Heights of Divisors of $x^n - 1$

Lola Thompson

Dartmouth College

October 4, 2009

Introduction

Definition

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value.

Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial, i.e.

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

Introduction

Definition

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value.

Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial, i.e.

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

- $\Phi_1(x), \Phi_2(x), ..., \Phi_{100}(x)$ all have height 1, i.e. all of the coefficients are in the set $\{0, \pm 1\}$. Based on this observation, it may be tempting to conjecture that "all cyclotomic polynomials have height 1."

Introduction

Definition

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value.

Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial, i.e.

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

- $\Phi_1(x), \Phi_2(x), ..., \Phi_{100}(x)$ all have height 1, i.e. all of the coefficients are in the set $\{0, \pm 1\}$. Based on this observation, it may be tempting to conjecture that "all cyclotomic polynomials have height 1."
- However, the pattern breaks down at $\Phi_{105}(x)$, which has height 2.

Introduction

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

(3) What is the normal height of $\Phi_n(x)$? What is it on average?

Introduction

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

(3) What is the normal height of $\Phi_n(x)$? What is it on average?

- The answer to (1) is known. The height can get arbitrarily large.

Introduction

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

(3) What is the normal height of $\Phi_n(x)$? What is it on average?

- The answer to (1) is known. The height can get arbitrarily large.
- In this talk, we'll answer (2) and give a generalization of this result to a larger family of polynomials.

Introduction

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

(3) What is the normal height of $\Phi_n(x)$? What is it on average?

- The answer to (1) is known. The height can get arbitrarily large.
- In this talk, we'll answer (2) and give a generalization of this result to a larger family of polynomials.
- The answer to (3) is not known. However, the theorems that we will discuss in this talk go a long way towards answering this question.

Outline

Bounding the Height of $\Phi_n(x)$

Let $A(n)$ denote the height of $\Phi_n(x)$.

Finding "good" upper and lower bounds for $A(n)$ has been of interest for some time.

- In 1946, P. Erdös 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. Vaughan showed in 1975 that this inequality can be reversed for infinitely many n.

Bounding the Height of $\Phi_n(x)$

Let $A(n)$ denote the height of $\Phi_n(x)$.

Finding "good" upper and lower bounds for $A(n)$ has been of interest for some time.

- In 1946, P. Erdös 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. 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.

Bounding the Height of $\Phi_n(x)$

Let $A(n)$ denote the height of $\Phi_n(x)$.

Finding "good" upper and lower bounds for $A(n)$ has been of interest for some time.

- In 1946, P. Erdös 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. 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.
- This result was improved upon by P.T. Bateman, C. Pomerance and R.C. Vaughan 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.

Maier's Upper Bound for $A(n)$

H. Maier took a different approach to bounding $A(n)$. Rather than finding an upper bound for integers n with a fixed number of prime factors, he sought to find an upper bound that holds "for almost all n," i.e. except for a set with density 0.

Theorem (H. Maier)

Let $\psi(n)$ be any function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $A(n)$ denote the height of $\Phi_n(x)$. Then $A(n) \leq n^{\psi(n)}$ for almost all n.

Maier proved that this upper bound is "best possible" for $A(n)$. In other words, if we tried to make the upper bound any smaller, there would be a positive proportion of integers n with $A(n)$ outside of the bound.

Maier's Lower Bound for $A(n)$

Maier used the same techniques to give a lower bound for $A(n)$:

Theorem (H. Maier)

Let $\varepsilon(n)$ be any function defined for all positive integers such that $\varepsilon(n) \to 0$ for $n \to \infty$. Let $A(n)$ denote the height of $\Phi_n(x)$. Then $A(n) \geq n^{\varepsilon(n)}$ for almost all n.

Bounding the Height of Any Divisor of $x^n - 1$

Let $B(n)$ denote the maximal height over all polynomial divisors of $x^n - 1$.

Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$ then we can think of $B(n)$ as the maximal height over all products of $\Phi_d(x)$ where $d \mid n$. Thus, $B(n)$ is, in some sense, a generalization of $A(n)$.

Much less is known about $B(n)$ than $A(n)$.

In 2005, C. Pomerance and N. Ryan proved that as $n \to \infty$, $\log B(n) \leq n^{(\log 3 + o(1))/\log\log n}$. They also showed that this inequality can be reversed for infinitely many n.

A Generalization of Maier's Upper Bound

The following gives a generalization of Maier's upper bound:

Theorem (T.)

Let $\psi(n)$ be any function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $\tau(n)$ denote the number of positive divisors of n. Then $B(n) \leq n^{\tau(n)\psi(n)}$ for almost all n.

Challenges In Generalizing Maier's Result

There are two ways in which the generalized version of Maier's result is more complicated than the original:

Challenges In Generalizing Maier's Result

There are two ways in which the generalized version of Maier's result is more complicated than the original:

- (1) In Maier's paper, we are given the polynomial whose height we were trying to bound.

  In the new scenario, we have to look over all possible products of $\Phi_d(x)$ where $d \mid n$ without knowing which one has maximal height.

Challenges In Generalizing Maier's Result

There are two ways in which the generalized version of Maier's result is more complicated than the original:

- (1) In Maier's paper, we are given the polynomial whose height we were trying to bound.

  In the new scenario, we have to look over all possible products of $\Phi_d(x)$ where $d \mid n$ without knowing which one has maximal height.

- (2) In Maier's paper, it suffices to assume that n is a product of distinct prime factors, since primes occurring to exponents greater than 1 in the factorization of n do not affect the height of $\Phi_n(x)$ (for example, $A(6) = A(12) = A(48)$).

  However, the same cannot be said for $B(n)$ (for example, $B(6) = 2, B(12) = 3, B(48) = 6$). So, in bounding $B(n)$, we also have to consider the case where the prime factors of n are not distinct.

Proof Sketch

Theorem (T.)

Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $\tau(n)$ denote the number of positive divisors of n. Then $B(n) \le n^{\tau(n)\psi(n)}$ for almost all n.

- To prove the generalization, we use a result (due to Pomerance and Ryan) that, for any n, $B(n) \le n^{\tau(n)} \prod_{d|n} A(d)$.

Proof Sketch

Theorem (T.)

Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $\tau(n)$ denote the number of positive divisors of n. Then $B(n) \le n^{\tau(n)\psi(n)}$ for almost all n.

- To prove the generalization, we use a result (due to Pomerance and Ryan) that, for any n, $B(n) \le n^{\tau(n)} \prod_{d|n} A(d)$.
- Let $A_0(n) = \max_{d|n} A(d)$. Then, from the inequality above, $B(n) \le n^{\tau(n)} A_0(n)^{\tau(n)}$.

Proof Sketch

Theorem (T.)

Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $\tau(n)$ denote the number of positive divisors of n. Then $B(n) \leq n^{\tau(n)\psi(n)}$ for almost all n.

- To prove the generalization, we use a result (due to Pomerance and Ryan) that, for any n, $B(n) \leq n^{\tau(n)} \prod_{d|n} A(d)$.
- Let $A_0(n) = \max_{d|n} A(d)$. Then, from the inequality above, $B(n) \leq n^{\tau(n)} A_0(n)^{\tau(n)}$.
- The result will follow if we can show that $A_0(n) \leq n^{\psi(n)}$ for almost all n.

Key Lemma

Lemma (T.)

Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $A_0(n) = \max_{d|n} A(d)$. Then $A_0(n) \leq n^{\psi(n)}$ for almost all n.

The proof proceeds in a manner similar to Maier's proof, with the following modifications:

- (1) Maier shows that $\log A(n) \ll \sum_{k=1}^{\omega(n)} 2^k \log p_k$ for all square-free integers n, where p_k is the k^{th} largest prime factor of n. We had to prove that $\log A_0(n) \ll \sum_{k=1}^{\omega(n)} 2^k \log p_k$ holds for *all* n, redefining p_k to be the k^{th} largest *distinct* prime factor of n.

Key Lemma

Lemma (T.)

Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Let $A_0(n) = \max_{d|n} A(d)$. Then $A_0(n) \leq n^{\psi(n)}$ for almost all n.

The proof proceeds in a manner similar to Maier's proof, with the following modifications:

- (2) Maier shows that if $2 < \eta < e$ then there is a constant $c(\eta) > 0$ such that for all natural numbers $k < \log\log x / \log \eta$, the set $\{n \leq x : \mu(n) \neq 0, \log p_k > \eta^{-k} \log x, k \geq k_0\}$ has asymptotic density 0 if k_0 is sufficiently large.

  We are able to remove the restriction that $\mu(n) \neq 0$ (ie. that n is square-free).

Further Directions

As mentioned earlier, much less is known about $B(n)$ than $A(n)$. Here are some possible areas for further research:

- H. Maier was able to show that his upper bound for $A(n)$ is "best possible." I am currently trying to determine whether the same holds for the upper bound for $B(n)$.

Further Directions

As mentioned earlier, much less is known about $B(n)$ than $A(n)$. Here are some possible areas for further research:

- H. Maier was able to show that his upper bound for $A(n)$ is "best possible." I am currently trying to determine whether the same holds for the upper bound for $B(n)$.

- H. Maier gave a lower bound of $n^{\varepsilon(n)}$ for $A(n)$ that holds for almost all integers n. It's certainly true that $n^{\varepsilon(n)} \leq A(n) \leq B(n)$, but can we find a better lower bound? Is it the case that $n^{\tau(n)\varepsilon(n)} \leq B(n)$ for almost all n?

Further Directions

As mentioned earlier, much less is known about $B(n)$ than $A(n)$. Here are some possible areas for further research:

- H. Maier was able to show that his upper bound for $A(n)$ is "best possible." I am currently trying to determine whether the same holds for the upper bound for $B(n)$.
- H. Maier gave a lower bound of $n^{\varepsilon(n)}$ for $A(n)$ that holds for almost all integers n. It's certainly true that $n^{\varepsilon(n)} \leq A(n) \leq B(n)$, but can we find a better lower bound? Is it the case that $n^{\tau(n)\varepsilon(n)} \leq B(n)$ for almost all n?
- Define $B_k(n)$ to be the maximal height over all products of at most k cyclotomic polynomials dividing $x^n - 1$. Can we find a lower bound for $B_k(n)$?

Further Directions

As mentioned earlier, much less is known about $B(n)$ than $A(n)$. Here are some possible areas for further research:

- H. Maier was able to show that his upper bound for $A(n)$ is "best possible." I am currently trying to determine whether the same holds for the upper bound for $B(n)$.

- H. Maier gave a lower bound of $n^{\varepsilon(n)}$ for $A(n)$ that holds for almost all integers n. It's certainly true that $n^{\varepsilon(n)} \leq A(n) \leq B(n)$, but can we find a better lower bound? Is it the case that $n^{\tau(n)\varepsilon(n)} \leq B(n)$ for almost all n?

- Define $B_k(n)$ to be the maximal height over all products of at most k cyclotomic polynomials dividing $x^n - 1$. Can we find a lower bound for $B_k(n)$?

- What is the normal order of $B(n)$? What is $B(n)$ on average?

References

[1] J. Suzuki, *On Coefficients of Cyclotomic Polynomials*.

[2] Y. Gallot, P. Moree and H. Hommerson, *Value Distribution of Cyclotomic Polynomial Coefficients*.

[3] P. Erdös, *On the Coefficients of the Cyclotomic Polynomial*.

[4] P.T. Bateman, *Note on the Coefficients of the Cyclotomic Polynomial*.

[5] P.T. Bateman, C. Pomerance, and R.C. Vaughan, *On the Size of the Coefficients of the Cyclotomic Polynomial*.

[6] H. Maier, *The Size of Coefficients of Cyclotomic Polynomials*.

[7] C. Pomerance, N. Ryan, *Maximal Height of Divisors of* $x^n - 1$.