Werk

Titel: Reducible lacunary polynomials

Autor: SCHINZEL, Andrzej

PURL: https://resolver.sub.uni-goettingen.de/purl?320141322_0013|log27

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Séminaire de Théorie des Nombres de Bordeaux
Année 1983-1984 - exposé n° 29

29-01
15 juin 1984

REDUCIBLE LACUNARY POLYNOMIALS

by

Andrzej SCHINZEL

-:-:-:-

Reducibility in this paper means a reducibility over the rational field $\mathbb{Q}$ and all the polynomials considered are supposed to have integral coefficients. The name lacunary polynomial is used to denote polynomials with a fixed number of terms like binomials, trinomials, etc., other names used in this context being sparse polynomials or fewnomials.

A dozen years ago I have published a survey paper [3] on this topic and I intend to present here results obtained since that time, but I must repeat some notions and a basic theorem.

A factorization of a polynomial f into powers of irreducible factors relatively prime in pairs will be denoted by

$$f \overset{\text{can}}{=} \text{const} \prod_{r=1}^{s} f_r^{e_r} .$$

If

$$\Phi(y_1, \dots, y_k) = y_1^{\alpha_1} \cdot \dots \cdot y_k^{\alpha_k} f(y_1, \dots, y_k) ,$$

where α_i are integers and f is a polynomial not divisible by any y_i $(1 \leq i \leq k)$ then

$$J\Phi(y_1, \dots, y_k) = f(y_1, \dots, y_k) .$$

A polynomial $g(y_1, \dots, y_k)$ is called reciprocal if

$$J(g(y_1^{-1}, \dots, y_k^{-1}) = \pm\, g(y_1, \dots, y_k) \ .$$

$L\Phi(y_1, \dots, y_k)$ is $J\Phi(y_1, \dots, y_k)$ deprived of all its irreducible reciprocal factors. The basic result concerning the factorization of $Lf(x)$ runs as follows (see [2], Th. 2 or [3], Th. 2 with $F(x_1, \dots, x_k) = a_o + \sum_{j=1}^{k} a_j x_j$) .

THEOREM 1. - Let $a_o, a_1, \dots, a_k$ be non-zero integers. For any integral vector $[n_1, \dots, n_k] \neq 0$ there exist an integral matrix $[\nu_{ij}]_{i \leq r,\, j \leq k}$ of rank r and an integral vector $[v_1, \dots, v_r]$ such that

(i) $\max |\nu_{ij}| \leq c_r(\sum_{j=0}^{k} a_j^2)$, where $c_r(a)$ is an effectively computable function,

(ii) $[n_1, \dots, n_k] = [v_1, \dots, v_r][\nu_{ij}]$

(iii) $L(a_o + \sum_{j=1}^{k} a_j \prod_{i=1}^{r} y_i^{\nu_{ij}}) \overset{can}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, \dots, y_r)^{e_\sigma}$

implies

$$L(a_o + \sum_{j=1}^{k} a_j x^{n_j}) \overset{can}{=} \text{const} \prod_{\sigma=1}^{s} LF_\sigma(x^{v_1}, \dots, x^{v_r})^{e_\sigma} \ .$$

This means that for fixed $a_o, \dots, a_k$ there are only finitely many types of factorization of $f(x) = a_o + \sum_{j=1}^{k} a_j x^{n_j}$ apart from reciprocal factors and it has the following striking consequence (see [4], Th. 2).

THEOREM 2. - If $a_j \neq 0$ $(0 \leq j \leq k)$ then either $L(a_o + \sum_{j=1}^{k} a_j x^{n_j})$ is irreducible of there are $[k/2]$ linearly independent integral vectors $[\gamma_{i_1}, \dots, \gamma_{i_k}]$ $(1 \leq i \leq [k/2])$ such that

$$\max |\gamma_{ij}| < c_o(\sum_{j=0}^{k} a_j^2)$$

and

$$\sum_{j=1}^{k} \gamma_{ij} n_j = 0 \qquad (1 \leq i \leq [\tfrac{k}{2}]) \ .$$

This theorem sharpens Corollary 2 on p. 137 of [3]. The value of $c_o(\sum_{j=1}^{k} a_1^2)$ obtained from the proof is extremely large, but the number $[k/2]$ is best possible.

Reciprocal factors of $a_o + \sum_{j=1}^{k} a_j x^{n_j}$ have not been so far described in a satisfactory fashion. For $k = 1$ and 2 they can be tackled but already for $k = 3$ there is an open problem. Let us consider these cases in more details. If $a_o \neq \pm a_1$ then $a_o + a_1 x^{n_1}$ has no reciprocal factor and its factorization is described fully by Theorem 1. If $a_o = \pm a_1$ then $a_o + a_1 x^{n_1} = a_1(x^{n_1} \pm 1)$ factorizes into cyclotomic factors and there are infinitely many different types of factorization. This is an indication that one cannot hope to obtain a result analogous to Theorem 1 concerning all possible factors but at the best all factors that are not cyclotomic. Let us call a polynomial $g(y_1, \dots, y_k)$ extended cyclotomic if it is of the form $J(h(\prod_{i=1}^{k} y_i^{\delta_i}))$, where h is a cyclotomic polynomial and $\delta_1, \dots, \delta_k$ are coprime integers. Denoting by $K\Phi(y_1, \dots, y_k)$ the polynomial $J\Phi(y_1, \dots, y_k)$ deprived of all its extended cyclotomic factors we can formulate

CONJECTURE 1. - Theorem 1 holds with L replaced by K .

For $k = 2$ the conjecture is true (see [2], Th. 5 and [3], Th. 3 with $F(x_1, x_2) = a_o + a_1 x_1 + a_2 x_2$) and we obtain the following result.

Either $K(a_o + \sum_{j=1}^{2} a_j x^{n_j})$ is irreducible or

$$n_j = \nu\nu_j\,, \quad |\nu_j| \leq c_1\Big(\sum_{j=0}^{2} a_j^2\Big) \quad (j = 1,\ 2)\,,$$

$K(a_o + \sum_{j=1}^{2} a_j x^{\nu_j})$ is reducible and

$$K\Big(a_o + \sum_{j=1}^{2} a_j x^{\nu_j}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma} \quad \text{implies}$$

$$K\Big(a_o + \sum_{j=1}^{2} a_j x^{n_j}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^\nu)^{e_\sigma}\,.$$

Moreover as has been proved recently ([7], Th. 2) we have

THEOREM 3. - The numbers of integer triples $\langle a_o, a_1, a_2 \rangle$ satisfying $|a_j| \leq a \quad (0 \leq j \leq 2)$ such that for at least one pair $\langle n_1, n_2 \rangle$ $a_o + \sum_{j=1}^{2} a_j x^{n_j}$ has a reciprocal factor is $O(a^2)$.

For $k = 3$ the situation is less satisfactory. An application of Theorem 1 gives after a long argument (see [1] and [5]) the following result.

Assume that $q(x) = a_o + \sum_{j=1}^{3} a_j x^{n_j}$ is not the product of two binomials. $Lq(x)$ is reducible if and only if either $q(x)$ can be split into two parts which have a non-reciprocal common factor or it can be represented in one of the forms

$$k(U^3+V^3+W^3-3UVW) = k(U+V+W)(U^2+V^2+W^2-UV-UW-VW) ,$$

$$k(U^2-4TUVW-T^2V^4-4T^2W^4) = k(U-TV^2-2TVW-2TW^2)(U+TV^2-2TVW+2TW^2)$$

$$k(U^2+2UV+V^2-W^2) = k(U+V+W)(U+V-W) ,$$

where $k = \pm \gcd(a_o, a_1, a_2, a_3)$, T, U, V, W are monomials in $Z[x]$ and the factors on the right hand side are non-reciprocal or finally

$$n_j = v\nu_j , \quad \nu_j < c_1(\sum_{i=0}^{3} a_i^2) \quad (1 \le i \le 3)$$

and

$$L(a_o + \sum_{j=1}^{3} a_j x^{\nu_j}) \text{ is reducible.}$$

Conjecture 1 is not proved for $k = 3$ in full generality. However (see [7], Th. 1) we have

THEOREM 4. - The number of integer quadruples $<a_o, a_1, a_2, a_3>$ satisfying $|a_j| \le a$ $(0 \le j \le 3)$ and such that for at least one triple $<n_1, n_2, n_3>$ $a_o + \sum_{j=1}^{3} a_j x^{n_j}$ has a reciprocal factor is $O(\frac{a^4}{(\log a)^{3/4}})$.

We propose

CONJECTURE 2. - The number of integer $(k+1)$-tuples $<a_o, a_1, \ldots, a_k>$ satisfying $|a_j| \le a$ $(0 \le j \le k)$ and such that for at least one k-tuple $<n_1, \ldots, n_k>$ $a_o + \sum_{j=1}^{k} a_j x^{n_j}$ has a reciprocal factor is $O(a^k)$.

Towards the proof of Conjectures 1 and 2 for $k > 3$ we have only made a small step embodied in the following theorem (see [6]).

THEOREM 5. - If $f(x) = a_o + \sum_{j=1}^{k} a_j x^{n_j}$ $(0 = n_o < n_1 < \ldots < n_k , \ a_o a_k \neq 0)$ then either all reciprocal irreducible factors of f are cyclotomic or there exist integers $\gamma_1, \ldots, \gamma_k$ satisfying

$$\sum_{j=1}^{k} \gamma_j n_j = 0 , \quad 0 < \max_{1 \le j \le k} |\gamma_j| \le \max_{0 \le j \le k} \frac{\log a_j^2}{\log 2}$$

or finally the following system of inequalities in fulfilled

$$\sum_{j=0}^{k-1} |a_j||n_j-n_i| > |a_k|\,(n_k-n_i) \quad \text{if} \quad n_i < \frac{n_k}{2} \ ,$$

$$\sum_{j=1}^{k} |a_j|\,|n_j-n_i| > |a_o|\,n_i \quad \text{if} \quad n_i > \frac{n_k}{2} \ ,$$

$$\sum_{j=1}^{k-1} |a_j|\,|n_j-\frac{n_k}{2}| > ||a_k|-|a_o||\frac{n_k}{2} \ .$$

Note that the last system of inequalities implies

$$\sum_{j=1}^{k-1} |a_j| > |a_o| + |a_k| \ .$$

-:-:-:-

REFERENCES

[1] M. FRIED and A. SCHINZEL, Reducibility of quadrinomials, Acta Arith. 21 (1972), 153-171.

[2] A. SCHINZEL, Reducibility of lacunary polynomials I, ibid. 16 (1969), 123-159.

[3] A. SCHINZEL, Reducibility of lacunary polynomials, Proc. Symposia Pure Math. 20 (1971), 135-149.

[4] A. SCHINZEL, A general irreducibility criterion, J. Indian Math. Soc. 37 (1973), 1-8.

[5] A. SCHINZEL, Reducibility of lacunary polynomials III, Acta Arith. 34 (1978), 227-266.

[6] A. SCHINZEL, Reducibility of lacunary polynomials IV, ibid. 43 (1984), 311-313.

[7] A. SCHINZEL, Reducibility of lacunary polynomials V, ibid. 43 (1984), 425-440.

(texte reçu le 6 août 1984)

-:-:-:-

Andrzej SCHINZEL
Instytut Matematyczny PAN
ul. Sniadeckich 8
P - WARSZAWA

Note added on October 25. Conjecture 1 has been proved for $k = 3$,

$$\sqrt{|a_o a_1 a_2 a_3|} \notin \mathbb{Q} \ .$$