SARAJEVO JOURNAL OF MATHEMATICS
Vol.9 (21) (2013), 3–28
DOI: 10.5644/SJM.09.1.01

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 $\mathcal{C}(f) = \{c_j : 0 \le j \le \deg(f)\}$ 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. A question that arises is to what extent the smallness of the coefficients is particular to $\Phi_n(x)$. We will try to answer this by investigating the coefficients of the other divisors of $x^n - 1$ as well. Our work suggests that as far as the behavior of its coefficients goes, $\Phi_n(x)$ does not have a special role amongst the divisors of $x^n - 1$. 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).

2010 *Mathematics Subject Classification.* 11B83, 11C08.
Key words and phrases. Cyclotomic polynomials, coefficient sets of polynomials.

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

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

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 $p \leq 3$ and $[-2, 2]$ otherwise. The set of coefficients of $\Phi_p(x)\Phi_q(x)$ is $[1, \min(p, q)]$.*

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.*

Let $B(n)$ be the maximum coefficient (in absolute value) that occurs amongst all monic divisors of $x^n - 1$. Pomerance and Ryan [9] conjectured and Kaplan [6] proved that $B(p^2q) = \min(p^2, q)$. Letting $B_+(n)$ denote the maximum amongst all the coefficients of all the monic divisors of $x^n - 1$, and $-B_-(n)$ the minimum, we have the following generalization of Kaplan's result.

Theorem 4. *Let p and q be distinct primes. Let $1 \leq p^* \leq q - 1$ 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 [6]. Ryan et al. [11] 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

$\min(p, p^*) + \min(p, q - p^*) \geq \min(p, q)$. A reformulation of Theorem 5 without tables 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 $0 \leq k \leq 63$ 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 $0 \leq k_j \leq 1$ 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}.

For reasons of space various proofs of lemmas have been suppressed. They can be found in the full version [4] of the paper.

2. Preliminaries

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

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

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 [12] 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) $\Phi_p(x) = (x^p - 1)/(x - 1) = 1 + x + \cdots + x^{p-1}$.
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 [9], 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 $f(= \sum_j c_j x^j)$, that is in the string $c_0c_1c_2 \ldots c_{\deg(f)}$, we replace each coefficient by its p-fold repetition (e.g. c_0c_1 becomes $c_0c_0c_0c_1c_1c_1$ if $p = 3$), 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 4 below together with (2).) Lam and Leung [7] gave an explicit description of the coefficients of $\Phi_{pq}(x)$.

Lemma 2. ([7]). *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 $0 \leq m < pq$. Then either $m = \alpha_1 p + \beta_1 q$ or $m = \alpha_1 p + \beta_1 q - pq$ with $0 \leq \alpha_1 \leq q - 1$ the unique integer such that $\alpha_1 p \equiv m \pmod q$ and $0 \leq \beta_1 \leq p-1$ the unique integer such that $\beta_1 q \equiv m \pmod p$. The cyclotomic coefficient $a_{pq}(m)$ equals*

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

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

A rather specific observation we will need involving binary cyclotomic polynomials is the following.

Lemma 3. *Let p and q be primes with $p < q$. Write $q = fp^2 + g$ with $0 < g < p^2$ and $\Phi_{pq}(x) = \sum_j a_j x^j$. We have*

$$\Phi_{pq}(x) = \sum_{j=0}^{fp-1} a_j x^j + x^{fp} - x^{fp+1} + x^{(f+1)p} + \sum_{j=(f+1)p+1}^{(p-1)(q-1)} a_j x^j.$$

Proof. See the extended version [4] of this paper. □

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 [8], that $\Psi_1(x) = 1$, $\Psi_p(x) = x - 1$ and

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

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 $|c_{pqr}(k)| \le [(p-1)(q-1)/r]+1 \le p-1$, where $[x]$ denotes the largest *integer* $\le x$. Let us call a ternary inverse cyclotomic polynomial $\Psi_{pqr}(x)$ extremal if for some k we have $|c_{pqr}(k)| = p - 1$. Moree [8] 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 it is 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 [10]) 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. ([5]). *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 square free 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 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:
$n = 7735 = 5 \cdot 7 \cdot 13 \cdot 17$, $\mathcal{C}(n) = [-7, 5] \backslash \{-6\}$
$n = 530689 = 17 \cdot 19 \cdot 31 \cdot 53$, $\mathcal{C}(n) = [-50, 52] \backslash \{-48, 47, 48, 49, 50, 51\}$.

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

Proof. See the extended version [4] of this paper. □

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 4. *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 study the coefficients of $\tau_{u,v}(x)$ by first considering the Taylor series around $x = 0$ of the denominator of $\tau_{u,v}(x)$. 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 $\mathcal{C}(\tau_{u,v}) \subseteq [-1, 1]$ 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 $\tau_{u,v} \equiv 1 - x (\text{mod } x^3)$ if $u \geq 3$. □

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

Lemma 5. *Let v be a positive integer with $3 \nmid v$. If $v \equiv 1 (\text{mod } 3)$, put*

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

If $v \equiv 2 (\text{mod } 3)$, put

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

We have $\tau_{3,v}(x) = f_v(x)$.

Proof. 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 $f_v(x) \equiv \tau_{3,v}(x) (\text{mod } x^v)$. We have $\deg(f_v) = 2v - 2 = \deg(\tau_{3,v})$, so 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 $v \equiv 1 (\text{mod } 3)$ 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 $v \equiv 2 (\text{mod } 3)$. □

Lemma 5 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 6. *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 5 that this property also holds. Proceeding as in the proof of Lemma 5 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 7. *Let $1 < u < v$ be coprime numbers. Put $h = (x-1)\tau_{u,v}(x)$. We have*

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

Proof. Put $d = (u-1)(v-1)$. Using the self-reciprocity of $\tau_{u,v}(x)$ we infer that $\tau_{u,v}(x) = x^d - x^{d-1} + \cdots - x + 1$. On writing $h(x) = \sum_j c_j x^j$, 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 4), we infer that $\{-2,-1,1,2\} \subseteq \mathcal{C}(h) \subseteq [-2,2]$. On invoking Corollary 2, the proof is then completed. □

Lemma 8. *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

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

It follows that $\mathcal{C}(\sigma_{u,v}) = [1,u]$. 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 of Lemma 8. See the extended version [4] of this paper. □

Lemma 9. *Let p and q be distinct primes. Put $f_{20} = \Phi_q\Phi_{p^2}$ We have*

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

Consequently f_{20} is flat iff $p > q$.

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

Lemma 10. *Let a, b, c be positive integers. Put*

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

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

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

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 $\mathcal{C}(\overline{g}) = [1, \mu]$.

Proof of Lemma 10. It is easy to find the maximum coefficient of g. 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. $c \ge a + b$. 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 numbers $\le \mu$ (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 $\le \mu$.

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 $c \le b$) we have to show that $\mu_{c_1} + 1$ also occurs as a 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 11. *Let p and q be distinct primes. Put $f_{24} = \Phi_{pq}\Phi_{p^2}$. Let $1 \le p^* \le q - 1$ be the inverse of p modulo q. Write $f_{24} = \sum_k c_k x^k$.*

1) *We have*

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

Consequently, 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_{24} equals

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

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 gives $c_{kp} = [\sigma_{p^*,p}(x)]_{x^k}$. 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 we have $1 \leq 2p^* < q$ 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 12. *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. See the extended version [4] of this paper. □

Lemma 13. *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 nonzero.*

Proof. Since $g = \sum c_j x^j$ is anti-self-reciprocal, it suffices to show that $c_j \neq 0$ for $0 \leq j \leq q+2$. Modulo x^{2q}, we have

$$g \equiv -(1 - 2x + x^2)(1 + 2x^3 + 3\sum_{j=2}^{\infty} x^{3j})(1 + x^q),$$

and so clearly $c_0, c_1, \ldots, c_{q-1}$ are all nonzero. By computation one checks that also c_q, c_{q+1} and c_{q+2} are nonzero. Alternatively the proof is completed on noting that the sum of any two coefficients in $(1 - 2x + x^2)(1 + 2x^3 + 3\sum_{j=2}^{\infty} x^{3j})$ that are q apart (here we use that $q \geq 5$) is nonzero. □

Lemma 14. *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 5 we find that

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

and hence $c_p = 0$. If $p \equiv 2 (\mathrm{mod}\ 3)$, then by Lemma 5 we find that

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

and hence $c_{p+2} = 0$. □

Lemma 15. *Put $f_{25} = (x-1)\Phi_{pq}\Phi_{p^2}$. Define $\gamma(p,q) = \min(p, p^*) + \min(p, q - p^*)$. Then*

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

Consequently, f_{25} is never flat.

Proof. See the extended version [4] of this paper. □

Lemma 16. *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 $q = 2$,

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

we easily compute that $d_j = 0$ with

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

This concludes the proof. □

Lemma 17. *Let p and q be distinct primes. Put $f_{30} = \Phi_p\Phi_q\Phi_{pq}\Phi_{p^2}$. We have*

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

Proof. Note that $f_{30} = (1 + x + \cdots + x^{pq-1})(1 + x^p + \cdots + x^{(p-1)p})$. 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 18. *We have $\mathcal{C}(f_{36}) = [-1, 1]$.*

Proof. See the extended version [4] of this paper. □

The next three lemmas will be used in order to establish Lemma 22.

Lemma 19. *Let p and q be distinct primes. Put $f_{38} = \Phi_p\Phi_q\Phi_{p^2q}$. We have $\mathcal{C}(f_{38}) \subseteq [-\min(p, q), \min(p, q)]$.*

Proof. Note that $f_{38} = \Phi_p f_{36} = \Phi_q f_{34}$. On using that $H(f_{34}) = 1$ (easy on using (5)) and $H(f_{36}) = 1$ (by Lemma 18) and invoking (3), it follows that $H(f_{38}) \leq \min(p, q)$. □

Lemma 20. *Let p and q be distinct odd 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 $[-\beta(p, q), 0] \subseteq \mathcal{C}(f_{38})$.*

Proof. See the extended version [4] of this paper. □

Lemma 21. *Let p and q be distinct odd primes. We have $\min \mathcal{C}(f_{38}) \geq -\beta(p, q)$.*

Proof. See the extended version [4] of this paper. □

In the proof of the next lemma we use the notation $\mathcal{C}_{\leq 0}(f)$ for $\mathcal{C}(f) \cap \mathbb{Z}_{\leq 0}$.

Lemma 22. *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*

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

Proof. Put $z_1 = \min(p,q)$. On noting that

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

we have $[1, \min(p,q)] \subseteq \mathcal{C}(f_{38})$. This in combination with Lemma 19 shows that $\mathcal{C}_{>0}(f_{38}) = [1, \min(p,q)]$. It remains to show that $\mathcal{C}_{\leq 0}(f_{38})$ is as asserted in the statement of the lemma.
1) The case $q = 2$. Here we have $\beta(p,2) = 2$.
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 $f_{38}(x) = 1 + 2x + 2x^2 + \ldots + 2x^{p-1} - 2x^{p+1} - 2x^{p+2} - \cdots - 2x^{2p-1} + 2x^{2p+1} + \ldots + 2x^{p^2-1} + x^{p^2}$ and hence $\mathcal{C}(f_{38}) = \{-2,0,1,2\}$.
2) The case $p = 2$. Here we have $\beta(2,q) = 1$.
If $q = 3$ we have to show (cf. statement of this lemma) that $\mathcal{C}_{\leq 0}(f_{38}) = \{-1\}$ (which follows by direct calculation) and for $q \geq 5$ that $\mathcal{C}_{\leq 0}(f_{38}) = [-1, 0]$.

We have

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

Assume $q \geq 5$. It is easy to see that $d_3 = 0$. Furthermore,

$$d_{q+1} = (-1)^{(q-1)/2}(1 + \sum_{j=1}^{(q-1)/2} (-1)^j 2) = -1.$$

It follows that $\mathcal{C}_{\leq 0}(f_{38}) = [-1, 0]$.
3) The case where both p and q are odd.
Here we invoke Lemma 20 and Lemma 21. □

Lemma 23. *Let p and q be distinct primes. Put $f_{39} = (x-1)\Phi_p\Phi_q\Phi_{p^2q}$. We have $\mathcal{C}(f_{39}) = [-2, 2]$.*

Proof. See the extended version [4] of this paper. □

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 results are not so easy to establish.

Lemma 24. *We have*

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

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

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

Lemma 25. *We have $\mathcal{C}(f_{42}) = [-1,1]$.*

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

$$(1+x^q+x^{2q}+\cdots)(1-x^p+x^{p^2}-x^{p^2+p}+\cdots+x^{(q-1)p^2}-x^{(q-1)p^2+p}). \quad (7)$$

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 $[-1,1] \subseteq \mathcal{C}(f_{42})$, the proof is completed. □

Indeed, some work needs to be done to infer that $\{-2,2\} \subseteq \mathcal{C}(f_{43})$. 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 $\rho(a,b)$ the smallest non-negative integer m such that $m \equiv a \pmod b$.

Lemma 26. *Write $f_{42} = \sum c_j x^j$ and $f_{43} = \sum d_j x^j$. Put*

$$k_1 = 1+\rho((p-1)p^{-2},q)p^2 \text{ and } k_2 = 1+\rho((p-1)q^{-1},p^2)q.$$

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

$$\rho(q^{-1},p^2)q + \rho(p^{-1},q)p^2 > p^2q \quad (8)$$

and

$$\rho(-q^{-1},p)pq + \rho(-p^{-2},q)p^2 + p + 1 > p^2q, \quad (9)$$

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

$$\rho(-q^{-1}, p^2)q + \rho(-p^{-1}, q)p^2 + p + 1 > p^2 q \tag{10}$$

and

$$\rho(q^{-1}, p)pq + \rho(p^{-2}, q)p^2 > p^2 q, \tag{11}$$

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 $m_1 \ge 0$ and $0 \le m_2 \le q - 1$. We say that k is *m-representable* if we can write $k = n_1 q + n_2 p^2 + p$ with $n_1 \ge 0$ and $0 \le n_2 \le q - 1$. From the proof of Lemma 25 it follows that if $k \le \deg(f_{42})$, then k can be p-representable in at most one way and be m-representable in at most one way. From this and (7), we infer that if $k \le \deg(f_{42})$, then

$$c_k = \begin{cases} 1 & \text{if } k \text{ is } p\text{-representable, but not } m\text{-representable;} \\ -1 & \text{if } k \text{ is } m\text{-representable, but not } p\text{-representable;} \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

We have

$$\begin{cases} k_1 \equiv 1 (\mathrm{mod}\ p^2); \\ k_1 \equiv p (\mathrm{mod}\ q), \end{cases} \quad \text{and} \quad \begin{cases} k_2 \equiv p (\mathrm{mod}\ p^2); \\ k_2 \equiv 1 (\mathrm{mod}\ q). \end{cases} \tag{13}$$

Suppose that $k_1 \le \deg(f_{42})$. Clearly k_1 is m-representable, because $k_1 > 1$ implies $k_1 > p$. Condition (8) ensures that k_1 is not p-representable. Thus, by (7), we have $c_{k_1} = -1$. On the other hand we see that $k_1 - 1$ is p-representable, but not m-representable by (9). 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 27. *Suppose that* $a > 1$ *and* $b > 1$ *are coprime integers. Then*

$$(a - \rho(b^{-1}, a), \rho(a^{-1}, b)) = (\rho(b^{-1}, a), b - \rho(a^{-1}, b)) = 1.$$

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

Proof. If $\rho(a^{-1}, b)$ is even, then $a - \rho(b^{-1}, a)$ must be odd and hence $\rho(b^{-1}, a)$ is even. If $\rho(a^{-1}, b)$ is odd, then $b - \rho(a^{-1}, b)$ is even and hence $\rho(b^{-1}, a)$ must be odd. □

Proof of Lemma 27. Put $\delta(a,b) = \rho(a^{-1},b)\rho(b^{-1},a) - (a-\rho(b^{-1},a))(b-\rho(a^{-1},b))$. 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

$$\delta(a,b) \equiv \rho(b^{-1},a)b \equiv 1 (\mathrm{mod}\ a) \text{ and } \delta(a,b) \equiv \rho(a^{-1},b)a \equiv 1 (\mathrm{mod}\ b),$$

and on invoking the Chinese remainder theorem the proof is completed. □

Lemma 28. *We have*

$$\rho(q^{-1},p^2)q + \rho(p^{-1},q)p^2 = \rho(-q^{-1},p)pq + \rho(-p^{-2},q)p^2 + p + 1$$

and

$$\rho(-q^{-1},p^2)q + \rho(-p^{-1},q)p^2 + p + 1 = \rho(q^{-1},p)pq + \rho(p^{-2},q)p^2.$$

Proof. Denote the numbers appearing in the left hand sides of (8), (9), (10) and (11), 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 $\rho(-q^{-1},p) = p - \rho(q^{-1},p)$, 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

$$k_j \equiv r_j(p,q) \equiv s_j(p,q) (\mathrm{mod}\ p^2q) \text{ for } 1 \le j \le 2. \tag{14}$$

Note that

$$\{r_j(p,q), s_j(p,q)\} \subseteq \{k_j, k_j + p^2q\} \text{ for } 1 \le j \le 2. \tag{15}$$

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

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

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, modulo 2, $\rho(q^{-1},p^2) \equiv \rho(p^{-2},q)$ and $\rho(p^{-1},q) \equiv$

$\rho(q^{-1}, p)$ and hence

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

which finishes the proof. □

Lemma 29. *Write $f_{43} = \sum_j d_j x^j$. There is a unique integer $1 \le j \le 2$ such that the conditions of part j of Lemma 26 are satisfied and hence $d_{k_j} = 2$. Furthermore, $d_{\deg(f_{42})-k_j+1} = -2$.*

Proof. We consider the cases $p \not\equiv 1 (\mathrm{mod}\ q)$ and $p \equiv 1 (\mathrm{mod}\ q)$ separately.
i) The case $p \not\equiv 1 (\mathrm{mod}\ q)$.
We have $q \ge 3$ and $k_1 > 1$. From (13) we infer that $k_1 + k_2 \equiv 1 + p (\mathrm{mod}\ p^2 q)$. Since clearly $1 + p < 1 + p^2 \le k_1 + k_2 < 1 + p + 2p^2 q$, we infer that

$$k_1 + k_2 = 1 + p + p^2 q. \tag{16}$$

Let us suppose that $k_1 \ge p^2(q-1) + p - q + 1 = \deg(f_{43}) = 1 + \deg(f_{42})$. By (16) 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 $r_2(p, q) \equiv k_2 (\mathrm{mod}\ p^2 q)$, we have $r_2(p, q) = k_2 + p^2 q > p^2 q$. Since $r_2(p, q) = s_2(p, q)$ by Lemma 28, it follows that if $k_1 > \deg(f_{42})$ and thus the conditions of part 1 (of Lemma 26) 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

$$r_1(p, q) + r_2(p, q) = 1 + p + 2p^2 q. \tag{17}$$

Hence $r_j(p, q) > p^2 q$ for some $1 \le j \le 2$. Let us assume w.l.o.g. that $r_2(p, q) > p^2 q$. Now if $r_1(p, q) > p^2 q$, then on using (15) we find

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

contradicting (17) and hence the conditions of both part 1 and part 2 cannot be satisfied at the same time.
ii) The case $p \equiv 1 (\mathrm{mod}\ q)$.
Here we can write $p = kq + 1$, with $k \ge 1$. We have $k_1 = 1 + 0p^2 = 1$ and $k_2 = 1 + kq = p$ and hence the conditions of part 1 are not satisfied. We

have to show that the conditions of part 2 are satisfied. Obviously $k_2 = p \leq \deg(f_{42})$. On noting that $\rho(-q^{-1}, p^2) = k^2q + 2k$ and $\rho(-p^{-1}, q) = q - 1$, the left side of equation (10) 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 (11):

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

(Alternatively one can invoke Lemma 28 to deduce that the left hand side of (11) equals the left hand side of (10) and hence exceeds p^2q.)

In both cases i) and ii), we conclude that there is a unique integer j such the conditions of part j of Lemma 26 are satisfied.

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

Proof of Lemma 24. By (3) and Lemma 25 we find that $\mathcal{C}(f_{43}) \subseteq [-2, 2]$. By Lemma 29 we have $\{-2, 2\} \subseteq C(f_{43})$. Since $d_0 = -1$ and $d_{\deg(f_{43})} = 1$, it remains to be determined 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 $j \leq \deg(f_{43}) = p^2 + p - 1$ and hence $0 \notin \mathcal{C}(f_{43})$.
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

$$x^{p^2q} - 1 = \Phi_1(x)\Phi_p(x)\Phi_q(x)\Phi_{pq}(x)\Phi_{p^2}(x)\Phi_{p^2q}(x), \tag{18}$$

we infer that $x^{p^2q} - 1$ has 64 divisors. We denote these by $f_0, \ldots, f_{63}$. If $k = \sum_{j=0}^{5} k_j 2^j$ 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 (18) is flat.

We will only establish the less trivial cases in Table 1, the easier ones being left as exercises to the reader. (Note that for some polynomials like f_{19} we have given more than one argument.)

-$f_0, f_1, f_2, f_3, f_4, f_5, f_{16}, f_{17}, f_{18}, f_{19}$: Use Theorem 1.
-f_6. Use Lemma 8.
-f_7. Use Corollary 3.
-f_8: Use Lemma 4.
-f_9. Use Lemma 7.
-$f_{16}, f_{17}, f_{18}, f_{32}, f_{33}, f_{34}$: Use identity (4).
-f_{20}: See Lemma 9.
-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 11.
-f_{25}: Invoke Lemma 15.
-f_{26}, f_{27}: Invoke Lemma 16.
-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 8), 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 17.
-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}: $f_{35} = (x^p - 1)\Phi_{pq}(x^p) = f_9(x^p)$. It follows that $\mathcal{C}(f_{35}) = \mathcal{C}(f_9) \cup \{0\}$. Now invoke Lemma 7.
-f_{36}: Invoke Lemma 18.
-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 22.
-f_{39}. Invoke Lemma 23.
-f_{40}: We have $f_{40} = \tau_{p^2,q}(x)$. Now invoke Lemma 4.
-f_{41}. Invoke Lemma 7.
-f_{42}. Invoke Lemma 25.
-f_{43}. Invoke Lemma 24.
-f_{44}: We have $\Phi_q(x)\Phi_{pq}(x)\Phi_{pq}(x^p) = (x^{p^2q} - 1)/(x^{p^2} - 1)$.

-$f_{48}, f_{49}, \ldots, f_{63}$.

Let $0 \leq j \leq 15$. 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 $\deg(f_j) \geq pq - 1$ 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 1

Table 1 comes in 4 parts, 1A, 1B, 1C and 1D, each listing $\mathcal{C}(f)$ for 16 monic divisors of $x^{p^2q} - 1$. For each of the tables there are some exceptions to the set $\mathcal{C}(f)$ given in the table and these are listed directly below the table. If $\min(p, q) > 3$, then there are no exceptions and $\mathcal{C}(f)$ can be read off directly from the table.

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 $\min(p,q) \leq 3$, 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 $1 \leq p^* < q$ 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 $p \leq 3$ 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 $\beta(p,q) = \min(p, q, q(\mathrm{mod}\ p^2), p^2 - q(\mathrm{mod}\ p^2))$.
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	$[-1,1]$

Table 1D (continued)

f	$\Phi_1(x)$	$\Phi_p(x)$	$\Phi_q(x)$	$\Phi_{pq}(x)$	$\Phi_{p^2}(x)$	$\Phi_{p^2q}(x)$	$\mathcal{C}(f)$
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 $1 \le p < q$ such that $pp^* \equiv 1 (\mathrm{mod}\ q)$ 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* $k \in \{28, 54\}$,
- $[\min([q/p],\ 1), \min([(q-1)/p] + 1,\ p)]$ *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* $k = 29$,
- $[-\min(p,\ q,\ q (\mathrm{mod}\ p^2),\ p^2 - q (\mathrm{mod}\ p^2)),\ \min(p,\ q)]$ *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* $\min(p,\ q) \leq 3$,
- $k = 25$ *and* $p \leq 3$ *and* $q \neq 2$,
- $k = 38$ *and* $p = 2$ *and* $q = 3$,
- $k = 41$ *and* $q \leq 3$.

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 $B(n) = H^*(x^n - 1)$. So far little is known about this function, see Pomerance and Ryan [9] and Thompson [13] for some results. In particular Pomerance and Ryan observe that from their limited numerical data it seems that if p and q are different primes, then $B(p^2q) = \min(p^2, q)$. This was subsequently proved by Kaplan [6]. Our work presented here leads to a reproof and a sharpening of this result (Theorem 4). 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 $x^n - 1$

Our work 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 10. *Let* p *and* q *be distinct primes. Let* f_e *be the number of flat monic divisors of* $x^{p^eq} - 1$*. Then* $f_{e+1} \geq 2f_e + 2^{e+2} - 1$.

Proof. See the extended version [4] of this paper. □

Remark. 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 $x^{p^eq} - 1$ 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 that $H(f_{22}) = \min(p^2, q) = B(p^2q)$. 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 11. *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 consequence of the inequality $\min(p, p^*) + \min(p, q - p^*) \geq \min(p, q)$ and Theorem 5. It does not follow from earlier work in this area ([6, 9, 11]).

Acknowledgement. Yves Gallot numerically verified Theorem 5 in the case that $\max(p, q) < 200$ and provided a reformulation of our main result not involving any tables (Theorem 9). Merci beaucoup, Yves!

References

[1] G. Bachman, *On ternary inclusion-exclusion polynomials*, Integers, 10 (2010), A48, 623–638.
[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] A. Decker and P. Moree, *Coefficient convexity of divisors of* $x^n - 1$, arXiv:1010.3938, pp. 34 (extended version of present paper).
[5] Y. Gallot and P. Moree, *Neighboring ternary cyclotomic coefficients differ by at most one*, J. Ramanujan Math. Soc., 24 (2009), 235–248.
[6] N. Kaplan, *Bounds for the maximal height of divisors of* $x^n - 1$, J. Number Theory, 129 (2009), 2673–2688.
[7] T.Y. Lam and K.H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, 103 (1996), 562–564.
[8] P. Moree, *Inverse cyclotomic polynomials*, J. Number Theory, 129 (2009), 667–680.
[9] C. Pomerance and N. C. Ryan, *Maximal height of divisors of* $x^n - 1$, Illinois J. Math., 51 (2007), 597–604.
[10] S. Rosset, *The coefficients of cyclotomic like polynomials of order 3*, unpublished manuscript (2008), pp. 5.
[11] N.C. Ryan, B.C. Ward and R. Ward, *Some conjectures on the maximal height of divisors of* $x^n - 1$, Involve 3 (2010), 451–457.
[12] R. Thangadurai, *On the coefficients of cyclotomic polynomials, Cyclotomic fields and related topics*, (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.

[13] L. Thompson, *Heights of divisors of* $x^n - 1$, Integers, 11A, Proceedings of the Integers Conference 2009 (2011), Article 20, 1–9.

(Received: February 17, 2012)
(Revised: October 2, 2012)

Andreas Decker
Achtern Diek 32
D-49377 Vechta, Germany
E–mail: andreasd@uni-bonn.de

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