MÉMOIRES DE LA S. M. F.

E. DOBROWOLSKI

On a question of Lehmer

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 35-39
<http://www.numdam.org/item?id=MSMF_1980_2_2__35_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 35-39

ON A QUESTION OF LEHMER

by

E. DOBROWOLSKI

Let f be a polynomial with integral coefficients. Define the measure of f by

$$M(f) = a \prod_{i=1}^{n} \max(1, |\alpha_i|)$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the zeros of f listed with proper multiplicity and a is the leading coefficient. D. H. Lehmer [5] asked whether for every $\varepsilon > 0$ there exists a monic polynomial f such that $1 < M(f) < 1+\varepsilon$.

P. E. Blanksby and H. L. Montgomery [1] and the present writer [2] obtained lower bounds for M(f) in terms of the degree of f. In this paper we give a lower bound for M(f) in terms of the number of non-zero coefficients of the polynomial f. The existence of such a bound (but not its form) has been announced by W. Lawton [4] .

Theorem 1 : If $F(z) \in \mathbb{Z}[z]$ is an irreducible non-cyclotomic polynomial, $F(z) \neq \pm z$, then

$$M(F) > 1 + \frac{\log 2e}{2e} \frac{1}{(k+1)^k}$$

where k is the number of non-zero coefficients of F.

The argument used in the proof gives the following corollary.

Corollary 1 : If F is a product of different cyclotomic polynomials and F has at most k non-zero coefficients then

$$\ell(F) < k^k + 1$$

where $\ell(F)$ denotes the sum of absolute values of the coefficients of F.

The omission of the assumption of irreducibility of the polynomial F in Theorem 1 leads to a more complicated situation. In the general case the present writer, W. Lawton and A. Schinzel [3] obtained the following result.

Theorem 2 : If $g(z) \in \mathbb{Z}[z]$ is a monic polynomial with $g(0) \neq 0$ that is not a product a cyclotomic polynomials then

$$M(g) > 1 + \frac{1}{\exp_{k+1} 2k^2}$$

where k is the number of non-zero coefficients of g.
(Here, $\exp_{k+1}$ denotes the (k+1)-th iterate of the exponential function).

In the proof we use notation of $\ell(f)$ and $M(f)$ as above. Further $|f|$ denotes the degree of f. For a vector $\underline{x}$, $\ell(\underline{x})$ denotes the sum of absolute values of coordinates of $\underline{x}$.

Lemma 1 : If α is a non-zero algebraic integer of degree n which is not a root of unity, and if p is a prime number, then

$$\left| \prod_{i,j=1}^{n} (\alpha_i^p - \alpha_j) \right| > p^n$$

Proof : This is Lemma 1 of [2] .

Lemma 2 : If $f(z) \in \mathbb{Z}[z]$ is an irreducible polynomial and

$$M(f) < 1 + \frac{\log 2e}{2e} \frac{1}{\ell(f)}$$

then f is a cyclotomic polynomial or $f(z) = \pm z$.

Proof : Let p be a prime number in the interval $e\ell(f) < p < 2e\ell(f)$. Suppose that f is not a cyclotomic polynomial and let $\alpha_1, \alpha_2, \ldots \alpha_{|f|}$ be its zeros. Lemma 1 gives

$$\ell(f)^{|f|} M(f)^{p|f|} \geq \Big| \prod_{i=1}^{|f|} f(\alpha_i^p) \Big| \geq p^{|f|}$$

which is inconsistent with the inequality assumed in the Lemma. This Lemma was also proved with $\frac{1}{6}$ in place of $\frac{\log 2e}{2e}$ by C. L. Stewart, M. Mignotte and M. Waldschmidt, see [6] .

Lemma 3 : Let $\underline{a} \in \mathbb{Z}^N$ be a vector with $\ell(\underline{a}) \geq (NB)^N + 1$ and $B > 1$ be a real number. Then there exist vectors $\underline{c} \in \mathbb{Z}^N$ and $\underline{r} \in \mathbb{Q}^N$ and a rational number q such that

(i) $\underline{a} = \underline{r} + q\,\underline{c}$

(ii) $0 \neq \ell(\underline{c}) \leq (NB)^N + B^{-1}$

(iii) $q \geq B.\ \ell(\underline{r})$

(Note that $\ell(\underline{a}) > \ell(\underline{c})$ so $\underline{a} \neq \underline{c}$).

Proof : Let $Q > 1$ be a real number. By Dirichlet's theorem there exist a rational integer t, $1 \leq t \leq Q^N$, such that

$$\Big\| t \frac{a_i}{\ell(\underline{a})} \Big\| \leq Q^{-1} \quad \text{for} \quad i = 1,2,\ldots,N$$

where $\underline{a} = (a_1, a_2, \ldots, a_N)$ and $\| \ \|$ denotes the distance to the nearest integer. Take $Q = NB$ and define $q = \frac{\ell(\underline{a})}{t}$. Define the vector $\underline{c} = (c_1, c_2, \ldots, c_N)$ by the conditions

$$\Big\| t \frac{a_i}{\ell(\underline{a})} \Big\| = \Big| t \frac{a_i}{\ell(\underline{a})} - c_i \Big| \ , \quad c_i \in \mathbb{Z} \qquad \text{for } i = 1,2,\ldots,N$$

and the vector $\underline{r} = (r_1, r_2, \ldots, r_N)$ by $\underline{r} = \underline{a} - q.\underline{c}$. Then (i) holds trivially. For (ii) note the inequality

$$\left| t - \sum_{i=1}^{N} |c_i| \right| = \left| \sum_{i=1}^{N} \left(t \frac{|a_i|}{\ell(\underline{a})} - |c_i|\right) \right| \leq \sum_{i=1}^{N} \left| t \frac{|a_i|}{\ell(\underline{a})} - |c_i| \right| \leq NQ^{-1} < 1.$$

Thus $t \geq 1$ implies that $\underline{c} \neq 0$. On the other hand

$$\ell(\underline{c}) = \sum_{i=1}^{N} |c_i| \leq \sum_{i=1}^{N} \left(\left| t \frac{a_i}{\ell(\underline{a})} \right| + Q^{-1} \right) \leq (NB)^N + B^{-1} .$$

Finally

$$\ell(\underline{r}) = \sum_{i=1}^{N} |a_i - q.c_i| = q \sum_{i=1}^{N} \left| t \frac{a_i}{\ell(\underline{a})} - c_i \right| \leq qB^{-1}$$

which proves (iii).

<u>Proof of Theorem 1</u> : Let $F(z) = \sum_{i=1}^{k} a_i z^{n_i} \in \mathbb{Z}[z]$. If the exponents $n_1, n_2, \ldots, n_k$ are fixed, then, with each vector $\underline{a} = (a_1, a_2, \ldots, a_k)$, we can associate the polynomial $a(z) = \sum_i a_i z^{n_i}$ and conversely. If $\ell(F) \leq (k+1)^k$ then the assertion of the theorem holds by Lemma 2. Otherwise, let $\underline{F} \in \mathbb{Z}^k$ be the vector corresponding to F. Then

$$\ell(\underline{F}) = \ell(F) > kB^k + 1 \qquad \text{with} \qquad B \geq 1 + \frac{\log 2e}{2e} \frac{1}{(k+1)^k} .$$

By Lemma 3 $\underline{F} = \underline{r} + q.\underline{c}$ with $\underline{r} \in \mathbb{Q}^k$ and $\underline{c} \in \mathbb{Z}^k$. Further $q \geq B.\ \ell(\underline{r})$ and $\underline{F} \neq \underline{c}$. If F,r,c are the corresponding polynomials then $F \neq c$ implies that $r \neq 0$ and $(F,c) = 1$ because of the irreducibility of F. Hence

$$\prod_{F(\alpha)=0} r(\alpha) = \prod_{F(\alpha)=0} (-q.c(\alpha))$$

and

$$\ell(r)^{|F|} M(F)^{|F|} \geqslant q^{|F|}$$

So $M(F) \geqslant B$.

<u>Proof of Corollary 1</u> : Assume that $\ell(F) > k^k + 1$. Then $\ell(F) > kB^k + 1$ with some $B > 1$ and, by Lemma 3, $F = r + q.c$ with $c(z) \in \mathbb{Z}[z]$ and $q \geqslant B\,\ell(r)$. Further $\ell(c) < \ell(F)$ and $|c| \leqslant |F|$. So F does not divide c and there exists a cyclotomic polynomial f dividing F and not dividing c. Hence

$$0 \neq \prod_{f(\alpha)=0} r(\alpha) = \prod_{f(\alpha)=0} (-q.c(\alpha))$$

and

$$\ell(r)^{|f|} M(f)^{|F|} \geqslant q^{|f|}$$

which gives the contradiction $1 = M(f) \geqslant B > 1$.

<u>References</u>

[1] P. E. Blanksby and H. L. Montgomery, Algebraic integers near the unit circle Acta Arith. 28 (1971), pp.355-369.

[2] E. Dobrowolski , On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. 34 (1979), pp.125-135.

[3] E. Dobrowolski, W. Lawton, A. Schinzel, On a problem of Lehmer, Acta Math. Acad. Sci. Hungaricae (to appear).

[4] W. Lawton, Asymptotic properties of roots of polynomials-preliminary report, Proceedings of the Seventh Iranian National Mathematical Conference, Azarabadegan University, Tabris, Iran, March 1976.

[5] D. H. Lehmer, Factorization of certain cyclotomic functions, Ann. Math. 2, 34 (1933), pp.461-479.

[6] C. L. Stewart, On a theorem of Kronecker and related question of Lehmer, Séminaire de théorie des nombres, Bordeaux, 1977-78, n°7, 11p.

Wrocław University
Institute of Mathematics
Pl. Grunwaldski 2/4
50-384 Wrocław (Poland)