Coefficients of (inverse) unitary cyclotomic polynomials

G. Jones, P. I. Kester, L. Martirosyan, P. Moree, L. Tóth, B. B. White and B. Zhang

November 6, 2019

Abstract

The notion of block divisibility naturally leads one to introduce unitary cyclotomic polynomials $\Phi_n^*(x)$. They can be written as certain products of cyclotomic poynomials. We study the case where n has two or three distinct prime factors using numerical semigroups, respectively Bachman's inclusion-exclusion polynomials. Given $m \geqslant 1$ we show that every integer occurs as a coefficient of $\Phi_{mn}^*(x)$ for some $n \geqslant 1$ following Ji, Li and Moree [9]. Here n will typically have many different prime factors. We also consider similar questions for the polynomials $(x^n - 1)/\Phi_n^*(x)$, the inverse unitary cyclotomic polynomials.

1 Introduction

1.1 (Inverse) (unitary) cyclotomic polynomials

The *cyclotomic polynomials* $\Phi_n(x)$ are defined by

$$\Phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (x - \exp(2\pi i j/n)) .$$

They are monic polynomials of degree $\varphi(n)$ (with φ Euler's totient function) and arise as irreducible factors on factorizing $x^n - 1$ over the rationals:

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

By Möbius inversion it follows from (1) that

$$\Phi_n(x) = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)} = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}, \tag{2}$$

where μ denotes the Möbius function.

A divisor d of n ($d, n \in \mathbb{N}$) is called a *unitary divisor* (or block divisor) if $(d, n/d) = 1$, notation $d \mid\mid n$ (this is in agreement with the standard notation $p^a \mid\mid n$ used for prime powers

p^a). If in (1) one only considers block divisors d of n, the resulting factors are the *unitary cyclotomic polynomials* $\Phi_d^*(x)$, that is, we have

$$x^n - 1 = \prod_{d||n} \Phi_d^*(x). \tag{3}$$

Just as the system of equations (1) (taking $n = 1, 2, \ldots$) implicitly uniquely defines the cyclotomic polynomials, so does the latter system of equations uniquely define the unitary cyclotomic polynomials (the reader preferring an explicit definition is referred to (6)). The polynomial $\Phi_n^*(x)$ is monic, has integer coefficients and is of degree $\varphi^*(n)$, with $\varphi^*(n) = \#\{j : 1 \leqslant j \leqslant n, (j,n)_* = 1\}$ and $(j,n)_* = \max\{d : d \mid j, d \mid\mid n\}$. If $n = \prod q_i$ is the factorization of n in pairwise coprime prime powers, then $\varphi^*(n) = \prod_i (q_i - 1)$. Note that $\varphi^*(n) \geqslant \varphi(n)$.

The unitary equivalent of (2) reads

$$\Phi_n^*(x) = \prod_{d||n} \left(x^{n/d} - 1\right)^{\mu^*(d)} = \prod_{d||n} \left(x^d - 1\right)^{\mu^*(n/d)}, \tag{4}$$

where $\mu^*(n) = (-1)^{\omega(n)}$ and $\omega(n)$ denotes the number of distinct prime factors of n. Note that since $\sum_{d||n} \mu^*(d) = 0$ for $n > 1$, we can alternatively write, for $n > 1$,

$$\Phi_n^*(x) = \prod_{d||n} \left(1 - x^d\right)^{\mu^*(n/d)}. \tag{5}$$

Comparison of (1) and (3) shows that $\Phi_n^*(x)$ is a product of cyclotomic polynomials. The next result, proved in [15] where also many connections with the theory of arithmetic functions are pointed out, makes this precise.

Theorem 1 (Moree and Tóth [15])**.** *For any natural number n we have*

$$\Phi_n^*(x) = \prod_{\substack{d|n \\ \kappa(d)=\kappa(n)}} \Phi_d(x), \tag{6}$$

where $\kappa(n) = \prod_{p|n} p$ is the square-free kernel of n.

Corollary 2. *If n is square-free, then $\Phi_n^*(x) = \Phi_n(x)$.*

This corollary is easily proved directly. In case n is square-free, $\mu^*(n) = \mu(n)$ and we see that the products in (2) and (4) are identical and therefore $\Phi_n(x) = \Phi_n^*(x)$.

By (1) and (3) we have, respectively,

$$\Psi_n(x) := \frac{x^n - 1}{\Phi_n(x)} = \prod_{d<n,\ d|n} \Phi_d(x), \text{ and } \Psi_n^*(x) := \frac{x^n - 1}{\Phi_n^*(x)} = \prod_{d<n,\ d||n} \Phi_d^*(x), \tag{7}$$

and thus both Ψ_n and Ψ_n^* are polynomials having integer coefficients.

The polynomials Ψ_n were dubbed *inverse cyclotomic polynomials* by Moree [13], who was the first to systematically study them. Meanwhile their study found some application in cryptography, see, e.g., [6, 7]. Their coefficients behave in various aspects very similar, but also in various aspects quite dissimilar to the ordinary cyclotomic coefficients.

The polynomials Ψ_n^* seem not have be systematically considered before. We will call them *inverse unitary cyclotomic polynomials*.

The behavior of (inverse) cyclotomic coefficients is and was a topic of intense study. The aim of this paper is to initiate the study of the coefficients of Φ_n^* and Ψ_n^*.

1.2 (Inverse) (unitary) cyclotomic coefficients

We write

$$\Phi_n(x) = \sum_{j=0}^{\infty} a_n(j)x^j,\ \Psi_n(x) = \sum_{j=0}^{\infty} c_n(j)x^j,\ \Phi_n^*(x) = \sum_{j=0}^{\infty} a_n^*(j)x^j,\ \Psi_n^*(x) = \sum_{j=0}^{\infty} c_n^*(j)x^j. \tag{8}$$

This notation looks perhaps strange to the reader, but implicitly defines the coefficients for every j, which serves our purposes.

It turns out that for many n the above polynomials are *flat* (that is, they have all their coefficients in $\{-1, 0, 1\}$). The smallest n for which the above four classes of polynomials are non-flat are, respectively, $105, 561, 60$ and 120, see the tables in Section 4. These tables perhaps also suggest that each of the four polynomial families has every integer occurring as a coefficient. The main result of this paper is that this is indeed the case.

Ji, Li and Moree [9, Theorem 1] showed that given a fixed integer $m \geqslant 1$ we have

$$\{a_{mn}(j) : n \geqslant 1,\ j \geqslant 0\} = \{c_{mn}(j) : n \geqslant 1,\ j \geqslant 0\} = \mathbb{Z}. \tag{9}$$

By a similar approach we will establish the following result.

Theorem 3. *Let $m \geqslant 1$ be fixed. We have*

$$\{a^*_{mn}(j) : n \geqslant 1,\ j \geqslant 0\} = \{c^*_{mn}(j) : n \geqslant 1,\ j \geqslant 0\} = \mathbb{Z}.$$

The proof will show that we actually can restrict to the case where n is square-free and coprime to m, cf. (10). The result of Ji, Li and Moree in case $m = 1$ is due to Suzuki [17], who adapted a proof of Issai Schur (see, e.g., Emma Lehmer [11]) showing that every negative even number occurs as a cyclotomic coefficient. Theorem 3 in case m is a prime power is due to Ji and Li [8].

1.3 Proof of Theorem 3

Inspection of the proof of Theorem 1 in [9] shows that the authors prove more than they claim, namely they show that

$$\{a_{mn}(j) : n \geqslant 1,\ n \text{ is square-free},\ (n, m) = 1,\ j \geqslant 0\} = \mathbb{Z}, \tag{10}$$

and the same result with $a_{mn}(j)$ replaced by $c_{mn}(j)$.

Proposition 4. *Let $m \geqslant 1$ be square-free. We have*

$$\{a^*_{mn}(j) : n \geqslant 1,\ j \geqslant 0\} = \{c^*_{mn}(j) : n \geqslant 1,\ j \geqslant 0\} = \mathbb{Z}.$$

Proof. If m is square-free, then the index mn of any coefficient appearing on the left hand side of (10) is square-free. By Corollary 2 it then follows that $a_{mn}(j) = a^*_{mn}(j)$ and so the result follows from (10) for the unitary cyclotomic coefficients. Likewise it follows for the inverse unitary cyclotomic coefficients. □

We are now ready to prove Theorem 3. By the latter result we could restrict to non-square-free m. However, this is not necessary as our argument works for every $m > 1$.

Proof of Theorem 3. The result for $m = 1$ is true by Proposition 4, so we may assume that $m > 1$.

Let $t \geqslant 1$ be arbitrary but fixed. We will show that $t - 1$ appears as a coefficient of $\Phi^*_{mn}(x)$ for some $n \geqslant 1$ (and in addition some variations of this).

Let $\pi(x; d, a)$ denote the number of primes $p \leqslant x$ that satisfy $p \equiv a (\text{mod } d)$, with a, d coprime integers. A quantitative version of Dirichlet's prime number theorem for arithmetic progressions states that, asymptotically, $\pi(x; d, a) \sim x/(\varphi(d) \log x)$. This implies that there exist an integer $n \geqslant 8m$ and primes $p_1, p_2, \ldots, p_t$ such that

$$n < p_1 < p_2 < \cdots < p_t < \frac{15}{8}n \text{ and } p_j \equiv 1(\text{mod } m), \quad j = 1, 2, \ldots, t.$$

Clearly $p_t < 2p_1$. Let q be any prime exceeding $2p_1$ and put

$$n_1 = \begin{cases} p_1 p_2 \cdots p_t q & \text{if } t \text{ is even;} \\ p_1 p_2 \cdots p_t & \text{otherwise.} \end{cases}$$

Note that m and n_1 are coprime and that $\mu^*(n_1) = -1$. Using these observations we conclude that

$$\begin{aligned}
\Phi^*_{mn_1}(x) &\equiv \prod_{d||mn_1,\ d<2p_1} (1 - x^d)^{\mu^*(\frac{mn_1}{d})} \ (\text{mod } x^{2p_1}) \\
&\equiv \prod_{d||m} (1 - x^d)^{\mu^*(\frac{m}{d})\mu^*(n_1)} \prod_{j=1}^{t} (1 - x^{p_j})^{\mu^*(\frac{mn_1}{p_j})} \ (\text{mod } x^{2p_1}) \\
&\equiv \Phi^*_m(x)^{\mu^*(n_1)} \prod_{j=1}^{t} (1 - x^{p_j})^{-\mu^*(mn_1)} \ (\text{mod } x^{2p_1}) \\
&\equiv \frac{1}{\Phi^*_m(x)} \prod_{j=1}^{t} (1 - x^{p_j})^{\mu^*(m)} \ (\text{mod } x^{2p_1}) \\
&\equiv \frac{1}{\Phi^*_m(x)} \Big(1 - \mu^*(m)(x^{p_1} + \ldots + x^{p_t})\Big) \ (\text{mod } x^{2p_1}). \qquad (11)
\end{aligned}$$

Let

$$\frac{1}{\Phi^*_m(x)} = \sum_{j=0}^{\infty} u^*_m(j) x^j$$

be the Taylor expansion of $1/\Phi_m^*(x)$ around $x = 0$. Noting that, for $|x| < 1$,

$$\frac{1}{\Phi_m^*(x)} = -\Psi_m^*(x)(1 + x^m + x^{2m} + \cdots)$$

and $m > m - \varphi^*(m) = \deg\Psi_m^*$, we see that $u_m^*(j)$ is an integer that only depends on the congruence class of j modulo m. Thus, in particular, if $k \geqslant p_j$ we have $u_m^*(k - p_j) = u_m^*(k - 1)$ since by assumption $p_j \equiv 1(\text{mod } m)$. Using this and (11) we infer that, for $p_t \leqslant k < 2p_1$,

$$a_{mn_1}^*(k) = u_m^*(k) - \mu^*(m)\sum_{j=1}^{t} u_m^*(k - p_j) = u_m^*(k) - \mu^*(m)tu_m^*(k - 1). \tag{12}$$

We consider two cases depending on whether $\mu^*(m) = 1$ or $\mu^*(m) = -1$.

Case 1. $\mu^*(m) = 1$. In this case m has at least two block divisors > 1 (since by assumption $m > 1$). Let $1 < q_1 < q_2$ be the smallest, respectively second smallest block divisor > 1 of m. Note that both q_1 and q_2 are prime powers and so $\mu^*(q_i) = -1$. Using (5) we see that

$$\begin{aligned}\frac{1}{\Phi_m^*(x)} &\equiv \frac{(1 - x^{q_1})(1 - x^{q_2})}{1 - x} \ (\text{mod } x^{q_2+2}) \\ &\equiv 1 + x + x^2 + \cdots + x^{q_1-1} - x^{q_2} - x^{q_2+1} \ (\text{mod } x^{q_2+2}).\end{aligned} \tag{13}$$

Thus $u_m^*(k) = 1$ if $k \equiv \beta(\text{mod } m)$ with $\beta \in \{0, 1\}$ and $u_m^*(k) = -1$ if $k \equiv \beta(\text{mod } m)$ with $\beta \in \{q_2, q_2 + 1\}$. This in combination with (12) shows that $a_{mn_1}^*(p_t) = 1 - t$. Since $n \geqslant 8m \geqslant 8q_2$ we have $p_t + q_2 < 15n/8 + n/8 = 2n < 2p_1$, and hence we may apply (12) with $k = p_t + q_2$ giving rise to $a_{mn_1}^*(p_t + q_2) = t - 1$. Since $\{1 - t, t - 1 \mid t \geqslant 1\} = \mathbb{Z}$ the result follows in this case.

Case 2. $\mu^*(m) = -1$. Here we notice that

$$\frac{1}{\Phi_m^*(x)} \equiv \begin{cases} 1 - x + x^2 \ (\text{mod } x^3) & \text{if } m \equiv 2(\text{mod } 4); \\ 1 - x \ (\text{mod } x^3) & \text{otherwise.}\end{cases}$$

Using this we find that $a_{mn_1}^*(p_t) = -1 + t$. Furthermore, $a_{mn_1}^*(p_t + 1) = 1 - t$ in case $m \equiv 2(\text{mod } 4)$ and $a_{mn_1}^*(p_t + 1) = -t$ otherwise. Since $\{-1 + t, -t \mid t \geqslant 1\} = \mathbb{Z}$ and $\{-1 + t, 1 - t \mid t \geqslant 1\} = \mathbb{Z}$, it follows that also $\{a_{mn}^*(j) : n \geqslant 1,\ j \geqslant 0\} = \mathbb{Z}$ in this case.

It remains to show that $\{c_{mn}^*(j) : n \geqslant 1,\ j \geqslant 0\} = \mathbb{Z}$. By Proposition 4 we may assume that $m > 1$. Let q be any prime exceeding $2p_1$ and put

$$n_2 = \begin{cases} p_1p_2 \cdots p_t & \text{if } t \text{ is even;} \\ p_1p_2 \cdots p_tq & \text{otherwise.}\end{cases}$$

Using that $\mu^*(n_2) = -\mu^*(n_1)$, we see that

$$\Psi_{mn_2}^*(x) = \frac{x^{mn_2} - 1}{\Phi_{mn_2}^*(x)} \equiv -\frac{1}{\Phi_{mn_2}^*(x)} \equiv -\Phi_{mn_1}^*(x) \ (\text{mod } x^{2p_1}),$$

and hence $c_{mn_2}^*(k) = -a_{mn_1}^*(k)$ for $k < 2p_1$. The proof is now completed by reasoning as in the case of unitary cyclotomic coefficients using formula (12) (which is valid for $p_t \leqslant k < 2p_1$). □

2 Connection with numerical semigroups

Let $a_1, \ldots, a_m$ be positive integers, and let $S(a_1, \ldots, a_m)$ be the set of all non-negative integer linear combinations of $a_1, \ldots, a_m$, that is,

$$S(a_1, \ldots, a_m) = \{x_1 a_1 + \ldots + x_m a_m \mid x_i \in \mathbb{Z}_{\geqslant 0}\}.$$

Then S is a *semigroup* (i.e., it is closed under addition). A semigroup S is said to be *numerical* if its complement $\mathbb{Z}_{\geqslant 0} \backslash S$ is finite. The numbers in this set are called *gaps*. It is easy to prove that $S(a_1, \ldots, a_m)$ is numerical if and ony if $a_1, \ldots, a_m$ are relatively prime. If S is numerical, the maximum gap is called the *Frobenius number* of S and denoted by $F(S)$. The *Hilbert series* of the numerical semigroup S is the formal power series $H_S(x) = \sum_{s \in S} x^s \in \mathbb{Z}[[x]]$. It is practical to multiply this by $1 - x$ as we then obtain a *polynomial*, called the *semigroup polynomial*:

$$P_S(x) = (1-x)H_S(x) = x^{F(S)+1} + (1-x) \sum_{\substack{0 \leqslant s \leqslant F(S) \\ s \in S}} x^s = 1 + (x-1) \sum_{s \notin S} x^s. \tag{14}$$

It is easy to see that the non-zero coefficients of P_S alternate between 1 and -1. From P_S one immediately reads off the Frobenius number:

$$F(S) = \deg(P_S(x)) - 1. \tag{15}$$

The following result is well-known, see, e.g., Bardomero and Beck [4], Moree [14] or Ramírez–Alfonsín [16, p. 34]. It seems to have been first proved by Székely and Wormald [18].

Theorem 5. *If $a, b > 1$ are coprime integers, then*

$$P_{S(a,b)}(x) = (1-x) \sum_{s \in S(a,b)} x^s = \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)}.$$

Using (15) it follows that $F(S(a,b)) = ab - a - b$, something that was already known to Sylvester in the 19th century.

The next result is a consequence of (4) and Theorem 5.

Theorem 6. *Let p and q be coprime prime powers > 1. We have $P_{S(p,q)}(x) = \Phi^*_{pq}(x)$.*

Corollary 7. *We have*

$$a^*_{pq}(k) = \begin{cases} 1 & \text{if } k \in S(p,q),\ \ k-1 \notin S(p,q); \\ -1 & \text{if } k \notin S(p,q),\ \ k-1 \in S(p,q); \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 8. *In case p and q are distinct primes, we have $P_{S(p,q)}(x) = \Phi_{pq}(x)$.*

The interpretation of $\Phi_{pq}(x)$ as a semigroup polynomial leads to trivial proofs of very classical facts about these so-called binary cyclotomic polynomials. E.g., that they are of height 1 (which was first proved by Migotti [12] and several years later by Bang [3]) and that the non-zero coefficients alternate between 1 and -1 (due to Carlitz [5]).

The polynomial $\Psi^*_{ab}(x)$ with $a < b$ coprime prime powers, in contrast to $\Phi^*_{ab}(x)$, is boring:

$$\Psi^*_{ab}(x) = \frac{(x^a - 1)(x^b - 1)}{(x - 1)} = -1 - x - \cdots - x^{a-1} + x^b + \cdots + x^{a+b-1}. \tag{16}$$

For further reading on the connection between numerical semigroups and cyclotomic polynomials the reader is referred to Moree [14].

3 Connection with inclusion-exclusion polynomials

Let $\rho = \{r_1, r_2, \ldots, r_s\}$ be a set of pairwise coprime natural numbers > 1 and put

$$n_0 = \prod_i r_i,\ n_i = \frac{n_0}{r_i},\ n_{ij} = \frac{n_0}{r_i r_j}\ [i \neq j], \ldots,$$

and define

$$Q_\rho(x) := \frac{(x^{n_0} - 1) \cdot \prod_{i<j}(x^{n_{ij}} - 1) \cdots}{\prod_i (x^{n_i} - 1) \cdot \prod_{i<j<k}(x^{n_{ijk}} - 1) \cdots}. \tag{17}$$

It can be shown that $Q_\rho(x)$ is a polynomial with *integer* coefficients. This class of polynomials was introduced by Bachman [1], who named them *inclusion-exclusion polynomials.* From the definition and Theorem 6 we infer that $P_{S(a,b)}(x) = Q_{\{a,b\}}(x)$.

Let $n > 1$ be an integer and $\prod_{i=1}^t p_i^{e_i}$ its canonical factorization. Comparison of (4) and (17) then shows that

$$\Phi^*_n(x) = Q_{\{p_1^{e_1}, \ldots, p_t^{e_t}\}}(x). \tag{18}$$

We will now derive some consequences of this identity in the ternary case $t = 3$. One of the tools that can be used here is a fundamental lemma of Kaplan [10] relating the case $t = 3$ to the case $t = 2$ (he formulated it for cyclotomic polynomials).

Given a polynomial f, we let $\mathcal{C}(f)$ denote the set of all coefficients of f and $H(f)$ the maximum element (in absolute value) in $\mathcal{C}(f)$. Combination of (18) and [1, Theorem 3] leads to the first assertion below. Combination of (18) and [2, Theorem] leads to the second assertion.

Theorem 9. *Let $p, q, r, s \geqslant 3$ be four pairwise coprime prime powers. Then $\mathcal{C}(\Phi^*_{pqr})$ is a string of consecutive integers, and for $r, s > \max(p, q)$, we have*

$$\mathcal{C}(\Phi^*_{pqr}) = \begin{cases} \mathcal{C}(\Phi^*_{pqs}) & \text{if } r \equiv s \pmod{pq}; \\ -\mathcal{C}(\Phi^*_{pqs}) & \text{if } r \equiv -s \pmod{pq}. \end{cases}$$

If $r \equiv \pm s \pmod{pq}$ and $r > \max(p, q) > s \geqslant 3$, then

$$H(\Phi^*_{pqs}) \leqslant H(\Phi^*_{pqr}) \leqslant H(\Phi^*_{pqs}) + 1. \tag{19}$$

The following is a consequence of Kaplan's work, cf. [2, (4)].

Corollary 10. *Let p^a and q^b be two fixed coprime prime powers and let r be a third prime. Then $\Phi^*_{p^a q^b r^c}$ is flat for every positive exponent c with $r^c \equiv \pm 1 \pmod{p^a q^b}$.*

See subsection 4.1 some numerical material demonstrating Theorem 9.

3.1 Ternary inverse unitary cyclotomic polynomials

It seems that most (but not all!) of the work on Ψ_{pqr} can be easily adapted to the inverse unitary setting. We merely give one example here.

Theorem 11. *Let $p < q < r$ pairwise coprime prime powers. We have*

$$H(\Psi^*_{pqr}) \leqslant \left[\frac{(p-1)(q-1)}{r}\right] + 1 \leqslant p - 1.$$

Proof. Using (2) and (4) we see that $\Psi^*_{pqr}(x) = \Phi^*_{pq}(x)\Psi^*_{pq}(x^r)$, and so

$$c^*_{pqr}(k) = \sum_{j=0}^{[\frac{k}{r}]} a^*_{pq}(k - jr)c^*_{pq}(j). \tag{20}$$

The number of j for which $0 \leqslant k - jr \leqslant \varphi^*(pq)$, and so $a^*_{pq}(k - jr)$ is potentially non-zero, is at most

$$\left[\frac{\varphi^*(pq)}{r}\right] + 1 = \left[\frac{(p-1)(q-1)}{r}\right] + 1 \leqslant p - 2 + 1 = p - 1.$$

Since $|a^*_{pq}(k - jr)| \leqslant 1$ by Corollary 7 and $|c^*_{pq}(j)| \leqslant 1$ by (16), the proof is concluded. □

4 Some numerical data

Let $n \geqslant 1$ and let $f_n \in \{\Phi_n, \Psi_n, \Phi^*_n, \Psi^*_n\}$, with its coefficients denoted as in (8). For a given integer $m \geqslant 2$, we list the smallest n such that $H(f_n) = m$, with $H(f)$ the maximum coefficient (in absolute value) of f. In addition we list the degree of f_n, the smallest k such that $|f_n(k)| = m$, and the value of $f_n(k)$.

Table 1: (Φ_n) Minimal n and k with $|a_n(k)| = m$

m	n	$\deg(\Phi_n)$	k	$a_n(k)$
2	$105 = 3 \cdot 5 \cdot 7$	48	7	-2
3	$385 = 5 \cdot 7 \cdot 11$	240	119	-3
4	$1365 = 3 \cdot 5 \cdot 7 \cdot 13$	576	196	-4
5	$1785 = 3 \cdot 5 \cdot 7 \cdot 17$	768	137	$+5$
6	$2805 = 3 \cdot 5 \cdot 11 \cdot 17$	1280	573	-6
7	$3135 = 3 \cdot 5 \cdot 11 \cdot 19$	1440	616	$+7$
8	$6545 = 5 \cdot 7 \cdot 11 \cdot 17$	3840	1528	-8
9	$6545 = 5 \cdot 7 \cdot 11 \cdot 17$	3840	1914	$+9$
10	$10465 = 5 \cdot 7 \cdot 13 \cdot 23$	6336	1196	-10
11	$10465 = 5 \cdot 7 \cdot 13 \cdot 23$	6336	1916	-11

For $m = 10, \ldots, 14$ it turns out that $n = 10465$.

Table 2: (Ψ_n) `Minimal` n `and` k `with` $|c_n(k)| = m$

m	n	$\deg(\Psi_n)$	k	$c_n(k)$
2	$561 = 3 \cdot 11 \cdot 17$	241	17	-2
3	$1155 = 3 \cdot 5 \cdot 7 \cdot 11$	675	33	-3
4	$2145 = 3 \cdot 5 \cdot 11 \cdot 13$	1185	44	$+4$
5	$3795 = 3 \cdot 5 \cdot 11 \cdot 23$	2035	132	-5
6	$5005 = 5 \cdot 7 \cdot 11 \cdot 13$	2125	201	-6
7	$5005 = 5 \cdot 7 \cdot 11 \cdot 13$	2125	310	-7
8	$8645 = 5 \cdot 7 \cdot 13 \cdot 19$	3461	227	-8
9	$8645 = 5 \cdot 7 \cdot 13 \cdot 19$	3461	240	$+9$
10	$11305 = 5 \cdot 7 \cdot 17 \cdot 19$	4393	240	-10
11	$11305 = 5 \cdot 7 \cdot 17 \cdot 19$	4393	306	$+11$

For $m = 10, \ldots, 21$ it turns out that $n = 11305$.

Table 3: (Φ_n^*) `Minimal` n `and` k `with` $|a_n^*(k)| = m$

m	n	$\deg(\Phi_n^*)$	k	$a_n^*(k)$
2	$60 = 2^2 \cdot 3 \cdot 5$	24	5	-2
3	$385 = 5 \cdot 7 \cdot 11$	240	119	-3
4	$780 = 2^2 \cdot 3 \cdot 5 \cdot 13$	288	78	-4
5	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$	560	107	-5
6	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$	560	111	$+6$
7	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$	560	210	-7
8	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$	560	213	-8
9	$3640 = 2^3 \cdot 5 \cdot 7 \cdot 13$	2016	626	-9
10	$3640 = 2^3 \cdot 5 \cdot 7 \cdot 13$	2016	648	$+10$
11	$3640 = 2^3 \cdot 5 \cdot 7 \cdot 13$	2016	748	$+11$
12	$3640 = 2^3 \cdot 5 \cdot 7 \cdot 13$	2016	761	$+12$
13	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	386	-13
14	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	419	-14
15	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	425	$+15$
16	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	474	-16
17	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	497	-17
18	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	475	-18
19	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	1440	558	$+19$

For $m = 20, \ldots, 41$ it turns out that $n = 9240$.

Table 4: (Ψ_n^*) Minimal n and k with $|c_n^*(k)| = m$

m	n	$\deg(\Psi_n^*)$	k	$c_n^*(k)$
2	$120 = 2^3 \cdot 3 \cdot 5$	64	8	-2
3	$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$	276	12	-3
4	$1008 = 2^4 \cdot 3^2 \cdot 7$	288	48	-4
5	$1820 = 2^2 \cdot 5 \cdot 7 \cdot 13$	956	475	$+5$
6	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	66	$+6$
7	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	103	$+7$
8	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	114	-8
9	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	111	-9
10	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	112	-10
11	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	121	$+11$
12	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	122	$+12$
13	$3080 = 2^3 \cdot 5 \cdot 7 \cdot 11$	1400	177	$+13$
14	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	5880	261	-14
15	$8580 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	5700	705	-15
16	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	5880	253	-16
17	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	5880	325	$+17$
18	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	5880	341	$+18$
19	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	5880	450	$+19$

For m=16, . . . , 21 it turns out that $n = 9240$.

The tables suggest that the (unitary) cyclotomic polynomials are generically of the same flatness as their inverses. However, generically an (inverse) cyclotomic polynomial seems to be rather flatter than its unitary equivalent.

4.1 Numerical material related to Theorem 9

If n has three or less block divisors that are prime powers, then $\mathcal{C}(\Phi_n^*)$ consists of consecutive integers: we have, e.g. , $\mathcal{C}(\Phi^*_{8\cdot 11\cdot 13}) = \{-4, 3\}$ and $\mathcal{C}(\Phi^*_{27\cdot 29\cdot 31}) = \{-8, \ldots, 8\}$. If n has four or more block divisors that are prime powers, this is not always true: we have, e.g., $\mathcal{C}(\Phi^*_{2^4\cdot 3^2\cdot 5^2\cdot 7}) = \{-49, \ldots, 44\}\backslash\{-48, -47, -45, -43, 40, 42, 43\}$.

In practice both the upper and lower bound in (19) are often assumed, here we give just two examples.

- Let $p = 2^2$, $q = 5$, $s = 3$, $r = 23$. Then $r \equiv s \pmod{pq}$ and $r > \max(p, q) > s = 3$. We have $H(\Phi^*_{pqs}) = H(\Phi^*_{pqr}) = 2$.
- Let $p = 3^2$, $q = 7$, $s = 5$, $r = 131$. Then $r \equiv s \pmod{pq}$ and $r > \max(p, q) > s > 3$. We have $H(\Phi^*_{pqr}) = H(\Phi^*_{pqs}) + 1 = 3$.

We do not know of any simple criteria that can be used to determine which of the two bounds must hold.

Acknowledgment. This paper is partly based on the outcome of a student project by Greyson Jones, Philip Kester and Brenden White that they carried out under the direction of Lilit Martirosyan at the University of North Carolina in Wilmington. The authors thank Gennady Bachman, Alexandru Ciolan and Andrés Herrera-Poyatos for helpful feedback on earlier verions.

References

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

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

[3] A. S. Bang, Om Ligningen $\phi_n(x) = 0$, *Nyt Tidsskr. Math.* (B) **6** (1895), 6–12.

[4] L. Bardomero and M. Beck, Frobenius coin-exchange generating functions, *Amer. Math. Monthly*, to appear, https://arxiv.org/abs/1901.00554.

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

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

[7] H. Hong, E. Lee, H.-S. Lee and C.-M. Park, Maximum gap in (inverse) cyclotomic polynomial, *J. Number Theory* **132** (2012), 2297–2315.

[8] C.-G. Ji, W.-P. Li, Values of coefficients of cyclotomic polynomials, *Discrete Math.* **308** (2008), 5860–5863.

[9] C.-G. Ji, W.-P. Li and P. Moree, Values of coefficients of cyclotomic polynomials II, *Discrete Math.* **309** (2009), 1720–1723.

[10] N. Kaplan, Flat cyclotomic polynomials of order three, *J. Number Theory* **127** (2007), 118–126.

[11] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.

[12] A. Migotti, Zur Theorie der Kreisteilungsgleichung, *S.-B. der Math.-Naturwiss. Classe der Kaiserlichen Akademie der Wissenschaften, Wien,* (2) **87** (1883), 7–14.

[13] P. Moree, Inverse cyclotomic polynomials, *J. Number Theory* **129** (2009), 667–680.

[14] P. Moree, Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers, *Amer. Math. Monthly* **121** (2014), 890–902.

[15] P. Moree and L. Tóth, Unitary cyclotomic polynomials, preprint.

[16] J. L. Ramírez–Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications **30**, Oxford University Press, Oxford, 2005.

[17] J. Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* **63** (1987), 279–280.

[18] L. A. Székely and N. C. Wormald, Generating functions for the Frobenius problem with 2 and 3 generators, *Math. Chronicle* **15** (1986), 49–57.

Greyson Jones, Philip Isaac Kester, Brenden Blake White
e-mails: rgj5866@uncw.edu, pk7312@uncw.edu, bbw7810@uncw.edu

Lilit Martirosyan
University of North Carolina, Wilmington
Department of Mathematics and Statistics
601 South College Road
Wilmington NC 28403-5970, USA.
e-mail: martirosyanl@uncw.edu

Pieter Moree
Max-Planck-Institut für Mathematik
Vivatsgasse 7, 53111 Bonn, Germany
E-mail: moree@mpim-bonn.mpg.de

László Tóth
Department of Mathematics
University of Pécs
Ifjúság útja 6, 7624 Pécs, Hungary
E-mail: ltoth@gamma.ttk.pte.hu

Bin Zhang
School of Mathematical Sciences
Qufu Normal University
Qufu 273165, P. R. China
E-mail: zhangbin100902025@163.com