involve

a journal of mathematics

Some conjectures on the maximal height of divisors of $x^n - 1$

Nathan C. Ryan, Bryan C. Ward and Ryan Ward

msp

2010 vol. 3, no. 4

INVOLVE 3:4 (2010)
https://doi.org/10.2140/involve.2010.3.451

Some conjectures on the maximal height of divisors of $x^n - 1$

Nathan C. Ryan, Bryan C. Ward and Ryan Ward

(Communicated by Kenneth S. Berenhaut)

Define $B(n)$ to be the largest height of a polynomial in $\mathbb{Z}[x]$ dividing $x^n - 1$. We formulate a number of conjectures related to the value of $B(n)$ when n is of a prescribed form. Additionally, we prove a lower bound for $B(n)$.

1. Introduction

The height $H(f)$ of a polynomial f is the largest coefficient of f in absolute value. Let

$$\Phi_n(x) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - e^{2\pi i a/n})$$

be the n-th cyclotomic polynomial. For example, for a prime p, we have

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1}.$$

Define the function $A(n) := H(\Phi_n(x))$. This function was originally studied by Erdős and has been much investigated since then. The second of the following two facts reduces the study of $A(n)$ to square-free n:

$$\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)} \text{ if } p \nmid n \quad \text{and} \quad \Phi_{np}(x) = \Phi_n(x^p) \text{ if } p \mid n. \tag{1-1}$$

The variant we study in the present paper was first defined in [Pomerance and Ryan 2007] and studied further in [Kaplan 2009]. In [Pomerance and Ryan 2007] the function

$$B(n) = \max\{H(f) : f \mid x^n - 1 \text{ and } f \in \mathbb{Z}[x]\}$$

is defined and a fairly good asymptotic bound is found. In the same paper there are two explicit formulas for n of a certain form: it is shown that $B(p^k) = 1$ and $B(pq) = \min\{p, q\}$. In the present paper, for n of a prescribed form, we are interested in finding explicit formulas for $B(n)$, discovering bounds for $B(n)$,

MSC2000: 11C08, 11Y70, 12Y05.
Keywords: cyclotomic polynomials, heights.

determining which divisors of $x^n - 1$ have height $B(n)$ and understanding the image of $B(n)$. One might consider the present paper a continuation of [Kaplan 2009], where it was shown that $B(p^2q) = \min\{p^2, q\}$ and where upper bounds were found for $B(n)$. Kaplan also found a better upper bound as well as a lower bound for $B(pqr)$, where $p < q < r$ are primes.

Our main theoretical result is a lower bound for $B(p^a q^b)$, but most of the content of the paper consists of conjectures about $B(n)$ of the kind described above. The conjectures are verified by extensive data computed in Sage (www.sagemath.org) and tabulated in [Ryan et al. 2010].

The paper is organized as follows. In Section 2 we describe our computations: the method and the scale. Section 3 provides a reasonably good lower bound for $B(n)$ in terms of its prime factorization. The first of the subsequent two sections, Section 4, is about $B(n)$ for n that are divisible by two distinct primes. Section 5 investigates what happens when 3 or more primes divide n. We conclude the paper with three further variants on the arithmetic function $B(n)$. For the first of these three variants, related data have also been tabulated in [Ryan et al. 2010].

2. Computations

Much of what is included in the present paper is the result of a great deal of machine computation. The function $B(n)$ is very difficult to compute. The best way we know to compute $B(n)$ is to do the following: observe that any f that would give a maximal height is a product of cyclotomic polynomials since

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{2-1}$$

So, to compute $B(n)$ we need to compute the set of divisors of n and its power set. We then iterate over the power set, multiplying the corresponding cyclotomic polynomials in each set. The largest height among the polynomials in this very long list is the value of $B(n)$.

We have computed $B(n)$ for almost 300,000 values of n, the largest being 56,796,482. This includes all n with four or fewer prime factors, and in particular every n less than 1000.

These computations were done in Sage, and took 30 processors several months on various systems at Bucknell University: many were run on a cluster node with dual quad core 3.33 GHz Xeons with 64GB of RAM. For example, $B(720)$ took 113 hours to compute and $B(840)$ took 550 hours.

The resulting data can be accessed freely at [Ryan et al. 2010]. We store all data we consider useful for formulating conjectures about $B(n)$. This includes n, $B(n)$, and the set of sets of cyclotomic polynomials which multiply to yield the maximal height.

form of n	conjecture	ranges	# data points
p^2q^2	4.1	$2 \le p < q < 60$	463
$2q^b$	4.2	$2 < q < 300$, $b = 2$	96
		$2 < q < 100$, $b = 3$	24
		$2 < q < 75$, $b = 4$	20
		$2 < q < 10$, $b = 5$	4
		$2 < q < 10$, $b = 6$	4
		$q \in \{3, 5\}$, $b = 7$	2
		$q \in \{3, 5\}$, $b = 8$	2
pq^b	4.2, 4.4	$2 < p < q < 85$, $b = 3$	301
		$2 < p < q < 35$, $b = 4$	92
		$2 < p < q < 15$, $b = 5$	14
		$2 < p < q < 10$, $b = 6$	13
pqr	5.1	$2 \le p < q < r < 150$	55530
$pqrs$	5.1	$2 \le p < q < r < s < 15$	1045
pqr^b	5.2	$2 \le q < r < 50$, $b = 2$	1490
		$2 \le q < r < 35$, $b = 3$	171
		$2 \le q < r < 35$, $b = 4$	13

Table 1. Summary of data motivating the conjectures in this paper. The data can be accessed at [Ryan et al. 2010].

We note that far less comprehensive computations have been done in [Abbott 2009], and a smaller set of data can be found at [Garcia 2006].

We present in the next section the conjectures we have formulated based on these computational data; the values of n so studied are summarized in Table 1.

3. Lower bound

We start by stating a lower bound for the function $B(n)$. (We thank Pieter Moree and the anonymous referee for independently pointing out this improvement to our earlier result.)

Theorem 3.1. *Suppose $n = uv$, with u and v coprime positive integers. Then $B(n) \ge \min\{u, v\}$.*

Proof. Since u and v are coprime, we note that $x^u - 1$ and $x^v - 1$ have $x - 1$ as greatest common divisor. Consider the divisor

$$(x^u - 1)(x^v - 1)/(x - 1)^2 \quad \text{of } x^{uv} - 1.$$

Let $w = \min\{u, v\}$ and observe that the coefficient of x^{w-1} is w. □

This result can be rephrased as follows:

Corollary 3.2. *We have* $B(p_1^{e_1} \cdots p_s^{e_s}) \geq \min\{p_1^{e_1}, \ldots, p_s^{e_s}\}$.

We observe that this bound is surprisingly good for the data we have computed, at least when n is divisible by two primes. Of the 5396 n in the database of the form $p^a q^b$, $B(n) = \min\{p^a, q^b\}$ a majority of the time (we exclude $(a, b) \in \{(1, 1), (1, 2), (2, 1)\}$ in this total as in those cases it is a theorem that $B(n) = \min\{p^a, q^b\}$).

4. When n is divisible by two primes

Evaluation of the function $A(p^a q^b)$ is straightforward. To see that $A(p^a q^b) = 1$, one can write down an explicit formula for $\Phi_{pq}(x)$ (see, e.g., [Lam and Leung 1996]) and then use (1-1). The situation for $B(p^a q^b)$ is not all like the situation for $A(p^a q^b)$.

By means of a thorough case-by-case analysis, one can find an explicit formula for $B(pq^2)$ [Kaplan 2009, Theorem 6] where p and q are distinct primes. The proof proceeds by computing the height of every possible divisor of $x^{pq^2} - 1$ and identifying which of those is largest. In that spirit we make the note of the following:

Conjecture 4.1. Let $p < q$ be primes. Then $B(p^2 q^2)$ is the larger of

$$H(\Phi_p(x)\Phi_q(x)\Phi_{p^2 q}(x)\Phi_{pq^2}(x)) \quad \text{and} \quad H(\Phi_p(x)\Phi_q(x)\Phi_{p^2}(x)\Phi_{q^2}(x)).$$

For example,

$$B(3^2 \cdot 5^2) = H(\Phi_3\Phi_5\Phi_{3^2 \cdot 5}\Phi_{3 \cdot 5^2}) \neq H(\Phi_3\Phi_5\Phi_{3^2}\Phi_{5^2}),$$
$$B(5^2 \cdot 11^2) = H(\Phi_5\Phi_{11}\Phi_{5^2}\Phi_{11^2}) \neq H(\Phi_5\Phi_{11}\Phi_{5^2 \cdot 11}\Phi_{5 \cdot 11^2}).$$

In addition to not having a proof for this conjecture, we also lack an explicit formula for the height of the polynomial. The conjecture has been checked for the primes indicated in Table 1.

An even more difficult problem is to deduce a formula for n of a more arbitrary form. For example, our computations suggest the following conjecture.

Conjecture 4.2. Let $p < q$ be odd primes.

(i) For any positive integer b, $B(2q^b) = 2$.

(ii) Suppose $b > 2$. Then $B(pq^b) > p$.

The difficulty here is that a case by case analysis as described above is not feasible.

We have computed data verifying the first part of the conjecture as indicated in Table 1. The cases $b = 1$ and $b = 2$ in the first part are theorems in [Pomerance and Ryan 2007] and [Kaplan 2009], respectively. We have verified the second half of the conjecture as indicated in Table 1.

The previous conjectures deals with what values of $B(pq^b)$ you get when you have two fixed primes and let one of the exponents vary. A related question is what happens when you have one fixed prime and two fixed exponents.

Theorem 4.3. *Fix a prime p and positive integers a and b. Then $B(p^a q^b)$ takes on only finitely many values as q ranges through the set of primes.*

Proof. This is a rephrasing of a special case of [Kaplan 2009, Theorem 4]. □

As a result of investigating this theorem computationally, we make the following observation:

Conjecture 4.4. For a fixed odd prime p and fixed positive integer b, the finite list of values $B(pq^b)$ as $q > p$ varies are all divisible by p.

We have checked this for the same range as which we have checked the second half of Conjecture 4.2. We observe that $B(7^2 83^2) = 64$, showing that the hypothesis on the factorization of n as pq^b is necessary.

5. When n is divisible by more than two primes

For products of three distinct primes, as noted in [Kaplan 2009, p. 2687], one of the products

$$\Phi_p(x)\Phi_q(x)\Phi_r(x)\Phi_{pqr}(x) \quad \text{or} \quad \Phi_1(x)\Phi_{pq}(x)\Phi_{pr}(x)\Phi_{qr}(x)$$

appears to give the largest height. Most of the time the first product gives the largest height. According to out data, of the 27492 n of the form pqr we have computed, the vast majority of the time the first product does give the maximal height while the second product only gives the maximal height only around half of the time (often they both give the maximal height). In general, one can make the following conjecture.

Conjecture 5.1. Let $n = p_1 \cdots p_t$ be square free. Then $B(n)$ is given by either

$$\prod_{\substack{d \mid n \\ \omega(d)\ \text{even}}} \Phi_d(x) \quad \text{or} \quad \prod_{\substack{d \mid n \\ \omega(d)\ \text{even}}} \Phi_d(x),$$

where $\omega(d)$ is the number of primes dividing d.

The conjecture is true when $t = 1$ and $t = 2$ [Pomerance and Ryan 2007, Lemma 2.1]. Our data supporting the conjecture for other n is listed in Table 1; in addition, the conjecture has been checked for $n = 2310$, the smallest product of five distinct primes.

For odd n, the analogue to Conjecture 4.4 would be: $B(pqr^b)$ is divisible by p. This statement is false for squarefree n, since $B(3 \cdot 31 \cdot 1009) = 599$, which is not divisible by 3. On the other hand, we can make the following conjecture.

Conjecture 5.2. Let $n = pqr^b$ where $p < q < r$, and $b > 1$. Then $B(n)$ is divisible by p. Moreover, $B(n) > p$.

Once more, our evidence for this is in Table 1. This conjecture is analogous to Conjectures 4.2 and 4.4.

6. Conclusions and future work

Above we have explicitly described several conjectures about the function $B(n)$. Implicitly, we have also suggested that proving explicit formulas for $B(n)$, especially by case-by-case analysis, is extremely difficult. In fact, even conjecturing formulas is difficult. A new method for proving formulas will be required before more progress can be made.

In addition to the obvious task of proving any of the conjectures included here and developing a new approach to proving these formulas, we propose the following related problems:

(1) Define the length of a polynomial $f = \sum_{n=0}^{d} a_n x^n$ to be $L(f) = \sum_{n=0}^{d} |a_n|$ and let
$$C(n) := \max\{L(f) : f \mid x^n - 1,\ f \in \mathbf{Z}[x]\}.$$

(2) Let $\mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field and define the function
$$D(n) := \max\{H(f) : f \in \mathbb{Q}(\zeta_n)[x],\ f \mid x^n - 1 \text{ and } f \text{ monic}\}.$$

Can any explicit formulas or bounds be found for these functions? The database at [Ryan et al. 2010] has data related to the first of these two problems.

In [Decker and Moree 2010], a number of problems related to $B(n)$ have been described. The authors investigate, among other things, the set of coefficients of divisors of $x^n - 1$ and show that in some cases the coefficients of each divisor are a list of consecutive integers (sometimes excluding zero). In the future, we may return to the questions posed by Decker and Moree and investigate them computationally. This problem was suggested to us by Pieter Moree and the anonymous referee.

References

[Abbott 2009] J. Abbott, "Bounds on factors in $\mathbb{Z}[x]$", preprint, 2009. arXiv 0904.3057

[Decker and Moree 2010] A. Decker and P. Moree, "Coefficient convexity of divisors of $x^n - 1$", preprint, 2010. arXiv 1010.3938

[Garcia 2006] F. Garcia, entry A114536 in *The on-line encyclopedia of integer sequences*, edited by N. J. A. Sloane, 2006.

[Kaplan 2009] N. Kaplan, "Bounds for the maximal height of divisors of $x^n - 1$", *J. Number Theory* **129**:11 (2009), 2673–2688. MR 2010h:11161 Zbl 05603993

[Lam and Leung 1996] T. Y. Lam and K. H. Leung, "On the cyclotomic polynomial $\Phi_{pq}(X)$", *Amer. Math. Monthly* **103**:7 (1996), 562–564. MR 97h:11150 Zbl 0868.11016

[Pomerance and Ryan 2007] C. Pomerance and N. C. Ryan, "Maximal height of divisors of $x^n - 1$", *Illinois J. Math.* **51**:2 (2007), 597–604. MR 2008j:12012 Zbl 05197699

[Ryan et al. 2010] N. C. Ryan, B. C. Ward, and R. E. Ward, Database on cyclotomic polynomials, 2010, available at http://www.eg.bucknell.edu/~theburg/projects/data/wards/cyclo.py/index.

Received: 2010-09-29 Revised: 2010-11-23 Accepted: 2010-12-01

nathan.ryan@bucknell.edu *Department of Mathematics, Bucknell University, Lewisburg, PA 17837, United States*

bryan.ward@bucknell.edu *Department of Mathematics, Bucknell University, Lewisburg, PA 17837, United States*

ryan.ward@bucknell.edu *Department of Mathematics, Bucknell University, Lewisburg, PA 17837, United States*

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2010 is US $100/year for the electronic version, and $120/year (+$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2010 vol. 3 no. 4