Reciprocal cyclotomic polynomials

Pieter Moree

Abstract

Let $\Psi_n(x)$ be the monic polynomial having precisely all non-primitive nth roots of unity as its simple zeros. One has $\Psi_n(x) = (x^n - 1)/\Phi_n(x)$, with $\Phi_n(x)$ the nth cyclotomic polynomial. The coefficients of $\Psi_n(x)$ are integers that like the coefficients of $\Phi_n(x)$ tend to be surprisingly small in absolute value, e.g. for $n < 561$ all coefficients of $\Psi_n(x)$ are ≤ 1 in absolute value. We establish various properties of the coefficients of $\Psi_n(x)$.

1 Introduction

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

$$\Phi_n(x) = \prod_{\substack{1\le j\le n\\(j,n)=1}} (x - \zeta_n^j) = \sum_{k=0}^{\varphi(n)} a_n(k)x^k,$$

where φ is Euler's totient function and ζ_n a primitive nth root of unity. The coefficients $a_n(k)$ are known to be integral. The study of the $a_n(k)$ began with the startling observation that for small n we have $|a_n(k)| \le 1$. The first counterexample to this inequality occurs for $n = 105$: $a_{105}(7) = -2$. The amazement over the smallness of $a_n(m)$ was eloquently phrased by D. Lehmer [10] who wrote: 'The smallness of $a_n(m)$ would appear to be one of the fundamental conspiracies of the primitive nth roots of unity. When one considers that $a_n(m)$ is a sum of $\binom{\phi(n)}{m}$ unit vectors (for example 73629072 in the case of $n = 105$ and $m = 7$) one realizes the extent of the cancellation that takes place'.

We define $\Psi_n(x)$ by

$$\Psi_n(x) = \prod_{\substack{1\le j\le n\\(j,n)>1}} (x - \zeta_n^j) = \sum_{k=0}^{n-\varphi(n)} c_n(k)x^k.$$

Note that $\Psi_n(x) = (x^n - 1)/\Phi_n(x)$. The identity $x^n - 1 = \prod_{d|n} \Phi_d(x)$ shows that

$$\Psi_n(x) = \prod_{d|n,d<n} \Phi_d(x),$$

Mathematics Subject Classification (2000). 11B83, 11C08 and thus the coefficients of $\Psi_n(x)$ are integers.

Note that for $|x| < 1$ we have

$$\frac{1}{\Phi_n(x)} = -\Psi_n(x)(1 + x^n + x^{2n} + \cdots).$$

Since $n > n - \varphi(n)$, it follows that the Taylor coefficients of $1/\Phi_n(x)$ are periodic with a period dividing n. This allows one to easily reformulate the results on the coefficients of $\Psi_n(x)$ obtained in this paper to the Taylor coefficients of $1/\Phi_n(x)$ as well.

The purpose of this note is to show that the non-primitive roots, like the primitive ones, conspire and study the extent to which this is the case.

2 Some basics

Note that

$$x^n - 1 = \prod_{d|n} \prod_{\substack{1 \le j \le n \\ (j,n)=d}} (x - \zeta_n^j) = \prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x). \tag{1}$$

It follows from this identity that

$$\Psi_n(x) = \frac{x^n - 1}{\Phi_n(x)} = \prod_{\substack{d|n \\ d<n}} \Phi_d(x). \tag{2}$$

We infer that $\Psi_n(x) \in \mathbb{Z}[x]$.

Lemma 1 *Let $n > 1$. We have*

$$\Psi_n(x) = -\prod_{\substack{d|n \\ d<n}} (1 - x^d)^{-\mu(\frac{n}{d})}.$$

Proof. By applying Möbius inversion one deduces from (1) that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}. \tag{3}$$

On using that $\sum_{d|n} \mu(n/d) = 0$, we infer that $\Phi_n(x) = \prod_{d|n}(1 - x^d)^{\mu(\frac{n}{d})}$, from which the result follows on invoking (2). □

Let $\mathrm{rad}(n) = \prod_{p|n} p$ be the *radical* of n. From the previous lemma it is not difficult to arrive at the next result, see e.g. Thangadurai [17] for the proof of the corresponding result for $\Phi_n(x)$.

Lemma 2 *Let $n > 1$. We have:*
1) $\Psi_{2n}(x) = (1 - x^n)\Psi_n(-x)$ *if n is odd;*
2) $\Psi_{pn}(x) = \Psi_n(x^p)$ *if $p|n$;*
3) $\Psi_{pn}(x) = \Psi_n(x^p)\Phi_n(x)$ *if $p \nmid n$;*
4) $\Psi_n(x) = \Psi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})$;
5) $\Psi_n(x) = -\Psi_n(\frac{1}{x})x^{n-\varphi(n)}$.

Put $V_n = \{c_n(k) : 0 \le k \le n-\varphi(n)\}$. If $n>1$ then by part 5 of the latter lemma we have that $a \in V_n$ implies that $-a \in V_n$. It also gives that if $n-\varphi(n)$ is even, then $c_n((n-\varphi(n))/2) = 0$.

Lemma 3 *If $n = 1$, then $V_n = \{1\}$. If n is a prime, then $V_n = \{-1, 1\}$. In the remaining cases we have $\{-1, 0, 1\} \subseteq V_n$.*

Proof. If $n = 1$, then $\Psi_n(x) = 1$. If n is a prime, then $\Psi_n(x) = x-1$. Next assume that n has at least two (not necessarily distinct) prime divisors. Note that this implies that $n - \varphi(n) \ge 2$. Note that $\Psi_n(x)$ is monic and that $\Psi_n(0) = -1$ by Lemma 1. It thus remains to be shown that $0 \in V_n$. In case n is not squarefree we have $\Psi_n(x) = -1 + O(x^2)$ by Lemma 1 and thus $c_n(1) = 0$. If n is odd and squarefree and $\mu(n) = -1$, then by Lemma 1 we find $\Psi_n(x) = -1 + x + O(x^3)$ and hence $c_n(2) = 0$ (here we use that $n - \varphi(n) \ge 2$). If n is odd and squarefree and $\mu(n) = 1$, then by Lemma 1 we find

$$\Psi_n(x) = \frac{(x^p - 1)}{1-x}(1 + O(x^{p+1})),$$

where p is the smallest prime divisor of n and hence $c_n(p) = 0$. Since $p \le n-\varphi(n)$ it follows that $0 \in V_n$. In case n is even and squarefree we invoke part 1 of Lemma 2 to complete the proof. $\square$

It is not difficult to prove that, as x tends to infinty,

$$\sum_{n \le x} \frac{\varphi(n)}{n} \sim \frac{x}{\zeta(2)} = x\frac{6}{\pi^2}.$$

Thus the average degree of $\Phi_n(x)$ and $\Psi_n(x)$ is $\frac{6}{\pi^2}n$, respectively $(1-\frac{6}{\pi^2})n$. We have $\frac{6}{\pi^2} = 0.60792710\cdots$ and $1 - \frac{6}{\pi^2} = 0.3920728\cdots$.

2.1 (Reciprocal) cyclotomic polynomials of low order

We define the order of $\Phi_n(x)$ and $\Psi_n(x)$ to be the number, $\omega_1(n)$, of distinct odd prime divisors of n. Instead of saying that f has order 3, we sometimes say that f is ternary. We define the *height* of a polynomial f in $\mathbb{Z}[x]$, $h(f)$, to be the maximum absolute value of the coefficients of f. In case $h(f) = 1$ we say that f is *flat*.

Low order examples (in the remainder of this section $p < q < r$ will be primes):
$\Psi_1(x) = 1$;
$\Psi_p(x) = -1 + x$;
$\Psi_{pq}(x) = -1 - x - x^2 - \ldots - x^{p-1} + x^q + x^{q+1} + \ldots + x^{p+q-1}$.
These examples in combination with parts 1 and 4 of Lemma 2 establish the correctness of the following result.

Lemma 4 *If $\Psi_n(x)$ is of order ≤ 2, then $\Psi_n(x)$ is flat.*

We like to point out that $\Psi_{pq}(x)$ has a rather simpler structure than $\Phi_{pq}(x)$. It can be shown, see e.g. Carlitz [7], Lam and Leung [9] and Thangadurai [17], that

$$\begin{aligned}\Phi_{pq}(x) &= \sum_{i=0}^{\rho} x^{ip} \sum_{j=0}^{\sigma} x^{jq} - x^{-pq} \sum_{i=\rho+1}^{q-1} x^{ip} \sum_{j=\sigma+1}^{p-1} x^{jq} \\ &= \sum_{i=0}^{\rho} x^{ip} \sum_{j=0}^{\sigma} x^{jq} - x \sum_{i=0}^{q-2-\rho} x^{ip} \sum_{j=0}^{p-2-\sigma} x^{jq},\end{aligned}$$

where ρ and σ are the unique nonnegative integers for which $(p-1)(q-1) = \rho p + \sigma q$ (note that $\rho \le q-2$ and $\sigma \le p-2$). As a consequence we have the following evaluation of the coefficients $a_{pq}(k)$.

Lemma 5 *Let $p < q$ be odd primes. Let ρ and σ be the unique nonnegative integers for which $(p-1)(q-1) = \rho p + \sigma q$. Then*

$$a_{pq}(k) = \begin{cases} 1 & \text{if } k = ip + jq \text{ for some } 0 \le i \le \rho,\ 0 \le j \le \sigma; \\ -1 & \text{if } k = 1 + ip + jq \text{ for some } 0 \le i \le q-2-\rho, 0 \le j \le p-2-\sigma; \\ 0 & \text{otherwise.} \end{cases}$$

Using the latter lemma it is easy to show that if $\Phi_n(x)$ is of order ≤ 2, then $\Phi_n(x)$ is flat.

For the convenience of the reader we will prove that there are unique nonnegative integers such that $(p-1)(q-1) = \rho p + \sigma q$ (this proof is taken from Ramírez Alfonsín's book [15, p. 34], with the observation that in case p and q are primes the auxiliary polynomial $Q(x)$ equals $\Phi_{pq}(x)$). We let $r(n)$ be the number of representations of n in the form $n = px + qy$ with $x, y \ge 0$. We have

$$R(x) = \sum_{i=0}^{\infty} r(i) x^i = \frac{1}{(1-x^p)(1-x^q)}.$$

Note that $R(x)(x^{pq}-1)(x-1) = \Phi_{pq}(x)$. By L'Hôpital's rule we find that $\Phi_{pq}(1) = 1$ and hence we have that

$$\frac{\Phi_{pq}(x)-1}{x-1} = \sum_{i=0}^{pq-p-q} g(i) x^i,$$

with $g(pq-p-q) = 1$. On the other hand,

$$\begin{aligned}\frac{\Phi_{pq}(x)-1}{x-1} &= R(x)(x^{pq}-1) + \frac{1}{1-x}; \\ &= \sum_{i=0}^{\infty} r(i) x^{pq+i} + \sum_{i=0}^{\infty} (1-r(i)) x^i; \\ &= \sum_{i=0}^{pq-1} (1-r(i)) x^i + \sum_{i=pq}^{\infty} (r(i-pq) + 1 - r(i)) x^i.\end{aligned}$$

On comparing the two expressions for $(\Phi_{pq}(x)-1)/(x-1)$ we arrive at various conclusions. First of all we see that $r((p-1)(q-1)) = 1$. Secondly it allows one to compute the *Frobenius number* $g(p,q)$. Given relatively prime positive integers $a_1,\ldots,a_n$ the largest natural number that is not representable as a non-negative integer combination of $a_1,\ldots,a_n$ is called the Frobenius number and denoted by $g(a_1,\ldots,a_n)$. On noting that $r(i-pq)\le r(i)$ comparison of the two expressions for $(\Phi_{pq}(x)-1)/(x-1)$ shows that $r(pq-p-q)=0$ and $r(pq-p-q+i)\ge 1$ for $i\ge 1$, which yields $g(p,q)=pq-p-q$.

By Lemma 1 we have

$$\Psi_{pqr}(x)=\frac{(x-1)(1-x^{pq})(1-x^{pr})(1-x^{qr})}{(1-x^p)(1-x^q)(1-x^r)}.$$

This can be written as

$$\Psi_{pqr}(x)=(x-1)\Big(\sum_{j_1=0}^{q-1}x^{j_1p}\Big)\Big(\sum_{j_2=0}^{r-1}x^{j_2q}\Big)\Big(\sum_{j_3=0}^{p-1}x^{j_3r}\Big). \tag{4}$$

Alternatively we can write, by part 3 of Lemma 2,

$$\Psi_{pqr}(x)=\Phi_{pq}(x)\Psi_{pq}(x^r). \tag{5}$$

Let the *denumerant* be defined as the number of non-negative integer representations of m by $a_1,a_2,\ldots,a_n$. Denote it by $d(m;a_1,\ldots,a_n)$. For $m<pq$ we infer from (4) that $c_{pqr}(k)=d(m-1;p,q)-d(m;p,q)$. For more on denumerants see Chapter 4 of Ramírez Alfonsín [15].

Lemma 6 *Let $p<q<r$ be odd primes. If $0\le k<r$, then we have $c_{pqr}(k)=-a_{pq}(k)\in\{-1,0,1\}$.*

Proof. Immediate from (5), $\Psi_{pq}(0)=-1$ and Lemma 5. □

The following result also relates $c_{pqr}(k)$ to $a_{pq}(k)$ in case $k>r$. (If k is outside the range $[0,\ldots,\varphi(n)]$ respectively, $[0,\ldots,n-\varphi(n)]$, then we put $a_n(k)=0$, respectively $c_n(k)=0$.

Lemma 7 *Let $p<q<r$ be odd primes. Put $\tau=(p-1)(r+q-1)$. Suppose that $qr>\tau$. If $k\le\tau$, then*

$$c_{pqr}(k)=-\sum_{j=0}^{m}a_{pq}(k-jr),$$

with m the unique integer such that $mr\le k<(m+1)r$. Furthermore,

$$c_{pqr}(\tau-k)=c_{pqr}(k) \tag{6}$$

and $c_{pqr}(k+qr)=-c_{pqr}(k)$. If $\tau<k<qr$, then $c_{pqr}(k)=0$.

Proof. We have

$$\Psi_{pqr}(x)=\Phi_{pq}(x)(1+x^r+\ldots+x^{(p-1)r})(x^{qr}-1). \tag{7}$$

Write

$$\Phi_{pq}(x)(1+x^r+\ldots+x^{(p-1)r})=\sum_{k=0}^{\tau}e_{pqr}(k)x^k. \tag{8}$$

Note that the polyniomal in (8) of degree τ and selfreciprocal. If $k\le\tau$, then $c_{pqr}(k)=-e_{pqr}(k)$ and $c_{pqr}(k+qr)=e_{pqr}(k)$. On combining all these observations the result easily follows. □

In 1895 Bang [4] proved that $h(\Phi_{pqr}(x))\le p-1$. The same bound applies to the height of $\Psi_{pqr}(x)$.

Theorem 1 *The height of $\Psi_{pqr}(x)$ is at most $p-1$. More precisely, we have*

$$h(\Psi_{pqr}(x))\le\Big[\frac{(p-1)(q-1)}{r}\Big]+1.$$

Proof. By (5) we find that

$$c_{pqr}(k)=\sum_{j=0}^{[k/r]}a_{pq}(k-jr)c_{pq}(j). \tag{9}$$

The number of j for which $0\le k-jr\le\varphi(pq)$ is

$$\le\Big[\frac{\varphi(pq)}{r}\Big]+1=\Big[\frac{(p-1)(q-1)}{r}\Big]+1\le p-2+1=p-1.$$

The proof is finished since $|a_{pq}(k-jr)|\le 1$ by Lemma 5 and $|c_{pq}(j)|\le 1$ by the identity $\Psi_{pq}(x)=-1-x-x^2-\ldots-x^{p-1}+x^q+x^{q+1}+\ldots+x^{p+q-1}$. □

We have seen that on average the degree of $\Phi_n(x)$ is less than that of $\Psi_n(x)$. It is left to the reader to show that if $p<q<r$ are odd primes, then $\deg(\Psi_{pqr}(x))<\deg(\Phi_{pqr}(x))$, except when $pqr\in\{105,165,195\}$.

3 Beiter's conjecture and its reciprocal analogue

In 1971 Sister Marion Beiter [5] put forward the conjecture that if $p<q<r$ are odd primes, then $\Phi_{pqr}(x)$ is of height at most $(p+1)/2$. As she pointed out, her conjecture is true for $p\le 5$. She also showed that the height is $\le p-\lfloor p/4\rfloor$. Bachman [1] showed that if either q or r is congruent to ±1 or ±2 modulo p, then the height is $\le(p+1)/2$. H. Möller [12] gave explicit examples of polynomials $\Phi_{pqr}(x)$, for every p, with a prescribed coefficient equal to $(p+1)/2$. This shows that the conjecture is best possible, if true. More precisely, Möller showed that if $q\equiv-2(\bmod p)$, $r\equiv-(p-1)(q-1)/2(\bmod pq)$, then $a_{pqr}((p-1)(qr+1)/2)=(p+1)/2$. For further results and references see Bachman [1, 2]. In general Beiter's conjecture remains unresolved.

The following result gives the analogue of the Beiter conjecture for the reciprocal polynomials.

Theorem 2 *Let $p < q < r$ be odd primes. Then $h(\Psi_{pqr}(x)) = p - 1$ iff*

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

In the remaining cases $h(\Psi_{pqr}(x)) < p - 1$.

Corollary 1 *Suppose that $h(\Psi_{pqr}(x)) = p - 1$ and $q + 2p$ is a prime, then also $h(\Psi_{pq(q+2p)}(x)) = p - 1$.*

By the above theorem and Dirichlet's theorem on arithmetic progressions it follows that for every prime $p \geq 3$ there are infinitely many pairs (q, r) such that $h(\Psi_{pqr}(x)) = p - 1$.

Theorem 2 follows from two theorems that deal with the necessity, respectively sufficiency part of its iff statement in combination with Theorem 1.

Theorem 3 *If $h(\Psi_{pqr}(x)) = p - 1$, then*

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

Proof. Let $j_{\min}$ be the smallest j such that $k - jr \leq \varphi(pq)$ and $j_{\max}$ be the largest j such that $k - jr \geq 0$. Then we can write (9) as

$$c_{pqr}(k) = \sum_{j=j_{\min}}^{j_{\max}} a_{pq}(k - jr) c_{pq}(j).$$

From $k - j_{\max} r \geq 0$ and $k - j_{\min} r \leq (p-1)(q-1)$ we infer that $(j_{\max} - j_{\min}) r \leq (p-1)(q-1) < (p-1)r$ and hence $j_{\max} - j_{\min} \leq p - 2$. In order to have $c_{pqr}(k) = p - 1$ for some k we must have $j_{\max} - j_{\min} = p - 2$. Thus $(j_{\max} - j_{\min}) r = (p-2)r \leq (p-1)(q-1)$. Since $(p-2)r$ is odd and $(p-1)(q-1)$ is even it follows that

$$r < \frac{(p-1)}{(p-2)}(q-1).$$

Let k be such that $|c_{pqr}(k)| = p - 1$. Then we must have that $c_{pq}(j) \neq 0$ for $j_{\min} \leq j \leq j_{\max}$. It follows from this that the pair $(j_{\min}, j_{\max})$ must be one of the following: $(0, p-2)$, $(1, p-1)$, $(q, q+p-2)$, $(q+1, q+p-1)$, and that $c_{pq}(j_{\min}) = c_{pq}(j_{\min} + 1) = \ldots = c_{pq}(j_{\max})$. Thus we have

$$p - 1 = |c_{pqr}(k)| = \Big| \sum_{j=j_{\min}}^{j_{\max}} a_{pq}(k - jr) \Big|.$$

We now make a case distinction according to whether $a_{pq}(k - jr) = 1$ for $j_{\min} \leq j \leq j_{\max}$, or $a_{pq}(k - jr) = -1$ for every $j_{\min} \leq j \leq j_{\max}$.

`First case.` For every $j_{\min} \leq j \leq j_{\max}$ we have $a_{pq}(k - jr) = 1$.

By Lemma 5 it follows that there must be non-negative integers i_m and j_m with $0 \leq i_m \leq \rho$ and $0 \leq j_m \leq \sigma$ such that

$$\begin{cases} k - j_{\max} r & = i_1 p + j_1 q; \\ k - (j_{\max} - 1) r & = i_2 p + j_2 q; \\ \cdots & = \cdots \\ k - j_{\min} r & = i_{p-1} p + j_{p-1} q, \end{cases}$$

Now if we would have $j_{m_1} = j_{m_2}$ for $m_1 \neq m_2$ by subtracting the corresponding equations we infer that $p|r$, a contradiction. Thus we must have $\{j_1, \ldots, j_{p-1}\} = \{0, 1, \ldots, p-2\}$ and hence $\sigma = p-2$. It follows that $q \equiv -1 (\text{mod } p)$ and $\rho = (q-p+1)/p$. Now select m_1 and m_2 such that $j_{m_2} = j_{m_1}+1$. On substracting the corresponding equations we infer that $\alpha r = \beta p + q$ for some integers α and β with $-\rho \leq \beta \leq \rho$. Note that $p-1 \leq \beta p + q < 2q - p + 1 < 2r$. It follows that $\alpha = 1$ and $r = \beta p + q$ and hence $r \equiv q \equiv -1 (\text{mod } p)$.
`Second case`. For every $j_{\min} \leq j \leq j_{\max}$ we have $a_{pq}(k - jr) = -1$.
By Lemma 5 it then follows that there must be non-negative integers i_m and j_m with $0 \leq i_m \leq q-2-\rho$ and $0 \leq j_m \leq p-2-\sigma$ such that

$$\begin{cases} k - j_{\max} r & = 1 + i_1 p + j_1 q; \\ k - (j_{\max} - 1) r & = 1 + i_2 p + j_2 q; \\ \cdots & = \cdots \\ k - j_{\min} r & = 1 + i_{p-1} p + j_{p-1} q, \end{cases}$$

For the same reason as above we must have $\{j_1, \ldots, j_{p-1}\} = \{0, 1, \ldots, p-2\}$. This implies $\sigma = 0$. It follows that $q \equiv 1 (\text{mod } p)$ and $\rho = (p-1)(q-1)/p$ and thus $\rho' := q-2-\rho = (q-p-1)/p$. Now select m_1 and m_2 such that $j_{m_2} = j_{m_1}+1$. On substracting the corresponding equations we infer that $\alpha r = \beta p + q$ for some integers α and β with $-\rho' \leq \beta \leq \rho'$. Note that $p+1 \leq \beta p + q < 2q - p - 1 < 2r$. It follows that $\alpha = 1$ and $r = \beta p + q$ and hence $r \equiv q \equiv 1 (\text{mod } p)$. □

Theorem 4 *Let $p < q < r$ be odd primes such that $r < (p-1)(q-1)/(p-2)$. If $q \equiv -1 (\text{mod } p)$ and $r \equiv -1 (\text{mod } p)$, then*

$$c_{pqr}(k) = \begin{cases} -1-m & \text{for } 0 \leq m \leq p-2,\ k = mr; \\ 0 & \text{for } k = 2; \\ m+1 & \text{for } 0 \leq m \leq p-2,\ k = (m+q)r, \end{cases}$$

and $V_{pqr} = \{-(p-1), -(p-2), \ldots, p-2, p-1\}$.

If $q \equiv 1 (\text{mod } p)$ and $r \equiv 1 (\text{mod } p)$, then

$$c_{pqr}(k) = \begin{cases} 1+m & \text{for } 0 \leq m \leq p-2,\ k = 1 + mr; \\ 0 & \text{for } k = 2; \\ -1-m & \text{for } 0 \leq m \leq p-2,\ k = 1 + (m+q)r, \end{cases}$$

and $V_{pqr} = \{-(p-1), -(p-2), \ldots, p-2, p-1\}$.

Proof. From the proof of Lemma 3 it follows that $c_{pqr}(2) = 0$.
`First case`. Assume that $q \equiv r \equiv -1 (\text{mod } p)$.
Note that $\rho = (q-p+1)/p$ and $\sigma = p-2$. Notice furthermore that we can write $r = \alpha p + q$ with $\alpha = (r-q)/p \geq 0$. The condition $r < (p-1)(q-1)/(p-2)$ ensures that $(p-2)\alpha \leq \rho$. Let $0 \leq m \leq p-2$ be arbitrary. We have $mr = m\alpha p + mq$ with $0 \leq m\alpha \leq (p-2)\alpha \leq \rho$ and $0 \leq m \leq \sigma = p-2$. By Lemma 5 we then infer that $a_{pq}(mr) = 1$. On invoking Lemma 7 and Theorem 1 the proof of this case is then completed.
`Second case`. Assume that $q \equiv r \equiv 1 (\text{mod } p)$.
We claim that $r(p-2) \leq (p-1)(q-1) - 2$. By assumption we have $r(p-2) <$

$(p-1)(q-1)$. Suppose that $r(p-2) = (p-1)(q-1)-1$. By considering this equation modulo p we see that it is impossible and thus $r(p-2) \le (p-1)(q-1)-2$. Note that $\sigma = 0$ and $\rho = (p-1)(q-1)/p$. We can write $r = \alpha p + q$ with $\alpha = (r-q)/p \ge 0$. The condition $r(p-2) \le (p-1)(q-1)-2$ ensures that $(p-2)\alpha \le q-2-\rho$. Let $0 \le m \le p-2$ be arbitrary. We have $1+mr = 1+m\alpha p+mq$ with $0 \le m\alpha \le (p-2)\alpha \le q-2-\rho$ and $0 \le m \le p-2-\sigma = p-2$. By Lemma 5 we then infer that $a_{pq}(1+mr) = 1$. On invoking Lemma 7 and Theorem 1 the proof of this case is then also completed. □

`Remark`. (Y. Gallot.) The above result suggests perhaps that in case n is of order at least two, V_n is always of the form $\{-a, -(a-1), \cdots, -1, 0, 1, \cdots, (a-1), a\}$ for some positive integer a. However, this is not the case. The smallest n for which V_n is not of this form 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 V_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 values smaller than the height is not in V_n.

3.1 The case where $p = 3$

In the case where $p = 3$ we can always explicitly compute V_{3qr} on invoking Theorem 3, Theorem 4 and Lemma 3. We obtain the following result.

Theorem 5 *Let $3 < q < r$ be odd primes.*
If $q \equiv 1 (\mathrm{mod}\ 3)$, $r \equiv 1 (\mathrm{mod}\ 3)$ and $r \le 2q-7$, then $V_{3qr} = \{-2, -1, 0, 1, 2\}$. In particular, $c_{3qr}(r+1) = 2$ and $c_{3qr}(r+1+qr) = -2$.
If $q \equiv 2 (\mathrm{mod}\ 3)$, $r \equiv 2 (\mathrm{mod}\ 3)$ and $r \le 2q-3$, then $V_{3qr} = \{-2, -1, 0, 1, 2\}$. In particular, $c_{3qr}(r) = -2$ and $c_{3qr}(r+qr) = 2$.
In the remaining cases $V_{3qr} = \{-1, 0, 1\}$ and then $\Psi_{3qr}(x)$ is flat.

`Remark`. The quoted results only give $r \le 2q-3$. Note, however, that if $q \equiv r \equiv 1 (\mathrm{mod}\ 3)$ and $r \le 2q-3$, then $r \le 2q-7$.

We now infer some consequences of Theorem 5. For this we need the following generalisation of Bertrand's Postulate.

Lemma 8 *If q is any prime, then the interval $(q, 2q-7]$ contains primes p_1 and p_2 with $p_i \equiv i (\mathrm{mod}\ 3)$.*

Proof. Molsen [13], cf. Moree [14], has shown that for $x \ge 199$ the interval $(x, \frac{8}{7}x]$ contains primes p_1 and p_2 with $p_i \equiv i (\mathrm{mod}\ 3)$. From this the result follows after some easy computations. □

Theorem 6
1) *Let r be any prime, then $\Psi_{15r}(x)$ and $\Psi_{21r}(x)$ are flat.*
2) *Let $q \ge 11$ be a prime. Then Ψ_{3qr} is flat for all primes $r \ge 2q-1$. However, there is at least one prime r such that $\Psi_{3qr}(x)$ is non-flat.*
3) *Let $3 < q < r$ be primes. For $k \le 16$ we have $|c_{3qr}(k)| \le 1$.*

Proof. 1) An immediate consequence of Theorem 5 and Lemma 4.
2) A consequence of Theorem 5 and Lemma 8.
3) By part 1 and Theorem 5 we infer that the smallest r for which $V_{3qr} \neq \{-1, 0, 1\}$ is $r = 17$. By Lemma 6 the proof is then completed. $\square$

3.2 Reciprocal polynomials of intermediary height

A variation of the methods used to establish Theorem 2 yields the following upper bound for $h(\Psi_{pqr}(x))$. Sometimes this bound is actually optimal, for example for the Chernick Carmichael numbers (see Lemma 13).

Theorem 7 *Let ρ and σ be the unique non-negative integers such that one has $(p-1)(q-1) = \rho p + \sigma q$. Put $\tau = (p-1)(q+r-1)$. If $qr > \tau$, then the height of $\Psi_{pqr}(x)$ is at most $\max\{\min(\rho+1, \sigma+1), \min(q-1-\rho, p-1-\sigma)\}$.*

Corollary 2 *If either $q \equiv -2 (\bmod\ p)$ or $q \equiv 2 (\bmod\ p)$ and $q > p+2$, then the height of $\Psi_{pqr}(x)$ is at most $(p+1)/2$.*

Proof. One easily checks that $qr > \tau$. We compute that

$$\sigma = \begin{cases} \frac{p-3}{2} & \text{if } q \equiv -2 (\bmod\ p); \\ \frac{p-1}{2} & \text{if } q \equiv 2 (\bmod\ p). \end{cases}$$

Proof of Theorem 7. We have to show that $|c_{pqr}(k)|$ does not exceed the bound stated. The conditions of Lemma 7 are satisfied and by property (6) we may take $k \leq \tau/2 < (p-1)r$. Now choose $0 \leq m \leq p-2$ such that $mr \leq k < (m+1)r$. By Lemma 7 we have

$$c_{pqr}(k) = -\sum_{v=0}^{m} a_{pq}(k - vr).$$

Let us consider the worst case where $m = p-2$ and a priori $|c_{pqr}(k)| \leq p-1$. We determine the maximum number of v with $0 \leq v \leq p-2$ for which $a_{pq}(k-vr) = 1$. Let us suppose that for $v_1, \ldots, v_t$ we have $a_{pq}(k - v_j r) = 1$ and hence, by Lemma 5, we have

$$\begin{cases} k - v_1 r = i_1 p + j_1 q; \\ k - v_2 r = i_2 p + j_2 q; \\ \ldots \\ k - v_t r = i_t p + j_t q, \end{cases}$$

where each j_m satisfies $0 \leq j_m \leq \sigma$. Now if $t > \sigma + 1$ two of the j_m must be equal. On subtracting the corresponding equations it would follow that $p|r$, a contradiction that shows that $t \leq \sigma + 1$. On using that $q \nmid r$, we likewise infer that $t \leq \rho + 1$. We infer that $c_{pqr}(k) \geq -\min(\rho+1, \sigma+1)$. Note that the same inequality actually holds for all $k < (p-1)r$.

We determine the maximum number of w with $0 \leq w \leq p-2$ for which $a_{pq}(k - wr) = -1$. Let us suppose that for $w_1, \ldots, w_t$ we have $a_{pq}(k - w_j r) = 1$ and hence, by Lemma 5, we have

$$\begin{cases} k - w_1 r = 1 + i_1 p + j_1 q; \\ k - w_2 r = 1 + i_2 p + j_2 q; \\ \ldots \\ k - w_t r = 1 + i_t p + j_t q, \end{cases}$$

where each j_m satisfies $0 \le j_m \le p-2-\sigma$. Now if $t > p-1-\sigma$ two of the j_m must be equal. On subtracting the corresponding equations it would follow that $p|r$, a contradiction that shows that $t \le p-1-\sigma$. Likewise we infer that $t \le q-1-\rho$. We infer that $c_{pqr}(k) \le \min(q-1-\rho, p-1-\sigma)$. On combining this with $c_{pqr}(k) \ge -\min(\rho+1, \sigma+1)$ we are done. $\square$

4 Further flatness results

In this section we present some further (near) flatness results.

Lemma 9 *If $r > (p-1)(q-1)$, then $\Psi_{pqr}(x)$ is flat.*

Proof. Note that if f and g are flat polynomials and $m > \deg(f)$, then $f(x)g(x^m)$ is flat. By (5) we have $\Psi_{pqr}(x) = \Phi_{pq}(x)\Psi_{pq}(x^r)$. The assumption on r implies that $r > \deg(\Phi_{pq}(x)) = (p-1)(q-1)$. Since both $\Phi_{pq}(x)$ and $\Psi_{pq}(x)$ are flat, the result now follows. $\square$

A variation of the latter proof making use of the identity $\Psi_{pn}(x) = \Psi_n(x^p)\Phi_n(x)$ if $p \nmid n$ (this is part 3 of Lemma 2), yields the following lemma.

Lemma 10 *Let p be a prime. Let h_1, h_2 be the height of $\Phi_n(x)$, respectively $\Psi_n(x)$. If $p > \varphi(n)$, then $\Psi_{np}(x)$ is of height h_1h_2.*

Using this result we easily infer the following one.

Lemma 11 *Let $3 < q < r < s$ be primes such that $s > 2(q-1)(r-1)$. Then*
1) $\Psi_{3qrs}(x)$ is of height at most 4.
2) If $r \equiv q \pmod 3$ and $r \equiv \pm 1 \pmod{3q}$, then $\Psi_{3qrs}(x)$ is flat.

Proof. 1) Beiter [5] has shown that $\Phi_{3qr}(x)$ is of height at most 2. By Theorem 5 we know that also $\Psi_{3qr}(x)$ is of height at most 2. Now apply the previous lemma with $n = 3qr$ and $p = s$.
2) Follows from the previous lemma, Theorem 5 and the result due to Kaplan [8, Theorem 1] (who extended on earlier work by Bachman [3]) that $\Phi_{3qr}(x)$ is flat if $r \equiv \pm 1 \pmod{3q}$. $\square$

`Remark`. Since $h(\Psi_{3\cdot 11\cdot 17\cdot 331}(x)) = 4$, we see that the 4 above cannot be replaced by a smaller number.

Recall that smallest n for which $\Phi_n(x)$ is non-flat is $n = 105$.

Lemma 12 *The smallest n for which $\Psi_n(x)$ is non-flat is $n = 561$.*

Proof. By computation one finds that $c_{561}(17) = -2$. By Lemma 4 it suffices to check that $\Psi_n(x)$ is flat for every odd squarefree $n \le 560$ with $\omega_1(n) \ge 3$. This leaves us with the sets

$$\mathcal{A} = \{105, 165, 195, 231, 255, 273, 285, 345, 357, 399, 435, 465, 483, 555\},$$

and $\mathcal{B} = \{385, 429, 455\}$, where the set $\mathcal{A}$ has all its elements divisible by 15 or 21. On applying part 1 of Theorem 6 we infer that $\Psi_n(x)$ is flat for every $n \in \mathcal{A}$.

By direct computation we find that $\Psi_{385}(x), \Psi_{429}(x)$ and $\Psi_{455}(x)$ are flat. $\square$

Since 561 is the smallest Carmichael number and the smallest number m for which $h(\Psi_m(x)) > 1$, one might wonder whether perhaps $h(\Psi_C(x)) > 1$ for every Carmichael number C. The answer is no, as the example $c = 2821$ shows. However, for the Chernick Carmichael numbers the answer turns out to be yes. In 1939 Chernick proved that if $k \geq 0$ is such that $6k+1$, $12k+1$ and $18k+1$ are all primes, then $C = (6k+1)(12k+1)(18k+1)$ is a Carmichael number. Examples occur for $k = 1, 6, 35, 45, 51, 56, \ldots$.

Lemma 13 *If $C = (6k+1)(12k+1)(18k+1)$ is a Chernick Carmichael number, then $c_C(24k+2) = -2$ and $h(\Psi_C(x)) = 2$.*

Proof. Put $p = 6k+1$, $q = 12k+1$ and $r = 18k+1$. We find $\rho = 1$ and $\sigma = p-2$. By Theorem 7 we infer that $h(\Psi_C(x)) \leq 2$. By Lemma 5 we have $a_C(2q) = 1$ and $a_C(p) = 1$. Now $c_C(2q) = -a_C(2q) - a_C(2q-r) = -a_C(2q) - a_C(p) = -2$. Thus $c_C(2q) = c_C(24k+2) = -2$ and $h(\Psi_C(x)) = 2$. $\square$

5 Sizable coefficients

The history of sizable coefficients goes back to Schur who in a letter in 1931 to Landau (see e.g. E. Lehmer [11]) proved that the $a_n(k)$ are unbounded. It is not difficult, see Suzuki [16], to adapt his argument so as to show that *every* integer shows up as a coefficient, that is $\{a_n(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$. Bungers [6], in his Ph.D. thesis proved that under the assumption that there are infinitely many twin primes, the $a_n(k)$ are also unbounded if n has at most three prime factors. E. Lehmer [11] eliminated the unproved assumption of the existence of infinitely twin primes from this. The strongest result in this direction to date is due to Bachman, who proved a result ([2, Theorem 1]), which implies that

$$\{a_{pqr}(k) : 3 \leq p < q < r \text{ primes}\} = \mathbb{Z}.$$

A minor variation of Suzuki's argument gives $\{c_n(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$. Since the next result is stronger, the details are left to the interested reader.

Theorem 8 *We have $\{c_{pqr}(k) : 3 \leq p < q < r \text{ primes}\} = \mathbb{Z}$.*

Proof. By Dirichlet's theorem on arithmetic progressions for every prime p there is a $q_0(p)$ such that for every $q > q_0(p)$ with $q \equiv \pm 1 (\mathrm{mod}\ p)$, there exists $r \equiv q (\mathrm{mod}\ p)$ with $q < r < (p-1)(q-1)/(p-2)$. The proof is then completed on invoking Theorem 4. $\square$

In the table below (part of a much large table computed by Yves Gallot) the minimal n, n_0, such that $c_{n_0}(k) = m$ for some k is given. The third column gives the degree of $\Psi_{n_0}(x)$. The fourth column gives the smallest k, k_0, for which $|c_{n_0}(k_0)| = m$.

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

m	n_0	$\deg(\Psi_{n_0})$	k_0	$c_{n_0}(k_0)$
1	1	0	0	$+1$
2	$561 = 3 \cdot 11 \cdot 17$	241	17	-2
3	$1155 = 3 \cdot 5 \cdot 7 \cdot 11$	675	33	-3
4	$2145 = 3 \cdot 5 \cdot 11 \cdot 13$	1185	44	$+4$
5	$3795 = 3 \cdot 5 \cdot 11 \cdot 23$	2035	132	-5
6	$5005 = 5 \cdot 7 \cdot 11 \cdot 13$	2125	201	-6
7	$5005 = 5 \cdot 7 \cdot 11 \cdot 13$	2125	310	-7
8	$8645 = 5 \cdot 7 \cdot 13 \cdot 19$	3461	227	-8
9	$8645 = 5 \cdot 7 \cdot 13 \cdot 19$	3461	240	$+9$
10	$11305 = 5 \cdot 7 \cdot 17 \cdot 19$	4393	240	-10
11	$11305 = 5 \cdot 7 \cdot 17 \cdot 19$	4393	306	$+11$

For $m = 10, \ldots, 21$ it turns out that $n_0 = 11305$.

Acknowledgement. As in many papers before this one, impressive computational assistance was provided by Yves Gallot. I am deeply grateful for all the work he did for me. Paul Tegelaar proofread an earlier version and Gennady Bachman updated me on recent results on the flatness of $\Phi_{3qr}(x)$.

In the context of assigning student projects to Alexander Bridi, Andreas Decker, Patrizia Dressler, Silke Glas and Thorge Jensen (and earlier Christine Jost and Janina Müttel), I considered cyclotomic polynomials. I thank them all for their enthusiasm and cheerful presence which added to the already pleasant atmosphere at the Max-Planck-Institut für Mathematik.

My belief that 561 is a boring number was expelled by Don Zagier who remarked that, on the contrary, it is interesting since it is the smallest Carmichael number. I thank him for this and several other helpful remarks.

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, *J. Number Theory* **100** (2003), 104–116.

[2] G. Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, *Proc. Amer. Math. Soc.* **132** (2004), 1943–1950 (electronic).

[3] G. Bachman, Flat cyclotomic polynomials of order three, *Bull. London Math. Soc.* **38** (2006), 53–60.

[4] A.S. Bang, Om Ligningen $\varphi_n(x) = 0$, *Nyt Tidsskrift for Mathematik (B)* **6** (1895), 6–12.

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

[6] R. Bungers, Über die Koeffizienten von Kreisteilungspolynomen, Dissertation, Göttingen, 1934, pp. 14.

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

[8] N. Kaplan, Flat cyclotomic polynomials of order three, *J. Number Theory*, to appear (available already electronically).

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

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

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

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

[13] K. Molsen, Zur Verallgemeinerung des Bertrandschen Postulates, *Deutsche Math.* **6** (1941), 248–256.

[14] P. Moree, Bertrand's Postulate for primes in arithmetical progressions, *Comput. Math. Appl.* **26** (1993), 35–43.

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

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

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

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