction

A Diophantine k-tuple is a set of k positive integers $\{a_1, \dots, a_k\}$ such that $a_i a_j + 1$ is a square for all $1 \le i < j \le k$. Dujella [4] proved that $k \le 5$. He, Togbé and Ziegler [10] proved that $k \le 4$. There are infinitely many quadruples. In fact, given any Diophantine triple $\{a, b, c\}$, if we set

$$d = a + b + c + 2abc + 2\sqrt{(ab + 1)(bc + 1)(ac + 1)}, \tag{1.1}$$

then $\{a, b, c, d\}$ is a Diophantine quadruple. Diophantine quadruples $\{a, b, c, d\}$ with $a < b < c < d$ with the property that d is given by formula (1.1) in terms of a, b, c are called *regular*. It is conjectured by Arkin, Hoggatt and Strauss [1], and by Gibbs [8], independently, that all Diophantine quadruples are regular, but this has not been proved yet.

Let $\{F_n\}_{n\ge0}$ be the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \ge 0$. It turns out that $\{F_{2n}, F_{2n+2}, F_{2n+4}\}$ is a Diophantine triple. Indeed, this is due to the formulas

$$F_{2n}F_{2n+2} + 1 = F_{2n+1}^2 \quad \text{and} \quad F_{2n}F_{2n+4} + 1 = F_{2n+2}^2,$$

2010 *Mathematics Subject Classification.* 11D72, 11D61, 11B39, 11J87.
Key words and phrases. Diophantine tuples, Fibonacci numbers, Subspace Theorem.
The first author is supported by JSPS KAKENHI Grant Number 16K05079.
The second author is supported by grant CPRR160325161141 from the NRF of South Africa, an A-rated scientist award from the NRF of South Africa and the grant no. 17-02804S of the Czech Granting Agency.

which are valid for all positive integers n. Inserting $a = F_{2n},\ b = F_{2n+2},\ c = F_{2n+4}$ into (1.1), we get, after some manipulations with Fibonacci numbers, that $d = 4F_{2n+1}F_{2n+2}F_{2n+3}$. Hence, $\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\}$ is a regular Diophantine quadruple for all positive integers n. Hoggatt and Bergum [11] conjectured that if $\{F_{2n}, F_{2n+2}, F_{2n+4}, d\}$ is a Diophantine quadruple, then necessarily $d = 4F_{2n+1}F_{2n+2}F_{2n+3}$. This was proved by Dujella in [3]. One may ask whether $d = 4F_{2n+1}F_{2n+2}F_{2n+3}$ can be a Fibonacci number, since then one would obtain a Diophantine quadruple of Fibonacci numbers. This was already proved not to be so by Jones in [12], who showed that $F_{6n+5} < d < F_{6n+6}$ holds for all $n \geq 1$.

The following conjecture appears in [9].

Conjecture 1.1. *There are no four positive integers* $a,\ b,\ c,\ d$ *such that* $\{F_a, F_b, F_c, F_d\}$ *is a Diophantine quadruple.*

While we do not know how to prove Conjecture 1.1, we prove the next best thing.

Theorem 1.2. *There are only finitely many Diophantine quadruples consisting of Fibonacci numbers.*

2. Preliminary results

In this section, we collect some results which will be used in our proof of Theorem 1.2. We start with some considerations about Fibonacci numbers. Let $(\alpha, \beta) = ((1+\sqrt{5})/2, (1-\sqrt{5})/2)$ be the two roots of the characteristic equation of the Fibonacci sequence $x^2 - x - 1 = 0$. Then the Binet formula for F_n is

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for all} \quad n \geq 0. \tag{2.1}$$

The Fibonacci sequence has a Lucas companion $\{L_n\}_{n\geq 0}$ given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. Its Binet formula is

$$L_n = \alpha^n + \beta^n \quad \text{for all} \quad n \geq 0. \tag{2.2}$$

There are many formulas involving Fibonacci and Lucas numbers. One which is useful to us is

$$L_n^2 - 5F_n^2 = 4(-1)^n \quad \text{for all} \quad n \geq 0. \tag{2.3}$$

The following result is proved in [9].

Lemma 2.1. *Assume that* $k \geq 1,\ n \geq 1$ *are integers and* $\{F_{2n}, F_{2n+2}, F_k\}$ *is a Diophantine triple. Then* $k = 2n+4$ *or* $k = 2n-2$ *(when* $n > 1$*) except when* $n = 2$*, in which case also* $k = 1$ *is possible.*

We next recall a result of Siegel concerning the finiteness of the number of solutions of a hyperelliptic equation.

LEMMA 2.2. *Let $\mathbb{K}$ be any number field and $\mathcal{O}_{\mathbb{K}}$ the ring of its algebraic integers. Let $f(X) \in \mathbb{K}[X]$ be a non-constant polynomial having at least 3 roots of odd multiplicity. Then the Diophantine equation*

$$y^2 = f(x)$$

has only finitely many solutions (x, y) in $\mathcal{O}_{\mathbb{K}}$.

We next need one more fact about Diophantine quadruples. The following result can be deduced from Theorem 1.5 in [7].

LEMMA 2.3. *Let $\{a, b, c, d\}$ be a Diophantine quadruple with $a < b < c < d$. If $c > 722b^4$, then the quadruple is regular.*

We prove two lemmas needed for the proof of Theorem 1.2.

LEMMA 2.4. *If k is a fixed nonzero integer, then the Diophantine equation $kF_n + 1 = x^2$ has only finitely many integer solutions (n, x).*

PROOF. Inserting $F_n = (x^2 - 1)/k$ into (2.3) and setting $y := L_n$, we get

$$y^2 = 5F_n^2 + 4(-1)^n = \frac{1}{k^2}\left(5x^4 - 10x^2 + (5 \pm 4k^2)\right).$$

Should the above equation have infinitely many integer solutions (x, y) it would follow, by Lemma 2.2 (we take $\mathbb{K} = \mathbb{Q}$), that one of the polynomials

$$f_{\pm,k}(X) = 5X^4 - 10X^2 + (5 \pm 4k^2)$$

has double roots. However, $f_{\pm,k}(X)' = 20X(X^2 - 1)$, so the only possible double roots of $f_{\pm,k}(X)$ are 0 or ± 1. Since $f_{\pm,k}(0) = 5 \pm 4k^2 \neq 0$ and $f_{\pm,k}(\pm 1) = \pm 4k^2 \neq 0$, it follows that $f_{\pm,k}(X)$ has in fact only simple roots, a contradiction. □

REMARK 2.5. In [13], all polynomials $P(X)$ of degree larger than 1 such that the Diophantine equation $F_n = P(x)$ has infinitely many integer solutions (n, x) were classified, so, in particular, we could have used this classification in the proof of Lemma 2.4. However, we preferred to give a direct proof of Lemma 2.4 especially since our proof reduces to an immediate verification of the hypotheses from Siegel's result stated in Lemma 2.2.

LEMMA 2.6. *Assume that k is a positive integer such that the Diophantine equation*

$$F_n F_{n+k} + 1 = x^2 \tag{2.4}$$

has infinitely many integer solutions (n, x). Then $k = 2, 4$ and all solutions have n even.

PROOF. Using (2.1) and (2.2), we get

$$F_n F_{n+k} + 1 = \frac{1}{5}(\alpha^n - \beta^n)(\alpha^{n+k} - \beta^{n+k}) + 1 = \frac{1}{5}\left(L_{2n+k} - (-1)^n L_k + 5\right).$$

Thus, if (n,x) satisfy (2.4), then $L_{2n+k} = 5x^2 + ((-1)^n L_k - 5)$. Inserting this into (2.3) (with n replaced by $2n+k$) and setting $y := F_{2n+k}$, we get

$$\begin{aligned} 5y^2 &= L_{2n+k}^2 - 4(-1)^k \\ &= 25x^4 + 10((-1)^n L_k - 5)x^2 + ((-1)^n L_k - 5)^2 - 4(-1)^k. \end{aligned}$$

Assuming that there are infinitely many integer solutions (n,x) to equation (2.4), it follows, by Lemma 2.2 (again, we take $\mathbb{K} = \mathbb{Q}$), that for $\zeta, \eta \in \{\pm 1\}$, one of the polynomials

$$g_{\zeta,\eta,k}(X) = 25X^4 + 10(\zeta L_k - 5)X^2 + (\zeta L_k - 5)^2 - 4\eta$$

has double roots. Now

$$g_{\zeta,\eta,k}(X)' = X(100X^2 + 20(\zeta L_k - 5))$$

so the only zeros of the derivative of $g_{\zeta,\eta,k}(X)$ are 0 and $\pm\sqrt{(5-\zeta L_k)/5}$.

Now $g_{\zeta,\eta,k}(0) = (\zeta L_k - 5)^2 - 4\eta$. If this is zero, then $\eta = 1$, and $\zeta L_k - 5 = \pm 2$. We thus get $\zeta L_k = 3, 7$, showing that $\zeta = 1$ and $k \in \{2,4\}$. Thus, $k \in \{2,4\}$ and $(-1)^n = \zeta = 1$, so n is even.

The other situation gives

$$g_{\zeta,\eta,k}(\pm\sqrt{(5-\zeta L_k)/5}) = -4\eta \neq 0.$$

Hence, this situation does not lead to double roots of $g_{\zeta,\eta,k}(X)$. Finally, when $k = 2,\ 4$ it is easy to see that if $F_n F_{n+k} + 1$ is a square then n is even. Indeed for n odd we have in fact

$$F_n F_{n+2} - 1 = F_{n+1}^2 \quad \text{and} \quad F_n F_{n+4} - 1 = F_{n+2}^2.$$

Hence, if also one of $F_n F_{n+2} + 1$ or $F_n F_{n+4} + 1$ is a square, we would get two squares whose difference is 2, which of course is impossible. ∎

3. Proof of Theorem 1.2

For a contradiction, we assume that there are infinitely many Diophantine quadruples of Fibonacci numbers. We denote a generic one by $\{F_a, F_b, F_c, F_d\}$ with $a < b < c < d$. Hence, $d \to \infty$ over such quadruples. Since

$$F_a F_d + 1 = \square$$

and $d \to \infty$, it follows, by Lemma 2.4, that $a \to \infty$. We next show that both $d - c \to \infty$ and $c - b \to \infty$. Assume say that $c - b = O(1)$ holds for infinitely many quadruples. Then there exists a positive integer k such that $c = b + k$ holds infinitely often. By Lemma 2.6, it follows that $k \in \{2,4\}$ and b is even. If $k = 2$, then by Lemma 2.1 applied several times, it follows that $(a,b,c,d) = (a, a+2, a+4, a+6)$, which contradicts the results of Dujella [3] and Jones [12]. Thus, we must have $c = b + 4$. Consider the following equations

$$F_a F_b + 1 = x^2 \quad \text{and} \quad F_a F_{b+4} + 1 = y^2$$

with some integers x and y. Multiplying the two relations above we get

$$F_a^2 F_b F_{b+4} + F_a(F_b + F_{b+4}) + 1 = (xy)^2.$$

Since $F_b F_{b+4} = F_{b+2}^2 \pm 1$ and $F_{b+4} + F_b = 3F_{b+2}$, we get

$$\begin{aligned}(xy)^2 &= F_a^2(F_{b+2}^2 \pm 1) + 3F_a F_{b+2} + 1\\ &= \left(F_a F_{b+2} + \frac{3}{2}\right)^2 - \left(\frac{5}{4} \mp F_a^2\right),\end{aligned}$$

so

$$\begin{aligned}\mp 4F_a^2 + 5 &= (2F_a F_{b+2} + 3)^2 - 4(xy)^2\\ &= (2F_a F_{b+2} + 3 - 2xy)(2F_a F_{b+2} + 3 + 2xy).\end{aligned}$$

The absolute value of the right–hand side is $\geq 2F_a F_{b+2} + 3 + 2xy \gg \alpha^{a+b}$, (because $2F_a F_{b+2} + 3 - 2xy$ is a nonzero integer), while of the left–hand side is $\ll \alpha^{2a}$. We thus get that

$$\alpha^{2a} \gg \alpha^{a+b},$$

showing that $b - a = O(1)$. By Lemma 2.6 again, it follows that $b - a \in \{2, 4\}$ with finitely many exceptions. The case $b = a+2$ leads, via Lemma 2.1 applied again several times, to the situation $(a, b, c, d) = (a, a+2, a+4, a+6)$, which we already saw that it is impossible, while the situation $b = a + 4$ together with $c = b + 4 = a + 8$, leads to

$$F_a F_{a+8} + 1 = \square,$$

which, by Lemma 2.6, can have only finitely many solutions a. Thus, $c - b \to \infty$. Notice that d was not used in the above argument (we only worked with the triple $\{F_a, F_b, F_c\}$). Thus, the same argument implies that $d - c \to \infty$ by working with the triple $\{F_b, F_c, F_d\}$ instead of the triple $\{F_a, F_b, F_c\}$.

Next assume that $c \geq 4b + 15$ infinitely often. Then

$$F_c \geq F_{4b+15} = F_{16}F_{4b} + F_{15}F_{4b-1} > 722F_{4b} > 722F_b^4,$$

so, by Lemma 2.3, it follows that the Diophantine quadruple $\{F_a, F_b, F_c, F_d\}$ is regular. Hence,

$$F_d = F_a + F_b + F_c + 2F_aF_bF_c + 2\sqrt{(F_aF_b + 1)(F_bF_c + 1)(F_aF_c + 1)}.$$

Since $F_m = \dfrac{\alpha^m}{\sqrt{5}}(1 + o(1))$ as $m \to \infty$, and $a \to \infty$, we get

$$\frac{\alpha^d}{\sqrt{5}}(1 + o(1)) = \frac{4}{5^{3/2}}\alpha^{a+b+c}(1 + o(1)),$$

showing that

$$\left|\alpha^{d-a-b-c} - \frac{4}{5}\right| = o(1), \quad \text{as} \quad a \to \infty.$$

Thus, $\alpha^{d-a-b-c} = 4/5$, which is impossible because $4/5$ does not belong to the multiplicative group generated by α.

Hence, $c \le 4b+14$ holds with finitely many exceptions. Thus, we arrived at the scenario where

$$F_bF_c + 1 = x^2$$

has infinitely many integer solutions (b, c, x) with $b < c \le 4b + 14$. Now the Corvaja-Zannier method based on the Subspace Theorem (see [2]) leads to the conclusion that there exists a line parametrized as

$$b = r_1 n + s_1, \quad c = r_2 n + s_2$$

for positive integers $r_1,\ r_2$ and integers $s_1,\ s_2$, such that for infinitely many positive integers n, there exists an integer v_n such that

$$F_{r_1 n+s_1} F_{r_2 n+s_2} + 1 = v_n^2.$$

We sketch the details of this deduction in the appendix. See also, for example, [5, 6] for completely worked out instances of this machinery. The condition $c \le 4b + 14$ implies $r_2 \le 4r_1$. The condition $c > b$ together with the fact that $c - b \to \infty$, implies that $r_2 > r_1$. By writing $s_1 = r_1 q + s_1'$ with $q = \lfloor s_1/r_1 \rfloor$ and $s_1' \in \{0, 1, \ldots, r_1 - 1\}$ and making the linear shift $n \mapsto n + \lfloor s_1/r_1 \rfloor$, we may assume that $s_1 \in \{0, 1, \ldots, r_1 - 1\}$. Finally, we may assume that $\gcd(r_1, r_2) = 1$ (otherwise, we let $\delta := \gcd(r_1, r_2)$ and replace n by δn). We may also assume that both $r_1 n$ and $r_2 n$ are even infinitely often (this is the case when n is even, for example), so $\beta^{r_1 n} = \alpha^{-r_1 n}$ and $\beta^{r_2 n} = \alpha^{-r_2 n}$. The other cases can be dealt with by similar arguments. We now use formula (2.1) and get

$$\begin{aligned} F_{r_1 n+s_1} F_{r_2 n+s_2} + 1 &= \frac{1}{5}(\alpha^{r_1 n+s_1} - \beta^{r_1 n+s_1})(\alpha^{r_2 n+s_2} - \beta^{r_2 n+s_2}) + 1 \\ &=: \frac{\alpha^{-n(r_1+r_2)}}{5} P_{r_1,r_2,s_1,s_2}(\alpha^n), \end{aligned}$$

where

$$P_{r_1,r_2,s_1,s_2}(X) = (\alpha^{s_1} X^{2r_1} - \beta^{s_1})(\alpha^{s_2} X^{2r_2} - \beta^{s_2}) + 5X^{r_1+r_2}.$$

Let $\mathbb{K} := \mathbb{Q}(\sqrt{5})$. We thus get that

$$P_{r_1,r_2,s_1,s_2}(\alpha^n) = \left(\frac{\alpha^{-n(r_1+r_2)/2}}{\sqrt{5}} \right)^2 v_n^2, \tag{3.1}$$

infinitely often with some integer v_n, and the right–hand side above is a square in $\mathcal{O}_{\mathbb{K}}$ for infinitely many n. Thus, the Diophantine equation

$$y^2 = P_{r_1,r_2,s_1,s_2}(x)$$

has infinitely many solutions (x, y) in $\mathcal{O}_{\mathbb{K}}$. In particular, $P_{r_1,r_2,s_1,s_2}(X)$ can have at most two roots of odd multiplicity by Lemma 2.2. In fact, we shall show that it has no root of odd multiplicity. Indeed, assume that z_0 is some root of odd multiplicity of $P_{r_1,r_2,s_1,s_2}(X)$. Let D be any positive integer. Infinitely many of our n will be in the same residue class r modulo D. Thus, such n can be written under the form $n = Dm + r$. We may then replace X by $X^D\alpha^r$ and work with $Q(X) := P_{r_1,r_2,s_1,s_2}(X^D\alpha^r)$. Equation

$$y^2 = Q(x)$$

still has infinitely many solutions (x, y) in $\mathcal{O}_{\mathbb{K}}$ (just take in (3.1) positive exponents n which are congruent to r modulo D), yet $Q(X)$ has at least D roots of odd multiplicity, namely all the roots of $X^D\alpha^r - z_0$. Since D is arbitrary (in particular, it can be taken to be any integer larger than 2), we conclude that this is possible only when $P_{r_1,r_2,s_1,s_2}(X)$ has all its roots of even multiplicity, so it is associated to the square of a polynomial in $\mathcal{O}_{\mathbb{K}}[X]$. So, let us write

$$P_{r_1,r_2,s_1,s_2}(X) = \gamma(X^{2r_1+2r_2} + \gamma_1 X^{2r_2} + \gamma_2 X^{r_1+r_2} + \gamma_3 X^{2r_1} + \gamma_4)$$

for some nonzero coefficients $\gamma, \gamma_1, \gamma_2, \gamma_3, \gamma_4$. Since $r_1 < r_2$, all the above monomials are distinct. Write $P_{r_1,r_2,s_1,s_2}(X) = \gamma R(X)^2$ for some monic polynomial $R(X) \in \mathbb{K}[X]$ and let us identify some monomials in $R(X)$. Certainly, $R(0) \neq 0$. Further, $\deg R(X) = r_1 + r_2$ and the last nonzero monomial in $R(X)$ is certainly X^{2r_1}. Hence, we get

$$P_{r_1,r_2,s_1,s_2}(X) = \gamma(X^{r_1+r_2} + \cdots + \delta_1 X^{2r_1} + \delta_0)^2,$$

for some nonzero coefficients δ_0, δ_1 which can be computed, up to sign, in terms of γ, γ_3, γ_4. Assume first that $R(X)$ does not have other monomials. Then

$$\begin{aligned}\gamma R(X)^2 = \gamma(&X^{2r_1+2r_2} + 2\delta_1 X^{3r_1+r_2} + \delta_1^2 X^{4r_1}\\ &+ 2\delta_0 X^{r_1+r_2} + 2\delta_0\delta_1 X^{2r_1} + \delta_0^2).\end{aligned}$$

The second leading monomial above is $X^{3r_1+r_2}$ and matching it with the second leading monomial in $P_{r_1,r_2,s_1,s_2}(X)$, which is X^{2r_2}, we get $r_2 = 3r_1$. Hence, since $\gcd(r_1, r_2) = 1$, we get $(r_1, r_2) = (1, 3)$.

Assume next that $R(X)$ contains monomials of intermediary degrees between $r_1 + r_2$ and $2r_1$. Let the leading one of them be of degree e. Thus,

$$R(X) = X^{r_1+r_2} + \delta X^e + \cdots + \delta_1 X^{2r_1} + \delta_0,$$

with some nonzero coefficient δ. Then the second leading monomial of $\gamma R(X)^2$ is $X^{r_1+r_2+e}$ and matching that with the second leading monomial appearing in $P_{r_1,r_2,s_1,s_2}(X)$ which is X^{2r_2}, we get that $r_1+r_2+e = 2r_2$, therefore $e = r_2-r_1$. The condition $e > 2r_1$ yields $r_2 > 3r_1$. Now let us look at X^{2e}. It might appear with nonzero coefficient in $R(X)^2$, or not. If it does, its degree must match the degree of one of the monomials of a lower degree in $P_{r_1,r_2,s_1,s_2}(X)$, which are $X^{r_1+r_2}$ or X^{2r_2}. We thus get $2e = 2r_2 - 2r_1 \in \{r_1 + r_2, 2r_2\}$, which give $r_2 = 3r_1$ or $r_2 = 2r_1$, respectively, none of which is possible since we just established that $r_2 > 3r_1$. So, X^{2e} cannot appear in $R(X)^2$. Well, that is only possible if $R(X)$ itself contains with a nonzero coefficient λ the monomial X^f such that $\delta^2 X^{2e}$ appearing in $R(X)^2$ is eliminated by the cross term

$2\lambda X^{r_1+r_2+f}$ of $R(X)^2$. Comparing degrees we get $r_1+r_2+f=2e=2r_2-2r_1$, so $f=r_2-3r_1$. However, since $f\geq 2r_1$, we get $r_2-3r_1\geq 2r_1$, so $r_2\geq 5r_1$, a contradiction since $r_2\leq 4r_1$. Hence, this case cannot appear.

Thus, the only possibility is $(r_1,r_2)=(1,3)$. Since $r_1=1$, it follows that $s_1=0$. Thus,

$$\begin{aligned}P_{r_1,r_2,s_1,s_2}(X)=P_{1,3,0,s_2}(X)&=(X^2-1)(\alpha^{s_2}X^6-\beta^{s_2})+5X^4\\&=\alpha^{-s_2}((X^2-1)(\alpha^{2s_2}X^6-(-1)^{s_2})+5\alpha^{s_2}X^4).\end{aligned}$$

We thus took

$$P_\zeta(X,Y)=(X^2-1)(Y^2X^6-\zeta)+5YX^4\quad\text{for}\quad\zeta\in\{\pm1\}.$$

We computed the derivative of $P_\zeta(X,Y)$ with respect to X and computed the resultant, with respect to the variable X, of this polynomial with $P_\zeta(X,Y)$. We got

$$Q_\zeta(Y):=\mathrm{Res}_X\left(P_\zeta(X,Y),\frac{\partial P_\zeta}{\partial X}(X,Y)\right).$$

So, the roots of $Q_\zeta(Y)$ are exactly the values of Y for which $P_\zeta(X,Y)$ has a double root as a polynomial in X. It turns out when $\zeta=1$, the only roots of $Q_1(Y)$ are zero, and the roots of an irreducible polynomial of degree 4, so such roots are not of the form α^{s_2} for some integer exponent s_2. However, when $\zeta=-1$, we have that

$$Q_{-1}(Y)=-256Y^{12}(Y^2-29Y-1)^2(27Y^2-527Y-27)^2,$$

and we recognize that α^7 and β^7 are roots of $Q_{-1}(Y)$. The factor $27Y^2-527Y-27$ has roots which are not algebraic integers, so they cannot be powers of α of integer exponent. Thus, the only possibilities are $s_2\in\{\pm7\}$. However,

$$P_{-1}(X,\alpha^7)=(X^2-\beta^4)^2G(X),$$

where

$$G(X)=\alpha^{14}X^4-(\alpha^{13}+\alpha^9)X^2-\alpha^8$$

is an irreducible polynomial of degree 4 in $\mathbb{K}[X]$. Replacing α^7 by β^7 above gives the conjugate of $P_{-1}(X^7,\alpha^7)$ in $\mathbb{K}[X]$. Thus, there is no instance in which $P_{r_1,r_2,s_1,s_2}(X)$ has all its roots of even multiplicity, which finishes the proof.

Appendix

Here, we prove the following lemma.

Lemma A.1. *Assume that there are infinitely many triples of positive integers (b,c,x) with $b<c\leq 4b+14$ such that*

$$F_bF_c+1=x^2. \tag{A.1}$$

Then there exist integers $r_1 > 0, r_2 > 0, s_1, s_2$ such that for infinitely many positive integers n there is an integer v_n with

$$F_{r_1 n+s_1} F_{r_2 n+s_2} + 1 = v_n^2.$$

PROOF. Since there are infinitely many values for the triple (b, c, x), we may assume that the parities of b and c are fixed. We also assume that b is large. Let $\zeta = (-1)^b,\ \eta = (-1)^c$. We take square roots in (A.1) getting

$$x = \frac{\alpha^{(b+c)/2}}{\sqrt{5}} F_{b,c}(1/\alpha),$$

where

$$F_{b,c}(z) = \sqrt{(1 - \zeta z^{2b})(1 - \eta z^{2c}) + 5z^{b+c}}.$$

We expand $F_{b,c}(z)$ in Taylor series around the origin getting

$$\begin{aligned} F_{b,c}(z) &= 1 + \frac{1}{2}(-\eta z^{2b} - \eta z^{2c} + \eta\zeta z^{2b+2c} + 5z^{b+c}) + \cdots \\ &\quad + \binom{1/2}{k}(-\zeta z^{2b} - \eta z^{2c} + \eta\zeta z^{2b+2c} + 5z^{b+c})^k + \cdots \\ &= \sum_{i,j\geq 0} C_{i,j} z^{ib+jc}. \end{aligned}$$

We separate in the above formula the terms with $i + j \leq 5$. We thus write

$$\text{(A.2)} \qquad \left| x - \frac{\alpha^{(b+c)/2}}{\sqrt{5}} \sum_{i+j\leq 5} C_{i,j}\alpha^{-ib-jc} \right| = \frac{\alpha^{(b+c)/2}}{\sqrt{5}} \left| \sum_{i+j\geq 6} C_{i,j}\alpha^{-ib-jc} \right|.$$

We estimate the right-hand side of (A.2). Note that the Taylor expansion of $F_{b,c}(z)$ comes from the Taylor expansion of

$$\sqrt{1+w} = \sum_{k\geq 0} \binom{1/2}{k} w^k,$$

with $w := -\zeta z^{2b} - \eta z^{2c} + \zeta\eta z^{2b+2c} + 5z^{b+c}$. The sum of the absolute values of the coefficients of w (as a polynomial in z) is ≤ 10. It thus follows easily, using $|\binom{1/2}{k}| < 1$, that $|C_{i,j}| < 10^{i+j}$. Since $b < c \leq 4b + 14$, it follows, from the above remarks, that the size of the right–hand side in (A.2) above is

$$\text{(A.3)} \qquad \ll \alpha^{5b/2} \left| \sum_{k\geq 6} \sum_{i+j=k} C_{i,j}\alpha^{-ib-jc} \right| \ll \alpha^{5b/2} \sum_{k\geq 6} k^2 \left(\frac{10}{\alpha^b}\right)^k \ll \alpha^{-7b/2}.$$

The above calculation is justified for b large because in this case $\alpha^b > 10$, so the above series is bounded by the second derivative of the geometric series in $10/\alpha^b$. We will apply the subspace theorem with the following data. We assume $b + c$ is even, for simplicity. The case when $b + c$ is odd can be treated similarly. We take $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. This is a real quadratic fields with two infinite places $|\bullet|_+$ and $|\bullet|_-$ given by $|y|_+ = |\sigma(y)|^{1/2}$ and $|y|_- = |\tau(y)|^{1/2}$, where σ and τ are the two embeddings of $\mathbb{K}$ in $\mathbb{R}$ given by $\sigma(\sqrt{5}) = \sqrt{5}$ and $\tau(\sqrt{5}) = -\sqrt{5}$, respectively. We take $\mathcal{S} = \{+, -\}$ to be the set consisting of the two infinite places of $\mathbb{K}$. We take $N = 22$ and define the following $2N$ linear forms in N-variables. Observe that there are $\binom{7}{2} = 21$ pairs (i, j) with $i + j \leq 5$, namely

$$\begin{aligned}&(0,0),\ (0,1),\ (0,2),\ (0,3),\ (0,4),\ (0,5),\ (1,0),\\ &(1,1),\ (1,2),\ (1,3),\ (1,4), (2,0),\ (2,1),\ (2,2),\ (2,3),\\ &(3,0),\ (3,1),\ (3,2),\ (4,0),\ (4,1),\ (5,0).\end{aligned} \tag{A.4}$$

We take

$$\mathbf{x} = (x_0, x_{i,j} : i + j \leq 5),$$

where we label the last 21 variables of $\mathbf{x}$ as in (A.4). As for the linear forms, we take

$$L_{0,+}(\mathbf{x}) = x_0 - \sum_{i+j\leq 5} C_{i,j} x_{i,j}, \quad L_{0,-}(\mathbf{x}) = x_0, \quad L_{i,j,\pm}(\mathbf{x}) = x_{i,j}, \quad i + j \leq 5.$$

We compute the double product

$$P = |L_{0,+}(\mathbf{x})|_+ |L_{0,-}(\mathbf{x})|_- \prod_{i+j\leq 5} |L_{i,j,+}(\mathbf{x})|_+ |L_{i,j,-}(\mathbf{x})|_-, \tag{A.5}$$

when $x_0 = x$ and $x_{i,j} = \dfrac{\alpha^{(b+c)/2}}{\sqrt{5}} \alpha^{-ib-jc}$ for $i + j \leq 5$. Since $|\bullet|_+$ leaves α unchanged while $|\bullet|_-$ maps α to β, it follows that

$$\prod_{i+j\leq 5} |L_{i,j,+}(\mathbf{x})|_+ |L_{i,j,-}(\mathbf{x})|_- = 5^{-21/2} \ll 1.$$

Since $x \in \mathbb{Q}$, it follows that $\tau(x) = x$, so $|L_{0,-}(\mathbf{x})|_- = |x|^{1/2}$, while since $\sigma(x) = x$ and $\sigma(\alpha) = \alpha$, it follows that

$$|L_{0,+}(\mathbf{x})|_+ = \left| x - \frac{\alpha^{(b+c)/2}}{\sqrt{5}} \sum_{i+j\leq 6} C_{i,j} \alpha^{-ib-jc} \right|^{1/2} \ll \alpha^{-7b/4},$$

by calculations (A.2) and (A.3). Thus, for the product P shown at (A.5)

$$P \ll \sqrt{x} \alpha^{-7b/4} \ll \alpha^{(b+c)/4} \alpha^{-7b/4} \ll \alpha^{-b/2}, \tag{A.6}$$

We now compute the height of $\mathbf{x}$. Recall $H(\mathbf{x}) = H(\lambda\mathbf{x})$ for every algebraic number λ, and that if the components of $\mathbf{x}$ are algebraic integers, then

$$|\mathbf{x}|_+ = \max\{|x_j|_+; 1 \leq j \leq N\}, \qquad |\mathbf{x}|_- = \max\{|x_j|_-; 1 \leq j \leq N\},$$

and

$$H(\mathbf{x}) = \max\{1, |\mathbf{x}|_+\} \cdot \max\{1, |\mathbf{x}|_-\}.$$

For us, the components of $\sqrt{5}\mathbf{x}$ are algebraic integers, so

$$\begin{aligned} |\mathbf{x}|_+ &\ll x^{1/2} \ll \alpha^{5b/4}, \\ |\mathbf{x}|_- &\ll \alpha^{(5c-(b+c)/2)/2} \ll \alpha^{(9c-b)/4} \ll \alpha^{35b/4}, \end{aligned} \tag{A.7}$$

so

$$H(\mathbf{x}) \ll \alpha^{10b}. \tag{A.8}$$

Thus, from (A.6) and (A.8), we get that

$$|L_{0,+}(\mathbf{x})_+|L_{0,-}(\mathbf{x})|_- \prod_{i+j\le 5} |L_{i,j,+}(\mathbf{x})|_+|L_{i,j,-}(\mathbf{x})|_- \ll H(\mathbf{x})^{-1/20}. \tag{A.9}$$

It follows, by the subspace theorem, that there exist only finitely many hyperplanes in $\mathbb{K}^N$ containing the solutions $\mathbf{x}$ of the above inequality (A.9). That is, there are finitely many nonzero many vectors $\mathbf{c}^{(\lambda)} = (c_1^{(\lambda)}, \ldots, c_N^{(\lambda)})$ for $\lambda = 1, \ldots, M$, such that any solution $\mathbf{x}$ of (A.9) satisfies

$$\sum_{i=1}^{N} c_i^{(\lambda)} x_i = 0 \quad \text{for some} \quad \lambda \in \{1, \ldots, M\}. \tag{A.10}$$

Assume that our $\mathbf{x}$ satisfies one of the equations (A.10). We distinguish two cases.

Case 1. $c_1^{(\lambda)} = 0$. This means that the unknown $x_0 = x$ is not involved in (A.10). In this case, the only variables involved are $x_{i,j}$ for $i + j \le 5$, so equation (A.10) is of the form

$$P(\alpha^b, \alpha^c) = 0,$$

where

$$P(X,Y) = \sum_{i+j\le 5} D_{i,j} X^i Y^j$$

is not the zero polynomial. This equation is an S-unit equation, where S is the multiplicative subgroup generated by α in $\mathbb{K}$. As such, by the theorem on the finiteness of the solutions to nondegenerate S-unit equations, it has finitely many projective solutions. In particular, if we take $(i,j) \ne (i_1, j_1)$ such that $D_{i,j} \ne 0$ and $D_{i_1,j_1} \ne 0$ (which must exist, otherwise $P(X,Y)$ is just a monomial, so $P(\alpha^b, \alpha^c) = 0$ has no positive integer solution (b,c) whatsoever), then $\alpha^{ib+jc}/\alpha^{i_1 b + j_1 c}$ takes only finitely many values. Thus, $(i-i_1)b + (j-j_1)c$ takes only finitely many values. Thus, (b,c) is a point on one of finitely many lines. Since there are infinitely many possibilities for (b,c), we conclude that there is some line containing infinitely many of them.

Case 2. $c_1^{(\lambda)} \ne 0$. In this case, we can express

$$x_0 = -\sum_{i=2}^{N} (c_i^{(\lambda)}/c_1^{(\lambda)}) x_{i,j} \tag{A.11}$$

using formula (A.10) and insert this into

$$x_0^2 = F_b F_c + 1 = \frac{1}{5}(\alpha^b - \zeta\alpha^{-b})(\alpha^c - \eta\alpha^{-c}) + 1. \tag{A.12}$$

Now x_0 is linear combination of monomials (of positive or negative degrees) in $(X, Y) = (\alpha^b, \alpha^c)$. If the resulting relation is degenerate (thus, if the above formula holds identically for all b and c), it then follows that

$$(X^2 - \zeta)(Y^2 - \eta) + 5XY$$

is associated to a square in $\mathbb{K}[X, Y]$. Since it is monic of degree 2 in both X and Y, it follows that we must have a relation of the form

$$(X^2 - \zeta)(Y^2 - \eta) + 5XY = (XY + \cdots + \delta)^2 \quad \text{in} \quad \mathbb{K}[X, Y]. \tag{A.13}$$

In the right–hand side of (A.13), we cannot have non–constant monomials different from XY, since otherwise upon squaring we would end up with monomials of degree at least three different than X^2Y^2 which do not exist in the left–hand side of (A.13). However,

$$(XY + \delta)^2 = X^2Y^2 + 2\delta XY + \delta^2$$

contains neither X^2, nor Y^2, which do appear in the left–hand side of (A.13), a contradiction. Thus, the relation is nondegenerate, meaning that relation (A.12) with x_0 given by (A.11) yields a relation of the form $Q(\alpha^b, \alpha^c) = 0$, with some nonzero polynomial $Q(X, Y) \in \mathbb{K}[X, Y]$. As in Case 1, the theorem on the finiteness of nondegenerate solutions of S-unit equations yields the conclusion that the point (b, c) belongs to finitely many lines.

Hence, there exists a line containing infinitely many points (b, c). In particular, there are rational numbers (r_1, s_1, r_2, s_2) such that for infinitely many n, the pair

$$(b, c) = (r_1 n + s_1, r_2 n + s_2)$$

consists a positive integers (b, c) satisfying equation (A.1) for some integer x (depending on n). It remains to justify that r_1, s_1, r_2, s_2 can be assumed to be integers. Well, let Δ be common denominator of r_1 and r_2. Since there are infinitely many n, infinitely many of them will be in the same residue class r (mod Δ). Thus, writing such n as $\Delta m + r$, we get

$$(b, c) = ((r_1\Delta)m + (r_1 r + s_1), (r_2\Delta)m + (r_2 r + s_2)).$$

Now m, $r_1\Delta$, $r_2\Delta$, b, c are all integers so $r_1 r + s_1$ and $r_2 r + s_2$ are also integers. Replacing (r_1, r_2) by $(r_1\Delta, r_2\Delta)$ and (s_1, s_2) by $(r_1 r + s_1, r_2 r + s_2)$, we may assume that r_1, r_2, s_1, s_2 are integers. Thus,

$$F_{r_1 m + s_1} F_{r_2 m + s_2} + 1 \tag{A.14}$$

is a square for infinitely many m. Clearly, r_1 and r_2 are positive. This finishes the proof of the lemma. $\square$

Acknowledgements.
We thank the referees for a careful reading of the manuscript and for suggesting changes which improved the quality of our paper. F. L. thanks A. Dujella for useful discussions. This work started at the DARF conference at Nihon University in January 2017 where both authors participated. They thank the organizers for the opportunity to attend this event. F. L. also worked on this paper while he was a long term guest of the Max Planck Institute for Mathematics in Bonn, Germany from January to July, 2017. He thanks that Institution for hospitality and support.

References

[1] J. Arkin, V. E. Hoggatt and E. G. Strauss, *On Euler's solution of a problem of Diophantus,* Fibonacci Quart. **17** (1979), 333–339.
[2] P. Corvaja and U. Zannier, *Diophantine equations with power sums and universal Hilbert sets,* Indag. Math. (N.S.) **9** (1998), 317–332.
[3] A. Dujella, *A proof of the Hoggatt-Bergum conjecture,* Proc. Amer. Math. Soc. **127** (1999), 1999–2005.
[4] A. Dujella, *There are only finitely many Diophantine quintuples,* J. Reine Angew. Math. **566** (2004), 183–214.
[5] C. Fuchs, F. Luca and L. Szalay, *Diophantine triples with values in binary recurrences,* Ann. Sc. Norm. Sup. Pisa **7** (2008), 579–608.
[6] C. Fuchs, C. Hutle, F. Luca and L. Szalay, *Diophantine triples with values in k-generalized Fibonacci sequences,* Bull. Malaysian Math. Soc., 2016, doi 10.1007/s40840-016-0405-4.
[7] Y. Fujita and T. Miyazaki, *The regularity of Diophantine quadruples,* Trans. Amer. Math. Soc., to appear.
[8] P. E. Gibbs, Computer Bulletin **17** (1978), 16.
[9] B. He, F. Luca and A. Togbé, *Diophantine triples of Fibonacci numbers,* Acta Arith. **175** (2016), 57–70.
[10] B. He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple,* Preprint (2016), arXiv:1610.04020v1.
[11] V. E. Hoggatt and G. E. Bergum, *A problem of Fermat and the Fibonacci sequence* Fibonacci Quart. **15** (1977), 323–330.
[12] B. W. Jones, *A second variation on a problem of Diophantus and Davenport,* Fibonacci Quart. **16** (1978), 155–165.
[13] I. Nemes and A. Pethö, *Polynomial values in linear recurrences,* J. Number Theory **24** (1986), 47–53.

Y. Fujita
Department of Mathematics
College of Industrial Technology
Nihon University
2-11-1 Shin-ei, Narashino, Chiba
Japan
E-mail: fujita.yasutsugu@nihon-u.ac.jp

F. Luca
School of Mathematics
University of the Witwatersrand
Private Bag X3, Wits 2050
South Africa
&
Max Planck Institute for Mathematics
Vivatsgasse 7, 53111 Bonn
Germany
&
Department of Mathematics
Faculty of Sciences
University of Ostrava
30. dubna 22, 701 03 Ostrava 1
Czech Republic
E-mail: florian.luca@wits.ac.za

Received: 11.3.2017.
Revised: 6.6.2017.