

# SOME CONJECTURES ON THE MAXIMAL HEIGHT OF DIVISORS OF $x^n - 1$

NATHAN C. RYAN, BRYAN C. WARD, AND RYAN WARD

ABSTRACT. 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  $B(p^a q^b)$  where  $p, q$  are distinct primes.

## 1. INTRODUCTION

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

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

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 studied since then. The following fact reduces the study of  $A(n)$  to square-free  $n$ :

$$(1.1) \quad \Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)} \text{ if } p \nmid n \text{ and } \Phi_{np}(x) = \Phi_n(x^p) \text{ if } p \mid n.$$

The variant we study in the present paper was first defined in [5] and studied further in [3]. In [5] 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. Also in [5] 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  $B(n)$ , 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 [3]. In [3], it is shown that

---

*Date:* February 24, 2009 and, in revised form, September 30, 2010.

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

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

$B(p^2q) = \min\{p^2, q\}$ . Additionally, the author found upper bounds for  $B(n)$ . Moreover, he found a better upper bound as well as a lower bound for  $B(pqr)$ , where  $p < q < r$  are three distinct primes.

Our main theoretical result is a lower bound for  $B(p^a q^b)$  but most of the content of the paper is various conjectures about  $B(n)$  of the kind described above. The conjectures are verified by extensive data computed in Sage [7] and tabulated in [6].

The paper is organized in follows. In the next section we describe our computations: the method and the scale. The first of the subsequent two sections is about  $B(n)$  for  $n$  that are divisible by two distinct primes. We give a reasonably good lower bound for such  $B(n)$  and a few conjectures about  $B(pq^b)$ . The third section investigates what happens when 3 or more primes divide  $n$ . We conclude the paper with two further variants on the arithmetic function  $B(n)$ . For the first of these two variants, related data have also been tabulated in [6].

## 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

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

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 distributed the computation over more than 30 processors and it took several months. The code was implemented in Sage [7]. As a result of our computations we were able to formulate the conjectures below.

A few words about the database that contains the results of our computations are in order. The data in this database can be accessed via [6]. We store all of the data we see to be useful to formulate conjectures about  $B(n)$ . This includes  $n$ ,  $B(n)$ , and the set of sets of cyclotomic polynomials which multiply to yield the maximal height.

We have computed  $B(n)$  for almost 300000 distinct  $n$ . These computations have taken 30 processors several months to compute (for example  $B(720)$  took 113 hours to compute and  $B(840)$  took 550 hours to compute) on various systems at Bucknell University: for example,

$n$	Ranges	Data Points	Relevant Conjectures
$p^2q^2$	$2 \leq p < q < 60$	463	Conjecture 3.3
$2q^b$	$2 < q < 300, b = 2$	96	Conjecture 3.4
$2q^b$	$2 < q < 100, b = 3$	24	
$2q^b$	$2 < q < 75, b = 4$	20	
$2q^b$	$2 < q < 10, b = 5$	4	
$2q^b$	$2 < q < 10, b = 6$	4	
$2q^b$	$q \in \{3, 5\}, b = 7$	2	
$2q^b$	$q \in \{3, 5\}, b = 8$	2	
$pq^b$	$2 < p < q < 85, b = 3$	301	Conjecture 3.4
$pq^b$	$2 < p < q < 35, b = 4$	92	Conjecture 3.6
$pq^b$	$2 < p < q < 15, b = 5$	14	
$pq^b$	$2 < p < q < 10, b = 6$	13	

TABLE 1. Data available at [6] and used in verifying the conjectures in Section 3

$n$	Ranges	Data Points	Relevant Conjecture
$pqr$	$2 \leq p < q < r < 150$	55530	Conjecture 4.1
$pqrs$	$2 \leq p < q < r < s < 15$	1045	
$pqr^b$	$2 \leq q < r < 50, b = 2$	1490	Conjecture 4.2
$pqr^b$	$2 \leq q < r < 35, b = 3$	171	
$pqr^b$	$2 \leq q < r < 35, b = 4$	13	

TABLE 2. Data available at [6] and used in verifying the conjectures in Section 4.

many were run on a cluster node with dual quad core 3.33ghz xeon with 64GB of ram. We have computed  $B(n)$  for  $n$  with 4 or fewer prime factors, and for  $n$  as large as 56796482. In particular, we have computed  $B(n)$  for every  $n$  less than 1000. We present in the next section the conjectures we have formulated based on these computational data and freely offer access to these data at [6]. We note that far less comprehensive computations have been done in [1] and a smaller set of data can be found at [2]. We summarize the data in the database that we use to verify our conjectures in Tables 1 and 2.

### 3. WHEN $n$ IS DIVISIBLE BY TWO PRIMES

Evaluation of the function  $A(p^aq^b)$  is rather straightforward. To see that  $A(p^aq^b) = 1$ , one can write down an explicit formula for  $\Phi_{pq}(x)$  (see, e.g., [4]) and then use (1.1). The situation for  $B(p^aq^b)$  is not all like the situation for  $A(p^aq^b)$ .

The best general result we have is:

**Theorem 3.1.**  $B(p^a q^b) \geq \min\{p^a, q^b\}$

Before proving the theorem, we prove the following:

**Lemma 3.2.** *For any integer  $n$  and prime  $p$ :*

$$\prod_{k=1}^n \Phi_{p^k}(x) = \sum_{c=0}^{p^n-1} x^c$$

*Proof.* The lemma follows from induction on  $n$  and an application of (1.1) to  $\Phi_{p^{n+1}}(x)$ .  $\square$

*Proof of Theorem 3.1.* Consider the following polynomial, a divisor of  $x^{p^a q^b} - 1$ :

$$(3.1) \quad \left( \prod_{i=1}^a \Phi_{p^i}(x) \right) \left( \prod_{j=1}^b \Phi_{q^j}(x) \right) = \left( \sum_{c=0}^{p^a-1} x^c \right) \left( \sum_{k=0}^{q^b-1} x^k \right),$$

where the equality follows from the lemma.

Assume that  $p^a < q^b$ . The coefficient of  $x^{p^a-1}$  in (3.1) can be seen to be

$$\sum_{k=0}^{p^a-1} (1)(1)$$

since each polynomial in the product has all its coefficients equal to 1. Thus:

$$B(p^a q^b) \geq H \left( \left( \prod_{i=1}^a \Phi_{p^i}(x) \right) \left( \prod_{j=1}^b \Phi_{q^j}(x) \right) \right) \geq p^a.$$

A similiar argument can show, that if  $q^b < p^a$ , then:

$$B(p^a q^b) \geq H \left( \left( \prod_{i=1}^a \Phi_{p^i}(x) \right) \left( \prod_{j=1}^b \Phi_{q^j}(x) \right) \right) \geq q^b.$$

Hence:

$$B(p^a q^b) \geq \min\{p^a, q^b\}$$

$\square$

We observe that this bound is surprisingly good for the data we have computed. Of the 5396  $n$  in the database of the form  $p^a q^b$  (for  $(a, b) \notin \{(1, 1), (1, 2), (2, 1)\}$ ),  $B(n) = \min\{p^a, q^b\}$  a majority of the time.

By means of a thorough case-by-case analysis, one can find an explicit formula for  $B(pq^2)$  [3, 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 3.3.** *Let  $p < q$  be primes. Then  $B(p^2q^2)$  is the larger of  $H(\Phi_p(x)\Phi_q(x)\Phi_{p^2q}(x)\Phi_{pq^2}(x))$  and  $H(\Phi_p(x)\Phi_q(x)\Phi_{p^2}(x)\Phi_{q^2}(x))$ .*

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

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 3.4.** *Let  $p < q$  be odd primes.*

- (1) *For any positive integer  $b$ ,  $B(2q^b) = 2$ .*
- (2) *Suppose  $b > 2$ . Then  $B(pq^b) > p$ .*

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

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 [5] and [3], 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 3.5.** *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 [3, Theorem 4]. □

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

**Conjecture 3.6.** *For a fixed odd prime  $p$  and fixed positive integer  $b$ , the finite list of values  $B(pq^b)$  as  $p < q$  varies are all divisible by  $p$ .*

We have checked this for the same range as which we have checked the second half of Corollary 3.4. We observe that  $B(7^2 83^2) = 64$ , showing that the hypothesis on the factorization of  $n$  as  $pq^b$  is necessary.

#### 4. WHEN $n$ IS DIVISIBLE BY MORE THAN TWO PRIMES

As noted in [3, p. 2687], one of the products  $\Phi_p(x)\Phi_q(x)\Phi_r(x)\Phi_{pqr}(x)$  or  $\Phi_1(x)\Phi_{pq}(x)\Phi_{pr}(x)\Phi_{qr}(x)$  appears to give the largest height. The majority of the time the first product gives the largest height. According to our 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 4.1.** *Let  $n = p_1 \cdots p_t$  be square free. Then  $B(n)$  is given by either*

$$\prod_{d|n, \omega(d) \equiv 1 \pmod{2}} \Phi_d(x) \text{ or } \prod_{d|n, \omega(d) \equiv 0 \pmod{2}} \Phi_d(x)$$

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

The conjecture is true when  $t = 1$  and  $t = 2$  [5, Lemma 2.1]. Our data supports the conjecture for  $n$  as listed in Table 2.

For  $n$  that are odd, the analogue to Conjecture 3.6 would be:  $B(pqr^b)$  is divisible by  $p$ . This statement is false for squarefree  $n$ :  $B(3 \cdot 31 \cdot 1009) = 599$  which is not divisible by 3. On the other hand, we can make the following conjecture:

**Conjecture 4.2.** *Let  $n = pqr^b$  where  $p < q < r$ , and  $b > 1$ . Then  $B(n)$  is divisible by  $p$ . Moreover,  $B(n) > p$ .*

We have evidence for this conjecture as indicated in Table 2. This conjecture is very much analogous to Conjecture 3.4 and Conjecture 3.6.

#### 5. 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 [6] has data related to the first of these two problems.

#### REFERENCES

1. John Abbott, *Bounds on factors in  $\mathbb{Z}[x]$* , 2009, <http://arxiv.org/abs/0904.3057>.
2. Felipe García, *The On-Line Encyclopedia of Integer Sequences*, A114536, 2006.
3. Nathan Kaplan, *Bounds for the maximal height of divisors of  $x^n - 1$* , J. Number Theory **129** (2009), no. 11, 2673–2688. MR MR2549523 (2010h:11161)
4. T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial  $\Phi_{pq}(X)$* , Amer. Math. Monthly **103** (1996), no. 7, 562–564. MR MR1404079 (97h:11150)
5. Carl Pomerance and Nathan C. Ryan, *Maximal height of divisors of  $x^n - 1$* , Illinois J. Math. **51** (2007), no. 2, 597–604 (electronic).
6. Nathan C. Ryan, Bryan C. Ward, and Ryan E. Ward, *Cyclotomic database search*, 2010, <http://www.eg.bucknell.edu/~theburg/projects/data/wards/cyclo.py/index>.
7. W. A. Stein et al., *Sage Mathematics Software (Version 3.3)*, The Sage Group, 2009, <http://www.sagemath.org>.

MATHEMATICS DEPARTMENT, BUCKNELL UNIVERSITY, LEWISBURG, PA 17837  
*E-mail address:* nathan.ryan@bucknell.edu

*E-mail address:* bryan.ward@bucknell.edu

*E-mail address:* ryan.ward@bucknell.edu