ACTA ARITHMETICA
152.4 (2012)

On the height of cyclotomic polynomials

by

BARTŁOMIEJ BZDĘGA (Poznań)

1. Introduction. The polynomial

$$\Phi_n(x) = \sum_{0\le m\le\varphi(n)} a_n(m)x^m = \prod_{k\le n,\ (k,n)=1} (x-\zeta_n^k)$$

where $\zeta_n = e^{2i\pi/n}$, is called the nth *cyclotomic polynomial*. We are interested in estimating its coefficients, so we define

$$A_n = \max_m |a_n(m)| \quad \text{and} \quad S_n = \sum_{m=0}^{\varphi(n)} |a_n(m)|.$$

We also define

$$\Psi_n(x) = \frac{1}{\Phi_n(x)} = \sum_{m\ge 0} c_n(m)x^m, \quad C_n = \max_m |c_n(m)|.$$

The polynomial $(1-x^n)\Psi_n(x)$ is called the nth *inverse cyclotomic polynomial* (see [11] for details). We remark that $c_n(m)$ is equal to the m'th coefficient of the nth inverse cyclotomic polynomial, where $0\le m' < n$ and $m'\equiv m \pmod n$.

We consider the numbers n which are odd and square-free only, since it is known that $A_{\ker(n)} = A_n = A_{2n}$, where $\ker(n)$ is the product of all distinct prime factors of n (see [14] for details). The same is true for inverse cyclotomic polynomials.

The order of Φ_n is the number $\omega(n)$ of primes dividing n. For $\omega(n)\le 4$ the following bounds are known:

$$(1)\qquad A_p = 1,\quad A_{pq}=1,\quad A_{pqr}\le \epsilon_3 p,\quad A_{pqrs}\le \epsilon_4 p^3 q,$$

where $p<q<r<s$ are primes. The first of them is obvious. The second one is due to A. Migotti [10].

2010 *Mathematics Subject Classification*: 11B83, 11C08, 11N56.
Key words and phrases: cyclotomic polynomial, inverse cyclotomic polynomial, divisors of x^n-1, height of a polynomial, bounds on coefficients.

DOI: 10.4064/aa152-4-2

The third one with $\epsilon_3 = 1$ is due to A. S. Bang [2]. It has been improved by some authors. Presently it is known that one can take $\epsilon_3 = 3/4$ (see [1, 4, 6]) and that one cannot replace ϵ_3 by a constant smaller than $2/3$ (see [7]). It is strongly believed that the estimate holds with $\epsilon_3 = 2/3$ (see [9, 15]). This conjecture is known as the Corrected Beiter Conjecture (see [7]).

The fourth inequality with $\epsilon_4 = 1$ was established by Bloom [5]. We use a simple argument from [3] to show that the inequality is true with $\epsilon_4 = \epsilon_3$.

For the inverse cyclotomic polynomials we know the following bounds

$$C_p = 1, \quad C_{pq} = 1, \quad C_{pqr} \le p - 1.$$

The first and the second of them are easy to obtain. The third was proved by P. Moree [11], who in the same paper proved that $p-1$ cannot be replaced by a smaller number.

For every $n = p_1 \cdots p_k$, where $p_1 < \cdots < p_k$ we define

$$M_n = \prod_{j=1}^{k-2} p_j^{2^{k-j-1}-1}.$$

In the general case, the following result by P. T. Bateman, C. Pomerance and R. C. Vaughan [3] for standard cyclotomic polynomials is known:

$$A_{p_1\ldots p_k} \le M_n \le n^{k^{-1}2^{k-1}-1}. \tag{2}$$

The same authors came up with the following conjecture (cf. [3, p. 175]).

Conjecture 1. *In the upper bound in* (2) *one can replace n by $\varphi(n)$.*

We prove this conjecture and moreover, we improve it by multiplying the right hand side by a constant depending on k only and rapidly decreasing when k grows. We also prove a similar result for the inverse cyclotomic polynomials and give the bound for the maximal magnitude B_n of the coefficients of any divisor of $x^n - 1$, improving on an earlier result of N. Kaplan [8] in case $n = p_1 \ldots p_k$ and $p_i \not\gg p_{i-1}$ for $i = 2, \ldots, k$. The idea of estimating the maximal magnitude of the coefficients of any divisor of $x^n - 1$ comes from C. Pomerance and N. C. Ryan [12].

We denote by ϵ_k the smallest positive real number for which the inequality $A_{p_1\ldots p_k} \le \epsilon_k M_{p_1\ldots p_k}$ holds with any distinct primes $p_1, \ldots, p_k$. In the same way we define $\epsilon_k^{\mathrm{inv}}$ for the inverse cyclotomic polynomial.

By Lemma 5 below, the ratio $S_{pqr}/(p^2qr)$ is bounded above, and hence we can define

$$d = \sup_{p,q,r} \frac{S_{pqr}}{p^2qr}, \quad \rho = \prod_{i=0}^{\infty} \left(\frac{2i+5}{2i+6}\right)^{4^{-i}}, \quad C = \left(\frac{3}{4}\epsilon_3^{3/2} d \rho^{1/8}\right)^{1/32}. \tag{3}$$

We know that $\epsilon_3 \le 3/4$ and by Lemma 5 we have $d \le \epsilon_3(2-\epsilon_3)/2 \le 15/32$.

Numerical computations give $\rho \approx 0.7993$ and therefore $C < 0.9541$. If $\epsilon_3 = 2/3$ then $d \le 4/9$ and so $C < 0.9473$.

Recall that the notation $g(k) = o_k(1)$ means that $g(k) \to 0$ as $k \to \infty$. Our main results are the following four theorems.

THEOREM 1. *We have* $(A_n/M_n)^{2^{-k}} \le C + o_k(1)$.

THEOREM 2. *We have* $(C_n/M_n)^{2^{-k}} \le C + o_k(1)$.

THEOREM 3. *We have* $(B_n/n^{(3^k-1)/(2k)-1})^{3^{-k}} \le C + o_k(1)$.

THEOREM 4. *We have* $M_n \le \varphi(n)^{k^{-1}2^{k-1}-1}$.

In the proof of Theorem 1 we also establish the following bounds:

$$A_{pqrs} \le \frac{3}{4}p^3q, \quad A_{pqrst} \le \frac{135}{512}p^7q^3r, \quad A_{pqrstu} \le \frac{18225}{262144}p^{15}q^7r^3s, \tag{4}$$

where we assumed $\epsilon_3 = 3/4$. For $\epsilon_3 = 2/3$ we establish constants $\frac{2}{3}$, $\frac{2}{9}$, $\frac{32}{729}$, respectively.

Also for the inverse cyclotomic polynomials,

$$C_{pqrs} \le \frac{3}{4}p^3q, \quad C_{pqrst} \le \frac{9}{16}p^7q^3r, \quad C_{pqrstu} \le \frac{10935}{131072}p^{15}q^7r^3s \tag{5}$$

for $\epsilon_3 = 3/4$. If $\epsilon_3 = 2/3$, then we obtain constants $\frac{2}{3}$, $\frac{4}{9}$, $\frac{8}{81}$, respectively

Let us remark that Theorem 1, but with a larger constant, can be obtained by the original method of P. T. Bateman, C. Pomerance and R. C. Vaughan. Our method is somewhat different. It is based on a different recursive formula given in Lemma 1. We also use some basic combinatorics, in particular the following theorem.

THEOREM 5 (E. Sperner, 1928). *Let* $A_1, \ldots, A_t \subset A$, *where* $\#A < \infty$. *If* $A_i \not\subset A_j$ *for every* $i \ne j$, *then* $t \le \binom{\#A}{\lfloor \#A/2 \rfloor}$. □

For the proof see [13].

2. Preliminaries. Our primary tool is the following lemma.

LEMMA 1. *Let* $p_1, \ldots, p_k$ *be distinct primes. Then*

$$\Phi_{p_1 \ldots p_k}(x) = f(x) \cdot \prod_{j=1}^{k-2} P_j(x), \tag{6}$$

where f *is a formal power series satisfying*

$$f(x) = (1 - x^{p_1 \ldots p_k}) \cdot \frac{\prod_{i=2}^{k}(1 - x^{p_2 \ldots p_k/p_i})}{\prod_{i=1}^{k}(1 - x^{p_1 \ldots p_k/p_i})}, \tag{7}$$

and $P_j = \prod_{i=j+2}^{k} \Phi_{p_1 \ldots p_j}(x^{p_{j+2} \ldots p_k/p_i})$.

LEMMA 2. *Let* $f(x)=\sum_{m=0}^{\infty} d_m x^m$. *If* $m<p_1\ldots p_k$ *then* $d_m\le b_{k-2}$, *where* $b_{k-2}=\binom{k-2}{\lfloor (k-2)/2\rfloor}$.

Lemmas 1 and 2 allow us to give the following recursive bound on ϵ_k.

LEMMA 3. *Put* $E_k=\frac{b_{k-2}d^{k-4}}{2^{k-3}}\prod_{j=1}^{k-2}\epsilon_j^{k-j-1}$. *Then* $\epsilon_k\le E_k$.

To start the induction we also need the estimates provided by Lemmas 4 and 5 below.

LEMMA 4. *We have* $\epsilon_4\le\epsilon_3$.

Proof. It is known that $S_1=2$ and $S_{pq}\le pq/2$ (see [5] for a proof of the second equality). By Lemma 4 [3, pp. 182–183],

$$A_{pqrs}\le A_{pqr}S_{pq}S_pS_1\le\epsilon_3\cdot p^3q,$$

so the estimate holds. ∎

Recall that d is defined in (3).

LEMMA 5. *We have* $d\le\epsilon_3(2-\epsilon_3)/2$.

Proof. Bloom [5] proved that

$$|a_{pqr}(m)|=|a_{pqr}(\varphi(pqr)-m)|\le 2(\lfloor m/qr\rfloor+1).$$

Thus

$$\begin{aligned}
S_{pqr}&\le 2\sum_{k=0}^{\varphi(pqr)/2}\min\{\epsilon_3p,2(\lfloor m/qr\rfloor+1)\}\\
&\le\epsilon_3p(\varphi(pqr)+2-2\lfloor\epsilon_3p/2\rfloor qr)+2qr\sum_{a=0}^{\lfloor\epsilon_3p/2\rfloor-1}(2a+2)\\
&=\epsilon_3p(p-1)(q-1)(r-1)+2\epsilon_3p-2\lfloor\epsilon_3p/2\rfloor\epsilon_3pqr\\
&\quad+2\lfloor\epsilon_3p/2\rfloor(2\lfloor\epsilon_3p/2\rfloor+1)qr\\
&<\epsilon_3(2-\epsilon_3)p^2qr/2,
\end{aligned}$$

which completes the proof. ∎

3. Proofs of Lemmas 1–3

Proof of Lemma 1. We prove this lemma by induction on k. For $k<5$ the statement holds by the results of [5]. Let us define

$$\widetilde{f}(x)=(1-x^{p_2\ldots p_k})\cdot\frac{\prod_{i=3}^{k}(1-x^{p_3\ldots p_k/p_i})}{\prod_{i=2}^{k}(1-x^{p_2\ldots p_k/p_i})}$$

and $\widetilde{P}_j(x)=\prod_{i=j+2}^{k}\varPhi_{p_2\ldots p_j}(x^{p_{j+2}\ldots p_k/p_i})$. By the inductive assumption,

$$\varPhi_{p_2\ldots p_k}=\widetilde{f}(x)\cdot\prod_{j=2}^{k-2}\widetilde{P}_j(x). \tag{8}$$

It is known that $\Phi_{np}(x) = \Phi_n(x^p)/\Phi_n(x)$ for a prime p not dividing n (see [14]). Then also

$$\Phi_{p_1\ldots p_k}(x) = \frac{\Phi_{p_2\ldots p_k}(x^{p_1})}{\Phi_{p_2\ldots p_k}(x)} \quad \text{and} \quad P_j(x) = \frac{\widetilde{P}_j(x^{p_1})}{\widetilde{P}_j(x)}.$$

From this and (8),

$$\Phi_{p_1\ldots p_k}(x) = \frac{\widetilde{f}_k(x^{p_1}) \cdot \prod_{j=2}^{k-2} \widetilde{P}_j(x^{p_1})}{\widetilde{f}_k(x) \cdot \prod_{j=2}^{k-2} \widetilde{P}_j(x)} = \frac{\widetilde{f}(x^p)}{\widetilde{f}(x)P_1(x)} \cdot \prod_{j=1}^{k-2} P_j(x).$$

Finally,

$$\frac{\widetilde{f}(x^{p_1})}{\widetilde{f}(x)} = P_1(x)(1 - x^{p_1\ldots p_k}) \cdot \frac{\prod_{i=2}^{k}(1 - x^{p_2\ldots p_k/p_i})}{\prod_{i=1}^{k}(1 - x^{p_1\ldots p_k/p_i})} = P_1(x)f(x),$$

which completes the proof. ■

Proof of Lemma 2. Let $n = p_1 \ldots p_k$. We define $f^*(x) = \sum_{m=0}^{n-1} d_m x^m$. Since $f^*(x) \equiv f(x) \pmod{x^n}$, it suffices to prove Lemma 2 with f^* instead of f. By (7) we have

$$f^*(x) \equiv \prod_{i=2}^{k}(1 - x^{p_2\ldots p_k/p_i}) \sum_{\alpha_1,\ldots,\alpha_k \ge 0} x^{\alpha_1 n/p_1 + \cdots + \alpha_k n/p_k} \pmod{x^n}. \tag{9}$$

Let

$$\Lambda = \{\lambda = (\lambda_2, \ldots, \lambda_k) : \lambda_i \in \{0,1\} \text{ for } i = 2, \ldots, k\}, \quad s(\lambda) = (-1)^{\lambda_2 + \ldots + \lambda_k}.$$

By (9),

$$d_m = \sum_{\lambda \in \Lambda} s(\lambda)\chi(m - \langle \lambda, v/p_1 \rangle), \tag{10}$$

where $\langle \cdot, \cdot \rangle$ is the scalar product in $\mathbb{R}^{k-1}$, $v = (n/p_2, \ldots, n/p_k)$ and

$$\chi(m) = \begin{cases} 1 & \text{if } m \text{ is of the form } \alpha_1 n/p_1 + \cdots + \alpha_k n/p_k, \\ 0 & \text{otherwise.} \end{cases}$$

We define a number $\beta(\lambda)$ and a vector $\alpha(\lambda) = (\alpha_2(\lambda_2), \ldots, a_k(\lambda_k))$ by the congruence

$$m - \langle \lambda, v/p_1 \rangle \equiv \beta(\lambda) n/p_1 + \langle \alpha(\lambda), v \rangle \pmod{n}. \tag{11}$$

The numbers $\alpha_i(0)$ and $\alpha_i(1)$ depend only on the residue class of m modulo p_i, so (11) holds for every $\lambda \in \Lambda$. We have the following equivalences:

$$\begin{aligned} &\chi(m - \langle \lambda, v/p_1 \rangle) = 1 \\ &\qquad \Leftrightarrow \langle \lambda, v/p_1 \rangle + \langle \alpha(\lambda), v \rangle \le m \\ &\qquad \Leftrightarrow \langle \lambda, v/p_1 \rangle + \langle \alpha(\lambda) - \alpha(\theta_{k-1}), v \rangle \le m - \langle \alpha(\theta_{k-1}), v \rangle, \end{aligned}$$

where $\theta_{k-1} = (0,\dots,0)$. We have

$$\langle \alpha(\lambda) - \alpha(\theta_{k-1}), v\rangle = \sum_{i=2}^{k} (\alpha_i(\lambda_i) - \alpha_i(0)) v_i = \sum_{i=2}^{k} (\alpha_i(1) - \alpha_i(0)) v_i \lambda_i = \langle \lambda, w\rangle,$$

where $w = ((\alpha_i(1) - \alpha_i(0))v_i)_{i=2}^k$. Therefore

$$\chi(m - \langle \lambda, v/p_1\rangle) = 1 \iff \langle \lambda, u\rangle \le D,$$

where $u = v/p_1 + w$ and $D = m - \langle \alpha(\theta_{k-1}), v\rangle$. By (10),

$$d_m = \sum_{\lambda\in\Lambda,\ \langle\lambda,u\rangle\le D} s(\lambda). \tag{12}$$

Without loss of generality we may assume that $0 \le u_k \le u_2,\dots,u_{k-1}$.

There is a natural bijection between Λ and the family of subsets of $\{2,\dots,k\}$, defined by

$$S_\lambda = \{i \in \{2,\dots,k\} : \lambda_i = 1\} \quad \text{for } \lambda \in \Lambda.$$

We say that $\lambda = (\lambda_2,\dots,\lambda_{k-1},0)$ is *maximal* if $\langle\lambda,u\rangle \le D$ and for every $\lambda' = (\lambda'_2,\dots,\lambda'_{k-1},0)$ such that $S_\lambda \subset S_{\lambda'}$ we have $\langle\lambda',u\rangle > D$. Note that for

$$\lambda^0 = (\lambda_2,\dots,\lambda_{k-1},0) \quad \text{and} \quad \lambda^1 = (\lambda_2,\dots,\lambda_{k-1},1)$$

the following statements are true:

- If λ^0 is not maximal and $\langle\lambda^0,u\rangle \le D$ then $\langle\lambda^1,u\rangle \le D$.
- If $\langle\lambda^1,u\rangle \le D$ then $\langle\lambda^0,u\rangle \le D$.
- $s(\lambda^0) + s(\lambda^1) = 0$.

From this observation and (12) we conclude that

$$|d_m| \le \#\{\lambda \in \Lambda : \lambda \text{ is maximal}\}. \tag{13}$$

Let $\lambda^1,\dots,\lambda^t \in \Lambda$ be maximal. By the definition of maximal λ, we have $S_{\lambda^i} \subset \{2,\dots,k-1\}$ and $S_{\lambda^i} \not\subset S_{\lambda^j}$ for every $i \ne j$. By Theorem 5 and (13), $|d_m| \le t \le \binom{k-2}{\lfloor (k-2)/2\rfloor}$. ∎

Proof of Lemma 3. For $f(x) = \sum_{m\ge0} a_m x^m \in \mathbb{Z}[[x]]$ we define $H, S \in [0,\infty]$ by

$$H(f) = \max_{m\ge0} |a_m|, \quad S(f) = \sum_{m\ge0} |a_m|.$$

We call $H(f)$ the *height* of f. Note that

$$H\Big(f(x)\prod_{i=1}^{k} Q_i(x)\Big) \le H(f)\prod_{i=1}^{k} S(Q_i), \tag{14}$$

$$S\Big(\prod_{i=1}^{k} Q_i(x)\Big) \le \prod_{i=1}^{k} S(Q_i) \tag{15}$$

for $Q_1, \ldots, Q_k \in \mathbb{Z}[x]$ and a formal power series f. By (15) we have, for $j < k$,

$$S_{p_1\ldots p_j} \le (\deg(\Phi_{p_1\ldots p_j}) + 1)A_{p_1\ldots p_j} \le \epsilon_j \cdot p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1},$$

as $\deg(\Phi_n) = \varphi(n) < n$ for $n > 1$. Then again by (15),

$$S(P_j) \le \epsilon_j^{k-j-1}(p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1})^{k-j-1}, \tag{16}$$

where P_j is defined in Lemma 1. Additionally,

$$S_{p_1p_2} < p_1p_2/2, \quad S_{p_1p_2p_3} \le d \cdot p_1^2 p_2 p_3. \tag{17}$$

Applying (14), (16), (17) and Lemma 2 to Lemma 1 we obtain

$$\begin{aligned} A_{p_1\ldots p_k} &\le \frac{b_{k-2}d^{k-4}}{2^{k-3}} \cdot \prod_{j=1}^{k-2} \epsilon_j^{k-j-1} \cdot \prod_{j=1}^{k-2} (p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1})^{k-j-1} \\ &= E_k M_n, \end{aligned}$$

which completes the proof. ∎

4. Proofs of Theorems 1–4

Proof of Theorem 1. Consider a sequence (e_n) given by the following conditions:

$$e_1 = e_2 = 1, \quad e_3 = e_4 = \epsilon_3,$$

$$e_k = \frac{b_{k-2}d^{k-4}}{2^{k-3}} \prod_{j=1}^{k-2} e_j^{k-j-1} \quad \text{for } k \ge 5.$$

By Lemmas 3 and 4 we have $\epsilon_k \le e_k$. We can easily compute that

$$e_5 = \frac{3}{4}\epsilon_3 d, \quad e_6 = \frac{3}{4}\epsilon_3^3 d^2, \quad \ldots \tag{18}$$

For $k \ge 7$,

$$\frac{e_k/e_{k-1}}{e_{k-1}/e_{k-2}} = \frac{\frac{db_{k-2}}{2b_{k-3}} \cdot e_1 \ldots e_{k-2}}{\frac{db_{k-3}}{2b_{k-4}} \cdot e_1 \ldots e_{k-3}} = e_{k-2} \cdot \frac{b_{k-2}b_{k-4}}{b_{k-3}^2},$$

so

$$e_k = e_{k-1}^2 \cdot \frac{b_{k-2}b_{k-4}}{b_{k-3}^2},$$

and hence

$$e_k = e_6^{2^{k-6}} \cdot \prod_{i=7}^{k} \left(\frac{b_{i-2}b_{i-4}}{b_{i-3}^2}\right)^{2^{k-i}}.$$

Note that

$$\frac{b_{i-2}b_{i-4}}{b_{i-3}^2} = \begin{cases} \dfrac{i-2}{i-1} & \text{for odd } i, \\ \dfrac{i-2}{i-3} & \text{for even } i. \end{cases}$$

Then

$$e_k^{1/2^{k-8}} = e_6^4 \quad \cdot \left(\frac{5}{6}\right)^2 \cdot \left(\frac{6}{5}\right) \cdot \left(\frac{7}{8}\right)^{1/2} \cdot \left(\frac{8}{7}\right)^{1/4} \cdot \ldots = e_6^4 \rho + o(1),$$

with ρ as in (3). ∎

For $\epsilon_3 = 3/4$, the bounds (4) follow from (18) and Lemma 5.

Proof of Theorem 2. By the well known formula $\Psi_{np}(x) = \Psi_n(x^p)\Phi_n(x)$ we have

$$c_{np}(m) = \prod_{j=0}^{\lfloor m/p \rfloor} c_n(j) a_n(m - jp).$$

We note that $a_n(t) = 0$ for $t \notin \{0, \ldots, \varphi(n)\}$, and therefore

$$C_{p_1 \ldots p_k} \le \left(\left\lfloor \frac{\varphi(p_1 \ldots p_{k-1})}{p_k} \right\rfloor + 1 \right) A_{p_1 \ldots p_{k-1}} C_{p_1 \ldots p_{k-1}} \le p_1 \ldots p_{k-2} \cdot A_n C_n$$

for $k \ge 2$. Thus

$$C_{p_1 \ldots p_k} \le C_{p_1 p_2} \prod_{j=2}^{k-1} (p_1 \ldots p_{j-1} \cdot A_{p_1 \ldots p_j}) \le \epsilon_2 \ldots \epsilon_{k-1} M_n.$$

Therefore

$$\epsilon_k^{\mathrm{inv}} \le \epsilon_2 \ldots \epsilon_{k-1} \le e_1 \ldots e_{k-1} = \frac{2b_{k-3}}{db_{k-2}} e_k$$

for $k \ge 6$. The proof is completed by invoking Theorem 1. ∎

We can also prove that

$$\epsilon_4^{\mathrm{inv}} \le \epsilon_3, \quad \epsilon_5^{\mathrm{inv}} \le \epsilon_3^2, \quad \epsilon_6^{\mathrm{inv}} \le \frac{3}{4} \epsilon_3^3 d.$$

Using Lemma 5 we obtain the inequalities from (5).

Proof of Theorem 3. We recall that every divisor of $x^n - 1$ is of the form $\prod_{d \in D} \Phi_d(x)$, where D is a set of divisors of n. By (14) and Theorem 1,

$$B_n \le A_n \prod_{d|n,\, d<n} S_d \le \frac{2}{n} \prod_{d|n} dA_d$$

$$\le \frac{2}{n} \Big(\prod_{d|n} d \Big) \Big(\prod_{d|n} \epsilon_{\omega(d)} \Big) \Big(\prod_{d|n} M_d \Big).$$

We have

$$\frac{1}{n}\prod_{d|n} d = n^{2^{k-1}-1},$$

$$\prod_{d|n} M_n(d) \le \prod_{\omega=1}^{k} \left(((\sqrt[k]{n})^{\omega})^{2^{\omega-1}/\omega-1}\right)^{\binom{k}{\omega}} = n^{(3^k-1)/(2k)-2^{k-1}}.$$

Put $\xi_\omega = \max\{2^{-\omega}\log\epsilon_\omega - \log C, 0\}$. Then

$$\log\Bigl(2\prod_{d|n}\epsilon_{\omega(d)}\Bigr) \sim \sum_{\omega=0}^{k}\binom{k}{\omega}\log\epsilon_\omega \le 3^k\log C + \sum_{\omega=0}^{k}\binom{k}{\omega}2^\omega\xi_\omega.$$

It remains to prove that the sum is of size $o(3^k)$. Let $\xi'_\omega = \sup\{\xi_\omega, \xi_{\omega+1}, \ldots\}$. By Theorem 1 for $\omega \to \infty$ we have $\xi_\omega \to 0$ and hence also $\xi'_\omega \to 0$. Therefore

$$\begin{aligned}\sum_{\omega=0}^{k}\binom{k}{\omega}2^\omega\xi_\omega &\le \xi'_0\sum_{\omega=0}^{\lfloor\log k\rfloor}\binom{k}{\omega}2^\omega + \xi'_{\lceil\log k\rceil}\sum_{\omega=0}^{k}\binom{k}{\omega}2^\omega\\ &= O(2^{\log k}e^{\log^2 k}\log k) + o(3^k) = o(3^k). \ \blacksquare\end{aligned}$$

Proof of Theorem 4. We have $M_1 = M_2 = 1$, so the conclusion holds for $k = 1, 2$. We argue by induction on k. We assume that $p_1 < \cdots < p_k$. Then for $k \ge 3$,

$$\begin{aligned}M_n &\le p_1^{2^{k-2}-1}\cdot\varphi(p_2\ldots p_k)^{2^{k-2}/(k-1)-1}\\ &= \left(\frac{p_1}{p_1-1}\right)^{\frac{2^{k-1}}{k}-1}\cdot\left(\frac{p_1^{k-1}}{\varphi(p_2\ldots p_k)}\right)^{\frac{2^{k-2}}{k-1}-\frac{2^{k-1}}{k(k-1)}}\cdot(\varphi(p_1\ldots p_k))^{\frac{2^{k-1}}{k}-1}\\ &\le \left(\frac{p_1}{p_1-1}\right)^{\frac{2^{k-1}}{k}-1}\cdot\left(\frac{p_1}{p_1+1}\right)^{2^{k-2}-\frac{2^{k-1}}{k}}\cdot(\varphi(p_1\ldots p_k))^{\frac{2^{k-1}}{k}-1}.\end{aligned}$$

Since

$$\frac{p_1}{p_1-1}\left(\frac{p_1}{p_1+1}\right)^2 < 1$$

and for $k \ge 3$ we have

$$\frac{2^{k-2}-\frac{2^{k-1}}{k}}{\frac{2^{k-1}}{k}-1} \ge 2,$$

the proof of Theorem 4 is complete. $\blacksquare$

5. Concluding remarks. Note that there exists a constant $c > 0$ such that for $C < c$ the bound from Theorem 1 is false. Indeed, if p_j is the jth odd prime number for $j \ge 1$, then

$$1 \le A_{p_1\ldots p_k} \le (C + o_k(1))^{2^k} M_n$$

and therefore

$$C + o_k(1) \geq M_n^{-2^k} = \prod_{j=1}^{\infty} p_j^{-2^{3-j}} + o_k(1).$$

Using the prime number theorem we easily see that the product is convergent to a positive constant c, which is relatively small. We then have

$$0 < c \leq \limsup_{n\to\infty} \left(\frac{A_n}{M_n}\right)^{2^{-\omega(n)}} \leq C < 1.$$

Recall the following conjecture of P. T. Bateman, C. Pomerance and R. C. Vaughan [3].

Conjecture 2. *For every k there exists a constant ϵ_k' such that*

$$A_n \geq \epsilon_k' n^{2^{k-1}/k-1}$$

for infinitely many cyclotomic polynomials Φ_n of order k.

If the conjecture is true, one of the most interesting questions is whether the maximal ϵ_k' is of the form $(C' + o(1))^{2^k}$ for some constant $0 < C' < 1$.

Acknowledgments. The author would like to thank Pieter Moree for his suggestions as to how to make the paper more interesting, and for making some corrections. The author would also like to thank Wojciech Gajda for his remarks on the paper.

References

[1] G. Bachman, *On the coefficients of ternary cyclotomic polynomials*, J. Number Theory 100 (2003), 104–116.

[2] A. S. Bang, *Om Ligningen $\Phi_n(x) = 0$*, Nyt Tidsskr. Math. Afdeling B 6 (1895), 6–12.

[3] P. T. Bateman, C. Pomerance and R. C. Vaughan, *On the size of the coefficients of the cyclotomic polynomial*, in: Topics in Classical Number Theory (Budapest, 1981), Colloq. Math. Soc. János Bolyai 34, North-Holland, 1984, 171–202.

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

[5] D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly 75 (1968), 370–372.

[6] B. Bzdęga, *Bounds on ternary cyclotomic coefficients*, Acta Arith. 144 (2010), 5–16.

[7] Y. Gallot and P. Moree, *Ternary cyclotomic polynomials having a large coefficient*, J. Reine Angew. Math. 632 (2009), 105–125.

[8] N. Kaplan, *Bounds for the maximal height of divisors of $x^n - 1$*, J. Number Theory 129 (2009), 2673–2688.

[9] B. Lawrence, *Bounding the coefficients of $\Phi_{pqr}(x)$*, Joint Mathematics Meeting of AMS/MAA (2009), 1046-11-1150.

[10] A. Migotti, *Zur Theorie der Kreisteilung*, S. B. Math.-Naturwiss. Cl. Kaiserlichen Akad. Wiss. Wien 87 (1883), 7–14.

[11] P. Moree, *Inverse cyclotomic polynomials*, J. Number Theory 129 (2009), 667–680.

[12] C. Pomerance and N. C. Ryan, *Maximal height of divisors of* $x^n - 1$, Illinois J. Math. 51 (2007), 597–604.

[13] E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. 27 (1928), 544–548.

[14] R. Thangadurai, *On the coefficients of cyclotomic polynomials*, in: Cyclotomic Fields and Related Topics (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, 311–322,.

[15] J. Zhao and X. Zhang, *A proof of the corrected Beiter conjecture*, arXiv:0910.2770v1 [math.NT].

Bartłomiej Bzdęga
Stróżyńskiego 15A/20
60-688 Poznań, Poland
E-mail: exul@wp.pl

Received on 29.12.2010
and in revised form on 14.8.2011 (6591)