HEIGHTS OF DIVISORS OF $x^n - 1$

LOLA THOMPSON

ABSTRACT. The height of a polynomial with integer coefficients is the largest coefficient in absolute value. Many papers have been written on the subject of bounding heights of cyclotomic polynomials. One result, due to H. Maier, gives a best possible upper bound of $n^{\psi(n)}$ for almost all n, where $\psi(n)$ is any function that approaches infinity as $n \to \infty$. We will discuss the related problem of bounding the maximal height over all polynomial divisors of $x^n - 1$ and give an analogue of Maier's result in this scenario.

For my adviser Carl Pomerance on his 65^{th} birthday

1. Introduction and statement of the principal result

Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial. The n^{th} cyclotomic polynomial is the unique monic irreducible polynomial over $\mathbb{Q}$ with the primitive n^{th} roots of unity as its roots. It has integer coefficients. The degree of $\Phi_n(x)$ is $\varphi(n)$, where φ is the Euler totient function.

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value. We will denote the height of a polynomial f by $H(f)$.

Much has been studied about $H(\Phi_n)$, which shall henceforth be denoted $A(n)$. In 1946, P. Erdős stated that $\log A(n) \leq n^{(1+o(1)) \log 2/ \log\log n}$. He held back its proof because of how complicated it was. R. C. Vaughan showed in 1975 that this inequality can be reversed for infinitely many n.

In 1949, P.T. Bateman gave a simple argument that if k is a given positive integer then $A(n) \leq n^{2^{k-1}}$ if n has exactly k distinct prime factors. Let $\omega(n)$ denote the number of distinct prime factors of n. By taking the log of both sides of Bateman's inequality and using the fact that the maximal order of $\omega(n)$ is $\frac{\log n}{\log\log n}$ [4, p.355], one can show that Bateman's result implies Erdős' result. Bateman's upper bound was improved upon by Bateman, C. Pomerance and Vaughan [1] in 1981, who showed that $A(n) \leq n^{2^{k-1}/k-1}$. They also showed that $A(n) \geq n^{2^{k-1}/k-1}/(5\log n)^{2^{k-1}}$ holds for infinitely many n with exactly k distinct odd prime factors.

Related to these problems are questions concerning the maximal height over all divisors of $x^n - 1$. It is well-known that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Thus, $x^n - 1$ has $\tau(n)$ distinct irreducible divisors, where $\tau(n)$ is the number of divisors of n. Therefore, $x^n - 1$ has $2^{\tau(n)}$ divisors in $\mathbb{Z}[x]$.

Let $B(n) = \max\{H(f) : f(x) \mid x^n - 1, f(x) \in \mathbb{Z}[x]\}$. In particular, $A(n) \le B(n)$ since $\Phi_n(x)$ divides $x^n - 1$ and $B(n)$ is the maximum height over all divisors of $x^n - 1$. In general, much less is known about $B(n)$ than $A(n)$. In 2005, Pomerance and N. Ryan [8] proved that as $n \to \infty$, $\log B(n) \le n^{(\log 3 + o(1))/\log\log n}$. They also showed that this inequality can be reversed for infinitely many n.

In [6], H. Maier found an upper bound for $A(n)$ that holds for most n.

Theorem 1.1 (Maier). *Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ as $n \to \infty$. Then $A(n) \le n^{\psi(n)}$ for almost all n, i.e., for all n except for a set with asymptotic density 0.*

Maier's upper bound has been shown to be best possible [5]. In this paper, we consider an upper bound for $B(n)$ that holds for most n.

Theorem 1.2. *Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ as $n \to \infty$. Then $B(n) \le n^{\tau(n)\psi(n)}$ for almost all n, i.e., for all n except for a set with asymptotic density 0.*

It is not yet known whether this upper bound for $B(n)$ is best possible.

2. Proof strategy for Theorem 1.2

Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$, then $B(n) = H\left(\prod_{d\in\mathcal{D}} \Phi_d(x)\right)$, where $\mathcal{D}$ is a subset of divisors of n for which $\prod_{d\in\mathcal{D}} \Phi_d(x)$ has maximal height over all products of distinct cyclotomic polynomials dividing $x^n - 1$.

In [8], Pomerance and Ryan show that if $f_1, ..., f_k \in \mathbb{Z}[x]$ with $\deg f_1 \le \cdots \le \deg f_k$ then $H(f_1 ... f_k) \le \prod_{i=1}^{k-1}(1+\deg f_i) \prod_{i=1}^{k} H(f_i)$. Thus, when $n > 1$,

$$B(n) = H\left(\prod_{d\in\mathcal{D}} \Phi_d(x)\right) \le \prod_{d\in\mathcal{D}} (1+\varphi(d)) \prod_{d\in\mathcal{D}} A(d) \le n^{\#\mathcal{D}} \prod_{d\in\mathcal{D}} A(d) \le n^{\tau(n)} \prod_{d|n} A(d). \tag{2.1}$$

Let $A_0(n) := \max_{d|n} A(d)$. Then from (2.1), $B(n) \le n^{\tau(n)} A_0(n)^{\tau(n)}$, since $A(d) \le A_0(n)$ for each $d \mid n$. So, if we show that $A_0(n) \le n^{\psi(n)}$ for almost all n, we will have

$$B(n) \le n^{\tau(n)} A_0(n)^{\tau(n)} \le n^{\tau(n)} \cdot n^{\tau(n)\psi(n)} = n^{\tau(n)(1+\psi(n))} \tag{2.2}$$

for almost all n. Since $\psi(n)$ is any function that goes to infinity as n approaches infinity, we will have proved the theorem.

Thus, we have reduced the proof of Theorem 1.2 to the following proposition, which shall be proven in section 4.

Proposition 2.1. *We have $A_0(n) \le n^{\psi(n)}$ for almost all n.*

3. Key Lemmas

Let $\omega(n)$ be defined as in section 1. Write the prime factorization of n as $p_1^{e_1} \cdots p_{\omega(n)}^{e_{\omega(n)}}$, where $p_1 > p_2 > \cdots > p_{\omega(n)}$, $e_k \ge 1$ for $1 \le k \le \omega(n)$. Thus, we have functions $p_k = p_k(n)$ defined when $k \le \omega(n)$. If $k > \omega(n)$, we let $p_k(n) = 1$.

To prove our proposition, we will show that for most integers, the size of the prime factors p_k decreases rapidly on a logarithmic scale as k increases.

Lemma 3.1. *Let $2 < \gamma < e$. The set $\{n : \omega(n) \ge \frac{\log\log n}{\log \gamma}\}$ has density 0.*

Proof. Since $2 < \gamma < e$ then $\log\gamma \in (0,1)$, so $1 < \frac{1}{\log\gamma}$. Now, the normal order of $\omega(n)$ is $\log\log n$ [7, p.111], so for each $\varepsilon > 0$, $\omega(n) < (1+\varepsilon)\log\log n$ must hold, except for a set of n with asymptotic density 0. In particular, since $\varepsilon = \frac{1}{\log\gamma} - 1 > 0$, then $\omega(n) < \frac{1}{\log\gamma}\log\log n$ for almost all n. □

Let $\mu(n)$ be the Möbius function. From [6, Lemma 5], we know that if $2 < \gamma < e$ then there is a constant $c(\gamma) > 0$ such that for each natural number $k <$log log x/log γ,

$$\#\{n \le x : \mu(n) \ne 0,\ \log p_k > \gamma^{-k}\log x\} \ll x e^{-c(\gamma)k}.$$

The following lemma says that we can remove the restriction that $\mu(n) \ne 0$, i.e., we do not need to assume that n is square-free.

Lemma 3.2. *Let $2 < \gamma < e$. Let $x > 1$. There are positive constants $c_0(\gamma), C_2$ such that for each natural number $k < \log\log x/\log\gamma$,*

$$\#\{n \le x : \log p_k > \gamma^{-k}\log x\} \le C_2 x e^{-c_0(\gamma)k}.$$

Proof. We adopt the same strategy as in [6]. The following is a classical result, due to Halberstam and Richert [3, Thm 01]: Let f be a non-negative multiplicative function such that for some numbers A and B and for all numbers $y \ge 0$, we have

$$\sum_{p \le y} f(p)\log p \le Ay, \qquad \sum_p \sum_{\nu \ge 2} \frac{f(p^\nu)}{p^\nu}\log p^\nu \le B, \tag{3.1}$$

where p runs over primes and ν runs over integers. Then, for all numbers $x > 1$,

$$\sum_{n \le x} f(n) \le (A+B+1)\frac{x}{\log x}\sum_{n \le x}\frac{f(n)}{n}. \tag{3.2}$$

We apply this theorem with $f(n) = b^{\omega([t,x],n)}$, where $w([t,x],n)$ is the number of distinct prime factors of n in the interval $[t,x]$, with $t = x^{\gamma^{-k}}$, $b > 1$ (b will be specified later). In order to apply the theorem, we need to check that both conditions in (3.1) are satisfied.

As usual, let $\theta(y) = \sum_{p\le y} \log p$. Since $\theta(y) \le 2y\log 2 < 2y$ [7, p.108] then

$$\sum_{p\le y} f(p)\log p \le 2by$$

for all y. Thus, the first condition is satisfied, with $A = 2b$.

Next, we show that the second condition is satisfied for a suitable number B, namely that the double sum converges. Consider the sum $\sum_p \sum_\nu \frac{\log p^\nu}{p^\nu} b^{\omega([t,y],p^\nu)}$, where p runs over primes, $\nu \ge 2$. Since ω counts only distinct prime factors, we have $\omega([t,y],p^\nu) \le 1$. So,

$$\sum_p \sum_{\nu\ge 2} \frac{\log p^\nu}{p^\nu} b^{\omega([t,y],p^\nu)} \le b\sum_p \left(\frac{2\log p}{p^2} + \frac{3\log p}{p^3} + \cdots\right) = b\sum_p \left(\frac{2}{p^2} + \frac{3}{p^3} + \cdots\right)\log p.$$

It is easy to see that

$$\sum_p \left(\frac{2}{p^2} + \frac{3}{p^3} + \cdots\right)\log p = 2\sum_p \frac{\log p}{p(p-1)} \tag{3.3}$$

holds, and that the sum in (3.3) is less than 4. Thus, the second condition is satisfied, with $B = 4b$.

Therefore, by (3.2), we have

$$\sum_{n\le x} b^{\omega([t,x],n)} \le (2b+4b+1)\frac{x}{\log x}\sum_{n\le x}\frac{f(n)}{n} \le 7b\frac{x}{\log x}\sum_{n\le x}\frac{f(n)}{n}. \tag{3.4}$$

Now, $\sum_{n\le x} \frac{f(n)}{n} \le \prod_{p\le x}\left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right)$, since f is a non-negative multiplicative function (certainly all prime factors of each $n \le x$ are in this product). Taking the log of both sides, we have

$$\begin{aligned}
\log\left(\sum_{n\le x}\frac{f(n)}{n}\right) &\le \log\prod_{p\le x}\left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right) \\
&= \log\prod_{p\le x}\left(1 + f(p)\left(\frac{1}{p} + \frac{1}{p^2} + \cdots\right)\right) \\
&= \log\prod_{p\le x}\left(1 + \frac{f(p)}{p-1}\right) = \sum_{p\le x}\log\left(1 + \frac{f(p)}{p-1}\right).
\end{aligned}$$

Thus,

$$\log\left(\sum_{n\le x}\frac{f(n)}{n}\right) \le \sum_{p\le x}\frac{f(p)}{p-1} = \sum_{p<t}\frac{1}{p-1} + \sum_{t\le p\le x}\frac{b}{p-1},$$

since $f(p) = 1$ when $p < t$ and $f(p) = b$ when $t \le p \le x$. By Mertens' first theorem [7, p.92],

$$\sum_{p<t} \frac{1}{p-1} + \sum_{t \le p \le x} \frac{b}{p-1} = \log\log x + (b-1)(\log\log x - \log\log t) + O(b).$$

Let α be the constant associated with $O(b)$. After undoing the logarithms, we are left with

$$\sum_{n \le x} \frac{f(n)}{n} \le C_1 \log x \left(\frac{\log x}{\log t}\right)^{b-1}, \tag{3.5}$$

where $C_1 = e^{\alpha b}$. Inserting (3.5) into (3.4), we have

$$\sum_{n \le x} b^{\omega([t,x],n)} \le 7bC_1 x \left(\frac{\log x}{\log t}\right)^{b-1}. \tag{3.6}$$

Let $C_2 = 7bC_1$. Let

$$N = \#\{n \le x : \omega([t,x],n) > \frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)\}.$$

Using (3.6), we have

$$N b^{\frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)} \le \sum_{n \le x} b^{\omega([t,x],n)} \le C_2 x \left(\frac{\log x}{\log t}\right)^{b-1}.$$

But

$$b^{\frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)} = e^{(1+\varepsilon)(b-1)(\log\log x - \log\log t)} = \left(\frac{\log x}{\log t}\right)^{(1+\varepsilon)(b-1)}.$$

So

$$N \le \frac{C_2 x (\frac{\log x}{\log t})^{b-1}}{(\frac{\log x}{\log t})^{(1+\varepsilon)(b-1)}} = C_2 x \left(\frac{\log x}{\log t}\right)^{-\varepsilon(b-1)}.$$

In other words,

$$\omega([t,x],n) \le \frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t) \tag{3.7}$$

for all $n \le x$ except for a set of cardinality at most $C_2 x (\frac{\log x}{\log t})^{-\varepsilon(b-1)}$.

Now, fix $\varepsilon > 0$, $b > 1$ such that $\frac{(1+\varepsilon)(b-1)}{\log b} \log\gamma \le 1$. Let $k < \log\log x / \log\gamma$. Recall that $t = x^{\gamma^{-k}}$. Then, if $\log p_k > \gamma^{-k} \log x$, we have

$$\omega([t,x],n) \ge k \ge \frac{(1+\varepsilon)(b-1)}{\log b} k \log\gamma. \tag{3.8}$$

Since $k \log\gamma = \log\log x - \log\log t$, we have $\omega([t,x],n) \ge \frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)$. But this contradicts (3.7) except for a set of cardinality at most $C_2 x (\frac{\log x}{\log t})^{-\varepsilon(b-1)}$. Thus, the set of $n \le x$ with $\log p_k > \gamma^{-k} \log x$ has a cardinality of at most $C_2 x (\frac{\log x}{\log t})^{-\varepsilon(b-1)}$. Since $t = x^{\gamma^{-k}}$, we have

$$\#\{n \le x : \log p_k > \gamma^{-k} \log x\} \le C_2 x e^{-k\varepsilon(b-1)\log(\gamma)}.$$

Taking $c_0(\gamma) = \varepsilon(b-1)\log(\gamma)$, we obtain the desired result. □

The following lemma says that, except for a sparse set of integers n, $\log p_k$ is small when k is sufficiently large.

Lemma 3.3. *Let $2 < \gamma < e$. Let $\varepsilon > 0$ be arbitrary and let $k_0 = \frac{\log(\varepsilon(1-e^{-c_0(\gamma)})/C_2)}{-c_0(\gamma)}$, where $c_0(\gamma)$ and C_2 are as in Lemma 3.2. Then, for x sufficiently large, the set $\{n \le x : \log p_k > \gamma^{-k} \log x$ for some $k \ge k_0\}$ has cardinality at most $2\varepsilon x$.*

Proof. Fix $\varepsilon > 0$. Let $\mathcal{S} = \{n \le x : \log p_k > \gamma^{-k} \log x$ for some $k \ge k_0\}$ and let $S_k = \{n \le x : \log p_k > \gamma^{-k} \log x\}$. By Lemma 3.2, we have

$$\# \mathcal{S} \le \sum_{k=\lceil k_0 \rceil}^{\lfloor \frac{\log\log x}{\log \gamma} \rfloor} \# \mathcal{S}_k + \#\{n : \omega(n) > \frac{\log\log x}{\log \gamma}\} \le \sum_{k=\lceil k_0 \rceil}^{\infty} C_2 x e^{-c_0(\gamma)k} + \varepsilon x$$

for sufficiently large x, since $\{n : \omega(n) > \frac{\log\log x}{\log\gamma}\}$ has density 0 by Lemma 3.1. But the sum on the right is a convergent geometric series, so

$$\# \mathcal{S} \le \frac{C_2 x e^{-c_0(\gamma)k_0}}{1 - e^{-c_0(\gamma)}} + \varepsilon x.$$

Thus, using the definition of k_0,

$$\#\{n \le x : \log p_k > \gamma^{-k} \log x \text{ for some } k \ge k_0\} \le 2\varepsilon x.$$

□

4. Proof of proposition 2.1

Proof. Maier shows in [2] that if $\psi(n)$ is any function defined on all positive integers n such that $\psi(n) \to \infty$ as $n \to \infty$ then $A(n) \le n^{\psi(n)}$ for almost all n. Key to this proof is the fact that

$$\log A(n) \le C \sum_{k=1}^{\omega(n)} 2^k \log p_k \tag{4.1}$$

for all square-free integers n, where $C > 0$ is a constant and $p_k = p_k(n)$ is as above.

We define the radical of n, denoted $\mathrm{rad}(n)$, to be the largest square-free divisor of n. Since $\Phi_n(x) = \Phi_{\mathrm{rad}(n)}(x^{n/\mathrm{rad}(n)})$, the coefficients of $\Phi_n(x)$ are the same as the coefficients of

$\Phi_{\mathrm{rad}(n)}(x)$. Thus, $A(n) = A(\mathrm{rad}(n))$. As a result, we can use (4.1) for any positive integer n, since

$$\log A(n) = \log A(\mathrm{rad}(n)) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k.$$

For each d dividing n, let $d = p_{1,d}^{e_{1,d}} p_{2,d}^{e_{2,d}} \cdots p_{\omega(d),d}^{e_{\omega(d),d}}$, where $p_{1,d} > p_{2,d} > \cdots > p_{\omega(d),d}$ and $e_{k,d} \geq 1$ for $1 \leq k \leq \omega(d)$. Also, let $p_{k,d} = 1$ for $k > \omega(d)$. Since $d \mid n$ then the primes dividing d also divide n. Thus, $p_{k,d} \leq p_k$ for all k, so

$$\sum_{k=1}^{\omega(d)} 2^k \log p_{k,d} \leq \sum_{k=1}^{\omega(d)} 2^k \log p_k \leq \sum_{k=1}^{\omega(n)} 2^k \log p_k.$$

Thus, $\log A(d) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k$ holds for all n and for all $d \mid n$. Since $\log A_0(n) = \log A(d)$ for some $d \mid n$ we then have $\log A_0(n) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k$.

Let $\varepsilon > 0$ be arbitrary and let k_0 be as in Lemma 3.3. Combining the above inequality with Lemma 3.3, we have

$$\log A_0(n) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k = C \sum_{k \leq \lfloor k_0 \rfloor} 2^k \log p_k + C \sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} 2^k \log p_k \tag{4.2}$$

$$\leq C \sum_{k \leq \lfloor k_0 \rfloor} 2^k \log p_k + C \sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} (2/\gamma)^k \log x \tag{4.3}$$

for all $n \leq x$ except for a set with cardinality $\leq 2\varepsilon x$. Since $2 < \gamma < e$ then $(2/\gamma) < 1$. Hence, $\sum_{k=\lfloor k_0 \rfloor}^{\omega(n)} (2/\gamma)^k$ is part of a convergent geometric series, so it is bounded above by some positive constant L that is independent of n.

Now, if $\sqrt{x} \leq n \leq x$ then $2 \log n > \log x$, so

$$\sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} (2/\gamma)^k \log x \leq 2 \log n \sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} (2/\gamma)^k = 2L \log n.$$

Then, if n is such that (4.3) holds,

$$\begin{aligned}\log A_0(n) &\le C \sum_{k\le\lfloor k_0\rfloor} 2^k \log p_k \ + 2L\log n \\ &\le 2^{\lfloor k_0\rfloor} C \sum_{k\le\lfloor k_0\rfloor} \log p_k \ + 2L\log n \\ &= 2^{\lfloor k_0\rfloor} C \log(\prod_{k\le\lfloor k_0\rfloor} p_k) + 2L\log n \\ &\le \log(n^{2^{\lfloor k_0\rfloor}C}) + \log(n^{2L}).\end{aligned}$$

Thus, $A_0(n) \le n^{2^{\lfloor k_0\rfloor}C} \cdot n^{2L}$. Then, we have

$$A_0(n) \le n^{2^{\frac{\log(\varepsilon(1-e^{-c_0(\gamma)})/C_2)}{-c_0(\gamma)}}} \cdot n^{2L} \le n^{e^{\frac{\log(\varepsilon(1-e^{-c_0(\gamma)})/C_2)}{-c_0(\gamma)}}} \cdot n^{2L} = n^{(\varepsilon(1-e^{-c_0(\gamma)})/C_2)^{\frac{-1}{c_0(\gamma)}}} \cdot n^{2L}.$$

As mentioned, this holds for all n with $\sqrt{x} \le n \le x$ and for which (4.3) holds. Therefore, for any $\varepsilon > 0$ there is a constant $C_3 = (\frac{\varepsilon(1-e^{-c_0(\gamma)})}{C_2})^{\frac{-1}{c_0(\gamma)}} + 2L$ such that for all sufficiently large x, every $n \le x$ satisfies $A_0(n) \le n^{C_3}$, except for at most $2\varepsilon x + \sqrt{x}$ of them. Since $\varepsilon > 0$ is arbitrary, this proves Proposition 2.1, which concludes the proof of our main theorem. $\square$

Acknowledgements. I would like to thank my adviser, Carl Pomerance, for the careful guidance and encouragement that he provided while I was writing this paper.

References

[1] 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. Janos Bolyai, vol. 34, North-Holland, Amsterdam, 1984, pp. 171-202.

[2] P. Erdős, *On the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **52** (1946), 179-184.

[3] R. R. Hall and G. Tenenbaum, *Divisors*. Cambridge University Press, Cambridge, 1988.

[4] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, 4th edition. Oxford University Press, London, 1962.

[5] H. Maier, *Cyclotomic polynomials with large coefficients*, Acta Arith. **64** (1993), 227-235.

[6] H. Maier, *The size of the coefficients of cyclotomic polynomials*, Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), 633-639, Progr. Math., 139, Birkhäuser Boston, Boston, MA, 1996.

[7] P. Pollack, *Not always buried deep: a second course in elementary number theory*. Amer. Math. Soc., Providence, 2009.

[8] C. Pomerance, N. Ryan, *Maximal height of divisors of* $x^n - 1$. Illinois J. Math. 51 (2007), no. 2, 597-604 (electronic).

Department of Mathematics, 6188 Kemeny Hall, Dartmouth College, Hanover, NH 03755, USA

E-mail address: `Lola.Thompson@Dartmouth.edu`