MAXIMAL HEIGHT OF DIVISORS OF $x^n - 1$

CARL POMERANCE AND NATHAN C. RYAN

ABSTRACT. The size of the coefficients of cyclotomic polynomials is a problem that has been well-studied. This paper investigates the following generalization: suppose $f(x) \in \mathbb{Z}[x]$ is a divisor of $x^n - 1$, so that $f(x)$ is the product of the cyclotomic polynomials corresponding to some of the divisors of n. We ask about the largest coefficient in absolute value over all such divisors $f(x)$ of $x^n - 1$, obtaining a fairly tight estimate for the maximal order of this function.

1. INTRODUCTION

We denote the nth cyclotomic polynomial by Φ_n, so that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}, \tag{1.1}$$

where $\mu(n)$ is the Möbius function. Note that Φ_n has integer coefficients, it is irreducible, and its roots are the primitive nth roots of 1. The degree of Φ_n is $\phi(n)$, where ϕ is the Euler totient function. Inverting (1.1), we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

For a nonzero polynomial $f \in \mathbb{C}[x]$, we define its height $H(f)$ to be the largest coefficient of f in absolute value.

In the middle of the last century, Bateman [3] obtained in a simple way an upper bound for $A(n) := H(\Phi_n)$; in particular, he showed that

$$A(n) \le n^{2^{k-1}} \tag{1.2}$$

Date: April 20, 2005 and, in revised form, June 14, 2005.

1991 *Mathematics Subject Classification.* 12Y05, 11C08, 11Y70.

Key words and phrases. cyclotomic polynomials, heights of polynomials.

The first author was supported in part by NSF grant DMS-0401422. The second author was supported in part by a GAANN Fellowship.

if n has exactly k distinct odd prime factors. Using the inequality $k \le (1+o(1)) \log n / \log\log n$ as $n \to \infty$, one then obtains the estimate

$$\log A(n) \le n^{(1+o(1)) \log 2/\log\log n}. \tag{1.3}$$

This last result was first stated by Erdős [6], but he held back its proof because of how complicated it was. Vaughan [13] showed that the inequality (1.3) could be reversed for infinitely many n; that is, with (1.3), we have

$$\limsup_{n\to\infty} \frac{\log\log A(n)}{\log n/\log\log n} = \log 2. \tag{1.4}$$

This result gives then the maximal order of $\log\log A(n)$.

In [4], Bateman, Pomerance, and Vaughan obtain a small improvement on (1.2), and show that it is nearly best possible. These results give then another proof of (1.4).

There have been many other papers dealing with coefficients of cyclotomic polynomials. We mention a few. In [7], the authors study the rth coefficient of the nth cyclotomic polynomial, while in [1], the author studies the maximal order of this statistic for a fixed value of r. In [8], the author studies $A(n)$ for "most" numbers n.

For a polynomial $f \in \mathbb{Z}[x]$, define

$$H^*(f) = \max\{H(g) : g \mid f \text{ and } g \in \mathbb{Z}[x]\}.$$

This paper investigates the following problem: we define the function

$$B(n) = H^*(x^n - 1)$$

and ask about its maximal order. In contrast to (1.4), we show that

$$\limsup_{n\to\infty} \frac{\log\log B(n)}{\log n/\log\log n} = \log 3. \tag{1.5}$$

The proof, which is not deep, uses (1.2) and a result from [4].

The second section of this paper presents explicit formulas for $B(n)$ when n is a prime power or a product of two distinct primes. The next three sections are devoted to a proof of (1.5). In the last section we conclude with some unsolved problems.

The second author first heard of the problem of finding explicit formulas for $B(n)$ when n is of a particular form while attending an MSRI Summer Graduate Program hosted by P. Borwein and M. Filaseta.

2. Explicit Formulas

We always have p, q as primes. Note that if $p \mid n$, then $\Phi_{pn}(x) = \Phi_n(x^p)$, so that $A(pn) = A(n)$. Thus, if one studies coefficients for cyclotomic polynomials, it is sufficient to consider the case that n is

squarefree. It is trivial that $A(p) = 1$, while in 1883 Migotti [9] showed that $A(pq) = 1$. We start our investigation of $B(n)$ by showing similar results for n of the same form.

Lemma 2.1. *Let $p < q$ be primes. Then $B(pq) = p$.*

Proof. The irreducible divisors of $x^{pq} - 1$ are: $\Phi_1(x)$, $\Phi_p(x)$, $\Phi_q(x)$, and $\Phi_{pq}(x)$, so there are 16 possibilities for a divisor f of $x^{pq} - 1$. Obviously we have $H(f) = 1$ for f with 0 or 4 irreducible factors. By Migotti's theorem, $H(f) = 1$ if f has just one irreducible factor. We have $\Phi_p(x)\Phi_{pq}(x) = (x^{pq}-1)/(x^q-1)$, so that $\Phi_p\Phi_{pq}$ has all coefficients 0 or 1, and similarly for $\Phi_q\Phi_{pq}$, and $\Phi_p\Phi_q\Phi_{pq}$, which at x is $(x^{pq}-1)/(x-1)$. This leaves the cases where $\Phi_1 \mid f$ and the case $f = \Phi_p\Phi_q$. In general, if $H(f) = 1$, then $H((x^k-1)f(x)) \le 2$ for any positive integer k. (In fact, if f has all coefficients 0 or 1, then $H((x^k - 1)f(x)) = 1$.) This then handles all of the cases with $\Phi_1 \mid f$ except $f = \Phi_1\Phi_p\Phi_q$. But this polynomial at x is $(x^p-1)\Phi_q(x)$, so $H(f) \le 2$ here as well. Finally we consider $f = \Phi_p\Phi_q$ and note that its height is p. □

Note that in general, if $n = uv$ where $(u, v) = 1$ and $u < v$, then $B(n) \ge H((x^u - 1)/(x - 1) \cdot (x^v - 1)/(x - 1)) = u$.

Now we characterize when $B(n) = 1$.

Proposition 2.2. *$B(n) = 1$ if and only if $n = p^k$*

Proof. Assume that $pq \mid n$ for primes $p < q$. Then by Lemma 2.1, we see that $B(n) \ge p > 1$.

Conversely, assume that $n = p^k$. Let $f = \Phi_{p^{j_1}} \cdots \Phi_{p^{j_r}}$ where $0 < j_1 < \cdots < j_r \le k$. Then

$$f(x) = \prod_{i=1}^{r} \sum_{a=0}^{p-1} x^{ap^{j_i}} = \sum_{i=1}^{r} \sum_{0 \le a_i \le p-1} x^{a_1 p^{j_1} + \cdots a_r p^{j_r}}.$$

We see that these exponents all have different base-p expansions, so that they are all distinct. Thus, f has all coefficients being 0 or 1, so that $H(f) = H(\Phi_1 f) = 1$ for each such f. This handles all divisors of $x^{p^k} - 1$ and so completes the proof. □

3. Preliminary Estimates

Let $c_i(f)$ be the coefficient of x^i in the polynomial $f(x)$. Note that for $f, g \in \mathbb{Z}[x]$ with $\deg f \le \deg g$, it is straightforward to see that

$$H(fg) \le (1 + \deg f)H(f)H(g). \tag{3.1}$$

Indeed, for each integer j,

$$c_j(fg) = \sum_i c_i(f)c_{j-i}(g).$$

The number of nonzero terms in this sum is at most the number of choices for i with $c_i(f) \neq 0$. But, the number of nonzero terms of a polynomial is at most one more than the degree, so that the number of nonzero terms in the sum is at most $1 + \deg f$. Thus, we have (3.1).

This observation is used in the proof of the following:

Lemma 3.1. *Let $f_1, \dots, f_k \in \mathbb{Z}[x]$, with $\deg f_1 \le \cdots \le \deg f_k$. Then*

$$H(f_1 \cdots f_k) \le \prod_{i=1}^{k-1}(1 + \deg f_i) \prod_{i=1}^{k} H(f_i).$$

Proof. The proof is by induction. The inequality is trivial when $k = 1$, and it is (3.1) when $k = 2$. Assume it holds for some $k \ge 2$. Writing $f_1 \dots f_{k+1}$ as f_1 times $f_2 \cdots f_{k+1}$, we have by the case for k and the case for 2 that

$$\begin{aligned} H(f_1 \cdots f_{k+1}) &\le (1 + \deg f_1)H(f_1)H(f_2 \cdots f_{k+1}) \\ &\le (1 + \deg f_1)H(f_1) \prod_{i=2}^{k}(1 + \deg f_i) \prod_{i=2}^{k+1} H(f_i). \end{aligned}$$

Thus, the result at $k + 1$ follows. □

Let $n > 1$ and let $f(x) \mid x^n - 1$ be such that $f(x) \in \mathbb{Z}[x]$ and $H(f) = B(n)$. In other words, fix f to be a divisor of $x^n - 1$ of maximal height. Set notation by writing $f = \Phi_{d_1} \cdots \Phi_{d_k}$, where $\phi(d_1) \le \cdots \le \phi(d_k)$. Then

$$B(n) = H(\Phi_{d_1} \cdots \Phi_{d_k}) \le \prod_{i=1}^{k-1}(1 + \phi(d_i)) \prod_{i=1}^{k} A(d_i).$$

For $d > 1$ we have that $1 + \phi(d) \le d$, and $1 + \phi(1) = 2$. Since $d \le n/2$ for $d \mid n$ and $d < n$, we may assume that each $d_i \le n/2$ for $i < k$. Thus,

$$\prod_{i=1}^{k-1}(1 + \phi(d_i)) \le 2 \prod_{i=1}^{k-1} n/2 \le n^{\tau(n)},$$

where $\tau(n)$ denotes the number of positive divisors of n.

Noting that the case $n = 1$ is trivial, we deduce the following proposition.

Proposition 3.2. *For each n, we have $B(n) \le n^{\tau(n)} \prod_{d \mid n} A(d)$.*

We realize our estimate is rather crude (in fact, the factor $n^{\tau(n)}$ may be replaced with $2n^{\tau(n)/2-1}$ and further improvements are possible), but Proposition 3.2 will suffice for our purposes.

4. Upper Bound

Let $\tau_k(n)$ denote the number of ordered solutions in positive integers of $x_1 \cdots x_k = n$. Known as the Piltz divisor function of order k, we have $\sum_n \tau_k(n)/n^s = \zeta(s)^k$, where ζ is the Riemann zeta function. Note that $\tau_2(n) = \tau(n)$, the ordinary divisor function. From the definition, we have

$$\tau_k(n) = \sum_{d|n} \tau_{k-1}(d).$$

Let $\omega(n)$ denote the number of distinct prime factors of n. We have $\tau_k(n) \geq k^{\omega(n)}$ for all n, with equality when n is squarefree.

We first show that

$$B(n) \leq n^{\tau(n)+\tau_3(n)/2}. \tag{4.1}$$

Indeed, by (1.2) and Proposition 3.2, we have

$$\begin{aligned}
\log B(n) &\leq \tau(n) \log n + \sum_{d|n} 2^{\omega(d)-1} \log d \\
&\leq \tau(n) \log n + \frac{1}{2} \log n \sum_{d|n} \tau(d) \\
&= \tau(n) \log n + \frac{1}{2} \tau_3(n) \log n.
\end{aligned}$$

This then gives (4.1).

It is known that for each fixed integer k,

$$\tau_k(n) \leq n^{(\log k + o(1))/\log\log n}, \quad n \to \infty. \tag{4.2}$$

This estimate for the ordinary divisor function, namely $k = 2$, was first proved by Wigert [14] in 1907, and Ramanujan [12] gave a more elementary proof of this case in 1915. The general estimate (4.2) was stated in Oppenheim [10], with the author claiming that it follows in the same way as Ramanujan's proof in the case $k = 2$. A proof of a somewhat more general result was given in Drozdova and Freĭman [5], also see Postnikov [11], section 4.1.

In light of (4.1), and (4.2) for $k = 2$ and 3, we have proved the upper bound in our main theorem:

Theorem 4.1. *As $n \to \infty$, we have $\log B(n) \leq n^{(\log 3 + o(1))/\log\log n}$.*

5. Lower Bound

It is now convenient to consider another polynomial norm: let $|f| = \max_{|z|=1} |f(z)|$ (where z runs over the unit circle in $\mathbb{C}$). Note that the triangle inequality implies that $|f| \le H(f)(\deg f + 1)$, so that a lower bound for $|f|$ also gives one for $H(f)$.

In [4] the authors prove a useful trigonometric lemma: Suppose that r, k are integers with $r \ge 2$, $k \ge 1$, and n is the product of k distinct primes each congruent to $2r \pm 1 \pmod{4r}$. Then

$$\left|\Phi_n\left((-1)^{k-1}e^{\pi i/(2r)}\right)\right| = \left(\cot\frac{\pi}{4r}\right)^{2^{k-1}}. \tag{5.1}$$

Further, if n is as above, it is clear that every divisor d of n is also a product of distinct primes congruent to $2r \pm 1 \pmod{4r}$. Define

$$\mathcal{D} = \mathcal{D}_n = \{d \mid n \ : \ \omega(d) \equiv 1 \pmod 2\}$$

and let

$$f = f_n = \prod_{d\in\mathcal{D}} \Phi_d.$$

Thus, by (5.1) we have

$$\left|f\left(e^{\pi i/(2r)}\right)\right| = \prod_{d\in\mathcal{D}} \left(\cot\frac{\pi}{4r}\right)^{2^{\omega(d)-1}} = \left(\cot\frac{\pi}{4r}\right)^{\frac{1}{2}\sum_{d\in\mathcal{D}} 2^{\omega(d)}}. \tag{5.2}$$

Now we analyze the expression $\sum_{d\in\mathcal{D}} 2^{\omega(d)}$ in (5.2). Since n is squarefree we have that

$$3^{\omega(n)} = \sum_{d\mid n} 2^{\omega(d)} = \sum_{d\in\mathcal{D}} 2^{\omega(d)} + \sum_{\substack{d\notin\mathcal{D}\\ d\mid n}} 2^{\omega(d)}. \tag{5.3}$$

We argue that the two sums on the right side of (5.3) are about the same size.

Lemma 5.1. *With notation as above,*

$$\sum_{\substack{d\notin\mathcal{D}\\ d\mid n}} 2^{\omega(d)} - \sum_{d\in\mathcal{D}} 2^{\omega(d)} = (-1)^{\omega(n)}.$$

Proof. As above, let $k = \omega(n)$. We have

$$S_1 := \sum_{d\in\mathcal{D}} 2^{\omega(d)} = \sum_{i\equiv 1 \pmod 2} \binom{k}{i} 2^i$$

and

$$S_0 := \sum_{\substack{d\notin\mathcal{D}\\ d\mid n}} 2^{\omega(d)} = \sum_{i\equiv 0 \pmod 2} \binom{k}{i} 2^i.$$

Then, by the binomial theorem, we have that

$$S_0 - S_1 = \sum_i \binom{k}{i} (-2)^i = (1-2)^k = (-1)^k,$$

so the lemma is proved. □

In light of Lemma 5.1, (5.3), and (5.2), we have

$$\left| f\left(e^{\pi i/(2r)}\right)\right| = \left(\cot \frac{\pi}{4r}\right)^{\frac{1}{4}\left(3^k - (-1)^k\right)}. \tag{5.4}$$

Since $\deg f \le n-1$ for $k \ge 1$, we have $B(n) \ge H(f) \ge |f|/n$, so that from (5.4) we have that

$$\log B(n) \ge \frac{1}{4}\left(3^k - 1\right) \log\left(\cot \frac{\pi}{4r}\right) - \log n. \tag{5.5}$$

Now, as in [4], we have

$$\cot \frac{\pi}{4r} > r$$

for $r \ge 2$. Summarizing, we have the following result.

Theorem 5.2. *If $r \ge 2$, $k \ge 1$ are integers and n is the product of k distinct primes that are congruent to $2r \pm 1 \pmod{4r}$, then*

$$\log B(n) > \frac{\log r}{4}\left(3^k - 1\right) - \log n.$$

We apply Theorem 5.2 in the case $r = 2$ and n the product of all of the primes congruent to 3 or 5 (mod 8) up to x. Then, as $x \to \infty$, we have by the prime number theorem for arithmetic progressions, that $x \sim 2 \log n$ and $k = \omega(n) \sim \log n / \log\log n$. Thus we have proved the following result.

Theorem 5.3. *There is an infinite set S of squarefree numbers n such that as $n \to \infty$, $n \in S$, we have*

$$\log B(n) \ge n^{(\log 3 + o(1))/\log\log n}.$$

With Theorem 4.1, we have now proved our main result (1.5).

6. Further Problems

Since Erdős first considered the maximal coefficient of the cyclotomic polynomial, many variations on this theme have been studied. We feel that the problem studied herein will admit the same variety of study.

If $f(x) \mid x^n - 1$ is such that $H(f) = B(n)$, how big are the remaining coefficients of f (compare to [7])? Define the co-height $\widetilde{B}(n)$ to be the height of $(x^n - 1)/f(x)$. Is it the case that $B(n)$ and $\widetilde{B}(n)$ are of approximately the same size?

What can be said about the normal or average order of $B(n)$?

From our limited numerical data, it seems that $B(p^2q) = \min\{p^2, q\}$ for different primes p, q. Does this always hold? It may be tempting to guess that $B(p^aq^b) = \min\{p^a, q^b\}$. But we found, for example, that $B(48) = 6$, $B(135) = 8$, $B(441) = 11$, and $B(675) = 35$, suggesting something subtler is occurring. As in [2], what if n is the product of three distinct primes?

References

1. G. Bachman, *On the coefficients of cyclotomic polynomials*, Mem. Amer. Math. Soc. **106** (1993), vi+80 pp.
2. ———, *On the coefficients of ternary cyclotomic polynomials*, J. Number Theory **100** (2003), 104–116.
3. P. T. Bateman, *Note on the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **55** (1949), 1180–1181.
4. P. T. Bateman, C. Pomerance, and R. C. Vaughan, *On the size of the coefficients of the cyclotomic polynomial*, Topics in classical number theory, Vol. I, II (Budapest, 1981), Colloq. Math. Soc. János Bolyai, vol. 34, North-Holland, Amsterdam, 1984, pp. 171–202.
5. A. A. Drozdova and G. A. Freĭman, *The estimation of certain arithmetic functions*, in Russian, Elabuž. Gos. Ped. Inst. Učen. Zap. **3** (1958), 160–165.
6. P. Erdős, *On the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **52** (1946), 179–184.
7. P. Erdős and R. C. Vaughan, *Bounds for the r-th coefficients of cyclotomic polynomials*, J. London Math. Soc. (2) **8** (1974), 393–400.
8. H. Maier, *The size of the coefficients of cyclotomic polynomials*, Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math., vol. 139, Birkhäuser Boston, 1996, pp. 633–639.
9. A. Migotti, *Zur Theorie der Kreisteilungsgleichung*, Sitz. Akad. Wiss. Wien (Math.) (2) **87** (1883), 7–14.
10. A. Oppenheim, *On an arithmetic function*, J. London Math. Soc. **1** (1926), 205–211.
11. A. G. Postnikov, *Introduction to analytic number theory*, translated from the 1971 Russian edition by G. A. Kandall, with an appendix by P. D. T. A. Elliott, Translations of Mathematical Monographs, vol. 68, Amer. Math. Soc., 1988.
12. S. Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. (2) **14** (1915), 347–409.
13. R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. **21** (1974), 289–295 (1975).
14. S. Wigert, *Sur l'ordre de grandeur du nombre des diviseurs d'un entier*, Arkiv för Matematik, Astronomi och Fysik **3** (1907), 1–9.

Mathematics Department, Dartmouth College, Hanover, NH 03755
E-mail address: carl.pomerance@dartmouth.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755
E-mail address: ncr@math.dartmouth.edu