On the solution of the equation $G_n=P(x)$*

Attila Pethö (Debrecen, Köln)

1. Introduction

Let $G_o, G_1, A, B \in \mathbb{Z}$, and $G_{n+1}=AG_n-BG_{n-1}$, for $n\geq 1$. Let α and β denote the roots of the characteristic polynomial X^2-AX+B of G_n. Finally let $D=A^2-4B$ - the discriminant of G_n -, $a=G_1-\beta G_o$, $b=G_1-\alpha G_o$ and $C=ab$. The recurrence is called non-degenerated, if α/β is not a root of unity and $C\neq 0$.

Under the assumption of non-degeneracy T.N. Shorey and C.L. Stewart [9] proved that all integer solutions x,n,q - $|x|, q\geq 2$ of the Diophantine equation

$$G_n=dx^q, \qquad 0\neq d\in Z \tag{1}$$

satisfy $\max\{n,|x|,q\}\leq C_1$, where C_1 is an effectively computable constant depending only on A,B,G_o,G_1 and d.

Let S denote the set of all nonzero integers composed of primes $p_1,\dots,p_t\in Z$. Then A. Pethö [6] proved that if $(A,B)=1$ then all integer solutions x,q,n,d - $|x|, q\geq 2$, $0\neq d\in S$ of (1) satisfy $\max\{n,|x|,q,d\}\leq C_2$, where C_2 is an effectively computable constant depending only on $A,B,G_o,G_1,p_1,\dots,p_t$.

Let $P(x)\in Z[x]$ and denote by $H(P)$ and $\deg(P)$ the height, i.e. the maximum of the absolut values of the coefficients of $P(x)$, and the degree of $P(x)$ respectively. In this paper we are dealing with the more general Diophantine equation

$$G_n=dx^q+P(x). \tag{2}$$

If $|B|=1$, G_n is non-degenerated, and $P(x)$ is a constant polynomial, then C.L. Stewart [10] was able to prove that (2)

---

* This work was written when the author was a visitor at the Universität zu Köln with the fellowship of the Alexander von Humboldt-Stiftung.

has only finitely many effectively computable integer solutions x,n,q with $|x|>1$, $q>2$.

This result was extended by I. Nemes and A. Pethö [4]. They proved that if G_n is a non-degenerated recurrence with $|B|=1$, and $H(P)<h$, $\deg(P)\le\min\{q(1-\gamma),q-3\}$, where h and γ denote positive real numbers, then all integer solutions n,x,q with $|x|>1$ of (2) satisfy $\max\{n,|x|,q\}<C_2$, where C_2 is an effectively computable constant depending only on A, G_o,G_1,d,h and γ.

For generalizations of this results we refer to T.N. Shorey and C.L. Stewart [9], P. Kiss [2] and I. Nemes and A. Pethö [4].

We shall prove in this paper (Theorem 3) that if $P(x)$ is a fixed polynomial and $q>\deg(P)+2$, then (2) has only finitely many effectively computable solutions $n,|x|>1,q$. This result is best possible in the restriction on q, as was shown in [5].

I. Nemes and A. Pethö [5] have given a necessary condition under which the equation

$$G_n=P(x)=a_kx^k+\dots+a_o \tag{3}$$

has infinitely many solutions. They have characterized the solutions in x too. In Theorem 1 we make more precise this characterization and describe the solutions in n. The result is a generalization of the well known Skolem-Lech-Mahler Theorem.

2. Results

Let $T_k(x)$ denote the k-th Tshebishef polynomial, i.e. let $T_o(x)=2$, $T_1(x)=x$, $T_k(x)=xT_{k-1}(x)-T_{k-2}(x)$.

Theorem 1. Let G_n be a linear recurrence with $|B|=1$, and $P(x)\in Z[x]$. Assume that (3) has infinitely many integer solutions n and x.

(i) If $\alpha\ne\beta$ then the set of solutions in n is equal to the union of a finite set and a finite number of arithmetical progressions.

(ii) *If* $k>1$, *then the set of integers* ka_kx+a_{k-1}, *where* x *runs through the solutions of* (3) *is equal to the union of a finite set and a finite number of recurrences with discriminants* D_i *such that* D/D_i *are squres of integers.*

(iii) *If* G_n *is non-degenerated and* $k\geq 2$, *then*

$$P(x)=\varepsilon\sqrt{q}T_k\left(\frac{2ka_k}{\eta\sqrt{E}}x+\frac{2a_{k-1}}{\eta\sqrt{E}}\right), \tag{4}$$

where $q=-B^nC/D, E=2(k-1)a_{k-1}^2-4ka_ka_{k-2}$ *and* $\varepsilon,\eta=\pm 1$.

Remark 1. (iii) and in a weaker form (ii) were proved by I.Nemes and A.Pethö [5] .

Remark 2. (i) is a generalization of the well known Skolem-Lech-Mahler theorem, which is true for more general exponential sums too. It seems to be an interesting question, whether (i) has a generalization to higher order recurrences, or second order recurrences with $|B|>1$.

Let R_n be a recursive sequence with $R_0=0$, $R_1=1$ and with a prime discriminant. Then $C=1$ and $R_n=(\alpha^n-\beta^n)/\sqrt{D}$. Let further $R_n^*=\alpha^n+\beta^n$ with the same α, and β, then $C^*=-D^*=-D$. The Fibonacci and Lucas sequences satisfy this conditions.

Theorem 2. *Put* $G_n=R_n$ *and assume that* (3) *has infinitely many integer solutions. Then* k *is odd*, k/n *and there exist integers* l_0,l_1 *such that* $l_1x+l_0=R_{n/k}$.

Put $G_n=R_n^*$ *and assume that* (3) *has infinitely many integer solutions. Then* k/n *and there exist integers* l_0,l_1 *such that either* $l_1x+l_0=R_{n/k}$ *or* $l_1x+l_0=R_{n/k}^*$.

Theorem 3. *Let G_n be a non-degenerated recurrence with* $|B|=1$ *and* $P(x)\in Z[x]$, $0\neq d\notin Z$. *There exists an effectively computable constant C_3 depending only on* A, G_o, G_1, d, *and* $P(x)$ *such that all integer solutions* $n, |x|>1$, $q>\deg(P)+2$ *of* (2) *satisfy* $\max\{n,|x|,q\}<C_3$.

3. Proofs

Proof of Theorem 1. Let us assume first that G_n is degenerated but $\alpha\neq\beta$. If $C=0$ then we may assume $a=G_1-\beta G_o=0$, i.e $\beta\in Q$, hence $\beta\in Z$, since it is an algebraic integer. By the assumption $|\alpha\beta|=1$, so $\beta=1$ or -1, and $\alpha=-\beta$. Assume now that α/β is a root of unity. Then $|\alpha/\beta|=1$, and by the assumption $|\alpha\beta|=1$, so $|\alpha^2|=1$. Hence we have seen that if G_n is degenerated, then α and β are roots of unity, consequently G_n is a periodic sequence of integers. This proves (i) and (ii) for degenerated sequences.

From now on we assume that G_n is non-degenerated, and $|\alpha|>|\beta|$. By $|B|=1$ is $D>0$, and so are α and β quadratic irrationalities. Hence G_n tends to infinity. If $\deg(P)=0$ then (3) has only finitely many solutions. Let $\deg(P)=1$, i.e. $P(x)=a_1x+a_o$, $a_1\neq 0$. Then $G_n \pmod{a_1}$ is periodic, hence the set of solutions n of (3) looks like described in (i).

In the following we assume that G_n is non-degenerated and $\deg(P)\geq 2$. (iii) and in a weaker form (ii) were proved by Nemes and Pethö [5]. To make our argument clear and complete, we give here the sketsh their proof.

Write $G_n=(a\alpha^n-b\beta^n)/(\alpha-\beta)$ and $H_n=a\alpha^n+b\beta^n$. Then $H_n\in Z$ and

$$DG_n^2 + 4CB^n=H_n^2 . \tag{5}$$

Let us replace G_n to $P(x)$ in (5), then we have an elliptic equation in the unknowns H_n and x with infinitely many distinct solutions

$$Q(x)=DP(x)^2 + 4CB^n = H_n^2 . \tag{6}$$

By the famous theorem of C.L. Siegel [8], (6) has only finitely many solutions, if $Q(x)$ has at least three simple zeros. We have seen that this condition is realized except when $P(x)$ is a solution of the following polynomial equation

$$DP(x)^2 + 4CB^n = P'(x)^2R(x), \tag{7}$$

where $R(x)\in Q[x]$ is of degree two without multiple roots. To solving (7) we applied a lemma of Schinzel [7] (Lemma 6, pages 26-28) and proved (iii).

Finally we showed that if x and n is a solution of (3) then either $P'(x)=0$ or there exists an integer z such that

$$D(ka_kx+a_{k-1})^2-z^2=DE. \tag{8}$$

From this follows that D/z^2. Let $D=d_1d_2^2$, where d_1 denotes a quadrat-free integer. d_1 is at least two because of the non-degeneracy. Let $z=d_1d_2u$, then (8) is equivalent to the equation

$$(ka_kx+a_{k-1})^2-d_1u^2=E. \tag{9}$$

Let $K=Q(\sqrt{d_1})$ and M the modul of K generated by $1,\sqrt{d_1}$. Let γ

be a fundamental unit in the group of units with norm 1 of the multiplicatorring of M. We may assume without loss of generality $|\gamma|>1$. Let δ' denote the conjugate of the element $\delta\in K$. By the theory of norm form equations (See Borevich-Shafarevich [1]) there exists finitely many non-associated elements $\delta_1,\dots,\delta_t\in M$ such that the elements of M with norm E are precisely those of form $\delta_i\gamma^h$, where $1\leq i\leq t$, and h runs over the integers.

Let x be a solution of (9). Then there exist integers h and i ($1\leq i\leq t$) such that

(10) $$2ka_kx+2a_{k-1}=\delta_i\gamma^h+\delta_i'\gamma'^h$$

By (iii) $G_n=P(x)=\varepsilon\sqrt{q}T_k((\delta_i\gamma^h+\delta_i'\gamma'^h)/\eta\sqrt{E})$. But $\delta_i\gamma^h\delta_i'\gamma'^h/(\eta\sqrt{E})^2=1$, so by the well known property of the Tshebishef polynomials

(11) $$G_n=\varepsilon\sqrt{q}\left(\frac{\delta_i}{\eta\sqrt{E}}\right)^k\gamma^{kh}+\varepsilon\sqrt{q}\left(\frac{\delta_i'}{\eta\sqrt{E}}\right)^k\gamma'^{kh}\quad.$$

(3) has by the assumption infinitely many solutions in n, so there exist some i for which (11) has infinitely many solutions. To solve this equation we apply the following

<u>Theorem</u> M (M. Mignotte [3]). <u>Suppose that</u> $u_m=\sum_{i=1}^{h}P_i(m)\alpha_i^m$, $v_n=\sum_{i=1}^{k}Q_i(n)\beta_i^n$, <u>where the</u> P's <u>and</u> Q's <u>are non zero polynomials</u> <u>and</u> $|\alpha_1|>|\alpha_2|\geq\dots\geq|\alpha_m|$, $|\beta_1|>|\beta_2|\geq\dots\geq|\beta_n|$, $|\alpha_1|>1$, $|\beta_1|>1$. <u>Then</u> (Mi) <u>There exists an effectively computable integer</u> m_o <u>such that, for</u> $m>m_o$ <u>the equation</u>

(12) $$u_m=v_n$$

implies $P_1(m)\alpha_1^m = Q_1(n)\beta_1^n$.

(Mii) If (12) has an infinity of solutions then α_1 and β_1 are multiplicately dependent.

(Miii) When P_1 and Q_1 are constants, the set of solutions (m,n) of (12) is equal to the union of a finite set and a finite number of arithmetical progressions.

It is clear that (11) fulfiles the conditions of (Miii), from which follows (i) at once. (ii) is finally a consequence of (i) and (10).

Remark 3. One can deduce from Theorem M, that G_n and H_n are closely related to the sequences staying on the right hand side of (10). Of course, the infinite part of the set of solutions (n, h) of (11) is covered by finitely many arithmetical progressions. Let $m_t=u_1t+u_2$ and $n_t=v_1t+v_2$, $t=1,2,\dots$ a pair of this. With the notations $\hat{\gamma}=\gamma^k$, $\tilde{c}_i=\varepsilon\sqrt{q}(\delta_i/\eta\sqrt{E})^k\,\gamma^{v_2k}$, $\tilde{d}_i=\varepsilon\sqrt{q}(\delta_i'/\varepsilon\sqrt{E})^k\,\gamma'^{v_2k}$, $\tilde{a}=a\alpha^{u_2}/(\alpha-\beta)$ and $\tilde{b}=-b\beta^{u_2}/(\alpha-\beta)$ (11) becomes the form

$$\tilde{a}\alpha^{u_1t}+\tilde{b}\beta^{u_1t}=\tilde{c}_i\hat{\gamma}^{v_1t}+\tilde{d}_i\hat{\gamma}'^{v_1t} .$$

Now (Mi) yields $\tilde{a}\alpha^{u_1t}=\tilde{c}_i\hat{\gamma}^{v_1t}$. Both $\hat{\gamma}$ and α are units in $Q(\sqrt{d_1})$, so if τ denotes a fundamental unit in this field with $|\tau|>1$ then there exist integers $U,V>0$ such that $\hat{\gamma}=\tau^V$ and $\alpha=\tau^U$. Hence $\tilde{a}/\tilde{c}_i=\tau^{(v_1V-u_1U)t}$ satisfies for all $t=0,1,\dots$, This means $v_1V-u_1U=0$, $\tilde{a}=\tilde{c}_i$, and $\hat{\gamma}^{v_1}=\alpha^{u_1}$. Finally $\varepsilon\sqrt{q}/(\eta\sqrt{E})^k\in Q(\sqrt{d_1})$, and its conjugate is either itself or -1 times itself.

Proof of Theorem 2. For $k=1$ is Theorem 2 trivial. Hence we may assume $k \geqq 2$. Both R_n and R_n^* are non-degenerated, so $P(x)$ satisfies (4).

Let we first examine the case $G_n=R_n$. Then $q=1/\varepsilon_n D$ with the notation $-B^n=1/\varepsilon_n$. In comparison the leading coefficients of (4) we have

$$a_k=\frac{\varepsilon}{\sqrt{\varepsilon_n D}}(2ka_k/\eta\sqrt{E})^k.$$

This follows that k is odd and $E=\varepsilon_n DF^2$, with an $F\in Z$. So $\frac{2ka_k}{\eta\sqrt{E}}=\sqrt{\varepsilon_n D}\frac{2ka_k}{\eta\varepsilon_n DF}=\sqrt{\varepsilon_n D}l_1$, or equivalently $2ka_k=l_1DF$ with an $l_1\in Z$. In comparison the constant terms of (4) we have analogously $2a_{k-1}=l_oDF$, with an $l_o\in Z$.

From the proof of Theorem 1 we know that x satisfies (8), which has actually the form

$$D^3F^2(l_1x+l_o)^2-z^2=4\varepsilon_n D^2F^2.$$

Hence z is divisible by DF. Let $z=DFy$, then

$$D(l_1x+l_o)^2-y^2=4\varepsilon_n.$$

This means that $l_1x+l_o=R_m$ for an m, and by (iii)

$$R_n=\varepsilon T_k(\sqrt{\varepsilon_n D}R_m)/\sqrt{\varepsilon_n D}\ .$$

From this follows k/n at once.

We discuss now the case $G_n=R_n^*$. If $E=F^2$ or $-F^2$, with an integer F (this satisfies always if k is odd) then we can prove the assertion as in the foregoing case.

Let us assume that $E=fF^2$ with integers f,F and $|f|\neq 1$ quadratfree. Then $\frac{2ka_k}{\eta\ fF}=\sqrt{f}\ \frac{2ka_k}{\eta\sqrt{fF}}=\sqrt{f}l_1$ and similairly $\frac{2a_{k-1}}{\eta\sqrt{fF}}=\sqrt{f}l_o$ with integers l_o,l_1. After cancellation with F^2 we have from (8)

$$D^{*}f^2(l_1x+l_o)^2-y^2 = 4D^{*}f. \tag{13}$$

If f would have an prime divisor p such that $p\nmid D^{*}$, then p^2 would divide the left hand side of (13) but it do not divide $4D^{*}f$. Hence $f=D^{*}$ or $-D^{*}$ and $l_1x+l_o = R_m$, for some m, finally k/n.

Proof of Theorem 3. Take $\gamma=1/2$, deg(P)=k, H(P)=max $|a_i|$. By the a theorem of Nemes and Pethö [4] there exists an effectively computable constant C_2 depending only on A,G_o,G_1, k and H(P) such that all integral solutions n, $|x|>1$, $q>\max\{k+3,2k\}$ of (2) satisfy

$$\max\{n,|x|, q\}< C_2.$$

If $k\leq 3$ then we have nothing to prove. Hence we may assume $k>3$, or equivalently $2k>k+3$. We shall see that if $k+3<q<2k$ then (2) has finitely many solutions.

Let us assume that there exists a q_o with $k+3<q_o<2k$ such that (2) has infinitely many solutions. Then by (iii) the polynomial $Q(x)=dx^{q_o}+P(x)=dx^{q_o}+a_kx^k+\dots+a_o$ fulfiles (4). Actually are E=0, but $2q_od\neq 0$ therefore Q(x) can not have the form (4).

References

[1] Z.I. Borevich and I.R. Safarevich, Number Theory, 2nd ed. Academic Press New York and London, 1967.

[2] P. Kiss, Differences of the terms of linear recurrences, to appear.

[3] M. Mignotte, Intersection des images de certaines suites recurrentes lineaires, Theor. Comput. Sci. 7 (1978), 117-121.

[4] I. Nemes and A. Pethö, Polynomial values in linear recurrences I, Publ. Math. Debrecen, to appear.

[5] I. Nemes and A. Pethö, Polynomial values in linear recurrences II., to appear.

[6] A. Pethö, Perfect powers in second order linear recurrences, J. Number Theory, 15 (1982) 5-13.

[7] A. Schinzel, Selected Topics on Polymomials, The University of Michigan Press, 1982.

[8] C.L. Siegel, The integer solutions of the equation $y^2=ax^n+bx^{n-1}+\dots+k$, J. London Math. Soc. 1 (1926), 66-68.

[9] T.N. Shorey and C.L. Stewart, On the Diophantine equation $ax^{2t}+bx^ty+cy^2=d$ and pure powers in recurrences, Math. Scand. 52 (1983), 24-36.

[10] C.L. Stewart, On some Diophantine equations and related linear recurrence sequences, Seminare Delange-Pisot-Poitou Theorie des Nomb. (1980-81), 317-321.

Mathematical Institute
Kossuth Lajos University
H-4010 Debrecen, Pf 12
Hungary

Mathematisches Institut der
Universität zu Köln
Weyertal 86-90
5000 Köln 41
Germany