involve
a journal of mathematics

Polynomial values in Fibonacci sequences

Adi Ostrov, Danny Neftin, Avi Berman and Reyad A. Elrazik

msp

2020 vol. 13, no. 4

INVOLVE 13:4 (2020)
https://doi.org/10.2140/involve.2020.13.597

Polynomial values in Fibonacci sequences

Adi Ostrov, Danny Neftin, Avi Berman and Reyad A. Elrazik

(Communicated by Kenneth S. Berenhaut)

The only perfect powers in the Fibonacci sequence are 0, 1, 8, and 144, and in the Lucas sequence, the only perfect powers are 1 and 4. We prove that in sequences that follow the same recurrence relation of the Lucas and Fibonacci sequences, there are always only finitely many polynomial values $g(\mathbb{Z})$ for any polynomial g which is not equivalent to a Dickson polynomial.

1. Introduction

The Fibonacci $F^{0,1}$ and Lucas $F^{2,1}$ sequences are special cases of generalized Fibonacci sequences $F^{a,b} = \{F_n\}_{n=0}^{\infty}$, $a, b \in \mathbb{Z}$, defined by the recurrence relation $F_{n+1} = F_n + F_{n-1}$, with initial values $F_0 = a$, $F_1 = b$.

Classical results show that 4 is the largest perfect square in the Lucas sequence and that 144 is the largest perfect square in the Fibonacci sequence [Cohn 1964]. Subsequently, much work was devoted to studying perfect powers in the Fibonacci and Lucas sequences, leading to their determination in [Bugeaud et al. 2006, §2]. This motivates the following natural question:

Question 1. For which polynomials $g \in \mathbb{Q}[x]$ does $F^{a,b}$, $a, b \in \mathbb{Z}$, contain only finitely many values from $g(\mathbb{Z})$?

The following theorem answers the question when g is not a Dickson polynomial composed with linear polynomials. For $m \in \mathbb{Q}^{\times}$, denote by $D_{d,m} \in \mathbb{Q}[x]$ the Dickson polynomial of degree d, that is, the unique polynomial of degree d satisfying

$$D_{d,m}\left(x + \frac{m}{x}\right) = x^d + \frac{m^d}{x^d}.$$

Define the (normalized) Chebychev polynomial of degree d to be $T_d := D_{d,1}$.

MSC2010: 11B39, 11C08.
Keywords: recurrence sequence, polynomial values, Fibonacci.

Let φ denote the golden ratio $(1+\sqrt{5})/2$, and let $\chi_{a,b}$ represent the norm of $a+b\varphi \in \mathbb{Z}[\varphi]$, so that $\chi_{a,b} = N_{\mathbb{Z}[\varphi]/\mathbb{Z}}(a+b\varphi) = a^2+ab-b^2$.

Theorem 1. *Let $F^{a,b}$, $a, b \in \mathbb{Z}$, be a generalized Fibonacci sequence, and $g(x) \in \mathbb{Q}[x]$ a polynomial of degree $d > 1$. Assume that $g(x) \neq \alpha_{\chi,d,m} D_{d,m}(\mu(x))$ for all linear $\mu \in \mathbb{Q}[x]$ and $m \in \mathbb{Z} \setminus \{0\}$, where $\alpha_{\chi,d,m} = \pm\sqrt{-\chi/(5m^d)}$ for $\chi = \chi_{a,b}$ or $-\chi_{a,b}$. Then $F^{a,b}$ contains only finitely many values from $g(\mathbb{Z})$; that is, $\#(g(\mathbb{Z}) \cap F^{a,b}) < \infty$. In particular, $F^{a,b}$ contains only finitely many perfect squares.*

If $g(x)$ is of the form $\alpha_{\chi,d,m} D_{d,m}(\mu(x))$, then $\alpha_{\chi,d,m} \in \mathbb{Q}$, and hence -5χ is a square if d is even, and $-5m\chi$ is a square if d is odd. Also, flipping the sign of $\chi = \chi_{a,b}$ corresponds to shifting the sequence by one element, that is, $\chi_{b,a+b} = -\chi_{a,b}$.

We note that the sequence $F^{a,b}$ may indeed have infinite intersection with $\pm\alpha_{\chi,d,1} T_d(\mathbb{Z})$. For example, the Lucas sequence, which has $|\chi_{2,1}| = 5$ and satisfies the identity $L_{2n} = L_n^2 - (-1)^n \cdot 2$ [Cohn 1964, (3)], has infinite intersection with $g(\mathbb{Z})$ for $g(x) = T_2(x) = x^2 - 2$ and for $g(x) = -T_2(ix) = x^2 + 2$, where $i = \sqrt{-1}$. The Fibonacci sequence, which has $|\chi_{0,1}| = 1$ and satisfies the identity $F_{3n} = 5F_n^3 + 3(-1)^n F_n$ [Nagy et al. 2019, Table 2], has infinite intersection with $g(\mathbb{Z})$ for

$$g(x) = \frac{1}{\sqrt{5}} T_3(\sqrt{5}x) = 5x^3 - 3x \quad \text{and} \quad g(x) = -\frac{1}{\sqrt{-5}} T_3(\sqrt{-5}x) = 5x^3 + 3x.$$

Also note that in all examples the values $\{n : F_n \in g(\mathbb{Z})\}$ constitute the union of arithmetic progressions up to a finite set, as shown in the final assertion of [Corvaja and Zannier 1998, Theorem 2] (applied to $F(X,Y) = X - g(Y)$).

Since $x^d \neq D_{d,m}(x)$ for $m \neq 0$ (as $(x+m/x)^d \neq x^d + m^d/x^d$) for $d \geq 2$, Theorem 1 implies there is a finite number of d-th powers in any generalized Fibonacci sequence. Note that the theorem does not give a uniform bound for all $d \geq 0$, and hence does not generalize [Bugeaud et al. 2006]. Finally, we note that the proof of the theorem is effective, generalizes to number fields and to other recurrence sequences; see Remark 6.

2. Preliminaries

2.1. ***Chebyshev and Dickson polynomials.*** Recall that $T_d \in \mathbb{Z}[x]$ denotes the normalized[1] Chebyshev polynomial, that is, the unique degree-d polynomial which satisfies $T_d(x+1/x) = x^d + 1/x^d$. For an algebraic $m \in \mathbb{C} \setminus \{0\}$, the Dickson polynomial $D_{d,m} \in \mathbb{Q}(m)[x]$ satisfies $D_{d,m}(x+m/x) = x^d + m^d/x^d$ [Schinzel

[1] The usual Chebychev polynomials are $\frac{1}{2}T_d(2x)$; see [Zieve and Mueller 2008, §3].

2000, §1.4, Corollary 2]. Thus

$$D_{d,m}\left(x+\frac{m}{x}\right)=x^d+\frac{m^d}{x^d}=m^{d/2}\left(\frac{x^d}{m^{d/2}}+\frac{m^{d/2}}{x^d}\right)$$
$$=m^{d/2}T_d\left(\frac{x}{\sqrt{m}}+\frac{\sqrt{m}}{x}\right)=m^{d/2}T_d\left(\frac{1}{\sqrt{m}}\left(x+\frac{m}{x}\right)\right). \tag{1}$$

Two polynomials f, g are called equivalent if $f=\ell_1\circ g\circ\ell_2$ for some linear $\ell_1,\ell_2\in\mathbb{C}[x]$. We use the following well known fact [Schinzel 2000, §1.4, Lemma 4]:

Lemma 2. *Suppose $g(x)\in\mathbb{C}[x]$ is of degree $d>1$ and satisfies*

$$(g(x)-a_1)(g(x)-a_2)=(x-r_1)(x-r_2)R(x)^2$$

for complex $a_1\neq a_2$, $r_1\neq r_2$, and $R(x)\in\mathbb{C}[x]$. Then $g(x)=\ell_1\circ T_d\circ\ell_2$, where

$$\ell_1(x)=\pm\frac{a_1-a_2}{4}x+\frac{a_1+a_2}{2}\quad\textit{and}\quad\ell_2^{-1}(x)=\frac{r_1-r_2}{4}x+\frac{r_1+r_2}{2}.$$

Similar results to the following lemma and corollary are well known in particular cases, including $p(x)=T_d(x)$ [Lidl et al. 1993, Lemma 6.15]. Since the proof appears to be new, we give it here:

Lemma 3. *Let $K\subset\mathbb{C}$ be a subfield, $\varepsilon\in\mathbb{C}^\times$, and $\mu(x)\in\mathbb{C}[x]\setminus K[x]$ be of degree 1. Suppose that all roots of $p(x)\in K[x]$ are real, and the minimal root r is different from the maximal one R. If $\varepsilon p(\mu(x))\in K[x]$, then $R+r\in K$ and $\mu(x)=\sqrt{m}\eta(x)+(R+r)/2$ for linear $\eta\in K[x]$, and $m\in K^\times$. Furthermore, $\varepsilon\in\sqrt{m}\cdot K$ if $p(x-(R+r)/2)$ is an odd polynomial, and $\varepsilon\in K$ otherwise.*

Proof. Let A be the set of roots of $p(x)$. Notice that $\mu^{-1}(A)$ is the set of zeros of $g(x):=\varepsilon p(\mu(x))\in K[x]$. Since $p(x), g(x)\in K[x]$, both A and $\mu^{-1}(A)$ are invariant under every K-automorphism σ, giving

$$\mu^{-1}(A)=\sigma(\mu^{-1}(A))=\sigma(\mu^{-1})(\sigma(A))=\sigma(\mu^{-1})(A).$$

Write $\mu^{-1}(x)=\gamma x+\delta$, so that $\sigma(\mu^{-1})(x)=\sigma(\gamma)x+\sigma(\delta)$. Note that the points of A lie on a segment whose endpoints are R, r. Thus the points $\mu^{-1}(A)$ lie on a segment in $\mathbb{C}$ whose end points are either $(\mu^{-1}(R),\mu^{-1}(r))=(\sigma(\mu^{-1})(R),\sigma(\mu^{-1})(r))$ or $(\mu^{-1}(R),\mu^{-1}(r))=(\sigma(\mu^{-1})(r),\sigma(\mu^{-1})(R))$. In the former case

$$\begin{aligned}R\gamma+\delta&=R\sigma(\gamma)+\sigma(\delta),\\ r\gamma+\delta&=r\sigma(\gamma)+\sigma(\delta),\end{aligned}\tag{2}$$

while in the latter, the ends flip:

$$\begin{aligned}R\gamma+\delta&=r\sigma(\gamma)+\sigma(\delta),\\ r\gamma+\delta&=R\sigma(\gamma)+\sigma(\delta).\end{aligned}\tag{3}$$

Since $R \neq r$, for σ in case (2), we have $\sigma(\delta)=\delta$ and $\sigma(\gamma)=\gamma$. For σ in case (3), σ flips the ends, and hence σ^2 fixes them, so that σ^2 is in case (2), that is $\sigma^2(\delta)=\delta$. Moreover, taking the difference of the two equations in (3) gives $\sigma(\gamma)=-\gamma$. Since $\sigma(\gamma)=\pm\gamma$ for every K-automorphism σ, we have $\gamma=\sqrt{m}$ for $m \in K$. Plugging this into (3) gives $(R+r)\sqrt{m}=\sigma(\delta)-\delta$.

Since (2) and (3) imply that every K-automorphism that fixes $\gamma=\sqrt{m}$ also fixes δ, we have $\delta=a+b\sqrt{m}\in K[\sqrt{m}]$. If $R=-r$, for σ as in (3) we also have $\sigma(\delta)=\delta$, and hence $\delta \in K$. Otherwise, case (3) gives $(R+r)\gamma=2b\gamma$, and hence

$$b=\frac{R+r}{2}\in K$$

and

$$\mu^{-1}(x)=\sqrt{m}\left(x+\frac{R+r}{2}\right)+a \quad \text{for } a \in K.$$

Thus

$$\mu(x)=\frac{1}{\sqrt{m}}(x-a)-\frac{R+r}{2}.$$

Note that since μ is assumed not to be in $K[x]$, case (2) holds for some σ and hence $R+r \in K$.

Write

$$q(x):=p\left(x-\frac{R+r}{2}\right)\in K[x],$$

and

$$\mu(x)+\frac{R+r}{2}=\sqrt{m}\eta(x)$$

for a linear $\eta \in K[x]$, so that $\varepsilon p(\mu(x))=\varepsilon q(\sqrt{m}\eta(x))$ and hence $\varepsilon q(\sqrt{m}x)$ are in $K[x]$. If q is odd, then $q(\sqrt{m}x)=\sqrt{m}s(x)$, where $s(x)\in K[x]$; thus $\varepsilon\cdot\sqrt{m}\in K$. Otherwise, q has at least one nonzero monomial of even degree, say $\varepsilon q_{2k}m^k x^{2k}\in K\cdot x^{2k}$ with $q_{2k}\in K\setminus\{0\}$, so that $\varepsilon \in K$. □

Corollary 4. *Let $K\subseteq\mathbb{C}$ be a field and $d\geq 2$ an integer. Suppose $q(x):=\varepsilon T_d(\mu(x))\in K[x]$ for $\varepsilon\in\mathbb{C}^\times$ and linear $\mu\in\mathbb{C}[x]$. Then $q(x)=\varepsilon m^{d/2}D_{d,m}(m\eta(x))$ for $m\in K^\times$ such that $\varepsilon m^{d/2}\in K$, where $\eta(x)=\mu(x)/\sqrt{m}\in K[x]$.*

Proof. All roots of $T_d(x)$ are real, the maximal root is $R=2$, and the minimal root is $r=-2$. If $\mu\in K[x]$, then $\varepsilon\in K$, and the claim follows with $m=1$. Otherwise, as $R+r=0$, Lemma 3 yields that $\mu(x)=\sqrt{m}\eta(x)\in K[x]$ for some $m\in K^\times$. Since in addition $T_d(x)=m^{-d/2}D_{d,m}(\sqrt{m}x)$ by (1), we get $q(x)=\varepsilon m^{d/2}D_{d,m}(m\eta(x))$. □

2.2. ***Siegel's theorem.*** We shall also use the following explicit version of Siegel's theorem [LeVeque 1964, Theorem 1] for the special case of hyperelliptic curves:

Theorem 5. *Let $f(x)\in K[x]$ be a polynomial of degree ≥ 3 over a number field K which factors as $f(x)=a\prod_{i=1}^{s}(x-\alpha_i)^{r_i}$ for distinct $\alpha_i\in\mathbb{C}$, for $a\in K$, and integers $r_i\geq 1$. If $y^2=f(x)$ has infinitely many solutions in the ring of integers of K, then at most two of the r_i are odd.*

In the case $K = \mathbb{Q}$ and $u(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ has at least three distinct simple roots, Baker [1969, Theorem 2][2] gave an (exponential) bound on $\max\{|x|, |z|\}$ for solutions (x, z) to $z^2 = u(x)$, in terms of $\max\{|a_i| : i = 0, \ldots, n\}$. In other words, the solution to $z^2 = u(x)$ is effective.

An effective solution to $y^2 = f(x)$ can be deduced in the case at least three of the multiplicities r_i of roots of f are odd. Indeed, this case reduces to the situation in Baker's theorem by a variable change $z = y/h(x)^2$, where $h(x) \in \mathbb{Q}[x]$ satisfies $h(x)^2 \mid f(x)$ and $f(x)/h(x)^2$ is square-free, since the resulting equation is $z^2 = u(x)$ with $u(x) = f(x)/h(x)^2$ has at least three simple roots.

3. Proof of Theorem 1

Recall that to a generalized Fibonacci sequence $F^{a,b}$, we attach $\chi_{a,b} = a^2 + ab - b^2$. Note that $\chi_{a,b} \neq 0$ for $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Indeed, if $a^2 + ab - b^2 = 0$, then

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

Since $a, b \in \mathbb{Z}$, this implies $\chi_{a,b} = 0$ if and only if $a = b = 0$.

Proof of Theorem 1. If $a = b = 0$, the only element in the sequence is 0, and the theorem holds trivially. Henceforth, as above, we may assume $\chi_{a,b} \neq 0$. We first claim that each element of $F^{a,b}$ gives rise to a unique integer solution to one of the two equations $y^2 = 5x^2 \pm 4\chi_{a,b}$ given by $(x, y) = (F_n, \sqrt{5F_n^2 - 4\chi_{a,b}})$ for even n, and $(x, y) = (F_n, \sqrt{5F_n^2 + 4\chi_{a,b}})$ for odd n. This is a consequence of the following generalized Cassini identity. By the definition of F_n, we have

$$\begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

and hence inductively one has

$$\begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} a+b & b \\ b & a \end{pmatrix}.$$

Taking the determinants of both sides gives the generalized Cassini identity:

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^n (a^2 + ab - b^2).$$

Substituting $F_{n+2} = F_n + F_{n+1}$ into the equation, we have the quadratic equation in F_{n+1}

$$F_n^2 + F_n F_{n+1} - F_{n+1}^2 = (-1)^n \chi_{a,b},$$

and hence

$$F_{n+1} = \frac{F_n \pm \sqrt{5F_n^2 + (-1)^{n+1} 4\chi_{a,b}}}{2}.$$

[2]Since then considerably better bounds have been found.

It follows that $5F_n^2+4(-1)^{n+1}\chi_{a,b}=y^2$ for some $y\in\mathbb{Z}$, proving the claim.

Hence, to prove the theorem it suffices to show that if one of the equations

$$y^2=5g(x)^2+4\chi, \quad \text{with } \chi=\chi_{a,b} \text{ or } -\chi_{a,b}, \tag{4}$$

has infinitely many solutions $(x, y)\in\mathbb{Z}^2$, then $g(x)=\alpha_{\chi,d,m}D_{d,m}(\mu(x))$ for some linear $\mu\in\mathbb{Q}[x]$ and some $m\in\mathbb{Z}$, with $d=\deg g$. Without loss of generality assume the equation with $\chi=\chi_{a,b}$ has infinitely many solutions.

Set $f(x):=5g(x)^2+4\chi$, $d:=\deg(g)$, and write $f(x)=\alpha\prod_{i=1}^{u}(x-x_i)^{r_i}\in\mathbb{C}[x]$. As $\deg f\geq 4$, if $y^2=f(x)$ has infinitely many solutions $(x, y)\in\mathbb{Z}^2$, then Theorem 5 implies that at most two of the r_i are odd.

The case where exactly one of the r_i is odd, contradicts $\deg f=2d$ is even. In the case all r_i are even, $f(x)=h(x)^2$ for some $h\in\mathbb{C}[x]$. As $\chi\neq 0$, we have

$$\deg(f-g^2)=\deg(h^2-5g^2)=\deg(h-\sqrt{5}g)+\deg(h+\sqrt{5}g)=0,$$

and so $\deg(h\pm\sqrt{5}g)=0$. This shows that g is constant contradicting $d>1$.

If exactly two of the r_i are odd, say r_1, r_2, we have the decomposition

$$\left(g(x)-2\sqrt{-\frac{\chi}{5}}\right)\left(g(x)+2\sqrt{-\frac{\chi}{5}}\right)=\frac{f(x)}{5}=(x-x_1)(x-x_2)R(x)^2$$

for $R(x)\in\mathbb{C}[x]$, and hence Lemma 2 with $a_1=-a_2=2\sqrt{-\chi/5}$ implies

$$g(x)=\pm\sqrt{-\frac{\chi}{5}}T_d(\ell_2(x))$$

for some linear $\ell_2\in\mathbb{C}[x]$.

Corollary 4 then implies $\ell_2(x)=(1/\sqrt{m})\mu(x)$ for some $\mu\in\mathbb{Q}[x]$, and $m\in\mathbb{Z}\backslash\{0\}$. Furthermore, it shows

$$g(x)=\pm\sqrt{-\frac{\chi}{5m^d}}D_{d,m}(\mu(x))$$

with

$$\alpha_{\chi,d,m}=\pm\sqrt{-\frac{\chi}{5m^d}}\in\mathbb{Q}.$$

Finally, to see that $g(x)=x^2$ is never of the above form, note that 0 is a branch point of $g(x)$, that is, the value of g at a root of $g'(x)$. On the other hand, 0 is never a branch point of $\alpha_{\chi,2,m}D_{2,m}(x)$. □

Remark 6. (1) The proof shows that if $g(\mathbb{Z})\cap F^{a,b}$ is infinite and $d=\deg g$ is even, then $\chi=\chi_{a,b}<0$. Together with the above observation that $F_n\in g(\mathbb{Z})$ gives a solution to (4) with $\chi=\chi_{a,b}$ for odd n, and with $\chi=-\chi_{a,b}$ for even n, this shows that $F^{a,b}$ intersects $g(\mathbb{Z})$ infinitely often at only one residue class of n mod 2.

(2) In the case $g(\mathbb{Z})\cap F^{a,b}$ is finite, Theorem 1 is effective, that is, gives an (exponential) bound on the largest value of n for which $F_n\in g(\mathbb{Z})$, in terms of the coefficients of g and $\chi_{a,b}$. Indeed, since the coefficients of f are bounded in

terms of the coefficients of g and $\chi_{a,b}$, and since Siegel's theorem is applied to the hyperelliptic curve $y^2 = f(x)$ in the case $f(x)$ has at least three roots with odd multiplicity, Baker's theorem gives the desired bound as described in Section 2.2.

(3) Finally the proof extends to the recurrence relations $G_{n+2} = \pm G_n + BG_{n+1}$ for rings of integers $R = O_K$ of number fields K, and $B \in R$. The main modification is replacing 5 by $B^2 + 4u$.

Theorem 7. *Let $R = O_K$ be the ring of integers of a number field K and $G^{a,b}$, $a, b \in R$, be the sequence given by $G_0 = a$, $G_1 = b$, and $G_{n+2} = uG_n + BG_{n+1}$ for $u \in \{1, -1\}$, and $B \in R$. Assume $B^2 + 4u \notin R^2$, and set $\chi_G := ua^2 + Bab - b^2$. Let $g(x) \in K[x]$ be a polynomial of degree $d > 1$ different from $\pm\alpha_{\chi,d,m} D_{d,m}(\mu(x))$ for all linear $\mu(x) \in K[x]$, $m \in R$ and*

$$\alpha_{\chi,d,m} = \sqrt{-\frac{\chi \cdot m^d}{B^2 + 4u}},$$

where $\chi = -\chi_G$ if $u = -1$ and $\chi \in \{\chi_G, -\chi_G\}$ if $u = 1$. Then $\#(g(R) \cap G^{a,b}) < \infty$.

Proof. First note that $\chi_G \neq 0$ since

$$b \neq \frac{B \pm \sqrt{B^2 + 4u}}{2} \cdot a,$$

as $B^2 + 4u \notin R^2$.

We adjust the relevant parts from the proof of the main theorem. In the generalized Cassini identity, we have the equation

$$\begin{pmatrix} G_{n+2} & G_{n+1} \\ G_{n+1} & G_n \end{pmatrix} = \begin{pmatrix} B & u \\ 1 & 0 \end{pmatrix} \begin{pmatrix} G_{n+1} & G_n \\ G_n & G_{n-1} \end{pmatrix}$$

and by induction

$$\begin{pmatrix} G_{n+2} & G_{n+1} \\ G_{n+1} & G_n \end{pmatrix} = \begin{pmatrix} B & u \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} Bb+ua & b \\ b & a \end{pmatrix}.$$

Thus, by taking determinants we find that

$$G_{n+2}G_n - G_{n+1}^2 = (-u)^n (ua^2 + Bab - b^2).$$

Setting $\chi_G = ua^2 + Bab - b^2$, we get the equation

$$uG_n^2 + BG_n G_{n+1} - G_{n+1}^2 = (-u)^n \chi_G,$$

and hence

$$G_{n+1} = \frac{BG_n \pm \sqrt{B^2 G_n^2 + 4uG_n^2 - 4(-u)^n \chi_G}}{2}.$$

Thus $(B^2+4u)G_n^2 - 4(-u)^n\chi_G = y^2,\ y \in R$, yielding the analogous equation to (4):

$$y^2 = f(x) = (B^2+4u)g(x)^2 + 4\chi,$$

where $\chi = -\chi_G$ when $u = -1$ and it takes two possible values $\chi \in \{\chi_G, -\chi_G\}$ when $u = 1$. Similarly to the proof of Theorem 1, an application of Theorem 5 shows that there are finitely many solutions in O_K to the equation $y^2 = f(x)$ if $f(x)$ has at least three roots of odd multiplicity. Again, it cannot have a single root of odd multiplicity since f is of even degree, and $f(x)$ cannot be a square since then $f(x) - (\sqrt{B^2+4u}\,g(x))^2 = 4\chi \neq 0$ is a nonzero constant difference of squares in $\mathbb{C}[x] \setminus \mathbb{C}$. Thus

$$f(x) = (x-x_1)(x-x_2)R^2(x)$$

for distinct $x_1, x_2 \in \mathbb{C}$ and $R(x) \in \mathbb{C}[x]$. Lemma 2 applied to the decomposition

$$\left(g(x) - 2\sqrt{-\frac{\chi}{B^2+4u}}\right)\left(g(x) + 2\sqrt{-\frac{\chi}{B^2+4u}}\right) = \frac{f(x)}{B^2+4u},$$

gives

$$g(x) = \pm\sqrt{-\frac{\chi}{B^2+4u}}\,T_d(\ell_2(x)).$$

The result now follows from Corollary 4. □

Acknowledgements

The authors thank the Mentoring Program of the Szold Institute for the opportunity it gave Elrazik and Ostrov in entering academic research. We thank Umberto Zannier, and Michael Zieve, and the referees for helpful comments. This paper originated as a project of Ostrov as part of the program, advised by Berman and Neftin, with the help of Elrazik. Ostrov was supported by the Israel Science Foundation (grant no. 662/15), and Neftin by the Binational Science Foundation (grant no. 2014173).

References

[Baker 1969] A. Baker, "Bounds for the solutions of the hyperelliptic equation", *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444. MR Zbl

[Bugeaud et al. 2006] Y. Bugeaud, M. Mignotte, and S. Siksek, "Classical and modular approaches to exponential Diophantine equations, I: Fibonacci and Lucas perfect powers", *Ann. of Math.* (2) **163**:3 (2006), 969–1018. MR Zbl

[Cohn 1964] J. H. E. Cohn, "Square Fibonacci numbers, etc", *Fibonacci Quart.* **2**:2 (1964), 109–113. MR Zbl

[Corvaja and Zannier 1998] P. Corvaja and U. Zannier, "Diophantine equations with power sums and universal Hilbert sets", *Indag. Math. (N.S.)* **9**:3 (1998), 317–332. MR Zbl

[LeVeque 1964] W. J. LeVeque, "On the equation $y^m = f(x)$", *Acta Arith.* **9** (1964), 209–219. MR Zbl

[Lidl et al. 1993] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific & Technical, Harlow, 1993. MR Zbl

[Nagy et al. 2019] M. Nagy, S. R. Cowell, and V. Beiu, "Survey of cubic Fibonacci identities — when cuboids carry weight", preprint, 2019. arXiv

[Schinzel 2000] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge University Press, 2000. MR Zbl

[Zieve and Mueller 2008] M. E. Zieve and P. Mueller, "On Ritt's polynomial decomposition theorems", preprint, 2008. arXiv

Received: 2019-12-14 Revised: 2020-04-21 Accepted: 2020-07-26

phzheveuubyhy@gmail.com *Department of Mathematics, Technion – Israel Institute of Technology, Haifa, Israel*

dneftin@technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, Haifa, Israel*

berman@technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, Haifa, Israel*

reyad@campus.technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, Haifa, Israel*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US $205/year for the electronic version, and $275/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2020 vol. 13 no. 4