ON THE COEFFICIENTS OF THE CYCLOTOMIC POLYNOMIAL

PAUL ERDÖS

The cyclotomic polynomial $F_n(x)$ is defined as the polynomial whose roots are the primitive nth roots of unity. It is well known that

$$F_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

For $n<105$ all coefficients of $F_n(x)$ are ± 1 or 0. For $n=105$, the coefficient 2 occurs for the first time. Denote by A_n the greatest coefficient of $F_n(x)$ (in absolute value). Schur proved that $\lim\sup A_n = \infty$. Emma Lehmer[1] proved that $A_n > cn^{1/3}$ for infinitely many n. In fact she proved that infinitely many such n's are of the form pqr with p, q, and r prime. In the present note we are going to prove that $A_n > n^k$ for every k and infinitely many n. This is implied by the still sharper theorem:

THEOREM 1.[2] *For infinitely many n*

$$A_n > \exp\left[c_1(\log n)^{4/3}\right].$$

Specifically we may take $n=2\cdot 3\cdot 5\cdots p_k$ for sufficiently large k.

Since

$$\max_{|x|=1} |F_n(x)| \leqq A_n[\phi(n)+1],$$

Theorem 1 follows at once from the following theorem.

THEOREM 2. *For infinitely many n*

$$\max_{|x|=1} |F_n(x)| > \exp\left[c_2(\log n)^{4/3}\right].$$

For the proof of Theorem 2 we require several lemmas.

LEMMA 1. *Let $f(x)$ be a polynomial of highest coefficient 1 of degree m with all its roots on the unit circle. Suppose that in the unit circle $f(x)$ assumes its maximum at x_0 ($|x_0|=1$), and let y_0 be the root of $f(x)$ closest to x_0. Then the arc between x_0 and y_0 is not less than π/m; and if it equals π/m, $f(x)=x^m-1$.*

Received by the editors May 5, 1945, and, in revised form, August 22, 1945.

[1] Bull. Amer. Math. Soc. vol. 42 (1936) p. 389. Reference to the older literature can be found in this paper.

[2] Throughout the paper c_i denotes a positive constant.

This is a theorem of M. Riesz.[3]

Set $n = 2 \cdot 3 \cdot 5 \cdots p_k$.

LEMMA 2. $p_k \sim \log n$.

LEMMA 3. *$\phi(n) \sim e^{-\gamma} n / \log \log n$, where γ is Euler's constant.*

Lemma 2 is a well known consequence of the prime number theorem, and Lemma 3 follows from Lemma 2 and a theorem of Mertens.[4]

LEMMA 4. *Suppose $p_k^a \leqq u \leqq p_k^{4/3}$ where $1 < a \leqq 4/3$, and let N be the number of integers not greater than u which are prime to n. Then for sufficiently large k,*

$$N > (1 + c_3) u \phi(n)/n.$$

PROOF. The integers in question are primes greater than p_k. By the prime number theorem

$$N \sim u/\log u - p_k/\log p_k \sim u/\log u.$$

Now $1/\log u \geqq 3/(4 \log p_k)$; and, by Lemmas 2 and 3, $\log p_k \sim \log \log n \sim e^{-\gamma} n/\phi(n)$. Lemma 4 now follows from $e^{-\gamma} < 3/4$.

LEMMA 5. *Suppose that for an infinite number of integers m we are given a polynomial $g_m(x)$ of highest coefficient 1 of degree m, with all its roots on the unit circle and symmetric with respect to the real axis, and with $|g_m(1)| = 1$, Let t_m be a function of m such that $t_m/m < \pi$ and $t_m \to \infty$ as $m \to \infty$. Suppose constants c_4, ϵ $(0 < \epsilon < 1,\ 0 < c_4 < 1)$ given such that for any u with $t_m^{1-\epsilon} \leqq u \leqq t_m$ the number of roots of $g_m(x) = g_m(e^{i\theta})$ with $|\theta| \leqq u/m$ is greater than $(1 + c_4)u/\pi$, that is, greater than $(1 + c_4)$ times the number of roots of $x^m = 1$ in the same interval. Then for sufficiently large m*

$$\max_{|x|=1} |g(x)| > \exp(c_5 t_m).^{5}$$

PROOF. Denote by A, B, C the following arcs:

$$A: \ |\theta| \leqq t_m^{1-\epsilon}/m,$$
$$B: \ |\theta| \leqq t_m/m,$$
$$C: \ |\theta| \leqq (t_m + \pi)/m.$$

We define new polynomials $h_m(x) = x^m + \cdots$ as follows. Outside B,

[3] Jber. Deutschen Math. Verein. vol. 23 (1914) pp. 354–368.

[4] See, for example, Hardy and Wright, *Introduction to the theory of numbers*, p. 349.

[5] An analogous but weaker theorem has been stated in a previous paper (Ann. of Math. vol. 44 (1943) p. 337.

h_m and g_m have the same roots. In A, h_m has no roots. On $B-A$ we place consecutive roots spaced by the angle $2\pi/m$. Finally the remaining roots of h_m are placed at the end points of B, half at each.

Let $\theta_1, \theta_2, \cdots$ and $\phi_1, \phi_2, \cdots$ denote the arguments of the roots of g_m and h_m in B above the real axis; we number them in increasing order of magnitude. Our construction implies

$$\phi_r \geqq \min\,(t_m^{1-\epsilon}/m + 2\pi r/m,\ t_m/m) \tag{1}$$

while the hypothesis of Lemma 5 translates into

$$\theta_r \leqq \max\,(t_m^{1-\epsilon}/m,\ 2\pi r/(1 + c_4)m). \tag{2}$$

From (1) and (2) we deduce $\phi_r \geqq \theta_r$, that is, the process has pushed roots of g_m away from 1. If $e^{i\theta}$, $e^{i\alpha}$ are points above the real axis respectively inside and outside B, then

$$\partial \mid (e^{i\alpha} - e^{i\theta})(e^{i\alpha} - e^{-i\theta}) \mid /\partial\theta = 8 \sin\theta(\cos\alpha - \cos\theta) < 0$$

so that the process reduces g_m outside B, that is,

$$\mid h_m(x) \mid \leqq \mid g_m(x) \mid \tag{3}$$

outside B.

We shall next prove

$$\mid h_m(1) \mid > \exp\,(c_6 t_m). \tag{4}$$

Take m large enough so that $t_m^{\epsilon} \geqq 2$ and confine r to the interval

$$\begin{aligned} (1 + c_4)t_m^{1-\epsilon}/2\pi &\leqq r \\ &\leqq (1 + c_4)t_m/4\pi. \end{aligned} \tag{5}$$

Then (2) reduces to

$$\theta_r \leqq 2\pi r/(1 + c_4)m. \tag{2$'$}$$

Since from (5) and $c_4 < 1$ we have $2\pi r \leqq t_m$, (1) similarly becomes

$$\phi_r \geqq 2\pi r/m. \tag{1$'$}$$

Combining (1′) and (2′) we find $\phi_r/\theta_r - 1 \geqq c_4$ whence

$$\left| 1 - \exp\,(i\phi_r) \right| \geqq c_7(1 - \exp\,(i\theta_r) \left|.\right.$$

From this it follows that $|h_m(1)| \geqq c_7^R |g_m(1)|$, where R is the number of values of r permitted in (5). Since for large m, $R > c_8 t_m$, we have $c_7^R > \exp(c_6 t_m)$, proving (4).

Let X denote the number of roots of h_m at the end points of B.

It follows from our hypothesis that $X > c_4 t_m/\pi$. We define a further polynomial $k_m(x) = x^m + \cdots$ by placing roots at the points with arguments $\pm\pi/m$, $\pm 3\pi/m$, $\pm 5\pi/m$, $\cdots$ on the arc A. If the number of these points is Y, then $Y < c_9 t_m^{1-\epsilon}$. We place $(X-Y)/2$ roots of k_m at each end point of B and otherwise the roots of h_m and k_m coincide.

In moving the Y roots to pass from h_m to k_m the greatest migration along the arc is from t_m/m to π/m. Hence

$$|k_m(1)| \geqq (c_{10}/t_m)^Y |h_m(1)|. \tag{6}$$

Outside the arc C the movement of roots tends to increase h_m; the worst place is right at the end points of C and there we have the similar estimate

$$|k_m(x)| \leqq (c_{11} t_m)^Y |h_m(x)| \tag{7}$$

outside C. Now k_m has roots all through B spaced $2\pi/m$ apart, and $k_m \neq x^m - 1$. By Lemma 1, k_m must assume its maximum at a point x_0 outside C. Then, applying (3), (7), (6), and (4) in succession, we obtain

$$\begin{aligned} |g_m(x_0)| &> (c_{11} t_m)^{-Y} (c_{10}/t_m)^Y \exp(c_6 t_m) \\ &= (c_{12}/t_m)^{2Y} \exp(c_6 t_m) \\ &> \exp(c_5 t_m), \end{aligned}$$

which completes the proof of Lemma 5.

PROOF OF THEOREM 2. Take $n = 2 \cdot 3 \cdot 5 \cdots p_k$. It is well known that $|F_n(1)| = 1$. In view of Lemma 4, we may apply Lemma 5 with m, $g_m(x)$, t_m, ϵ replaced by $\phi(n)$, $F_n(x)$, $p_k^{4/3}$ and $1/6$ respectively. The conclusion is precisely Theorem 2.

Theorem 2 is probably not the best result. It should not be difficult to extend the method to show that

$$A_n > \exp(\log n)^k$$

for every k and infinitely many n. A very much stronger result may be true, namely

$$A_n > \exp(c_{13} n/\log\log n) \tag{8}$$

for infinitely many n. If true, this would be essentially the best possible result, because for a certain c_{14} and all n,

$$A_n < \exp(c_{14} n/\log\log n).$$

(The proof is omitted.)

The possibility that (7) may be true is indicated in the following theorem.

THEOREM 3. *Let n be the product of k distinct primes $p_1, p_2, \cdots, p_k$ and denote by $f(x)$ the number of integers not greater than x which are relatively prime to n. Let*

$$P=(1-1/p_1)\cdots(1-1/p_k),$$
$$g(x)=f(x)-Px.$$

Then there exists an x_0, $1\leqq x_0<n$, such that

$$|g(x_0)|>c_{15}2^{k/2}(\log k)^{-1/2}. \tag{9}$$

The connection between Theorem 3 and (8) is as follows. The function $g(x)$ measures how much the roots of $F_n(x)$ are displaced from the uniform distribution. Lemma 5 then suggests that it might be possible to prove

$$\max_{|x|=1}|F_n(x)|>\exp\left[c_{16}2^{k/2}(\log k)^{-1/2}\right]. \tag{10}$$

If in particular we take $n=2\cdot 3\cdot 5\cdots p_k$, then

$$p_k\sim\log n\sim k\log k,$$

and (10) is a result similar to (8).

PROOF OF THEOREM 3. The usual sieve process gives

$$f(x)=[x]-\sum_{p|n}\left[\frac{x}{p}\right]+\sum_{pq|n}\left[\frac{x}{pq}\right]-\cdots=\sum_{r|n}\mu(r)[x/r].$$

Define $(x/r)=x/r-[x/r]$, so that $g(x)=\sum_{r|n}\mu(r)(x/r)$. Then

$$\sum_{x=1}^{n}[g(x)]^2=\sum_{r,s|n}\mu(r)\mu(s)\sum_{x=1}^{n}(x/r)(x/s).$$

Let $r=ud$, $s=vd$, $(u,v)=1$. Then the final sum becomes

$$\begin{aligned}\sum_{x=1}^{n}(x/r)(x/s)&=nd(rs)^{-2}\sum_{a=0}^{d-1}[a+a+d+\cdots+a+(u-1)d]\\&\quad\cdot[a+a+d+\cdots+a+(v-1)d]\\&=n(3rs-3r-3s+d^2+2)/12rs.\end{aligned}$$

In carrying out the second summation, the first three terms vanish. Hence

$$\begin{aligned}12\sum_{x=1}^{n}[g(x)]^2&=n\sum_{r,s|n}(d^2+2)\mu(r)\mu(s)/rs\\&=n(2^kP+2P^2).\end{aligned}$$

Now $P > c_{17}/\log k$, as follows a fortiori from Lemma 3. Hence

$$\sum_{x=1}^{n} [g(x)]^2 > c_{18} n 2^k / \log k,$$

from which the existence of an x_0 satisfying (9) follows at once.

I am indebted to Dr. Irving Kaplansky who shortened some of the proofs and extensively revised the first draft of the manuscript.

UNIVERSITY OF MICHIGAN