ACTA ARITHMETICA
173.2 (2016)

On a generalization of the Beiter Conjecture

by

Bartłomiej Bzdęga (Poznań)

1. Introduction. Let Φ_n be the nth cyclotomic polynomial, i.e. the unique monic polynomial irreducible over integers, whose roots are all primitive nth roots of unity. We assume that $n = p_1 \ldots p_w$ and $2 < p_1 < p_2 < \cdots < p_w$ are primes, since $\Phi_{2n}(x) = \Phi_n(-x)$ for odd n and $\Phi_{np}(x) = \Phi_n(x^p)$ for a prime p dividing n. In this case we call the number $w = \omega(n)$ the *order* of Φ_n.

Let A_n denote the maximal absolute value of a coefficient of Φ_n. We say briefly that A_n is the height of Φ_n. For $w \in \{0, 1, 2\}$, determining A_n is easy and we have $A_1 = A_{p_1} = A_{p_1p_2} = 1$. For $w = 3$ it is known that $A_{p_1p_2p_3} \le \frac{3}{4}p_1$ (see [1]). The Corrected Beiter Conjecture states that $A_{p_1p_2p_3} \le \frac{2}{3}p_1$ (see [4] and references given there for details). The constant $2/3$ is best possible if the conjecture is true.

For cyclotomic polynomials of any order we set

$$M_n = \prod_{i=1}^{w-2} p_i^{2^{w-1-i}-1},$$

where the empty product, which occurs if $w \le 2$, equals 1. P. T. Bateman, C. Pomerance and R. C. Vaughan [2] proved that $A_n \le M_n$. In [3] the present author proved that $A_n \le C_w M_n$, where $C_w^{2^{-w}}$ converges to approximately 0.95 with $w \to \infty$. However, so far no good general class of Φ_n for which A_n is close to $C_w M_n$ has been known.

It has not even been known whether M_n gives the optimal order for the upper bound on A_n. For example we have $A_{p_1\ldots p_5} \le C_5 p_1^7 p_2^3 p_3$, but it has not been clear whether maybe $A_{p_1\ldots p_5} \le C'_5 p_1^8 p_2^2 p_3$ for some other constant C'_5. All known constructions of Φ_n with large height required most prime factors of n to be of almost the same size.

2010 *Mathematics Subject Classification*: 11B83, 11C08.
Key words and phrases: cyclotomic polynomial, coefficient, height of a polynomial.
Received 24 March 2015; revised 15 January 2016.
Published online 11 May 2016.

DOI: 10.4064/aa8119-1-2016

One of the main purposes of this paper is to show that M_n is optimal, i.e. in the upper bound on A_n it cannot be replaced by any smaller product of the form $p_1^{\alpha_1} \dots p_w^{\alpha_w}$ in the sense described below.

For a fixed w we define the following strict lexicographical order on $\mathbb{R}^w$:

$$(\alpha_1, \dots, \alpha_w) \prec (\beta_1, \dots, \beta_w)$$
$$\Leftrightarrow \ \alpha_w = \beta_w, \alpha_{w-1} = \beta_{w-1}, \dots, \alpha_{k+1} = \beta_{k+1} \text{ and } \alpha_k < \beta_k \text{ for some } k \le w.$$

For $\alpha = (\alpha_1, \dots, \alpha_w)$ and $n = p_1 \dots p_w$ we set $M_n^{(\alpha)} = p_1^{\alpha_1} \dots p_w^{\alpha_w}$. Note that if $\alpha \prec \beta$ are fixed and p_i is large enough compared to $p_1 \dots p_{i-1}$ for all $i \le w$, then $M_n^{(\alpha)} < M_n^{(\beta)}$.

We say that $M_n^{(\alpha)}$ is the *optimal bound* on A_n for a fixed w if there exists a constant b_w such that $A_n \le b_w M_n^{(\alpha)}$ for all odd squarefree n with $\omega(n) = w$ and α is smallest possible in the sense of the order $\prec$.

We have to explain what it means that p_i is large enough compared to $p_1 \dots p_{i-1}$ for all $i \le w$. Let $h : \mathbb{R}_+ \to \mathbb{R}_+$ be any function, preferably growing fast. We say that a sequence of primes $p_1, \dots, p_w$ is *h-growing* if $p_i \ge h(p_1 \dots p_{i-1})$ for $i = 1, \dots, w$ (an empty product equals 1). With a small abuse of notation we will also write that the number $n = p_1 \dots p_w$ is h-growing.

The following theorem is the main result of this paper.

THEOREM 1. *For every $w \ge 3$, $\varepsilon > 0$ and $h : \mathbb{R}_+ \to \mathbb{R}_+$ there exists an h-growing $n = p_1 \dots p_w$ such that $A_n > (1 - \varepsilon) c_w M_n$, where*

$$M_n = \prod_{i=1}^{w-2} p_i^{2^{w-1-i}-1} \quad \textit{and} \quad c_w = \frac{1}{w} \cdot \left(\frac{2}{\pi}\right)^{3 \cdot 2^{w-3}} \cdot \left(\prod_{k=3}^{w-1} k^{2^{w-1-k}}\right)^{-1}.$$

By this theorem and the already mentioned result from [3], M_n is the optimal bound on A_n. Furthermore,

$$\lim_{w \to \infty} c_w^{2^{-w}} = \left(\frac{2}{\pi}\right)^{3/8} \cdot \prod_{k=3}^{\infty} k^{-2^{-k-1}} \approx 0.71.$$

Let us define the wth *Beiter constant* in the following natural way:

$$B_w = \limsup_{\omega(n)=w} (A_n / M_n).$$

For example, we know that $B_0 = B_1 = B_2 = 1$ and $2/3 \le B_3 \le 3/4$. If the Corrected Beiter Conjecture is true, then $B_3 = 2/3$.

For all w we have

$$c + o(1) < B_w^{2^{-w}} < C + o(1), \quad w \to \infty,$$

with $c \approx 0.71$ and $C \approx 0.95$. It would be interesting to know the asymptotics of B_w. For example, we expect that the following natural conjecture is true.

CONJECTURE 2. *The limit $\lim_{w \to \infty} B_w^{2^{-w}}$ exists.*

2. Preliminaries and the binary case. For $n > 1$ we define the value

$$L_n = \max_{|z|=1} |\Phi_n(z)|.$$

It was already considered by several authors [2, 5, 6] while estimating A_n. If S_n denotes the sum of the absolute values of the coefficients of Φ_n, then for $n > 1$ we have

$$A_n \geq \frac{S_n}{\deg \Phi_n + 1} \geq \frac{L_n}{n}.$$

We express $|\Phi_n(z)|$ as a real function of $x = \arg(z)$ for $|z| = 1$. For all $n \geq 1$ let

$$F_n(x) = \prod_{d|n} \left(\sin \frac{d}{2} x\right)^{\mu(n/d)},$$

where μ is the Möbius function. It is readily seen (see proof of Lemma 3 below) that this expression serves to define a continuous function of the real variable x. Moreover, $|F_n(x)| = |F_n(x + 2\pi)|$ and $F_{np}(x) = F_n(px)/F_n(x)$ for any prime p not dividing n.

Lemma 3. *For $n > 1$ we have $|\Phi_n(e^{ix})| = |F_n(x)|$.*

Proof. By elementary computations $|1 - z| = 2\left|\sin \frac{1}{2} x\right|$. Then we use the well known formula $\Phi_n(z) = \prod_{d|n} (1 - z^d)^{\mu(n/d)}$. Note that $\Phi_n(e^{ix})$ is a bounded continuous function of x, so if the product $F_n(x_0)$ is not defined for some x_0 (which happens only for finitely many values of $0 \leq x_0 < 2\pi$), then we can replace it by its limit as $x \to x_0$. ∎

A consequence of Lemma 3 is that $F_n(x_0) = 0$ if and only if $x_0 = 2\pi t_0/n$ for some t_0 coprime to n. Also, we have

$$L_n = \max_{|z|=1} |\Phi_n(z)| = \max_{0 \leq x < 2\pi} |F_n(x)|$$

as long as $n > 1$. Additionally, we set $L_1 = \max_{0 \leq x < 2\pi} |F_1(x)| = 1$.

It is easy to determine $L_{p_1} = p_1$. Let us consider the case $w = 2$.

Theorem 4. *Let $p_1 < p_2$ be primes and let a be the unique integer such that $p_1 \mid p_2 + 2a$ and $|a| < p_1/2$. Then*

$$L_{p_1 p_2} \geq \frac{4(p_1 - 2)p_2}{\pi^2 |2a + 1|}.$$

Proof. Set

$$x = \left(1 + \frac{1}{p_1} + \frac{2a + 1}{p_1 p_2}\right)\pi.$$

Then

$$\left|\sin\frac{p_1p_2x}{2}\right| = \left|\sin\frac{p_1p_2+p_2+2a+1}{2}\pi\right| = 1,$$

$$\left|\sin\frac{x}{2}\right| = \left|\cos\left(\frac{1}{2p_1}+\frac{2a+1}{2p_1p_2}\right)\pi\right| \geq 1-\frac{1}{p_1}-\frac{|2a+1|}{p_1p_2} \geq 1-\frac{2}{p_1},$$

where we have used the inequality $\cos t \geq 1-\frac{2}{\pi}\cdot|t|$ for $|t| \leq \pi/2$. Furthermore,

$$\left|\sin\frac{p_1x}{2}\right| = \left|\sin\left(\frac{p_1+1}{2}+\frac{2a+1}{2p_2}\right)\pi\right| = \left|\sin\frac{2a+1}{2p_2}\pi\right| \leq \frac{|2a+1|\pi}{2p_2},$$

$$\left|\sin\frac{p_2x}{2}\right| = \left|\sin\left(\frac{p_2}{2}+\frac{p_2+2a}{2p_1}+\frac{1}{2p_1}\right)\pi\right| = \left|\sin\frac{\pi}{2p_1}\right| \leq \frac{\pi}{2p_1},$$

where we have used the inequality $|\sin t| \leq |t|$ for $t \in \mathbb{R}$. By the above inequalities we obtain

$$L_{p_1p_2} \geq |F_{p_1p_2}(x)| = \left|\frac{\sin(x/2)\sin(p_1p_2x/2)}{\sin(p_1x/2)\sin(p_2x/2)}\right| \geq \frac{4(p_1-2)p_2}{\pi^2|2a+1|}. \ \blacksquare$$

3. Derivative of F_n. It is not difficult to prove that F_n is a differentiable function. Let $f_n(x)$ be its derivative. Define

$$D_n = \min_{x\colon F_n(x)=0} |f_n(x)|.$$

The aim of this section is to prove the following theorem.

THEOREM 5. *For all positive integers w and all $\varepsilon > 0$ there exists a function $h_{w,\varepsilon} : \mathbb{R}_+ \to \mathbb{R}_+$, depending only on w and ε, such that*

$$\frac{n}{2}(L_{p_1}L_{p_1p_2}\ldots L_{p_1\ldots p_{w-1}})^{-1} \leq D_n < (1+\varepsilon)\frac{n}{2}(L_{p_1}L_{p_1p_2}\ldots L_{p_1\ldots p_{w-1}})^{-1}$$

for all $h_{w,\varepsilon}$-growing $n = p_1\ldots p_w$.

In order to prove this theorem we will need some lemmas.

LEMMA 6. *Let p be a prime not dividing n. If $F_{np}(x_1) = 0$, then*

$$f_{np}(x_1) = \frac{pf_n(x_1p)}{F_n(x_1)}.$$

Proof. We have $x_1 = 2\pi t_1/(np)$ for some t_1 coprime to np, so $F_n(px_1) = 0$ and $F_n(x_1) \neq 0$. Using the equality $F_{np}(x) = F_n(px)/F_n(x)$ and the quotient rule we obtain

$$f_{np}(x_1) = \frac{pf_n(px_1)F_n(x_1) - F_n(px_1)f_n(x_1)}{(F_n(x_1))^2} = \frac{pf_n(x_1p)}{F_n(x_1)}. \ \blacksquare$$

LEMMA 7. *We have*

$$D_{np} \geq pD_n/L_n.$$

Moreover, for all $\varepsilon > 0$ there exists a function $h_\varepsilon : \mathbb{R}_+ \to \mathbb{R}_+$, depending only on ε, such that

$$D_{np} < (1+\varepsilon)p\frac{D_n}{L_n} \qquad \textit{for all } p > h_\varepsilon(n).$$

Proof. Let x_0 and x_1 be such that $F_n(x_0) = F_{np}(x_1) = 0$, $|f_n(x_0)| = D_n$ and $|f_{np}(x_1)| = D_{np}$. Since $x_1 = 2t_1\pi/(np)$ for some t_1 coprime to np, we have $px_1 = 2t_1\pi/n$. Therefore $F_n(px_1) = 0$ and hence $|f_n(px_1)| \geq D_n$. By applying this inequality and Lemma 6 we obtain

$$D_{np} = |f_{np}(x_1)| = \frac{p|f_n(px_1)|}{|F_n(x_1)|} \geq p\frac{D_n}{L_n}.$$

To obtain the opposite inequality, let

$$x_0 = \frac{2t_0\pi}{n} \quad \text{and} \quad x_1' = \frac{x_0+2t\pi}{p} = \frac{2(t_0+tn)\pi}{np} \quad \text{with any } t \not\equiv -\frac{t_0}{n} \pmod{p}.$$

Then $F_{np}(x_1') = 0$ and $f_n(px_1') = D_n$. Again by Lemma 6,

$$D_{np} \leq |f_{np}(x_1')| = \frac{p|f_n(px_1')|}{|F_n(x_1')|} = p\frac{D_n}{\left|F_n\left(\frac{x_0+2t\pi}{p}\right)\right|}.$$

By choosing an appropriate t we can have $\left|F_n\left(\frac{x_0+2t\pi}{p}\right)\right|$ as close to L_n as we wish when $p \to \infty$. ∎

Now we are ready to prove the main theorem of this section.

Proof of Theorem 5. Fix $\varepsilon > 0$ and let $\varepsilon' = \sqrt[w]{1+\varepsilon} - 1$. Let $h_{\varepsilon'}$ be the function given by Lemma 7. If $n = p_1 \ldots p_w$ is $h_{\varepsilon'}$-growing, then

$$p_i\frac{D_{p_1\ldots p_{i-1}}}{L_{p_1\ldots p_{i-1}}} \leq D_{p_1\ldots p_i} < (1+\varepsilon')p_i\frac{D_{p_1\ldots p_{i-1}}}{L_{p_1\ldots p_{i-1}}}$$

for $i = 1, \ldots, w$ (empty product equals 1). By these inequalities,

$$\frac{nD_1}{L_1L_{p_1}L_{p_1p_2}\ldots L_{p_1\ldots p_{w-1}}} \leq D_n < (1+\varepsilon')^w\frac{nD_1}{L_1L_{p_1}L_{p_1p_2}\ldots L_{p_1\ldots p_{w-1}}}.$$

Note that $(1+\varepsilon')^w = 1+\varepsilon$, $L_1 = 1$ and $D_1 = 1/2$. So the conclusion of the theorem holds with $h_{w,\varepsilon} = h_{\varepsilon'} = h_{\sqrt[w]{1+\varepsilon}-1}$, which clearly depends only on w and ε. ∎

4. Proof of the main result. In the following lemma we give a lower bound on L_{np} which depends on the residue class of p modulo n.

LEMMA 8. *Let $\varepsilon > 0$ and $n = p_1 \ldots p_w$ be fixed. Choose $x_M \in [0, 2\pi)$ such that $F_n(x_M) = L_n$, and $x_0 = 2t_0\pi/n$ for which $F_n(x_0) = 0$ and $|f_n(x_0)| = D_n$. Let*

$$b = \min_{k\in\mathbb{Z}}\left|\frac{nx_M}{2\pi} - pt_0 + nk\right|.$$

Then

$$L_{np} > (1-\varepsilon)L_n\frac{np}{2b\pi D_n}$$

for every p large enough. Furthermore, if $p_1 > w$ and r is an integer coprime to n such that $\left|\frac{nx_M}{2\pi} - r\right|$ is smallest possible, then

$$L_{np} > (1-\varepsilon)L_n\frac{1}{\pi(w+1)}\cdot\frac{np}{D_n}$$

for every sufficiently large $p \equiv r/t_0 \pmod n$.

Proof. We have $F_{np}(x) = F_n(px)/F_n(x)$, so

$$L_{np} = \max_{0\le x<2\pi}\left|\frac{F_n(px)}{F_n(x)}\right| \ge \max_{k\in\mathbb{Z}}\frac{|F_n(x_M+2k\pi)|}{\left|F_n\left(\frac{x_M+2k\pi}{p}\right)\right|} = \frac{L_n}{\min_{k\in\mathbb{Z}}\left|F_n\left(\frac{x_M+2k\pi}{p}\right)\right|}.$$

Let k_0 be an integer for which $|(x_M+2k_0\pi)/p - x_0|$ is smallest possible. Then

$$\begin{aligned}\min_{k\in\mathbb{Z}}\left|F_n\left(\frac{x_M+2k\pi}{p}\right)\right| &\le \left|F_n\left(\frac{x_M+2k_0\pi}{p}\right)\right| \\ &\sim |f_n(x_0)|\cdot\left|\frac{x_M+2k_0\pi}{p} - x_0\right| \quad (\text{as } p\to\infty) \\ &= D_n\frac{2\pi}{np}\left|\frac{nx_M}{2\pi} - t_0p + k_0n\right| \\ &= D_n\frac{2b\pi}{np}.\end{aligned}$$

Therefore

$$L_{np} > (1+o(1))\frac{L_n}{D_n\frac{2b\pi}{np}} \sim L_n\frac{np}{2b\pi D_n}$$

as $p\to\infty$, which completes the proof of the first statement.

For $p \equiv r/t_0 \pmod n$ we have

$$b = \min_{k\in\mathbb{Z}}\left|\frac{nx_M}{2\pi} - pt_0 + nk\right| = \left|\frac{nx_M}{2\pi} - r\right| \le \frac{w+1}{2}$$

since, in view of $p_1 > w$, at most w consecutive integers are not coprime to n. ■

Simple calculations show that Theorem 4 gives a better lower bound for $L_{p_1p_2}$ than Lemma 8. Therefore we use Theorem 4 in the proof of the main result. As $A_n \ge L_n/n$ for $n > 1$, Theorem 1 is an immediate consequence of the following theorem.

THEOREM 9. *For every $w \ge 3$, $\varepsilon > 0$ and $h : \mathbb{R}_+ \to \mathbb{R}_+$ there exists an h-growing $n = p_1\ldots p_w$ such that $L_n > (1-\varepsilon)c_wnM_n$, where c_w and M_n are defined in Theorem 1.*

Proof. We prove this by induction on $w = \omega(n)$. The induction starts with $w = 2$.

Our inductive assumption is that for all $\varepsilon' > 0$ and a function $h : \mathbb{R}_+ \to \mathbb{R}_+$ there exists an h-growing $n = p_1 \dots p_w$ such that $L_{p_1 p_2} > (1-\varepsilon')\frac{4}{\pi^2}p_1 p_2$ and $L_{p_1\dots p_i} > (1-\varepsilon')c_i p_1 \dots p_i M_{p_1\dots p_i}$ for $3 \le i \le w$. By Theorem 4 it is true for $w = 2$ with $p_1 \mid p_2 - 2$ (note that the second part of the inductive assumption is empty when $w = 2$).

Now we show the inductive step. Let $w \ge 2$. Without loss of generality we may assume that h satisfies the requirements of Theorem 5 and $h(1) \ge w$. By Lemma 8 and Dirichlet's theorem on primes in arithmetic progressions, there exists $p_{w+1} > h(p_1 \dots p_w)$ for which

$$L_{p_1\dots p_{w+1}} > (1-\varepsilon')L_n \frac{np_{w+1}}{\pi(w+1)D_n}.$$

By Theorem 5,

$$D_n > (1-\varepsilon')^{-1}\frac{n}{2} \cdot \frac{1}{L_{p_1}L_{p_1p_2}\dots L_{p_1\dots p_{w-1}}}.$$

For given $\varepsilon > 0$ we choose $\varepsilon' = 1 - \sqrt[w+1]{1-\varepsilon}$. By the above inequalities and the inductive assumption,

$$\begin{aligned} L_{p_1\dots p_{w+1}} &> (1-\varepsilon')^2 \frac{2p_{w+1}}{\pi(w+1)} L_{p_1}L_{p_1p_2}\dots L_{p_1\dots p_w} \\ &> (1-\varepsilon')^{w+1}\frac{2p_{w+1}}{\pi(w+1)}p_1\frac{4}{\pi^2}p_1\prod_{i=3}^{w}(c_i p_1\dots p_i M_{p_1\dots p_i}) \\ &= (1-\varepsilon)\left(\frac{8}{\pi^3(w+1)}\prod_{i=3}^{w}c_i\right)\left(p_{w+1}\prod_{i=1}^{w}(p_1\dots p_i M_{p_1\dots p_i})\right). \end{aligned}$$

The exponent of p_k in $\prod_{i=1}^{w}(p_1\dots p_i M_{p_1\dots p_i})$ for $k \le w$ equals

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

so

$$p_{w+1}\prod_{i=1}^{w}(p_1\dots p_i M_{p_1\dots p_i}) = p_1\dots p_{w+1}M_{p_1\dots p_{w+1}}.$$

It remains to evaluate the constant by using a similar method:

$$\frac{8}{\pi^3(w+1)}\prod_{i=3}^{w}c_i = \frac{8}{\pi^3(w+1)}\prod_{i=3}^{w}\left(\frac{1}{i}\left(\frac{2}{\pi}\right)^{3\cdot 2^{i-3}}\left(\prod_{k=3}^{i-1}k^{2^{i-1-k}}\right)^{-1}\right)$$

$$= \frac{1}{w+1}\left(\frac{2}{\pi}\right)^{3\cdot 2^{w-2}} \frac{1}{3\cdot 4\cdot \ldots \cdot w}\Big(\prod_{i=3}^{w}\prod_{k=3}^{i-1} k^{2^{i-1-k}}\Big)^{-1}$$

$$= \frac{1}{w+1}\left(\frac{2}{\pi}\right)^{3\cdot 2^{w+1-3}} \Big(\prod_{t=3}^{w+1-1} t^{2^{w+1-1-t}}\Big)^{-1} = c_{w+1}$$

for $w \geq 2$. ∎

Acknowledgements. The author is partially supported by the NCN grant no. 2012/07/D/ST1/02111.

The author would like to thank Pieter Moree for the invitation to Max Planck Institute in Bonn and for the good time spent there.

References

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

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

[3] B. Bzdęga, *On the height of cyclotomic polynomials*, Acta Arith. 152 (2012), 349–359.

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

[5] S. Konyagin, H. Maier and E. Wirsing, *Cyclotomic polynomials with many primes dividing their orders*, Period. Math. Hungar. 49 (2004), 99–106.

[6] H. Maier, *Anatomy of integers and cyclotomic polynomials*, in: Anatomy of Integers, CRM Proc. Lecture Notes 46, Amer. Math. Soc., 2008, 89–95.

Bartłomiej Bzdęga
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
61-614 Poznań, Poland
E-mail: exul@amu.edu.pl