PORTUGALIAE MATHEMATICA
Vol. 8 — Fasc. 2 — 1949

ON THE COEFFICIENTS OF THE CYCLOTOMIC POLYNOMIAL

by P. ERDÖS (at SYRACUSE, N. Y.)

(Recebido em 1949, Novembro, 8)

The cyclotomic polynomial $F_n(x)$ is defined as the polynomial of highest coefficient 1 whose roots are the primitive nth roots of unity. It is well known that the degree of $F_n(x)$ is $\varphi(n)$ and all its coefficients are integers. Further it is well known that $F_n(x)$ is given by the following formula

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

Denote by A_n the greatest coefficient of $F_n(x)$ (in absolute value). For $n<105$, $A_n=1$. For $n=105$, $A_n=2$. I. Schur proved that $\overline{\lim}\, A_n=\infty$. Emma Lehmer[1] proved that $A_n>cn^{1/3}$ for infinitely many n, and I proved that $A_n>\exp((\log n)^{4/3})$, for infinitely many n.[2] Bateman[3] found a very simple proof that for a suitable c_1 and all n

$$(1) \qquad A_n < \exp(n^{c_1/\log \log n}), \quad (\exp z = e^z).$$

In the present note I prove that for suitable c_2 we have for infinitely many n

$$(2) \qquad A_n > \exp(n^{c_2/\log \log n}).$$

Thus (1) and (2) determine the right order of magnitude of $\log \log A_n$. The proof of (2) will be very similar to that of $A_n>\exp((\log n)^{4/3})$, but the present paper can be read without reference to the previous one.

[1] *Bull. Amer. Math. Soc.* vol. 42 (1936) pp. 389-392.

[2] *Bull. Amer. Math. Soc.*, vol. 52 (1946) pp. 179-184.

[3] To be published in *Bull. Amer. Math. Soc.*

Since

$$\max_{|z|=1} |F_n(z)| \leq A_n(\varphi(n)+1),$$

(2) will immediately follow from the following

THEOREM. *For infinitely many* n

$$\max_{|z|=1} |F_n(z)| > \exp\left(n^{c_1/\log\log n}\right).$$

Let m be large; denote by $p_1 < p_2, \cdots$ the consecutive primes $\geq m$. Define

$$n = p_1 p_2 \cdots p_k,\ k = [m^{1/10}].$$

A well known theorem of Ingham[1] states that the number of primes in $(m, m+m^{5/8})$ is greater than $m^{5/8}/(2\log m) > k$. Thus

(3) $$p_k < m + m^{5/8}$$

Hence

(4) $m^k < n < (m+m^{5/8})^k$ or $n = (1+o(1))\, m^k$ (since $k \leq m^{1/10}$).

By $\varphi(x, n)$ we denote the number of integers $\leq x$ which are relatively prime to n. Put $t = \left[\dfrac{k}{10^5}\right]$. Then for $r < 2t$ we evidently have

(5) $$\binom{k}{r} \Big/ \binom{k}{r-1} = \frac{k-r+1}{r} > 49999.$$

Put

$$\sum_r = \sum \frac{1}{p_{i_1} \cdots p_{i_r}},\ \sum_r(x) = \sum \left[\frac{x}{p_{i_1} \cdots p_{i_r}}\right],$$

where the summation extends over all distinct sets of primes taken r at a time from $p_1, p_2, \cdots, p_k$.

Now we have to prove a few lemmas:

LEMMA 1. *Let* $1 \leq s \leq p_1^{1/10}$, *define the interval* I_s as $(s+1/4)\, p_1^{2t-1} \leq x \leq (s+3/4)\, p_1^{2t-1}$. Then if x is in I_s we have

$$\varphi(x, n) > x\frac{\varphi(n)}{n} + \frac{1}{10}\binom{k}{2t-1}.$$

We have by the Sieve of Eratosthenes

$$\varphi(x, n) = x - \sum_1(x) + \sum_2(x) - \cdots - \sum_{2t-1}(x),$$

1 *Quart. J. Math. Oxford Ser.*, vol. 8 (1937) pp. 255-266.

(since $\sum_{2t}(x)=\sum_{2t+1}(x)=\cdots=0$). Now as in (4) (if $p_1>m$ is sufficiently large)

$$p_1^{2t-1}<p_{i_1}\cdots p_{i_{2t-1}}<p_k^{2t-1}<p_1^{2t-1}\left(1+\frac{1}{p_1^{3/8}}\right)^{p_1^{1/10}}<p_1^{2t-1}[1+O(p_1^{-1/4})].$$

Hence trivially

$$\frac{x}{p_{i_1}\cdots p_{i_{2t-1}}}-\left[\frac{x}{p_{i_1}\cdots p_{i_{2t-1}}}\right]>\frac{1}{5}$$

(since $s\,p_{i_1}\cdots p_{i_{2t-1}}=s\,p_1^{2t-1}+O(p_1^{2t-1}/p_1^{1/8})=s\,p_1^{2t-1}+o(p_1^{2t-1})$.

Thus by omitting the square brackets we evidently have

$$\varphi(x,n)>x(1-\textstyle\sum_1+\sum_2-\cdots-\sum_{2t-1})+\frac{1}{5}\binom{k}{2t-1}-\binom{k}{2t-2}-$$
$$-\binom{k}{2t-4}-\cdots>x(1-\textstyle\sum_1+\sum_2-\cdots)+x\sum_{2t}+\frac{1}{6}\binom{k}{2t-1}$$

since $\sum_1>\sum_2>\cdots$, and by (5)

$$\binom{k}{2t-2}+\binom{k}{2t-4}+\cdots<2\binom{k}{2t-2}<\binom{k}{2t-1}\Big/30.$$

Further

$$\textstyle\sum_{2t}<\binom{k}{2t}\Big/p_1^{2t}<\frac{k}{t}\binom{k}{2t-1}\Big/p_1^{2t}<2\cdot10^5\binom{k}{2t-1}\Big/p_1^{2t}$$

Thus finally

$$\varphi(x,n)>x\frac{\varphi(n)}{n}-10^6\binom{k}{2t-1}\Big/p_1^{9/10}+\frac{1}{6}\binom{k}{2t-1}>x\frac{\varphi(n)}{n}+\frac{1}{10}\binom{k}{2t-1}$$

for sufficiently large p_1, which proves lemma 1.

LEMMA 2. *Define the interval* I_s as $((s-1/4)\cdot p_1^{2t-1}\leqq x\leqq(s+1/4)p_1^{2t-1})$, $1\leqq s\leqq p_1^{1/10}$. *Then if* x *is in* I_s

$$\varphi(x,n)>x\frac{\varphi(n)}{n}-3\binom{k}{2t-2}.$$

We have for the x in I_s (as in the proof of lemma 1)

$$\varphi(x,n)=x-\textstyle\sum_1(x)+\cdots-\sum_{2t-1}(x)>x(1-\sum_1+\cdots-\sum_{2t-1})-$$
$$-\binom{k}{2t-2}-\binom{k}{2t-4}-\cdots>x\frac{\varphi(n)}{n}-x\textstyle\sum_{2t}-2\binom{k}{2t-2}>$$
$$>x\frac{\varphi(n)}{n}-3\binom{k}{2t-2}$$

since as in the proof of lemma 1

$$x\sum_{2t} < x\binom{k}{2t}\Big/p_1^{2t} < 2\binom{k}{2t}\Big/p_1^{9/10} < \binom{k}{2t-2},$$

which proves lemma 2.

LEMMA 3. *Let* $p_1^{2r-1} \leqq x \leqq p_1^{2r}$. *Then*

$$\varphi(x, n) > x\frac{\varphi(n)}{n} - 2\binom{k}{2t}.$$

We have for $p_1^{2r-1} \leqq x \leqq p_1^{2r}$ (as in the proof of lemma 1)

$$\varphi(x, n) = x - \sum_1(x) + \cdots - \sum_{2r-1}(x) > x(1 - \sum_1 + \cdots - \sum_{2r-1}) -$$

$$- \binom{k}{2r-2} - \binom{k}{2r-4} - \cdots > x\frac{\varphi(n)}{n} - x\sum_r - 2\binom{k}{2r-2} >$$

$$> x\frac{\varphi(n)}{n} - p_1^{2r}\binom{k}{2r}\Big/p_1^{2r} - 2\binom{k}{2r-2} > x\frac{\varphi(n)}{n} - 2\binom{k}{2r} \quad \text{q. e. d.}$$

LEMMA 4. *Let* $p_1^{2r-2} \leqq x \leqq p_1^{2r-1}$. *Then*

$$\varphi(x, n) > x\frac{\varphi(n)}{n} - 2\binom{k}{2r-2}.$$

We have for $p_1^{2r-2} \leqq x \leqq p_1^{2r-1}$ (as in the proof of lemma 1).

$$\varphi(x, n) = x - \sum_1(x) + \cdots + \sum_{2r-2}(x) > x(1 - \sum_1 + \cdots + \sum_{2r-2}) -$$

$$- \binom{k}{2r-2} - \binom{k}{2r-4} - \cdots > x(1 - \sum_1 + \cdots) - 2\binom{k}{2r-2} =$$

$$= x\frac{\varphi(n)}{n} - 2\binom{k}{2r-2} \qquad \text{q. e. d.}$$

Let $1 = a_1 < a_2 < \cdots < a_{\varphi(n)/2}$ be the integers $< n/2$ relatively prime to n. The roots of $F_n(z)$ are clearly of the form

$$x_j = \exp(2\pi i a_j/n), \bar{x}_j = \exp(-2\pi i a_j/n).$$

Put $A = (p_1^{1/10} + 3/4)\, p_1^{2t-1}$ and denote by I, the arc

$$I = [\exp(2\pi i A/n), \exp(-2\pi i A/n)].$$

Let $x_i, \bar{x}_i, i = 1, 2, \cdots, U$ be the roots of $F_n(z)$ in I. These x_i clearly correspond to the a_i satisfying $1 \leqq a_i \leqq (p_1^{1/10} + 3/4)p_1^{2t-1}$. In other words

$$U = \varphi[(p_1^{1/10} + 3/4)\, p_1^{2t-1}, n) = \varphi(A, n).$$

Define the polynomial $G_n(z)$ of highest coefficient 1 and degree $\varphi(n)$ as follows:

$$G_n[\exp(\pm 2\pi j i/\varphi(n))] = 0 \quad \text{for} \quad 1 \leqq j \leqq U,$$
$$G_n[\exp(\pm 2\pi a_j i/n)] = 0 \quad \text{for} \quad j > U.$$

A theorem of TURÁN-RIESZ[1] states that if a polynomial of degree m assumes its absolute maximum in the unit circle at z_0 and x_0 is the closest of its root on the unit circle, then the arc (z_0, x_0) is $\geqq \pi/n$, equality only for $z^n - e^{i\alpha}$, α neal.

Now we estimate

$$\left|\frac{G_n(1)}{F_n(1)}\right| = \prod_{i=1}^{U}\left|\frac{1-y_i}{1-x_i}\right|^2 \tag{6}$$

where $y_i, \bar{y}_i$ denote the roots of $G_n(z)$. (6) is evident since all but the first U roots of $F_n(z)$ and $G_n(z)$ coincide. Next we write

$$\prod_{i=1}^{U}\left|\frac{1-y_i}{1-x_i}\right|^2 = \Pi_1 \cdot \Pi_2 \cdot \Pi_3 \cdot \Pi_4$$

where in Π_1, i is such that a_i is in one of the intervals $I_s\, 1 \leqq s \leqq p_1^{1/10}$ (for the definition of I_s see lemma 1), in Π_2, a_i is in one of the I'_s (see lemma 2), in Π_3, $p_1^{2r-1} \leqq a_i < p_1^{2r}$ $2 \leqq 2r \leqq 2t-2$, and in Π_4, $p_1^{2r-2} \leqq$ $\leqq a_i < p_1^{2r-1}$, $1 \leqq 2r-1 \leqq 2t-1$. Further we write

$$\Pi_1 = \Pi_1^{(1)} \cdot \Pi_1^{(2)} \cdots \Pi_1^{[p_1^{1/10}]}$$

where in $\Pi_1^{(s)}$, a_i is in one of the I_s. It follows from lemma 1 that if a_i is in any of the I_s then y_i is farther from 1 than x_i and in fact the length of the arc (x_i, y_i) is greater than

$$\frac{2\pi}{10\,\varphi(n)}\binom{k}{2t-1} > \frac{2\pi}{10\,n}\binom{k}{2t-1}$$

A very simple calculation then shows that (since in I_s, $1-x_i <$ $< 2\pi(s+1)\,p_1^{2t-1}/n$)

$$\left|\frac{1-y_i}{1-x_i}\right| > 1 + \frac{\binom{k}{2t-1}}{30\,(s+1)\,p_1^{2t-1}}.$$

The number of the x_i in I_s is clearly greater than

$$\frac{1}{2}p_1^{2t-1}\left(1 - \sum_{i=1}^{k}\frac{1}{p_i}\right) > \frac{1}{3}p_1^{2t-1}.$$

[1] M. RIESZ, *Jber. Deutschen Math. Verein.* vol. 23 (1914) pp. 354-368; P. TURÁN, *Acta Univ. Szeged.* vol. 11 (1946) pp. 106-113.

Thus
$$\Pi_1^{(s)} > \left(1 + \frac{1}{30}\binom{k}{2t-1}\Big/[(s+1)p_1^{2t-1}]\right)^{2/3\, p_1^{2t-1}}.$$

Hence

$$(7)\quad \log(\Pi_1^{(s)}) > \frac{2}{3}p_1^{2t-1}\left[\frac{\binom{k}{2t-1}}{30(s+1)p_1^{2t-1}} - \frac{1}{2}\left(\frac{\binom{k}{2t-1}}{30(s+1)p_1^{2t-1}}\right)^2\right] >$$
$$> \frac{1}{50}\binom{k}{2t-1}\Big/s+1$$

since
$$\binom{k}{2t-1} < \frac{k^{2t-1}}{(2t-1)!} < \frac{p_1^{2t-1}}{(2t-1)!}$$

Thus from (7)
$$(8)\qquad \log(\Pi_1) > \sum_{s\le p_1^{1/10}} \log(\Pi_1^{(s)}) > \frac{\log p_1}{600}\binom{k}{2t-1}.$$

Now we estimate Π_2. We write
$$\Pi_2 = \prod_{1\le s\le p_1^{1/10}} (\Pi_2^{(s)}),$$

where in $\Pi_2^{(s)}, a_i$ is in I_s. From lemma 2 we obtain (as in the estimation of $\Pi_1^{(s)}$) for the a_i in I_s

$$\left|\frac{1-y_i}{1-x_i}\right| > 1 - \frac{4\binom{k}{2t-2}}{(s-1/4)p_1^{2t-1}} \quad \left(\text{since } \frac{\Phi(n)}{n} > 1 - \sum_{i=1}^{k}\frac{1}{p_i} > \frac{3}{4}\right).$$

The number of the a_i 's in I_s in evidently $< \frac{1}{2}p_1^{2t-1}$. Hence

$$\Pi_2^{(s)} > \left(1 - \frac{4\binom{k}{2t-2}}{(s-1/4)p_1^{2t-1}}\right)^{p_1^{2t-1}}$$

or (as in the estimation of $\log \Pi_1^{(s)}$)
$$\log \Pi_2^{(s)} > -5\binom{k}{2t-2}\Big/s-1/4.$$

Hence finally
$$(9)\qquad \log(\Pi_2) = \sum_{1\le s\le p_1^{1/10}} \log(\Pi_2^{(s)}) > -\binom{k}{2t-2}\log p_1.$$

Now we estimate Π_3. We write
$$\Pi_3 = \prod_{r=1}^{t-1} (\Pi_3^{(r)}),$$

where in $\Pi_3^{(r)}$, $p_1^{2r-1} \leqq a_i \leqq p_1^{2r}$. Now

$$\Pi_3^{(r)} = \prod_{t=1}^{p_1-1} (\Pi_3^{(r)}(t)),$$

where in $\Pi_3^{(r)}(t)$, $t p_1^{2r-1} \leqq a_i \leqq (t+1) p_1^{2r-1}$. For the a_i in $\Pi_3^{(r)}(t)$ we have from lemma 3 (as in the estimation of Π_1 and Π_2)

$$\left|\frac{1-y_i}{1-x_i}\right| > 1 - \frac{3\binom{k}{2r}}{t p_1^{2r-1}}$$

and the number of a's in $t p_1^{2r-1} \leqq a_i \leqq (t+1) p_1^{2r-1}$ is $\leqq p_1^{2r-1}$. Thus (as in the estimation of Π_1 and Π_2)

$$\log(\Pi_3^{(r)}(t)) > -4\binom{k}{2r}\Big/t$$

and hence

$$\log(\Pi_3^{(r)}) > -5\binom{k}{2r}\log p_1 .$$

Thus finally

$$(10) \qquad \log(\Pi_3) > -5\log p_1\left[\binom{k}{2t-2} + \binom{k}{2t-4} + \cdots\right] >$$

$$> -6\binom{k}{2t-2}\log p_1 .$$

In the same way we obtain

$$(11) \qquad \log(\Pi_4) > -6\binom{k}{2t-2}\log p_1 .$$

Thus we obtain from (8), (9), (10) and (11)

$$\log(\Pi_1) + \log(\Pi_2) + \log(\Pi_3) + \log(\Pi_4) > \log p_1\left[\binom{k}{2t-1}\Big/600 - \right.$$

$$\left. -13\binom{k}{2t-2}\right] > \binom{k}{2t-2}\log p_1/1000 ,$$

or

$$(12) \qquad |G_n(1)| > \exp\left[\frac{\binom{k}{2t-1}\log p_1}{1000}\right],$$

since n has more than one distinct prime factor, and thus $F_n(1)=1$.

Assume now that $G_n(z)$ assumes its absolute maximum in the unit circle at z_0. Without loss of generality we can assume that the real part of z_0 is positive. By the previously quoted theorem of TURÁN-RIESZ[1] z_0 cannot lie on the arc

$$\left\{\exp\left(-2\pi i\frac{U}{\varphi(n)}\right),\ \exp\left(2\pi i\frac{U}{\varphi(n)}\right)\right\}.$$

Now we estimate $G_n(z_0)/F_n(z_0)$. We have

$$\left|\frac{G_n(z_0)}{F_n(z_0)}\right| = \prod_{a_i \text{ in } I} \frac{(z_0-y_i)(z_0-\overline{y}_i)}{(z_0-x_i)(z_0-\overline{x}_i)}$$

Now we make use of the well known and elementary result that $(z_0-z)(z_0-\overline{z})$ increases as z moves away from z_0 towards 1. Hence

$$\left|\frac{G_n(z_0)}{F_n(z_0)}\right| < \prod_{\substack{s=1\\ a_i \text{ in } I_s'}}^{p_1^{1/10}} \left|\frac{(z_0-y_i)(z_0-\overline{y}_i)}{(z_0-x_i)(z_0-\overline{x}_i)}\right| \prod_{a_i<p_1^{2t-1}} \left|\frac{(z_0-y_i)(z_0-\overline{y}_i)}{(z_0-x_i)(z_0-\overline{x}_i)}\right|,$$

since for the a_i in I_s' and the $a_i \leqq p_1^{2t-1}$ we cannot assume that y_i is farther from 1 (i. e. closer to z_0) than x_i. Further trivially

$$\left|\frac{G_n(z_0)}{F_n(z_0)}\right| < \prod_{\substack{s=1\\ a_i \text{ in } I_s'}}^{p_1^{1/10}} \left(1+\left|\frac{y_i-x_i}{z_0-x_i}\right|\right) \prod_{a_i<p_1^{2t-1}} \left(1+\left|\frac{y_i-x_i}{z_0-x_i}\right|\right)$$

The arc (y_i, x_i) may (by lemma 2) be assumed to be less than $6\pi\binom{k}{2t-2}/\varphi(n)$ and since z_0 is not on the arc, $\exp(-2\pi i\,U/\varphi(n))$, $\exp(2\pi i U/\varphi(n))$, the arc (z_0, x_i) is greater than $2\pi p_1^{2t-1}([p_1^{1/10}]-s+1/2)/n$, if a_i is in I_s'. Thus for the a_i in I_s' (by a simple calculation)

$$\left|\frac{y_i-x_i}{z_0-x_i}\right| < \frac{4\binom{k}{2t-2}}{([p_1^{1/10}]-s+1/2)\,p_1^{2t-1}}.$$

The number of the a_i with x_i in I_s' is clearly less than $\frac{1}{2}p_1^{2t-1}$. Thus

$$\sum_{\substack{s=1\\ a_i \text{ in } I_s'}}^{p_1^{1/10}} \log\left(1+\left|\frac{y_i-x_i}{z_0-x_i}\right|\right) < 4\binom{k}{2t-2}\sum_{s\leqq p_1^{1/10}} \frac{1}{s-1/2} < \binom{k}{2t-2}\log p_1.$$

Similarly for the $a_i<p_1^{2t-1}$, $\left|\frac{y_i-x_i}{z_0-x_i}\right| < 10\binom{k}{2t-2}\Big/p_1^{2t-1+1/10}$ (by lemmas 3 and 4). Thus

$$\sum_{a_i<p_1^{2t-1}} \log\left(1+\left|\frac{y_i-x_i}{z_0-x_i}\right|\right) < 10\binom{k}{2t-2}\Big/p_1^{1/10} < \binom{k}{2t-2}.$$

[1] Reference 1, p. 67.

Hence finally

$$\log|G_n(z_0)| - \log|F_n(z_0)| < 2\binom{k}{2t-2}\log p_1 . \tag{13}$$

In fact it is very likely that $|G_n(z_0)| < |F_n(z_0)|$, but (13) suffices for our purpose.

Now we can prove our theorem. We obtain from $|G_n(z_0)| > |G_n(1)|$, (12) and (13)

$$\log|F_n(z_0)| > \log|G_n(z_0)| - 2\binom{k}{2t-2}\log p_1 > \log|G_n(1)| -$$

$$-2\binom{k}{2t-2}\log p_1 > \log p_1\left[\binom{k}{2t-1}\Big/1000 - 2\binom{k}{2t-2}\right] >$$

$$> \binom{k}{2t-1}\frac{\log p_1}{2000} > \left(\frac{k}{2t-1}\right)^{2t-1}\frac{\log p_1}{2000} > \left(\frac{k}{2t}\right)^{2t} > e^{k/5000} .$$

Now from (4)

$$k = (1+o(1))\frac{\log n}{\log m} = (1+o(1))\frac{\log n}{10\log k}$$

or

$$k = (1+o(1))\frac{\log n}{10\log\log n} > \frac{\log n}{20\log\log n} .$$

Hence finally

$$\log|F_n(z_0)| > e^{\log n/(10^5 \log\log n)} = n^{1/(10^5\cdot\log\log n)} \qquad \text{q. e. d.}$$

By the same method we could prove that there exist two consecutive roots of $F_n(z)$, x_i and x_{i+1}, so that everywhere on (x_i, x_{i+1})

$$\log|F_n(z_0)| < -n^{c/\log\log n} .$$