ON THE GROWTH OF THE CYCLOTOMIC POLYNOMIAL IN THE INTERVAL (0, 1)

by P. ERDÖS

(Received 16th November, 1956)

Let

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

be the nth cyclotomic polynomial, and denote by A_n the absolute value of the largest coefficient of $F_n(x)$. Schur proved that

$$\lim_{n\to\infty} \sup A_n = \infty,$$

and Emma Lehmer [5] showed that $A_n > cn^{1/3}$ for infinitely many n; in fact she proved that n can be chosen as the product of three distinct primes. I proved [3] that there exists a positive constant c_1 such that, for infinitely many n,

$$A_n > \exp\{n^{c_1/\log\log n}\}, \quad \text{...(1)}$$

and Bateman [1] proved very simply that, for every $\epsilon > 0$ and all $n > n_0(\epsilon)$,

$$A_n < \exp\{n^{(1+\epsilon)\log 2/\log\log n}\}.$$

My proof of (1) followed immediately from the fact that, for infinitely many n,

$$\max_{|x|\leqslant 1} |F_n(x)| > \exp\{n^{c_2/\log\log n}\}. \quad \text{....................................(2)}$$

The proof of (2) was quite complicated.

Some time ago Kanold* asked me if I could estimate the growth of $|F_n(x)|$ in the interval (0, 1). I have now found a very simple proof that there exists a positive constant c_3 such that, for infinitely many n,

$$\max_{0\leqslant x\leqslant 1} |F_n(x)| > \exp\{n^{c_3/\log\log n}\}, \quad \text{...................................(3)}$$

which, of course, implies (2) and therefore (1).

I conjecture that (3) is satisfied for every $c_3 < \log 2$, so that Bateman's result is best possible.

Proof of (3). It follows easily from the Prime Number Theorem, or from the more elementary result

$$\pi(x) > \tfrac{1}{2}\frac{x}{\log x},$$

that there are arbitrarily large integers t for which

$$\pi(t + t^{1/4}) - \pi(t) > \tfrac{1}{10} t^{1/4}/\log t.$$

Denote by $p_1, p_2, \ldots, p_k$, where $k > \frac{1}{10} t^{1/4}/\log t$, the primes in the interval $(t, t + t^{1/4})$ in ascending order of magnitude. Put $n = \prod_{i=1}^{k} p_i$, and

$$F_n(x) = F_n^{(1)}(x) F_n^{(2)}(x), \quad \text{...(4)}$$

where, in $F_n^{(1)}(x)$, d runs through the divisors of n satisfying $v(n/d) \leqslant l$. Here l is the greatest integer less than $\frac{1}{2}(k-2)$ which satisfies $l \not\equiv k \pmod 2$, and $v(d)$ denotes the number of distinct

* Oral communication.

https://doi.org/10.1017/S2040618500033517 Published online by Cambridge University Press

prime factors of d. Put

$$x = 1 - p_1^{-l-\frac{1}{2}}.$$

Clearly, if $v(n/d) > l$, then $n/d > p_1^{l+1}$. Thus

$$|x^{n/d} - 1| > 1 - (1 - p_1^{-l-\frac{1}{2}})^{p_1^{l+1}} > 1 - \exp(-p_1^{1/2}).$$

Hence

$$|F_n^{(2)}(x)| > \{1 - \exp(-p_1^{1/2})\}^{2^k} > \tfrac{1}{4}, \qquad \text{.................................(5)}$$

since $\exp(p_1^{1/2}) > 2^k$ (because $p_1 > k^4$).

We now estimate $|F_n^{(1)}(x)|$. Assume that $v(n/d) = r \leqslant l$.
Then, clearly, since $r \leqslant k \leqslant p_1^{1/4}$,

$$p_1^r < \frac{n}{d} < p_k^r,$$

so that

$$p_1^r < \frac{n}{d} < (p_1 + p_1^{1/4})^r < p_1^r(1 + 2p_1^{-1/2}).$$

Thus

$$1 - (1 - p_1^{-l-\frac{1}{2}})^{n/d} = \frac{n}{dp_1^{l+\frac{1}{2}}} + O\left(\frac{n^2}{d^2 p_1^{2l+1}}\right) = \frac{1}{p_1^{l-r+\frac{1}{2}}}\{1 + O(p_1^{-\frac{1}{2}})\}. \qquad \text{...............(6)}$$

We therefore have, from (6) and the definition of $F_n^{(1)}(x)$,

$$|F_n^{(1)}(x)| > p_1^L\{1 + O(p_1^{-1/2})\}^{-2^k}, \qquad \text{.................................(7)}$$

where

$$\begin{aligned} L &= -\sum_{r=0}^{k} (-1)^{k-l+r}(r + \tfrac{1}{2})\binom{k}{l-r} \\ &= -\sum_{r=0}^{k} (-1)^{k-l+r}\, r\binom{k}{l-r} + \tfrac{1}{2}\sum_{r=0}^{k} (-1)^{k-l+r}\binom{k}{l-r} \\ &= (-1)^{k-l+1}\left\{\binom{k-2}{l} - \tfrac{1}{2}\binom{k-1}{l}\right\}. \end{aligned}$$

Thus, from the definition of l and by a simple computation, we obtain

$$L > \frac{1}{2k}\binom{k-2}{l} > c_4 k^{-3/2} 2^k. \qquad \text{...................................(8)}$$

It follows from (7) and (8), since $p_1 > k^4$, that

$$|F_n^{(1)}(x)| > \exp\{c_4 k^{-3/2} 2^k \log p_1 - c_5 2^k p_1^{-1/2}\} > \exp(c_6 k^{-3/2} 2^k). \qquad \text{...............(9)}$$

Thus, from (4), (5) and (9),

$$|F_n(x)| > \tfrac{1}{4}\exp(c_6 k^{-3/2} 2^k). \qquad \text{...................................(10)}$$

Now

$$n = p_1 p_2 \ldots p_k < (p_1 + p_1^{1/4})^k < 2p_1^k < 2\exp(5k\log k), \text{........................(11)}$$

since

$$p_1 < t + t^{1/4} < (\tfrac{1}{10} t^{1/4}/\log t)^5 < k^5,$$

and (1) follows immediately from (10) and (11).

https://doi.org/10.1017/S2040618500033517 Published online by Cambridge University Press

Denote by $\phi(n, k)$ the number of integers m such that $1 \leqslant m \leqslant k$ and $(m, n) = 1$. Clearly

$$\phi(n, k) = k \prod_{p|n} \left(1 - \frac{1}{p}\right) + \alpha 2^{v(n)-1}, \text{ where } -1 < \alpha < 1. \qquad \text{(12)}$$

I have proved [2] that, for every n, there exists a k such that

$$\left| \phi(n, k) - k \prod_{p|n} \left(1 - \frac{1}{p}\right) \right| > c_7 2^{\frac{1}{4} v(n)} / \log v(n),$$

and conjectured [2] that the error term in (12) is $o(2^{v(n)})$ for $v(n) \to \infty$. Vijayaraghavan [6] and Lehmer [4] disproved this conjecture, and in fact Vijayaraghavan proved that in (12) α can come as near as one wishes to both -1 or $+1$.

Now one can pose the following problem : Let $n \leqslant x$; then, from

$$v(n) < (1 + \epsilon) \log x / \log \log x$$

and (12), we obtain

$$\phi(n, k) = k \prod_{p|n} \left(1 - \frac{1}{p}\right) + O\{2^{(1+\epsilon) \log x / \log \log x}\}. \qquad \text{(13)}$$

I believe that the error term in (13) cannot be replaced by

$$O\{2^{(1-c_8) \log x / \log \log x}\}.$$

If this could be proved it might enable one to show that (3) holds for every $c_3 < \log 2$.

REFERENCES

1. P. T. Bateman, Note on the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc.* 55 (1949), 1180–1181.

2. P. Erdös, On the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc.*, **52** (1946), 179–184.

3. P. Erdös, On the coefficients of the cyclotomic polynomial, *Portugaliae Math.*, **8** (1949), 63–71.

4. D. H. Lehmer, The distribution of totatives, *Canadian Math. J.*, **7** (1955), 347–357.

5. Emma Lehmer, On the magnitude of the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.

6. T. Vijayaraghavan, On a problem in elementary number theory, *J. Indian Math. Soc.* (N.S.), **15** (1951), 51–56.

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY
BIRMINGHAM