# BOUNDS FOR THE $r$-th COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

P. ERDŐS AND R. C. VAUGHAN

## 1. *Introduction*

We consider the cyclotomic polynomials

$$\Phi_n(z) = \prod_{\substack{m=1 \\ (m,n)=1}}^{n} (z - e(m/n)), \tag{1}$$

where $e(\alpha) = e^{2\pi i \alpha}$, and write $\Phi_n$ in the form

$$\Phi_n(z) = \sum_{r=0}^{\phi(n)} a_r(n) z^r, \tag{2}$$

where $\phi$ is Euler's function.

Bounds for $a_r(n)$ in terms of $n$ have been obtained by a number of people **[1, 3, 4, 5, 6, 12, 13, 14, 16]**. Bateman **[2]** has shown that

$$|a_r(n)| < \exp(n^{c/\log\log n})$$

and Erdős **[7, 8]** has shown that this is best possible.

Mirsky has mentioned in conversation that it is possible to obtain a bound for $a_r(n)$ which is independent of $n$. Moreover, Möller **[15**; (9) and Satz 3] has shown that

$$|a_r(n)| \leqslant p(r) - p(r-2), \tag{3}$$

where $p(m)$ is the number of partitions of $m$, and also that

$$\max_n |a_r(n)| > r^m \; (r \geqslant r_0(m)). \tag{4}$$

There is clearly a close connection between the size of $a_r(n)$ and the values $\Phi_n(z)$ takes as $|z| \to 1-$. Thus we first of all prove

THEOREM 1. *For each $z$ with $|z| < 1$ we have*

$$|\Phi_n(z)| < \exp\left(\tau(1-|z|)^{-1} + C_1(1-|z|)^{-3/4}\right), \tag{5}$$

*where*

$$\tau = \prod_p \left(1 - \frac{2}{p(p+1)}\right). \tag{6}$$

Although this cannot be far from the truth, we suspect that the right hand side of (5) should be

$$\exp\left(o((1-|z|)^{-1})\right)$$

as $|z| \to 1-$.

Our main theorem is

Received 1 September, 1972.

[J. LONDON MATH. SOC. (2), 8 (1974), 393–400]

THEOREM 2. *We have*

$$|a_r(n)| < \exp(2\tau^{1/2} r^{1/2} + C_2 r^{3/8}), \tag{7}$$

*and*

$$\limsup_{n\to\infty} |a_r(n)| > \exp\left(C_3 \left(\frac{r}{\log r}\right)^{1/2}\right) \quad (r > r_0). \tag{8}$$

Clearly (8) is much sharper than (4). By (6) we have $\tau < \frac{1}{2}$, and by a classical result of Hardy and Ramanujan **[10]** we have

$$\log(p(r) - p(r-2)) \sim \pi\sqrt{(\tfrac{2}{3})}\, r^{1/2}$$

as $r \to \infty$. Thus we see that (7) is stronger than (3).

In view of our remark following Theorem 1, we expect that

$$\max_n |a_r(n)| < \exp(o(r^{1/2})) \tag{9}$$

as $r \to \infty$. We also believe that (8) should hold for $\limsup a_r(n)$ and $-\liminf a_r(n)$, but we have been unable to prove this for all $r$. If we write $r = 2^m t$ where $t$ is odd, then we can combine our proof of (8) with the relationship

$$\Phi_{2^{m+1}n}(z) = \Phi_n(-z^{2^m}) \qquad (n \text{ odd})$$

to obtain the lower bound

$$\exp\left(C_3 \left(\frac{t}{\log t}\right)^{1/2}\right) \quad (t > t_0)$$

in each case, but this is weaker if $m$ is large.

A question suggests itself in connection with this. If $f_X(n)$ is the number of partitions of $n$ into primes between $X$ and $2X$, then how large does $n$ have to be before $f_X$ is a monotone increasing function of $n$? Possibly $n \gg X$ will suffice.

In §§2 and 3 we prove (5) and (7) respectively. Then in §4 we establish some lemmas which enable us to prove (8) in §5.

## 2. *Proof of Theorem* 1

It is convenient to note here that

$$\Phi_n(z) = \prod_{d|n} (1 - z^d)^{\mu(n/d)} \quad (n > 1, |z| \neq 1), \tag{10}$$

where $\mu$ is Möbius' function. This follows easily from the well known formula

$$\Phi_n(z) = \prod_{d|n} (z^d - 1)^{\mu(n/d)} \qquad (|z| \neq 1).$$

When $n = 1$, (5) is trivial. We thus assume $n > 1$ and then on appealing to (10) we obtain, for $|z| < 1$,

$$|\Phi_n(z)| = \exp\left(\sum_{d|n} \mu\left(\frac{n}{d}\right) \log|1 - z^d|\right)$$

$$= \exp\left(\operatorname{Re} \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(1 - z^d)\right),$$

where we have taken the principal value of the logarithm. Now $\log(1-z^d)$ is regular for $|z|<1$ and has the Taylor expansion

$$-\sum_{h=1}^{\infty}\frac{z^{hd}}{h}$$

in this region. We use this and interchange the order of summation to obtain

$$|\Phi_n(z)| = \exp\left(-\mathrm{Re}\sum_{j=1}^{\infty}\frac{z^j}{j}\sum_{d|n,\, d|j} d\mu\left(\frac{n}{d}\right)\right). \tag{11}$$

By Theorems 271 and 272 of Hardy and Wright [**11**] we see that the inner sum is Ramanujan's sum $c_n(j)$, and we have

$$\sum_{d|n,\, d|j} d\mu\left(\frac{n}{d}\right) = \mu\left(\frac{n}{(n,j)}\right)\phi(n)\Big/\phi\left(\frac{n}{(n,j)}\right). \tag{12}$$

By (10) it is easily seen that

$$\Phi_n(z) = \Phi_m(z^{n/m})$$

where

$$m = \prod_{p|n} p,$$

so that to prove the theorem it suffices to assume that $n$ is squarefree. Then, by (12), we have

$$\left|\sum_{d|n,\, d|j} d\mu\left(\frac{n}{d}\right)\right| \leqslant \phi((n,j)) \leqslant \phi(j_0),$$

where $j_0 = \prod_{p|j} p$. Hence, by (11),

$$|\Phi_n(z)| \leqslant \exp\left(\sum_{j=1}^{\infty}\frac{\phi(j_0)}{j}|z|^j\right). \tag{13}$$

Let $f$ be the multiplicative function with $f(p^m) = -(m-1)(p-1)^2$. Then

$$\sum_{d|j} f(d)\phi(j/d) = \phi(j_0),$$

$\sum f(d)d^{-2}$ converges absolutely to $\prod(1-(p+1)^{-2})$, and

$$\sum_{d>X}|f(d)|\, d^{-2} < X^{-1/4}\prod(1+p^{-3/2}) \ll X^{-1/4}.$$

Hence

$$\sum_{j\leqslant X}\frac{\phi(j_0)}{j} = \sum_{d\leqslant X}\frac{f(d)}{d}\left(\frac{X}{d}\prod_p(1-p^{-2})+O((X/d)^{3/4})\right) = \tau X + O(X^{3/4}).$$

A partial summation applied to the sum in (13) establishes (5).

## 3. *Proof of* (7)

We use Theorem 1 with $|z| = 1-(\tau/r)^{1/2}$, and Cauchy's inequalities for the coefficients of a power series, whence

$$|a_r(n)| < \exp(2\tau^{1/2}r^{1/2} + C_2 r^{3/8})$$

as required.

## 4. *Lemmas for the proof of* (8)

Throughout this and the next section we assume that $r$ is large,

$$X = r^{1/2}, \tag{14}$$

$$Y = \tfrac{1}{100} X (\log X)^{1/2} \tag{15}$$

and $p_j$ ($j = 1, \ldots, s$) are the $\pi(Y) - \pi(X)$ prime numbers satisfying

$$X < p_1 < \ldots < p_s \leqslant Y. \tag{16}$$

LEMMA 1. *Let $k$ be the largest integer $j$ such that $p_j < \frac{3}{2} p_1$. Then every integer $m$ with $m > C_4 X$ can be written in the form*

$$m = \sum_{j=1}^{k} h_j p_j$$

*with $h_j \geqslant 0$.*

*Proof.* Let $R(u)$ be the number of representations of $u$ as the sum of two primes $p', p''$ with $p_1 < p', p'' < \frac{3}{2} p_1$. By an application of any of the modern forms of the sieve (see, for instance, Prachar [**17**; Kapitel II, Satz 4.8]), we have

$$R(u) \ll p_1 (\log p_1)^{-2} \prod_{p \mid u} \frac{p}{p-1}.$$

Thus by Cauchy's inequality and some elementary estimates we have

$$\sum_{\substack{u \\ R(u) > 0}} 1 \gg p_1.$$

This means that there are at least $C_5 p_1 + 1$ numbers $u$, with $2p_1 < u < 3p_1$, which can be written in the form $u = p' + p''$ with $p_1 < p', p'' < \frac{3}{2} p_1$. Hence there are at least $C_5 p_1 + 1$ residue classes $u$ modulo $p_1$ so that

$$u \equiv p' + p'' \pmod{p_1}.$$

Let

$$v = [p_1 / [C_5 p_1]] + 1. \tag{17}$$

Then by repeated application of the Cauchy-Davenport theorem (for an account of which see, for instance, Theorem 15, Chapter I, of Halberstam and Roth [**9**]) we can write every residue class $u$ modulo $p_1$ in the form

$$u \equiv p_1' + p_1'' + \ldots + p_v' + p_v'' \pmod{p_1}$$

with

$$p_1 < p_j', p_j'' < \tfrac{3}{2} p_1.$$

By (17), $v$ is bounded. Let $C_4 > 6v$. Then since $2vp_1 < p_1' + \ldots + p_v'' < 3vp_1$ we are able, by subtracting a suitable multiple of $p_1$, to write every $m > \frac{1}{2} C_4 p_1$ in the form

$$m = \sum_{j=1}^{k} h_j p_j.$$

Moreover $C_4 X > \frac{1}{2} C_4 p_1$. This proves Lemma 1.

We now introduce some further notation that we require in this and the next section. Let $b_m$ be the coefficient of $z^m$ in the Taylor expansion of

$$(1 - z^{p_1})^{-1} \ldots (1 - z^{p_s})^{-1}$$

in powers of $z$, valid when $|z| < 1$. Clearly $b_m$ is just the number of different ways of choosing $h_1, \ldots, h_s$ with $h_j \geqslant 0$ so that

$$h_1 p_1 + \ldots + h_s p_s = m.$$

In addition, let

$$T = \left[\frac{1}{10} r\right] \tag{18}$$

and

$$S = p_s \left[\frac{r}{100 p_s}\right]. \tag{19}$$

LEMMA 2. *For at least one integer $m$ with $T < m \leqslant T+S$ we have*

$$b_m - b_{m-1} > \exp\left(C_6 \left(\frac{r}{\log r}\right)^{1/2}\right).$$

*Proof.* It suffices to show that

$$b_{T+S} - b_T > \exp\left(C_7 \left(\frac{r}{\log r}\right)^{1/2}\right). \tag{20}$$

Since $p_s \mid S$, $b_{T+S} - b_T$ is the number of ways of choosing $h_1, \ldots, h_s$ so that $h_j \geqslant 0$, $h_s < S/p_s$ and

$$T + S = \sum_{j=1}^{s} h_j p_j.$$

Let $g(v)$ be the number of ways of choosing $h_{k+1}, \ldots, h_{s-1}$ so that $h_j \geqslant 0$ and

$$v = \sum_{j=k+1}^{s-1} h_j p_j.$$

Then, by Lemma 1 and (14),

$$b_{T+S} - b_T \geqslant \sum_{0 \leqslant v \leqslant r/50} g(v). \tag{21}$$

This last expression is at least as large as the number of ways of choosing $h_{k+1}, \ldots, h_{s-1}$ so that $h_j \geqslant 0$ and

$$\sum_{j=k+1}^{s-1} h_j p_j \leqslant \tfrac{1}{50} r.$$

Thus, if we write

$$d = s - 1 - k = \pi(Y) - 1 - \pi(\tfrac{3}{2} p_1), \tag{22}$$

the sum in (21) is

$$\geqslant \prod_{j=k+1}^{s-1} \left(1 + \left[\frac{r}{50 d p_j}\right]\right)$$

$$> \prod_{j=k+1}^{s-1} \frac{r}{50 d p_j}.$$

Hence, by (14),

$$\sum_{0 \leqslant v \leqslant r/50} g(v) > \exp\left(d \log \frac{X^2}{50d} - \vartheta(Y) + \vartheta(\tfrac{3}{2} p_1) + \log p_s\right), \tag{23}$$

where as usual $\vartheta(x) = \sum_{p \leqslant x} \log p$.

By (14), (15), (22) and the prime number theorem with a reasonable error term,

$$d = \tfrac{1}{100}X(\log X)^{-1/2} - \tfrac{3}{2}X(\log X)^{-1} - \tfrac{1}{200}X(\log\log X)(\log X)^{-3/2}$$
$$+\tfrac{1}{100}(1+\log 100)\,X(\log X)^{-3/2} + O(X(\log X)^{-2}),$$
$$\log\frac{X^2}{50d} = \log X + \tfrac{1}{2}\log\log X + \log 2 + O((\log X)^{-1/2})$$

and

$$\vartheta(Y) - \vartheta(\tfrac{3}{2}p_1) - \log p_s = \tfrac{1}{100}X(\log X)^{1/2} - \tfrac{3}{2}X + O(X(\log X)^{-1}). \tag{24}$$

Hence

$$d\log\frac{X^2}{50d} = \tfrac{1}{100}X\,(\log X)^{1/2} + \tfrac{1}{100}(1+\log 200)\,X(\log X)^{-1/2}$$
$$-\tfrac{3}{2}X + O(X(\log\log X)(\log X)^{-1}). \tag{25}$$

By (21), (23), (24) and (25) we see that

$$b_{T+S} - b_T > \exp\left(C_7\, X(\log X)^{-1/2}\right).$$

As an immediate consequence of this and (14) we have (20), and hence the lemma.

LEMMA 3. *Suppose $m$ satisfies $T < m \leqslant T+S$. Then if $r-m$ is odd we can choose prime numbers $q_1, q_2$ and $q_3$ so that*

$$r - m = q_1 + q_2 + q_3$$

*and*

$$\tfrac{1}{4}r < q_1 < q_2 < q_3 < \tfrac{1}{3}r.$$

*On the other hand, if $r-m$ is even we can choose prime numbers $q_1, q_2, q_3$ and $q_4$ so that*

$$r - m = q_1 + q_2 + q_3 + q_4$$

*and*

$$\tfrac{1}{5}r < q_1 < q_2 < q_3 < q_4 < \tfrac{1}{4}r.$$

The above lemma follows by a straightforward application of the Hardy-Littlewood-Vinogradov method. There are a number of accounts of this method. One that springs to mind is Prachar [**17**; Kapitel VI].

## 5. *Proof of* (8)

We show that there are arbitrarily large values of $n$ for which $|a_r(n)| \geqslant \lambda$, where

$$\lambda = \tfrac{1}{625}\exp\left(C_6\left(\frac{r}{\log r}\right)^{1/2}\right). \tag{26}$$

For suppose not. Let $n_0 = p_1 \ldots p_s P$, where $P$ is a product of primes larger than $r$, chosen so that $\mu(n_0) = 1$. We first of all take $n = n_0$. By (10)

$$\Phi_n(z) = (1-z)(1-z^{p_1})^{-1} \ldots (1-z^{p_s})^{-1} \times \text{ other terms},$$

and it is easily seen that

$$a_r(n) = b_r - b_{r-1} = \Delta_0, \text{ say}.$$

Thus, by our assumption,

$$|\Delta_0| < \lambda. \tag{27}$$

Now let $P_1$ be a prime greater than $P$ and $q$ any prime with

$$p_s < q < r. \tag{28}$$

Then if $n = n_0 q P_1$ we have

$$\Phi_n(z) = (1-z)\left(\sum_{m=0}^{\infty} b_m z^m\right)\left(\sum_{h=0}^{\infty} z^{hq_1}\right) \times \text{ other terms,}$$

so that

$$\begin{aligned} a_r(n) &= b_r - b_{r-1} + \sum_{1 \leqslant h \leqslant r/q} (b_{r-hq} - b_{r-hq-1}) \\ &= \Delta_0 + \Delta_1(q), \text{ say.} \end{aligned}$$

Thus, by (27) and our assumption, we must have

$$|\Delta_1(q)| < 2\lambda. \tag{29}$$

Now let $P_2$ be a prime greater than $P_1$, and $q_1$ and $q_2$ be any primes satisfying

$$p_s < q_1 < q_2 < r. \tag{30}$$

Then if $n = n_0 q_1 q_2 P_1 P_2$ we have

$$\Phi_n(z) = (1-z)\left(\sum_{m=0}^{\infty} b_m z^m\right)\left(\sum_{h_1=0}^{\infty} z^{h_1 q_1}\right)\left(\sum_{h_2=0}^{\infty} z^{h_2 q_2}\right) \times \text{other terms,}$$

so that

$$a_r(n) = \Delta_0 + \Delta_1(q_1) + \Delta_1(q_2) + \Delta_2(q_1, q_2),$$

where

$$\Delta_2(q_1, q_2) = \sum_{\substack{h_1, h_2 \geqslant 1 \\ h_1 q_1 + h_2 q_2 \leqslant r}} (b_{r-h_1 q_1 - h_2 q_2} - b_{r-h_1 q_1 - h_2 q_2 - 1}).$$

Thus, by (27), (28), (29) and our assumption, we have for all $q_1, q_2$ satisfying (30),

$$|\Delta_2(q_1, q_2)| < 6\lambda.$$

Proceeding inductively we see that for each set of $j$ ($\geqslant 3$) primes $q_1, \ldots, q_j$ satisfying

$$p_s < q_1 < \ldots < q_j < r \tag{31}$$

we have

$$|\Delta_j(q_1, \ldots, q_j)| < (j+1)^j \lambda, \tag{32}$$

where

$$\Delta_j(q_1, \ldots, q_j) = \sum_{\substack{h_1, \ldots, h_j \geqslant 1 \\ h_1 q_1 + \ldots + h_j q_j \leqslant r}} (b_{r-h_1 q_1 - \ldots - h_j q_j} - b_{r-h_1 q_1 - \ldots - h_j q_j - 1}).$$

But if $r/(j+1) < q_1 < \ldots < q_j < r/j$, then

$$\Delta_j(q_1, \ldots, q_j) = b_{r-q_1-\ldots-q_j} - b_{r-q_1-\ldots-q_j-1}.$$

Thus, by Lemmas 2 and 3 and (26) we see at once that there is a set of primes $q_1, \ldots q_j$ with $j = 3$ or 4, satisfying (31), and such that (32) is false.

This contradiction enables us to assert that $|a_r(n)| \geqslant \lambda$ for arbitrarily large values of $n$ and thus, by (26), the proof of (8) is complete.

## *References*


1. A. S. Bang, " Om Ligningen $\phi_n(x) = 0$ ", *Nyt Tidsskrift for Mathematik* (B), 6 (1895), 6–12.
2. P. T. Bateman, " Note on the coefficients of the cyclotomic polynomial ", *Bull. Amer. Math. Soc.*, 55 (1949), 1180–1181.
3. M. Beiter, " The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$ ", *Amer. Math. Monthly*, 71 (1964), 769–770.
4. D. M. Bloom, " On the coefficients of the cyclotomic polynomials ", *Amer. Math. Monthly*, 75 (1968), 372–377.
5. L. Carlitz, " The number of terms in the cyclotomic polynomial $F_{pq}(x)$ ", *Amer. Math. Monthly*, 73 (1966), 979–981.
6. P. Erdős, " On the coefficients of the cyclotomic polynomial ", *Bull. Amer. Math. Soc.*, 52 (1946), 179–184.
7. ——— " On the coefficients of the cyclotomic polynomial ", *Portugaliae Math.*, 8 (1949), 63–71.
8. ——— " On the growth of the cyclotomic polynomial in the interval (0, 1) ", *Proc. Glasgow Math. Assoc.*, 3 ( 1956–58), 102–104.
9. H. Halberstam and K. F. Roth, *Sequences* (Clarendon Press, Oxford, 1966).
10. G. H. Hardy and S. Ramanujan, " Asymptotic formulae in combinatory analysis ", *Proc. London Math. Soc.*, 17 (1918), 75–115.
11. ——— and E. M. Wright, *An introduction to the theory of numbers*, fourth edition (Clarendon Press, Oxford, 1965).
12. D. H. Lehmer, " Some properties of the cyclotomic polynomial ", *J. Math. Anal. App.*, 15 (1966), 105–117.
13. E. Lehmer, " On the magnitude of the coefficients of the cyclotomic polynomial ", *Bull. Amer. Math. Soc.*, 42 (1936), 389–392.
14. A. Migotti, " Zur Theorie der Kreisteillungsgleichung ", *S.B der Math.–Naturwiss. Classe der Kaiserlichen Akademie der Wissenschaften, Wien*, 87 (1883), 7–14.
15. H. Möller, " Über die i-ten Koeffizienten der Kreisteilungspolynome ", *Math. Ann.*, 188 (1970), 26–38.
16. ———, " Über die Koeffizienten des n-ten Kreisteilungspolynoms ", *Math. Z.* 119 (1971), 33–40.
17. K. Prachar, *Primzahlverteilung* (Springer–Verlag, Berlin, 1957).



Imperial College of Science and Technology,
London, S.W.7.

The University,
Sheffield.