Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Maximum gap in (inverse) cyclotomic polynomial

Hoon Hong [a], Eunjeong Lee [b,*], Hyang-Sook Lee [c], Cheol-Min Park [d]

[a] *Dept. of Mathematics, North Carolina State University, Raleigh, NC 27695-8205, USA*
[b] *Institute of Mathematical Sciences, Ewha Womans University, Seoul, 120-750, South Korea*
[c] *Dept. of Mathematics, Ewha Womans University, Seoul, 120-750, South Korea*
[d] *National Institute for Mathematical Sciences, Daejeon, 305-811, South Korea*

A R T I C L E   I N F O

A B S T R A C T

Let $g(f)$ denote the maximum of the differences (gaps) between two consecutive exponents occurring in a polynomial f. Let Φ_n denote the n-th cyclotomic polynomial and let Ψ_n denote the n-th inverse cyclotomic polynomial. In this note, we study $g(\Phi_n)$ and $g(\Psi_n)$ where n is a product of odd primes, say $p_1 < p_2 < p_3$, etc. It is trivial to determine $g(\Phi_{p_1})$, $g(\Psi_{p_1})$ and $g(\Psi_{p_1 p_2})$. Hence the simplest non-trivial cases are $g(\Phi_{p_1 p_2})$ and $g(\Psi_{p_1 p_2 p_3})$. We provide an exact expression for $g(\Phi_{p_1 p_2})$. We also provide an exact expression for $g(\Psi_{p_1 p_2 p_3})$ under a mild condition. The condition is almost always satisfied (only finite exceptions for each p_1). We also provide a lower bound and an upper bound for $g(\Psi_{p_1 p_2 p_3})$.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

The n-th cyclotomic polynomial Φ_n and the n-th inverse cyclotomic polynomial Ψ_n are defined by

$$\Phi_n(x) = \prod_{\substack{1 \leqslant j \leqslant n \\ (j,n)=1}} \left(x - \zeta_n^j\right), \qquad \Psi_n(x) = \prod_{\substack{1 \leqslant j \leqslant n \\ (j,n)>1}} \left(x - \zeta_n^j\right),$$

where ζ_n is a primitive n-th root of unity. For example, we have

$$\Phi_3(x) = 1 + x + x^2,$$

---

* Corresponding author.
E-mail addresses: hong@ncsu.edu (H. Hong), ejlee127@ewha.ac.kr (E. Lee), hsl@ewha.ac.kr (H.-S. Lee), mpcm@nims.re.kr (C.-M. Park).

$$\Phi_{3.5}(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8,$$

$$\Psi_3(x) = -1 + x,$$

$$\Psi_{3.5}(x) = -1 - x - x^2 + x^5 + x^6 + x^7,$$

$$\Psi_{3.5.7}(x) = -1 + x - x^3 + x^4 - x^5 - x^{10} + x^{11} - x^{12} - x^{17} + x^{18} - x^{19} + x^{21} - x^{22} + x^{35}$$
$$- x^{36} + x^{38} - x^{39} + x^{40} + x^{45} - x^{46} + x^{47} + x^{52} - x^{53} + x^{54} - x^{56} + x^{57}.$$

There have been extensive studies on the coefficients of cyclotomic polynomials [1,2,4,6,8,11,14]. Recently there have been also studies on the coefficients of inverse cyclotomic polynomials [3,13]. In this note, we study the exponents of (inverse) cyclotomic polynomials. In particular, we are interested in the *maximum gap*, $g(f)$, which is the maximum of the differences (gaps) between two consecutive exponents occurring in f where $f = \Phi_n$ or $f = \Psi_n$. More precisely the maximum gap is defined as follows:

Definition 1 (*Maximum gap*). Let $f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$ where $c_1, \ldots, c_t \neq 0$ and $e_1 < \cdots < e_t$. Then the maximum gap of f, written as $g(f)$, is defined by

$$g(f) = \max_{1 \leqslant i < t} (e_{i+1} - e_i), \qquad g(f) = 0 \quad \text{when } t = 1.$$

For example, $g(\Phi_{3.5}) = 2$ because 2 is the maximum among $1 - 0, 3 - 1, 4 - 3, 5 - 4, 7 - 5, 8 - 7$.

It can be visualized by the following diagrams where a long bar represents a polynomial. The black color indicates that the corresponding exponent (term) occurs in the polynomial and the white color indicates that it does not.

One immediately notices that the maximum gap is essentially the length of a longest white block *plus* 1. For example, a longest white block in $\Phi_{3.5}$ has length 1. Hence $g(\Phi_{3.5}) = 1 + 1 = 2$.

Our initial motivation came from its need for analyzing the complexity [7] of a certain paring computation over elliptic curves [5,10,15,16]. It turns out that the computing time of the Ate$_i$ pairing [10,15,16] over elliptic curves essentially depends on the maximum gaps of the inverse cyclotomic polynomials whose degree are decided from the parameters of the elliptic curves. However, it seems to be a curious problem on its own and it could be also viewed as a first step toward the detailed understanding of the sparsity structure of Φ_n and Ψ_n.

In this note, we tackle the simplest non-trivial cases, namely, $g(\Phi_{p_1 p_2})$ and $g(\Psi_{p_1 p_2 p_3})$ where $p_1 < p_2 < p_3$ are odd primes. As far as we are aware, there were no published results on this problem. We will provide an exact expression for $g(\Phi_{p_1 p_2})$ in Theorem 1. We will also provide an exact expression for $g(\Psi_{p_1 p_2 p_3})$ under a mild condition in Theorem 2. In Remark 1 we will show that the condition is very mild. Finally we will provide a lower bound and an upper bound for $g(\Psi_{p_1 p_2 p_3})$ in Theorem 3.

In order to obtain the results, we had to overcome a few difficulties. It can be easily shown that $\Phi_{p_1 p_2}$ and $\Psi_{p_1 p_2 p_3}$ are sums and products of simple polynomials with trivial gap structures. However adding and multiplying them could introduce new gaps, eliminate existing gaps or change the sizes of existing gaps etc., in intricate manners, via accumulation or cancellation of terms, making the analysis

very challenging. We overcame the obstacles in two ways: (1) find mild conditions on p_1, p_2, p_3 that ensure that accumulation or cancellation do not occur; (2) find mild conditions that allow us to bound the sizes of gaps arising from accumulation or cancellation and show that such gaps cannot be the maximum gap.

This note is structured as follows. In the following section (Section 2), we will quickly take care of trivial cases, in order to identify the simplest non-trivial cases to tackle. A reader can safely skip over this section. In the subsequent section (Section 3), we will provide the main results on the simplest non-trivial cases. In the final section, we will prove the main results (Section 4).

2. Trivial cases

In this section, we will quickly take care of trivial cases, in order to identify the simplest non-trivial cases that will be tackled in the next section. A reader can safely skip this section. In the following we will use basic properties of (inverse) cyclotomic polynomials without explicit references. The basic properties of cyclotomic polynomials can be found in any standard textbooks. The basic properties of inverse cyclotomic polynomials can be found in Lemma 2 of [13].

- Since

$$\Phi_n(x) = \Phi_{\hat{n}}\big(x^{\frac{n}{\hat{n}}}\big), \qquad \Psi_n(x) = \Psi_{\hat{n}}\big(x^{\frac{n}{\hat{n}}}\big),$$

  we immediately have

$$g(\Phi_n) = \frac{n}{\hat{n}} g(\Phi_{\hat{n}}), \qquad g(\Psi_n) = \frac{n}{\hat{n}} g(\Psi_{\hat{n}}),$$

  where $\hat{n}$ is the radical of n. Thus we will, without losing generality, restrict n to be squarefree.
- Since

$$\Phi_{2n}(x) = \pm\Phi_n(-x), \qquad \Psi_{2n}(x) = \pm\big(1 - x^n\big)\Psi_n(-x)$$

  for odd n, we immediately have

$$g(\Phi_{2n}) = g(\Phi_n), \qquad g(\Psi_{2n}) = \max\big\{g(\Psi_n), \deg(\Phi_n)\big\}.$$

  Thus we will, without losing generality, further restrict n to be squarefree and odd, that is, a product of zero or more distinct odd primes.
- Consider the case when n is a product of *zero* odd primes, that is $n = 1$. Since

$$\Phi_1(x) = -1 + x, \qquad \Psi_1(x) = 1,$$

  we have

$$g(\Phi_1) = 1, \qquad g(\Psi_1) = 0.$$

- Consider the case when n is a product of *one* odd primes, that is $n = p_1$. Since

$$\Phi_{p_1}(x) = 1 + x + \cdots + x^{p_1 - 1}, \qquad \Psi_{p_1}(x) = -1 + x,$$

  we have

$$g(\Phi_{p_1}) = 1, \qquad g(\Psi_{p_1}) = 1.$$

- Consider the case when n is a product of *two* odd primes, that is $n = p_1 p_2$ where $p_1 < p_2$. Since

$$\Psi_{p_1 p_2}(x) = -\left(1 + x + \cdots + x^{p_1 - 1}\right) + \left(x^{p_2} + x^{p_2 + 1} + \cdots + x^{p_2 + p_1 - 1}\right),$$

we have

$$g(\Psi_{p_1 p_2}) = p_2 - (p_1 - 1).$$

Hence the simplest non-trivial cases are $g(\Phi_{p_1 p_2})$ and $g(\Psi_{p_1 p_2 p_3})$. We will tackle these cases in the following section.

3. Main results

In this section, we tackle the simplest non-trivial cases identified in the previous section. In particular, we provide an exact expression for $g(\Phi_{p_1 p_2})$ in Theorem 1. We also provide an exact expression for $g(\Psi_{p_1 p_2 p_3})$ under a mild condition in Theorem 2. In Remark 1 we show that the condition is very mild. Finally we provide a lower bound and an upper bound for $g(\Psi_{p_1 p_2 p_3})$ in Theorem 3.

Theorem 1. *Let $n = p_1 p_2$ where $p_1 < p_2$ are odd primes. Then we have*

$$g(\Phi_n) = p_1 - 1.$$

Theorem 2. *Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes satisfying the condition:*

$$p_2 \geqslant 4(p_1 - 1) \quad or \quad p_3 \geqslant p_1^2. \tag{1}$$

Then we have

$$g(\Psi_n) = 2n \frac{1}{p_1} - \deg(\Psi_n).$$

Theorem 3. *Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes. Then we have*

$$\max\left\{ p_1 - 1, 2n \frac{1}{p_1} - \deg(\Psi_n) \right\} \leqslant g(\Psi_n) < 2n \left(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} \right) - \deg(\Psi_n).$$

Remark 1. We make several remarks.

- Note that the condition (1) in Theorem 2 is "almost always" satisfied. Thus we "almost always" have

$$g(\Psi_n) = 2n \frac{1}{p_1} - \deg(\Psi_n).$$

More precisely, for each p_1, only finitely many out of infinitely many (p_2, p_3) violate the condition (1).
- Let V_{p_1} be the finite set of (p_2, p_3) violating the condition (1). For several small p_1 values and for every $(p_2, p_3) \in V_{p_1}$, we carried out direct calculation of $g(\Psi_n)$, obtaining the following frequency table

p_1	$\#V_{p_1}$	$\#V_{p_1}^{(1)}$	$\#V_{p_1}^{(2)}$	$\#V_{p_1}^{(3)}$
3	1	1	0	0
5	12	12	0	0
7	40	39	0	1
11	147	137	9	1
13	252	244	6	2
17	528	504	23	1
19	690	671	18	1
23	1155	1126	27	2

where

$$V_{p_1}^{(1)} = \left\{ (p_2, p_3) \in V_{p_1} \colon g(\Psi_n) = 2n\frac{1}{p_1} - \deg(\Psi_n) \right\},$$

$$V_{p_1}^{(2)} = \left\{ (p_2, p_3) \in V_{p_1} \colon g(\Psi_n) = p_1 - 1 \right\},$$

$$V_{p_1}^{(3)} = V_{p_1} - \left(V_{p_1}^{(1)} \cup V_{p_1}^{(2)} \right).$$

• The table suggests that even among the finite set V_{p_1}, we have almost always

$$g(\Psi_n) = 2n\frac{1}{p_1} - \deg(\Psi_n)$$

and sometimes

$$g(\Psi_n) = p_1 - 1$$

and very rarely

$$g(\Psi_n) > \max\left\{ p_1 - 1, 2n\frac{1}{p_1} - \deg(\Psi_n) \right\}.$$

• In fact, when $p_1 = 3$ or 5, the table shows that

$$g(\Psi_n) = 2n\frac{1}{p_1} - \deg(\Psi_n).$$

• It is important to recall that for each p_1, for instance $p_1 = 23$, there are infinitely many possible values for (p_2, p_3). The table shows that for those *infinitely many* possible values of (p_2, p_3), the maximum gap is exactly the lower bound in Theorem 3, namely,

$$g(\Psi_n) = \max\left\{ p_1 - 1, 2n\frac{1}{p_1} - \deg(\Psi_n) \right\}$$

except for only two values of (p_2, p_3). In other words, it seems that the lower bound in Theorem 3 is almost always exactly the maximum gap. The more detailed computational results (not given in the table) also suggest that the maximum gap is very close to the lower bound when it is not the same as the lower bound. Hence there is a hope for improving the upper bound. We leave it as an open problem. Any progress will require full understanding on the intricate cancellations occurring while adding and multiplying polynomials.

4. Proof

In this section, we prove the three theorems given in the previous section. We begin by listing several short-hand notations that will be used throughout the proofs without explicit references.

Notation 1 *(Notations used in the proof).*

$$\varphi(n) = \deg(\Phi_n),$$

$$\mathrm{tdeg}(f) = \text{the trailing degree of a univariate polynomial } f.$$

4.1. Proof of Theorem 1

Theorem 1 follows immediately from Lemma 3 and Lemma 4.

Lemma 1. *Let A and B be polynomials. If there is no cancellation of terms while adding the two polynomials, then*

$$g(A + B) \leqslant \max\big\{g(A), g(B), \mathrm{tdeg}(B) - \deg(A), \mathrm{tdeg}(A) - \deg(B)\big\}.$$

Proof. We consider several cases.

Case 1. $\mathrm{tdeg}(B) > \deg(A)$. The gaps of $A + B$ occurs in A, B and between A and B. Thus

$$g(A + B) = \max\big\{g(A), g(B), \mathrm{tdeg}(B) - \deg(A)\big\}.$$

Since $\mathrm{tdeg}(A) - \deg(B) < 0$, we have

$$g(A + B) = \max\big\{g(A), g(B), \mathrm{tdeg}(B) - \deg(A), \mathrm{tdeg}(A) - \deg(B)\big\}.$$

Case 2. $\mathrm{tdeg}(A) > \deg(B)$. By switching the role of A and B in Case 1, we have

$$g(A + B) = \max\big\{g(A), g(B), \mathrm{tdeg}(B) - \deg(A), \mathrm{tdeg}(A) - \deg(B)\big\}.$$

Case 3. $\deg(A) \geqslant \mathrm{tdeg}(B)$ and $\deg(B) \geqslant \mathrm{tdeg}(A)$. Since there is no cancellation of terms, we have

$$g(A + B) \leqslant \max\big\{g(A), g(B)\big\}.$$

Since $\mathrm{tdeg}(B) - \deg(A) \leqslant 0$ and $\mathrm{tdeg}(A) - \deg(B) \leqslant 0$, we have

$$g(A + B) \leqslant \max\big\{g(A), g(B), \mathrm{tdeg}(B) - \deg(A), \mathrm{tdeg}(A) - \deg(B)\big\}. \qquad \square$$

Lemma 2. *Let A and B be polynomials. If all the non-zero coefficients of A have the same sign and all the non-zero coefficients of B have the same sign, then we have*

$$g(AB) \leqslant \min\{u, v\},$$

where

$$u = \max\{g(B), g(A) + \text{tdeg}(B) - \deg(B)\},$$
$$v = \max\{g(A), g(B) + \text{tdeg}(A) - \deg(A)\}.$$

Proof. Let $A = \sum_{i=1}^{t} a_i x^{e_i}$ where $a_i > 0$ and $e_1 < e_2 < \cdots < e_t$. Let

$$C_j = \sum_{i=1}^{j} a_i x^{e_i} B.$$

Note $AB = C_t$.

We claim that $g(C_j) \leqslant \max\{g(B), g(A) + \text{tdeg}(B) - \deg(B)\}$ for $j = 1, \ldots, t$. We will prove the claim by induction on j. First, the claim is true for $j = 1$ since

$$g(C_1) = g(a_1 x^{e_1} B) = g(B) \leqslant \max\{g(B), g(A) + \text{tdeg}(B) - \deg(B)\}.$$

Next assume that the claim is true for j. We will show that the claim is true for $j + 1$. For this, note that

$$g(C_{j+1}) = g(C_j + a_{j+1} x^{e_{j+1}} B).$$

Since all the non-zero coefficients of A have the same sign and all the non-zero coefficients of B have the same sign, there is no cancellation of terms in the above summation of C_j and $a_{j+1} x^{e_{j+1}} B$. Thus, from Lemma 1, we have

$$g(C_{j+1}) \leqslant \max\{g(C_j), g(a_{j+1} x^{e_{j+1}} B), \text{tdeg}(a_{j+1} x^{e_{j+1}} B) - \deg(C_j), \text{tdeg}(C_j) - \deg(a_{j+1} x^{e_{j+1}} B)\}.$$

Note

$$g(C_j) \leqslant \max\{g(B), g(A) + \text{tdeg}(B) - \deg(B)\},$$
$$g(a_{j+1} x^{e_{j+1}} B) = g(B),$$
$$\deg(C_j) = e_j + \deg(B),$$
$$\text{tdeg}(C_j) = \text{tdeg}(A) + \text{tdeg}(B),$$
$$\deg(a_{j+1} x^{e_{j+1}} B) = e_{j+1} + \deg(B),$$
$$\text{tdeg}(a_{j+1} x^{e_{j+1}} B) = e_{j+1} + \text{tdeg}(B).$$

Note

$$\text{tdeg}(a_{j+1} x^{e_{j+1}} B) - \deg(C_j) = (e_{j+1} + \text{tdeg}(B)) - (e_j + \deg(B))$$
$$\leqslant g(A) + \text{tdeg}(B) - \deg(B),$$
$$\text{tdeg}(C_j) - \deg(a_{j+1} x^{e_{j+1}} B) = (\text{tdeg}(A) + \text{tdeg}(B)) - (e_{j+1} + \deg(B))$$
$$\leqslant 0.$$

Thus

$$g(C_{j+1}) \leqslant \max\{\max\{g(B), g(A) + \text{tdeg}(B) - \text{deg}(B)\}, g(B), g(A) + \text{tdeg}(B) - \text{deg}(B)\}$$
$$= \max\{g(B), g(A) + \text{tdeg}(B) - \text{deg}(B)\}.$$

Hence, we have proved the claim for $C_1, \ldots, C_t$. Since $AB = C_t$, we have

$$g(AB) \leqslant u = \max\{g(B), g(A) + \text{tdeg}(B) - \text{deg}(B)\}.$$

By switching the role of A and B, we can also prove, in the identical way, that

$$g(AB) \leqslant v = \max\{g(A), g(B) + \text{tdeg}(A) - \text{deg}(A)\}.$$

Hence we have $g(AB) \leqslant \min\{u, v\}$. $\square$

Lemma 3. *Let $p_1 < p_2$ be odd primes. Then we have*

$$g(\Phi_{p_1 p_2}) \leqslant p_1 - 1.$$

Proof. From [9,13,12,14], $\Phi_{p_1 p_2}$ has the form

$$\Phi_{p_1 p_2}(x) = \sum_{i=0}^{\rho} x^{ip_1} \cdot \sum_{j=0}^{\sigma} x^{jp_2} - x \cdot \sum_{i=0}^{p_2-2-\rho} x^{ip_1} \cdot \sum_{j=0}^{p_1-2-\sigma} x^{jp_2},$$

where ρ and σ are the unique integers such that $p_1 p_2 + 1 = (\rho+1)p_1 + (\sigma+1)p_2$ with $0 \leqslant \rho \leqslant p_2 - 2$ and $0 \leqslant \sigma \leqslant p_1 - 2$. It is also known that accumulation/cancellation of terms does not occur when we expand the above expression for $\Phi_{p_1 p_2}(x)$. It will be more convenient to rewrite the above expression into the following equivalent form

$$\Phi_{p_1 p_2}(x) = A \cdot B + C \cdot D,$$

where

$$A = \sum_{i=0}^{\rho} x^{ip_1}, \qquad B = \sum_{j=0}^{\sigma} x^{jp_2},$$

$$C = \sum_{i=0}^{p_2-2-\rho} x^{ip_1}, \qquad D = -x \sum_{j=0}^{p_1-2-\sigma} x^{jp_2}.$$

Note that

$$
\begin{array}{lll}
\text{tdeg}(A) = 0, & \text{deg}(A) = \rho p_1, & g(A) = p_1, \\
\text{tdeg}(B) = 0, & \text{deg}(B) = \sigma p_2, & g(B) = p_2, \\
\text{tdeg}(C) = 0, & \text{deg}(C) = (p_2 - 2 - \rho)p_1, & g(C) = p_1, \\
\text{tdeg}(D) = 1, & \text{deg}(D) = (p_1 - 2 - \sigma)p_2 + 1, & g(D) = p_2.
\end{array}
$$

Thus

$$g(B) + \text{tdeg}(A) - \deg(A) = p_2 - \rho p_1$$
$$= p_2 - p_1 p_2 - 1 + p_1 + (\sigma + 1)p_2$$
$$\leqslant p_2 - p_1 p_2 - 1 + p_1 + (p_1 - 1)p_2$$
$$= p_1 - 1,$$
$$g(A) + \text{tdeg}(B) - \deg(B) = p_1 - \sigma p_2$$
$$\leqslant p_1,$$
$$g(D) + \text{tdeg}(C) - \deg(C) = p_2 - (p_2 - 2 - \rho)p_1$$
$$= p_2 - p_2 p_1 + 2p_1 + \rho p_1$$
$$= p_2 - p_2 p_1 + 2p_1 + p_1 p_2 + 1 - p_1 - (\sigma + 1)p_2$$
$$= p_1 + 1 - \sigma p_2$$
$$\leqslant p_1 + 1,$$
$$g(C) + \text{tdeg}(D) - \deg(D) = p_1 + 1 - ((p_1 - 2 - \sigma)p_2 + 1)$$
$$= p_1 - (p_1 - 2 - \sigma)p_2$$
$$\leqslant p_1.$$

By Lemma 2, we have

$$g(AB) \leqslant \min\{\max\{p_2, p_1\}, \max\{p_1, p_1 - 1\}\} = \min\{p_2, p_1\} = p_1, \qquad (2)$$
$$g(CD) \leqslant \min\{\max\{p_2, p_1\}, \max\{p_1, p_1 + 1\}\} = \min\{p_2, p_1 + 1\} = p_1 + 1. \qquad (3)$$

Here we could apply Lemma 1 to bound $g(AB + CD)$. However, it would not be helpful since we would get a bound which is at least $p_1 + 1$. We want a tighter bound, namely $p_1 - 1$. For this, we exploit the *particular* way AB and CD are overlapping. We begin by noting

$$\text{tdeg}(AB) = 0, \quad \deg(AB) = \rho p_1 + \sigma p_2 = \varphi(p_1 p_2),$$
$$\text{tdeg}(CD) = 1, \quad \deg(CD) = (p_2 - 2 - \rho)p_1 + (p_1 - 2 - \sigma)p_2 + 1.$$

Hence

$$\text{tdeg}(CD) - \text{tdeg}(AB) = 1,$$
$$\deg(AB) - \deg(CD) = 2(\rho p_1 + \sigma p_2 - p_1 p_2 + p_1 + p_2) - 1$$
$$= 2(1 - p_1 - p_2 + p_1 + p_2) - 1 = 1.$$

So we have the following overlapping between AB and CD and the resulting $AB + CD$:
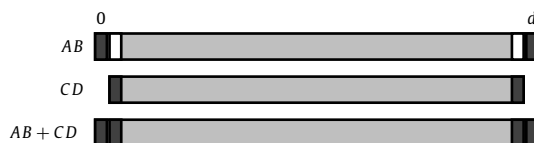
where each exponent is colored in black, white and gray to indicate that the exponent occurs, does not occur, and may or may not occur, respectively. The letter d is the shorthand for the degree of the polynomial AB. Note that the exponents 1 and $d-1$ in AB are colored in white because AB and CD do not share any exponents. As the result, the exponents $0, 1, d-1, d$ occur in $AB + CD$, and are colored in black.

Due to the way the polynomials AB and CD are overlapped, while adding CD to AB, none of the terms of CD can ever increase the gaps already in AB. Hence

$$g(AB + CD) \leqslant g(AB).$$

Thus using inequality (2) we deduce that

$$g(\Phi_{p_1 p_2}) = g(AB + CD) \leqslant p_1.$$

Hence in order to prove the first claim: $g(\Phi_{p_1 p_2}) \leqslant p_1 - 1$, it only remains to show that $g(\Phi_{p_1 p_2}) \neq p_1$. We will do so by contradiction. Suppose that $g(\Phi_{p_1 p_2}) = p_1$. Then there must occur two exponents, say α and β, in the polynomial $AB + CD$ such that $\beta - \alpha = p_1$ and all the exponents in between them do not occur in $AB + CD$. Note that $\alpha \geqslant 1$ and $\beta \leqslant d - 1$. Then we are in the situation described by the colorings in the following diagram:
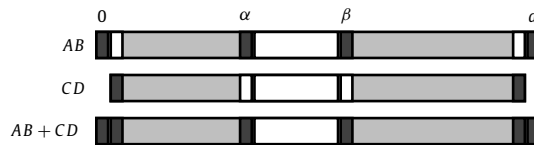
In the above diagram, the exponents α and β in the polynomial $AB + CD$ are colored in black because they occur in $AB + CD$ and all the exponents in between them are colored in white because they do not occur in $AB + CD$. Since there is no cancellation of terms while summing AB and CD, all the exponents in between α and β in AB and CD cannot occur either, hence colored in white also. Now from Formula (2), we have $g(AB) \leqslant p_1$. Since $\beta - \alpha = p_1$, the exponents α and β must occur in AB, hence colored in black. Since AB and CD do not share any exponents, the exponents α and β must *not* occur in CD, hence colored in white. Thus we have justified all the colorings in the above diagram.

Now we are ready to derive a contradiction. From the diagram, we see that

$$g(CD) \geqslant (\beta + 1) - (\alpha - 1) = \beta - \alpha + 2 = p_1 + 2,$$

but by inequality (3), we have

$$g(CD) \leqslant p_1 + 1.$$

This is a contradiction. Hence $g(\Phi_{p_1 p_2}) \neq p_1$. Thus we finally have

$$g(\Phi_{p_1 p_2}) \leqslant p_1 - 1. \qquad \square$$

Lemma 4. *Let $p_1 < p_2$ be odd primes. Then we have*

$$g(\Phi_{p_1 p_2}) \geqslant p_1 - 1.$$

Proof. We will show this by finding a gap of size $p_1 - 1$. We begin by recalling

$$AB = \sum_{i=0}^{\rho} x^{ip_1} \cdot \sum_{j=0}^{\sigma} x^{jp_2},$$

$$CD = -x \cdot \sum_{i=0}^{p_2-2-\rho} x^{ip_1} \cdot \sum_{j=0}^{p_1-2-\sigma} x^{jp_2},$$

where ρ and σ are the unique integers such that

$$p_1 p_2 + 1 = (\rho + 1)p_1 + (\sigma + 1)p_2$$

with $0 \leqslant \rho \leqslant p_2 - 2$ and $0 \leqslant \sigma \leqslant p_1 - 2$.

We claim that $\rho \geqslant 1$. Suppose otherwise. Then $\rho = 0$ and thus we have

$$p_1 p_2 + 1 = p_1 + (\sigma + 1)p_2.$$

Taking both sides modulo p_2, we see $1 \equiv p_1 \pmod{p_2}$. Since $1 < p_1 < p_2$, this is a contradiction. Hence $\rho \geqslant 1$.

Thus the polynomial AB must have the following form:

$$AB = 1 + x^{p_1} + \text{terms of degree higher than } p_1 \text{ if there is any.}$$

On the other hand, the polynomial CD must have the following form:

$$CD = -x - \text{terms of degree higher than } p_1 \text{ if there is any.}$$

Thus the polynomial $AB + CD$ must have the following form:

$$\Phi_{p_1 p_2}(x) = AB + CD = 1 - x + x^{p_1} + \text{terms of degree higher than } p_1. \qquad (4)$$

Thus there is a gap of size $p_1 - 1$ between x and x^{p_1}. Hence we finally have

$$g(\Phi_{p_1 p_2}) \geqslant p_1 - 1. \qquad \square$$

4.2. Proof of Theorem 2

Theorem 2 follows immediately from Lemma 5, Lemma 6 and Lemma 7.

Lemma 5. *Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes satisfying*

$$\text{D1:} \quad 2n\frac{1}{p_1} > \frac{4}{3}\deg(\Psi_n).$$

Then we have

$$g(\Psi_n) = 2n\frac{1}{p_1} - \deg(\Psi_n).$$

Proof. By Lemma 2 in [13] we have

$$\Psi_{p_1 p_2 p_3}(x) = \Phi_{p_1 p_2}(x) \cdot \Psi_{p_1 p_2}\left(x^{p_3}\right)$$

$$= \Phi_{p_1 p_2}(x) \cdot \Phi_{p_1}\left(x^{p_3}\right) \cdot \Psi_{p_1}\left(x^{p_2 p_3}\right)$$

$$= \Phi_{p_1 p_2}(x) \cdot \Phi_{p_1}\left(x^{p_3}\right) \cdot \left(-1 + x^{p_2 p_3}\right).$$

We expand the above expression and name the parts as follows

$$-\underbrace{\Phi_{p_1 p_2}(x) \cdot \Phi_{p_1}\left(x^{p_3}\right)}_{A_0} + \underbrace{x^{p_2 p_3} \Phi_{p_1 p_2}(x) \cdot \Phi_{p_1}\left(x^{p_3}\right)}_{A_1}.$$
$$\underbrace{\hspace{6cm}}_{\Psi_{p_1 p_2 p_3}(x)}$$

Let λ be the gap, if exists, between A_0 and A_1, that is, $\lambda = \text{tdeg}(A_1) - \deg(A_0)$. Note

$$\deg(A_0) = \deg(\Psi_n) - p_2 p_3 = \deg(\Psi_n) - n\frac{1}{p_1},$$

$$\text{tdeg}(A_1) = p_2 p_3 = n\frac{1}{p_1}.$$

Thus

$$\lambda = n\frac{1}{p_1} - \left(\deg(\Psi_n) - n\frac{1}{p_1}\right) = 2n\frac{1}{p_1} - \deg(\Psi_n).$$

Note that

$$\lambda = 2n\frac{1}{p_1} - \deg(\Psi_n)$$

$$= 3n\frac{1}{p_1} - 2\deg(\Psi_n) + \deg(A_0)$$

$$= \frac{3}{2}\left(2n\frac{1}{p_1} - \frac{4}{3}\deg(\Psi_n)\right) + \deg(A_0)$$

$$> \deg(A_0)$$

$$\geqslant g(A_0) = g(A_1).$$

Thus $\lambda > 0$ and the gap between A_0 and A_1 exists. Hence

$$g(\Psi_n) = \max\{g(A_0), \lambda, g(A_1)\} = \lambda = 2n\frac{1}{p_1} - \deg(\Psi_n). \qquad \square$$

Lemma 6. *Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes satisfying:*

$$\text{D2:} \quad 2p_3 > p_2(p_1 - 1).$$

Then we have

$$g(\Psi_n) = 2n\frac{1}{p_1} - \deg(\Psi_n).$$

Proof. By Lemma 2 in [13] we have

$$\begin{aligned}
\Psi_{p_1 p_2 p_3}(x) &= \Phi_{p_1 p_2}(x) \cdot \Psi_{p_1 p_2}(x^{p_3}) \\
&= \Phi_{p_1 p_2}(x) \cdot \Phi_{p_1}(x^{p_3}) \cdot \Psi_{p_1}(x^{p_2 p_3}) \\
&= \Phi_{p_1 p_2}(x) \cdot (1 + x^{p_3} + \cdots + x^{(p_1-1)p_3}) \cdot (-1 + x^{p_2 p_3}).
\end{aligned}$$

We expand the above expression and name the parts as follows

$$-\underbrace{\left(\underbrace{\Phi_{p_1 p_2}(x)}_{B_0} + \cdots + \underbrace{x^{(p_1-1)p_3}\Phi_{p_1 p_2}(x)}_{B_{p_1-1}} \right)}_{A_0} + \underbrace{x^{p_2 p_3}\left(\underbrace{\Phi_{p_1 p_2}(x)}_{B_0} + \cdots + \underbrace{x^{(p_1-1)p_3}\Phi_{p_1 p_2}(x)}_{B_{p_1-1}} \right)}_{A_1}.$$

$$\underbrace{}_{\Psi_{p_1 p_2 p_3}(x)}$$

Let

$$\lambda = \mathrm{tdeg}(A_1) - \deg(A_0) = 2n\frac{1}{p_1} - \deg(\Psi_n).$$

From D2, we have

$$\begin{aligned}
\lambda &= 2n\frac{1}{p_1} - \deg(\Psi_n) \\
&= 2p_2 p_3 - p_1 p_2 p_3 + (p_1 - 1)(p_2 - 1)(p_3 - 1) \\
&= p_2 p_3 - p_1 p_3 + p_3 + p_1 - 1 - p_2(p_1 - 1) \\
&> (p_2 - p_1)p_3 + p_3 + p_1 - 1 - 2p_3 \\
&= (p_2 - p_1 - 2)p_3 + p_3 + p_1 - 1. \tag{5}
\end{aligned}$$

Thus $\lambda > 0$, i.e. there is no overlap between A_0 and A_1. Note that $g(A_0) = g(A_1)$. Thus

$$g(\Psi_n) = \max\{\lambda, g(A_0)\}.$$

We claim that $\lambda > g(A_0)$. Note

$$\mathrm{D2} \quad \Leftrightarrow \quad \varphi(p_1 p_2) < 2p_3 - (p_1 - 1).$$

We will split the proof into the following two cases:

Case 1. $\varphi(p_1 p_2) < p_3$.

Note that $\deg(B_0) = \varphi(p_1 p_2)$ and $\mathrm{tdeg}(B_1) = p_3$. Hence there is no overlap between B_0 and B_1. Likewise there is no overlap between B_i and B_{i+1} for all $i = 1, \ldots, p_1 - 2$. Note

$$g(B_0) = g(B_1) = \cdots = g(B_{p_1-1}) = g(\Phi_{p_1 p_2}) = p_1 - 1$$

from Theorem 1. Hence

$$g(A_0) = \max\{p_3 - \varphi(p_1 p_2), p_1 - 1\}.$$

From Eq. (5), we have

$$\lambda > (p_2 - p_1 - 2)p_3 + p_3 + p_1 - 1 > p_3 > p_3 - \varphi(p_1 p_2),$$

$$\lambda > (p_2 - p_1 - 2)p_3 + p_3 + p_1 - 1 > p_1 - 1.$$

Thus we have proved that $\lambda > g(A_0)$ when $p_3 > \varphi(p_1 p_2)$.

Case 2. $p_3 \leqslant \varphi(p_1 p_2) < 2p_3 - (p_1 - 1)$.

Note

$$\mathrm{tdeg}(B_2) - \deg(B_0) = 2p_3 - \varphi(p_1 p_2) > 0.$$

Thus $B_0, B_1, \ldots, B_{p_1-1}$ overlap as the following diagram shows.


In the above diagram, the tail exponent and the leading exponent of B_0 are colored in black to indicate that they actually occur in B_0. The other exponents are colored in gray to indicate that they may or may not occur. The same is done for $B_2, \ldots, B_{p_1-1}$ since they have the same sparsity structure (shifting does not change the sparsity structure). In B_0, there occurs at least one exponent between 0 and p_3. Otherwise we would have $p_3 - 0 > p_1 - 1 = g(B_0)$ which is impossible. Let α be the largest such exponent. Then $p_3 - \alpha \leqslant p_1 - 1$. Since

$$2p_3 > \alpha + p_3 \geqslant 2p_3 - (p_1 - 1) > \varphi(p_1 p_2),$$

the exponent $\alpha + p_3$ lies between $\varphi(p_1 p_2)$ and $2p_3$ in B_1.
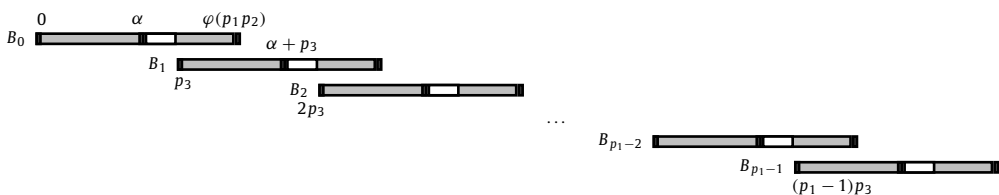
Now we consider the polynomials $E_1, L_1, L_2, \ldots, L_{p_1-2}$ and E_2 indicated in the following diagram
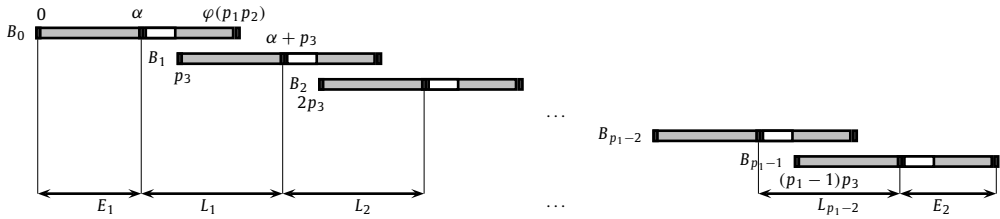
where $\deg(E_1) = \alpha$, $\mathrm{tdeg}(E_2) = \deg(\Psi_n) - \alpha$ and $\deg(L_i) = \mathrm{tdeg}(L_{i+1})$. Since $L_1, L_2, \ldots, L_{p_1-2}$ have the same gap structure, we have

$$g(L_1) = g(L_2) = \cdots = g(L_{p_1-2}).$$

Hence, we have

$$g(A_0) = \max\{g(E_1), g(E_2), g(L_1)\}.$$

From Theorem 1 and Eq. (5), we have

$$\lambda > (p_2 - p_1 - 2)p_3 + p_3 + p_1 - 1 > p_1 - 1 = g(\Phi_{p_1 p_2}) \geqslant g(E_1), g(E_2).$$

Note

$$g(L_1) \leqslant (\alpha + p_3) - \alpha = p_3.$$

From Eq. (5), we have

$$\begin{aligned}
\lambda &= 2n\frac{1}{p_1} - \deg(\Psi_n) \\
&> p_3(p_2 - p_1 - 2) + p_3 + p_1 - 1 \\
&> p_3 \\
&\geqslant g(L_1).
\end{aligned}$$

Thus we have proved that $\lambda > g(A_0) = \max\{g(E_1), g(L_1)\}$ when $p_3 \leqslant \varphi(p_1 p_2) < 2p_3 - (p_1 - 1)$. $\square$

Lemma 7. *Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes. Then we have*

$$\text{C1} \vee \text{C2} \quad \Rightarrow \quad \text{D1} \vee \text{D2},$$

where

$$\begin{aligned}
&\text{C1:} \quad 4(p_1 - 1) \leqslant p_2, \\
&\text{C2:} \quad\quad p_1^2 \leqslant p_3, \\
&\text{D1:} \quad\quad 2n\frac{1}{p_1} > \frac{4}{3}\deg(\Psi_n), \\
&\text{D2:} \quad p_2(p_1 - 1) < 2p_3.
\end{aligned}$$

Proof. Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes. We will prove the contrapositive.

$$\neg D1 \wedge \neg D2 \quad \Rightarrow \quad \neg C1 \wedge \neg C2.$$

Let

$$V = \left\{ (p_1, p_2, p_3) : \neg\, D1 \wedge \neg D2 \wedge p_1 < p_2 \wedge p_2 < p_3 \right\}.$$

It suffices to prove

$$(p_1, p_2, p_3) \in V \quad \Rightarrow \quad \neg C1 \wedge \neg C2.$$

Note

$$V = \left\{ (p_1, p_2, p_3) : h_1 \leqslant 0 \wedge h_2 \leqslant 0 \wedge h_3 < 0 \wedge h_4 < 0 \right\},$$
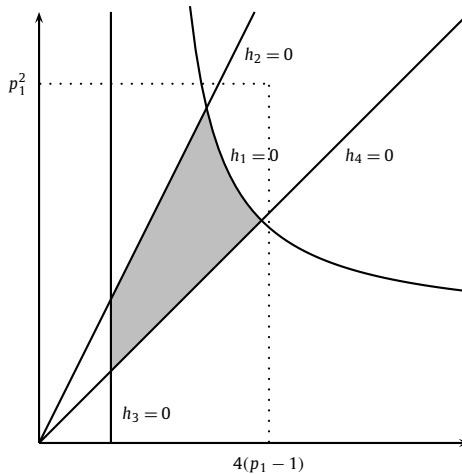
where

$$h_1 = 2n \frac{1}{p_1} - \frac{4}{3} \deg(\Psi_n),$$

$$h_2 = 2p_3 - p_2(p_1 - 1),$$

$$h_3 = p_1 - p_2,$$

$$h_4 = p_2 - p_3.$$

The shaded area in the plot below shows the cross section of the set V for a fixed p_1.

By finding the p_2 coordinate of the intersection point between the curves $h_1 = 0$ and $h_4 = 0$, we have

$$(p_1, p_2, p_3) \in V \quad \Rightarrow \quad p_2 \leqslant 2(p_1 - 1) + \sqrt{4p_1^2 - 10p_1 + 6}$$

$$\Rightarrow \quad p_2 < 2(p_1 - 1) + \sqrt{4(p_1 - 1)^2}$$

$$\Rightarrow \quad p_2 < 4(p_1 - 1)$$

$$\Rightarrow \quad \neg C1.$$

By finding the p_3 coordinate of the intersection point between the curves $h_1 = 0$ and $h_2 = 0$, we have

$$(p_1, p_2, p_3) \in V \quad \Rightarrow \quad p_3 \leqslant \frac{1}{2}(p_1 - 1)\left(p_1 + 1 + \sqrt{p_1^2 + 2p_1 - 3}\right)$$

$$\Rightarrow \quad p_3 < \frac{1}{2}(p_1 - 1)\left(p_1 + 1 + \sqrt{(p_1 + 1)^2}\right)$$

$$\Rightarrow \quad p_3 < (p_1 - 1)(p_1 + 1)$$

$$\Rightarrow \quad p_3 < p_1^2$$

$$\Rightarrow \quad \neg C2. \quad \square$$

4.3. Proof of Theorem 3

Theorem 3 follows immediately from Lemma 8 and Lemma 9.

Lemma 8. Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes. We have

$$\max\left\{ p_1 - 1, 2n\frac{1}{p_1} - \deg(\Psi_n) \right\} \leqslant g(\Psi_n).$$

Proof. We recall the diagram in the proof of Lemma 6:

$$-\left(\underbrace{\Phi_{p_1 p_2}(x)}_{B_0} + \cdots + \underbrace{x^{(p_1 - 1)p_3}\Phi_{p_1 p_2}(x)}_{B_{p_1 - 1}} \right) + x^{p_2 p_3}\left(\underbrace{\Phi_{p_1 p_2}(x)}_{B_0} + \cdots + \underbrace{x^{(p_1 - 1)p_3}\Phi_{p_1 p_2}(x)}_{B_{p_1 - 1}} \right).$$

$$\underbrace{\phantom{-\left(\Phi_{p_1 p_2}(x) + \cdots + x^{(p_1 - 1)p_3}\Phi_{p_1 p_2}(x) \right)}}_{A_0} \quad \underbrace{\phantom{x^{p_2 p_3}\left(\Phi_{p_1 p_2}(x) + \cdots + x^{(p_1 - 1)p_3}\Phi_{p_1 p_2}(x) \right)}}_{A_1}$$

$$\underbrace{}_{\Psi_{p_1 p_2 p_3}(x)}$$

Let $\lambda = \mathrm{tdeg}(A_1) - \deg(A_0)$. Then we have

$$\lambda = p_2 p_3 - \left(\deg(\Psi_n) - p_2 p_3\right) = 2 p_2 p_3 - \deg(\Psi_n) = 2n\frac{1}{p_1} - \deg(\Psi_n).$$

If $\lambda \leqslant 0$, then $\lambda \leqslant g(\Psi_n)$ obviously. If $\lambda > 0$, there exists a gap between A_0 and A_1, thus $\lambda \leqslant g(\Psi_n)$. We recall Eq. (4):

$$\Phi_{p_1 p_2}(x) = 1 - x + x^{p_1} + \text{terms of degree higher than } p_1.$$

Therefore there exists a gap in B_0 of size $p_1 - 1$. Since $p_1 < p_3$, we have

$$\Psi_n(x) = 1 - x + x^{p_1} + \text{terms of degree higher than } p_1.$$

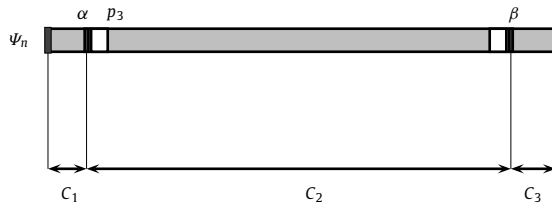Hence, $p_1 - 1 \leqslant g(\Psi_n)$. $\quad \square$

Lemma 9. *Let $n = p_1 p_2 p_3$ where $p_1 < p_2 < p_3$ are odd primes. Then*

$$g(\Psi_n) < 2n\left(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3}\right) - \deg(\Psi_n).$$

Proof. Let $U = 2n(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3}) - \deg(\Psi_n)$. Then lemma follows from the following claims.

Claim 1. $g(\Psi_n) \leqslant \max\{p_1 - 1, \deg(\Psi_n) - 2(p_3 - (p_1 - 1))\}$.

Let α be the largest exponent less than p_3 occurring in Ψ_n and $\beta = \deg(\Psi_n) - \alpha$.

Then we have

$$g(\Psi_n) = \max\{g(C_1), g(C_2), g(C_3)\}.$$

Note that $g(C_1) = g(C_3) \leqslant p_1 - 1$ and $g(C_2) \leqslant \deg(\Psi_n) - 2\alpha$. Since $\alpha \geqslant p_3 - (p_1 - 1)$, we have

$$g(C_2) \leqslant \deg(\Psi_n) - 2(p_3 - (p_1 - 1)).$$

Therefore, we have

$$g(\Psi_n) \leqslant \max\{p_1 - 1, \deg(\Psi_n) - 2(p_3 - (p_1 - 1))\}.$$

Claim 2. $U > p_1 - 1$.

Note that

$$
\begin{aligned}
&U - (p_1 - 1) \\
&= 2n\left(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3}\right) - \deg(\Psi_n) - (p_1 - 1) \\
&= 2(p_1 p_2 + p_2 p_3 + p_3 p_1) - (p_1 p_2 p_3 - (p_1 - 1)(p_2 - 1)(p_3 - 1)) - (p_1 - 1) \\
&= 2(p_1 p_2 + p_2 p_3 + p_3 p_1) - p_1 p_2 p_3 + (p_1 - 1)(p_2 p_3 - p_2 - p_3) \\
&= 2(p_1 p_2 + p_2 p_3 + p_3 p_1) - p_1 p_2 p_3 + p_1 p_2 p_3 - p_1 p_2 - p_1 p_3 - p_2 p_3 + p_2 + p_3 \\
&= 2(p_1 p_2 + p_2 p_3 + p_3 p_1) - p_1 p_2 - p_1 p_3 - p_2 p_3 + p_2 + p_3 \\
&= p_1 p_2 + p_2 p_3 + p_3 p_1 + p_2 + p_3 \\
&> 0.
\end{aligned}
$$

Claim 3. $U > \deg(\Psi_n) - 2(p_3 - (p_1 - 1))$.

Note that

$$U - \big(\deg(\Psi_n) - 2\big(p_3 - (p_1 - 1)\big)\big)$$

$$= 2n\left(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3}\right) - 2\deg(\Psi_n) + 2\big(p_3 - (p_1 - 1)\big)$$

$$= 2(p_1 p_2 + p_2 p_3 + p_3 p_1) - 2\big(p_1 p_2 p_3 - (p_1 - 1)(p_2 - 1)(p_3 - 1)\big) + 2p_3 - 2(p_1 - 1)$$

$$= 2(p_1 p_2 + p_2 p_3 + p_3 p_1) - 2(p_1 p_2 + p_2 p_3 + p_3 p_1 - p_1 - p_2 - p_3 + 1) + 2p_3 - 2(p_1 - 1)$$

$$= 2p_1 + 2p_2 + 2p_3 - 2 + 2p_3 - 2p_1 + 2$$

$$= 2p_2 + 4p_3$$

$$> 0. \qquad \square$$

Acknowledgments

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, J. Number Theory 100 (2003) 104–116.
[2] M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, Fibonacci Quart. 16 (1978) 302–306.
[3] B. Bzdęga, On the height of cyclotomic polynomials, arXiv preprint, arXiv:1012.3897v1, December 2010.
[4] J. Fintzen, Cyclotomic polynomial coefficients $a(n, k)$ with n and k in prescribed residue classes, J. Number Theory 131 (2011) 1852–1863.
[5] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, J. Cryptology 23 (2) (2009) 224–280.
[6] Y. Gallot, P. Moree, Ternary cyclotomic polynomials having a large coefficient, J. Reine Angew. Math. 632 (2009) 105–125.
[7] H. Hong, E. Lee, H.S. Lee, C.M. Park, Simple and exact formula for minimum loop length in Ate$_i$ pairing based on Brezing–Weng curves, Des. Codes Cryptogr. (2012), http://dx.doi.org/10.1007/s10623-011-9605-y, in press.
[8] N. Kaplan, Flat cyclotomic polynomials of order three, J. Number Theory 127 (2007) 118–126.
[9] T.Y. Lam, K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, Amer. Math. Monthly 103 (1996) 562–564.
[10] E. Lee, H.S. Lee, C.M. Park, Efficient and generalized pairing computation on abelian varieties, IEEE Trans. Inform. Theory 55 (4) (2009) 1793–1803.
[11] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, Bull. Amer. Math. Soc. 42 (1936) 389–392.
[12] H. Lenstra, Vanishing sums of roots of unity, in: Proc. Bicentennial Congress Wiskundig Genootschap, Part II, Vrije Univ., Amsterdam, 1978, pp. 249–268.
[13] P. Moree, Inverse cyclotomic polynomials, J. Number Theory 129 (3) (2009) 667–680.
[14] R. Thangadurai, On the coefficients of cyclotomic polynomials, in: Cyclotomic Fields and Related Topics, Pune, 1999, Bhaskaracharya Pratishthana, Pune, 2000, pp. 311–322.
[15] F. Vercauteren, Optimal pairings, IEEE Trans. Inform. Theory 56 (1) (2010) 455–461.
[16] C. Zhao, F. Zhang, J. Huang, A note on the Ate pairing, Int. J. Inf. Secur. 7 (6) (2008) 379–382.