[8] S. Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. Ser. 2, 14 (1915), p. 347–409; Collected papers, p. 78–128.
[9] A. Selberg, *On the normal density of primes in small intervals and the difference between consecutive primes*, Arch. math. Naturvid. 47 (6) (1943), p. 87–105.

DÉPARTEMENT DE MATHÉMATIQUES
U.E.R. DES SCIENCES
123, rue Albert Thomas
87060 Limoges Cedex, France

Reçu le 27. 1. 1978
et dans la forme modifiée le 4. 6. 1978 (1037)

ACTA ARITHMETICA
XXXIV (1979)

On a question of Lehmer and the number of irreducible factors of a polynomial

by

E. Dobrowolski (Wrocław)

1. In 1933 D. H. Lehmer [5] posed the following question:

Let a be a non-zero algebraic integer of degree n, $a_1 = a, a_2, \ldots, a_n$ its conjugates over the rationals and let

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

Is it true that for every positive ε there exists an algebraic integer a such that $1 < M(a) < 1+\varepsilon$?

Clearly, $M(a) \geqslant 1$ and Kronecker's theorem [3] asserts that $M(a) = 1$ implies that a is a root of unity.

In the case where a is not reciprocal (i.e. when a and $1/a$ are not conjugate) Lehmer's question was answered in the negative in 1971 by C. J. Smyth [8]. He showed that if β_0 denotes the real root of the equation $x^3-x-1 = 0$ and a is not reciprocal, then either $M(a) \geqslant \beta_0$ or a is a root of unity. This implies the well-known Siegel's result that β_0 is the smallest PV-number.

In the same year, P. E. Blanksby and H. L. Montgomery [2] showed in the general case that if a is not a root of unity, then

$$M(a) \geqslant 1+\frac{1}{52n\log 6n}.$$

An estimation on $M(a)$ of the same order was recently obtained by C. L. Stewart [9] who used a different argument. Stewart's proof is based on a construction of an auxiliary polynomial with small coefficients.

In this paper we modify the method of Stewart and prove

Theorem 1. *Let a be non-zero algebraic integer of degree n. If ε is an arbitrary positive constant and $n > n_0(\varepsilon)$, and*

$$M(a) \leqslant 1+(1-\varepsilon)\left(\frac{\log\log n}{\log n}\right)^3,$$

then a is a root of unity.

An easy computation shows that if we replace $1-\varepsilon$ by $1/1200$, then the assertion of our theorem holds for all n.

With Lehmer's problem is closely connected a conjecture of A. Schinzel and H. Zassenhaus [6] concerning $\overline{|\alpha|} = \max_{1\leqslant i\leqslant n}|\alpha_i|$. They conjectured that there exist a positive constant C such that the inequality

$$\overline{|\alpha|} \leqslant 1+\frac{C}{n}$$

implies that α is a root of unity.

The result of Smyth gives the positive answer for non-reciprocal α. In the general case our theorem gives

COROLLARY. *Let α be a non-zero algebraic integer of degree n. If ε is an arbitrary positive constant and $n > n_0(\varepsilon)$, and*

$$\overline{|\alpha|} \leqslant 1+\frac{2-\varepsilon}{n}\left(\frac{\log\log n}{\log n}\right)^3,$$

then α is a root of unity.

Let f be a polynomial with integral coefficients. Denote:

$|f|$ — the degree of f,

$\|f\|$ — the sum of squares of its coefficients,

$\omega(f)$ — the number of distinct irreducible factors of f,

$\Omega(f)$ — the number of irreducible factors of f counted with multiplicities,

$\Omega_1(f)$ — the number of non-cyclotomic irreducible factors of f counted with multiplicities.

In [7] A. Schinzel conjectured that if $f(0)\neq 0$ then for an arbitrary $\varepsilon > 0$

(A) $\Omega_1(f) = O\big(|f|^{\varepsilon}(\log\|f\|)^{1-\varepsilon}\big)$,

(B) $\Omega(f) = O\big(|f|^{\varepsilon}(\log\|f\|)^{1-\varepsilon}\big)$,

(C) $\omega(f) = o\big(|f|^{\varepsilon}(\log\|f\|)^{1-\varepsilon}\big)$ (as $|f|$ tends to infinity).

Also A. Schinzel observed that Theorem 1 implies (A). Next the author of this paper and A. Schinzel noticed that (B) and (C) are false in the general case.

More precisely, we have

THEOREM 2. (i) *If f is a polynomial with $f(0)\neq 0$ and ε is an arbitrary positive number, then*

$$\Omega_1(f) = O\big(|f|^{\varepsilon}(\log\|f\|)^{1-\varepsilon}\big).$$

(ii) *For every positive $\varepsilon < \frac{1}{2}$ and every n there exists a polynomial f with $f(0)\neq 0$ and $|f| > n$ such that*

$$\omega(f) > c\,|f|^{\varepsilon}(\log\|f\|)^{1-\varepsilon} \quad \textit{with} \quad c = c(\varepsilon) > 0.$$

(iii) *For every positive c there exists a polynomial f with $f(0)\neq 0$ and $|f| > c$ such that*

$$\Omega(f) > c\,|f|^{1/2}(\log\|f\|)^{1/2}.$$

The author is very grateful to Professor A. Schinzel for helpful comments which allow to improve the constant of Theorem 1 from $4/27$ to $1-\varepsilon$.

2. The proofs are based on three lemmas, the first of which is a slightly modified Stewart's [9] version of Siegel's lemma. For the convenience of the reader we give full details.

LEMMA 1. *Let b_{ij} $(1\leqslant i\leqslant N,\ 1\leqslant j\leqslant M)$ be algebraic integers in a field K, such that for each j not all b_{ij} $(1\leqslant i\leqslant N)$ are zero. Let $[K:Q] = n$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ denote the embeddings of K in the complex numbers. If $N > Mn$, then the system of equations*

$$\sum_{i=1}^{N} b_{ij}x_i = 0 \qquad (1\leqslant j\leqslant M)$$

has a solution in rational integers $x_1, x_2, \ldots, x_N$, not all of which are zero, whose absolute values are at most

$$Y = \Big(2\sqrt{2}\,(N+1)\Big(\prod_{j=1}^{M}\prod_{k=1}^{n}\max_i|\sigma_k(b_{ij})|\Big)^{1/nM}\Big)^{nM/(N-nM)}.$$

Proof. Let $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ be the real embeddings of K and $\sigma_{r_1+1}, \ldots, \sigma_n$ be the complex with $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ for $i = 1, 2, \ldots, r_2$ and $n = r_1+2r_2$.

Put

$$\tau_i = \begin{cases}\sigma_i & \text{for} \quad 1\leqslant i\leqslant r_1,\\ \operatorname{Re}\sigma_i & \text{for} \quad r_1 < i\leqslant r_1+r_2,\\ \operatorname{Im}\sigma_i & \text{for} \quad r_1+r_2 < i\leqslant n.\end{cases}$$

Let $0\leqslant y_i\leqslant Y$ for $i = 1, 2, \ldots, N$ and $\eta = [Y]-Y+1 > 0$. For $(Y+\eta)^N$ N-tuples we have

$$\Big|\tau_k\Big(\sum_{i=1}^{N} b_{ij}y_i\Big)\Big| \leqslant NY\max_{1\leqslant i\leqslant N}|\tau_k(b_{ij})| = A_{kj}$$

for $k = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, M$.

Thus the numbers $\tau_k\big(\sum_{i=1}^{N} b_{ij}\,y_i\big)$ lie in the intervals $I_{kj} = [-A_{kj}, A_{kj}]$ with lengths $2A_{kj}$. Now divide each of the intervals I_{kj} into L_j equal parts. If

$$\prod_{j=1}^{M} L_j^n < (Y+\eta)^N, \tag{1}$$

then by pigeon-hole principle there exist two different N-tuples $(y_1, y_2, \ldots, y_N)$ and $(y_1', y_2', \ldots, y_N')$ such that

$$\left|\tau_k\Big(\sum_{i=1}^{N} b_{ij} y_i\Big) - \tau_k\Big(\sum_{i=1}^{N} b_{ij} y_i'\Big)\right| \leqslant \frac{2NY}{L_j} \max |\tau_k(b_{ij})|$$

for $1 \leqslant k \leqslant n$ and $1 \leqslant j \leqslant M$.

Put $x_i = y_i - y_i'$ for $i = 1, 2, \ldots, N$. Then $\max_i |x_i| \leqslant Y$ and not all x_i's are zero. To prove the lemma it remains to show that

$$\sum_{i=1}^{N} b_{ij} x_i = 0 \quad \text{for} \quad j = 1, 2, \ldots, M.$$

On the left-hand sides we have algebraic integers and thus it suffices to show that absolute values of their norms are less than 1. For $k \leqslant r_1$ we have

$$\Big|\sigma_k\Big(\sum_i b_{ij} x_i\Big)\Big| = \Big|\tau_k\Big(\sum_i b_{ij} x_i\Big)\Big| \leqslant \frac{2NY}{L_j} \max_i |\sigma_k(b_{ij})|.$$

For $r_1 + r_2 \geqslant k > r_1$

$$\Big|\sigma_k\Big(\sum_i b_{ij} x_i\Big)\sigma_{k+r_2}\Big(\sum_i b_{ij} x_i\Big)\Big| = \Big(\operatorname{Re}\sigma_k\Big(\sum_i b_{ij} x_i\Big)\Big)^2 + \Big(\operatorname{Im}\sigma_k\Big(\sum_i b_{ij} x_i\Big)\Big)^2$$
$$\leqslant 2\Big(\frac{2NY}{L_j}\Big)^2 \max_i |\sigma_k(b_{ij})\sigma_{k+r_2}(b_{ij})|.$$

Put

$$l_j = \left(\frac{Y^N}{\prod_{i=1}^{M}\prod_{k=1}^{n}\max_i |\sigma_k(b_{it})|}\right)^{1/nM} \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|^{1/n}$$

and $L_j = [l_j]$ for $j = 1, 2, \ldots, M$.

Now (1) is satisfied and our choice of Y assures that all the L_j are positive numbers. The choice of Y implies also the relations

$$2\sqrt{2}\, Y \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|^{1/n} > 1 > L_j - l_j$$

and

$$2\sqrt{2}\,(N+1)\, Y \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|^{1/n} - l_j = 0.$$

Hence

$$\Big|N_{K/Q}\Big(\sum_i b_{ij} x_i\Big)\Big| = \Big|\prod_{k=1}^{n} \sigma_k\Big(\sum_i b_{ij} x_i\Big)\Big| \leqslant 2^{r_2}\Big(\frac{2NY}{L_j}\Big)^n \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|$$
$$\leqslant \Big(1 + L_j^{-1}\Big(2\sqrt{2}\, NY \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|^{1/n} - L_j\Big)\Big)^n$$
$$< \Big(1 + L_j^{-1}\Big(2\sqrt{2}\,(N+1)\, Y \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|^{1/n} - l_j\Big)\Big)^n = 1.$$

LEMMA 2. *If a is a non-zero algebraic integer of degree n, then either*

(i) $a_i^r \neq a_j^s$ *for rational integers* $r > s \geqslant 1$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$,

and

(ii) $\Big|\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}} (a_i^p - a_j)\Big| \geqslant p^n$ *for prime numbers* p

hold or a is a root of unity.

Proof. (i) If $a_i^r = a_j^s$, then a_i^r and a_i^s are conjugates and there exists a $\sigma \in \operatorname{Gal}(K/Q)$ (where $K = Q(a_1, a_2, \ldots, a_n)$) such that $\sigma(a_i^r) = a_i^s$. Furthermore, there exists a rational integer k such that $\sigma^k = \mathrm{id}_K$. For this k we have

$$a_i^{r^k} = \sigma^k(a_i^{r^k}) = \big(\sigma^k(a_i^r)\big)^{r^{k-1}} = \big(\sigma^{k-1}(a_i^{r^{k-1}})\big)^s = \ldots = a_i^{s^k}$$

which means that a is a root of unity.

(ii) Define

$$f(X) = \prod_{i=1}^{n} (X - a_i) \quad \text{and} \quad f_p(X) = \prod_{i=1}^{n} (X - a_i^p).$$

Then $f(X) = f_p(X) + p\,g(X)$, $g(X) \in \boldsymbol{Z}[X]$, and

$$\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}} (a_i^p - a_j) = \prod_{i=1}^{n} \big(f_p(a_i^p) + p\,g(a_i^p)\big) = p^n \prod_{i=1}^{n} g(a_i^p).$$

If a is not a root of unity, then by (i) $\prod_{i,j}(a_i^p - a_j) \neq 0$ and $\prod_{i=1}^{n} g(a_i^p)$ is a non-zero rational integer and its absolute value is at least 1.

LEMMA 3. *If a is an algebraic number of degree n and*

$$P = \{p\colon \deg(a^p) < n\}$$

(the letter p being reserved for prime numbers), then

$$|P| \leqslant \frac{\log n}{\log 2}.$$

Proof. For integers s and j $(1 \leqslant j \leqslant n)$, write

$$I(s, j) = \{i\colon\ \alpha_i^s = \alpha_j^s\}.$$

The sets $I(s, j)$ have the following properties:

(i) $|I(s, j)| = |I(s, i)|$ for $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, and different sets $I(s, i)$, $i = 1, 2, \ldots, n$, are disjoint;

(ii) if $(r, s) = 1$, then $|I(r, i) \cap I(s, j)| \leqslant 1$;

(iii) if $(r, s) = 1$, then $|I(rs, j)| \geqslant |I(r, j)| \cdot |I(s, j)|$.

Equality (i) is obvious. To prove (ii) observe that

$$k, l \in I(s, j) \cap I(r, i) \Rightarrow \alpha_k^s = \alpha_l^s \text{ and } \alpha_k^r = \alpha_l^r$$
$$\Rightarrow \alpha_k^{(r,s)} = \alpha_l^{(r,s)} \Rightarrow \alpha_k = \alpha_l \Rightarrow k = l.$$

To obtain (iii) consider the inequality

$$|I(rs, j)| \geqslant \Big|\bigcup_{i \in I(r,j)} I(s, i)\Big|.$$

By (ii), each component of the sum on the right appears exactly one time and, by (i), these components have the same cardinality $|I(s, i)|$. This proves (iii).

Finally,

$$2^{|P|} \leqslant \prod_{p \in P} |I(p, i)| \leqslant \Big|I\Big(\prod_{p \in P} p, i\Big)\Big| \leqslant n;$$

hence

$$|P| \leqslant \frac{\log n}{\log 2}.$$

3. Proof of Theorem 1. Assume that α is not a root of unity. Put in Lemma 1:

$$N = n\left[\varepsilon^{-1/2} \frac{\log n}{\log\log n}\right]^2, \quad M = 2\left[\varepsilon^{-1} \frac{\log n}{\log\log n}\right], \tag{2}$$

$$b_{ij} = \begin{cases} \dfrac{d^{j-1}}{dx^{j-1}} (x^{i-1})\Big|_{x=\alpha} & \text{for } j > 1, \\ \alpha^{i-1} & \text{for } j = 1, \end{cases} \qquad i = 1, 2, \ldots, N,$$

i.e.,

$$[b_{ij}] = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ \alpha & 1! & \ldots & 0 \\ \alpha^2 & 2\alpha & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{N-1} & (N-1)\alpha^{N-2} & \ldots & (N-1)(N-2)\cdot\ldots\cdot(N-M+1)\alpha^{N-M} \end{bmatrix}$$

Lemma 1 then assures the existence of a non-trivial integer solution $x_1, x_2, \ldots, x_N$ of the equations

$$\sum_{i=1}^{N} b_{ij} x_i = 0, \quad j = 1, 2, \ldots, M,$$

which satisfy

$$\max_{1 \leqslant i \leqslant N} |x_i| \leqslant Y = \big(2\sqrt{2}(N+1) N^{(M-1)/2} M(\alpha)^{N/n}\big)^{nM/(N-nM)}. \tag{3}$$

Now we set

$$a_i = x_i \quad \text{for} \quad i = 1, 2, \ldots, N$$

and

$$F(X) = \sum_{i=1}^{N} a_i X^{i-1}.$$

Our selection of b_{ij} assures that

$$F(\alpha) = F^{(1)}(\alpha) = F^{(2)}(\alpha) = \ldots = F^{(M-1)}(\alpha) = 0$$

which means that

$$f(X)^M | F(X).$$

Assume without lost of generality that

$$\log M(\alpha) = A(n) \left(\frac{\log\log n}{\log n}\right)^3 \quad \text{with} \quad A(n) < 1. \tag{4}$$

Then (3) gives

$$Y \leqslant N^{2\varepsilon^{-1} + o(1)} \tag{5}$$

where $o(1)$ denotes a function of n tending to 0.

We assert that for each prime p from the interval

$$\left(\frac{\log n}{\log\log n}\right)^2 < p < \frac{2-\varepsilon}{A(n)} \frac{(\log n)^2}{\log\log n}, \tag{6}$$

we have

$$F^{(r)}(\alpha^p) = 0$$

for every $n > n_0(\varepsilon)$ and every r from the interval

$$0 \leqslant r \leqslant 2\varepsilon^{-1} - 1 - p\varepsilon^{-1} A(n) \frac{\log\log n}{(\log n)^2} - \frac{\varepsilon}{4}. \tag{7}$$

Indeed, suppose that $F^{(r)}(\alpha^p) \neq 0$ and r satisfies (6). Since

$$f(X)^{M-r} | F^{(r)}(X),$$

we have by Lemma 2

$$\Big|\prod_{i=1}^{n} F^{(r)}(\alpha_i^p)\Big| \geqslant \Big|\prod_{i=1}^{n} f(\alpha_i^p)^{M-r}\Big| \geqslant p^{n(M-r)}.$$

On the other hand,

$$\left|\prod_{i=1}^{n} F^{(r)}(\alpha_i^p)\right| \leqslant (N^{r+1}Y)^n M(\alpha)^{pN}$$

and we get

$$YN^{r+1}M(\alpha)^{p\frac{N}{n}} \geqslant p^{M-r}.$$

Hence by (4), (5), and (6)

$$(M-r)\log p \leqslant \big(r+1+2\varepsilon^{-1}+o(1)\big)\log N + p\frac{N}{n}\log M(\alpha)$$
$$\leqslant \big(4\varepsilon^{-1}-\varepsilon/4+o(1)\big)\log n.$$

On the other hand,

$$(M-r)\log p \geqslant \big(4\varepsilon^{-1}-o(1)\big)\log n$$

and we get a contradiction for n large enough.

Since $F^{(r)}(\alpha^p)=0$ for all primes p from the interval (6) and all r from (7), $F(X)$ is divisible by $f_p(X)^{V_p}$ with

$$V_p = \left[2\varepsilon^{-1}-p\varepsilon^{-1}A(n)\frac{\log\log n}{(\log n)^2}-\frac{\varepsilon}{4}\right].$$

By Lemma 3 the degree of $f_p(X)$ is equal to n for all primes p with no more than $\left[\frac{\log n}{\log 2}\right]$ exceptions.

Hence

$$\frac{N}{n} \geqslant \sum_{\frac{(\log n)^2}{(\log\log n)^2}<p<\frac{2-\varepsilon}{2}\frac{(\log n)^2}{A(n)\log\log n}} \left[2\varepsilon^{-1}-p\varepsilon^{-1}A(n)\frac{\log\log n}{(\log n)^2}-\frac{\varepsilon}{4}\right]-\frac{\log n}{\log 2}2\varepsilon^{-1}$$
$$\geqslant \frac{(2\varepsilon^{-1}-1-\varepsilon/4)\big(2-\varepsilon-o(1)\big)}{2A(n)}\,\frac{(\log n)^2}{(\log\log n)^2}-$$
$$-\varepsilon^{-1}A(n)\frac{(2-\varepsilon)^2-o(1)}{4A(n)^2}\,\frac{(\log n)^2}{(\log\log n)^2}$$

and we get

$$A(n) \geqslant 1-\varepsilon+\varepsilon^3/8-o(1)$$

which proves Theorem 1.

The assertion of the Corollary follows for reciprocal α from the inequality

$$\overline{|\alpha|}^{n/2} \geqslant M(\alpha).$$

For α non-reciprocal the assertion follows from Smyth's result [8].

4. Proof of Theorem 2. (i) Assume that $f(0)\neq 0$. Put

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

where $\alpha_1,\alpha_2,\ldots,\alpha_n$ are the zeros of the polynomial f listed with proper multiplicity, and a_f is its leading coefficient.

Let

$$f(X) = f_0(X)\prod_{i=1}^{m} f_i(X)^{\beta_i} \tag{8}$$

where f_i are for $i>0$ distinct non-cyclotomic polynomials and f_0 is a product of cyclotomic factors.

Then

$$M(f) = \prod_{i=1}^{m} M(f_i)^{\beta_i}.$$

If f_i is not a monic polynomial, then

$$M(f_i) \geqslant a_{f_i} \geqslant 2.$$

If f_i is monic, then Theorem 1 gives

$$M(f_i) \geqslant 1+c\left(\frac{\log\log|f_i|}{\log|f_i|}\right)^3 \quad (\text{where } c>0).$$

This result however is non-trivial only for $|f_i|>2$, but if $|f_i|\leqslant 2$, then direct computation gives $M(f_i)\geqslant(1+\sqrt{5})/2$. Hence in all cases we have

$$\log M(f_i) \geqslant \frac{1}{(\log|f_i|)^3} \geqslant \frac{1}{|f_i|^{\varepsilon}}. \tag{9}$$

On the other hand, Landau [4] showed that

$$M(f) \leqslant \|f\|^{1/2}.$$

Thus (9) gives

$$\log\|f\| \geqslant \sum_{i=1}^{m}\frac{\beta_i}{|f_i|^{\varepsilon}}.$$

By comparison of the degrees of polynomials in (8) we get

$$|f| \geqslant \sum_{i=1}^{m}\beta_i|f_i|.$$

Finally, Hölder's inequality gives

$$\Omega_1(f) = \sum_{i=1}^{m}\beta_i \leqslant \sum_{i=1}^{m}(\beta_i|f_i|)^{\varepsilon}\left(\frac{\beta_i}{|f_i|^{\varepsilon}}\right)^{1-\varepsilon} \leqslant \left(\sum_{i=1}^{m}\beta_i|f_i|\right)^{\varepsilon}\left(\sum_{i=1}^{m}\frac{\beta_i}{|f_i|^{\varepsilon}}\right)^{1-\varepsilon}$$
$$\leqslant |f|^{\varepsilon}(\log\|f\|)^{1-\varepsilon}.$$

(ii) We use Lemma 1 to construct a suitable polynomial F divisible by a high power of the polynomial $x-1$. To this end, put

$$N = M^2+2M, \quad a = 1, \quad n = 1$$

in formula (3) (Section 3). We get a polynomial F with

$$(x-1)^M | F(X), \qquad |F| = N$$

for which

$$h(F) \leqslant \left(2\sqrt{2}(N+1)N^{(M-1)/2}\right)^{M/(N-M)} \leqslant 4M \qquad \text{and} \qquad \|F\| \leqslant 48M^4.$$

Let Φ_p, for a prime p, denote the pth cyclotomic polynomial. We have

$$\Phi_p(1) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = p$$

where ζ_p^i are the primitive pth roots of unity. Hence if $\Phi_p \nmid F$, then

$$\left|\prod_{i=1}^{p-1} F(\zeta_p^i)\right| \geqslant \left|\prod_{i=1}^{p-1}(1-\zeta_p^i)\right|^M = p^M.$$

On the other hand,

$$\left|\prod_{i=1}^{p-1} F(\zeta_p^i)\right| \leqslant \left((|F|+1)h(F)\right)^{p-1} \leqslant (3M)^{3(p-1)}.$$

Thus $p \geqslant c_1 M$ where c_1 is an absolute positive constant and $\Phi_q | F$ for q prime and less than $c_1 M$ and

$$\Omega(F) > \omega(F) \geqslant \pi(c_1 M) \gg M(\log M)^{-1}$$
$$\gg M^{2\varepsilon}(\log M)^{1-\varepsilon} \gg |F|^{\varepsilon}(\log \|F\|)^{1-\varepsilon}$$

provided that $0 < \varepsilon < 1/2$.

(iii) Let

$$f(x) = \prod_{n=1}^{N}(x^n-1)^{N-n+1}.$$

We shall prove that $f(x)$ fulfils desired conditions. For N tending to infinity we have the following asymptotic formulas:

$$|f| \sim \tfrac{1}{6}N^3, \tag{10}$$

$$\Omega(f) = \sum_{n=1}^{N}(N-n+1)d(n) \sim \tfrac{1}{2}N^2\log N \tag{11}$$

where $d(n)$ denotes the number of divisors of n.

Furthermore,

$$\|f\| = \frac{1}{2\pi}\int_0^{2\pi} |f(e^{i\theta})|^2\,d\theta \leqslant \max_{|z|=1}|f(z)|^2 = \max_{|z|=1}\left| z^{\sum_{n=1}^{N-1}(N-n)} f(z)\right|^2 \tag{12}$$

$$= \max_{|z|=1}\left|\prod_{N\geqslant k>l\geqslant 1}(z^k-z^l)\right|^2 = \max_{|z|=1}\left|\det\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & z & \dots & z^{N-1} \\ 1 & z^2 & \dots & z^{2(N-1)} \\ \dots & \dots & \dots & \dots \\ 1 & z^{N-1} & \dots & z^{(N-1)^2}\end{bmatrix}\right|^2 \leqslant N^{2N}.$$

The same estimation for $\max_{|z|=1}|f(z)|$ was obtained in a different way by F. V. Atkinson in [1].

(10), (11), and (12) prove (iii).

References

[1] F. V. Atkinson, *On a problem of Erdős and Szekeres*, Canad. Math. Bull. 4 (1961), pp. 7–12.

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

[3] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), pp. 133–175.

[4] E. Landau, *Sur quelques théorèmes de M. Petrovich relatifs aux zéros des fonctions analytiques*, Bull. Soc. Math. France 33 (1905), pp. 1–11.

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

[6] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Mich. Math. J. (1965), pp. 81–84.

[7] A. Schinzel, *On the number of irreducible factors of a polynomial*, Colloq. Math. Soc. János Bolyai 13 (1974), pp. 305–314.

[8] C. J. Smyth, *On the product of conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), pp. 169–175.

[9] C. L. Stewart, *Algebraic integers whose conjugates lie near the unit circle*, Bull. Soc. Math. France 196 (1978), pp. 169–176.

WROCŁAW UNIVERSITY
INSTITUTE OF MATHEMATICS

Received on 1. 6. 1978
and in revised form on 14. 10. 1978 (1076)