POLYNOMIAL VALUES IN FIBONACCI SEQUENCES

ADI OSTROV, DANNY NEFTIN, AVI BERMAN, AND REYAD A. ELRAZIK

Abstract. 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 is always 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 [4]. Subsequently, much work was devoted to studying perfect powers in the Fibonacci and Lucas sequences, leading to their determination in [3, §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. Let $D_{d,m}$ denote the normalized degree d Dickson polynomial, cf. Remark 4. 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 $m \in \mathbb{Z}$, where $\alpha_{\chi,d,m} = \pm\sqrt{-\frac{\chi}{5m^d}}$, for $\chi = \chi_{a,b}$ or $-\chi_{a,b}$. Then $F^{a,b}$ contains only finitely many values from $g(\mathbb{Z})$, that is, $\#\big(g(\mathbb{Z}) \cap F^{a,b}\big) < \infty$. In particular, $F^{a,b}$ contains only finitely many perfect squares.

Date: December 14, 2019.

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, $\chi_{b,a+b} = -\chi_{a,b}$.

Recall that $D_{d,1}$ is the normalized Chebyshev polynomial T_d. 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 $|\chi_{2,1}| = 5$, 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 $i = \sqrt{-1}$, and the Fibonacci sequence, which has $|\chi_{0,1}| = 1$, has infinite intersection with $g(\mathbb{Z})$, for $g(x) = \frac{1}{\sqrt{5}}T_3(\sqrt{5}x) = 5x^3 - 3x$ and $g(x) = -\frac{1}{\sqrt{-5}}T_3(\sqrt{-5}x) = 5x^3 + 3x$. Also note that in all examples the values $\{n \,|\, F_n \in g(\mathbb{Z})\}$ appear in arithmetic progressions, as Corvaja–Zannier [7, Theorem 2] show. Finally, we note that the proof of the theorem is effective, generalizes to number fields and to other recurrence sequences, see Remark 5.

The authors thank the "Mentoring" program of the Szold Institute for the opportunity it gave the first and fourth authors in entering academic research. We thank Umberto Zannier and Michael Zieve for helpful comments on the manuscript and literature. This paper originates in a project of the first author as part of the program, advised by the second and third authors, with the help of the fourth author. The first author was supported by the Israel Science Foundation (grant no. 662/15), and the second by the Binational Science Foundation (grant no. 2014173).

2. Preliminaries

2.1. **Chebyshev and Dickson polynomials.** Let $T_d \in \mathbb{Z}[x]$ denote the normalized Chebyshev polynomial, that is, the unique degree d polynomial which satisfies

$$T_d(x + \frac{1}{x}) = x^d + \frac{1}{x^d}.$$

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 [12, §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

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

Similar results to the following lemma are well known in particular cases, including $p(x) = T_d(x)$ [10, Lemma 6.15]. Since the proof appears to be new, we give it here:

Lemma 3. Let $\varepsilon \in \mathbb{C} \setminus \{0\}$, and $\mu(x) \in \mathbb{C}[x] \setminus \mathbb{Q}[x]$ with $\deg \mu = 1$. Suppose $p(x) \in \mathbb{Q}[x]$ has real roots, such that the minimal root r is different from the maximal one R. If $\varepsilon p(\mu(x)) \in \mathbb{Q}[x]$, then $R + r \in \mathbb{Q}$ and $\mu(x) = \sqrt{m}\mu'(x) + (R+r)/2$ for $\mu'(x) \in \mathbb{Q}[x]$, and $m \in \mathbb{Q}^\times$. Furthermore, $\varepsilon \in \sqrt{m} \cdot \mathbb{Q}$ if $p(x - (R+r)/2)$ is an odd polynomial, and $\varepsilon \in \mathbb{Q}$ otherwise.

Proof. Let A be the set of roots of $p(x)$. Notice that $\mu^{-1}(A)$ is the set of zeros of $g(x) := \varepsilon p(\mu(x)) \in \mathbb{Q}[x]$. Since $p(x), g(x) \in \mathbb{Q}[x]$ both A and $\mu^{-1}(A)$ are invariant under every field 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 $\big(\mu^{-1}(R), \mu^{-1}(r)\big) = \big(\sigma(\mu^{-1})(R), \sigma(\mu^{-1})(r)\big)$ or $\big(\mu^{-1}(R), \mu^{-1}(r)\big) = \big(\sigma(\mu^{-1})(r), \sigma(\mu^{-1})(R)\big)$. In the former case:

$$\begin{aligned} R\gamma + \delta &= R\sigma(\gamma) + \sigma(\delta) \\ r\gamma + \delta &= r\sigma(\gamma) + \sigma(\delta), \end{aligned} \tag{1}$$

while in the latter, the ends flip:

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

Since $R \neq r$, for σ in case (1), we have $\sigma(\delta) = \delta$ and $\sigma(\gamma) = \gamma$. For σ in case (2), σ flips the ends, and hence σ^2 fixes them, so that σ^2 is in case (1), that is $\sigma^2(\delta) = \delta$. Moreover, taking the difference of the two equations in (2) gives $\sigma(\gamma) = -\gamma$. Since $\sigma(\gamma) = \pm\gamma$ for every automorphism σ, we have $\gamma = \sqrt{m}$ for $m \in \mathbb{Q}$. Plugging this into (2) gives $(R+r)\sqrt{m} = \sigma(\delta) - \delta$.

Since (1) and (2) imply that every automorphism that fixes $\gamma = \sqrt{m}$ also fixes δ, we have $\delta = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$. If $R = -r$, for σ as in (2) we also have $\sigma(\delta) = \delta$, and hence $\delta \in \mathbb{Q}$. Otherwise, case (2) gives $(R+r)\gamma = 2b\gamma$, and hence $b = \frac{R+r}{2} \in \mathbb{Q}$ and $\mu^{-1}(x) = \sqrt{m}(x + \frac{R+r}{2}) + a$ for $a \in \mathbb{Q}$. Thus $\mu(x) = \frac{1}{\sqrt{m}}(x-a) - \frac{R+r}{2}$. Note that since μ is assumed not to be rational, case (2) holds for some σ and hence $R + r \in \mathbb{Q}$.

Write $q(x) := p(x - \frac{R+r}{2}) \in \mathbb{Q}[x]$, and $\mu(x) + \frac{R+r}{2} = \sqrt{m}\mu'(x)$ for a linear $\mu' \in \mathbb{Q}[x]$, so that $\varepsilon p(\mu(x)) = \varepsilon q(\sqrt{m}\mu'(x))$ and hence $\varepsilon q(\sqrt{m}x)$ are in $\mathbb{Q}[x]$. If q is odd, then $q(\sqrt{m}x) = \sqrt{m}q'(x)$ where $q'(x) \in \mathbb{Q}[x]$, thus $\varepsilon \cdot \sqrt{m} \in \mathbb{Q}$. Otherwise, q has at least one nonzero monomial of even degree, say $\varepsilon q_{2k} m^k x^{2k} \in \mathbb{Q} \cdot x^{2k}$ with $q_{2k} \in \mathbb{Q} \setminus \{0\}$, so that $\varepsilon \in \mathbb{Q}$. □

Remark 4. Applying the above lemma with $p = T_d$ shows that the only polynomials $\varepsilon T_d(\mu(x)) \in \mathbb{Q}[x]$ with linear μ are the Dickson polynomials $D_{d,m}(x) \in \mathbb{Q}[x]$ which

satisfy $D_{d,m}(x) = m^{d/2}T_d(x/\sqrt{m})$. For $x \neq 0$, one then has:

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

2.2. **Effective Siegel.** We shall also use Siegel's theorem for the special case of hyperelliptic curves. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree ≥ 3 which factors as $f(x) = a\prod_{i=1}^{s}(x-\alpha_i)^{r_i}$ for distinct $\alpha_i \in \overline{\mathbb{Q}}$, for $a \in \mathbb{Q}$, and for integers $r_i \geq 1$. Then [9] and [11] show that if the equation $y^2 = f(x)$ has infinitely many integral solutions then at most two of the r_i's are odd.

In the case of hyperelliptic curves, effective versions of the theorem were given using Baker's method, see [1], [2] and references therein. These bound the solutions to $y^2 = f(x)$ in terms of the coefficients of f.

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

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

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 follows from the following generalized Cassini identity. By 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 following quadratic equation in F_{n+1}:

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

and hence:

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

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

$$y^2 = 5g(x)^2 + 4\chi \text{ with } \chi = \chi_{a,b} \text{ or } -\chi_{a,b} \tag{3}$$

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 Siegel's theorem (§2.2) implies that at most two of the r_i's are odd.

The case where exactly one of the r_i's is odd, contradicts $\deg f = 2d$ is even. In case all r_i's are even, $f(x) = h(x)^2$ for some $h \in \mathbb{C}[x]$. As $\chi \neq 0$, we have that $\deg(f - g^2) = \deg(h^2 - 5g^2) = \deg(h - \sqrt{5}g) + \deg(h + \sqrt{5}g) = 0$, 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's are odd, say r_1, r_2, we have the decomposition

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

for $R(x) \in \mathbb{C}[x]$, and hence Lemma 2 with $a_1 = -a_2 = 2\sqrt{-\frac{\chi}{5}}$ implies that $g(x) = \pm\sqrt{-\frac{\chi}{5}} T_d(\ell_2(x))$ for some linear $\ell_2 \in \mathbb{C}[x]$.

Lemma 3 and Remark 4 then imply that $\ell_2(x) = (1/\sqrt{m})\mu(x)$ for some $\mu \in \mathbb{Q}[x]$, and $m \in \mathbb{Z} \setminus \{0\}$. Furthermore, they show

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

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 which 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 5. (a) Note that 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 (3) 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.
(b) Another approach to proving Theorem 1 is using [6, Theorem 2], which relies on the Subspace Theorem, rather than on Siegel's theorem.
(c) In case $g(\mathbb{Z}) \cap F^{a,b}$ is infinite, note that the coefficients of f are bounded in terms of the coefficients of g and $\chi_{a,b}$. Since Siegel's theorem for hyperelliptic curves is

known to be effective, see Section 2.2, the theorem gives an (exponential) bound on the largest value of n for which $F_n \in g(\mathbb{Z})$.
(d) Finally note that the proof extends to the following recurrence relations $G_{n+2} = \pm G_n + BG_{n+1}$ and rings R. The main modification is replacing "5" by "B^2+4u".

Theorem 6. 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 $u \in \{\pm 1\}$. 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 $\alpha_{\chi,d,m} D_{d,m}(\mu(x))$ for all linear $\mu(x) \in \mathbb{Q}[x]$, $m \in \mathbb{Z}$ and $\alpha_{\chi,d,m} = \pm\sqrt{-\frac{\chi}{(B^2+4u)m^d}}$, where $\chi = -\chi_G$ if $u = -1$ and $\chi = \pm\chi_G$ 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 following 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

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

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

$$uG_n^2 + BG_nG_{n+1} - G_{n+1}^2 = (-u)^n\chi_G, \text{ and hence}$$

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

Thus $(B^2 + 4u)G_n^2 - 4(-u)^n\chi_G = y^2$, $y \in \mathbb{Z}$, yielding the analogous equation to (3):

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

where this time $\chi = \pm\chi_G$ when $u = 1$ and $\chi = -\chi_G$ when $u = -1$. Applying Lemma 3 to the decomposition

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

gives $g(x) = \pm\sqrt{-\frac{\chi}{B^2+4u}}T_d(\ell_2(x))$. The result then follows once again from Lemma 3 and Remark 4. □

References

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation. Proc. Camb. Phil. Soc. 65 (1969), 439–444.

[2] A. Bérczes; J.-H. Evertse, K. Győry, Effective results for hyper- and superelliptic equations over number fields. Publ. Math. Debrecen 82 (2013), 727–756.

[3] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential diophantine equations I. Fibonnaci and Lucas perfect powers. Annals of Mathematics 163 (2006), 969–1018.

[4] J. H. E. Cohn, Square Fibonacci Numbers, Etc. Fibonacci Quarterly 2 (1964), 109–113.

[5] P. Corvaja, U. Zannier, S-Unit points on analytic hypersurfaces. Ann. Scient. Éc. Norm. Sup. (2005), 76–92.

[6] P. Corvaja, U. Zannier, Some new applications of the subspace theorem. Compositio Mathematica 131 (2002), 319–340.

[7] P. Corvaja, U. Zannier, Diophantine equations with power sums and Universal Hilbert Sets. Indag. Mathem., N.S., 9 (3). 317–332.

[8] S. Lang, Fundamentals of Diophantine Geometry. Springer–Verlag, New York (1983).

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

[10] R. Lidl, G. L. Mullen, G. Turnwald, Dickson Polynomials. Monographs and Surveys in Pure and Applied Mathematics 65.

[11] J.-H. Evertse, J. H. Silverman, Uniform bounds for the number of solutions to $Y^n = f(X)$. Mathematical Proceedings of the Cambridge Philosophical Society 100 (1986), 237–248.

[12] A. Schinzel, Polynomials with special regard to reducibility. Cambridge University Press (2000).

Department of Mathematics, Technion - IIT, Israel