COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI

34. TOPICS IN CLASSICAL NUMBER THEORY

BUDAPEST (HUNGARY), 1981. (publ. Dec. 1984)

ON THE SIZE OF THE COEFFICIENTS OF THE CYCLOTOMIC POLYNOMIAL

P.T. BATEMAN, C. POMERANCE* and R.C. VAUGHAN

1. INTRODUCTION

Let Φ_n denote the polynomial with constant term 1 whose zeros are the primitive n-th roots of unity. Thus $\Phi_1(z)=1-z$ and

$$\prod_{d\mid n} \Phi_d(z) = 1 - z^n,$$

so that if $n>1$ we have

$$\Phi_n(z) = \prod_{d\mid n} (1-z^d)^{\mu(n/d)} =$$

* The work of the second-named author was supported by a grant from the National Science Foundation.

$$= \prod_{d|n} (z^d-1)^{\mu(n/d)} = z^{\varphi(n)}\Phi_n(1/z),$$

where μ and φ denote the functions of Möbius and Euler.

If m is odd and i is any positive integer, then

$$\Phi_{2^i m}(z) = \Phi_m(-z^{2^{i-1}}).$$

Further, if m is odd and $p_1, p_2, \ldots, p_k$ are the distinct primes dividing m, then

$$\Phi_m(z) = \Phi_{p_1 p_2 \ldots p_k}(z^{m/(p_1 p_2 \ldots p_k)}).$$

Thus the non-zero coefficients of Φ_n are determined up to sign by the set of odd primes dividing n.

We write

$$\Phi_n(z) = \sum_{m=0}^{\varphi(n)} a(m,n)z^m$$

and put

$$A(n) = \max_{m=0,1,\ldots,\varphi(n)} |a(m,n)|,$$

$$S(n) = \sum_{m=0}^{\varphi(n)} |a(m;n)|.$$

For example, since $\Phi_1(z)=1-z$ and $\Phi_p(z)=1+z+\ldots+z^{p-1}$ for any prime p, we have at once that $A(1)=1$, $S(1)=2$, $A(p)=1$, $S(p)=p$. If p and q are distinct odd primes, we have MIGOTTI's classical result that $A(pq)=1$ (see [1], [4], [10], [11]). Since the degree of Φ_n is $\varphi(n)$, we have the trivial inequalities

$$\frac{S(n)}{n} \le \frac{S(n)}{1+\varphi(n)} \le A(n) \le S(n) \qquad (n\ge 2).$$

As indicated earlier, the value of $A(n)$ or $S(n)$ depends only on the set of odd primes dividing n.

In this paper we consider the growth of $A(n)$ and $S(n)$ when the number of odd prime factors of n is fixed. On the one hand we shall prove a more specific form (Theorem 1) of the following result.

THEOREM A. *If k is a given positive integer, then*

$$S(n)/n \le A(n) \le n^{2^{k-1}/k-1}$$

for all n having exactly k distinct odd prime factors

Theorem A sharpens the inequality

$$A(n) \le S(n) \le n^{2^{k-1}} \tag{1}$$

proved in [2]. The second inequality of Theorem A is proved by establishing the recursive inequality

$$A(p_1p_2\cdots p_k) \le A(p_1p_2\cdots p_{k-1}) \prod_{j=0}^{k-2} S(p_1p_2\cdots p_j),$$

where $p_1, p_2, \ldots, p_k$ are distinct odd primes, and combining it with a theorem of Carlitz on $S(p_1p_2)$. A similar but superficially more complicated recursive argument was used in [12] to prove the inequality

$$A(n) \le c_k \varphi(n)^{2^{k-1}/k-1} \tag{2}$$

for all n with exactly k distinct odd prime factors, where $c_k=1$ for $k\le 3$ and $c_k=3^{2^{k-4}}$ for $k\ge 4$. For large k it is easy to see that (2) is slightly weaker than the inequality of Theorem A.

We remark that, since

$$\frac{n}{\varphi(n)} = \prod_{p|n} \frac{p}{p-1} \le \prod_{j=0}^{k} \frac{j+2}{j+1} = k+2$$

for all n with exactly k distinct odd prime factors, an inequality of the form

$$A(n) \le c_k' n^{2^{k-1}/k-1} \tag{3}$$

(for all n with exactly k distinct odd prime factors) implies an inequality of the form (2) with

$$c_k = c_k'(k+2)^{2^{k-1}/k-1}.$$

We chose the form (3) in Theorem A, since our proof of Theorem 1 naturally gives $c_k'=1$. Although (2) may very well be true with $c_k=1$, it does not seem easy to get such a result unless we assume that the smallest odd prime factor of n is large.

In the opposite direction it seems reasonable to make the following conjecture.

CONJECTURE B. If k is a given positive integer, there exists a positive constant c_k depending only on k such that

$$A(n) \ge S(n)/n \ge c_k n^{2^{k-1}/k-1}$$

for infinitely many n with exactly k distinct odd prime factors.

We shall show (Theorem 2) that Conjecture B is a consequence of the celebrated prime k-tuples conjecture. In addition we shall prove a more specific form (Theorem 3) of the following unconditional result, which is weaker than the assertion of Conjecture B by a logarithmic factor.

THEOREM C. *If k is a given positive integer, then*

$$A(n) \geq S(n)/n \geq n^{2^{k-1}/k-1}\Big/(5 \log n)^{2^{k-1}}$$

for infinitely many n with exactly k distinct odd prime factors.

A basic tool in obtaining Theorems 2 and 3 is the following elementary result.

LEMMA 5. *Suppose r is a positive integer greater than 1 and n is a product of k primes each congruent to $2r-1$ or $2r+1$ modulo $4r$. Then*

$$|\phi_n((-1)^{k-1} e^{\pi i/(2r)})| = (\cot \tfrac{\pi}{4r})^{2^{k-1}} > r^{2^{k-1}}.$$

In addition the following result on the distribution of prime numbers is essential for Theorem 3.

LEMMA 8. *If k is a given positive integer, there are infinitely many odd positive integers r for which we can find k distinct primes $p_1, p_2, \ldots, p_k$ satisfying*

$$p_i \equiv 2r + 1 \pmod{4r}, \quad p_i < 5kr \log r$$

for $i=1,2,\ldots,k$.

If the number of prime factors of n is unrestricted, we remark that the following results on the order of magnitude of $A(n)$ are known. If $A(n)>1$ (which requires $n\geq 105$), then

$$(4) \qquad \frac{\operatorname{loglog} A(n)}{\log 2} \leq$$

$$\leq \frac{\log n}{\operatorname{loglog} n} + \frac{\log n}{(\operatorname{loglog} n)^2} + O\left(\frac{\log n}{(\operatorname{loglog} n)^3}\right).$$

On the other hand

$$(5) \qquad \frac{\operatorname{loglog} A(n)}{\log 2} \geq$$

$$\geq \frac{\log n}{\log\log n} + (1-\log 2)\frac{\log n}{(\log\log n)^2} +$$

$$+ o(\frac{\log n}{(\log\log n)^3}),$$

for an infinite sequence of values of n.

The result (4) follows immediately from (1) by using the known estimate

$$\omega(n) < \frac{\log n}{\log\log n} + \frac{\log n}{(\log\log n)^2} +$$

$$+ o(\frac{\log n}{(\log\log n)^3}),$$

where $\omega(n)$ is the number of distinct prime factors of n.

The result (5), which improves upon a series of earlier results by Paul Erdős, was first obtained in [15] but is proved more simply in [14]. It can also be deduced from Lemma 5 by taking $r=2$ or $r=3$ and using the readily verified fact that if m_k is the product of the first k primes congruent to $2r-1$ or $2r+1$ modulo

$4r$, then

$$k = \frac{\log m_k}{\log\log m_k} + \{1-\log \varphi(2r)\}\frac{\log m_k}{(\log\log m_k)^2} +$$

$$+ o(\frac{\log m_k}{(\log\log m_k)^3}).$$

2. LEMMAS FOR THE UPPER BOUND.

LEMMA 1. (cf. [4]) *If* p *and* q *are distinct odd primes, then* $S(pq) \leq (pq-1)/2$, *with equality if and only if* $|p-q|=2$.

PROOF. We may suppose $p<q$. Then CARLITZ proved in [5] that

$$S(pq) = 1 + 2u(pq-1-qu)/p,$$

where u is the integer between 0 and p such that $qu \equiv -1 \pmod p$. (See also Hilfssatz 3 of [12].) For integral u the quadratic function

$$f(u) = u(pq-1-qu)$$

is largest when $u=(p-1)/2$, since

$$f(u+1) - f(u) = q(p-1-2u) - 1.$$

Hence

$$S(pq) \le 1 + \frac{p-1}{p}\left(pq-1-q\,\frac{p-1}{2}\right) = \frac{p^2q-q+2}{2p},$$

with equality if and only if $q(p-1)/2 \equiv -1 \pmod p$, i.e. if and only if $q \equiv 2 \pmod p$. Now $q \ge p+2$ and so

$$S(pq) \le \frac{p^2q-p}{2p} = \frac{pq-1}{2},$$

with equality if and only if $q=p+2$.

LEMMA 2. *If* $p, q,$ *and* r *are odd primes and* $p<q<r$, *then* $A(pqr) \le p-1$.

LEMMA 2 is a classical result of BANG. For a proof see [1] or [4]. In [3] the bound $A(pqr) \le [(3p+1)/4]$ was obtained; this coincides with Bang's result if p is 3 or 5, but is sharper if $p \ge 7$.

LEMMA 3. *If* $p_1, p_2, \ldots, p_k$ *are distinct odd primes then*

$$\Phi_{p_1p_2\cdots p_k}(z) = \Phi_{p_1p_2\cdots p_{k-1}}(z^{p_k}) \times$$

$$\times \prod_{j=0}^{k-2} \Phi_{p_1p_2\cdots p_j}\left(z^{p_{j+2}p_{j+3}\cdots p_{k-1}}\right) \Big/ \Phi_1\left(z^{p_1p_2\cdots p_{k-1}}\right)$$

where the first factor in the product is to be interpreted as $\Phi_1(z^{p_2p_3\cdots p_{k-1}})$ *and the last factor in the product is to be interpreted as* $\Phi_{p_1p_2\cdots p_{k-2}}(z)$.

PROOF. We repeatedly use the identity

$$\text{(6)} \qquad \Phi_{pn}(z) = \Phi_n(z^p)/\Phi_n(z),$$

where p is a prime and n is any integer not divisible by p. We begin by noting that

$$\Phi_{p_1p_2\cdots p_k}(z) =$$

$$= \Phi_{p_1p_2\cdots p_{k-1}}(z^{p_k}) \Big/ \Phi_{p_1p_2\cdots p_{k-1}}(z).$$

Applying (6) to the preceding denominator, we obtain

$$\phi_{p_1p_2\cdots p_k}(z) =$$

$$= \phi_{p_1p_2\cdots p_{k-1}}(z^{p_k})\phi_{p_1p_2\cdots p_{k-2}}(z)$$

$$/\phi_{p_1p_2\cdots p_{k-2}}(z^{p_{k-1}}).$$

Applying (6) to the preceding denominator, we get

$$\phi_{p_1p_2\cdots p_k}(z) = \phi_{p_1p_2\cdots p_{k-1}}(z^{p_k}) \times$$

$$\times\ \phi_{p_1p_2\cdots p_{k-2}}(z) \times$$

$$\times\ \phi_{p_1p_2\cdots p_{k-3}}(z^{p_{k-1}})\Big/\phi_{p_1p_2\cdots p_{k-3}}(z^{p_{k-2}p_{k-1}}).$$

Repeated use of (6) on the various denominators which occur leads to the result of the lemma.

REMARK. We shall apply Lemmas 3 and 4 only for $k \geq 4$, but both sides make sense even for $k=1$ if the empty product which occurs in that case is interpreted as 1.

LEMMA 4. *If* $p_1, p_2, \ldots, p_k$ *are distinct odd primes*

then

$$A(p_1p_2\cdots p_k) \leq$$

$$\leq A(p_1p_2\cdots p_{k-1}) \prod_{j=0}^{k-2} S(p_1p_2\cdots p_j).$$

PROOF. For $|z|<1$ we have the expansion

$$\phi_1(z^{p_1p_2\cdots p_{k-1}})^{-1} = (1-z^{p_1p_2\cdots p_{k-1}})^{-1} =$$

$$= 1 + z^{p_1p_2\cdots p_{k-1}} + z^{2p_1p_2\cdots p_{k-1}} + \ldots .$$

Thus the identity of Lemma 3 gives

$$a(m, p_1p_2\cdots p_k) =$$

$$= \sum_{r, s_0, s_1, \ldots, s_{k-2}, t}' \{a(r, p_1p_2\cdots p_{k-1}) \times$$

$$\times \prod_{j=0}^{k-2} a(s_j, p_1p_2\cdots p_j)\},$$

where the dash indicates that the sum is to be extended over those values of $r, s_0, s_1, \ldots, s_{k-2}, t$ satisfying

(7) $$p_k r + \sum_{j=0}^{k-2} p_{j+2}\cdots p_{k-1}s_j + p_1p_2\cdots p_{k-1}t = m,$$

$$0 \le r \le \varphi(p_1p_2\cdots p_{k-1}),$$

$$0 \le s_j \le \varphi(p_1p_2\cdots p_j), \quad 0 \le t.$$

Since we need only consider those m with $m < p_1p_2\cdots$ $\cdots p_k$, it follows that $t<p_k$. Moreover, for given values of $m,s_0,s_1,\ldots,s_{k-2}$ the integer t is determined modulo p_k by (7). Hence, if $m,s_0,s_1,\ldots,s_{k-2}$ are given, there is at most one possible choice for t and then r is determined by (7). Thus

$$|a(n,p_1p_2\cdots p_k)| \le$$

$$\le A(p_1p_2\cdots p_{k-1}) \prod_{j=0}^{k-2} S(p_1p_2\cdots p_j)$$

and the inequality of the lemma follows.

3. PROOF OF THE UPPER BOUND.

THEOREM 1. *If* $k\ge3$ *and* $p_1,p_2,\ldots,p_k$ *are odd primes with* $p_1<p_2<\ldots<p_k$, *then*

$$S(p_1p_2\cdots p_k)/(p_1p_2\cdots p_k) <$$

$$< A(p_1p_2\cdots p_k) < \prod_{i=1}^{k-2} p_i^{2^{k-i-1}} - 1.$$

PROOF. For $k=3$ the assertion of the theorem coincides with Bang's theorem (Lemma 2). For $k=4$ Lemma 4 gives

$$A(p_1p_2p_3p_4) \le$$

$$\le A(p_1p_2p_3)S(1)S(p_1)S(p_1p_2).$$

Using the fact that $S(1)=2$, $S(p_1)=p_1$ and applying Lemmas 1 and 2, we obtain

$$A(p_1p_2p_3p_4) \le (p_1-1)2p_1(p_1p_2-1)/2 =$$

$$= (p_1-1)p_1(p_1p_2-1),$$

a result obtained in [4] which is slightly sharper than the inequality of Theorem 1 for $k=4$. If $k\ge5$, we have

(8) $$A(p_1p_2\cdots p_k) \le$$

$$\le A(p_1p_2\cdots p_{k-1})S(1)S(p_1)S(p_1p_2) \times$$

$$\times \prod_{j=3}^{k-2} S(p_1p_2\cdots p_j).$$

Applying the estimate $S(1)S(p_1)S(p_1p_2) < p_1^2p_2$ and using the inequality

$$S(p_1p_2\cdots p_j) < p_1p_2\cdots p_jA(p_1p_2\cdots p_j)$$

for $j=3,\dots,k-2$, we obtain from (8)

(9) $$A(p_1p_2\cdots p_k) < p_1^{k-2}p_2^{k-3} \cdots$$

$$\cdots p_{k-3}^2p_{k-2} \prod_{j=3}^{k-1} A(p_1p_2\cdots p_j).$$

If we assume the inequality

$$A(p_1p_2\cdots p_j) < \prod_{i=1}^{j-2} p_i^{2^{j-i-1}-1}$$

to be known for $j=3,4,\dots,k-1$ and then use (9), we obtain the analogous estimate for $A(p_1p_2\cdots p_k)$. Thus Theorem 1 is proved.

REMARK 1. Note that the bound of Theorem 1 is independent of p_{k-1} and p_k. (Cf. [7] or [10]).

REMARK 2. Since $p_1<p_2<\dots<p_k$ and

$$\sum_{i=1}^{k-2} (2^{k-i-1}-1) = 2^{k-1} - k,$$

it follows from Theorem 1 that

$$A(p_1p_2\cdots p_k) < (p_1p_2\cdots p_k)^{(2^{k-1}-k)/k},$$

which gives the conclusion of Theorem A of the Introduction.

REMARK 3. As indicated in the Introduction, it would be reasonable to conjecture that (2) holds with $c_k=1$, or more specifically that

(10) $$A(p_1p_2\cdots p_k) \le \prod_{i=1}^{k-2} (p_i-1)^{2^{k-i-1}} - 1$$

for primes p_i with $p_1<p_2<\dots<p_k$. Although Beiter's improvement of Lemma 2 would be helpful if used in the

above proof, it does not appear to give (10), even for $k=4$, unless we assume that $p_1 \geq 17$.

4. A TRIGONOMETRICAL LEMMA.

LEMMA 5. *Suppose r is an integer greater than 1 and n is a product of k distinct prime numbers each congruent to $2r-1$ or $2r+1$ modulo $4r$. Then*

$$|\phi_n((-1)^{k-1} e^{\pi i/(2r)})| = (\cot \frac{\pi}{4r})^{2^{k-1}} > r^{2^{k-1}}.$$

PROOF. We first note that if d is the product of j primes each congruent to $2r-1$ or $2r+1$ modulo $4r$, then $d \equiv \pm 1 \pmod{4r}$ if j is even and $d \equiv 2r \pm 1 \pmod{4r}$ if j is odd. Thus, if n is as given in the hypothesis of the lemma and if $d|n$, then

$$e^{\pi i d/(2r)} = \mu(d) e^{\pm \pi i/(2r)}.$$

Hence

$$\phi_n((-1)^{k-1} e^{\pi i/(2r)}) =$$

$$= \prod_{d|n} \{1 + (-1)^k e^{\pi i d/(2r)}\}^{\mu(n/d)} =$$

$$= \prod_{d|n} \{1 + \mu(n/d) e^{\pm \pi i/(2r)}\}^{\mu(n/d)},$$

so that

$$|\phi_n((-1)^{k-1} e^{\pi i/(2r)})| =$$

$$= (\frac{2 \cos \pi/(4r)}{2 \sin \pi/(4r)})^{2^{k-1}} \geq (\frac{\cos \pi/(4r)}{\pi/(4r)})^{2^{k-1}} >$$

$$> r^{2^{k-1}}.$$

5. DEDUCTION OF CONJECTURE B FROM THE PRIME k-TUPLES CONJECTURE.

The prime k-tuples conjecture was apparently first discussed in [6] and is now usually formulated as follows.

PRIME k-TUPLES CONJECTURE. Suppose that $a_1, a_2, \ldots$ $\ldots a_k$ are positive integers and $b_1, b_2, \ldots, b_k$ are any integers such that the following condition is satisfied: for each prime p the congruence

(11) $$(a_1x+b_1)(a_2x+b_2)\ldots(a_kx+b_k) \equiv 0 \pmod p$$

has fewer than p solutions. Then there are infinitely many positive integers h such that a_1h+b_1, $a_2h+b_2,\ldots$ $\ldots,a_kh+b_k$ are all primes.

THEOREM 2. *If the prime k-tuples conjecture holds for a particular value of k, then*

$$A(n) \geq S(n)/n \geq 2^{-2^{k-1}}(k!)^{-2^{k-1}/k}\, n^{2^{k-1}/k-1}$$

for infinitely many positive integers n with exactly k odd prime factors.

PROOF. We apply the prime k-tuples conjecture with

$$b_i = (-1)^i, \quad a_i = 2(2[\tfrac{i-1}{2}]+1)A_k,$$

where A_k is the product of the odd primes not exceeding k. Clearly the congruence (11) has no solutions if $p\leq k$. If $p>k$, then, since

$$2[\tfrac{i-1}{2}] + 1 \leq i,$$

the coefficients $a_1,a_2,\ldots,a_k$ are relatively prime to p and thus (11) has exactly k solutions modulo p.

Thus there are infinitely many positive integers h such that the integers

$$p_i = 2(2[\tfrac{i-1}{2}]+1)A_kh + (-1)^i \qquad (i=1,2,\ldots,k)$$

are all prime. Clearly

$$p_i \equiv 2A_kh + (-1)^i \pmod{4A_kh} \qquad (i=1,2,\ldots,k).$$

Thus we may apply Lemma 5 with $r=A_kh$ and $n=p_1p_2\cdots p_k$. Since $p_i\leq 2ir$, we have $n\leq 2^kk!r^k$. Hence

$$S(n) \geq |\Phi_n((-1)^{k-1}\, e^{\pi i/(2r)})| >$$

$$> r^{2^{k-1}} \geq \left(\frac{n}{2^kk!}\right)^{2^{k-1}/k}$$

and the theorem is proved.

REMARK. The result of Theorem 2 may be written in a form analogous to that used in Theorem 1, namely

(12) $$A(p_1p_2\cdots p_k) \geq \frac{S(p_1p_2\cdots p_k)}{p_1p_2\cdots p_k} \geq$$

$$\geq \{2^{-2^{k-1}}(k!)^{-2^{k-1}}/k\} \prod_{i=1}^{k-2} p_i^{2^{k-i-1}-1}$$

for infinitely many k-tuples of odd primes $p_1<p_2<\cdots<p_k$. Of course (12) is somewhat weaker than the inequality of Theorem 2, whereas Theorem 1 is stronger than Theorem A.

6. SOME LEMMAS FROM ANALYTIC NUMBER THEORY.

If $y>2$ and m and l are coprime positive integers, we recall that $\pi(y;m,l)$ denotes the number of primes not exceeding y which are congruent to l modulo m.

LEMMA 6. *If* $y>2$, *then*

$$\pi(y;m,l) = \frac{1}{\varphi(m)}\int_2^Y \frac{du}{\log u} + O(\frac{y}{(\log y)^{100}})$$

for all m *less than* $(\log y)^{3/2}$ *and all* l *relatively prime to* m, *where the constant implied by the big* O *symbol is absolute and effectively computable.*

PROOF. This lemma may be readily deduced from formula (36)in [13]. The estimate of the lemma would still be true if the assumption $m < (\log y)^{3/2}$ were replaced by the assumption $m < (\log y)^u$ for some fixed u; however for $u\geq 2$ the proof requires Siegel's theorem and accordingly the O-constant is then no longer effectively computable.

LEMMA 7. *There is a constant* E *such that*

$$\sum_{q \text{ odd},\ 1\leq q\leq y} \frac{1}{\varphi(q)} = \frac{105\ \zeta(3)}{2\pi^4}\log y + E + O(\frac{\log y}{y})$$

for $y>2$.

PROOF. See [8].

LEMMA 8. *If* k *is a given positive integer, there exist infinitely many odd positive integers* r *for which we can find* k *distinct primes* $p_1,p_2,\ldots,p_k$ *satisfying*

$$p_i \equiv 2r + 1 (\text{mod } 4r),\quad p_i < 5kr\log r$$

for $i=1,2,\ldots,k$.

PROOF. For large positive x we define the following finite sets depending on x. Let P be the set of primes congruent to 3 modulo 4 which lie in the interval $(x, 7x]$. Let Q be the set of odd integers which lie in the interval $(0.8\, k \log x,\ 2.4\, k \log x]$. Let M be the set of ordered pairs (p,q) such that $p\in P$, $q\in Q$, and $p\equiv 1 \pmod q$.

The lemmas of the present section enable us to estimate the cardinality of M. By Lemma 6 we have

$$|M| = \sum_{q\in Q} \{\pi(7x;\ 4q,\ 2q+1) - \pi(x;\ 4q,\ 2q+1)\} =$$

$$= \sum_{q\in Q} \{\frac{1}{2\varphi(q)} \int_x^{7x} \frac{du}{\log u} + O(\frac{x}{(\log x)^{100}})\}.$$

Now

$$\int_x^{7x} \frac{du}{\log u} = \frac{6x}{\log x} + O(\frac{x}{(\log x)^2})$$

and by Lemma 7

$$\sum_{q\in Q} \frac{1}{\varphi(q)} = \frac{105\ \zeta(3)}{2\pi^4} \log 3 + O(\frac{\log\log x}{\log x}).$$

Hence

$$|M| = \frac{315\ \zeta(3)\log 3}{2\pi^4} \frac{x}{\log x} + O(\frac{x \log\log x}{(\log x)^2}) >$$

$$> 2.1 \frac{x}{\log x}$$

for x sufficiently large.

Let us consider the function f on M defined by

$$f(p,q) = \frac{p-1}{2q}.$$

In view of the definitions of P and Q, the range of f is contained in the set R consisting of the odd integers which lie in the interval

$$(\frac{x-1}{4.8\ k \log x},\ \frac{7x-1}{1.6\ k \log x}).$$

Since

$$|R| = \frac{25}{12} \frac{x}{k \log x} + O(1),$$

we must have $k\ |R| < |M|$ for large x. Hence, if x is sufficiently large, the function f must take on some value r at least k times. In other words, if x is sufficiently large, there exists an element r of R and k distinct pairs $(p_1,q_1),(p_2,q_2),\ldots,(p_k,q_k)$ in M such that

$$\frac{p_1-1}{2q_1} = \frac{p_2-1}{2q_2} = \ldots = \frac{p_k-1}{2q_k} = r.$$

Clearly the primes p_i are distinct and

$$p_i \equiv 2r+1 \pmod{4r}.$$

Also

$$p_i \le 2q_i r + 1 \le 4.8\ kr \log x + 1.$$

Since $\log r = \log x + O(\log\log x)$, we have

$$p_i < 5\ kr \log r$$

if x is sufficiently large. Since r tends to infinity with x, there are infinitely many odd positive integers r for which the conclusion of the lemma holds.

Thus the proof is complete.

REMARK. The constant 5 occurring in Lemma 8 could be replaced by any number greater than

$$\frac{2\pi^4 e}{105\ \zeta(3)} = 4.19575\ldots .$$

This can be seen by changing the definitions of P and Q in the proof so that P becomes the set of primes congruent to 3 modulo 4 which lie in the interval $(x, (K+1)x]$ and Q becomes the set of odd integers which lie in the interval

$$\left(\frac{(1+1/K)\pi^4}{105\ \zeta(3)}\ k \log x,\ \frac{(1+1/K)\pi^4 e}{105\ \zeta(3)}\ k \log x\right],$$

where K is a large positive constant.

7. AN UNCONDITIONAL RESULT.

THEOREM 3. *If* k *is a given positive integer, there are infinitely many positive integers* n *with exactly* k *distinct odd prime factors* $p_1,p_2,\ldots,p_k$ *such that*

$$A(n) \ge \frac{S(n)}{n} \ge$$

$$\geq \frac{p_k^{2^{k-1}-k}}{(5\ k \log p_1)^{2^{k-1}}} \geq \frac{\prod_{i=1}^{k-2} p_i^{2^{k-i-1}-1}}{(5\ k \log p_1)^{2^{k-1}}}$$

where $p_1<p_2<\ldots<p_k$.

PROOF. Let r be a positive integer for which the conclusion of Lemma 8 holds, i.e., for which there exist k primes $p_1, p_2, \ldots, p_k$ with

$$p_1 \equiv p_2 \equiv \ldots \equiv p_k \equiv 2r + 1 \pmod{4r}$$

and

$$p_1 < p_2 < \ldots < p_k < 5\ kr \log r.$$

Put $n=p_1 p_2 \ldots p_k$. Since

$$p_k < 5\ kr \log r < 5\ kr \log p_1,$$

Lemma 5 gives

$$S(n) \geq |\Phi_n((-1)^{k-1} e^{\pi i/(2r)})| >$$

$$> r^{2^{k-1}} > p_k^{2^{k-1}} / (5\ k \log p_1)^{2^{k-1}}.$$

Hence

$$\frac{S(n)}{n} \geq \frac{S(n)}{p_k^k} > \frac{p_k^{2^{k-1}-k}}{(5\ k \log p_1)^{2^{k-1}}}.$$

Since $p_1<p_2<\ldots<p_k$ and $\sum_{i=1}^{k-2} (2^{k-i-1}-1) = 2^{k-1} - k$, the final conclusion is immediate and the theorem is proved.

REMARK 1. Since $p_1 \leq n^{1/k} \leq p_k$, Theorem C of the Introduction is an immediate consequence of Theorem 3.

REMARK 2. For $k=3$ results of the above type but without a logarithmic factor may be found in [9] and [12].

REMARK 3. The constant 5 occurring in Theorem 3 could be replaced by any number greater than

$$\frac{\pi^5 e}{420\ \zeta(3)} = 1.64767\ldots\ .$$

To obtain such an improved constant it would suffice to

(a) take advantage of the factor $\pi/4$ squandered in Lemma 5,

(b) gain a factor 1/2 by using primes congruent to $2r-1$ modulo $4r$ as well as primes congruent to $2r+1$ modulo $4r$, and

(c) take advantage of the factor $2\pi^4 e/\{525\ \zeta(3)\}$ mentioned in the remark at the end of the previous section.

REFERENCES

[1] Bang, A.S., Om Ligningen $\Phi_n(x)=0$, *Nyt Tidsskrift for Mat.* 6B (1895), 6-12.

[2] Bateman, P.T., Note on the coefficients of the cyclotomic polynomial, *Bull.Amer.Math.Soc.* 55 (1949), 1180-1181.

[3] Beiter, M., Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}, II, *Duke Math.J.* 38 (1971), 591-594.

[4] Bloom, D.M., On the coefficients of the cyclotomic polynomials, *Amer.Math.Monthly* 75 (1968), 372-377.

[5] Carlitz, L., The number of terms in the cyclotomic polynomial $F_{pq}(x)$, *Amer.Math.Monthly* 73 (1966), 979-981.

[6] Dickson, L.E., A new extension of Dirichlet's theorem on prime numbers, *Messenger Math.* (2) 33 (1904), 155-161.

[7] Justin, J., Bornes des coefficients du polynôme cyclotomique et de certains autres polynômes, *C.R. Acad.Sci.Paris*, Ser. A-B, 268 (1969), A995-A997.

[8] Landau, E., On a Titchmarsh-Estermann sum, *J.London Math.Soc.* 11 (1936), 242-245.

[9] Lehmer, Emma, On the magnitude of the coefficients of the cyclotomic polynomial, *Bull.Amer.Math.Soc.* 42 (1936), 389-392.

[10] Lenstra, H.W., Jr., Vanishing sums of roots of unity, *Proceedings Bicentennial Congress Wiskundig Genootschap*, Part II, pp. 249-268, Math.Centre Tracts, 101, Math Centrum, *Amsterdam*, 1979.

[11] Migotti, A., Zur Theorie der Kreistheilungsgleichung, *Sitz. Akad. Wiss.Wien (Math.)* (2) 87 (1883), 7-14.

[12] Möller, H., Über die Koeffizienten des n-ten Kreisteilungspolynoms, *Math.Z.* 119 (1971), 33-40.

[13] Page, A., On the number of primes in an arithmetic progression, *Proc. London Math.Soc.* (2) 39 (1935), 116-141.

[14] Saffari, B., to appear.

[15] Vaughan, R.C., Bounds for the coefficients of cyclotomic polynomials, *Michigan Math.J.* 21 (1975), 289-295.

P.T.Bateman
Dept.of Math., Univ. of Illinois
1409 West Green Street
Urbana, Ill. 61801
USA

C.Pomerance
Dept. of Math.,
Univ. of Georgia
Athens, Georgia 30602
USA

R.C.Vaughan
Dept. of Math., Imperial College
Huxley Building, Queen's Gate
London, SW7 2BZ
U.K.