POLITECNICO DI TORINO
Repository ISTITUZIONALE

A survey on coefficients of cyclotomic polynomials

Original
A survey on coefficients of cyclotomic polynomials / Sanna, Carlo. - In: EXPOSITIONES MATHEMATICAE. - ISSN 0723-0869. - STAMPA. - (2022). [10.1016/j.exmath.2022.03.002]

Availability:
This version is available at: 11583/2962581 since: 2022-05-04T09:04:05Z

Publisher:
Elsevier

Published
DOI:10.1016/j.exmath.2022.03.002

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
Elsevier postprint/Author's Accepted Manuscript

© 2022. This manuscript version is made available under the CC-BY-NC-ND 4.0 license http://creativecommons.org/licenses/by-nc-nd/4.0/.The final authenticated version is available online at: http://dx.doi.org/10.1016/j.exmath.2022.03.002

(Article begins on next page)

12 October 2024

arXiv:2111.04034v2 [math.NT] 15 Dec 2021

A Survey on Coefficients of Cyclotomic Polynomials

Carlo Sanna

Politecnico di Torino
Department of Mathematical Sciences
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
carlo.sanna.dev@gmail.com

Abstract

Cyclotomic polynomials play an important role in several areas of mathematics and their study has a very long history, which goes back at least to Gauss (1801). In particular, the properties of their coefficients have been intensively studied by several authors, and in the last 10 years there has been a burst of activity in this field of research. This concise survey attempts to collect the main results regarding the coefficients of the cyclotomic polynomials and to provide all the relevant references to their proofs.

Contents

1 Introduction **1**
1.1 Definitions and basic facts . . . 1

2 Binary cyclotomic polynomials **3**

3 Ternary cyclotomic polynomials **6**
3.1 Bounds on the height and Beiter's conjecture . . . 6
3.2 Flatness . . . 8
3.3 Jump one property . . . 9

4 Higher order cyclotomic polynomials **10**

5 Height of cyclotomic polynomials **10**
5.1 Asymptotic bounds on $A(n)$ . . . 10
5.2 Bounds on $A(n)$ in terms of prime factors . . . 11
5.3 The dual function $a(j)$ . . . 11

6 Maximum gap **12**

7 The set of coefficients **12**

8 Formulas for the coefficients **13**

9 Miscellaneous results **14**

10 Algorithms and numerical data **14**

11 Relatives of cyclotomic polynomials **15**
11.1 Inverse cyclotomic polynomials . . . 15
11.2 Divisors of $X^n - 1$ . . . 17
11.3 Inclusion-exclusion polynomials . . . 18
11.4 Unitary cyclotomic polynomials . . . 19

References **20**

1 Introduction

Cyclotomic polynomials play an important role in several areas of mathematics and their study has a very long history, which goes back at least to Gauss (1801) [64].

For instance, cyclotomic polynomials appear in: the solution of the problem of which regular n-gons are constructible with straightedge and compass (Gauss–Wantzel theorem [99, p. 46]); elementary proofs of the existence of infinitely many prime numbers equal to 1, respectively -1, modulo n, which is a special case of Dirichlet's theorem on primes in arithmetic progressions [112, Sections 48–50]; Witt's proof [128] of Wedderburn's little theorem that every finite domain is a field [86, Section 13]; the "cyclotomic criterion" in the study of primitive divisors of Lucas and Lehmer sequences [24]; and lattice-based cryptography [110, 113].

In particular, the coefficients of cyclotomic polynomials have been intensively studied by several authors, and in the last 10 years there has been a burst of activity in this field of research. This concise survey attempts to collect the main results regarding the coefficients of the cyclotomic polynomials and to provide all the relevant references to their proofs. Previous surveys on this topic were given by Lenstra (1979) [91], Vaughan (1989) [125], and Thangadurai (2000) [122].

Acknowledgments The author is grateful to Tsit-Yuen Lam, Pieter Moree, and Carl Pomerance, for providing useful suggestions that improved the quality of this survey. The author is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino.

1.1 Definitions and basic facts

Let n be a positive integer. The *nth cyclotomic polynomial* $\Phi_n(X)$ is defined as the monic polynomial whose roots are the nth primitive roots of unity, that is,

$$\Phi_n(X) := \prod_{\substack{1 \le k \le n \\ \gcd(n,k)=1}} \left(X - e^{2\pi \mathrm{i} k/n}\right). \tag{1}$$

The word "cyclotomic" comes from the ancient Greek words "cyclo" (circle) and "tomos" (cutting), and refers to how the nth roots of unit divide the circle into equal parts. Note that, incidentally, the Greek letter Φ looks a bit like a cut circle. The degree of $\Phi_n(X)$ is equal to $\varphi(n)$, where φ is the Euler totient function. Despite its definition in terms of complex numbers, it can be proved that $\Phi_n(X)$ has integer coefficients. Furthermore, $\Phi_n(X)$ is irreducible over $\mathbb{Q}$ and, consequently, it is the minimal polynomial of any primitive nth root of unity. The irreducibility of $\Phi_n(X)$ for n prime was first proved by Gauss (1801) [64], and the irreducibility of $\Phi_n(X)$ in general was first proved by Kronecker (1854) [85]. Weintraub (2013) [127] presented proofs of the irreducibility of $\Phi_n(X)$ due to Gauss, Kronecker, Schönemann, and Eisenstein, for n prime, and Dedekind, Landau, and Schur,[1] for every n.

From (1) it follows easily that

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X), \tag{2}$$

[1] Perhaps curiously, Schur's proof of the irreducibility of $\Phi_n(X)$ was set to rhymes [42, pp. 38–41].

which in turn, by the Möbius inversion formula, yields that

$$\Phi_n(X) = \prod_{d \mid n} \left(X^{n/d} - 1\right)^{\mu(d)} = \prod_{d \mid n} \left(X^d - 1\right)^{\mu(n/d)}, \tag{3}$$

where μ is the Möbius function. In particular, we have that

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1, \tag{4}$$

for every prime number p.

The next lemma collects some important elementary identities, which can be proved either using (3) or checking that both sides have the same zeros [91, 122].

Lemma 1.1. *For every positive integer n and every prime number p, we have that:*

(i) $\Phi_{pn}(X) = \Phi_n(X^p)$ *if* $p \mid n$*;*

(ii) $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ *if* $p \nmid n$*;*

(iii) $\Phi_{2n}(X) = (-1)^{\varphi(n)}\Phi_n(-X)$ *if* $2 \nmid n$*;*

(iv) $\Phi_n(X) = \Phi_{\mathrm{rad}(n)}(X^{n/\mathrm{rad}(n)})$*, where* $\mathrm{rad}(n)$ *is the product of the primes dividing* n*;*

(v) $\Phi_n(1/X) = X^{-\varphi(n)}\Phi_n(X)$ *if* $n > 1$*.*

Starting from $\Phi_1(X) = X - 1$ and using Lemma 1.1's (i) and (ii), one can inductively compute the cyclotomic polynomials. The first ten cyclotomic polynomials are:

$$\begin{aligned}
&\Phi_1(X) = X - 1 && \Phi_6(X) = X^2 - X + 1\\
&\Phi_2(X) = X + 1 && \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\\
&\Phi_3(X) = X^2 + X + 1 && \Phi_8(X) = X^4 + 1\\
&\Phi_4(X) = X^2 + 1 && \Phi_9(X) = X^6 + X^3 + 1\\
&\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 && \Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1
\end{aligned}$$

A natural observation is that the coefficients of the cyclotomic polynomials are very small, and one could be even tempted to conjecture that they are always in $\{-1, 0, +1\}$. The first counterexample to this conjecture occurs for $n = 105$, since we have

$$\begin{aligned}
\Phi_{105}(X) = {} & X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - \mathbf{2}X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34}\\
& + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15}\\
& + X^{14} + X^{13} + X^{12} - X^{9} - X^{8} - \mathbf{2}X^{7} - X^{6} - X^{5} + X^{2} + X + 1.
\end{aligned}$$

It is no coincidence that $105 = 3 \cdot 5 \cdot 7$ is the smallest odd positive integer having three different prime factors. Indeed, every cyclotomic polynomial $\Phi_n(X)$ such that n has less than three odd prime factors has all its coefficients in $\{-1, 0, +1\}$ (see Section 2).

For every positive integer n, let us write

$$\Phi_n(X) = \sum_{j \geq 0} a_n(j) X^j, \quad a_n(j) \in \mathbb{Z},$$

so that $a_n(j)$ is the coefficient of X^j in $\Phi_n(X)$. (Note that $a_n(j) = 0$ for $j \notin [0, \varphi(n)]$.) The peculiarity of the smallness of the coefficients of the cyclotomic polynomials was very well explained by D. H. Lehmer (1966) [89], who wrote: "The smallness of $|a_n(j)|$ would appear to be one of the fundamental conspiracies of the primitive nth roots of unity. When one considers that $a_n(j)$ is a sum of $\binom{\varphi(n)}{j}$ unit vectors (for example 73629072 in the case of $n = 105$, $j = 7$) one realizes the extent of the cancellation that takes place."

In light of Lemma 1.1's (iii) and (iv), for the purpose of studying the coefficients of $\Phi_n(X)$ it suffices to consider only odd squarefree integers n. A squarefree positive integer n, or a cyclotomic polynomial $\Phi_n(X)$, is *binary*, *ternary*, ... if the number of prime factors of n is 2, 3, ..., respectively. The *order* of $\Phi_n(X)$ is the number of prime factors of n. From Lemma 1.1's (v) we have that for every integer $n > 1$ the cyclotomic polynomial $\Phi_n(X)$ is *palindromic*, that is,

$$a_n(\varphi(n) - j) = a_n(j), \qquad \text{for } j = 0, \dots, \varphi(n).$$

We conclude this section by defining the main quantities that have been considered in the study of the coefficients of the cyclotomic polynomials. First, we have $A(n)$, $A^+(n)$, and $A^-(n)$, which are defined as follows

$$A(n) := \max_{j \geq 0} |a_k(j)|, \quad A^+(n) := \max_{j \geq 0} a_k(j), \quad A^-(n) := \min_{j \geq 0} a_k(j).$$

In general, the *height* of a polynomial $P \in \mathbb{C}[X]$ is defined as the maximum of the absolute values of the coefficients of P, and P is *flat* if its height is not exceeding 1. Thus, $A(n)$ is the height of $\Phi_n(X)$. We also let $\mathcal{A}(n) := \{a_n(j) : 0 \leq j \leq \varphi(n)\}$ be the set of coefficients of $\Phi_n(X)$. Moreover, we let $\theta(n) := \#\{j \geq 0 : a_n(j) \neq 0\}$ be the number of nonzero coefficients of $\Phi_n(X)$. The *maximum gap* of a nonzero polynomial $P(X) = \sum_{i=1}^{k} c_k X^{e_k} \in \mathbb{C}[X]$, where $c_1, \dots, c_k \in \mathbb{C}^*$ and $e_1 < \cdots < e_k$, is defined as $G(P) := \max\{e_{j+1} - e_j : j < k\}$. We let $G(n) := G(\Phi_n)$ denote the maximum gap of $\Phi_n(X)$. Note that by (4) we have that $A(p) = A^+(p) = A^-(p) = 1$, $\mathcal{A}(p) = \{1\}$, $\theta(p) = p$, and $G(p) = 1$, for every prime number p. Thus, the first interesting case in the study of these quantities is the one of binary cyclotomic polynomials.

2 Binary cyclotomic polynomials

The understanding of the coefficients of binary cyclotomic polynomials is quite complete. Let p and q be distinct prime numbers. From (3) it follows that

$$\Phi_{pq}(X) = \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}.$$

Migotti (1883) [101] and Bang (1895) [17] proved that the coefficients of every binary cyclotomic polynomial belong to $\{+1, -1, 0\}$. Beiter (1964) [20] gave a first criterion to enstablish if $a_{pq}(j)$ is equal to $+1$, -1, or 0. This criterion is a bit difficult to apply, but she used it to compute the midterm coefficient of $\Phi_{pq}(X)$. Using a different method, Habermehl, Richardson, and Szwajkos (1964) [67] determined the coefficients of $\Phi_{3p}(X)$, for $p > 3$. Carlitz (1966) [38] gave a formula for the number of nonzero coefficients of $\Phi_{pq}(X)$, and Lenstra (1979) [91] proved an expansion for $\Phi_{pq}(X)$, which was then rediscovered by Lam and Leung (1996) [87], that leads to an explicit determination of $a_{pq}(j)$.

Moree (2014) [106] generalized this formula to binary inclusion-exclusion polynomials (see Section 11.3), and he also showed a connection with numerical semigroups.

The following theorem gives a precise description of the coefficients of binary cyclotomic polynomials [87, 91, 106, 122].

Theorem 2.1. *Let $p < q$ be distinct prime numbers, and let $\overline{p}$ and $\overline{q}$ be the unique positive integers such that $pq + 1 = p\overline{p} + q\overline{q}$. (Equivalently, $\overline{p}$ is the inverse of p modulo q and $\overline{q}$ is the inverse of q modulo p.) We have that:*

(i) It holds

$$\Phi_{pq}(X) = \sum_{i=0}^{\overline{p}-1} X^{pi} \sum_{j=0}^{\overline{q}-1} X^{qj} - X^{-pq} \sum_{i=\overline{p}}^{q-1} X^{pi} \sum_{j=\overline{q}}^{p-1} X^{qj}.$$

(ii) For every nonnegative integer $j < pq$, we have that either $j = px + qy$ or $j = px + qy - pq$ with $x < q$ the unique nonnegative integer such that $px \equiv j \pmod{q}$ and $y < p$ the unique nonnegative integer such that $qy \equiv j \pmod{p}$; and it holds

$$a_{pq}(j) = \begin{cases} +1 & \text{if } j = px + qy \text{ with } 0 \le x < \overline{p},\ 0 \le y < \overline{q}; \\ -1 & \text{if } j = px + qy - pq \text{ with } \overline{p} \le x < q,\ \overline{q} \le y < p; \\ 0 & \text{otherwise.} \end{cases}$$

(iii) The number of positive coefficients of $\Phi_{pq}(X)$ is equal to $\overline{p}\,\overline{q}$, the number of negative coefficients is equal to $\overline{p}\,\overline{q} - 1$, and (thus) the number of nonzero coefficients of $\Phi_{pq}(X)$ is equal to $2\overline{p}\,\overline{q} - 1$.

(iv) The nonzero coefficients of $\Phi_{pq}(X)$ alternates between $+1$ and -1.

(v) The midterm coefficient of $\Phi_{pq}(X)$ satisfies $a_{pq}(\varphi(pq)/2) = (-1)^{\overline{p}-1}$.

Moree [106] gave a nice way to illustrate Theorem 2.1's (ii) by using what he called an *LLL-diagram* (for Lenstra, Lam, and Leung). This is a $p \times q$ matrix constructed as follows. Start with 0 in the bottom-left entry, add p for every move to the right, add q for every move upward, and reduce all entries modulo pq. The numbers in the bottom-left $\overline{p} \times \overline{q}$ submatrix are the exponents of the positive terms of $\Phi_{pq}(X)$, and the numbers in the top-right $(p - \overline{p}) \times (q - \overline{q})$ submatrix are the exponents of the negative terms of $\Phi_{pq}(X)$. For example, the LLL-diagram for the binary cyclotomic polynomial

$$\begin{aligned}\Phi_{5\cdot 7}(X) = X^{24} - X^{23} + X^{19} - X^{18} + X^{17} - X^{16} + X^{14} - X^{13} \\ + X^{12} - X^{11} + X^{10} - X^{8} + X^{7} - X^{6} + X^{5} - X + 1\end{aligned}$$

is the following

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

By Theorem 2.1's (iii), for every binary number $n = pq$, with $p < q$ primes, the number of nonzero coefficients of $\Phi_n(X)$ is $\theta_n = 2\overline{p}\,\overline{q} - 1$. From $pq + 1 = p\overline{p} + q\overline{q}$ it follows in an elementary way that $\theta_n > n^{1/2}$ [59, Section 3.1]. Lenstra (1979) [91] proved that for every $\varepsilon > 0$ there exist infinitely many binary $n = pq$ such that $\theta_n < p^{8/13+\varepsilon}$. The proof is based on a result of Hooley (1973) [71] that says that for every $\varepsilon > 0$ there exist infinitely many prime number p such that $P(p-1) > p^{5/8-\varepsilon}$, where $P(n)$ denotes the largest prime factor of n. Hooley's result has been improved by several authors. Currently, the best bound is $P(p-1) > p^{0.677}$, which is due to Baker and Harman (1998) [16]. This reduces the exponent $8/13$ of Lenstra's bound to $1/(1 + 0.677) = 0.596\ldots$. Using a different method, Bzdęga (2012) [29] proved that there are infinitely many binary numbers n such that $\theta_n < n^{1/2+\varepsilon}$, and also gave upper and lower bounds for the number $H_\varepsilon(x)$ of binary $n \le x$ such that $\theta_n < n^{1/2+\varepsilon}$. Fouvry (2013) [59] proved the following asymptotic formula for $H_\varepsilon(x)$.

Theorem 2.2. *For $\varepsilon \in (0, 1/2)$, let*

$$C(\varepsilon) := \frac{2}{1+2\varepsilon} \log\left(\frac{1+2\varepsilon}{1-2\varepsilon}\right).$$

Then for every $\varepsilon_0 > 0$, uniformly for $\varepsilon \in (12/15 + \varepsilon_0, 1/2 - \varepsilon_0)$, we have that

$$H_\varepsilon(x) \sim C(\varepsilon)\,\frac{x^{1/2+\varepsilon}}{\log x} \tag{5}$$

as $x \to +\infty$.

Furthermore, Fouvry [59] provided an upper bound and a lower bound for $H_\varepsilon(x)$ of the same order of (5), and showed that the Elliott–Halberstam Conjecture implies that (5) holds in the range $\varepsilon \in (\varepsilon_0, 1/2 - \varepsilon_0)$.

Hong, Lee, Lee, and Park (2012) [70] determined the maximum gap of binary cyclotomic polynomials, and Moree (2014) [106] gave another proof of the result using numerical semigroups. Yet another short proof was given by Kaplan (2016) [37, End of Section 2.1]. Furthermore, Camburu, Ciolan, Luca, Moree, and Shparlinski (2016) [37] determined the number of maximum gaps of $\Phi_{pq}(X)$, and the existence of particular gaps in the case in which $q \equiv \pm 1 \pmod{p}$. The following theorem collects these results [37, 70, 106].

Theorem 2.3. *Let $p < q$ be prime numbers. Then:*

(i) $G(pq) = p - 1$.

(ii) The number of maximum gaps of $\Phi_{pq}(X)$ is equal to $2\lfloor q/p \rfloor$.

(iii) $\Phi_{pq}(X)$ contains the sequence of consecutive coefficients

$$\pm 1, \underbrace{0, \ldots, 0}_{m \text{ times}}, \pm 1$$

for all $m \in \{0, \ldots, p-2\}$ if and only if $q \equiv \pm 1 \pmod{p}$.

Cafure and Cesaratto (2021) [36] considered the coefficients of $\Phi_{pq}(X)$ as a word over the ternary alphabet $\{+1, -1, 0\}$, and provided an algorithm that, given as input $p < q$ and the quotient and remainder of the division of q by p, computes $\Phi_{pq}(X)$ performing $O(pq)$ simple operations on words. Chu (2021) [40] proved that the exponents of the positive, respectively negative, terms of $\Phi_{pq}(X)$ are in arithmetic progression if and only if $q \equiv 1 \pmod{p}$, respectively $q \equiv -1 \pmod{p}$.

3 Ternary cyclotomic polynomials

Ternary cyclotomic polynomials are the simplest ones for which the behavior of the coefficients is not completely understood. Kaplan (2007) [77, Lemma 1] proved the following lemma, which provides a formula for the coefficients of ternary cyclotomic polynomials. This is known as *Kaplan's lemma* and has been used to prove several results on ternary cyclotomic polynomials [47, 60, 61, 63, 72, 108, 130, 131, 132, 136, 137].

Lemma 3.1 (Kaplan's lemma)**.** *Let $p < q < r$ be odd prime numbers and let $j \geq 0$ be an integer. For every integer $i \in [0, pq)$, put*

$$b_i := \begin{cases} a_{pq}(i) & \text{if } ri \leq j; \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$a_{pqr}(j) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}),$$

where $f(m)$ is the unique integer such that $f(m) \equiv r^{-1}(j-m) \pmod{pq}$, $0 \leq f(m) < pq$.

Lemma 3.1 reduces the computation of $a_{pqr}(j)$ to that of $a_{pq}(i)$, which in turn is provided by Theorem 2.1's (ii). Note that in order to compute $a_{pqr}(j)$ using Lemma 3.1 and Theorem 2.1's (ii) it is not necessary to compute $f(m)$ and $f(m+q)$, but it suffices to compute $[f(m)]_p$, $[f(m)]_q$, $[f(m+q)]_p$, and $[f(m+q)]_q$, which can be easier, where $[k]_p$ and $[k]_q$ are the unique nonnegative integers $x < q$ and $y < p$ such that $px \equiv k \pmod{q}$ and $qy \equiv k \pmod{p}$, for every integer k. Actually, since $[f(m)]_p = [f(m+q)]_p$, it suffices to compute $[f(m)]_p$, $[f(m)]_q$, and $[f(m+q)]_q$.

For the rest of this section, let $p < q < r$ be odd prime numbers and let $n = pqr$ be a ternary integer. The next subsections describe the main themes of research on ternary cyclotomic polynomials.

3.1 Bounds on the height and Beiter's conjecture

Upper bounds for the height of ternary cyclotomic polynomials have been studied by many authors. Bang (1895) [17] proved that $A(pqr) \leq p - 1$. Beiter (1968) [21] made the following conjecture, which is known as *Beiter's conjecture*.

Conjecture 3.1 (Beiter's conjecture)**.** *$A(pqr) \leq \frac{1}{2}(p+1)$ for all odd primes $p < q < r$.*

Beiter (1968) [21] proved her conjecture in the case in which $q \equiv \pm 1 \pmod{p}$ or $r \equiv \pm 1 \pmod{p}$. As a consequence, Beiter's conjecture is true for $p = 3$. Also, Bloom (1968) [25] showed that Beiter's conjecture is true for $p = 5$. Beiter (1971) [22] improved Bang's bound to $A(pqr) \leq p - \lfloor (p+1)/4 \rfloor$. Möller (1971) [103] proved that for every odd prime number p there exists a ternary cyclotomic polynomial $\Phi_{pqr}(X)$, with $p < q < r$, having a coefficient equal to $(p+1)/2$. This shows that Beiter's conjecture, if true, is the best possible. Bachman (2003) [10] proved an upper bound for $A^+(pqr)$ and a lower bound for $A^-(pqr)$ in terms of p and the inverses of q and r modulo p. As corollaries, he deduced that: Beiter's conjecture is true if q or r is equal to $\pm 1, \pm 2$ modulo p; we have $A(pqr) \leq p - \lceil p/4 \rceil$; and $A^+(pqr) - A^-(pqr) \leq p$, in particular either

$A^+(pqr) \le (p-1)/2$ or $A^-(pqr) \ge -(p-1)/2$. Note that the first two corollaries improve the previous results of Beiter [21, 22]. Regarding the third, Bachman (2004) [11] also proved that for every odd prime number p there exist infinitely many ternary cyclotomic polynomials $\Phi_{pqr}(X)$, with $p < q < r$, such that $\mathcal{A}(pqr) = [-(p-1)/2, (p+1)/2] \cap \mathbb{Z}$, and similarly for the interval $[-(p+1)/2, (p-1)/2]$. Leher (2007) [88, p. 70] found a counterexample to Beiter's conjecture, that is, $A(17 \cdot 29 \cdot 41) = 10 > (17+1)/2$. Let $M(p) := \max_{p<q<r} A(p)$. For every odd prime p, Gallot and Moree (2009) [61] defined an effectively computable set of natural numbers $\mathcal{B}(p)$ such that if $\mathcal{B}(p)$ is nonempty then

$$M(p) \ge p - \min(\mathcal{B}(p)) > (p+1)/2,$$

and so Beiter's conjecture is false for p. Then, for $p \ge 11$ they showed that $\mathcal{B}(p)$ is nonempty and $\max(\mathcal{B}(p)) = (p-3)/2$. Moreover, for every $\varepsilon > 0$, they proved that

$$\left(\tfrac{2}{3} - \varepsilon\right) p \le M(p) \le \tfrac{3}{4} p, \tag{6}$$

for all sufficiently large p. In light of these results, they formulated the following:

Conjecture 3.2 (Corrected Beiter's conjecture)**.** *$M(p) \le \frac{2}{3}p$ for every prime p.*

Zhao and Zhang (2010) [138] gave a sufficient condition for the Corrected Beiter conjecture and proved it when $p = 7$. (Note that for $p = 7$ the Corrected Beiter Conjecture is equivalent to the original Beiter Conjecture.) Moree and Roşu (2012) [108] showed that for each odd integer $\ell \ge 1$ there exist infinitely many odd primes $p < q < r$ such that

$$\mathcal{A}(pqr) = [-(p-\ell-2)/2, (p+\ell+2)/2] \cap \mathbb{Z}.$$

This provides a family of cyclotomic polynomials that contradict the Beiter conjecture and have the largest coefficient range possible. Bzdęga (2010) [27] improved Bachman's bounds [10] by giving the following theorem.

Theorem 3.2. *Let $p < q < r$ be odd primes and let q' and r' be the inverses of q and r modulo p, respectively. Then*

$$A^+(pqr) \le \min\{2\alpha + \beta, p - \beta\}, \quad -A^-(pqr) \le \min\{p + 2\alpha - \beta, \beta\},$$

$$A(pqr) \le \min\{2\alpha + \beta^*, p - \beta^*\},$$

where $\alpha := \min\{q', r', p-q', p-r'\}$, β is the inverse of αqr modulo p, and $\beta^* := \min\{\beta, p-\beta\}$.

As an application of Theorem 3.2, Bzdęga proved a density result showing that the Corrected Beiter conjecture holds for at least $25/27 + O(1/p)$ of all the ternary cyclotomic polynomials with the smallest prime factor dividing their order equal to p. He also proved that for these polynomials the average value of $A(pqr)$ does not exceed $(p+1)/2$. Moreover, for every prime $p \ge 13$, he provided some new classes of ternary cyclotomic polynomials $\Phi_{pqr}(X)$ for which the set of coefficients is very small. Luca, Moree, Osburn, Saad Eddin, and Sedunova (2019) [93], using Theorem 3.2 and some analytic estimates for constrained ternary integers that they developed, showed that the relative density of ternary integers for which the correct Sister Beiter conjecture holds true is at least $25/27$.

Gallot, Moree, and Wilms (2011) [63] initiated the study of

$$M(p,q) := \max\{A(pqr) : r > q\}.$$

They remarked that $M(p,q)$ can be effectively computed for any given odd primes $p < q$. For $p = 3, 5, 7, 11, 13, 19$, they proved that the set $\mathcal{Q}_p$ of primes q with $M(p,q) = M(p)$ has a subset of positive density, which they determined, and they also conjectured the value of the natural density of $\mathcal{Q}_p$. Moreover, they computed or bound $M(p,q)$ for p and q satisfying certain conditions, and they posed several problems regarding $M(p,q)$ [63, Section 11]. Cobeli, Gallot, Moree, and Zaharescu (2013) [41], using techniques from the study of the distribution of modular inverses, in particular bounds on Kloosterman sums, improved the lower bound in (6) to

$$M(p) > \tfrac{2}{3}p - 3p^{3/4}\log p,$$

for every prime p, and

$$M(p) > \tfrac{2}{3}p - Cp^{1/2},$$

for infinitely many primes p, where $C > 0$ is a constant. Moreover, they proved that

$$\liminf_{x\to+\infty} \frac{\#\{q : p < q \le x,\ M(p,q) > (p+1)/2\}}{\#\{p : p \le x\}} \ge \frac{\#\mathcal{B}(p)}{p-1}.$$

Duda (2014) [47] put $M_{q'}(p) := \max\{M(p,q) : q \equiv q' \pmod p\}$ and proved one of the main conjectures on $M(p,q)$ of Gallot, Moree, and Wilms [63, Conjecture 8], that is, for all distinct primes p and q' there exists $q_0 \equiv q' \pmod p$ such that for every prime $q \ge q_0$ with $q \equiv q' \pmod p$ we have $M(p,q) = M_{q'}(p)$. Also, he gave an effective method to compute $M_q(p)$, from which it follows an algorithm to effectively compute $M(p)$, since $M(p) = \max\{M_q(p) : q < p\}$.

Kosyak, Moree, Sofos, and Zhang (2021) [84] conjectured that every positive integer is of the form $A(n)$, for some ternary integer n. They proved this conjecture under a stronger form of Andrica's conjecture on prime gaps, that is, assuming that $p_{n+1} - p_n < \sqrt{p_n} + 1$ holds for every $n \ge 31$, where p_n denotes the nth prime number. Furthermore, they showed that almost all positive integers are of the form $A(n)$ where $n = pqr$ with $p < q < r$ primes is a ternary integer and $\#\mathcal{A}(n) = p + 1$ (which is the maximum possible value for this cardinality). A nice survey regarding these connections between cyclotomic polynomials and prime gaps was given by Moree (2021) [107].

3.2 Flatness

Recall that a cyclotomic polynomial $\Phi_n(X)$ is *flat* if $A(n) = 1$. Several families of flat ternary cyclotomic polynomials have been constructed, but a complete classification is still not known. Beiter (1978) [23] characterized the primes $r > q > 3$ such that $\Phi_{3qr}(X)$ is flat. In particular, there are infinitely many such primes. Bachman (2006) [12] proved that if $p \ge 5$, $q \equiv -1 \pmod p$, and $r \equiv 1 \pmod{pq}$ then $\Phi_{pqr}(X)$ is flat. Note that, for every prime $p \ge 5$, the existence of infinitely many primes q and r satisfying the aforementioned congruences is guaranteed by Dirichlet's theorem on primes in arithmetic progressions. Flanagan (2007) [58] improved Bachman's result by relaxing the congruences to $q \equiv \pm 1 \pmod p$ and $r \equiv \pm 1 \pmod{pq}$. Kaplan (2007) [77] used Lemma 3.1 to show that last congruence suffices, that is, the following holds:

Theorem 3.3. *$\Phi_{pqr}(X)$ is flat for all primes $p < q < r$ with $r \equiv \pm 1 \pmod{pq}$.*

Luca, Moree, Osburn, Saad Eddin, and Sedunova (2019) [93] proved some asymptotic formulas for ternary integers that, together with Theorem 3.3, yield that for every sufficiently large $N > 1$ there are at least $CN/\log N$ ternary integers $n \leq N$ such that $\Phi_n(X)$ is flat, where $C := 1.195\ldots$ is an explicit constant.

Ji (2010) [72] considered odd primes $p < q < r$ such that $2r \equiv \pm 1 \pmod{pq}$ and showed that in such a case $\Phi_{pqr}(X)$ is flat if and only if $p = 3$ and $q \equiv 1 \pmod 3$. For $a \in \{3, 4, 5\}$, Zhang (2017) [132] gave similar characterizations for the odd primes such that $ar \equiv \pm 1 \pmod{pq}$ and $\Phi_{pqr}(X)$ is flat (see also [137] for a weaker result for the case $a = 4$). For $a \in \{6, 7\}$, Zhang (2020, 2021) [135, 136] characterized the odd primes such that $q \equiv \pm 1 \pmod p$, $ar \equiv \pm 1 \pmod{pq}$, and $\Phi_{pqr}(X)$ is flat. Zhang (2017) [133] also showed that if $p \equiv 1 \pmod w$, $q \equiv 1 \pmod{pw}$, and $r \equiv w \pmod{pq}$, for some integer $w \geq 2$, then $A^+(pqr) = 1$. (See also the unpublished work of Elder (2012) [50].) Furthermore, for $q \not\equiv 1 \pmod p$ and $r \equiv -2 \pmod{pq}$, Zhang (2014) [130] constructed an explicit j such that $a_{pqr}(j) = -2$, so that $\Phi_{pqr}(X)$ is not flat. Regarding nonflat ternary cyclotomic polynomials with small heights, Zhang (2017) [131] showed that for every prime $p \equiv 1 \pmod 3$ there exist infinitely many q and r such that $A(pqr) = 3$.

3.3 Jump one property

Gallot and Moree (2009) [60] proved that neighboring coefficients of ternary cyclotomic polynomials differ by at most one. They called this property *jump one property.*

Theorem 3.4 (Jump one property)**.** *Let n be a ternary integer. Then*

$$|a_n(j) - a_n(j-1)| \leq 1$$

for every integer $j \geq 1$.

Corollary 3.1. *Let n be a ternary integer. Then $\mathcal{A}(n)$ is a set of consecutive integers.*

Gallot and Moree used the *jump one property* to give a different proof of Bachman's result [11] on ternary polynomials with optimally large set of coefficients. Their proof of the jump one property makes use of Kaplan's lemma. Previously, Leher (2007) [88, Theorem 57] proved the bound $|a_n(j) - a_n(j-1)| \leq 4$ using methods from the theory of numerical semigroups. A different proof of the jump one property was given by Bzdęga (2010) [27]. Furthermore, for every ternary integer n, Bzdęga (2014) [31] gave a characterization of the positive integers j such that $|a_n(j) - a_n(j-1)| = 1$. A coefficient $a_n(j)$ is *jumping up*, respectively *jumping down*, if $a_n(j) = a_n(j-1) + 1$, respectively $a_n(j) = a_n(j-1) - 1$. Since cyclotomic polynomials are palindromic, the number of jumping up coefficients is equal to the number of jumping down coefficients. Let J_n denote such number. Bzdęga [31] proved that $J_n > n^{1/3}$ for all ternary integers n. As a corollary, $\theta_n > n^{1/3}$. Also, he showed that Schinzel Hypothesis H implies that for every $\varepsilon > 0$ we have $J_n < 10n^{1/3+\varepsilon}$ for infinitely many ternary integers n. Camburu, Ciolan, Luca, Moree, and Shparlinski (2016) [37] gave an unconditional proof that $J_n < n^{7/8+\varepsilon}$ for infinitely many ternary integers n.

4 Higher order cyclotomic polynomials

There are few specific results regarding cyclotomic polynomials of order greater than three. Bloom (1968) [25] proved that, for odd prime numbers $p < q < r < s$, it holds $A(pqrs) \leq p(p-1)(pq-1)$. Kaplan (2010) [79] constructed the first infinite family of flat cyclotomic polynomials of order four. Precisely, he proved that $\Phi_{3\cdot 5\cdot 31\cdot s}(X)$ is flat for every prime number $s \equiv -1 \pmod{465}$. Also, he suggested that all flat cyclotomic polynomials $\Phi_{pqrs}(X)$ satisfy $q \equiv -1 \pmod{p}$, $r \equiv \pm 1 \pmod{pq}$, and $s \equiv \pm 1 \pmod{pqr}$. Furthermore, Bzdęga (2012) [28] proved the upper bounds

$$A(pqrs) \leq \frac{3}{4}p^3 q, \quad A(pqrst) \leq \frac{135}{512}p^7 q^3 r, \quad A(pqrstu) \leq \frac{18225}{262144}p^{15} q^7 r^3 s,$$

for all odd prime numbers $p < q < r < s < t < u$.

5 Height of cyclotomic polynomials

5.1 Asymptotic bounds on $A(n)$

Schur (1931)[2] was the first to prove that the coefficients of cyclotomic polynomials can be arbitrarily large, that is, $\sup_{n\geq 1} A(n) = +\infty$. E. Lehmer (1936) [90] presented Schur's proof and proved the stronger result that $A(n)$ is unbounded also when n is restricted to ternary integers. Erdős (1946) [52] proved that $A(n) > \exp(C(\log n)^{4/3})$ for infinitely many positive integers n, for some constant $C > 0$. His proof rests on a lower bound for the maximum of $|\Phi_n(X)|$ on the unit circle, and the simple consideration that $|\Phi_n(z)| \leq nA(n)$ for every $z \in \mathbb{C}$ with $|z| \leq 1$. This is essentially the main technique that has then been used to prove lower bounds for $A(n)$ [35, 53, 54, 81, 94, 95, 97, 124]. Furthermore, Erdős suggested that[3] $A(n) > \exp(n^{C/\log\log n})$ for infinitely many positive integers n, for some constant $C > 0$, and claimed that this is the best possible upper bound. Bateman (1949) [18] gave a short proof that, for every $\varepsilon > 0$, it holds $A(n) < \exp(n^{(1+\varepsilon)\log 2/\log\log n})$ for all sufficiently large integers n. Hence, the lower bound suggested by Erdős, if true, is indeed the best possible. Then Erdős (1949) [53] proved that in fact $A(n) > \exp(n^{C/\log\log n})$ for infinitely many positive integers n, for some constant $C > 0$, by showing that $\max_{|z|=1} |\Phi_n(z)| > \exp(n^{C/\log\log n})$ for infinitely many positive integers n. His proof of this last fact is quite involved. Later, Erdős (1957) [54] found a simpler proof of the fact that $\max_{x\in(0,1)} |\Phi_n(x)| > \exp(n^{C/\log\log n})$ for infinitely many positive integers n, which again implies the lower bound on $A(n)$. He conjectured that one can take every positive constant $C < \log 2$, and so Bateman's result is the best possible. This conjecture was settled by Vaughan (1974) [124], who proved that actually $C = \log 2$ is admissible (see also [35] for an alternative proof).

In summary, the maximal order of $A(n)$ is given by the following theorem [18, 124].

Theorem 5.1 (Bateman–Vaughan)**.** *On the one hand, for every $\varepsilon > 0$, we have*

$$A(n) < \exp\bigl(n^{(\log 2+\varepsilon)/\log\log n}\bigr)$$

[2] Unpublished letter to Landau, see [90].

[3] The following formula was printed incorrectly in Erdős' paper [52], see [18].

for all sufficiently large positive integers n. On the other hand, we have

$$A(n) > \exp\bigl(n^{\log 2/\log\log n}\bigr)$$

for infinitely many positive integers n.

Maier (1990, 1996) [94, 96] proved that $n^{f(n)} < A(n) < n^{g(n)}$ for almost all positive integers, where f and g are arbitrary functions such that $f(n) \to 0$ and $g(n) \to +\infty$ as $n \to +\infty$. Furthermore, Maier (1993) [95] proved that for any constant $C > 0$ the inequality $A(n) \geq n^C$ holds on a set of positive lower density. It is well known that $\omega(n) \sim \log\log n$ as $n \to +\infty$ over a set of natural density 1, where $\omega(n)$ is the number of distinct prime factors of n (see, e.g., [121, Ch. III.3]). For every $C > 1$, let $\mathcal{E}_C$ be the set of squarefree integers n such that $\omega(n) \geq C \log\log n$. Maier (2001) [97] proved that for every $C > 2/\log 2$ and $\varepsilon > 0$ the inequality $A(n) > \exp((\log n)^{(C\log 2)/2-\varepsilon})$ holds for almost all $n \in \mathcal{E}_C$. Later, Konyagin, Maier, and Wirsing (2004) [81] showed that, actually, such lower bound for $A(n)$ holds for all positive integers with $\omega(n) \geq C \log\log n$. The key part of their proof is a strong upper bound on the third moment of the function $\log|\Phi_n(z)|$ over the unit circle.

5.2 Bounds on $A(n)$ in terms of prime factors

Felsch and Schmidt (1968) [56] and, independently, Justin (1969) [76] proved that $A(n)$ has an upper bound that does not depend on the two largest prime factors of n. Let $n = p_1 \cdots p_k$, where $p_1 < \cdots < p_k$ are odd prime numbers and $k \geq 3$. Bateman, Pomerance, and Vaughan (1984) [19] proved that $A(n) \leq M(n)$, where $M(n) := \prod_{j=1}^{k-2} p_j^{2^{k-j-1}-1}$ (see also [98] for an upper bound of a similar form for $|\Phi_n(X)|$ on the unit circle). Furthermore, they conjectured that $M(n) \leq \varphi(n)^{2^{k-1}/k-1}$. This conjecture was proved by Bzdęga (2012) [28], who also proved that $A(n) \leq C_k M(n)$, where $(C_k)_{k\geq 3}$ is a sequence such that $C_k^{2^{-k}}$ converges to a constant less than 0.9541, as $k \to +\infty$. In the opposite direction, Bzdęga (2016) [33] proved that for every $k \geq 3$ and $\varepsilon > 0$ there exists n such that $A(n) > (c_k - \varepsilon)M(n)$, where $(c_k)_{k\geq 3}$ is a sequence such that $c_k^{2^{-k}}$ converges to a constant that is about 0.71, as $k \to +\infty$. In particular, this last result implies that in the upper bound on $A(n)$ the product $M(n)$ is optimal, which means that, in a precise sense, it cannot be replaced by a smaller product of $p_1, \ldots, p_{k-2}$. Furthermore, Bzdęga (2017) [34] proved several asymptotic bounds for quantities such as $A(n)$, the sum of the absolute values of the coefficients of $\Phi_n(X)$, the sum of the squares of the coefficients of $\Phi_n(X)$, and the maximum of the absolute value of $\Phi_n(X)$ on the unit circle, as $p_1 \to +\infty$ and k is fixed.

5.3 The dual function $a(j)$

For every positive integer j define

$$a(j) := \max_{n\geq 1} |a_n(j)|. \tag{7}$$

Thus $a(j)$ is somehow a dual version of $A(n)$. From (3) it follows that $a_{pqn}(j) = a_n(j)$ for all prime numbers $p > q > j$ not dividing n. Hence, in (7) the maximum can be replaced by a limit superior. Erdős and Vaughan (1974) [55] proved that $\log a(j) <$

$2\tau^{1/2}j^{1/2} + Cj^{3/8}$ for all positive integers j, where $\tau := \prod_p \left(1 - \frac{2}{p(p+1)}\right)$ and $C > 0$ is a constant, and conjectured that $\log a(j) = o(j^{1/2})$ as $j \to +\infty$. Also, they showed that $\log a(j) \gg j^{1/2}/(\log j)^{1/2}$ for all sufficiently large integers j. Vaughan (1974) [124] proved that $\log a(j) \gg j^{1/2}/(\log j)^{1/4}$ for infinitely many positive integers j. Montgomery and Vaughan (1985) [104] determined the order of magnitude of $\log a(j)$ by proving that that $\log a(j) \asymp j^{1/2}/(\log j)^{1/4}$ for all sufficiently large integers j. Finally, Bachman (1993) [9] proved the asymptotic formula $\log a(j) \sim Cj^{1/2}/(\log j)^{1/4}$, where $C > 0$ is a constant given by a quite complicate expression.

6 Maximum gap

Al-Kateeb, Ambrosino, Hong, and Lee (2021) [2] proved that $G(pm) = \varphi(m)$ for every prime number p and for every squarefree positive integer m with $p > m$. This was previously numerically observed by Ambrosino, Hong, and Lee (2017) [4, 5]. The proof is based on a new divisibility property regarding a partition of $\Phi_{pm}(X)$ into "blocks" (see also [1, 3]). Furthermore, Al-Kateeb, Ambrosino, Hong, and Lee [2] conjectured that $G(pm) \leq \varphi(m)$ for every prime number p and for every squarefree positive integer m with $p < m$.

7 The set of coefficients

Suzuki (1987) [120] gave a short proof that every integer appears as the coefficient of some cyclotomic polynomial. (Note that now this follows, for example, from Bachman's result on ternary cyclotomic polynomials with an optimally large set of coefficients [11]). Ji and Li (2008) [73] proved that, for each fixed prime power p^ℓ, every integer appears as the coefficient of a cyclotomic polynomial of the form $\Phi_{p^\ell n}(X)$. Ji, Li, and Moree (2009) [74] generalized this result by showing that, for each fixed positive integer m, every integer appears as the coefficient of a cyclotomic polynomial of the form $\Phi_{mn}(X)$. Then Fintzen (2011) [57] determined the set $\{a_n(j) : n \equiv a \pmod{d},\ j \equiv b \pmod{f}\}$ for any given nonnegative integers $a < d$ and $b < f$ (see also [129]). In particular, she showed that this set is either $\mathbb{Z}$ or $\{0\}$.

Recall that $\mathcal{A}(n) := \{a_n(j) : 0 \leq j \leq \varphi(n)\}$ is the set of coefficients of $\Phi_n(X)$. Kaplan (2007, 2010) [77, Theorems 2 and 3][79, Theorem 4] proved[4] the following two results regarding a kind of periodicity of $\mathcal{A}(n)$.

Theorem 7.1. *Let n be a binary integer, and let p and q be prime number greater than the largest prime factor of n and such that $p \equiv \pm q \pmod{n}$. Then $\mathcal{A}(pn) = \mathcal{A}(qn)$.*

Theorem 7.2. *Let n be a positive integer, and let p and q be prime numbers greater than n and satisfying $p \equiv q \pmod{n}$. Then $\mathcal{A}(pn) = \mathcal{A}(qn)$.*

[4] [77, Theorems 2 and 3] are stated with $A(n)$ in place of $\mathcal{A}(n)$, but their proofs show that the result do indeed hold with $\mathcal{A}(n)$.

8 Formulas for the coefficients

Let $n > 1$ be an integer. From (3) it follows that

$$\Phi_n(X) = \prod_{d=1}^{\infty} \left(1 - X^d\right)^{\mu(n/d)}, \tag{8}$$

with the convention that $\mu(x) = 0$ if x is not an integer. Therefore, each coefficient $a_n(j)$ depends only on the values $\mu(n/d)$, with d a positive integer not exceeding j, and using (8) one can obtain formulas for $a_n(j)$ for each fixed j. For instance, we have

$$\begin{aligned} a_n(1) &= -\mu(n), \\ a_n(2) &= \tfrac{1}{2}\mu(n)^2 - \tfrac{1}{2}\mu(n) - \mu\left(\tfrac{n}{2}\right), \\ a_n(3) &= \tfrac{1}{2}\mu(n)^2 - \tfrac{1}{2}\mu(n) + \mu(n)\mu\left(\tfrac{n}{2}\right) - \mu\left(\tfrac{n}{3}\right). \end{aligned}$$

In general, Möller (1970) [102] proved that

$$a_n(j) = \sum_{\substack{\lambda_1 + 2\lambda_2 + \cdots + j\lambda_j = j \\ \lambda_1, \ldots, \lambda_j \geq 0}} \prod_{d=1}^{j} (-1)^{\lambda_d} \binom{\mu(n/d)}{\lambda_d},$$

for every integer $j \geq 0$ (see [62, Lemma 4] for a short proof).

Kazandzidis (1963) [80] and D. H. Lehmer (1966) [89] noted that, by Newton's identities for the symmetric elementary polynomials in terms of power sums, we have

$$a_n(j) = \sum_{\substack{\lambda_1 + 2\lambda_2 + \cdots + j\lambda_j = j \\ \lambda_1, \ldots, \lambda_j \geq 0}} \prod_{t=1}^{j} \frac{(-c_n(t)/t)^{\lambda_t}}{\lambda_t!},$$

where

$$c_n(t) := \sum_{\substack{1 \leq k \leq n \\ \gcd(n,k) = 1}} e^{2\pi \mathbf{i} k t/n} = \varphi(n) \frac{\mu(n/\gcd(n,t))}{\varphi(n/\gcd(n,t))},$$

is a *Ramanujan's sum* and the second equality is due to Hölder (1936) [69]. Deaconescu and Sándor (1987) [43] (see also [116, pp. 258–259]) gave another formula for $a_n(j)$ in terms of a determinant involving Ramanujan's sums. Furthermore, Eaton (1939) [49] proved a formula for $a_n(j)$ in terms of a sum having each addend either equal to -1 or $+1$ depending on a quite involved rule.

Grytczuk and Tropak (1991) [66] provided another method to compute $a_n(j)$, which makes use of the recurrence

$$a_n(j) = -\frac{\mu(n)}{j} \sum_{i=0}^{j-1} a_n(i)\, \mu(\gcd(n, j-i))\, \varphi(\gcd(n, j-i)), \qquad \text{for } j > 0,$$

with $a_n(0) = 1$. By using this method, they found for $m = \pm 2, \ldots, \pm 9$, and 10 the minimal positive integer j for which there exists a positive integer n such that $a_n(j) = m$.

Herrera-Poyatos and Moree (2021) [68] wrote a survey on formulas for $a_n(j)$ involving Bernoulli numbers, Stirling numbers, and Ramanujan's sums. Also, they introduced a new uniform approach that makes possible to provide shorter proofs for some of such formulas and also to derive new ones.

9 Miscellaneous results

Carlitz (1967) [39] proved some asymptotic formulas involving the sum of squares of the coefficients of $\Phi_n(X)$. Endo (1974) [51] proved that 7 is the minimal nonnegative integer j such that $|a_n(j)| > 1$ for some positive integer n. Dresden (2004) [46] proved that for every $n \geq 3$ the middle coefficient of $\Phi_n(X)$ is either 0, and in such a case n is a power of 2, or an odd integer. Dunand (2012) [48] studied the coefficients of the inverse of $\Phi_m(X)$ modulo $\Phi_n(X)$, where m and n are distinct divisors of pq, with $p < q$ primes, and discussed an application to torus-based cryptography. Musiker and Reiner (2014) [111] gave an interpretation of $a_n(j)$ as the torsion order in the homology of certain simplicial complexes. An alternative proof of this results was given by Meshulam (2012) [100]. Chu (2021) [40] gave necessary conditions on n so that the powers of positive, respectively negative, coefficients of $\Phi_n(X)$ are in arithmetic progression. For all integers $j, v \geq 0$, let

$$\overline{a}(j) := \lim_{N \to +\infty} \frac{1}{N} \sum_{n \leq N} a_n(j)$$

be the average value of the jth coefficient of the cyclotomic polynomials, and let

$$\delta(j, v) := \lim_{N \to +\infty} \frac{1}{N} \#\{n \leq N : a_n(j) = v\},$$

be the frequency that such coefficient is equal to v. Möller (1970) [102] proved that $\overline{a}(j) = \frac{6}{\pi^2} e_j$ for every integer $j \geq 1$, where $e_j > 0$ is a rational number. Gallot, Moree, and Hommersom (2011) [62] derived explicit formulas for $\overline{a}(j)$ and $\delta(j, v)$. Also, they verified that $f_j := e_j j \prod_{p \leq j} (p+1)$ is an integer for every positive integer $j \leq 100$, and asked whether it is true in general. Gong (2009) [65] proved that indeed every f_j is an integer, and also showed that, for every integer m, we have that $m \mid f_j$ for every sufficiently large j.

10 Algorithms and numerical data

Arnold and Monagan (2011) [8] presented three algorithms for computing the coefficients of the nth cyclotomic polynomial, and wrote a fast implementation using machine-precision arithmetic. The first algorithm computes $\Phi_n(X)$ by a series of polynomial divisions using Lemma 1.1's (ii). This method is well known [26], but Arnold and Monagan optimized the polynomial division by way of the discrete Fast Fourier Transform. The second algorithm computes $\Phi_n(X)$ as a quotient of sparse power series using (3). In such algorithm, $\Phi_n(X)$ is treated as a truncated power series. Multiplication of a truncated power series by $X^d - 1$ is easy, and division by $X^d - 1$ is equivalent to multiplication by the power series $-\sum_{j=0}^{\infty} X^{dj}$. This algorithm was further improved in a subsequent work [7]. The third algorithm, which they called the "big prime algorithm", generates the terms of $\Phi_n(X)$ sequentially, in a manner which reduces the memory cost.

With their implementation, Arnold and Monagan produced a large amount of data on the coefficients of $\Phi_n(X)$ for n in the range of billions [6]. For instance, they found the minimal positive integer n such that $A(n)$ is greater than n, n^2, n^3, and n^4, respectively. Also, they computed $A(n)$ when n is equal to the product of the first 9 odd prime numbers. (Partial computations on the cases of n equal to the product of the first 7 and 8 odd prime numbers were previously done by Koshiba (1998, 2000) [82, 83].)

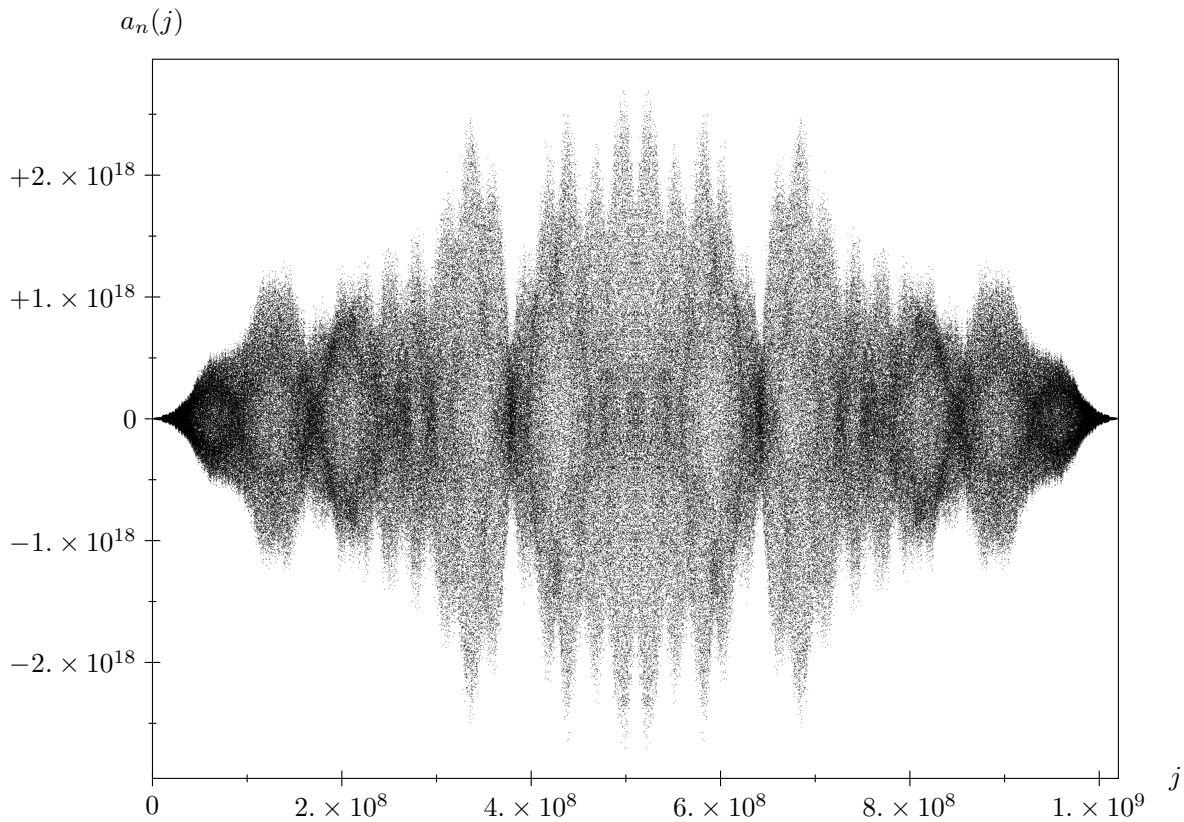

Figure 1: A plot of the coefficients of $\Phi_n(X)$ for $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$. The $\varphi(n) + 1 = 1,021,870,081$ coefficients were computed using the program `SPS4_64` of Arnold and Monagan [6]. Then the plot was produced by selecting a random sample of $500,000$ coefficients.

Other numerical data on the coefficients of the cyclotomic polynomial can be found on the Online Encyclopedia of Integer Sequences [117]. See for instance sequences `A117223`, `A117318`, `A138474`, and `A138475` of Noe.

11 Relatives of cyclotomic polynomials

In this section we collect results regarding the coefficients of polynomials that are closely related to cyclotomic polynomials.

11.1 Inverse cyclotomic polynomials

Let n be a positive integer. The *nth inverse cyclotomic polynomial* $\Psi_n(X)$ is defined as the monic polynomial whose roots are exactly the nonprimitive nth roots of unity, that is,

$$\Psi_n(X) := \prod_{\substack{1 \le k \le n \\ \gcd(n,k) > 1}} \left(X - e^{2\pi \mathbf{i} k/n}\right) = \frac{X^n - 1}{\Phi_n(X)}. \tag{9}$$

Note that $\Phi_n(X)$ has degree $n-\varphi(n)$. From (2) and (9) it follows that

$$\Psi_n(X) = \prod_{\substack{d \mid n \\ d > 1}} \Phi_d(X).$$

In particular, $\Psi_n(X)$ has integer coefficients. Moreover, from (9) we get that

$$\frac{1}{\Phi_n(X)} = \frac{\Psi_n(X)}{X^n - 1} = -\Psi_n(X) \sum_{j=0}^{\infty} X^{nj}.$$

Thus, the Taylor coefficients of $1/\Phi_n(X)$ are purely periodic, and the period consists of the $n-\varphi(n)+1$ coefficients of $-\Phi_n(X)$ followed by $\varphi(n)-1$ zeros. The next lemma collects some basic identities, which follows easily from Lemma 1.1 and (9).

Lemma 11.1. *For every positive integer n and every prime number p, we have that:*

(i) $\Psi_{pn}(X) = \Psi_n(X^p)$ *if* $p \mid n$;

(ii) $\Psi_{pn}(X) = \Phi_n(X)\Psi_n(X^p)$ *if* $p \nmid n$;

(iii) $\Psi_{2n}(X) = (-1)^{\varphi(n)}(1-X^n)\Psi_n(-X)$ *if* $2 \nmid n$;

(iv) $\Psi_n(X) = \Psi_{\mathrm{rad}(n)}(X^{n/\mathrm{rad}(n)})$;

(v) $\Psi_n(1/X) = -X^{-(n-\varphi(n))}\Psi_n(X)$ *if* $n > 1$.

Similarly to cyclotomic polynomials, in light of Lemma 11.1's (iii) and (iv), for the purpose of studying the coefficients of the inverse cyclotomic polynomial $\Psi_n(X)$ it suffices to consider only odd squarefree integers n. For a squarefree positive integer n, the inverse cyclotomic polynomial $\Psi_n(X)$ is *binary*, *ternary*, ... if the number of prime factors of n is 2, 3, ... The *order* of $\Psi_n(X)$ is the number of prime factors of n. It is easy to check that $\Psi_1(X) = 1$, $\Psi_p(X) = X - 1$, and

$$\Psi_{pq}(X) = X^{p+q-1} + X^{p+q-2} + \cdots + X^q - X^{p-1} - X^{p-2} - \cdots - 1$$

for all prime numbers $p < q$. Hence, the simplest nontrivial case in the study of the coefficients of $\Psi_n(X)$ occurs for ternary n.

Let $C(n)$ denote the height of $\Psi_n(X)$. Moree (2009) [105] proved that

$$C(pqr) \leq \left\lfloor \frac{(p-1)(q-1)}{r} \right\rfloor + 1 \leq p-1,$$

for all odd primes $p < q < r$. Also, he showed that $C(pqr) = p-1$ if and only if $q \equiv r \equiv \pm 1 \pmod{p}$ and $r < \frac{p-1}{p-2}(q-1)$. Furthermore, he provided several results on flat inverse cyclotomic polynomials. For instance, he showed that $\Psi_{15r}(X)$ and $\Psi_{21r}(X)$ are flat, for every prime p, and that $\Psi_{pqr}(X)$ is flat for all primes $p < q$ and $r > (p-1)(q-1)$. Furthermore, he proved that every integer appears as the coefficient of some inverse cyclotomic polynomial. Bzdęga (2014) [32] proved a formula for $C(pqr)$ in the case in which $r = \alpha p + \beta q \leq \varphi(pq)$ for some positive integers α, β. Using such formula, he gave necessary and sufficient conditions for $\Psi_{pqr}(X)$ being flat in such a case. Hong, Lee, Lee, and Park (2012) [70] proved that $G(\Psi_{pqr}) = 2qr - \deg(\Psi_{pqr})$ for all odd primes $p < q < r$ such that $q > 4(p-1)$ or $r > p^2$. Also, they gave lower and upper bound for $G(\Psi_{pqr})$ for general Ψ_{pqr}. In general, many papers regarding the coefficients of cyclotomic polynomials also provide related results for the coefficients of inverse cyclotomic polynomials [7, 8, 28, 37, 57, 60, 62, 68, 93].

11.2 Divisors of $X^n - 1$

A natural generalization of the study of the coefficients of $\Phi_n(X)$ is the study of the coefficients of divisors of $X^n - 1$. Note that, in light of (2) and the irreducibility of cyclotomic polynomials, $X^n - 1$ has $2^{\tau(n)}$ monic divisors in $\mathbb{Z}[X]$, where $\tau(n)$ is the number of (positive) divisors of n, which are given by products of distinct cyclotomic polynomials $\Phi_d(X)$ with d a divisor of n. Let $B(n)$ be the maximum height of the monic divisors of $X^n - 1$. Justin (1969) [76] showed that $B(n)$ has an upper bound that is independent from the largest prime factor of n. Pomerance and Ryan (2007) [114] proved that

$$\limsup_{n\to+\infty} \frac{\log\log B(n)}{\log n/\log\log n} = \log 3.$$

Furthermore, they showed that $B(pq) = p$ for all primes $p < q$, and that $B(n) = 1$ if and only if n is a prime power. Kaplan (2009) [78] proved that $B(p^2q) = \min\{p^2, q\}$ for all distinct primes p and q, and that

$$\tfrac{1}{3}(3p^2q - p^3 + 7p - 6) \le B(pqr) \le p^2q^2,$$

for all primes $p < q < r$. Moreover, letting $n = p_1^{e_1}\cdots p_k^{e_k}$, where $p_1 < \cdots < p_k$ are prime numbers, $e_1, \ldots, e_k$ are positive integers, and $k \ge 2$. Kaplan proved the upper bound $B(n) < \prod_{j=1}^{k-1} p_i^{4\cdot 3^{k-2}E-e_j}$, where $E := \prod_{j=1}^{k} e_j$. Bzdęga (2012) [28] showed that $B(n) < (C + o(1))^{3^k} n^{(3^k-1)/(2k)-1}$, as $k \to +\infty$, where $C < 0.9541$ is an effectively computable constant. Zhang (2019) [134] improved Kaplan's bound to $B(n) < \left(\frac{2}{5}\right)^{\prod_{j=2}^{k} e_j} p_i^{4\cdot 3^{k-2}E-e_j}$. Ryan, Ward, and Ward (2010) [115] proved that $B(n) \ge \min\{u, v\}$ whenever $n = uv$, where u and v are coprime positive integers. In particular, this implies that $B(n) \ge \min\{p_1^{e_1}, \cdots, p_k^{e_k}\}$. Furthermore, they made several conjectures on $B(n)$, for n having two, three, or four prime factors, based on extensive numerical computations. Some of these conjectures were proved by Wang (2015) [126]. In particular, he showed that for all odd primes $p < q < r$ and every positive integer b we have that: $B(pq^b)$ is divisible by p, $B(2q^b) = 2$, if $b \ge 3$ then $B(pq^b) > p$, and if $q \equiv \pm r \pmod p$ and $b \le 5$ then $B(pq^b) = B(pr^b)$. Thompson (2011) [123] proved that $B(n) \le n^{\tau(n)f(n)}$ for almost all positive integers n, where $f(n)$ is any function such that $f(n) \to +\infty$ as $n \to +\infty$. Decker and Moree (2013) [45] (see also the extended version [44]) determined the set of coefficients of each of the 64 divisors of $X^{p^2q} - 1$, where p and q are distinct primes. In particular, their result shows that for most of the divisors the set of coefficients consists of consecutive integers. Moreover, they proved that if f_e is the number of flat divisors of $X^{p^eq} - 1$, for each integer $e \ge 1$, then $f_{e+1} \ge 2f_e + 2^{e+2} - 1$.

For each integer $r \ge 1$, let $B(r, n)$ be the maximum of the absolute value of the coefficient of X^r in $f(X)$, as $f(X)$ ranges over the monic divisors of $X^n - 1$. Somu (2016) [118] gave upper and lower bounds for $B(r, n)$ that imply

$$\limsup_{n\to+\infty} \frac{\log B(r, n)}{\log n/\log\log n} = r\log 2.$$

In the same work, Somu proved that if ℓ and m are positive integers, then there exist a positive integer n and a monic divisor $f(X)$ of $X^n - 1$ having exactly m irreducible factors such that each integers in $[-\ell, \ell]$ appears among the coefficients of $f(X)$. Moreover, he showed that for all integers $c_1, \ldots, c_r$ there exist a positive integer n and a divisor $f(X) = \sum_{j=1}^{\deg(f)} d_jX^j$, with $f_i \in \mathbb{Z}$, of $X^n - 1$ such that $d_i = c_i$ for $i = 1, \ldots, r$. Later Somu (2017) [119] proved that the set of such n has positive natural density.

11.3 Inclusion-exclusion polynomials

Inclusion-exclusion polynomials were introduced by Bachman (2010) [13] as a kind of combinatorial generalization of cyclotomic polynomials. Let bold letters $\boldsymbol{n}, \boldsymbol{d}, \ldots$ denote finite sets of pairwise coprime integers greater than 1. Furthermore, for each $\boldsymbol{n} = \{n_1, \ldots, n_k\}$, where $n_1, \ldots, n_k > 1$ are pairwise coprime integers, put $\|\boldsymbol{n}\| := n_1 \cdots n_k$, $\mu(\boldsymbol{n}) := (-1)^k$, and $\varphi(\boldsymbol{n}) := \prod_{i=1}^{k}(n_i - 1)$. The $\boldsymbol{n}$*th inclusion-exclusion polinomial* is defined as

$$\Phi_{\boldsymbol{n}}(X) = \prod_{\boldsymbol{d} \subseteq \boldsymbol{n}} \left(X^{\|\boldsymbol{n}\|/\|\boldsymbol{d}\|} - 1\right)^{\mu(\boldsymbol{d})}. \tag{10}$$

Note the striking resemblance of (3) and (10). In particular, we have that

$$\Phi_{\{p_1,\ldots,p_k\}}(X) = \Phi_{p_1 \cdots p_k}(X),$$

for all prime numbers $p_1 < \cdots < p_k$.

Many results regarding cyclotomic polynomials can be generalized to inclusion-exclusion polynomials, and it might be even more natural to prove them directly for inclusion-exclusion polynomials [31, 37, 40, 47, 106]. Also, the $\boldsymbol{n}$*th inverse inclusion-exclusion polynomial*, defined by $\Psi_{\boldsymbol{n}}(X) := (X^{\|\boldsymbol{n}\|} - 1)/\Phi_{\boldsymbol{n}}(X)$, has been studied [32].

The following theorem summarizes the basic properties of inclusion-exclusion polynomials, including the fact that they are indeed polynomials [13].

Theorem 11.2. *For every $\boldsymbol{n} = \{n_1, \ldots, n_k\}$, where $n_1, \ldots, n_k > 1$ are pairwise coprime integers, we have that*

$$\Phi_{\boldsymbol{n}}(X) = \prod_{\omega}(X - \omega),$$

where ω runs over the $\|\boldsymbol{n}\|$th roots of unity satisfying $\omega^{\|\boldsymbol{n}\|/n_i} \neq 1$ for all $i = 1, \ldots, k$. Moreover, the degree of $\Phi_{\boldsymbol{n}}(X)$ is equal to $\varphi(\boldsymbol{n})$ and it holds

$$\Phi_{\boldsymbol{n}}(X) = \prod_{d} \Phi_d(X),$$

where d runs over the divisors of $\|\boldsymbol{n}\|$ such that $(d, n_i) > 1$ for every $i = 1, \ldots, k$. In particular, $\Phi_{\boldsymbol{n}}(X)$ has integer coefficients.

Let p, q, r, s be pairwise coprime integers greater than 1. Bachman (2010) [13] proved that the set of coefficients of every *ternary inclusion-exclusion polynomial* $\Phi_{\{p,q,r\}}(X)$ consists of consecutive integers and, assuming $p < q < r$, it depends only on the residue class of r modulo pq. Let $A(p, q, r)$ denote the height of $\Phi_{\{p,q,r\}}(X)$. Bachman and Moree (2011) [15] showed that, if $r \equiv \pm s \pmod{pq}$ and $r > \max\{p, q\} > s \geq 1$, then

$$A(p, q, s) \leq A(p, q, r) \leq A(p, q, s) + 1.$$

For every $\boldsymbol{n} = \{n_1, \ldots, n_k\}$, where $n_1 < \cdots < n_k$ are pairwise coprime integers greater than 1, let $A(\boldsymbol{n})$ be the height of $\Phi_{\boldsymbol{n}}(X)$ and put $M(\boldsymbol{n}) := \prod_{j=1}^{k-2} n_j^{2^{k-j-1}-1}$. Also, let D_k be the smallest real number for which the inequality $A(\boldsymbol{n}) \leq D_k M(\boldsymbol{n})$ holds for all sufficiently large n_1. Bzdęga (2013) [30] proved that $(C_1 + o(1))^{2^k} < D_k < (C_2 + o(1))^{2^k}$, as $k \to \infty$, where $C_1, C_2 > 0$ are constants, with $C_1 \approx 0.5496$ and $C_2 \approx 0.9541$. Furthermore, Liu (2014) [92] studied the polynomial obtained by restricting (10) to the sets $\boldsymbol{d}$ with at most two elements.

11.4 Unitary cyclotomic polynomials

Let n be a positive integer. A *unitary divisor* of n is a divisor d of n such that d and n/d are relatively prime. Moree and Tóth (2020) [109] defined the *nth unitary cyclotomic polynomial* as

$$\Phi_n^*(X) := \prod_{\substack{1 \le k \le n \\ \gcd^*(n,k)=1}} \left(X - e^{2\pi \mathbf{i} k/n}\right),$$

where $\gcd^*(n,k)$ denotes the maximum unitary divisor of n which is a divisor of k. It can be proved that $\Phi_n^*(X)$ has integer coefficients. Moreover, the following analogs of (2) and (3) holds:

$$X^n - 1 = \prod_{d \,||\, n} \Phi_d^*(X),$$

where $d \,||\, n$ means that d is a unitary divisor of n, and

$$\Phi_n^*(X) = \prod_{d \,||\, n} \left(X^{n/d} - 1\right)^{\mu^*(d)},$$

where $\mu^*(n) := (-1)^{\omega(n)}$. Every unitary cyclotomic polynomial can be written as an inclusion-exclusion polynomial, precisely $\Phi_n^*(X) = \Phi_{\{p_1^{e_1},\ldots,p_k^{e_k}\}}(X)$ for $n = p_1^{e_1} \cdots p_k^{e_k}$, where $p_1 < \cdots < p_k$ are prime numbers and $e_1, \ldots, e_k$ are positive integers. Furthermore, every unitary cyclotomic polynomial is equal to a product of cyclotomic polynomials:

$$\Phi_n^*(X) = \prod_{\substack{d \,|\, n \\ \mathrm{rad}(d) = \mathrm{rad}(n)}} \Phi_d(X).$$

These and other properties of unitary cyclotomic polynomials were proved by Moree and Tóth [109]. Jones, Kester, Martirosyan, Moree, Tóth, White, and Zhang (2020) [75] proved that, given any positive integer m, every integer appears as a coefficient of $\Phi_{mn}^*(X)$, for some positive integer n. Also, they showed the analog result for coefficients of the *inverse unitary cyclotomic polynomial* $\Psi_n^*(X) := (X^n - 1)/\Phi_n^*(X)$. Bachman (2021) [14] proved that, fixed three distinct odd primes p, q, r and $\varepsilon > 0$, for every sufficiently large positive integer a, depending only on ε, there exist positive integers b and c such that the the set of coefficients of $\Phi_{p^a q^b r^c}^*(X)$ contains all the integers in the interval $\left[-(\frac{1}{4} - \varepsilon)p^a, (\frac{1}{4} - \varepsilon)p^a\right]$. As a consequence, every integer appears as the coefficient of some ternary unitary cyclotomic polynomial. Furthermore, he provided an infinite family of ternary unitary cyclotomic polynomials $\Phi_{p^a q^b r^c}^*(X)$ whose sets of coefficients consist of all the integers in $[-(p^a - 1)/2, (p^a + 1)/2]$, and he pointed out that this interval is as large as possible.

References

[1] A. Al-Kateeb, *Structures and properties of cyclotomic polynomials*, ProQuest LLC, Ann Arbor, MI, 2016, Thesis (Ph.D.)–North Carolina State University.

[2] A. Al-Kateeb, M. Ambrosino, H. Hong, and E. Lee, *Maximum gap in cyclotomic polynomials*, J. Number Theory **229** (2021), 1–15.

[3] A. Al-Kateeb, H. Hong, and E. Lee, *Block structure of cyclotomic polynomials*, 2017, https://arxiv.org/abs/1704.04051.

[4] M. Ambrosino, *Maximum gap of (inverse) cyclotomic polynomials*, Ph.D. thesis, North Carolina State University, North Carolina, 2017.

[5] M. Ambrosino, H. Hong, and E. Lee, *Lower bounds for maximum gap in (inverse) cyclotomic polynomials*, 2017, https://arxiv.org/abs/1702.07650.

[6] A. Arnold and M. Monagan, *Cyclotomic Polynomials*, 2010, http://wayback.cecm.sfu.ca/~ada26/cyclotomic/.

[7] A. Arnold and M. Monagan, *A high-performance algorithm for calculating cyclotomic polynomials*, 2010, pp. 112–120.

[8] A. Arnold and M. Monagan, *Calculating cyclotomic polynomials*, Math. Comp. **80** (2011), no. 276, 2359–2379.

[9] G. Bachman, *On the coefficients of cyclotomic polynomials*, Mem. Amer. Math. Soc. **106** (1993), no. 510, vi+80.

[10] G. Bachman, *On the coefficients of ternary cyclotomic polynomials*, J. Number Theory **100** (2003), no. 1, 104–116.

[11] G. Bachman, *Ternary cyclotomic polynomials with an optimally large set of coefficients*, Proc. Amer. Math. Soc. **132** (2004), no. 7, 1943–1950.

[12] G. Bachman, *Flat cyclotomic polynomials of order three*, Bull. London Math. Soc. **38** (2006), no. 1, 53–60.

[13] G. Bachman, *On ternary inclusion-exclusion polynomials*, Integers **10** (2010), A48, 623–638.

[14] G. Bachman, *Coefficients of unitary cyclotomic polynomials of order three*, 2021, https://arxiv.org/abs/2111.08847.

[15] G. Bachman and P. Moree, *On a class of ternary inclusion-exclusion polynomials*, Integers **11** (2011), A8, 14.

[16] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), no. 4, 331–361.

[17] A. S. Bang, *Om Ligningen* $\varphi_n(x) = 0$, Nyt Tidss. for Math. **6** (1895), 6–12 (Danish).

[18] P. T. Bateman, *Note on the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **55** (1949), 1180–1181.

[19] 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. János Bolyai, vol. 34, North-Holland, Amsterdam, 1984, pp. 171–202.

[20] M. Beiter, *The midterm coefficient of the cyclotomic polynomial* $F_{pq}(x)$, Amer. Math. Monthly **71** (1964), no. 7, 769–770.

[21] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* $F_{pqr}(x)$, Amer. Math. Monthly **75** (1968), 370–372.

[22] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* F_{pqr}*. II*, Duke Math. J. **38** (1971), 591–594.

[23] M. Beiter, *Coefficients of the cyclotomic polynomial $F_{3qr}(x)$*, Fibonacci Quart. **16** (1978), no. 4, 302–306.

[24] Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122, With an appendix by M. Mignotte.

[25] D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly **75** (1968), 372–377.

[26] W. Bosma, *Computation of cyclotomic polynomials with Magma*, Computational algebra and number theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 213–225.

[27] B. Bzdęga, *Bounds on ternary cyclotomic coefficients*, Acta Arith. **144** (2010), no. 1, 5–16.

[28] B. Bzdęga, *On the height of cyclotomic polynomials*, Acta Arith. **152** (2012), no. 4, 349–359.

[29] B. Bzdęga, *Sparse binary cyclotomic polynomials*, J. Number Theory **132** (2012), no. 3, 410–413.

[30] B. Bzdęga, *Inclusion-exclusion polynomials with large coefficients*, Integers **13** (2013), Paper No. A74, 3.

[31] B. Bzdęga, *Jumps of ternary cyclotomic coefficients*, Acta Arith. **163** (2014), no. 3, 203–213.

[32] B. Bzdęga, *On a certain family of inverse ternary cyclotomic polynomials*, J. Number Theory **141** (2014), 1–12.

[33] B. Bzdęga, *On a generalization of the Beiter conjecture*, Acta Arith. **173** (2016), no. 2, 133–140.

[34] B. Bzdęga, *Products of cyclotomic polynomials on unit circle*, Int. J. Number Theory **13** (2017), no. 10, 2515–2530.

[35] B. Bzdęga, A. Herrera-Poyatos, and P. Moree, *Cyclotomic polynomials at roots of unity*, Acta Arith. **184** (2018), no. 3, 215–230.

[36] A. Cafure and E. Cesaratto, *Binary cyclotomic polynomials: Representation via words and algorithms*, Combinatorics on Words (Cham) (T. Lecroq and S. Puzynina, eds.), Springer International Publishing, 2021, pp. 65–77.

[37] O.-M. Camburu, E.-A. Ciolan, F. Luca, P. Moree, and I. E. Shparlinski, *Cyclotomic coefficients: gaps and jumps*, J. Number Theory **163** (2016), 211–237.

[38] L. Carlitz, *The number of terms in the cyclotomic polynomial $F_{pq}(x)$*, Amer. Math. Monthly **73** (1966), 979–981.

[39] L. Carlitz, *The sum of the squares of the coefficients of the cyclotomic polynomial*, Acta Math. Acad. Sci. Hungar. **18** (1967), 295–302.

[40] H. V. Chu, *On arithmetic progressions of powers in cyclotomic polynomials*, Amer. Math. Monthly **128** (2021), no. 3, 268–272.

[41] C. Cobeli, Y. Gallot, P. Moree, and A. Zaharescu, *Sister Beiter and Kloosterman: a tale of cyclotomic coefficients and modular inverses*, Indag. Math. (N.S.) **24** (2013), no. 4, 915–929.

[42] H. Cremer, *Carmina mathematica und andere poetische Jugendsünden*, 7. Aufl., Aachen: Verlag J. A. Mayer, 1982.

[43] M. Deaconescu and I. Sándor, *Variations on a theme by Hurwitz*, Gaz. Mat., Perfecț. Metod. Metodol. Mat. Inf. **8** (1987), no. 4, 186–191.

[44] A. Decker and P. Moree, *Coefficient convexity of divisors of $x^n - 1$*, 2011.

[45] A. Decker and P. Moree, *Coefficient convexity of divisors of $x^n - 1$*, Sarajevo J. Math. **9(21)** (2013), no. 1, 3–28.

[46] G. P. Dresden, *On the middle coefficient of a cyclotomic polynomial*, Amer. Math. Monthly **111** (2004), no. 6, 531–533.

[47] D. Duda, *The maximal coefficient of ternary cyclotomic polynomials with one free prime*, Int. J. Number Theory **10** (2014), no. 4, 1067–1080.

[48] C. Dunand, *On modular inverses of cyclotomic polynomials and the magnitude of their coefficients*, LMS J. Comput. Math. **15** (2012), 44–58.

[49] J. E. Eaton, *A formula for the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **45** (1939), no. 2, 178–186.

[50] S. Elder, *Flat cyclotomic polynomials: A new approach*, 2012.

[51] M. Endo, *On the coefficients of the cyclotomic polynomials*, Comment. Math. Univ. St. Paul. **23** (1974/75), no. 2, 121–126.

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

[53] P. Erdős, *On the coefficients of the cyclotomic polynomial*, Portugal. Math. **8** (1949), 63–71.

[54] P. Erdős, *On the growth of the cyclotomic polynomial in the interval* $(0, 1)$, Proc. Glasgow Math. Assoc. **3** (1957), 102–104.

[55] P. Erdős and R. C. Vaughan, *Bounds for the r-th coefficients of cyclotomic polynomials*, J. London Math. Soc. (2) **8** (1974), 393–400.

[56] V. Felsch and E. Schmidt, *Über Perioden in den Koeffizienten der Kreisteilungspolynome* $F_{np}(x)$, Math. Z. **106** (1968), 267–272.

[57] J. Fintzen, *Cyclotomic polynomial coefficients $a(n, k)$ with n and k in prescribed residue classes*, J. Number Theory **131** (2011), no. 10, 1852–1863.

[58] T. J. Flanagan, *On the coefficients of ternary cyclotomic polynomials*, Master's thesis, University of Nevada, Las Vegas, 2007.

[59] É. Fouvry, *On binary cyclotomic polynomials*, Algebra Number Theory **7** (2013), no. 5, 1207–1223.

[60] Y. Gallot and P. Moree, *Neighboring ternary cyclotomic coefficients differ by at most one*, J. Ramanujan Math. Soc. **24** (2009), no. 3, 235–248.

[61] Y. Gallot and P. Moree, *Ternary cyclotomic polynomials having a large coefficient*, J. Reine Angew. Math. **632** (2009), 105–125.

[62] Y. Gallot, P. Moree, and H. Hommersom, *Value distribution of cyclotomic polynomial coefficients*, Unif. Distrib. Theory **6** (2011), no. 2, 177–206.

[63] Y. Gallot, P. Moree, and R. Wilms, *The family of ternary cyclotomic polynomials with one free prime*, Involve **4** (2011), no. 4, 317–341.

[64] C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae, 1801 (Latin), Available in English translation in *Springer-Verlag, New York, 1986*. Translation by A. A. Clarke. Revised by W. C. Waterhouse, C. Greither and A. W. Grootendorst and with a preface by Waterhouse.

[65] S. Gong, *On a problem regarding coefficients of cyclotomic polynomials*, J. Number Theory **129** (2009), no. 12, 2924–2932.

[66] A. Grytczuk and B. Tropak, *A numerical method for the determination of the cyclotomic polynomial coefficients*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 15–19.

[67] H. Habermehl, S. Richardson, and M. A. Szwajkos, *A note on coefficients of cyclotomic polynomials*, Math. Mag. **37** (1964), no. 3, 183–185.

[68] A. Herrera-Poyatos and P. Moree, *Coefficients and higher order derivatives of cyclotomic polynomials: Old and new*, Expo. Math. **39** (2021), no. 3, 309–343.

[69] O. Hölder, *Zur Theorie der Kreisteilungsgleichung* $K_m(x) = 0$, Prace Mat.-Fiz. **43** (1936), 13–23 (German).

[70] H. Hong, E. Lee, H.-S. Lee, and C.-M. Park, *Maximum gap in (inverse) cyclotomic polynomial*, J. Number Theory **132** (2012), no. 10, 2297–2315.

[71] C. Hooley, *On the largest prime factor of* $p + a$, Mathematika **20** (1973), 135–143.

[72] C. Ji, *A specific family of cyclotomic polynomials of order three*, Sci. China Math. **53** (2010), no. 9, 2269–2274.

[73] C.-G. Ji and W.-P. Li, *Values of coefficients of cyclotomic polynomials*, Discrete Math. **308** (2008), no. 23, 5860–5863.

[74] C.-G. Ji, W.-P. Li, and P. Moree, *Values of coefficients of cyclotomic polynomials. II*, Discrete Math. **309** (2009), no. 6, 1720–1723.

[75] G. Jones, P. I. Kester, L. Martirosyan, P. Moree, L. Tóth, B. B. White, and B. Zhang, *Coefficients of (inverse) unitary cyclotomic polynomials*, Kodai Math. J. **43** (2020), no. 2, 325–338.

[76] J. Justin, *Bornes des coefficients du polynôme cyclotomique et de certains autres polynômes*, C. R. Acad. Sci. Paris Sér. A-B **268** (1969), A995–A997.

[77] N. Kaplan, *Flat cyclotomic polynomials of order three*, J. Number Theory **127** (2007), no. 1, 118–126.

[78] N. Kaplan, *Bounds for the maximal height of divisors of* $x^n - 1$, J. Number Theory **129** (2009), no. 11, 2673–2688.

[79] N. Kaplan, *Flat cyclotomic polynomials of order four and higher*, Integers **10** (2010), A30, 357–363.

[80] G. S. Kazandzidis, *On the cyclotomic polynomial: Coefficients*, Bull. Soc. Math. Grèce (N.S.) **4** (1963), no. 1, 1–11.

[81] S. Konyagin, H. Maier, and E. Wirsing, *Cyclotomic polynomials with many primes dividing their orders*, Period. Math. Hungar. **49** (2004), no. 2, 99–106.

[82] Y. Koshiba, *On the calculations of the coefficients of the cyclotomic polynomials*, Rep. Fac. Sci. Kagoshima Univ. (1998), no. 31, 31–44.

[83] Y. Koshiba, *On the calculations of the coefficients of the cyclotomic polynomials. II*, Rep. Fac. Sci. Kagoshima Univ. (2000), no. 33, 55–59.

[84] A. Kosyak, P. Moree, E. Sofos, and B. Zhang, *Cyclotomic polynomials with prescribed height and prime number theory*, Mathematika **67** (2021), no. 1, 214–234.

[85] L. Kronecker, *Mémoire sur les facteures irréductibles de l'expression* $x^n - 1$, J. Math. Pures et Appls. **19** (1854), 177–192.

[86] T. Y. Lam, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001.

[87] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly **103** (1996), no. 7, 562–564.

[88] E. Leher, *Applications of the minimal transversal method in numerical semigroups*, Ph.D. thesis, Tel Aviv University, Tel Aviv, 2007.

[89] D. H. Lehmer, *Some properties of the cyclotomic polynomial*, J. Math. Anal. Appl. **15** (1966), 105–117.

[90] E. Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **42** (1936), no. 6, 389–392.

[91] H. W. Lenstra, Jr., *Vanishing sums of roots of unity*, Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, Math. Centre Tracts, vol. 101, Math. Centrum, Amsterdam, 1979, pp. 249–268.

[92] R. I. Liu, *Coefficients of a relative of cyclotomic polynomials*, Acta Arith. **165** (2014), no. 4, 301–325.

[93] F. Luca, P. Moree, R. Osburn, S. Saad Eddin, and A. Sedunova, *Constrained ternary integers*, Int. J. Number Theory **15** (2019), no. 2, 407–431.

[94] H. Maier, *The coefficients of cyclotomic polynomials*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 349–366.

[95] H. Maier, *Cyclotomic polynomials with large coefficients*, Acta Arith. **64** (1993), no. 3, 227–235.

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

[97] H. Maier, *Cyclotomic polynomials whose orders contain many prime factors*, Period. Math. Hungar. **43** (2001), no. 1-2, 155–164.

[98] H. Maier, *Anatomy of integers and cyclotomic polynomials*, Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, pp. 89–95.

[99] G. E. Martin, *Geometric constructions*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1998.

[100] R. Meshulam, *Homology of balanced complexes via the Fourier transform*, J. Algebraic Combin. **35** (2012), no. 4, 565–571.

[101] A. Migotti, *Zur Theorie der Kreisteilung*, Wien. Ber. **87** (1883), 8–14 (German).

[102] H. Möller, *Über die i-ten Koeffizienten der Kreisteilungspolynome*, Math. Ann. **188** (1970), 26–38.

[103] H. Möller, *Über die Koeffizienten des n-ten Kreisteilungspolynoms*, Math. Z. **119** (1971), 33–40.

[104] H. L. Montgomery and R. C. Vaughan, *The order of magnitude of the mth coefficients of cyclotomic polynomials*, Glasgow Math. J. **27** (1985), 143–159.

[105] P. Moree, *Inverse cyclotomic polynomials*, J. Number Theory **129** (2009), no. 3, 667–680.

[106] P. Moree, *Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers*, Amer. Math. Monthly **121** (2014), no. 10, 890–902.

[107] P. Moree, *Prime gaps and cyclotomic polynomials*, Nieuw Arch. Wisk (to appear).

[108] P. Moree and E. Roşu, *Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients*, Int. J. Number Theory **8** (2012), no. 8, 1883–1902.

[109] P. Moree and L. Tóth, *Unitary cyclotomic polynomials*, Integers **20** (2020), Paper No. A65, 21.

[110] T. Mukherjee, *Cyclotomic polynomials in Ring-LWE homomorphic encryption schemes*, Master's thesis, Rochester Institute of Technology, New York, 2016.

[111] G. Musiker and V. Reiner, *The cyclotomic polynomial topologically*, J. Reine Angew. Math. **687** (2014), 113–132.

[112] T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm, 1951.

[113] S. H. Park, S. Kim, D. H. Lee, and J. H. Park, *Improved ring LWR-based key encapsulation mechanism using cyclotomic trinomials*, IEEE Access **8** (2020), 112585–112597.

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

[115] N. C. Ryan, B. C. Ward, and R. Ward, *Some conjectures on the maximal height of divisors of $x^n - 1$*, Involve **3** (2010), no. 4, 451–457.

[116] J. Sándor and B. Crstici, *Handbook of number theory. II*, Kluwer Academic Publishers, Dordrecht, 2004.

[117] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org.

[118] S. T. Somu, *On the coefficients of divisors of $x^n - 1$*, J. Number Theory **167** (2016), 284–293.

[119] S. T. Somu, *On the distribution of numbers related to the divisors of $x^n - 1$*, J. Number Theory **170** (2017), 3–9.

[120] J. Suzuki, *On coefficients of cyclotomic polynomials*, Proc. Japan Acad. Ser. A Math. Sci. **63** (1987), no. 7, 279–280.

[121] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015, Translated from the 2008 French edition by Patrick D. F. Ion.

[122] R. Thangadurai, *On the coefficients of cyclotomic polynomials*, Cyclotomic fields and related topics (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, pp. 311–322.

[123] L. Thompson, *Heights of divisors of $x^n - 1$*, Integers **11** (2011), no. 4, 543–551.

[124] R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. **21** (1974), 289–295 (1975).

[125] R. C. Vaughan, *Coefficients of cyclotomic polynomials and related topics*, Proceedings of the Congress on Number Theory (Spanish) (Zarauz, 1984), Univ. País Vasco-Euskal Herriko Unib., Bilbao, 1989, pp. 43–68.

[126] S. Wang, *Maximal height of divisors of $x^{pq^b} - 1$*, Int. J. Number Theory **11** (2015), no. 1, 67–79.

[127] S. H. Weintraub, *Several proofs of the irreducibility of the cyclotomic polynomials*, Amer. Math. Monthly **120** (2013), no. 6, 537–545.

[128] E. Witt, *Über die Kommutativität endlicher Schiefkörper*, Abh. Math. Sem. Univ. Hamburg **8** (1931), no. 1, 413 (German).

[129] P. Yuan, *Coefficients of cyclotomic polynomials*, Southeast Asian Bull. Math. **36** (2012), no. 5, 753–756.

[130] B. Zhang, *A note on ternary cyclotomic polynomials*, Bull. Korean Math. Soc. **51** (2014), no. 4, 949–955.

[131] B. Zhang, *The height of a class of ternary cyclotomic polynomials*, Bull. Korean Math. Soc. **54** (2017), no. 1, 43–50.

[132] B. Zhang, *Remarks on the flatness of ternary cyclotomic polynomials*, Int. J. Number Theory **13** (2017), no. 2, 529–547.

[133] B. Zhang, *The upper bound of a class of ternary cyclotomic polynomials*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **60(108)** (2017), no. 1, 25–32.

[134] B. Zhang, *A remark on bounds for the maximal height of divisors of $x^n - 1$*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **62(110)** (2019), no. 2, 209–214.

[135] B. Zhang, *The flatness of a class of ternary cyclotomic polynomials*, Publ. Math. Debrecen **97** (2020), no. 1-2, 201–216.

[136] B. Zhang, *The flatness of ternary cyclotomic polynomials*, Rend. Semin. Mat. Univ. Padova **145** (2021), 1–42.

[137] B. Zhang and Y. Zhou, *On a class of ternary cyclotomic polynomials*, Bull. Korean Math. Soc. **52** (2015), no. 6, 1911–1924.

[138] J. Zhao and X. Zhang, *Coefficients of ternary cyclotomic polynomials*, J. Number Theory **130** (2010), no. 10, 2223–2237.