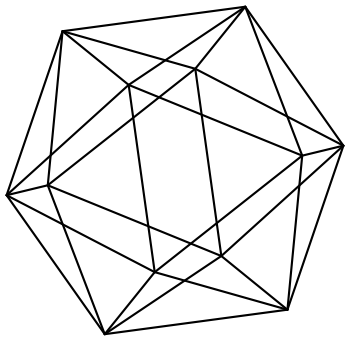
Max-Planck-Institut für Mathematik
Bonn

Coefficient convexity of divisors of $x^n - 1$

by

Andreas Decker
Pieter Moree



Max-Planck-Institut für Mathematik
Preprint Series 2010 (92)

Coefficient convexity of divisors of $x^n - 1$

Andreas Decker
Pieter Moree

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Achtern Diek 32
49377 Vechta
Germany

MPIM 10-92

Coefficient convexity of divisors of $x^n - 1$

Andreas Decker and Pieter Moree

Abstract

We say a polynomial $f \in \mathbb{Z}[x]$ is *strongly coefficient convex* if the set of coefficients of f consists of consecutive integers only. We establish various results suggesting that the divisors of $x^n - 1$ that are in $\mathbb{Z}[x]$ have the tendency to be strongly coefficient convex and have small coefficients. The case where $n = p^2q$ with p and q primes is studied in detail.

1 Introduction

Let $f(x) = \sum_{j=0}^{\infty} c_j x^j$ be a polynomial. We put $\mathcal{C}_0(f) = \{c_j\}$. Trivially $\mathcal{C}_0(f) = \mathcal{C}(f) \cup \{0\}$, where $\mathcal{C}(f) = \{c_j : 0 \leq j \leq \deg(f)\}$ denotes the set of coefficients of f. If there exist integers a and b such that $\mathcal{C}_0(f)$ consists of the consecutive integers $a, a+1, \ldots, b-1, b$, then we say that f is *coefficient convex* and write $\mathcal{C}_0(f) = [a, b]$. If $\mathcal{C}(f) = [a, b]$, then we say that f is *strongly coefficient convex*. We say that f is *flat* if $\mathcal{C}(f) \subseteq [-1, 1]$. Note that if f is flat, then f is also coefficient convex. Typically we denote polynomial coefficients by c_j and d_j.

The nth cyclotomic polynomial $\Phi_n(x)$ (see the next section for details) has the property that its coefficients tend to be small in absolute value, e.g., for $n < 105$ it is flat. If n has at most three distinct odd prime factors, it can be shown [5] that Φ_n is coefficient convex. Since $\Phi_n(x)$ is a polynomial divisor of $x^n - 1$ the question arises what one can say about the flatness of the other divisors of $x^n - 1$, the size of their coefficients and coefficient convexity. Since the number of divisors of $x^n - 1$ rapidly increases, we are only able to say something conclusive in case n has a modest number of divisors. If $n = pq$ or $n = p^2q$, then $x^n - 1$ has 16, respectively 64 monic divisors (these cases are covered by Theorems 2, 3, 4 and 5).

An exception here is the case where n is a prime power, say $n = p^e$. Then the number of divisors can get large, but they have a simple structure. Using the uniqueness of the base p representation Pomerance and Ryan [11] proved that the divisors of $x^{p^e} - 1$ are all flat. We leave it to the reader to prove the following easy strengthening of this result.

Theorem 1 *Let $e \geq 1$ be an integer and g be a monic divisor of $x^{p^e} - 1$. We have $\mathcal{C}(g) = \{1\}$ if $g = (x^{p^j} - 1)/(x - 1)$ for some $0 \leq j \leq e$. Furthermore, if $p = 2$*

Mathematics Subject Classification (2000). 11B83, 11C08
Keywords and phrases. cyclotomic polynomials, coefficient sets of polynomials

and $g = (x-1)(x^{2^j}-1)/(x^2-1)$*, then for* $1 \le j \le e$ *we have* $\mathcal{C}(g) = \{-1, 1\}$*. In the remaining cases we have*

$$\mathcal{C}(g) = \begin{cases} [0,1] & \text{if } x-1 \nmid g; \\ [-1,1] & \text{if } x-1 | g. \end{cases}$$

Theorem 2 *Let* $p < q$ *be primes. Except for* $(x-1)\Phi_{pq}(x)$ *and* $\Phi_p(x)\Phi_q(x)$ *all monic divisors of* $x^{pq}-1$ *are flat. The set of coefficients of* $(x-1)\Phi_{pq}(x)$ *is of the form* $\{-2,-1,1,2\}$ *if* $p \le 3$ *and* $\{-2,-1,0,1,2\}$ *otherwise. The set of coefficients of* $\Phi_p(x)\Phi_q(x)$ *is* $\{1, \ldots, \min(p,q)\}$*.*

Corollary 1 *All divisors* $f \in \mathbb{Z}[x]$ *of* $x^{pq}-1$ *are coefficient convex.*

Theorem 3 *Let* p *and* q *be distinct primes. Then the monic polynomial divisors of* $x^{p^2q}-1$ *are coefficient convex, with the exception (in case* $q = 2$*),* $(x+1)\Phi_p\Phi_{2p^2}$*, where the coefficient set equals* $\{-2,0,1,2\}$*. If* $\min(p,q) > 3$*, then all monic divisors - except* $x-1$ *- are strongly coefficient convex.*

Pomerance and Ryan [11] conjectured and Kaplan [7] proved that the maximum coefficient that occurs amongst all monic divisors of $x^{p^2q}-1$ equals $\max(p^2, q)$. Letting $B_+(n)$ denote the maximum amongst all the coefficients of all the monic divisors, and $-B_-(n)$ the minimum, we have the following generalization of Kaplan's result.

Theorem 4 *Let* p *and* q *be distinct primes. Let* $1 \le p^* \le q-1$ *be the inverse of* p *modulo* q*. We have* $B_-(p^2q) = \min(p, p^*) + \min(p, q-p^*)$ *and* $B_+(p^2q) = \min(p^2, q)$

Note that if $q < p$, then the result gives $B_-(p^2q) = B_+(p^2q) = q$. (For a more formal definition of $B_\pm(n)$ see Section 4.) The analogue of the latter theorem in case $n = pqr$ is not known, for some partial results see Kaplan [7]. Ryan et al. [14] posed some conjectures on the basis of extensive numerical calculation.

The results stated above (except for Theorem 1) are special cases of Theorem 5, our main result, e.g., Theorem 2 can be read off from Table 1A. In the derivation of Theorem 4 we have to use in addition that $\min(p, p^*) + \min(p, q-p^*) \ge \min(p, q)$. A 'tableless' reformulation of Theorem 5 is given in Section 3.1.

Theorem 5 *Let* p *and* q *be distinct primes. Let* $f(x) \in \mathbb{Z}[x]$ *be a monic divisor of* $x^{p^2q}-1$*. Then there exists an integer* $0 \le k \le 63$ *such that*

$$f(x) = f_k(x) = \Phi_1^{k_0}\Phi_p^{k_1}\Phi_q^{k_2}\Phi_{pq}^{k_3}\Phi_{p^2}^{k_4}\Phi_{p^2q}^{k_5},$$

with $0 \le k_j \le 1$ *and* $k = \sum_{j=0}^{5} k_j 2^j$ *the binary expansion of* k*. The set of coefficients of* f_k*,* $\mathcal{C}(f_k)$*, is given in Table* 1*.*

The difficulty of computing $\mathcal{C}(f)$ varies rather dramatically; from utterly trivial to challenging in case of f_{25}, f_{38} and f_{43}..

2 Preliminaries

The nth cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \sum_{k=0}^{\varphi(n)} a_n(k)x^k = \prod_{d|n}(x^d - 1)^{\mu(n/d)}, \tag{1}$$

where $\mu(n)$ is the Möbius function and $\varphi(n)$ Euler's totient function. Let $p \neq q$ be primes. From (1) we deduce, e.g., that

$$\Phi_{pq}(x) = \frac{(x-1)(x^{pq}-1)}{(x^p-1)(x^q-1)}, \tag{2}$$

a formula that will be used repeatedly.

We will need the following elementary properties of $\Phi_n(x)$ (see, e.g., Thangadurai [15] for proofs and a nice introduction to cyclotomic polynomials). Throughout we use the letters p and q to denote primes.

Lemma 1
1) $\Phi_n(x) \in \mathbb{Z}[x]$.
2) $\Phi_n(x)$ *is irreducible over the rationals.*
3) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
4) $\Phi_p(x) = (x^p - 1)/(x - 1) = 1 + x + \ldots + x^{p-1}$.
5) *If* $p|n$, *then* $\Phi_{pn}(x) = \Phi_n(x^p)$.
6) *If* $n > 1$ *is odd, then* $\Phi_{2n}(x) = \Phi_n(-x)$.
7) *For all positive integers* $n > 1$, *we have* $\Phi_n(1/x)x^{\phi(n)} = \Phi_n(x)$, *that is* $\Phi_n(x)$ *is* `self-reciprocal`.

For a nonzero polynomial $f \in \mathbb{C}[x]$, we define its *height* $H(f)$ to be the largest coefficient of f in absolute value. For a nonzero polynomial $f \in \mathbb{R}[x]$, we define $H_+(f)$, respectively $H_-(f)$ to be the largest, respectively smallest coefficient of f. (In that case $H(f) = \max\{H_+(f), |H_-(f)|\}$.) As in [11], the observation that if $H(f) = m$, then $H((x^k - 1)f(x)) \leq 2m$ for any positive integer k will be used a few times. We also use that if $f, g \in \mathbb{Z}[x]$ with $\deg(f) \leq \deg(g)$, then

$$H(fg) \leq (1 + \deg(f))H(f)H(g). \tag{3}$$

Another easy observation we need is that if $k > \deg(f)$, and $m \geq 1$ is an arbitrary integer, then

$$\mathcal{C}_0(f(x)(1 + x^k + x^{2k} + \cdots + x^{km})) = \mathcal{C}_0(f). \tag{4}$$

If $k > \deg(f) + 1$, then $\mathcal{C}(f(x)(1 + x^k + x^{2k} + \cdots + x^{km})) = \mathcal{C}(f) \cup \{0\}$. A closely related observation is that

$$\mathcal{C}(\Phi_p(x)f(x^p)) = \mathcal{C}(f). \tag{5}$$

To see this note that if in the coefficient string of f we replace each coefficient by its p-fold repetition, we get the coefficient string of $\Phi_p(x)f(x^p)$.

2.1 Binary cyclotomic polynomials

In this subsection we consider the binary cyclotomic polynomials $\Phi_{pq}(x)$ with p and q distinct primes.

In 1883 Migotti proved that Φ_{pq} is flat. Carlitz [3] noted that if we drop the zero coefficients in $\Phi_{pq}(x)$, the positive and negative terms occur alternately, as, e.g., in

$$\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1.$$

(To prove this, one can invoke Lemma 3 below together with (2)). Lenstra [9] (see also Lam and Leung [8]) gave an explicit description of the coefficients of $\Phi_{pq}(x)$.

Lemma 2 *Let p and q be distinct odd primes. Let ρ and σ be the (unique) non-negative integers for which $1 + pq = (\rho + 1)p + (\sigma + 1)q$. Let $0 \le m < pq$. Then either $m = \alpha_1 p + \beta_1 q$ or $m = \alpha_1 p + \beta_1 q - pq$ with $0 \le \alpha_1 \le q - 1$ the unique integer such that $\alpha_1 p \equiv m (\mathrm{mod}\ q)$ and $0 \le \beta_1 \le p - 1$ the unique integer such that $\beta_1 q \equiv m (\mathrm{mod}\ p)$. The cyclotomic coefficient $a_{pq}(m)$ equals*

$$\begin{cases} 1 & \text{if } m = \alpha_1 p + \beta_1 q \text{ with } 0 \le \alpha_1 \le \rho,\ 0 \le \beta_1 \le \sigma; \\ -1 & \text{if } m = \alpha_1 p + \beta_1 q - pq \text{ with } \rho + 1 \le \alpha_1 \le q - 1,\ \sigma + 1 \le \beta_1 \le p - 1; \\ 0 & \text{otherwise.} \end{cases}$$

The latter lemma does not include the case where $p = 2$ and q is odd. However, by Lemma 1 we have $\Phi_{2q}(x) = \Phi_q(-x) = 1 - x + x^2 - \cdots + x^{q-1}$.

2.2 Inverse cyclotomic polynomials

We define $\Psi_n(x) = (x^n - 1)/\Phi_n(x) = \sum_{k=0}^{n-\varphi(n)} c_n(k)x^k$ to be the nth *inverse cyclotomic polynomial*. It is easy to see, see, e.g., Moree [10], that $\Psi_1(x) = 1$, $\Psi_p(x) = x - 1$ and

$$\Psi_{pq}(x) = -1 - x - x^2 - \ldots - x^{p-1} + x^q + x^{q+1} + \ldots + x^{p+q-1}. \tag{6}$$

For $n < 561$ the polynomials $\Psi_n(x)$ are flat. Let $2 < p < q < r$ be odd primes. It is not difficult to show that $|c_{pqr}(k)| \le [(p-1)(q-1)/r] + 1 \le p - 1$. Let us call a ternary inverse cyclotomic polynomial $\Psi_{pqr}(x)$ extremal if for some k we have $|c_{pqr}(k)| = p-1$. Moree [10] showed that a ternary inverse cyclotomic polynomial is extremal iff

$$q \equiv r \equiv \pm 1 (\mathrm{mod}\ p) \text{ and } r < \frac{(p-1)}{(p-2)}(q-1).$$

Moreover, he showed that for an extremal ternary inverse cyclotomic polynomial $\Psi_{pqr}(x)$ one has $\mathcal{C}(\Psi_{pqr}) = [-(p-1), p-1]$, and thus that they are strongly coefficient convex.

2.3 Inclusion-exclusion polynomials

Let $\rho = \{r_1, r_2, \ldots, r_s\}$ be a set of natural numbers satisfying $r_i > 1$ and $(r_i, r_j) = 1$ for $i \ne j$, and put

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

For each such ρ we define a function Q_ρ by

$$Q_\rho(x) = \frac{(x^{n_0}-1)\prod_{i<j}(x^{n_{i,j}}-1)\cdots}{\prod_i(x^{n_i}-1)\prod_{i<j<k}(x^{n_{i,j,k}}-1)\cdots}$$

It turns out that Q_ρ is a polynomial, the inclusion-exclusion polynomial. This class of divisors of $x^{n_0}-1$ was introduced by Bachman [1]. He showed that with $D_\rho = \{d : d|n_0 \text{ and } (d, r_i) > 1 \text{ for all } i\}$, we have $Q_\rho(x) = \prod_{d\in D}\Phi_d(x)$. Furthermore, he showed that ternary ($s = 3$) inclusion-exclusion polynomials are coefficient convex. Earlier Gallot and Moree [5] (for alternative proofs, see Bzdęga [2] and Rosset [13]) had shown that in case $s = 3$ and r_1, r_2, r_3 are distinct primes, this result is true.

2.4 On the coefficient convexity of Φ_n and Ψ_n

In [5] Theorems 7 and 8 were announced and it was promised that the present paper would contain the proofs. Here this promise is fulfilled.

In [5] the following result was established. (Its analogue for Ψ_n is false in general.)

Theorem 6 *Let n be ternary, that is $n = pqr$ with $2 < p < q < r$ odd primes. Then, for $k \geq 1$, $|a_n(k) - a_n(k-1)| \leq 1$.*

It follows that if n is ternary, then Φ_n is strongly coefficient convex. Using the latter result one easily proves the following one.

Theorem 7 *Suppose that n has at most 3 distinct prime factors, then Φ_n is coefficient convex.*

Proof. In case n has at most two distinct odd factors, by Lemma 2 and Lemma 1 we infer that Φ_n is flat and hence coefficient convex. Now suppose that n is odd. Let $\kappa(n) = \prod_{p|n} p$ be the squarefree kernel of n. Then, by part 4 of Lemma 1 we have $\mathcal{C}(\Phi_n) = \mathcal{C}(\Phi_{\gamma(n)}) \cup \{0\}$ if $\kappa(n) < n$. The proof is now completed on invoking Theorem 6. □

Numerical computation suggest that if Φ_n is ternary, then Φ_{2n} is coefficient convex. If this would be true, then in Theorem 7 one can replace '3 distinct prime factors' by '3 distinct odd prime factors'. This is best possible as the following examples show:
$n = 7735 = 5 \cdot 7 \cdot 13 \cdot 17, \quad \mathcal{C}(n) = [-7, 5] - \{-6\}$
$n = 530689 = 17 \cdot 19 \cdot 31 \cdot 53, \quad \mathcal{C}(n) = [-50, 52]\backslash\{-48, 47, 48, 49, 50, 51\}$.

Theorem 8 *Suppose that n has at most 2, respectively 3, distinct odd prime factors, then Ψ_n is flat, respectively, coefficient convex.*

Proof. If $p|n$, then $\Psi_{pn}(x) = \Psi_n(x^p)$. Thus we may restrict to the case where n is squarefree. If $n = 1$, then $\Psi_1 = 1$. If n is a prime, then $\Psi_n = x - 1$. If n is composed of two primes, $n = pq$, with $p < q$, then

$$\Psi_{pq} = -1 - x - x^2 - \cdots - x^{p-1} + x^q + x^{q+1} + \cdots + x^{p+q-1}.$$

If $2 < p < q$, then $\Psi_{2pq} = (1 - x^{pq})\Psi_{pq}(-x)$. Note that the degree of Ψ_{pq} is smaller than pq and since $\Psi_{pq}(-x)$ is flat, it follows that Ψ_{2pq} is flat. We conlude that if n has at most two distinct odd prime factors, then Ψ_n is flat. It remains to consider the case where $n = pqr$, $2 < p < q < r$, repectively $n = 2pqr$ with $2 < p < q < r$.
Case 1. $n = pqr$. We have $\Psi_{pqr}(x) = \Phi_{pq}(x)\Psi_{pq}(x^r)$. From this identity we infer that

$$c_{pqr}(k) = \sum_{j=0}^{[k/r]} a_{pq}(k - jr)c_{pq}(j).$$

Put $V_n = \{c_n(k) : 0 \le k \le n - \varphi(n)\}$. Choose k_1 such that $c_{pqr}(k_1) = \max V_{pqr} = \mu_+$. Then since $|a_{pq}(k-jr)c_{pq}(j)| \le 1$, we infer that $\{1, \dots, \mu_+\} \subseteq \{c_{pqr}(k_1 - jr) : 0 \le j \le [k_1/r]\}$. Similarly one choses k_2 such that $c_{pqr}(k_1) = \min V_{pqr} = \mu_-$ and finds that $\{\mu_-, \dots, -1\} \subseteq \{c_{pqr}(k_2 - jr) : 0 \le j \le [k_2/r]\}$ and hence $V_{pqr} = \{\mu_-, \dots, \mu_+\}$ (by [10, Lemma 3] we have $0 \in V_{pqr}$). Thus Φ_{pqr} is coefficient convex.
Case 2. $n = 2pqr$. A small modification of the above argument gives that $\Psi_{pqr}(-x)$ is coefficient convex. Using that $\Psi_{2n}(x) = (1 - x^n)\Psi_n(-x)$ if n is odd and that $n > n - \varphi(n) = \deg(\Psi_n)$, we infer that also Ψ_{2pqr} is coefficient convex.
Thus the proof is completed. □

Gallot considered the coefficient convexity of Ψ_n for many n and found that the smallest n for which it is non-convex is $n = 23205 = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$. Here the height is 13, but 12 (and -12) are not included in $\mathcal{C}(\Psi_n)$. Further examples (in order of appearance) are 46410 (height 13, ± 12 not there), 49335 (height 34, ± 33 not found), 50505 (height 15, ± 14 not found). There are also examples where a whole range of values smaller than the height is not in $\mathcal{C}(\Psi_n)$.

2.5 Auxiliary polynomials

In this subsection we determine $\mathcal{C}(f)$ for various auxiliary polynomials f (where possible we have adopted the notation of Theorem 5).

Lemma 3 *Let $u > 1$ and $v > 1$ be coprime natural numbers. Put*

$$\tau_{u,v}(x) = \frac{(x-1)(x^{uv}-1)}{(x^u-1)(x^v-1)}.$$

Then $\tau_{u,v}(x) \in \mathbb{Z}[x]$ is a self-reciprocal flat divisor of $x^{uv} - 1$. If $1 < u < v$, then

$$\mathcal{C}(\tau_{u,v}) = \begin{cases} \{-1, 1\} & \text{if } u = 2; \\ [-1, 1] & \text{otherwise.} \end{cases}$$

The non-negative coefficients of $\tau_{u,v}$ alternate in sign.

Proof. The assumption on u and v ensures that $(x^u - 1, x^v - 1) = x - 1$. Using this assumption we infer that $\tau_{u,v}(x) \in \mathbb{Z}[x]$. That $\tau_{u,v}(x)$ is a self-reciprocal divisor of $x^{uv} - 1$ is obvious. We claim that all coefficients r_j with $j < uv$ in $(1 + x^u + x^{2u} + \cdots)(1 + x^v + x^{2v} + \cdots) = \sum r_j x^j$ are in $\{0, 1\}$. Now if

$r_j \geq 2$ and $j < uv$, we can find non-negative $\alpha_1, \alpha_2, \beta_1$ and β_2 such that $j = \alpha_1 u + \beta_1 v = \alpha_2 u + \beta_2 v$, with $\alpha_1 \neq \alpha_2$ both smaller than v. The latter equality implies however $v|(\alpha_1 - \alpha_2)$. This contradiction completes the proof of the claim. It follows that $\mathcal{C}(\tau_{u,v}) \in \{-1, 0, 1\}$ and that the non-negative signs alternate. The claim regarding $\mathcal{C}(\tau_{u,v})$ follows on noting that $\tau_{u,v} = (x^v+1)/(x+1)$ if $u = 2$ and $\tau_{u,v} \equiv 1 - x (\mathrm{mod}\ x^3)$ if $u \geq 3$. □

`Remark`. Given relatively prime positive integers $a_1, \ldots, a_n$ there is a largest number $g(a_1, \ldots, a_n)$, called the *Frobenius number*, that is not representable as a non-negative integer combination of $a_1, \ldots, a_n$. Let $n = 2$ and a_1 and a_2 be coprime. Using properties of $\tau_{a_1,a_2}(x)$ it is shown at p. 34 in [12] that $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$. It is no coincidence that deg $\tau_{u_1,u_2} = g(u_1, u_2) + 1$, see e.g., [5, Section 2].

In case $p = 3$, the next lemma shows that $\tau_{3,v}(x)$ can be easily explicitly given.

Lemma 4 *If $v \equiv 1 (\mathrm{mod}\ 3)$, then $\tau_{3,v}(x)$ equals*

$$(1-x)(1 + x^3 + x^6 + \cdots + x^{v-1}) + x^v + (x-1)(x^{v+1} + x^{v+4} + \cdots + x^{2v-3}).$$

If $v \equiv 2 (\mathrm{mod}\ 3)$, then $\tau_{3,v}(x)$ equals

$$(1-x)(1 + x^3 + x^6 + \cdots + x^{v-2}) + x^v + (x-1)(x^{v+2} + x^{v+5} + \cdots + x^{2v-3}).$$

Proof. Let us denote the polynomial above by $f_v(x)$. Modulo x^v we have

$$\tau_{3,v}(x) = \frac{(x-1)(x^{3v}-1)}{(x^3-1)(x^v-1)} \equiv (1-x)(1 + x^3 + x^6 + \cdots).$$

We infer that $f_v(x) \equiv \tau_{3,v}(x) (\mathrm{mod}\ x^v)$. To finish the proof it is enough to show that $f_v(x)$ is self-reciprocal (clearly $\tau_{3,v}(x)$ is self-reciprocal). That is, we have to show that $f_v(1/x)x^{2(v-1)} = f_v(x)$. That this is the case is easily seen on rewriting $f_v(x)$, in case $v \equiv 1 (\mathrm{mod}\ 3)$ as

$$(1-x)(1 + x^3 + x^6 + \cdots + x^{v-4}) + x^{v-1} + (x-1)(x^{v+1} + x^{v+4} + \cdots + x^{2v-3}),$$

and as

$$(1-x)(1 + x^3 + x^6 + \cdots + x^{v-2}) + x^{v-1} + (x-1)(x^{v-1} + x^{v+2} + \cdots + x^{2v-3}),$$

in case $v \equiv 2 (\mathrm{mod}\ 3)$. □

The latter lemma shows that identical consecutive coefficients do not appear in $\tau_{3,v}(x)$ if $(3, v) = 1$. The following lemma determines all polynomials $\tau_{3,v}(x)$ with this property.

Lemma 5 *Let $1 < u < v$ be coprime integers. Consecutive coefficients of $\tau_{u,v}(x)$ are always distinct iff $u \leq 3$.*

Corollary 2 *We have $0 \in \mathcal{C}((x-1)\tau_{u,v}(x))$ iff $u > 3$.*

Proof. If $u = 2$ we have $\tau_{2,v}(x) = (x^v + 1)/(x + 1)$ and so consecutive coefficients are always distinct. If $u = 3$ it is seen from Lemma 4 that this property also holds. Proceding as in the proof of Lemma 4 we find that modulo x^v we have $\tau_{u,v}(x) \equiv (1 - x)(1 + x^u + x^{2u} + \cdots)$ and hence, if $u \geq 4$, the second and third coefficient of $\tau_{u,v}(x)$ both equal zero. □

Lemma 6 *Let $1 < u < v$ be coprime numbers. Put $h = (x - 1)\tau_{u,v}(x)$. We have*

$$\mathcal{C}(h) = \begin{cases} \{-2, -1, 1, 2\} & \text{if } u \leq 3; \\ \{-2, -1, 0, 1, 2\} & \text{otherwise.} \end{cases}$$

Proof. Put $d = (u - 1)(v - 1)$. Using the self-reciprocity of $\tau_{u,v}(x)$ we infer that $h(x) = x^d - x^{d-1} + \cdots - x + 1$. On writing $h = \sum_j c_j x^j$, we now deduce that $c_0 = -1$, $c_1 = 2$, $c_d = -2$ and $c_{d+1} = 1$. Since clearly $\mathcal{C}(h) \subseteq [-2, 2]$ (use Lemma 3), we infer that

$$\{-2, -1, 1, 2\} \subseteq \mathcal{C}(h) \subseteq \{-2, -1, 0, 1, 2\}.$$

On invoking Corollary 2, the proof is then completed. □

Lemma 7 *Let u, v be natural numbers. Put*

$$\sigma_{u,v}(x) = \frac{(x^u - 1)}{(x - 1)} \frac{(x^v - 1)}{(x - 1)} = \sum_{j=0}^{u+v-2} c_j x^j$$

W.l.o.g. assume that $u \leq v$. We have

$$c_j = \begin{cases} j + 1 & \text{if } 0 \leq j \leq u - 1; \\ u & \text{if } u \leq j \leq v - 1; \\ v + u - j - 1 & \text{if } v \leq j \leq v + u - 2. \end{cases}$$

It follows that $\mathcal{C}(\sigma_{u,v}) = \{1, \ldots, u\}$. If $(u, v) = 1$, then $\sigma_{u,v}(x) | x^{uv} - 1$.

Corollary 3 *If $u < v$, then $\mathcal{C}((x - 1)\sigma_{u,v}(x)) = [-1, 1]$.*

Corollary 4 *If $(u, v) = 1$, then $B(uv) \geq B_+(uv) = \min(u, v)$.*

Corollary 5 *Put $f_{22} = \Phi_p \Phi_q \Phi_{p^2}$. Then $\mathcal{C}(f_{22}) = [1, \min(p^2, q)]$.*

Proof. Modulo x^u we have

$$\sigma_{u,v}(x) \equiv \frac{1}{(1 - x)^2} \equiv \sum_{j=1}^{u} j x^{j-1} (\text{mod } x^u),$$

showing that $c_j = j + 1$ if $0 \leq j \leq u - 1$. That $c_j = u$ if $u \leq j \leq v - 1$ is obvious. Using that $\sigma_{u,v}$ is self-reciprocal, it then follows that $c_j = v + u - j - 1$ if $v \leq j \leq v + u - 2$.

If $(u, v) = 1$, then $((x^u - 1)/(x - 1), (x^v - 1)/(x - 1)) = 1$ and using this we infer that $\sigma_{u,v}(x) | x^{uv} - 1$. □

Lemma 8 *Let p and q be distinct primes. Put $f_{20} = \Phi_q \Phi_{p^2}$ We have*

$$\mathcal{C}(f_{20}) = \begin{cases} \{1, \ldots, \min([\frac{q-1}{p}] + 1, p)\} & \text{if } p < q; \\ \{0, 1\} & \text{if } p > q. \end{cases}$$

In particular, f_{20} is flat iff $p > q$.

Proof. Left as an exercise to the interested reader. □

Lemma 9 *Let a, b, c be positive integers. Put*

$$g_{a,b,c}(x) = (1 + x + \ldots + x^{a-1} + 2x^a + \ldots + 2x^{a+b-1})(1 + x + x^2 + \ldots + x^{c-1}).$$

Alternatively one can write

$$g_{a,b,c}(x) = \Big(\frac{2x^{a+b} - x^a - 1}{x - 1}\Big)\Big(\frac{x^c - 1}{x - 1}\Big).$$

Suppose a is odd. Then $g(= g_{a,b,c})$ is coefficient convex. We have $\mathcal{C}(g) = [1, \mu]$, with

$$\mu = \begin{cases} 2c & \text{if } c \leq b; \\ \min(b + c, a + 2b) & \text{if } c > b. \end{cases}$$

Corollary 6 *Put $\overline{g} = x^{a+b+c-2} g_{a,b,c}(1/x)$. We have*

$$\overline{g} = \overline{g}_{a,b,c} = \Big(\frac{x^{a+b} + x^b - 2}{x - 1}\Big)\Big(\frac{x^c - 1}{x - 1}\Big).$$

If a is odd, then $\overline{g}$ is coefficient convex and $\mathcal{C}(\overline{g}) = \{1, \ldots, \mu\}$.

Proof. To find the maximum coefficient of g is easy. It is the coefficient convexity that is slightly less trivial. Write $g = \sum_{j=0}^{a+b+c-2} d_j x^j$. We consider two cases.
Case 1. $c \geq a + b$. We have to show that all coefficients $1, 2, \ldots, \mu$, where $\mu = a + 2b$, occur. It is easy to see that $\{d_0, \ldots, d_{a+b-1}\}$ contains all odd number $\leq \mu$ (here we use the assumption that a is odd). Likewise one sees that $\{d_c, \ldots, d_{a+b+c-2}\}$ contains all even integers $\leq \mu$.
Case 2. $c < a + b$. Here we proceed by induction with respect to c. For $c = 1$ we have 1 and 2 as coefficients and we are done. Suppose the result is true up to c_1. We want to show it for $c = c_1 + 1$. Here at most two new coefficient values can arise, namely the previous maximum, μ_{c_1}, with 1 added and the previous maximum with 2 added. In the latter case (which only arises if $c \leq b$) we have to show that $\mu_{c_1} + 1$ also occurs as coefficient. The coefficient of $d_{a+c-1} = 2c$ is the new maximum here. Note that $d_{a+c-2} = 2c - 1$. Thus using the induction hypothesis the set of coefficients equals $\{1, 2, \ldots, \mu_{c_1}, \mu_{c_1} + 1, \mu_{c_1} + 2\}$ and is hence coefficient convex. □

By $[f]_{x^k}$ we denote the coefficient of x^k in f.

Lemma 10 *Let p and q be distinct primes. Put $f_{24} = \Phi_{pq} \Phi_{p^2}$. Let $1 \leq p^* \leq q - 1$ be the inverse of p modulo q. Write $f_{24} = \sum_j c_j x^j$.*
1) *We have*

$$\mathcal{C}(f_{24}) = \begin{cases} \{-\min(q - p^*, p), \ldots, \min(p^*, p)\} & \text{if both } p \text{ and } q \text{ are odd;} \\ \{-\min(q - p^*, p), \ldots, \min(p^*, p)\} \backslash \{0\} & \text{otherwise.} \end{cases}$$

In particular, f_{24} is flat iff $q = 2$.
2) *Let $k \geq 0$ and $\min(p, q) > 2$. We have $c_{1+kp} = -[\sigma_{q-p^*,p}(x)]_{x^k}$ and $c_{kp} = [\sigma_{p^*,p}(x)]_{x^k}$. If $2p^* < q$, then $c_{2+kp} = [x^{q-2p^*}\sigma_{p^*,p}(x)]_{x^k}$. If $2p^* > q$, then $c_{-1+kp} = -[x^{2p^*-q}\sigma_{q-p^*,p}(x)]_{x^k}$.*

Proof. 1) The case where p or q is even is left to the reader. So let us assume that both p and q are odd. The kth coefficient, c_k, in f equals

$$\sum_{0\leq k-jp<pq,\ 0\leq j\leq p-1} a_{pq}(k-jp).$$

Since this is a sum of binary cyclotomic coefficients by Lemma 2 we have

$$-(q-1-\rho) \leq c_k \leq \rho+1 \text{ and } -p \leq c_k \leq p.$$

On noting that $\rho + 1 = p^*$ we thus obtain that $-m_2 \leq c_j \leq m_1$ with $m_2 = \min(q-p^*, p)$ and $m_1 = \min(p^*, p)$. Using Lemma 2 we obtain that $c_{jp} = \sum_{j_1=0}^{j} a_{pq}(j_1 p) = j+1$ for $0 \leq j \leq m_1 - 1$. Likewise we find on using that $1 = (\rho+1)p + (\sigma+1)q - pq$ that $c_{jp+1} = -j-1$ for $0 \leq j \leq m_2 - 1$. Since $f_{24} \equiv 1 - x (\mathrm{mod}\ x^3)$, it follows that $0 \in \mathcal{C}(f_{24})$.
2) Note that c_{1+kp} is the coefficient of x^{1+kp} in

$$\Phi_p(x^p) \sum_{0\leq j<q} a_{pq}(1+jp)x^{1+jp}.$$

Using Lemma 2 we then infer that the latter polynomial equals

$$-x\Big(\frac{x^{p(q-p^*)}-1}{x^p-1}\Big)\Big(\frac{x^{p^2}-1}{x^p-1}\Big).$$

It follows that c_{1+kp} is the coefficient of x^k in $-\sigma_{q-p^*,p}(x)$. A similar argument implies $c_{kp} = [\sigma_{p^*,p}(x)]_{x^k}$. From $1 + pq = p^*p + q^*q$ we obtain $2 = 2p^*p + (2q^* - p)q - pq$. The assumption $2p^* < q$ implies $q^* > p/2$ and hence $1 \leq 2p^* < q$ and $1 \leq 2q^* - p < q^*$. Reasoning as before we then find that c_{2+kp} is the coefficient of x^k in $x^{q-2p^*}\sigma_{p^*,p}(x)$. Likewise the final assertion is established. □

Lemma 11 *Put $f_{25} = (x-1)\Phi_{pq}\Phi_{p^2}$. Define $\gamma(p,q) = \min(p,p^*)+\min(p,q-p^*)$. Suppose $\min(p,q) > 2$. Write $f_{25} = \sum d_j x^j$. We have $\{d_{1+kp}\}_{k=0}^{\infty} = [0, \gamma(p,q)]$. If $2p^* < q$, then $\{d_{2+kp}\}_{k=0}^{\infty} = [-\gamma(p,q), 0]$. If $2p^* > q$, then $\{d_{kp}\}_{k=0}^{\infty} = [-\gamma(p,q), 0]$.*

Proof. Using part 2 of Lemma 10 we find that $d_{1+kp} = c_{kp} - c_{1+kp} = [\sigma_{p^*,p}(x) + \sigma_{q-p^*,p}(x)]_{x^k}$. Note that

$$\tau(x) := \sigma_{p^*,p}(x) + \sigma_{q-p^*,p}(x) = \Big(\frac{x^{q-p^*}+x^{p^*}-2}{x-1}\Big)\Big(\frac{x^p-1}{x-1}\Big).$$

We have

$$\tau(x) = \begin{cases} \overline{g}_{q-2p^*,p^*,p}(x) & \text{if } q > 2p^*; \\ \overline{g}_{2p^*-q,q-p^*,p}(x) & \text{if } q < 2p^*. \end{cases}$$

On invoking Corollary 6 we then obtain, after an easy computation to verify that $\mu = \gamma(p,q)$, that $\{d_{1+kp}\}_{k=0}^{\infty} = \mathcal{C}(\tau) \cup \{0\} = [0, \gamma(p,q)]$.

Using part 2 of Lemma 10 and the assumption $q > 2p^*$, we find that

$$d_{2+kp} = -c_{2+kp} + c_{1+kp} = -[x^{q-2p^*}\sigma_{p^*,p}(x) + \sigma_{q-p^*,p}(x)]_{x^k}.$$

Now

$$x^{q-2p^*}\sigma_{p^*,p}(x) + \sigma_{q-p^*,p}(x) = \Big(\frac{2x^{q-p^*} - x^{q-2p^*} - 1}{x-1}\Big)\Big(\frac{x^p - 1}{x-1}\Big) = g_{q-2p^*,p^*,p}(x).$$

Using Lemma 9 we obtain that $\{d_{2+kp}\}_{k=0}^{\infty} = \mathcal{C}(-\tau) \cup \{0\} = [-\gamma(p,q), 0]$.

The proof of the final assertion is similar and left to the reader. □

Lemma 12 *Let $q > 3$ be a prime. Then the coefficients of the polynomial $g := (x-1)(1+x^3+x^6)\Phi_{3q}(x)$ are all non-zero.*

Proof. Since the polynomial under consideration is anti self-reciprocal, it suffices to show that $c_i \neq 0$ for $0 \leq i \leq q+2$. Using Lemma 4 we see that modulo x^q, we have $g \equiv (1-2x+x^2)h(x^3)$, where h is a polynomial with only negative coefficients. If $q \equiv 1 (\mathrm{mod}\ 3)$, then using Lemma 4 we find that $c_q = 5$, $c_{q+1} = -1$ and $c_{q+2} = -4$. For $q = 5$ one checks that c_5, c_6, c_7 are all non-zero. If $q > 5$ and $q \equiv 2 (\mathrm{mod}\ 3)$, one computes that $c_q = -4$, $c_{q+1} = -1$ and $c_{q+2} = 5$. □

Lemma 13 *Let $p > 3$ be a prime. Then $0 \in \mathcal{C}((x-1)\Phi_{3p}\Phi_{p^2})$.*

Proof. Put $f(x) = (x-1)\Phi_{3p}\Phi_{p^2}$. If $p \equiv 1 (\mathrm{mod}\ 3)$, then by Lemma 4 we find that

$$f(x) \equiv -(1-x)^2(1+x^3+\ldots+x^{p-4}) - x^{p-1} (\mathrm{mod}\ x^{p+1}),$$

and hence $c_p = 0$. If $p \equiv 2 (\mathrm{mod}\ 3)$, then by Lemma 4 we find that

$$f(x) \equiv -(1-x)^2(1+x^3+\ldots+x^{p-2}) - 2x^p + 3x^{p+1} (\mathrm{mod}\ x^{p+3}),$$

and hence $c_{p+2} = 0$. □

Lemma 14 *Put $f_{25} = (x-1)\Phi_{pq}\Phi_{p^2}$. Define $\gamma(p,q) = \min(p,p^*) + \min(p, q-p^*)$. Then*

$$\mathcal{C}(f_{25}) = \begin{cases} [-\gamma(p,q), \gamma(p,q)] \backslash \{0\} & \text{if } p \leq 3 \text{ and } q \neq 2; \\ [-\gamma(p,q), \gamma(p,q)] & \text{otherwise.} \end{cases}$$

In particular, f_{25} is never flat.

Proof. Note that if $\mathcal{C}(f) \subseteq [-a,b]$ with a and b non-negative, then $\mathcal{C}((x-1)f) \subseteq [-a-b, a+b]$. By Lemma 10 we thus infer that $\mathcal{C}(f_{25}) \subseteq [-\gamma(p,q), \gamma(p,q)]$.
If $q = 2$, then $\gamma(p,2) = 2$ and one easily sees that $\mathcal{C}(f_{25}) = [-2,2]$.
If $p = 2$ and $q = 3$, then $\mathcal{C}(f_{25}) = [-\gamma(2,3), \gamma(2,3)] \backslash \{0\} = [-3,3] \backslash \{0\}$.
If $p = 2$ and $q > 3$, then the coefficients of f_{24} are alternating in sign and so $0 \notin \mathcal{C}(f_{25})$. One infers that $\mathcal{C}(f_{25}) = [-\gamma(2,q), \gamma(2,q)] \backslash \{0\} = [-4,4] \backslash \{0\}$.
Assume that $\min(p,q) > 2$. Then from $\mathcal{C}(f_{25}) \subseteq [-\gamma(p,q), \gamma(p,q)]$ and Lemma 11 we conclude that $\mathcal{C}_0(f_{25}) = [-\gamma(p,q), \gamma(p,q)]$. It remains to determine whether $0 \in \mathcal{C}(f_{25})$.
If $\min(p,q) > 3$, then the coefficient of x^3 is zero, so assume that $\min(p,q) = 3$.
If $p = 3$, then by Lemma 12 we see that $0 \notin \mathcal{C}(f_{25})$.
If $q = 3$, then by Lemma 13 we see that $0 \in \mathcal{C}(f_{25})$. □

Lemma 15 *Let p and q be distinct primes. Put $f_{26} = \Phi_p\Phi_{pq}\Phi_{p^2}$ and $f_{27} = (x-1)f_{26}$. Then $\mathcal{C}(f_{26}) = [0,1]$ and $\mathcal{C}(f_{27}) = [-1,1]$.*

Proof. Write $f_{26} = \sum_j c_j x^j$ and $f_{27} = \sum_j d_j x^j$. Note that $f_{26} = (\Phi_p\Phi_{pq})\Phi_p(x^p) = \Phi_p(x^q)\Phi_p(x^p)$ and thus f_{26} has only non-negative coefficients. Since the equation $aq + bp = a'q + b'p$ with $a, a' \leq p-1$ has only the solution $a = a'$ and $b = b'$ it follows that $\mathcal{C}(f_{26}) \subseteq [0,1]$. On checking that $c_0 = 1$ and $c_1 = 0$ it follows that $\mathcal{C}(f_{26}) = [0,1]$ and hence $\mathcal{C}(f_{27}) \subseteq [-1,1]$. Note that $d_0 = -1$, $d_1 = 1$. Using that, in case $q = 2$,

$$-f_{27} \equiv \frac{x^p+1}{x+1} (\text{mod } x^{p+1}),$$

we easily compute that $d_j = 0$ with

$$j = \begin{cases} 9 & \text{if } p = 2,\ q = 3; \\ 4 & \text{if } p = 2,\ q > 3; \\ p & q = 2,\ p \geq 3; \\ 2 & \text{if } p \geq 3,\ q \geq 3. \end{cases}$$

This concludes the proof. □

Lemma 16 *Let p and q be distinct primes. Put $f_{30} = \Phi_p\Phi_q\Phi_{pq}\Phi_{p^2}$. We have*

$$\mathcal{C}(f_{30}) = \{1, \ldots, \min(p,q)\}.$$

Proof. Note that $f_{30} = (1 + x + \ldots + x^{pq-1})(1 + x^p + \ldots + x^{(p-1)p})$. Write $f_{30} = \sum c_k x^k$. We have

$$0 \leq c_k = \sum_{\substack{0 \leq k - jp < pq \\ 0 \leq j \leq p-1}} 1 \leq \min(p,q).$$

For $0 \leq r \leq \min(p,q) - 1$ we have $c_{rp} = r + 1$. It is easy to see that 0 is not in $\mathcal{C}(f_{30})$. □

Lemma 17 *We have $\mathcal{C}(f_{36}) = [-1,1]$.*

Proof. Rewriting shows that $f_{36}(x) = \Phi_q(x)\Phi_{pq}(x^p)$. Because of the alternating character of the coefficients of Φ_{pq} after dropping the zeros, we immediately conclude that $H_+(f_{36}) = 1$ and $H_-(f_{36}) \geq -1$. It is also obvious that we have $H_-(f_{36}) = -1$ if $p > q$. In case $p < q$ we express f_{36} differently:

$$f_{36}(x) \;=\; \Phi_q(x)\Phi_{p^2q}(x) = \frac{(x^q-1)}{(x-1)} \cdot \frac{(x^{p^2q}-1)}{(x^{pq}-1)} \cdot \frac{(x^p-1)}{(x^{p^2}-1)}.$$

Using the power series for $(1 - x^{p^2})^{-1}$ we obtain

$$\begin{aligned} f_{36}(x) &= \frac{(x^p-1)(x^q-1)}{1-x} \cdot \frac{x^{p^2q}-1}{x^{pq}-1} \cdot \frac{1}{1-x^{p^2}} \\ f_{36}(x) &= (1 + x + \ldots + x^{p-1} - x^q - x^{q+1} - \ldots - x^{p+q-1}) \cdot \\ &\quad (1 + x^{pq} + \ldots + x^{(p-1)pq}) \cdot (1 + x^{p^2} + x^{2p^2} + \ldots). \end{aligned} \tag{7}$$

Let us assume that $H_-(f_{36}) > -1$. If we look at the coeffcient of x^q we can see that $-x^q$ occurs as a combination of $-x^q$ from the first factor and 1 from the other two factors. Since $pq > q$ a positive contribution can only occur if q can be written as $n\cdot p^2+r$ with $1 \le r \le p-1$. But if we assume $q = n\cdot p^2+r$ for such n and r, the coefficient of x^{p+q-1} is -1, because we have the combination $-x^{p+q-1}$ with twice the factor 1. There cannot be any positive contribution because otherwise $p+q-1$ can be written as $n'\cdot p^2+r'$ with $1 \le r' \le p-1$. But this would imply $p-1 = n'\cdot p^2+r'-n\cdot p^2-r$ and because $p^2 > 2p-1$ we even have $p-1 = r'-r$. But obviously $r'-r \le (p-1)-1$. Therefore the assumption that $H_-(f_{36}) > -1$ must be false and we conclude $H_-(f_{36}) = -1$.

From (7) we infer that the coefficient of x^p is zero if $p < q$. If $p > q$, then clearly $f_{36} \equiv \Phi_q(x) (\mathrm{mod}\ x^{q+1})$ and the coefficient of x^q is zero. We conclude that the coefficient of $x^{\min(p,q)}$ is zero and hence the proof is completed. □

Lemma 18 *Let p and q be distinct primes. Put $f_{38} = \Phi_p\Phi_q\Phi_{p^2q}$ and $\beta(p,q) = \min(p, q, q(\mathrm{mod}\ p^2), p^2-q(\mathrm{mod}\ p^2))$. We have*

$$\mathcal{C}(f_{38}) = \begin{cases} \{-2,0,1,2\} & \text{if } q = 2; \\ \{-1,1,2\} & \text{if } p = 2 \text{ and } q = 3; \\ [-\beta(p,q), \min(p,q)] & \text{otherwise.} \end{cases}$$

Proof. Note that $f_{38} = \Phi_p f_{36} = \Phi_q f_{34}$. On using that $H(f_{34}) = 1$ (trivial) and $H(f_{36}) = 1$ (by Lemma 7) and invoking (3), it follows that $H(f_{38}) \le \min(p,q)$.
1) $q = 2$. We have $\Phi_{2p^2}(x) = \Phi_{2p}(x^p) = \Phi_p(-x^p)$. Then $f_{38}(x) = (1+x+\ldots+x^{p-1})(1+x)(1-x^p+x^{2p}-\ldots+x^{p^2-p})$. Since $(1+x+\ldots+x^{p-1})(1-x^p+x^{2p}-\ldots+x^{p^2-p}) = 1+x+\ldots+x^{p-1}-x^p-x^{p+1}-\ldots-x^{2p-1}+\ldots+x^{p^2-p}+x^{p^2-p+1}+\ldots+x^{p^2-1}$, we have $f_{38}(x) = 1+2x+2x^2+\ldots+2x^{p-1}-2x^{p+1}-2x^{p+2}-\cdots-2x^{2p-1}+2x^{2p+1}+\ldots+2x^{p^2-1}+x^{p^2}$.
2) $q > 2$. Put $z_1 = \min(p,q)$. On noting that, modulo x^{z_1},

$$f_{38} \equiv \Phi_p\Phi_q \equiv \frac{1}{(1-x)^2} \equiv \sum_{j=1}^{z_1} jx^{j-1},$$

we find that $1,\ldots,\min(p,q)$ are amongst the coefficients. If $q < p$, calculating the coefficient of x^{p+q-1} shows that this is $-q$, because $p+q-1 < pq$.

$$\begin{aligned} f_{38}(x) &= \Phi_p(x)\Phi_q(x)\Phi_{pq}(x^p) \\ &= (1+2x+\ldots+qx^{q-1}+\ldots+qx^{p-1}+\ldots+x^{p+q-2})(1-x^p+x^{pq}\mp\ldots) \\ &= 1+2x+\ldots+qx^{q-1}+\ldots+qx^{p-1}+\ldots+x^{p+q-2} \\ &\quad -x^p-2x^{p+1}-\ldots-qx^{p+q-1}-\ldots-qx^{2p-1}-\ldots-x^{2p+q-2}+x^{pq}\pm\ldots \end{aligned}$$

Furthermore, if $q \ge 3$ then $2p+q-2 < 3p-1 < pq$, so we have the coefficients $[-q, 0]$ from $-qx^{2p-1}$ to $0x^{2p+q-1}$.
Now assume that $p < q$.

$$\begin{aligned} f_{38}(x) &= \Phi_p(x)\Phi_q(x)\Phi_{pq}(x^p) \\ &= (1+2x+\ldots+px^{p-1}+\ldots+px^{q-1}+\ldots+x^{p+q-2})(1-x^p+x^{p^2}\mp\ldots) \end{aligned}$$

Now write $q = fp^2 + g$, $\Phi_{pq}(x) = \sum a_k x^k$ and $(p-1)(q-1) = \rho p + \sigma q$ with $0 < g < p^2$. Note that $f < \rho$, because otherwise using $\sigma \leq p-2$ and $f \geq \rho$ we have

$$\begin{aligned} \rho p + \sigma q &\leq pq - 2q + fp = pq - q - p + ((f+1)p - q) \\ &\leq pq - p - q < (p-1)(q-1), \end{aligned}$$

which contradicts $\rho p + \sigma q = (p-1)(q-1)$.
Therefore $a_{fp} = 1$ and even $a_{(f+1)p} = 1$. In analogy $f < q - \rho$, because $f \geq q - \rho$ implies

$$\rho p + \sigma q \geq pq - fp > pq - q/p > pq - q > (p-1)(q-1).$$

So we also have $a_{fp+1} = -1$. Because $(fp+1) < q$, the terms $x^{fp} - x^{fp+1} + x^{(f+1)p}$ occur consecutively in $\Phi_{pq}(x)$.
Let $0 \leq y \leq \beta(p,q)$. Now we are able to calculate the coefficient of x^{y+q-1} in $f_{38}(x)$, for $y \neq p$. We use the fact that the signs of the coefficients in $\Phi_{pq}(x)$ alternate. So it is sufficient to know the the lowest and the highest (by degree) influencing term of $\Phi_{pq}(x^p)$. The lowest one is obviously 1 combined with $(p-y)x^{y+q-1}$ of the first factor. Since $y \leq p^2 - g$, we have $y + q - 1 < p^2 - g + fp^2 + g = (f+1)p^2$, so the highest contribution is $-x^{(fp+1)p}$ combined with $(g + y - p)x^{g-1+y-p}$ if $p - y < g < 2p - y$ or $px^{g-1+y-p}$ if $g \geq 2p - y$. Therefore the coefficient of x^{y+q-1} for the case $2p - y \leq g < p^2$ is:

$$(p-y) + p - p + \ldots + p - p = -y.$$

Now allow $y = p$ as one possibility and calculate the coefficient of $x^{2p+q-y-1}$ in $f_{38}(x)$. The lowest contribution is $-x^p$ together with $yx^{q+p-y-1}$. The highest contribution is $-x^{(fp+1)p}$, if $(f+1)p^2 > q + 2p - 1 - y$ or equivalently $p^2 - g + y > 2p - 1$. If $y = p$, then $p^2 - g \geq \beta(p,q) \geq y$, so $p^2 - g + y > 2p - 1$. Otherwise just assume $y > 2p - 1 - (p^2 - g)$. The second factor then contributes $px^{g+p-1-y}$, the coefficient p arises because

$$p - 1 \leq g + p - 1 - y \leq g - 1 \leq q - 1.$$

So in this case the coefficient is

$$-y + p - p + \ldots + p - p = -y.$$

The argument for the first coefficient does not work for $2p - y > g$, that is for $y < 2p - g$, the second one does not work for $y \leq 2p - 1 - (p^2 - g)$, that is for $y < 2p - (p^2 - g)$. If both fail, then $0 \leq 2y \leq 4p - p^2 - 2$, so $p = 2$ and $y \in \{0, 1\}$ or $p = 3$ and $y = 0$.
If $p = 2$ we have to find a -1 and a zero coefficient in

$$\begin{aligned} f_{38}(x) &= \Phi_2(x)\Phi_q(x)\Phi_{2q}(x^2) \\ &= (1 + 2x + \ldots + 2x^{q-1} + x^q)(1 - x^2 + x^4 - x^6 + \ldots + x^{2q-2}) \end{aligned}$$

For $q = 3$ there is no 0 coefficient. If $q \geq 5$ it is easy to see that the coefficient of x^3 is 0. Furthermore the coefficient of x^{q+1} is -1, because

$$2x^{q-1} \cdot (-x^2) + 2x^{q-3} \cdot x^4 + 2x^{q-5} \cdot (-x^6) \ldots + 1 \cdot (\pm x^{q+1})$$

is either $(-2+2-2\pm\ldots+2-1)x^{q+1} = -x^{q+1}$ or $(-2+2-2\pm\ldots-2+1)x^{q+1} = -x^{q+1}$.
If $p = 3$ we have to find a 0 coefficient. We have

$$\begin{aligned} f_{38}(x) &= \Phi_3(x)\Phi_q(x)\Phi_{3q}(x^3) \\ &= (1+2x+3x^2\ldots+3x^{q-1}+2x^q+x^{q+1})(1-x^3+x^9\ldots) \end{aligned}$$

If $q \geq 7$ it is easy to see that the coefficient of x^5 is 0. If $q = 5$ then the coeffcient of x^9 is 0 (by explicit computation).
So it remains to be shown that in the cases $0 < g < p$ and $p^2 - p < g < p^2$ all other coefficients are larger than or equal to $-g$ and $-(p^2 - g)$, respectively.
Therefore we use:

$$\begin{aligned} \Phi_{pq}(x) &= \sum a_k x^k \\ &= \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)} \\ &= (1-x)(1+x^p+\ldots+x^{p(q-1)})(1+x^q+x^{2q}\ldots). \end{aligned}$$

Let S be the numerical semigroup generated by the primes p and q, that is the set of all linear combination of p and q of the form $mp+nq$ with $m, n \geq 0$.
Note that $a_k = 1$ if $k \in S$ and $k-1 \notin S$, $a_k = -1$ if $k \notin S$ and $k-1 \in S$ and $a_k = 0$ in the remaining cases (cf. [5]).

For the lower bound of the coefficients we consider the coefficient of x^j in f_{38}, called d_j. Since $f_{38}(x) = (1+2x+\ldots+px^{p-1}+\ldots+px^{q-1}+\ldots+x^{p+q-2})\Phi_{pq}(x^p)$, contributions depend on combinations of these two factors. So we may express the j-th coefficient as

$$d_j = \sum_{0 \leq j-kp \leq p+q-2} \min\{j-kp+1, p, p+q-1-j+kp\} \cdot a_k.$$

Let

$$e_k = \begin{cases} \min\{j-kp+1, p, p+q-1-j+kp\} & \text{if } 0 \leq j-kp \leq p+q-2 \\ 0 & \text{otherwise,} \end{cases}$$

so $d_j = \sum e_k a_k$.
To get a lower bound denote with n the smallest number such that $a_n = -1$ and $0 \leq j - np \leq p+q-2$, so we have a negative contribution in the above sum. In analogy denote N as the largest number such that $a_N = -1$ and $0 \leq j - Np \leq p+q-2$. Put $d = N - n$. If n and N do not exist, then $d_j \geq 0$ and we are done, so next assume that n and N exist.

If $d > 0$ (and hence $n < N$) a lower bound for the coefficient of x^j can be determined by using the alternate character of $\Phi_{pq}(x^p)$. If $n < k < N$, then $p \leq j - Np + p \leq j - kp \leq j - np - p \leq p+q-2-p = q-2$. So $\min\{j-kp+1, p, p+q-1-j+kp\} = p$. This implies that

$$d_j = \sum_{0 \leq j-kp \leq p+q-2} \min\{j-kp+1, p, p+q-1-j+kp\} \cdot a_k$$

$$
\begin{aligned}
&\geq \sum_{n\leq k\leq N} \min\{j-kp+1, p, p+q-1-j+kp\}\cdot a_k \\
&= -\min\{j-np+1, p, p+q-1-j+np\}+p-p\pm\ldots-p+p \\
&\quad -\min\{j-Np+1, p, p+q-1-j+Np\} \\
&\geq p-(p+q-1-j+np)-(j-Np+1) = -q+Np-np.
\end{aligned}
$$

We infer that

$$d_j \geq -fp^2-g+dp. \tag{8}$$

The above inequality does not suffice to deal with small d. To this end we will need the following claims.

Claim 1: Let m be an arbitrary integer. If $d<mp$, then there exist non-negative integers x and y with $x<n\leq N<y$ such that $y-x\leq mp$ and $a_x=a_y=1$.

We now prove the claim. Note that $a_n=-1$ implies that $n\notin S$ and $n-1\in S$ and further we have $N\notin S$ and $N-1\in S$. Using $n-1\in S$ we have $n-1+mp\in S$. Because $n-1+mp\geq N$, $n-1+mp\in S$ and $N\notin S$ we have $n-1+mp>N$. So there is at least one $N<y<n+mp$ with $y-1\notin S$ and $y\in S$, so $a_y=1$. But again $y-1\notin S$ implies $y-1-mp\notin S$ and we have $n-1\in S$. Therefore there exists an x with $y-mp\leq x<n$ and $x-1\notin S$ and $x\in S$, so $a_x=1$. Furthermore we have $y-x\leq mp$ and $x<n\leq N<y$.

Claim 2: Given the above situation, we have $e_x+e_y\geq\min\{q-mp^2+p, p\}$.

The proof is rather short. If $j-yp+1\geq p$ then $e_y=p$, because $p+q-1-j+yp\geq p+q-1-j+Np+p\geq p$ and we are done. Otherwise

$$p+q-1-j+xp\geq p+q-1-j+yp-mp^2=p+q-mp^2-e_y$$

and clearly $j-xp+1\geq j-np+1+p\geq p$, so $e_x+e_y\geq p+q-mp^2$.

Now we are able to finish this lemma with the two following cases.

Case 1: $0<g<p$.

If $d\geq fp$, then by (8) we have $d_j\geq -g$, so we may assume that $d<fp$. Using Claim 1 we find x and y like described above. Now using Claim 2 we find that $q-fp^2+p=p+g$ and

$$
\begin{aligned}
d_j &= \sum e_k a_k \geq e_x+\sum_{n\leq k\leq N} e_k a_k + e_y \\
&\geq \min\{q-fp^2+p, p\}-p+p\mp\ldots+p-p=\min\{g+p, p\}-p=0.
\end{aligned}
$$

Case 2: $p^2-p<g<p^2$.

If $d\geq(f+1)p$, then by (8) we have $d_j\geq p^2-g>0$, so we may assume that $d<(f+1)p$.

Now we can use again Claim 1 and Claim 2 to find that $q-(f+1)p^2+p=p+g-p^2$ and

$$
\begin{aligned}
d_j &= \sum e_k a_k \geq e_x+\sum_{n\leq k\leq N} e_k a_k + e_y \\
&\geq \min\{q-(f+1)p^2+p, p\}-p+p\mp\ldots+p-p \\
&= \min\{g+p-p^2, p\}-p=-(p^2-g),
\end{aligned}
$$

which finishes the proof. □

Lemma 19 *Let p and q be distinct primes. Put $f_{39} = (x-1)\Phi_p\Phi_q\Phi_{p^2q}$. We have $\mathcal{C}(f_{39}) = \{-2,-1,0,1,2\}$.*

Proof. Since $f_{39} = f_{36}(x^p-1)$ and $H(f_{36}) = 1$ by Lemma 17, we immediately conclude that $\mathcal{C}(f_{39}) \subseteq \{-2,-1,0,1,2\}$. Since f_{39} is anti self-reciprocal it is enough to show that, e.g. $0,1,2$ are in $\mathcal{C}(f_{39})$. Because f_{39} is monic, this is clear for 1. Write $f_{39} = \sum_j c_j x^j$.
If $p > q$, we see that $f_{39}(x) = (-1-x-\ldots-x^{q-1}+x^p+\ldots+x^{p+q-1})\Phi_{pq}(x^p)$. On noting that $\Phi_{pq}(x^p) \equiv 1-x^p (\mathrm{mod}\ x^{p+1})$, we obtain $f_{39}(x) = -1-x-\ldots-x^{q-1}+2x^p (\mathrm{mod}\ x^{p+1})$. On noting that $\Phi_{pq}(x^p) = 1-x^p+x^{pq}\mp\ldots$, it is obvious that the coefficient of x^q equals 0. It is also easy to note that there are only two combinations for x^p which sum to a coefficient of two. Hence $c_q = 0$ and $c_p = 2$.
If $p < q$, we have $f_{39}(x) = (-1-x-\ldots-x^{p-1}+x^q+\ldots+x^{p+q-1})\Phi_{pq}(x^p)$ and $\Phi_{pq}(x^p) = 1-x^p+x^{p^2}\ldots$. We will show that the coefficients -2 and 0 occur in this case (thus also 2 by self-reciproity). If $p = 2$ either the coefficient of x^q or x^{q+1} is 0. If $p \neq 2$ and $q > 2p$ it is easy to see that the coefficient of x^{2p} is 0. In case of $p < q < 2p$ and $p \neq 2,3$ the coefficient of x^{p^2-1} equals 0. The last case is $p = 3$ and $q = 5$, where $0 \in \mathcal{C}(f_{39})$ can be shown by explicit computation (x^{15} and x^{16}).
Let ρ and σ be as in Lemma 2. Write $\Phi_{pq}(x) = \sum a_k x^k$ and $q = mp+g$ with $0 < g < p$ and $M = m+1$. Finally $M + k_M pq = \rho_M p + \sigma_M q$ with $0 \leq \rho_M < q$, $0 \leq \sigma_M < p$ and $0 \leq k_M \leq 1$. Note that $m < M < q$.
Now we study six different cases.
If $\rho_M \leq \rho$ and $\sigma_M \leq \sigma$ then $a_M = 1$ by Lemma 2 and of course $a_1 = -1$. Now determine the coefficient of x^{p+q}. The only contributions arise from x^q of the first factor times $-x^p$ of the second factor and $-x^g$ times x^{Mp}. Therefore $c_{p+q} = a_1 - a_M = -2$.
Before discussing the last five cases, we will establish a small useful result.
If $a_j = 1$ and $a_{j+M} = -1$, then the coefficient of $x^{jp+p+q-1}$ is 2. This is easy to check since obviously the only contributions are x^{p+q-1} times x^{jp} and $-x^{g-1}$ times $-x^{(j+M)p}$.
The next case we study is $\rho_M > \rho$ and $\sigma_M > \sigma$. Since $a_0 = 1$ and $a_M = -1$, we can use the result above.
The third case is $\rho_M > \rho$ and $\sigma_M = 0$. But this is not an actual case, as it would imply

$$\begin{aligned} pq+1 &= (\rho+1)p+(\sigma+1)q \leq (\rho_M+1-1)p+(\sigma+1)q \\ &= M+(\sigma+1)q < (\sigma+2)q \leq pq, \end{aligned}$$

which is a contradiction.
The next case is $\rho_M > \rho$ and $0 < \sigma_M \leq \sigma$.
Because of $M < q$ and $\sigma_M > 0$ we must have $k_M = 1$. Now $a_{(\sigma+1-\sigma_M)q} = 1$ and $a_{(\sigma+1)q+\rho_M p-pq} = -1$ and $(\sigma+1)q+\rho_M p-pq-(\sigma+1-\sigma_M)q = \rho_M p+\sigma_M q-pq = M$, so we can use the result above.
The case $\rho_M = 0$ and $\sigma_M > \sigma$ again does not occur, because then $M + k_M pq = \sigma_M q < pq$ and therefore $k_M = 0$ and so $M = \sigma_M q \geq q$, contradicting $M < q$.
The last remaining case is $0 < \rho_M \leq \rho$ and $\sigma_M > \sigma$.
Again, $M < q$ and $\sigma_M > \sigma > 0$, so $k_M = 1$. Now $a_{(\rho+1-\rho_M)p} = 1$ and

$a_{(\rho+1)p+\sigma_M q-pq} = -1$ and $(\rho+1)p+\sigma_M q-pq-(\rho+1-\rho_M)p = \sigma_M q+\rho_M p-pq = M$, so we can use the result above. □

Lemma 20 *We have*

$$\mathcal{C}(f_{41}) = \begin{cases} \{-2,-1,1,2\} & \text{if } q \le 3; \\ \{-2,-1,0,1,2\} & \text{otherwise.} \end{cases}$$

Proof. We have

$$f_{41} = (x-1)\Phi_{pq}\Phi_{p^2q} = \frac{(x-1)^2(x^{p^2q}-1)}{(x^q-1)(x^{p^2}-1)} = (x-1)f_{40} = (x-1)\tau_{p^2,q}(x).$$

Since $H(f_{40}) = 1$ by Lemma 3, it follows that $H(f_{41}) \le 2$. Modulo x^2 the congruence $f_{41} \equiv -(x-1)^2 \equiv -1+2x$ holds. Using that f_{41} is anti-self-reciprocal we infer from this that $\{-2,-1,1,2\} \in \mathcal{C}(f_{41})$.
If $q = 2$, then $f_{41} = -1 + 2x - 2x^2 + \cdots - 2x^{p^2-1} + x^{p^2}$ and hence $0 \notin \mathcal{C}(f_{41})$.
If $q = 3$, then $f_{41} \equiv -(1+x^{p^2})\sum_k (x^{3k} - 2x^{3k+1} + x^{3k+2}) \bmod x^{2p^2}$, from which we infer that $0 \notin \mathcal{C}(f_{41})$.
If $q \ge 5$, then $f_{41} \equiv -(x-1)^2 \equiv -1 + 2x - x^2 \pmod{x^4}$ and hence $0 \in \mathcal{C}(f_{41})$. □

2.5.1 The polynomials f_{42} and f_{43}

Let p and q be distinct primes. Put $f_{42} = \Phi_p\Phi_{pq}\Phi_{p^2q} = \sum c_j x^j$ and $f_{43} = (x-1)f_{42} = \sum d_j x^j$. It is not difficult to find cases where only very few of the coefficients of f_{43} are equal to 2. For example, if (p,q) is in the following set:

$$\{(11,241),(13,377),(17,577),(19,181),(29,421),(41,3361),(43,3697)\},$$

there are precisely two coefficients equal to 2 (as computed by Yves Gallot). This suggests that perhaps the following resuls is not so easy to establish.

Lemma 21 *We have*

$$\mathcal{C}(f_{43}) = \begin{cases} \{-2,-1,1,2\} & \text{if } q = 2; \\ \{-2,-1,0,1,2\} & \text{otherwise.} \end{cases}$$

The analogue of this result for f_{42} is easy enough. Note that

$$\deg(f_{42}) = p^2(q-1) + p - q.$$

Lemma 22 *We have* $\mathcal{C}(f_{42}) = \{-1,0,1\}$.

Proof. Write $f_{42} = \sum_j c_j x^j$. Note that

$$f_{42} = \frac{(x^p-1)(x^{p^2q}-1)}{(x^q-1)(x^{p^2}-1)}.$$

Around $x = 0$, f_{42} has power series

$$(1 + x^q + x^{2q} + \cdots)(1 - x^p + x^{p^2} - x^{p^2+p} + \cdots + x^{(q-1)p^2} - x^{(q-1)p^2+p}). \qquad (9)$$

Note that if $c_j \geq 2$, then there exist non-negative $\alpha_1, \alpha_2, \beta_1$ and β_2 such that

$$\alpha_1 \neq \alpha_2,\ \beta_1 \neq \beta_2,\ j = \alpha_1 q + \beta_1 p^2 = \alpha_2 q + \beta_2 p^2 \leq \deg(f_{42}) < p^2 q.$$

This is impossible. By a similar argument one sees that $c_j \geq -1$. Since clearly $\{-1, 0, 1\} \in \mathcal{C}(f_{42})$, the proof is completed. □

Indeed, some work needs to be done to infer that $\{-2, 2\} \in \mathcal{C}(f_{43})$. The idea is to show that in f_{42} the combinations $1, -1$ and $-1, 1$ appear as consecutive coefficients and then use that $f_{43} = (x-1)f_{42}$.

Let us denote by $\{a; b\}$ the smallest non-negative integer m such that $m \equiv a (\mathrm{mod}\ b)$.

Lemma 23 *Write* $f_{42} = \sum c_j x^j$ *and* $f_{43} = \sum d_j x^j$. *Put*

$$k_1 = 1 + \{\frac{p-1}{p^2}; q\}p^2 \text{ and } k_2 = 1 + \{\frac{p-1}{q}; p^2\}q.$$

1) *Suppose that* $1 < k_1 \leq \deg(f_{42})$. *If furthermore,*

$$\{\frac{1}{q}; p^2\}q + \{\frac{1}{p}; q\}p^2 > p^2 q \tag{10}$$

and

$$\{\frac{-1}{q}; p\}pq + \{\frac{-1}{p^2}; q\}p^2 + p + 1 > p^2 q, \tag{11}$$

then $c_{k_1-1} = 1$, $c_{k_1} = -1$ *and* $d_{k_1} = 2$.
2) *Suppose that* $k_2 \leq \deg(f_{42})$. *If furthermore,*

$$\{\frac{-1}{q}; p^2\}q + \{\frac{-1}{p}; q\}p^2 + p + 1 > p^2 q \tag{12}$$

and

$$\{\frac{1}{q}; p\}pq + \{\frac{1}{p^2}; q\}p^2 > p^2 q, \tag{13}$$

then $c_{k_2-1} = 1$, $c_{k_2} = -1$ *and* $d_{k_2} = 2$.

Proof. We say that k is *p-representable* if we can write $k = m_1 q + m_2 p^2$ with $m_1 \geq 0$ and $0 \leq m_2 \leq q-1$. We say that k is *m-representable* if we can write $k = n_1 q + n_2 p^2 + p$ with $n_1 \geq 0$ and $0 \leq n_2 \leq q-1$. From the proof of Lemma 22 it follows that if $k \leq \deg(f_{42})$, then k can be p-representable in at most one way and be m-representable in at most one way. We infer that if $k \leq \deg(f_{42})$, then

$$c_k = \begin{cases} 1 & \text{if } k \text{ is } p\text{-representable, but not } m\text{-representable;} \\ -1 & \text{if } k \text{ is } m\text{-representable, but not } p\text{-representable;} \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

We have

$$\begin{cases} k_1 \equiv 1 (\mathrm{mod}\ p^2); \\ k_1 \equiv p (\mathrm{mod}\ q), \end{cases} \text{ and } \begin{cases} k_2 \equiv p (\mathrm{mod}\ p^2); \\ k_2 \equiv 1 (\mathrm{mod}\ q). \end{cases} \tag{15}$$

Suppose that $k_1 \leq \deg(f_{42})$. Clearly k_1 is m-representable, because $k_1 > 1$ implies $k_1 > p$. Condition (10) ensures that k_1 is not p-representable. Thus,

by (14), we have $c_{k_1} = -1$. On the other hand we see that $k_1 - 1$ is p-representable, but not m-representable by (11). It follows that $c_{k_1-1} = 1$. Since $d_{k_1} = c_{k_1-1} - c_{k_1} = 1 - (-1) = 2$, we have established part 1. Part 2 can be derived in a similar way, but here it is not needed to require $k_2 > 1$. □

We will show that some of the numbers appearing in the latter lemma are actually equal. For this the reciprocity law formulated in Corollary 7 is needed. As usual by (m, n) we denote the greatest common divisor of m and n.

Lemma 24 *Let a and b be coprime integers exceeding one. Then*

$$(a - \{\frac{1}{b}; a\}, \{\frac{1}{a}; b\}) = (\{\frac{1}{b}; a\}, b - \{\frac{1}{a}; b\}) = 1.$$

Corollary 7 *Suppose that both $a > 1$ and $b > 1$ are odd and coprime. Then the congruence $\{\frac{1}{a}; b\} \equiv \{\frac{1}{b}; a\} (\mathrm{mod}\ 2)$ holds.*

Proof. If $\{\frac{1}{a}; b\}$ is even, then $a - \{\frac{1}{b}; a\}$ must be odd and hence $\{\frac{1}{b}; a\}$ is even. If $\{\frac{1}{a}; b\}$ is odd, then $b - \{\frac{1}{a}; b\}$ is even and hence $\{\frac{1}{b}; a\}$ must be odd. □

Proof of Lemma 24. Put $\delta(a, b) = (\{\frac{1}{a}; b\})(\{\frac{1}{b}; a\}) - (a - \{\frac{1}{b}; a\})(b - \{\frac{1}{a}; b\})$. It is enough to show that $\delta(a, b) = 1$. Since clearly $-ab+1 < \delta(a, b) < ab$, it is enough to show that $\delta(a, b) \equiv 1 (\mathrm{mod}\ ab)$. We have $\delta(a, b) \equiv \{\frac{1}{b}; a\}b \equiv 1 (\mathrm{mod}\ a)$ and $\delta(a, b) \equiv \{\frac{1}{a}; b\}a \equiv 1 (\mathrm{mod}\ b)$, and on invoking the Chinese remainder theorem the proof is completed. □

Lemma 25 *We have*

$$\{\frac{1}{q}; p^2\}q + \{\frac{1}{p}; q\}p^2 = \{\frac{-1}{q}; p\}pq + \{\frac{-1}{p^2}; q\}p^2 + p + 1$$

and

$$\{\frac{-1}{q}; p^2\}q + \{\frac{-1}{p}; q\}p^2 + p + 1 = \{\frac{1}{q}; p\}pq + \{\frac{1}{p^2}; q\}p^2.$$

Proof. Denote the numbers appearing in the left hand sides of (10), (11), (12) and (13), by $r_1(p, q), s_1(p, q), r_2(p, q), s_2(p, q)$, respectively. We have to show that $r_1(p, q) = s_1(p, q)$ and $r_2(p, q) = s_2(p, q)$. On noting that $\{\frac{-1}{q}; p\} = p - \{\frac{1}{q}; p\}$, etc., it is easily seen that $r_1(p, q) = s_1(p, q)$ implies $r_2(p, q) = s_2(p, q)$, thus it is enough to show that $r_1(p, q) = s_1(p, q)$. By considering r_1, r_2, s_1, s_2 modulo p^2 and q and invoking the Chinese remainder theorem we infer that

$$k_j \equiv r_j(p, q) \equiv s_j(p, q) (\mathrm{mod}\ p^2q) \text{ for } 1 \le j \le 2. \tag{16}$$

Note that

$$\{r_j(p, q), s_j(p, q)\} \in \{k_j, k_j + p^2q\} \text{ for } 1 \le j \le 2. \tag{17}$$

Thus it is enough to show that $r_1(p, q) \equiv s_1(p, q) (\mathrm{mod}\ 2p^2q)$.
1) $p = 2$. Recall that the Legendre symbol $(\frac{-1}{q})$ equals $(-1)^{(q-1)/2}$ in case q is odd. We have $r_1(2, q) = \{\frac{1}{q}; 4\}q + \{\frac{1}{2}; q\}4 = 4q + 2 - (\frac{-1}{q})q$, on noting that

$\{\frac{1}{q};4\} = 2 - (\frac{-1}{q})$ and $\{\frac{1}{2};q\} = (q+1)/2$. On noting that $\{\frac{-1}{q};2\} = 1$ and $\{\frac{-1}{4};q\}4 = (2-(\frac{-1}{q}))q - 1$, one infers that

$$s_1(2,q) = \{\frac{-1}{q};2\}2q + \{\frac{-1}{4};q\}4 + 2 + 1 = 4q + 2 - (\frac{-1}{q})q = r_1(2,q).$$

2) $q = 2$. By an argument easier than that for case 1 one infers that $r_1(p,2) = s_1(p,2) = 2p^2 + 1$.
3) p, q odd. It suffices to show that $r_1(p,q) \equiv s_1(p,q) (\mathrm{mod}\ 2)$. Now using Corollary 7 we have $\{\frac{1}{q};p^2\} = \{\frac{1}{p^2};q\} (\mathrm{mod}\ 2)$ and $\{\frac{1}{p};q\} = \{\frac{1}{q};p\} (\mathrm{mod}\ 2)$ and hence

$$\begin{aligned}
\{\frac{1}{q};p^2\}q + \{\frac{1}{p};q\}p^2 &\equiv \{\frac{1}{q};p^2\} + \{\frac{1}{p};q\} \equiv \{\frac{1}{p^2};q\} + \{\frac{1}{q};p\} \\
&\equiv q - \{\frac{1}{p^2};q\} + p - \{\frac{1}{q};p\} \equiv \{\frac{-1}{p^2};q\} + \{\frac{-1}{q};p\} \\
&\equiv \{\frac{-1}{q};p\}pq + \{\frac{-1}{p^2};q\}p^2 + p + 1 \ (\mathrm{mod}\ 2),
\end{aligned}$$

which finishes the proof. □

Lemma 26 *There is a unique integer $1 \le j \le 2$ such that the conditions of part j of Lemma 23 are satisfied and hence $d_{k_j} = 2$. Furthermore, $d_{\deg(f_{42})-k_j+1} = -2$.*

Proof. First, suppose that $p \not\equiv 1 (\mathrm{mod}\ q)$ (which especially excludes $q = 2$). This implies $k_1 > 1$. From (15) we infer that $k_1 + k_2 \equiv 1 + p (\mathrm{mod}\ p^2q)$. Since clearly $1 + p < 1 + p^2 \le k_1 + k_2 < 1 + p + 2p^2q$, we infer that

$$k_1 + k_2 = 1 + p + p^2q. \tag{18}$$

Let us suppose that $k_1 \ge p^2(q-1) + p - q + 1 = \deg(f_{43}) > \deg(f_{42})$. By (18) we then have $k_2 \le p^2 + q$. Since $q \ge 3$ and $p^2 + p \ge 6$ it follows that

$$\begin{aligned}
k_2 &\le p^2 + q \le 2p^2 + p + q - 6 = 3(p^2-2) + p + q - p^2 \\
&\le q(p^2-2) + p + q - p^2 = qp^2 + p - q - p^2 = (q-1)p^2 + p - q,
\end{aligned}$$

so $k_2 \le \deg(f_{42})$. Since $r_2(p,q) > p^2 + q \ge k_2$ and $r_2(p,q) \equiv k_2 (\mathrm{mod}\ p^2q)$, we have $r_2(p,q) = k_2 + p^2q > p^2q$. Since $r_2(p,q) = s_2(p,q)$ by Lemma 25, it follows that if $k_1 > \deg(f_{42})$ and thus the conditions of part 1 are not satisfied, then the conditions of part 2 are satisfied. By a similar argument we infer that if $k_2 > \deg(f_{42})$ and thus the conditions of part 2 are not satisfied, then the conditions of part 1 are satisfied.

It remains to deal with the case where $k_j \le \deg(f_{42})$ for $1 \le j \le 2$. Note that

$$r_1(p,q) + r_2(p,q) = 1 + p + 2p^2q. \tag{19}$$

Hence $r_j(p,q) > p^2q$ for some $1 \le j \le 2$. Let us assume that $r_2(p,q) > p^2q$. Now if $r_1(p,q) > p^2q$, then

$$r_1(p,q) + r_2(p,q) = k_1 + p^2q + r_2(p,q) > 1 + p^2 + 2p^2q,$$

contradicting (19).

Now suppose that $p \equiv 1 (\mathrm{mod}\ q)$, so $p = kq + 1$. This implies that $k_1 = 1 + 0p^2 = 1$ and $k_2 = 1 + kq = p$ and hence the conditions of part 1 are not satisfied. It is easy to see that $c_0 = 1$ and $c_1 = 0$, so $d_1 = 1$.
For part 2 we have $k_2 = p \leq \deg(f_{42})$. On noting that $\{\frac{-1}{q}; p^2\} = k^2q + 2k$ and $\{\frac{-1}{p}; q\} = q - 1$, the left side of equation (12) becomes:

$$(k^2q + 2k)q + (q-1)p^2 + p + 1 = k^2q^2 + 2kq + p^2q - p^2 + p + 1 = p^2q + p > p^2q.$$

Similarly we have for the left side of equation (13):

$$(p-k)pq + 1 \cdot p^2 = p^2q - p(p-1) + p^2 = p^2q + p > p^2q.$$

(Alternatively one can invoke Lemma 25 to deduce that the left hand side of (13) equals the left hand side of (12) and hence exceeds p^2q.) It follows that either the conditions of part 1 or those of part 2 are satisfied, but cannot be satisfied at the same time.

The final asseertion follows on noting that f_{42} is self-reciprocal and using that $f_{43} = (x-1)f_{42}$. □

`Example`. Using the latter lemma, one can derive the following examples (in each case one of k_1, k_2 is larger than $\deg(f_{42})$ and hence the remaining one satisfies all conditions.
1) If $p^2 + p - 1 \equiv 0 (\mathrm{mod}\ q)$, then $d_{p^2+p} = 2$.
2) If $p^2 - p + 1 \equiv 0 (\mathrm{mod}\ q)$, then $d_{p^2+1} = 2$.
3) If $q \equiv 1 - p (\mathrm{mod}\ p^2)$, then $d_{q+p} = 2$.
4) If $q \equiv p - 1 (\mathrm{mod}\ p^2)$, then $d_{q+1} = 2$.
5) If $p \equiv 1 (\mathrm{mod}\ q)$, then $d_p = 2$.

Proof of Lemma 21. By (3) and Lemma 22 we find that $\mathcal{C}(f_{43}) \subseteq \{-2, -1, 0, 1, 2\}$. By Lemma 26 we have $\{-2, 2\} \subseteq C(f_{43})$. Since $d_0 = -1$ and $d_{\deg(f_{43})} = 1$, it remains to be shown when $0 \in \mathcal{C}(f_{43})$. If both p and q are odd, then $d_2 = 0$. If $q = 2$, then f_{43} has the power series (around $x = 0$)

$$f_{43} = (-1 + x^p - x^{p^2} + x^{p^2+p})(1 - x + x^2 - x^3 + x^4 - x^5 + \cdots)$$

and since p is odd we find that $d_j \neq 0$ for $j \leq \deg(f_{43}) = p^2 + p - 1$. If $p = 2$, then f_{43} has the power series (around $x = 0$)

$$f_{43} = (1 + x^q + x^{2q} + x^{3q}) \sum_{k=0}^{\infty} (-x^{4k} + x^{4k+1} + x^{4k+2} - x^{4k+3}).$$

From this we see that $d_q = 0$ if $q \equiv 1 (\mathrm{mod}\ 4)$ and $d_{q+1} = 0$ if $q \equiv 3 (\mathrm{mod}\ 4)$. Since $q + 1 < \deg(f_{43}) = 3q - 1$, it follows that $0 \in \mathcal{C}(f_{43})$ if $p = 2$. □

3 The proof of the main theorem

Proof of Theorem 5. From $x^n - 1 = \prod_{d|n} \Phi_d(x)$ and the fact that the Φ_d are irreducible over the rationals, we infer that any divisor of $x^n - 1$ with integer

coefficients is of the form $\pm\prod_{d|n}\Phi_d^{e_d}(x)$, with $e_i \in \{0,1\}$. Thus we have $2^{d(n)}$ monic divisors, where $d(n)$ denotes the number of divisors of n.

From the identity

$$x^{p^2q}-1 = \Phi_1(x)\Phi_p(x)\Phi_q(x)\Phi_{pq}(x)\Phi_{p^2}(x)\Phi_{p^2q}(x), \tag{20}$$

we infer that $x^{p^2q}-1$ has 64 divisors. We denote these by $f_0,\ldots,f_{63}$. If $k=\sum_{j=0}^{5}k_j2^j$ is the base 2 expansion of k, then we put

$$f_k(x) = \Phi_1(x)^{k_0}\Phi_p(x)^{k_1}\Phi_q(x)^{k_2}\Phi_{pq}(x)^{k_3}\Phi_{p^2}(x)^{k_4}\Phi_{p^2q}(x)^{k_5}.$$

Thus $\{f_0(x),\ldots,f_{63}(x)\}$ is the set of all monic divisors of $x^{p^2q}-1$. Note that $\Phi_1(x)=x-1$, $\Phi_p(x)=1+x+\cdots+x^{p-1}$ and $\Phi_q(x)=1+x+\cdots+x^{q-1}$. Thus these three divisors have all height 1. By Lemma 2 we have $H(\Phi_{pq}(x))=1$. On noting that $\Phi_{p^2}(x)=\Phi_p(x^p)$ and $\Phi_{p^2q}(x)=\Phi_{pq}(x^p)$, it then follows that each of the six cyclotomic polynomials appearing in (20) is flat.

We will only establish the less trivial cases in Table 1, the easier ones being left as exercises to the reader.

-$f_0, f_1, f_2, f_3, f_4, f_5, f_{16}, f_{17}, f_{18}, f_{19}$: Use Theorem 1.

-f_6. Use Lemma 7.

-f_7. Use Corollary 3.

-f_8: Use Lemma 3.

-f_9. Use Lemma 6.

-$f_{16}, f_{17}, f_{18}, f_{32}, f_{33}, f_{34}$: Use identity (4).

-f_{20}: See Lemma 8.

-f_{21}, f_{37}: Note that $\Phi_1(x)\Phi_q(x)=x^q-1$.

-f_{22}: See Corollary 5.

-f_{19}, f_{23}, f_{27}. Use that $\Phi_1(x)\Phi_p(x)\Phi_{p^2}(x)=x^{p^2}-1$.

-f_{24}: Invoke Lemma 10.

-f_{25}: Invoke Lemma 14.

-f_{26}, f_{27}: Invoke Lemma 15.

-f_{28}: We have $f_{28}=\Phi_p(x^p)\Phi_q(x^p)$. On invoking the result that $\mathcal{C}(\Phi_p\Phi_q)=[1,\min(p,q)]$ (follows by Lemma 7), the assertion follows.

-f_{29}: If $p=2$, then consecutive coefficients in f_{28} are distinct and hence $0\notin\mathcal{C}(f_{29})$.

-f_{30}: See Lemma 16.

-f_{31}. Note that $f_{31}=(x^{p^2q}-1)/\Phi_{p^2q}(x)=\Psi_{p^2q}(x)=\Psi_{pq}(x^p)$. Thus, $\mathcal{C}(f_{31})=[-1,1]$ by (6).

-f_{34}: Using (5) we find that $\mathcal{C}(f_{34})=\mathcal{C}(f_8)$.

-f_{35}: $f_{35}=(x^p-1)\Phi_{pq}(x^p)=f_9(x^p)$. Now invoke Lemma 6.

-f_{36}: Invoke Lemma 17.

-f_{37}: We have $f_{37}=(x^q-1)\Phi_{pq}(x^p)$. Noting that $q+jp\neq kp$, we infer that $\mathcal{C}(f_{37})=[-1,1]$.

-f_{38}: Invoke Lemma 18.

-f_{39}. Invoke Lemma 19.

-f_{40}: We have $f_{40}=\tau_{p^2,q}(x)$. Now invoke Lemma 3.

-f_{41}. We have $f_{41}=(x-1)\tau_{p^2,q}(x)$. Now invoke Lemma 6.

-f_{42}. Invoke Lemma 22.

-f_{43}. Invoke Lemma 21.
-f_{44}: We have $\Phi_q(x)\Phi_{pq}(x)\Phi_{pq}(x^p) = (x^{p^2q}-1)/(x^{p^2}-1)$.
-Let $0 \le j \le 15$. Note that

$$f_{j+48} = f_j\Phi_{p^2}(x)\Phi_{p^2q}(x) = f_j\Phi_p(x^p)\Phi_{pq}(x^p) = f_j(1+x^{pq}+x^{2pq}+\cdots+x^{(p-1)pq}),$$

it follows by (4) that if $\deg(f_j) < pq-1$, then $\mathcal{C}(f_{j+48}) = \mathcal{C}(f_j)\cup\{0\}$.
We have $\deg(f_j) > pq-1$ iff
-$q=2$, $j=11$;
-$p=2$, $j=13$;
-$j=14$;
-$j=15$. Using these two observations and Table 1A, one easily arrives at Table 1D. □

Table 1A

f	$\Phi_1(x)$	$\Phi_p(x)$	$\Phi_q(x)$	$\Phi_{pq}(x)$	$\Phi_{p^2}(x)$	$\Phi_{p^2q}(x)$	$\mathcal{C}(f)$
0	0	0	0	0	0	0	$\{1\}$
1	1	0	0	0	0	0	$\{-1,1\}$
2	0	1	0	0	0	0	$\{1\}$
3	1	1	0	0	0	0	$[-1,1]$
4	0	0	1	0	0	0	$\{1\}$
5	1	0	1	0	0	0	$[-1,1]$
6	0	1	1	0	0	0	$[1,\min(p,q)]$
7	1	1	1	0	0	0	$[-1,1]$
8	0	0	0	1	0	0	$[-1,1]$
9	1	0	0	1	0	0	$[-2,2]$
10	0	1	0	1	0	0	$[0,1]$
11	1	1	0	1	0	0	$[-1,1]$
12	0	0	1	1	0	0	$[0,1]$
13	1	0	1	1	0	0	$[-1,1]$
14	0	1	1	1	0	0	$\{1\}$
15	1	1	1	1	0	0	$[-1,1]$

If $\min(p,q)=2$, then $\mathcal{C}(f_8)=\{-1,1\}$.
If $\min(p,q)\le 3$, then $\mathcal{C}(f_9)=\{-2,-1,1,2\}$.
If $q=2$, then $\mathcal{C}(f_{11})=\{-1,1\}$.
If $p=2$, then $\mathcal{C}(f_{13})=\{-1,1\}$.

We put $\alpha(p,q)=\min([\frac{q-1}{p}]+1,p)$.
By p^* we denote the unique integer with $1\le p^*<q$ such that $pp^*\equiv 1(\mathrm{mod}\ q)$.
We define $\gamma(p,q)=\min(p,p^*)+\min(p,q-p^*)$.

Table 1B

f	$\Phi_1(x)$	$\Phi_p(x)$	$\Phi_q(x)$	$\Phi_{pq}(x)$	$\Phi_{p^2}(x)$	$\Phi_{p^2q}(x)$	$\mathcal{C}(f)$
16	0	0	0	0	1	0	$[0,1]$
17	1	0	0	0	1	0	$[-1,1]$
18	0	1	0	0	1	0	$\{1\}$
19	1	1	0	0	1	0	$[-1,1]$
20	0	0	1	0	1	0	$[\min([\frac{q}{p}],1),\alpha(p,q)]$
21	1	0	1	0	1	0	$[-1,1]$
22	0	1	1	0	1	0	$[1,\min(p^2,q)]$
23	1	1	1	0	1	0	$[-1,1]$
24	0	0	0	1	1	0	$[-\min(p,q-p^*),\min(p,p^*)]$
25	1	0	0	1	1	0	$[-\gamma(p,q),\gamma(p,q)]$
26	0	1	0	1	1	0	$[0,1]$
27	1	1	0	1	1	0	$[-1,1]$
28	0	0	1	1	1	0	$[0,\min(p,q)]$
29	1	0	1	1	1	0	$[-\min(p,q),\min(p,q)]$
30	0	1	1	1	1	0	$[1,\min(p,q)]$
31	1	1	1	1	1	0	$[-1,1]$

If $p=2$, then $\mathcal{C}(f_{17})=\{-1,1\}$.
If $\min(p,q)=2$, then $\mathcal{C}(f_{24})=[-\min(p,q-p^*),\min(p,p^*)]\backslash\{0\}$.
If $p\le 3$ and $q\neq 2$, then $\mathcal{C}(f_{25})=[-\gamma(p,q),\gamma(p,q)]\backslash\{0\}$.
If $p=2$, then $\mathcal{C}(f_{29})=\{-2,-1,1,2\}=[-\min(2,q),\min(2,q)]\backslash\{0\}$.

Table 1C

f	$\Phi_1(x)$	$\Phi_p(x)$	$\Phi_q(x)$	$\Phi_{pq}(x)$	$\Phi_{p^2}(x)$	$\Phi_{p^2q}(x)$	$\mathcal{C}(f)$
32	0	0	0	0	0	1	$[-1,1]$
33	1	0	0	0	0	1	$[-1,1]$
34	0	1	0	0	0	1	$[-1,1]$
35	1	1	0	0	0	1	$[-2,2]$
36	0	0	1	0	0	1	$[-1,1]$
37	1	0	1	0	0	1	$[-1,1]$
38	0	1	1	0	0	1	$[-\beta(p,q),\min(p,q)]$
39	1	1	1	0	0	1	$[-2,2]$
40	0	0	0	1	0	1	$[-1,1]$
41	1	0	0	1	0	1	$[-2,2]$
42	0	1	0	1	0	1	$[-1,1]$
43	1	1	0	1	0	1	$[-2,2]$
44	0	0	1	1	0	1	$[0,1]$
45	1	0	1	1	0	1	$[-1,1]$
46	0	1	1	1	0	1	$[0,1]$
47	1	1	1	1	0	1	$[-1,1]$

We put $\beta(p,q) = \min(p, q, q(\text{mod } p^2), p^2 - q(\text{mod } p^2))$.
If $p = 2$, then $\mathcal{C}(f_{33}) = \{-1, 1\}$.
If $\min(p, q) = 2$, then $\mathcal{C}(f_{34}) = \{-1, 1\}$.
If $q = 2$, then $\mathcal{C}(f_{38}) = \{-2, 0, 1, 2\}$.
If $q = 3$ and $p = 2$, then $\mathcal{C}(f_{38}) = \{-1, 1, 2\}$.
If $q = 2$, then $\mathcal{C}(f_{40}) = \{-1, 1\}$.
If $q \leq 3$, then $\mathcal{C}(f_{41}) = \{-2, -1, 1, 2\}$.
If $q = 2$, then $\mathcal{C}(f_{43}) = \{-2, -1, 1, 2\}$.

Table 1D

f	$\Phi_1(x)$	$\Phi_p(x)$	$\Phi_q(x)$	$\Phi_{pq}(x)$	$\Phi_{p^2}(x)$	$\Phi_{p^2q}(x)$	$\mathcal{C}(f)$
48	0	0	0	0	1	1	$[0, 1]$
49	1	0	0	0	1	1	$\{-1, 1\}$
50	0	1	0	0	1	1	$[0, 1]$
51	1	1	0	0	1	1	$[-1, 1]$
52	0	0	1	0	1	1	$[0, 1]$
53	1	0	1	0	1	1	$[-1, 1]$
54	0	1	1	0	1	1	$[0, \min(p, q)]$
55	1	1	1	0	1	1	$[-1, 1]$
56	0	0	0	1	1	1	$[-1, 1]$
57	1	0	0	1	1	1	$[-2, 2]$
58	0	1	0	1	1	1	$[0, 1]$
59	1	1	0	1	1	1	$[-1, 1]$
60	0	0	1	1	1	1	$[0, 1]$
61	1	0	1	1	1	1	$[-1, 1]$
62	0	1	1	1	1	1	$\{1\}$
63	1	1	1	1	1	1	$[-1, 1]$

If $q = 2$, then $\mathcal{C}(f_{59}) = \{-1, 1\}$.
If $p = 2$, then $\mathcal{C}(f_{61}) = \{-1, 1\}$.

3.1 Compact reformulation of Theorem 5

For reference purposes a more compact version of Theorem 5 might be useful. We give it here (this reformulation was given by Yves Gallot).

Theorem 9 *Let p and q be distinct primes. Let $f(x) \in \mathbb{Z}[x]$ be a monic divisor of $x^{p^2q} - 1$. There exists an integer $k = \sum_{j=0}^{5} k_j 2^j$ with $k_j \in \{0, 1\}$ (the binary expansion of k) such that*

$$f(x) = f_k(x) = \Phi_1^{k_0} \cdot \Phi_p^{k_1} \cdot \Phi_q^{k_2} \cdot \Phi_{pq}^{k_3} \cdot \Phi_{p^2}^{k_4} \cdot \Phi_{p^2q}^{k_5}.$$

Let p^* be the unique integer with $1 \leq p < q$ such that $pp^* \equiv 1 \pmod{q}$ and $\mathcal{I}(f_k)$ be the integer interval:

- $[1,\ 1]$ *for* $k \in \{0, 2, 4, 14, 18, 62\}$,
- $[0,\ 1]$ *for* $k \in \{10, 12, 16, 26, 44, 46, 48, 50, 52, 58, 60\}$,

- $[-2,\ 2]$ *for* $k \in \{9, 35, 39, 41, 43, 57\}$,
- $[1,\ \min(p,\ q)]$ *for* $k \in \{6, 30\}$,
- $[0,\ \min(p,\ q)]$ *for* $k \in \{28, 54\}$,
- $[\min(\lfloor q/p \rfloor,\ 1), \min(\lfloor (q-1)/p \rfloor + 1,\ p)]$ *for* $k = 20$,
- $[1,\ \min(p^2,\ q)]$ *for* $k = 22$,
- $[-\min(p,\ q - p^*),\ \min(p,\ p^*))]$ *for* $k = 24$,
- $[-\min(p,\ p^*) - \min(p,\ q - p^*),\ \min(p,\ p^*) + \min(p,\ q - p^*)]$ *for* $k = 25$,
- $[-\min(p,\ q),\ \min(p, q)]$ *for* $k = 29$,
- $[-\beta(p,q) = \min(p,\ q,\ q \pmod{p^2},\ p^2 - q \pmod{p^2},\ \min(p,\ q)]$ *for* $k = 38$,
- $[-1,\ 1]$ *otherwise.*

Then $\mathcal{C}_0(f_k) = \mathcal{I}(f_k)$ *except for* $k = 38$ *and* $q = 2$. *If* $q = 2$, $\mathcal{C}_0(f_{38}) = \mathcal{C}(f_{38}) = \{-2, 0, 1, 2\}$. *We have* $\mathcal{C}(f_k) = \mathcal{C}_0(f_k)$ *except for the following cases (where* $\mathcal{C}(f_k) = \mathcal{C}_0(f_k) \setminus \{0\}$*):*

- $k = 1$,
- $k \in \{13, 17, 29, 33, 61\}$ *and* $p = 2$,
- $k \in \{11, 40, 43, 59\}$ *and* $q = 2$,
- $k \in \{8, 24, 34\}$ *and* $\min(p,\ q) = 2$,
- $k = 9$ *and* $\min(p,\ q) \le 3$,
- $k = 25$ *and* $p \le 3$ *and* $q \ne 2$,
- $k = 38$ *and* $p = 2$ *and* $q = 3$,
- $k = 41$ *and* $q \le 3$.

3.2 Earlier work on $x^{p^2q} - 1$

The only earlier work we are aware of is that by Kaplan [7], who proved that if $p \ne q$, then $B(p^2q) = \min(p^2, q)$. He first remarks that since $B(pq) = \min(p, q)$, it remains to deal with the 48 divisors of $x^{p^2q} - 1$ that do not divide $x^{pq} - 1$. For those in his Table 1 he gives an upper bound on the height. Since as we have seen in the proof of Theorem 5, $H(f_{j+48}) = H(f_j)$ for $0 \le j \le 15$, it is actually enough to deal with only 32 divisors (namely those in our Table 1B and 1C). A further remark is that where in his Table 1, p is given as upper bound, one needs $\min(p, q)$ (as not always $p \le \min(p^2, q)$). As Kaplan pointed out to the authors it is easy to see that this replacement can be made. On doing so and comparing with our results the upper bound he gives for the height are seen to be equalities, except (for certain choices of p and q) in the cases listed in Table 2.

Table 2

f	$H(f)$	$H(f)$
	Kaplan	exact
20	$\leq \min(p,q)$	$\min(p, [\frac{q-1}{p}]+1)$
24	$\leq \min(p,q)$	$\min(p,p^*)$
25	$\leq \min(p,q)$	$\min(p,p^8)+\min(p,q-p^*)$
45	≤ 2	1

Note that two of the three 'challenging' polynomials mentioned in the introduction do not appear in the table. For f_{38} it is easy to see that $H(f_{38}) = \min(p,q)$ (but challenging to determine $\mathcal{C}(f_{38})$). For f_{43} it is easy to see that $H(f_{43}) \leq 2$, but challenging to establish that $H(f_{43}) = 2$. Of course in order to compute $B(p^2q)$ it is not the best strategy to compute $H(f)$ exactly for every divisor of $x^{p^2q}-1$.

4 Heights of divisors of $x^n - 1$

For a polynomial $f \in \mathbb{Z}[x]$, we define

$$H^*(f) = \max\{H(g) : g|f \text{ and } g \in \mathbb{Z}[x]\}.$$

Put $B(n) = H^*(x^n-1)$. Sofar little is known about this function. Pomerance and Ryan [11] have established the following three results concerning $B(n)$, the fourth is due to Justin [6] and, independently, Felsch and Schmidt [4].

Theorem 10
1) *Let $p<q$ be primes. Then $B(pq)=p$.*
2) *We have $B(n)=1$ if and only if $n=p^k$.*
3) *We have*

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

4) *$B(n)$ is bounded above by a function that does not depend on the largest prime factor of n.*
5) *Let p and q be different primes. Then $B(p^2q) = \min(p^2,q)$.*

In their paper Pomerance and Ryan observe that from their limited numerical data it seems that part 5 holds. This was subsequently proven by Kaplan [7]. Our work presented here leads to a reproof. Kaplan's paper contains various further results on $B(n)$.

For a polynomial $f \in \mathbb{Z}[x]$, we define

$$H^*_{\pm}(f) = \max\{|H_{\pm}(g)| : g|f \text{ and } g \in \mathbb{Z}[x]\}.$$

Furthermore we define $B_{\pm}(n) = H^*_{\pm}(x^n-1)$. Numerical observations suggest that often $B_+(n) > B_-(n)$, and this is our main motivation for introducing these functions. In fact, if $p<q$ are primes, then $B_+(pq)=p$ and $B_-(pq)=2$.

5 Flat divisors of $x^n - 1$

The present article suggests that many divisors of $x^n - 1$ are flat. It seems therefore natural to try to obtain an estimate for the number of flat divisors of $x^n - 1$.

The following result offers a modest contribution in this direction.

Theorem 11 *Let p and q be distinct primes. Let f_e be the number of flat monic divisors of $x^{p^e q} - 1$. Then $f_{e+1} \geq 2f_e + 2^{e+2} - 1$.*

Proof. Every divisor of $x^{p^{e+1}q} - 1$ is of the form
a) $f(x)$
b) $f(x)\Phi_{p^{e+1}}(x)$
c) $f(x)\Phi_{p^{e+1}q}(x)$,
or
d) $f(x)\Phi_{p^{e+1}}(x)\Phi_{p^{e+1}q}(x)$,
with $f(x)$ a divisor of $x^{p^e q} - 1$. Lower bounds for the number of flat divisors amongst the various types are considered below:
a) The divisors of this form contribute f_e to f_{e+1}.
b) Note that we can write $f(x)\Phi_{p^{e+1}}(x) = f(x)\Phi_p(x^{p^e})$. Suppose $f(x)$ divides $x^{p^e} - 1$. Since $f(x)\Phi_p(x^{p^e})|x^{p^{e+1}} - 1$ it is flat by Theorem 1. Since $x^{p^e} - 1$ has 2^{1+e} monic divisors, we see that there are at least 2^{1+e} flat divisors of $x^{p^{e+1}q} - 1$ of the form b.
c) Note that we can write $f(x)\Phi_{p^{e+1}q}(x) = f(x)\Phi_{pq}(x^{p^e})$. Suppose $f(x)$ divides $x^{p^e} - 1$. In case $f(x) = x^{p^e} - 1$, then $H(f(x)\Phi_{pq}(x^{p^e})) = 2$ by Lemma 6. In the remaining case $\deg(f) < p^e$ and by (4) and Theorem 1 we infer that $H(f(x)\Phi_{pq}(x^{p^e})) = H(f(x)) = 1$. We conclude that there are at least $2^{1+e} - 1$ flat divisors of $x^{p^{e+1}q} - 1$ of the form c.
d) We have $\Phi_{p^{e+1}}(x)\Phi_{p^{e+1}q}(x) = (x^{p^{e+1}q} - 1)/(x^{p^e q} - 1)$. In case $f(x) = x^{p^e q} - 1$, then $H(f(x)\Phi_{pq}(x^{p^e})) = H(x^{p^{e+1}q} - 1) = 1$. In the remaining cases we find, by (4), that $H(f(x)\Phi_{p^{e+1}}(x)\Phi_{p^{e+1}q}(x)) = H(f(x))$. Thus there are at least f_e flat divisors of $x^{p^{e+1}q} - 1$ of the form d.

On adding the contributions of each of the four forms, the result follows. □

`Remark 1`. The above argument with $e = 1$ in combination with Theorem 2 leads to the following list of 35 divisors of $x^{p^2 q} - 1$ that are flat:
a) $f_0, \ldots, f_{15}$, excluding f_6 and f_9
b) $f_{16}, f_{17}, f_{18}, f_{19}$
c) f_{32}, f_{33}, f_{34}
d) $f_{48}, \ldots, f_{63}$, excluding f_{54} and f_{57}.
Note that the full list of flat divisors is longer.

`Remark 2`. By induction one easily proves that for $e \geq 2$ we have

$$f_e \geq 2^{e-1} f_1 + (4e - 5)2^{e-1} + 1.$$

By Theorem 2 we have $f_1 = 14$ and hence it follows that $f_e \geq (4e + 9)2^{e-1} + 1$. The total number of divisors of $x^{p^e q} - 1$ is 2^{2+2e}, denote this by n_e. Then $f_e \gg \sqrt{n_e} \log n_e$. Can one improve on this ?

6 A variation

We have $H(f_6) = \min(p, q) = B(pq)$. Likewise we have $H(f_{22}) = \min(p^2, q) = B(p^2q)$. Both f_6 and f_{22} are special in the sense that they have only non-negative coefficients. It might therefore be more reasonable to consider only balanced divisors of $x^n - 1$, that is divisors having both positive and negative coefficients. Let us denote this analogue of $B(n)$ by $B'(n)$. Put

$$C(n) = \max\{|\mathcal{C}_0(f)| - 1 : f | x^n - 1,\ f \text{ is balanced}\}.$$

Theorem 12 *We have*
1) $B'(pq) = 2$ *and* $C(pq) = 4$.
2) $B'(p^2q) = B_-(p^2q) = \min(p, p^*) + \min(p, q - p^*)$ *and* $C(p^2q) = 2B'(p^2q)$.

This result is a corollary of Theorem 5.

`Acknowledgement`. The bulk of this paper was written in August/September 2008 during an internship of the first author with the second author. The initial aim was to prove the conjecture of Ryan and Pomerance that $B(p^2q) = \min(p^2, q)$. This was relatively soon achieved, but then we learned that independently this had already been done by Kaplan [7]. Then the aim became to compute the maximum and minimum coefficient of each of the 64 monic divisors of $x^{p^2q} - 1$. With the more recent focus on coefficient convexity (see, e.g., [1, 2, 5, 13]) in mind the aim was even set higher: to compute the coefficient set of all of the divisors.

We like to thank the interns Richard Cartwright (2008) and Oana-Maria Camburu (2010) for helpful remarks. However, our greatest indebtness is to Yves Gallot for his computational assistance. In particular, he numerically verified Theorem 5 in case $\max(p, q) < 200$. Merci beaucoup, Yves !

References

[1] G. Bachman, On ternary inclusion-exclusion.polynomials, arXiv:1006.0518, submitted.

[2] B. Bzdęga, Bounds on ternary cyclotomic coefficients, *Acta Arith.* **144** (2010), 5–16.

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

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

[5] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248..

[6] 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.

[7] N. Kaplan, Bounds for the maximal height of divisors of $x^n - 1$, *J. Number Theory* **129** (2009), 2673–2688.

[8] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.

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

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

[11] C. Pomerance and N. C. Ryan, Maximal height of divisors of $x^n - 1$, *Illinois J. Math.* **51** (2007), 597–604.

[12] J.L. Ramirez Alfonsin, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications **30**, Oxford University Press, Oxford, 2005.

[13] S. Rosset, The coefficients of cyclotomic like polynomials of order 3, unpublished manuscript (2008), pp. 5.

[14] N.C. Ryan, B.C. Ward and R. Ward, Some conjectures on the maximal height of divisors of $x^n - 1$, arXiv:1009.5970.

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

Achtern Diek 32, D-49377 Vechta, Germany.
e-mail: andreasd@uni-bonn.de

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