

Polynomial values in linear recurrences

I. NEMES and A. PETHŐ (Debrecen)

1. Introduction

Let $A_1, \dots, A_k$ and $G_0, G_1, \dots, G_{k-1}$ be integers. We have for the n -th term of a k -order linear recurrence

$$(1) \quad G_n = A_1 G_{n-1} + \dots + A_k G_{n-k} \quad \text{for } n = k, k+1, \dots$$

Let $\alpha_1, \dots, \alpha_t$ be the distinct roots of the characteristic polynomial of the recurrence

$$(2) \quad X^k - A_1 X^{k-1} - \dots - A_k.$$

Throughout this paper we assume that α_1 has multiplicity one. Then for $n \geq 0$ we have

$$(3) \quad G_n = E_1 \alpha_1^n + P_2(n) \alpha_2^n + \dots + P_t(n) \alpha_t^n,$$

where $P_i(n)$ is a polynomial with degree less than the multiplicity of α_i in the characteristic polynomial of G_n , and where E_1 and the coefficients of $P_i(n)$ are elements of the field $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$.

Finally let $T(x) = B_m x^m + \dots + B_0$ be a polynomial with integer coefficients. Its degree will be denoted by $\deg T$, while its height, $\max \{|B_i|; i=0, \dots, m\}$ by $\mathcal{H}(T)$.

The Diophantine equation

$$(4) \quad G_n = E x^q + T(x) E \neq 0, \quad \text{integer}$$

was investigated by several authors. Naturally, most of the results are known for $T(x) = 0$.

SHOREY and STEWART [4] proved for general linear recurrences that (4) has finitely many solutions in q , assuming $|\alpha_1| > |\alpha_j|$, $j=2, \dots, t$. Under some other restriction on G_n , recently P. KISS [2] was able to generalize their result when $\deg T < c_1 q$.

For nondegenerate second order linear recurrences SHOREY and STEWART [4] derived much more, namely (4) has finitely many solutions in integers $|x| > 1$, $q \geq 2$, n . The second author investigated in [3] for nondegenerate second order linear recurrences the slightly more general equation

$$(5) \quad G_n = w x^q$$

with $w \in S$, where S is the set of nonzero integers composed solely of primes from some fixed finite set. He showed assuming yet $(A_1, A_2) = 1$ that (5) has finitely many solutions in integers $|x| > 1$, $q \geq 2$, n and $w \in S$.

STEWART [7] was dealing with the case $T(x) = c$, where c is a fixed integer. For nondegenerate second order recurrences with $|A_2| = 1$ he proved the finiteness of the solution in integers $|x| > 1$, $q > 2$, c, n of (4).

All the above mentioned results are effective.

In the present paper we shall derive some results for (4), when $T(x)$ is a polynomial with some restriction.

2. Main results

Theorem 1. Let G_n satisfy (3), $\alpha_1, \alpha_2 \neq 1$, $|\alpha_1| > |\alpha_2| > |\alpha_j|$, $j = 3, \dots, t$ and $G_n - E_1 \alpha_1^n \neq 0$ for $n > c_2$. Further let $\mathcal{H}(T) < H_1$ and $\deg T \leq qc_3$, where $H_1 > 0$ real number. Then all integer solutions $n, |x| > 1$, $q \geq 2$ of the equation (4) satisfy $q < c_4$, where c_2, c_3 and c_4 are effectively computable constants depending on E, G_n and H_1 .

For second order linear recurrences we prove a more precise result.

Theorem 2. Let G_n be a nondegenerate second order linear recurrence with $|A_2| = 1$. Further let $\mathcal{H}(T) < H_2$ and $\deg T \leq \min \{q(1-\gamma), q-3\}$ where H_2 and $\gamma < 1$ are positive real numbers. Then all integer solutions $n, |x| > 1$, $q \geq 2$ of (4) satisfy

$$\max \{n, |x|, q\} < c_5,$$

where c_5 is an effectively computable constant depending on E, G_n, γ and H_2 .

Remark. Theorem 2 is in the restriction of $\deg T$ best possible. Let L_n denote a Lucas sequence, i.e. $L_0 = 2$, $L_1 = \alpha + \beta$ and $L_n = (\alpha + \beta)L_{n-1} + L_{n-2}$, where $\alpha\beta = -1$ and $\alpha + \beta$ integer. Then, as is well known, $L_n = \alpha^n + \beta^n$. Further it is easy to see that $L_{2n} = L_n^2 + (-1)^n 2$. This means that both equations $L_n = x^2 + 2$ and $L_n = x^2 - 2$ have infinitely many integer solutions n, x . Therefore in Theorem 2 the assumption $\deg T \leq q - 3$ is necessary.

3. Auxiliary results

The most important result we use is Lemma 6 of [4].

Lemma. Let α be a real algebraic number larger than one from the field k . Let $[K:Q] = D$, E, A and B be elements of K , $EAB \neq 0$, finally δ a positive real number. If $Ex^q = A\alpha^n + B$ with $|B| < \alpha^{n(1-\delta)}$ and n, x, q integers larger than one then $q < c_6$ is a constant, effectively computable in terms of D, E, A, α and δ .

The following theorem was proved by C. L. SIEGEL [5] for the first time but in noneffective form. Using the upper estimate for linear forms of logarithms of algebraic numbers A. BAKER [1] proved it in effective form.

Theorem A. Let $F(x)$ be a monic polynomial of degree n and with integer coefficients. Let it have at least three simple zeros. Then the integer solutions x, y of the equation $Ay^2 = F(x)$ where A is an integer, satisfy $\max\{|x|, |y|\} < c_7$ a constant effectively computable in terms of A and the coefficients of $F(x)$.

4. Proofs

In the sequel $c_8, c_9, \dots$ will denote positive numbers effectively computable in terms of E, G_n, H_i and γ .

PROOF OF THEOREM 1. We may assume α_1 to be positive by changing if necessary the sign of E_1 . Further since α_1 is an algebraic integer with absolute value strictly larger than all its conjugates, on taking norm we see that either $\alpha_1 > 1$ or α_1 is one of 0 or 1. But these two cases were excluded so we may assume $\alpha_1 > 1$. Put

$$B_1(n) = P_2(n)\alpha_2^n + \dots + P_t(n)\alpha_t^n$$

$$D_1 = \max\{\deg P_i(n); i = 2, \dots, t\}.$$

It is easy to show that

$$(6) \quad 2|B_1| < c_8 n^{D_1} |\alpha_2|^n.$$

Assume that for a polynomial $T(x)$ with $\mathcal{H}(T) \leq H_1$ and $\deg T < qc_3$, $n, |x| > 1$, q is a solution of (4). We shall give an estimate for c_3 in the proof.

Write (4) in the form

$$Ex^q = E_1\alpha_1^n + B_1(n) - T(x).$$

Assume first that

$$(7) \quad B_1(n) - T(x) = 0$$

in which case

$$(8) \quad E_1\alpha_1^n = Ex^q$$

also holds. We distinguish two cases.

If $1 > |\alpha_2| \cong |\alpha_j|$, $j = 3, \dots, t$, then $\lim_{n \rightarrow \infty} B_1(n) = 0$ which means $|B_1(n)| < 1$ for $n > c_8$. Further $T(x)$ is a polynomial with integer coefficients, therefore (7) has for $n > c_8$ no solutions. By (8) $q = c_9 \frac{n}{\log |x|} < c_{10}$ because of $|x| \geq 2$.

If $|\alpha_2| > 1$, then write

$$B_1(n) = P_2(n)\alpha_2^n \left(1 + \sum_{i=3}^t \frac{P_i(n)}{P_2(n)} \left(\frac{\alpha_i}{\alpha_2}\right)^n\right).$$

The quantity in the brackets tends to 1 if n tends to infinity, so for $n > c_{11}$ $|B_1(n)| > |P_2(n)| |\alpha_2|^n (1 - \varepsilon') > |\alpha_2|^{n(1-\varepsilon)}$. On the other hand $T(x) \leq m H_1 |x|^m$. From (8) we have $|x| = (|E_1/E| |\alpha_1|^n)^{1/q}$, hence $|T(x)| \leq c_{12} m |\alpha_1|^{nm/q} < |\alpha_1|^{c_{13}nm/q}$. By (7) $|\alpha_2|^{n(1-\varepsilon)} < |B_1(n)| = |T(x)| < |\alpha_1|^{c_{13}nm/q}$. This implies $m > c_{14} \frac{\log |\alpha_2|}{\log |\alpha_1|} q$. Therefore

if $c_3 \leq c_{13} \frac{\log |\alpha_2|}{\log |\alpha_1|}$ then (7) and (8) have only finitely many solutions in $n, q, |x| > 1$ which are effectively computable.

In the sequel we assume that $B_1(n) - T(x) \neq 0$. Put $\delta = (1 - \vartheta)/2$, where $\vartheta = 0$ if $\alpha_2 \leq 1$, and $\vartheta = \frac{\log |\alpha_2|}{\log |\alpha_1|}$ otherwise. Since $\alpha_1 > 1$ we have by (6) $|B_1| < \frac{1}{2} \alpha_1^{n(1-\delta)}$ for $n > c_{14}$. We choose c_{15} such that $|E||x|^{c_{15}} > 2E_1 + 1$. If q is large enough then $\frac{|T(x)|}{|x|^{q-c_{15}}} < 1$. Write (4) in the form

$$Ex^{c_{15}} = \frac{E_1 \alpha_1^n + B_1(n)}{x^{q-c_{15}}} - \frac{T(x)}{x^{q-c_{15}}}.$$

Taking absolute values, and applying the above estimates we have

$$2|E_1| + 1 < |Ex^{c_{15}}| \leq \left| \frac{E_1 \alpha_1^n + B_1(n)}{x^{q-c_{15}}} \right| + 1.$$

Hence $2|E_1||x|^{q-c_{15}} \leq |E_1 \alpha_1^n + B_1(n)| \leq 2|E_1| \alpha_1^n$, so $|x|^{q-c_{15}} < \alpha_1^n$. Further $|T(x)| \leq m H_1 |x|^m < |x|^{c_{16}q}$, with $c_{16} < 1$. Hence $|T(x)| < \alpha_1^{c_{16}qn/(q-c_{15})} < \frac{1}{2} \alpha_1^{n(1-\delta)}$ when δ is small enough. So we have $|B_1(n) + T(x)| \leq \alpha_1^{n(1-\delta)}$.

Note that if $n < c_{17}$ and (4) holds then $q < c_{18}$ as required. Of course since

$$|x|^m (Ex^{q-m} - mH_1) \leq |E||x|^q - |T(x)| \leq |Ex^q + T(x)| = |G_n| \leq c_{19} \alpha_1^n$$

the required inequality for q holds.

Finally by the Lemma if $n > c_{20}$ and (4) holds then $q < c_1$ as was stated.

PROOF OF THEOREM 2. The assumption $|A_2| = 1$ means $|\alpha_1 \alpha_2| = 1$. We show that α_1 and α_2 are real numbers. Of course if one of them had a nonzero imaginary part then $|\alpha_1| = |\alpha_2|$ would hold since they are roots of a polynomial with integer coefficients. This imply $|\alpha_1| = |\alpha_2| = 1$.

But α_1/α_2 cannot be a root of unity by nondegeneracy. Thus α_1, α_2 are real numbers and $|\alpha_1| > 1 > |\alpha_2|$ holds since $|\alpha_1 \alpha_2| = 1$. Further the equation $A_2 \alpha_2^n = T(x)$ has only finitely many solutions, since with n large enough $0 < |T(x)| = |A_2 \alpha_2^n| < 1$. Therefore $n < c_{21}$, which implies $q, |x| < c_{22}$.

In the sequel we assume $A_2 \alpha_2^n \neq T(x)$. Now we shall prove $q < c_{23}$. Assume that (4) has a solution $n, q, |x| > 1$ such that $q \geq c_{23}$, with $\frac{\log q H_2}{q \log 2} < \frac{\gamma}{2}$, and $q \frac{\gamma}{4} > 1 + \frac{\gamma}{4}$. Then

$$|T(x)| < m H_2 |x|^m < |x|^{m + \frac{\log H_2 m}{\log 2}} < |x|^{q(1-\gamma) + \frac{\log q H_2}{\log 2}}.$$

Applying the assumption we have

$$q(1-\gamma) + \frac{\log q H_2}{\log 2} < q(1-\gamma) + q \frac{\gamma}{2} = q \left(1 - \frac{\gamma}{2}\right) < q - 1.$$

Hence $\frac{|T(x)|}{|x|^{q-1}} < 1$. From this follows as in the proof of Theorem 1 $|x|^{q-1} < \alpha_1^n$,

and $|T(x)| < \alpha_1^{(1-\delta)}$ with $\delta = \frac{\gamma}{4}$. Finally it is obvious that $P_2(n)|\alpha_2|^n < \alpha_1^{n(1-\delta)}$.

Now applying the Lemma we conclude that q is bounded by an effectively computable constant.

Now let q and $T(x)$ be fixed with $\deg T < q(1-\gamma)$ and consider the equation

$$G_n = Ex^q + T(x) = T_1(x).$$

It is well known that $G_{n+1}^2 - A_1 G_{n+1} G_n + A_2 G_n^2 = C A_n^2$, with $C = G_1^2 - A_1 G_1 G_0 + A_2 G_0^2$ (see for example [3] Lemma 1). From this follows $DG_n^2 + 4CA_n^2 = z^2$, with $D = A_1^2 - 4A_2 \neq 0$ and z an integer. Replacing G_n by $Ex^q + T(x)$, and taking $|A_2| = 1$ into account we have

$$R(x) = D(Ex^q + T(x))^2 \pm 4C = DT_1^2(x) \pm 4C = z^2.$$

This is an elliptic equation, and by means of Theorem A it has finitely many solutions in x, z when $R(x)$ has at least three simple zeros. Let $(R(x), R'(x)) = Q(x)$. It is well known that a root ω of $R(x)$ has multiplicity at least two if and only if ω is a root of $Q(x)$. Further $(R(x), T_1(x)) = 1$ because of $c \neq 0$, and $R'(x) = 2D T_1(x) T_1'(x)$ so $\deg Q(x) \leq q-1$. This means that if either $\deg Q(x) < q-1$ or it has at least one multiple root then $R(x)$ has at least three simple zeros and we are ready.

Hence the only wrong case is when $Q(x) = T_1'(x)$, and $R(x) = T_1'(x)^2 S(x)$ with a polynomial $S(x)$ with rational coefficients of degree two with not any multiple roots. Let $S(x) = s_2 x^2 + s_1 x + s_0$ and consider the equation

$$D(Ex^q + T(x))^2 \pm 4C = (2qEx^{q-1} + T'(x))^2 (s_2 x^2 + s_1 x + s_0).$$

The coefficient of x^{2q-1} and that of x^{2q-2} on the left hand side is 0, because of $\deg T(x) < q-3$, while the coefficient of x^{2q-1} on the right hand side is $4q^2 E^2 s_1$, and that of x^{2q-2} is $4q^2 E^2 s_0$. This means $s_1 = s_0 = 0$, and $S(x) = s_2 x^2$ which is a contradiction.

References

- [1] A. BAKER, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439–444.
- [2] P. KISS, Differences of the Terms of Linear Recurrences, *to appear*.
- [3] A. PETHŐ, Perfect Powers in Second Order Linear Recurrences, *Journal of Number Theory* **15** (1982), 5–13.
- [4] T. N. SHOREY, C. L. STEWART, On the Diophantine equation $ax^{2t} + bx_t y + cy^2 = d$ and pure powers in recurrences sequences *Math. Scand.* **52** (1983), 24–36.
- [5] C. L. SIEGEL, The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \dots + k$, *J. London Math. Soc.* **1** (1920), 66–68.
- [6] V. G. SPRINDŽUK, Hyperelliptic Diophantine equations and number of the class of the ideals (in Russian) *Acta Arithmetica* **30** (1976), 95–108.
- [7] C. L. STEWART, On some Diophantine Equations and Related Linear Recurrence Sequences, *Seminare Delange-Pisot-Poitou Theorie des Nombres* (1980–81), 317–321.

(Received January 3, 1983.)

MATHEMATICAL INSTITUT
KOSSUTH LAJOS UNIVERSITY
H-4010 DEBRECEN, Pf. 12.
HUNGARY