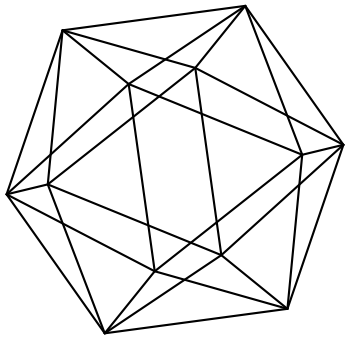
Max-Planck-Institut für Mathematik
Bonn

Cyclotomic polynomials at roots of unity

by

Bartłomiej Bzdęga
Andrés Herrera-Poyatos
Pieter Moree



Max-Planck-Institut für Mathematik
Preprint Series 2016 (45)

Cyclotomic polynomials at roots of unity

Bartłomiej Bzdęga
Andrés Herrera-Poyatos
Pieter Moree

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

Faculty of Mathematics and Computer Science
Adam Mickiewicz University
Umultowska 87
61-614 Poznan
Poland

Faculty of Science
University of Granada
Avenida de la Fuente Nueva
18071 Granada
Spain

MPIM 16-45

CYCLOTOMIC POLYNOMIALS AT ROOTS OF UNITY

BARTŁOMIEJ BZDĘGA, ANDRÉS HERRERA-POYATOS AND PIETER MOREE

ABSTRACT. The n^{th} cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial of an n^{th} primitive root of unity. Hence $\Phi_n(x)$ is trivially zero at primitive n^{th} roots of unity. Using finite Fourier analysis we derive a formula for $\Phi_n(x)$ at the other roots of unity. This allows one to explicitly evaluate $\Phi_n(e^{2\pi i/m})$ with $m \in \{3,4,5,6,8,10,12\}$. We use this evaluation with $m=5$ to give a simple reproof of a result of Vaughan (1975) on the maximum coefficient (in absolute value) of $\Phi_n(x)$. We also obtain a formula for $\Phi_n'(e^{2\pi i/m})/\Phi_n(e^{2\pi i/m})$ with $n \neq m$, which is effectively applied to $m \in \{3,4,6\}$. Furthermore, we compute the resultant of two cyclotomic polynomials in a novel very short way.

1. INTRODUCTION

The study of cyclotomic polynomials Φ_n has a long and venerable history[1]. In this paper we mainly focus on two aspects: values at roots of unity and heights. These two aspects are related. In order to explain the connection we have to recall the notion of height. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$ be a polynomial of degree $d = \deg f$. Then its height $H(f)$ is defined as $H(f) = \max_{0\le j\le d} |a_j|$. Now if z is on the unit circle, then for $n > 1$ we obviously have

$$A_n := H(\Phi_n) \geq \frac{\sum_{0\le j\le d} |a_n(j)|}{d+1} \geq \frac{|\Phi_n(z)|}{\varphi(n)+1} \geq \frac{|\Phi_n(z)|}{n}, \tag{1}$$

where $\Phi_n(x) = \sum_{j=0}^{d} a_n(j)x^j$ and $d = \deg \Phi_n = \varphi(n)$, with φ Euler's totient function. This inequality shows that if we can pinpoint any z on the unit circle for which $|\Phi_n(z)|$ is large, then we can obtain a non-trivial lower bound for A_n (cf. Bzdęga [3]).

In this paper we show that there is an infinite sequence of integers n such that $|\Phi_n(z_n)|$ is large, with z_n an appropriately chosen primitive fifth root of unity. It is easy to deduce (see the proof of Theorem 33) that for this sequence $\log\log A_n \geq (\log 2 + o(1))\log n/\log\log n$ as n tends to infinity, which reproves a result of Vaughan [17]. The infinite sequence is found using Theorem 1, our main result.

We evaluate $\Phi_n(e^{2\pi i/m})$ for $m \in \{1,2,3,4,5,6\}$ and every $n \geq 1$ in, respectively, Lemmas 4, 7, 23, 24, 28 and 25. For $m \in \{1,2\}$ these results are folklore and we recapitulate them for the convenience of the reader. For $m \in \{3,4,6\}$ the results were obtained by Motose [14], but they need some small corrections (for details see the beginning of Section 5). We reprove these results using a different method which has the advantage of reducing the number of cases being considered. Using a computer algebra package we verified our results for $n \leq 5000$. We note that the field $\mathbb{Q}(e^{2\pi i/m})$ is of degree at most 2 if and only if $m \in \{1,2,3,4,6\}$.

Our main result expresses $\Phi_n(\xi_m)$, with ξ_m an arbitrary primitive m^{th} root of unity, in

Date: August 2016.

Mathematics Subject Classification (2000). 11N37, 11Y60

[1]Even involving poems, e.g. I. Schur's proof of the irreducibility of $\Phi_n(x)$ set to rhyme [5, pp. 38-41].

terms of the set of Dirichlet characters modulo m. This result allows one to explicitly evaluate $\Phi_n(\xi_m)$ also for $m \in \{5, 8, 10, 12\}$ (values of m not covered in the literature so far).

Theorem 1. *Let $n, m > 1$ be coprime integers. By $G(m)$ we denote the multiplicative group modulo m and by $\widehat{G}(m) = Hom((\mathbb{Z}/m\mathbb{Z})^*, \mathbb{C}^*)$ the set of Dirichlet characters modulo m. For all $\chi \in \widehat{G}(m)$ let*

$$C_\chi(\xi_m) = \sum_{g \in G(m)} \overline{\chi}(g) \log(1 - \xi_m^g),$$

where we take the logarithm with imaginary part in $(-\pi, \pi]$. Then

$$\Phi_n(\xi_m) = \exp\left(\frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} C_\chi(\xi_m)\chi(n) \prod_{p|n} (1 - \overline{\chi}(p)) \right).$$

The theorem is especially easy to use if $\widehat{G}(m)$ only consists of the trivial and quadratic characters. This occurs precisely if $(\mathbb{Z}/m\mathbb{Z})^*$ is a direct product of cyclic groups of order two. It is elementary to classify those m and one finds that $m \in \{1, 2, 3, 4, 6, 8, 12, 24\}$.

A variant of Theorem 1 for $\Phi_n'(\xi_m)/\Phi_n(\xi_m)$ is also obtained (Theorem 31). It is used to evaluate $\Phi_n'(\xi_m)/\Phi_n(\xi_m)$ for $m \in \{3, 4, 6\}$.

Kronecker polynomials are monic products of cyclotomic polynomials and a monomial. For them some of our results can be applied (see Section 8).

A question related to computing $\Phi_n(\xi_m)$ is that of determining its degree as an algebraic integer. This was considered in extenso by Kurshan and Odlyzko [9]. Their work uses Gauss and Ramanujan sums, the non-vanishing of Dirichlet L-series at 1, and the construction of Dirichlet characters with special properties.

2. Preliminaries

We recall some relevant material on cyclotomic fields as several of our results can be reformulated in terms of cyclotomic fields. Most books on algebraic number theory contain a chapter on cyclotomic fields, for the advanced theory see, e.g., Lang [10]. Furthermore we consider elementary properties of self-reciprocal polynomials and the (generalized) Jordan totient function.

The results in Section 2.6 and Lemma 14 in Section 2.7 are our own, but given their elementary nature they have been quite likely observed before. The proof of Theorem 9 is new.

2.1. **Important notation.** We write double exponents not as a^{b^c}, but as $(a)\hat{}b^c$ in those cases where we think it enhances the readability.

Throughout we use the letters p and q to denote primes. For a natural number n we will refer to the exponent of p in the prime factorization of n by $\nu_p(n)$, i.e., $p^{\nu_p(n)} \parallel n$.

A primitive n^{th} root of unity is a complex number z satisfying $z^n = 1$, but not $z^d = 1$ for any $d < n$. We let ξ_n denote any primitive n^{th} root of unity. It is of the form ζ_n^j with $1 \le j \le n$, $(j, n) = 1$ and $\zeta_n = e^{2\pi i/n}$.

2.2. **Cyclotomic polynomials.** In this section we recall some material on cyclotomic polynomials we will need later in the paper. For proofs see, e.g., Thangadurai [16].

A definition of the n^{th} cyclotomic polynomial is

$$\Phi_n(x) = \prod_{1 \le j \le n,\ (j,n)=1} (x - \zeta_n^j) \in \mathbb{C}[x]. \tag{2}$$

It is monic of degree $\varphi(n)$, has integer coefficients and is irreducible over $\mathbb{Q}$. In $\mathbb{Q}[x]$ we have the factorization into irreducibles

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

By Möbius inversion we obtain from this that

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

with μ the Möbius function.

Lemma 2 and Corollary 3 summarize some further properties of $\Phi_n(x)$.

Lemma 2. *We have*
a) $\Phi_{pn}(x) = \Phi_n(x^p)$ *if* $p \mid n$;
b) $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ *if* $p \nmid n$;
c) $\Phi_n(x) = x^{\varphi(n)}\Phi_n(1/x)$ *for* $n > 1$.

Corollary 3. *We have*

$$\Phi_n(-x) = \begin{cases} (-1)^{\varphi(n)}\Phi_{2n}(x) & \text{if } 2 \nmid n; \\ (-1)^{\varphi(n)}\Phi_{n/2}(x) & \text{if } 2 \parallel n; \\ \Phi_n(x) & \text{if } 4 \mid n. \end{cases}$$

2.3. **Calculation of $\Phi_n(\pm 1)$.** The evaluation of $\Phi_n(1)$ is a classical result. For completeness we formulate the result and give two proofs of it, the first taken from Lang [11, p. 74].

Lemma 4. *We have*

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^e; \\ 1 & \text{otherwise,} \end{cases}$$

with p a prime number and $e \geq 1$.

Proof. By (3) we have

$$\frac{x^n - 1}{x - 1} = \prod_{d|n,\ d>1} \Phi_d(x). \tag{5}$$

Thus

$$n = \prod_{d|n,\ d>1} \Phi_d(1). \tag{6}$$

We see that $p = \Phi_p(1)$. Furthermore, $p^f = \Phi_p(1)\Phi_{p^2}(1)\cdots\Phi_{p^f}(1)$. Hence, by induction $\Phi_{p^f}(1) = p$. We infer that $\prod_{d\in\mathcal{Q},\ d|n} \Phi_d(1) = n$, where $\mathcal{Q}$ is the set of all prime powers > 1. Thus for the composite divisors d of n, we have $\Phi_d(1) = \pm 1$. Assume inductively that for $d \mid n$ and $d < n$ we have $\Phi_d(1) = 1$. Then we see from our product that $\Phi_n(1) = 1$ too. □

The reader might recognize the von Mangoldt function Λ in Lemma 4. Recall that the von Mangoldt function Λ is defined as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^e,\ e \geq 1; \\ 0 & \text{otherwise.} \end{cases}$$

In terms of the von Mangoldt function we can reformulate Lemma 4 in the following way.

Lemma 5. *We have $\Phi_1(1) = 0$. For $n > 1$ we have $\Phi_n(1) = e^{\Lambda(n)}$.*

We will give a reproof of this lemma in which the von Mangoldt function arises naturally.

Proof of Lemma 5. By Möbius inversion the identity (6) for all $n > 1$ determines $\Phi_m(1)$ uniquely for all $m > 1$. This means that it is enough to verify that $\log n = \sum_{d|n,\ d>1} \Lambda(d)$ for all $n > 1$. Since $\Lambda(1) = 0$ it is enough to verify that $\log n = \sum_{d|n} \Lambda(d)$ for all $n > 1$. This is a well known identity in elementary prime number theory. □

The Prime Number Theorem in the equivalent form $\sum_{n\le x} \Lambda(n) \sim x$ yields in combination with Lemma 5 the following proposition.

Proposition 6. *The Prime Number Theorem is equivalent with the statement that*

$$\sum_{2<n\le x} \log(\Phi_n(1)) \sim x,\ x \to \infty.$$

In a similar vein, Amoroso [1] considered a variant h of the Mahler measure and established that the estimate $h(\prod_{n\le x} \Phi_n) \ll x^{1/2+\epsilon}$ for every $\epsilon > 0$ is equivalent with the Riemann Hypothesis.

2.4. **Calculation of $\Phi_n(-1)$.** Once one has calculated $\Phi_n(1)$, the evaluation of $\Phi_n(-1)$ follows on invoking Corollary 3.

Lemma 7. *We have*

$$\Phi_n(-1) = \begin{cases} -2 & \text{if } n = 1; \\ 0 & \text{if } n = 2; \\ p & \text{if } n = 2p^e; \\ 1 & \text{otherwise.} \end{cases}$$

with p a prime number and $e \ge 1$.

Remark 8. It is also possible to prove this lemma along the lines of the proof of Lemma 4, see Motose [14].

2.5. **Cyclotomic fields.** Several of the results in this paper can be rephrased in terms of cyclotomic fields. A field is said to be cyclotomic if it is of the form $\mathbb{Q}[x]/(\Phi_m(x))$ for some $m \ge 1$. It is isomorphic to $\mathbb{Q}(\zeta_m)$ which is the one obtained by adjoining ζ_m to $\mathbb{Q}$. It satisfies $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \deg \Phi_m = \varphi(m)$ and has $\mathbb{Z}[\zeta_m]$ as its ring of integers.

A field automorphism σ of $\mathbb{Q}(\zeta_m)$ is completely determined by the image of ζ_m. This has to be root of unity of order m and hence $\sigma(\zeta_m) = \zeta_m^j$ with $1 \le j \le m$ and $(j, m) = 1$. It follows that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ and that the norm of an algebraic number α in $\mathbb{Q}(\zeta_m)$ satisfies

$$N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = \prod_{1\le j\le m,(j,m)=1} \sigma_j(\alpha), \tag{7}$$

where σ_j denotes the automorphism that sends ζ_m to ζ_m^j. It also follows that $\Phi_m(x)$, the minimal polynomial of ζ_m, satisfies (2).

Let $(j, m) = 1$. We have $\Phi_n(\zeta_m^j) = \Phi_n(\sigma_j(\zeta_m)) = \sigma_j(\Phi_n(\zeta_m))$ and so in order to compute $\Phi_n(\zeta_m^j)$ it is enough to compute $\Phi_n(\zeta_m)$. In particular if and only if one of the values $\Phi_n(\zeta_m^j)$ is rational, then all of them are equal.

Let k be an integer. On combining (7) and (2) we infer that

$$N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(k - \zeta_m) = \Phi_m(k). \tag{8}$$

The resultant of two monic polynomials f and g having roots $\alpha_1, \ldots, \alpha_k$, respectively $\beta_1, \ldots, \beta_l$ is given by

$$\rho(f,g) = \prod_{i=1}^{k}\prod_{j=1}^{l}(\alpha_i - \beta_j) = \prod_{i=1}^{k} g(\alpha_i).$$

In particular it follows from (2) that

$$\rho(\Phi_m, \Phi_n) = \prod_{1\le j\le m,\ (j,m)=1} \Phi_n(\zeta_m^j). \tag{9}$$

E. Lehmer (1930) [12], Diederichsen (1940) [7], Apostol (1970) and Louboutin (1997) [13] all computed the resultant of cyclotomic polynomials (see also Sivaramakrishnan [15, Chapter X]). More recently Dresden (2012) [8] gave yet another proof. Here we present a very short new proof.

Theorem 9. *If $n > m > 1$, then*

$$\rho(\Phi_n, \Phi_m) = \begin{cases} p^{\varphi(m)} & \text{if } n/m = p^k \text{ for some prime } p \text{ and } k \ge 1; \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Assume that $n > m > 1$. Then there exist a prime p such that $\nu_p(n) > \nu_p(m)$. Put $n = Np^e$ and $m = Mp^f$ with $p \nmid M, N$. Obviously $e > f \ge 0$.

Note that by the Chinese Remainder Theorem every primitive residue j modulo m can be uniquely written as

$$j \equiv ap^f + bM \pmod m,$$

where a and b are primitive residues respectively modulo M and p^f. We will use this fact. In order to make the notation shorter we will write $\prod_j$, $\prod_a$ and $\prod_b$ for the product over primitive residues respectively modulo m, M and p^f.

First we consider the case $M \ne N$. We have

$$\begin{aligned}\rho(\Phi_n, \Phi_m) &= \prod_j \Phi_n(\zeta_m^j) = \prod_j \frac{\Phi_N(\zeta_{Mp^f}^{jp^e})}{\Phi_N(\zeta_{Mp^f}^{jp^{e-1}})} = \prod_j \frac{\Phi_N(\zeta_M^{jp^{e-f}})}{\Phi_N(\zeta_M^{jp^{e-f-1}})} \\ &= \prod_a \prod_b \frac{\Phi_N(\zeta_M^{ap^e + bMp^{e-f}})}{\Phi_N(\zeta_M^{ap^{e-1} + bMp^{e-f-1}})} = \left(\prod_a \frac{\Phi_N(\zeta_M^{ap^e})}{\Phi_N(\zeta_M^{ap^{e-1}})}\right)^{\varphi(p^f)} = 1.\end{aligned}$$

For $M = N$ we need to replace the quotients by their limits. Using the L'Hôpital rule and the substitution $j \equiv ap^f + bM$, we obtain

$$\Phi_n(\zeta_m^j) = \lim_{z\to\zeta_m^j} \frac{\Phi_N(z^{p^e})}{\Phi_N(z^{p^{e-1}})} = p\zeta_M^{\varphi(p^e)} \frac{\Phi'_N(\zeta_M^{ap^e})}{\Phi'_N(\zeta_M^{ap^{e-1}})}.$$

After taking the product over all primitive a modulo m, the derivatives cancel out. So for $M = N$ we have

$$\rho(\Phi_n, \Phi_m) = \prod_a \prod_b (p\zeta_M^{a\varphi(p^e)}) = p^{\varphi(m)} \zeta_M^{\varphi(p^e)\varphi(p^f)\sum_a a} = p^{\varphi(m)},$$

where we used that $M \mid \sum_a a$ for $M > 2$. If $M = 2$ then $\zeta_M = -1$, $p > 2$ and $\varphi(p^e)$ is even. □

Corollary 10. *Let $n > m > 1$. The algebraic integer $\Phi_n(\zeta_m)$ is not a unit in $\mathbb{Z}[\zeta_m]$ if and only if n/m is a prime power.*

2.6. **Self-reciprocal polynomials.** A polynomial f of degree d is said to be self-reciprocal if $f(x) = x^d f(1/x)$. If $f(x) = -x^d f(1/x)$, then f is said to be anti-self-reciprocal. Lemma 2c says that Φ_n is self-reciprocal for $n \geq 2$. Note that Φ_1 is anti-self-reciprocal.

Lemma 11. *Let $f \in \mathbb{R}[x]$ be a self-reciprocal polynomial. Then for $|z| = 1$ we have*

$$f(z) = \pm |f(z)| z^{\frac{\deg f}{2}}.$$

If $f \in \mathbb{R}[x]$ is an anti-self-reciprocal polynomial, then for $|z| = 1$ we have

$$f(z) = \pm i |f(z)| z^{\frac{\deg f}{2}}.$$

Proof. Let $d = \deg f$. If f is self-reciprocal and $|z| = 1$ we have $f(z) = z^d f(1/z) = z^d \overline{f(z)}$. Multiplying both sides by $f(z)$ and taking the square root we obtain the first claim.

If f is anti-self-reciprocal and $|z| = 1$ we have $f(z) = -z^d f(1/z) = -z^d \overline{f(z)}$ and the proof is analogous. □

The behaviour of a self-reciprocal f and its first derivative at ± 1 is easily determined.

Proposition 12. *Let f be a polynomial of degree $d \geq 1$.*
Suppose that f is self-reciprocal.
a) *We have $f'(1) = f(1)d/2$;*
b) *If $2 \nmid d$, then $f(-1) = 0$. If $2 \mid d$, then $f'(-1) = -f(-1)d/2$.*
Suppose that f is anti-self-reciprocal.
a) *We have $f(1) = 0$;*
b) *If $2 \mid d$, then $f(-1) = 0$. If $2 \nmid d$, then $f'(-1) = -f(-1)d/2$.*

Proof. If f is self-reciprocal, then $f(z) = z^d f(1/z)$. If f is anti-self-reciprocal we have $f(z) = -z^d f(1/z)$. Differentiating both sides and substituting $z = \pm 1$ gives the result. □

The next result concerns the behaviour of self-reciprocal polynomials in roots of unity other than ± 1.

Lemma 13. *Let $f \in \mathbb{Z}[x]$ be a self-reciprocal polynomial of even degree d and $m \in \{3, 4, 6\}$. Then $\xi_m^{-d/2} f(\xi_m)$ is an integer.*

Proof. For any m with $\varphi(m) = 2$ the field $\mathbb{Q}(\xi_m)$ is quadratic. Hence we can write $\xi_m^{-d/2} f(\xi_m) = a + b\xi_m$ with a and b integers. Since by assumption f is self-reciprocal we have $a + b\xi_m^{-1} = \xi_m^{d/2} f(\xi_m^{-1}) = \xi_m^{-d/2} f(\xi_m) = a + b\xi_m$. Hence $b = 0$ and the result follows. □

2.7. **The (generalized) Jordan totient function.** Let $k \geq 1$ be an integer. The k^{th} Jordan totient function is defined by

$$J_k(n) = \sum_{d \mid n} \mu(\frac{n}{d}) d^k.$$

As J_k is a Dirichlet convolution of multiplicative functions, it is itself multiplicative. One has

$$J_k(n) = n^k \prod_{p \mid n} (1 - \frac{1}{p^k}).$$

Given a character χ and an integer $k \geq 0$ we define

$$J_k(\chi; n) = \sum_{d \mid n} \mu(\frac{n}{d}) d^k \chi(d). \tag{10}$$

Since $J_k(\chi;\cdot)$ is a Dirichlet convolution of multiplicative functions, it is a multiplicative function itself. The next lemma demonstrates that it is an analogue of the Jordan totient function. Recall that $\mathrm{rad}(n)=\prod_{p\,|n}p$ is the radical, sometimes also called the squarefree kernel, of n.

Lemma 14. *Let χ be a character modulo m and $k\geq 0$ an integer. We have*

$$J_k(\chi;n)=\prod_{p^e\|n}p^{k(e-1)}\chi(p^{e-1})(p^k\chi(p)-1)=\left(\frac{n}{\mathrm{rad}(n)}\right)^k\chi\left(\frac{n}{\mathrm{rad}(n)}\right)\prod_{p\,|n}(p^k\chi(p)-1).$$

If n is squarefree, then $J_k(\chi;n)=\prod_{p\,|n}(p^k\chi(p)-1)$. If $(m,n)=1$, then

$$J_k(\chi;n)=\chi(n)n^k\prod_{p\,|n}\left(1-\frac{\overline{\chi}(p)}{p^k}\right).$$

Proof. The proof follows by the usual arguments from the elementary theory of arithmetic functions. □

3. Cyclotomic values in arbitrary roots of unity

Let us consider two positive integers n,m with $n>1$ and $m\geq 1$. In this section we present general facts about the value $\Phi_n(\xi_m)$. Clearly $\Phi_n(\xi_m)=0$ if and only if $n=m$. Hence we study the case $n\neq m$.

The next result is due to Kurshan and Odlyzko [9, Corollary 2.3]. We give a simpler reproof of it (suggested to us by Peter Stevenhagen).

Lemma 15. *Let $n\geq 2$. The cyclotomic value $\Phi_n(\xi_m)$ is non-zero and real if and only if $m\mid\varphi(n)$.*

Proof. The number $\Phi_n(\xi_m)$ is real if and only if $\Phi_n(\xi_m)=\overline{\Phi_n(\xi_m)}=\Phi_n(\xi_m^{-1})$. By the self-reciprocity of Φ_n we see that this is equivalent with $\Phi_n(\xi_m)=\xi_m^{-\varphi(n)}\Phi_n(\xi_m)$, which is equivalent with $n=m$ or $m|\varphi(n)$. On noting that $n\nmid\varphi(n)$ and $\Phi_n(\xi_m)=0$ if and only if $n=m$, the proof is completed. □

Lemma 11 shows that for $n\geq 2$ we have $\Phi_n(\xi_m)=\pm|\Phi_n(\xi_m)|\xi_m^{\varphi(n)/2}$. The next result shows that the sign is given by $(-1)^{\varphi(n/m;n)}$, where $\varphi(x;n)$ is the number of positive integers $j\leq x$ with $(j,n)=1$.

Lemma 16. *Write $\xi_m=\zeta_m^j$. For $n\geq 2$ we have $\Phi_n(\xi_m)=(-1)^{\varphi(nj/m;n)}|\Phi_n(\xi_m)|\xi_m^{\varphi(n)/2}$.*

Proof. Let us consider the function $g(t)=e^{-it\varphi(n)/2}\Phi_n(e^{it})$ with $t\in[0,2\pi)$. The self reciprocity of Φ_n ensures that $g(t)$ is invariant under conjugation and hence real. Note that g is differentiable. Furthermore, the set of roots of g equals $\{2\pi j/n : 1\leq j<n,(j,n)=1\}$. All of the roots are simple. Since $g(0)=\Phi_n(1)>0$ we infer that $g(t)=(-1)^{\varphi(nt/(2\pi);n)}|\Phi_n(e^{it})|$, which by substituting $t=2\pi j/m$ yields the result. □

Corollary 17. *Write $\xi_m=\zeta_m^j$. In case $\Phi_n(\xi_m)\in\{-1,1\}$ for some $n\geq 2$, then we have $\Phi_n(\xi_m)=(-1)^{\varphi(nj/m;n)+j\varphi(n)/m}$.*

Proof. Write $\xi_m=\zeta_m^j$. If $\Phi_n(\xi_m)\in\{-1,1\}$, then $\Phi_n(\xi_m)=(-1)^{\varphi(nj/m;n)}\xi_m^{\varphi(n)/2}$. By Lemma 15 we obtain that $m\mid\varphi(n)$. The result now follows on noting that $\xi_m^{\varphi(n)/2}=(-1)^{j\varphi(n)/m}$. □

Lemma 18. *Let us assume that there exists $p \equiv 1 \pmod{m}$ and $k \geq 1$ such that $n = p^k n'$ with $p \nmid n'$.*
a) *If $n' \neq m$, then $\Phi_n(\xi_m) = 1$.*
b) *If $n' = m$, then $\Phi_n(\xi_m) = p$.*

Proof.
a) We have $\Phi_n(x) = \Phi_{n'}(x^{p^k})/\Phi_{n'}(x^{p^{k-1}})$ due to Lemma 2. By noting that $\xi_m^p = \xi_m$ it follows that

$$\Phi_n(\xi_m) = \frac{\Phi_{n'}(\xi_m^{p^k})}{\Phi_{n'}(\xi_m^{p^{k-1}})} = 1.$$

b) We apply L'Hôpital's rule and obtain

$$\Phi_n(\xi_m) = \frac{p^k \xi_m^{p^k-1} \Phi'_m(\xi_m^{p^k})}{p^{k-1} \xi_m^{p^{k-1}-1} \Phi'_m(\xi_m^{p^{k-1}})} = p. \qquad \square$$

A version of Lemma 18 has already been stated by Motose [14, Section 4]. Nonetheless, it contains a mistake since his lemma claims that $\Phi_n(\xi_m) = 1$ for case b).

Lemma 19. *Let us assume that there exists $p \equiv -1 \pmod{m}$ and $k \geq 1$ such that $n = p^k n'$ with $p \nmid n'$.*
a) *If $n' = 1$, then $\Phi_n(\xi_m) = -\xi_m^{(-1)^k}$.*
b) *If $n' \neq m$, then $\Phi_n(\xi_m) = \xi_m^{(-1)^k \varphi(n')}$. Furthermore, if $n' \geq 3$, then $\Phi_n(\xi_m) = \xi_m^{\varphi(n)/2}$.*
c) *If $n' = m$, then $\Phi_n(\xi_m) = -p\xi_m^{(-1)^k \varphi(m)}$.*

Proof.
a) By (3) we have

$$\Phi_{p^k}(\xi_m) = \frac{\xi_m^{p^k} - 1}{\xi_m^{p^{k-1}} - 1}.$$

Assertion a) is easily established on noting that $\xi_m^{p^k} = \xi_m^{(-1)^k}$.
b) We have $\Phi_n(x) = \Phi_{n'}(x^{p^k})/\Phi_{n'}(x^{p^{k-1}})$. In light of the self-reciprocity of $\Phi_{n'}$ we find that

$$\Phi_n(\xi_m) = \frac{\Phi_{n'}\left(\xi_m^{(-1)^k}\right)}{\Phi_{n'}\left(\xi_m^{(-1)^{k+1}}\right)} = \xi_m^{(-1)^k \varphi(n')}.$$

Furthermore, if $n' \geq 3$, then $\varphi(n)/2 = p^{k-1}(p-1)\varphi(n')/2 \equiv (-1)^k \varphi(n') \pmod{m}$.
c) L'Hôpital's rule yields

$$\Phi_n(\xi_m) = \frac{p^k \xi_m^{p^k-1} \Phi'_m(\xi_m^{p^k})}{p^{k-1} \xi_m^{p^{k-1}-1} \Phi'_m(\xi_m^{p^{k-1}})} = p\xi_m^{2(-1)^k} \frac{\Phi'_m(\xi_m^{(-1)^k})}{\Phi'_m(\xi_m^{(-1)^{k+1}})}.$$

Assertion c) follows on differentiating the equality $\Phi_m(z) = z^{\varphi(m)} \Phi_m(1/z)$ giving rise to

$$\Phi'_m(\xi_m^{(-1)^k}) = -\xi_m^{(-1)^k(\varphi(m)-2)} \Phi'_m(\xi_m^{(-1)^{k+1}}). \qquad \square$$

4. The values - general method

In this section we present a general method of computing $\Phi_n(\xi_m)$. Our first step is to reduce to the case where m is coprime to n. In order to do this, we write $n = n_1 n_2$, where $n_1 = \prod_{p^e \| n,\ p \nmid m} p^e$ is the largest divisor of n which is coprime to m. By the equations of Lemma 2 and by an induction on n_2 we have

$$\Phi_n(\xi_m) = \prod_{d \mid n_2} \Phi_{n_1}(\xi_m^d)^{\mu(n_2/d)}. \tag{11}$$

For small n_2 this formula is quite effective.

Therefore throughout this section we assume that $m, n > 1$ are coprime.

Proof of Theorem 1. Note that $\log(1-\xi_m^d)$ considered as a function d is periodic with period m and so it can be treated as a function $G(m) \to \mathbb{C}$. It follows that

$$\log(1-\xi_m^d) = \frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} C_\chi(\xi_m)\chi(d).$$

We find that $\log \Phi_n(\xi_m)$, up to a multiple of $2\pi i$, equals

$$\sum_{d \mid n} \mu(\frac{n}{d}) \log(1-\xi_m^d) = \frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} C_\chi(\xi_m) J_0(\chi; n).$$

The proof is completed by invoking Lemma 14 with $k = 0$. □

Remark 20. A character χ may be omitted if there exists a prime $p \mid n$ for which $\overline{\chi}(p) = 1$. In particular, the principal character may be omitted. It makes computing $\Phi_n(\xi_m)$ using Theorem 1 a less daunting task.

If we wish only to compute $|\Phi_n(\xi_m)|$, then in addition we may omit all characters χ satisfying $\chi(-1) = -1$, since for such characters we have

$$C_\chi(\xi_m) = \frac{1}{2} \sum_{g \in G(m)} \left(\overline{\chi}(g) \log(1-\xi_m^g) + \overline{\chi}(-g) \log(1-\xi_m^{-g}) \right) \in i\mathbb{R}.$$

Corollary 21. *Let $(m,n) = 1$ and $n > 1$.*
a) *If n has any prime divisor q congruent to 1 modulo m, then $\Phi_n(\xi_m) = 1$.*
b) *If $m \in \{3,4,6\}$ and n has no prime divisor congruent to 1 modulo m then*

$$\Phi_n(\xi_m) = -(\xi_m)\ ^\wedge(-(-2)^{\omega(n)-1}).$$

Proof.
a) As $\overline{\chi}(p) = \overline{\chi}(1) = 1$ we have $\prod_{p|n}(1-\overline{\chi}(p)) = 0$, so $\Phi_n(\xi_m) = e^0 = 1$.
b) Note that there is only one non-principal character χ and that it satisfies $\chi(-1) = -1$. Therefore $\prod_{p|n}(1-\overline{\chi}(p)) = 2^{\omega(n)}$ and $C_\chi(\xi_m) = \log(1-\xi_m) - \log(1-\xi_m^{-1})$. It follows that

$$\Phi_n(\xi_m) = \exp\left(\frac{1}{2}(\log(1-\xi_m) - \log(1-\xi_m^{-1}))\chi(n) 2^{\omega(n)} \right) = -(\xi_m)\ ^\wedge(-(-2)^{\omega(n)-1}),$$

as desired. □

Corollary 22. *Let $m \in \{5,8,10,12\}$ and $n > 1$ be coprime with m. Suppose that n has no prime divisor $\pm 1 \pmod m$. Then*

$$\log|\Phi_n(\xi_m)| = (-1)^{\Omega(n)-1} 2^{\omega(n)-1} \log|\gamma_m|,$$

where

$$\gamma_m = \begin{cases} 1+\xi_m & \text{if } m=5; \\ 1+\xi_m+\xi_m^2 & \text{if } m\in\{8,10\}; \\ 1+\xi_m+\xi_m^2+\xi_m^3+\xi_m^4 & \text{if } m=12. \end{cases}$$

Proof. The only non-principal character for which $C_\chi(\xi_m)$ has non-zero real part is the quadratic character χ. We have $\Re C_\chi(\xi_m) = -2\log|\gamma_m|$ and by Theorem 1

$$\log|\Phi_n(\xi_m)| = -\frac{1}{2}(\log|\gamma_m|)\ \chi(n)\ \prod_{p\mid n}(1-\overline{\chi}(p)).$$

The assumption on n we made implies that $\overline{\chi}(p) = -1$ for all $p \mid n$ and hence $\chi(n) = (-1)^{\Omega(n)}$ and so $\prod_{p\mid n}(1-\overline{\chi}(p)) = 2^{\omega(n)}$. □

5. Cyclotomic values in roots of unity of low order

In this section we apply the obtained results in order to easily compute $\Phi_n(\zeta_m)$ for $m \in \{3,4,5,6\}$. For $m \in \{3,4,6\}$ these values have already been computed by Motose [14]. However, some of the results in Section 3 allow us to provide shorter proofs. For $m \in \{1,2\}$ the computation is folklore and it was discussed in Section 2.3.

In [14], there are some inaccuracies. As we mention in Section 3 in part (1) of the first lemma one has also to require that $m \neq l$. This oversight leads to the incorrect assertion in Proposition 3 that if $p \equiv 1 \pmod 3$ for some prime divisor p of m, then $\Phi_n(\zeta_3) = 1$. This is false as $\Phi_{3p^k}(\zeta_3) = p$. A similar remark applies to Proposition 4, where $\Phi_{6p^k}(\zeta_6) = p$, rather than 1 as claimed. In the statement of Proposition 3 part (2) one has to read $l+k$ instead of $l+k-1$. As the proof is carried out correctly, this is a typo. As consequence of the typo in Proposition 3, the exponent in case (6) in Proposition 4 is computed to be $l+s+k$ instead of $l+s+k-1$.

5.1. Calculation of $\Phi_n(i)$.

Lemma 18 and Lemma 19 reduce the number of possible cases. Hence it is not difficult to establish the following result.

Lemma 23. *We have $\Phi_n(i) = 1$ except for the cases listed in the table below.*

n	$\Phi_n(i)$
1	$i-1$
2	$i+1$
4	0
$4p^k$	p
p_3^k	$(-1)^{k+1}i$
$2p_3^k$	$(-1)^k i$
$p_3^k q_3^l,\ 2p_3^k q_3^l$	-1

Here p, p_3 and q_3 are primes such that $p_3 \neq q_3$ and $p_3 \equiv q_3 \equiv 3 \pmod 4$. Furthermore, k and l are arbitrary positive integers.

Proof. The first three entries of the table follow by direct computation and hence we may assume that $n \neq 1,2,4$.

- In case $4 \mid n$ we have $\Phi_n(i) = \Phi_{n/2}(-1)$ and, by applying Lemma 7, $\Phi_n(i)$ is seen to equal p if $n = 4p^k$ and 1 otherwise.
- In case $4 \nmid n$, we separately consider three subcases:

a) The integer n has a prime factor $p \equiv 1 \pmod 4$.
By Lemma 18 we have $\Phi_n(i) = 1$.
b) The integer n is odd and has no prime factor $p \equiv 1 \pmod 4$.
Thus we can write $n = q_1^{e_1} \cdots q_r^{e_r}$ with $q_j \equiv 3 \pmod 4$ and $e_j \geq 1$ for every $1 \leq j \leq r$.
By Lemma 19 it follows that $\Phi_n(i) = (-1)^{e_1+1} i$ if $r = 1$, $\Phi_n(i) = -1$ if $r = 2$ and $\Phi_n(i) = 1$ otherwise.
c) The integer n is even and has no prime factor $p \equiv 1 \pmod 4$.
Note that $\Phi_n(i) = \Phi_{n/2}(-i) = \overline{\Phi_{n/2}(i)}$ and hence the result follows from subcase b).

Since we have covered all cases, the proof is concluded. □

5.2. **Calculation of $\Phi_n(\zeta_3)$.**

Lemma 24. *We have $\Phi_n(\zeta_3) = 1$ except for the cases listed in the table below.*

n	$\Phi_n(\zeta_3)$
1	$\zeta_3 - 1$
3	0
$3p^k$	p
q^k	$-1/\zeta$
$3q^k$	$-q\zeta$
$q_1^{e_1} \dots q_r^{e_r},\ r \geq 2$	$1/\zeta$
$3q_1^{e_1} \dots q_r^{e_r},\ r \geq 2$	ζ

Here $p \not\equiv 2 \pmod 3$ is a prime. The integers q and $q_1, \dots, q_r$ are primes congruent to 2 modulo 3 with $r \geq 2$ and $q_1, \dots, q_r$ distinct. Furthermore, k and $e_1, \dots, e_r$ are arbitrary positive integers and $\zeta = (\zeta_3)^{\wedge}(-1)^s$ with $s = \Omega(n) - \omega(n) = \Omega(n/\mathrm{rad}(n))$.

Proof. The first two entries of the table follow by direct computation and hence we may assume that $n \neq 1, 3$.

- In case $9 \mid n$ we have $\Phi_n(\zeta_3) = \Phi_{n/3}(1)$ by invoking Lemma 2. This yields 3 if n is a power of 3 and 1 otherwise.
- In case $9 \nmid n$ we separately consider three subcases:
  a) The integer n has a prime factor $p \equiv 1 \pmod 3$.
  Lemma 18 yields $\Phi_n(\zeta_3) = p$ if $n = 3p^k$ and 1 otherwise.
  b) The integer n has no prime factor $p \equiv 1 \pmod 3$ and $3 \nmid n$.
  Thus we can write $n = q_1^{e_1} \cdots q_r^{e_r}$ with $q_j \equiv 2 \pmod 3$ and $e_j \geq 1$ for every $1 \leq j \leq r$.
  We distinguish two cases:
  $r = 1$. By Lemma 19a it follows that $\Phi_{q_1^{e_1}}(\zeta_3) = -(\zeta_3)^{\wedge}(-1)^{s-1} = -1/\zeta$.
  $r \geq 2$. On applying Lemma 19b we obtain $\Phi_n(\zeta_3) = (\zeta_3)^{\wedge}(-1)^{s+1} = 1/\zeta$.
  c) The integer n has no prime factor $p \equiv 1 \pmod 3$ and $3 \mid n$.
  Note that $\Phi_n(\zeta_3) = \Phi_{n/3}(1)/\Phi_{n/3}(\zeta_3)$ as a consequence of Lemma 2. Hence the result follows from the subcase b) and Lemma 4. □

5.3. **Calculation of $\Phi_n(\zeta_6)$.** In our computation of $\Phi_n(\zeta_6)$ we make freely use of the fact that $-\zeta_3 = \zeta_6^{-1}$.

Lemma 25. *We have $\Phi_n(\zeta_6) = 1$ except for the cases listed in the table below.*

n	$\Phi_n(\zeta_6)$
1	ζ_3
2	ζ_6+1
3	$2\zeta_6$
6	0
$6p^k$	p
$2q^k$	$-\zeta$
$6q^k$	$-q/\zeta$
$q_1^{e_1}\dots q_r^{e_r}$ *(different from* 2 *and* $2q^k$*)*	ζ
$3q_1^{e_1}\dots q_r^{e_r}$ *(different from* 6 *and* $6q^k$*)*	$1/\zeta$

Here p is 3 *or a prime number congruent to* 1 *modulo* 6*. The integers q and $q_1,\dots,q_r$ are* 2 *or primes congruent to* 5 *modulo* 6 *with $r\geq 1$ and $q_1,\dots,q_r$ distinct. Furthermore k and $e_1,\dots,e_r$ are arbitrary positive integers and $\zeta=(\zeta_3)^{\wedge}(-1)^s$ with $s=\Omega(n)-\omega(n)=\Omega(n/\mathrm{rad}(n))$.*

Proof. The first four entries of the table follow by direct computation and hence we may assume that $n\neq 1,2,3,6$.

- In case $\nu_3(n)\geq 2$ we have $\Phi_n(\zeta_6)=\Phi_{n/3}(-1)$, which yields 3 if $n=6\cdot 3^k$ and 1 otherwise.
- In case $\nu_3(n)\leq 1$ we separately consider three subcases:
  a) The integer n has a prime factor $p\equiv 1 \pmod 6$.
  By Lemma 18 we obtain p if $n=6p^k$ and 1 otherwise.
  b) The integer n has no prime factor $p\equiv\pm 1 \pmod 6$.
  There are two possibilities:
    i) $n=2^{k+1}$. We have $\Phi_n(\zeta_6)=\Phi_{n/2}(\zeta_3)=-(\zeta_3)^{\wedge}(-1)^k=-\zeta$.
    ii) $n=6\cdot 2^k$. We have $\Phi_n(\zeta_6)=\Phi_{n/2}(\zeta_3)=-2(\zeta_3)^{\wedge}(-1)^{k+1}=-2/\zeta$.
  c) The integer n has no prime factor $p\equiv 1 \pmod 6$ and it has a prime factor $q\equiv -1 \pmod 6$.
  There are three possibilities:
    i) $n=q^k$. Lemma 19a yields $\Phi_n(\zeta_6)=-(\zeta_6)^{\wedge}(-1)^k=\zeta$.
    ii) $n=q^kn'$ with $1<n'\neq 6$ and $q\nmid n'$. Lemma 19b implies $\Phi_n(\zeta_6)=(\zeta_6)^{\wedge}((-1)^k\varphi(n'))$.
    Thus we have $\Phi_{2q^k}(\zeta_6)=-\zeta$. Let us assume $n'>2$. Now we compute $\zeta_6^{\varphi(n')}$.
    – If $3\nmid n'$, then $\zeta_6^{\varphi(n')}=\zeta_3^{\varphi(n')/2}=(\zeta_3)^{\wedge}(-1)^{\Omega(n')-\omega(n')+1}$ and $\Phi_n(\zeta_6)=\zeta$.
    – If $3\mid n'$, then $\zeta_6^{\varphi(n')}=\zeta_3^{\varphi(n'/3)}=(\zeta_3)^{\wedge}(-1)^{\Omega(n')-\omega(n')}$ and $\Phi_n(\zeta_6)=1/\zeta$.
    iii) $n=6q^k$. We have $\Phi_n(\zeta_6)=\Phi_{n/3}(-1)/\Phi_{n/3}(\zeta_6)=-q/\zeta$. □

Lemma 26. *Let $m\in\{1,2,3,4,6\}$ and $n>m$ be integers. Then*

$$|\Phi_n(\xi_m)|=\begin{cases}p & \text{if } n/m=p^k \text{ is a prime power;}\\ 1 & \text{otherwise.}\end{cases}$$

Proof. For $m=1,2$ the result follows by Lemma 4, respectively Lemma 7. So we may assume that $m\in\{3,4,6\}$ (and so $n>m\geq 3$). Since $\deg\Phi_n=\varphi(n)$ is even for $n\geq 4$, it follows by Lemma 13 that $\Phi_n(\zeta_m)=\zeta_m^{\varphi(n)/2}a$, with a an integer. Letting the Galois automorphisms of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ act on both sides of this identity we see that $|\Phi_n(\xi_m)|$ is an integer that is independent of the specific choice of ξ_m. The result now follows from Theorem 9 and the identity (9). □

Remark 27. Lemma 26 can also be deduced from Lemmas 4, 7, 23, 24 and 25.

5.4. **Calculation of $\Phi_n(\zeta_5)$.** We use Corollary 22 and Lemma 16 to compute $\Phi_n(\zeta_5)$. One can also compute $\Phi_n(\zeta_m)$ for $m \in \{8, 10, 12\}$ by a similar procedure. Nonetheless, the number of possible cases significantly increases for those values of m.

Lemma 28. *We have $\Phi_n(\zeta_5) = 1$ except for the cases listed in the table below.*

n	$\Phi_n(\zeta_5)$
1	$\zeta_5 - 1$
5	0
$5p^k$	p
q^k	$-(\zeta_5)^\wedge(-1)^k$
$q^k n_1, q \nmid n_1$	$(\zeta_5)^\wedge((-1)^k\varphi(n_1))$
n_2	$(-1)^{\varphi(n/5;n)}\zeta_5^{\varphi(n)/2}\lvert 1+\zeta_5\rvert^\wedge((-1)^{\Omega(n)+1}2^{\omega(n)-1})$
$5n_1$	$e^{\Lambda(n_1)}/\Phi_{n_1}(\zeta_5)$

Here p is 5 or a prime number congruent to 1 modulo 5 and q is a prime congruent to -1 modulo 5. The integers $n_1, n_2 \geq 2$ are not divisible by 5 and verify

- *$p' \not\equiv 1 \pmod 5$ for every prime p' dividing n_1;*
- *$p' \not\equiv \pm 1 \pmod 5$ for every prime p' dividing n_2.*

Furthermore, k is an arbitrary positive integer.

Proof. The first two entries of the table follow by direct computation and hence we may assume that $n \neq 1, 5$.

- In case $\nu_5(n) \geq 2$ we have $\Phi_n(\zeta_5) = \Phi_{n/5}(1)$, which yields 5 if $n = 5^{k+1}$ and 1 otherwise.
- In case $\nu_5(n) = 0$ we separately consider three subcases:
  a) The integer n has a prime factor $p \equiv 1 \pmod 5$.
  By Lemma 18 we obtain p if $n = 5p^k$ and 1 otherwise.
  b) The integer n has no prime factor $p \equiv 1 \pmod 5$ and it has a prime factor $q \equiv -1 \pmod 5$. There are two possibilities:
    i) $n = q^k$. Lemma 19a yields $\Phi_n(\zeta_5) = -(\zeta_5)^\wedge(-1)^k$.
    ii) $n = q^k n_1'$ with $q \nmid n_1'$. Lemma 19b implies $\Phi_n(\zeta_5) = (\zeta_5)^\wedge((-1)^k\varphi(n'))$.
  c) The integer n has no prime factor $p \equiv \pm 1 \pmod 5$.
  Corollary 22 shows $|\Phi_n(\zeta_5)| = |1+\zeta_5|^\wedge((-1)^{\Omega(n)+1}2^{\omega(n)-1})$. The value $\Phi_n(\zeta_5)$ is obtained by Lemma 16.
- In case $\nu_5(n) = 1$ we have $\Phi_n(\zeta_5) = \Phi_{n/5}(1)/\Phi_{n/5}(\zeta_5) = e^{\Lambda(n/5)}/\Phi_{n/5}(\zeta_5)$. □

6. The logarithmic derivative $f_n(z)$ of $\Phi_n(z)$

In this section we consider the logarithmic derivative $f_n(z)$ of $\Phi_n(z)$. Thus

$$f_n(z) = (\log \Phi_n(z))' = \frac{\Phi_n'(z)}{\Phi_n(z)}.$$

If we compute $f_n(\xi_m)$, then we can use the value $\Phi_n(\xi_m)$ to obtain $\Phi_n'(\xi_m)$. First, we calculate $f_n(\pm 1)$ with elementary methods. Later, we apply the ideas presented in Section 4 to develop a general method for computing $f_n(\zeta_m)$ when $(n, m) = 1$. Note that as a consequence of (11) we can reduce the computation of $f_n(\zeta_m)$ to the case when n and m are coprime. Indeed for $n = n_1 n_2$, where $n_1 = \prod_{p^e \| n,\ p \nmid m} p^e$, we have

$$f_n(\xi_m) = \sum_{d \mid n_2} \mu(n_2/d) f_{n_1}(\xi_m^d). \tag{12}$$

This method will be used to easily obtain $f_n(\zeta_m)$ for $m \in \{3,4,6\}$.

Lemma 29. *We have $f_n(1) = \varphi(n)/2$ for $n > 1$ and $f_n(-1) = -\varphi(n)/2$ for every $n \neq 2$.*

Proof. The proof follows from applying Lemma 12 with $f = \Phi_n$ and $d = \varphi(n)$. □

Corollary 30. *We have*

$$\Phi_n'(1) = \begin{cases} 1 & \text{if } n = 1; \\ p\varphi(n)/2 & \text{if } n = p^e; \\ \varphi(n)/2 & \text{otherwise.} \end{cases} \qquad \Phi_n'(-1) = \begin{cases} 1 & \text{if } n = 2; \\ -p\varphi(n)/2 & \text{if } n = p^e; \\ -\varphi(n)/2 & \text{otherwise.} \end{cases}$$

Theorem 31. *Let us assume that $n, m > 1$ are coprime. For all $\chi \in \widehat{G}(m)$ put*

$$c_\chi(\xi_m) = \sum_{g \in G(m)} \frac{\xi_m^{-1}\xi_m^g}{1-\xi_m^g}\overline{\chi}(g).$$

Then

$$f_n(\xi_m) = -\frac{n}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} c_\chi(\xi_m)\chi(n) \prod_{p \,|\, n}(1 - \frac{\overline{\chi}(p)}{p}).$$

Proof. Logarithmic differentiation of (4) yields

$$f_n(z) = -\sum_{d \,|n} \mu\big(\frac{n}{d}\big) \frac{dz^{d-1}}{1-z^d}.$$

The function $\xi_m^{d-1}/(1-\xi_m^d)$ of variable d can be treated as a function $G(m) \to \mathbb{C}$. Therefore for all $d \mid n$ we have

$$\frac{\xi_m^{d-1}}{1-\xi_m^d} = \frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} c_\chi(\xi_m)\chi(d).$$

Applying this to the above formula on f_n we obtain

$$f_n(\zeta_m) = -\frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} c_\chi(\xi_m) \sum_{d \,|n} \mu(\frac{n}{d}) d\chi(d) = -\frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G}(m)} c_\chi(\xi_m) J_1(\chi; n).$$

The proof is completed by invoking Lemma 14 with $k = 1$. □

Corollary 32. *Set $m \in \{3,4,6\}$ and $n > 1$ coprime. We have*

$$f_n(\xi_m) = \frac{\varphi(n)}{2\xi_m} \left(1 - (-1)^{\Omega(n_-)} \frac{1+\xi_m}{1-\xi_m} \prod_{p \,|\, n_-} \frac{p+1}{p-1}\right),$$

where n_- is the product of the prime powers $p^k \parallel n$ with $p \equiv -1 \pmod m$.

Proof. In case $m \in \{3,4,6\}$ there are precisely two characters: the principal character χ_1 and the non-principal character χ_2. A simple computation gives

$$c_{\chi_1}(\xi_m) = \frac{1-\xi_m^{-1}}{1-\xi_m} = -\xi_m^{-1}, \qquad c_{\chi_2}(\xi_m) = \frac{1+\xi_m^{-1}}{1-\xi_m}.$$

Theorem 31 yields

$$f_n(\xi_m) = \frac{\xi_m^{-1}}{2} n \prod_{p \,|\, n}(1 - \frac{1}{p}) - \frac{1+\xi_m^{-1}}{2(1-\xi_m)} n\chi_2(n) \prod_{p \,|n}(1 - \frac{\overline{\chi_2}(p)}{p}),$$

which is easily rewritten in the desired way by noting that $\chi_2(n) = (-1)^{\Omega(n_-)}$. □

7. The result of Vaughan

We use Corollary 22 to give an alternative proof of the following theorem by Vaughan [17].

Theorem 33. *Let A_n denote the height of Φ_n. There exist infinitely many integers n for which*

$$\log\log A_n \geq (\log 2 + o(1))\frac{\log n}{\log\log n}.$$

Proof. Let x be large and n be a product of all primes $p \leq x$ satisfying $p \equiv \pm 2 \pmod 5$. By two equivalent versions of the prime number theorem for arithmetic progressions we have

$$\log n = \sum_{p\leq x,\ p\equiv\pm 2 \pmod 5} \log p \sim \frac{x}{2},$$

respectively

$$\omega(n) = \sum_{p\leq x,\ p\equiv\pm 2 \pmod 5} 1 \sim \frac{x}{2\log x}.$$

It follows that $\log\log n \sim \log x$ and so

$$\omega(n) \sim \frac{\log n}{\log\log n} \tag{13}$$

as x (and hence n) tends to infinity. Recall that by Corollary 22 we have

$$\log|\Phi_n(\xi_5)| = (-2)^{\omega(n)-1}\log|1+\xi_5|.$$

One checks that there is a primitive fifth root of unity ζ for which $\log|1+\zeta| > 0$, but also one for which $\log|1+\zeta| < 0$. Thus we can choose a primitive fifth root of unity z_n for which $\log|\Phi_n(z_n)| > 0$. By Corollary 22 and the asymptotic equality (13) we infer that there is an x_0 such that for all $x \geq x_0$ the corresponding n satisfies $\log|\Phi_n(z_n)| > \log n$. It follows that for $x \geq x_0$ (and hence n) tending to infinity the asymptotic inequality

$$\log\log A_n \geq \log\log\left(\frac{|\Phi_n(z_n)|}{n}\right) = (\log 2 + o(1))\frac{\log n}{\log\log n}$$

holds true, where the first inequality is a consequence of (1). □

8. Application to Kronecker polynomials

A *Kronecker polynomial* is a monic polynomial with integer coefficients having all of its roots on or inside the unit disc. The following result of Kronecker relates Kronecker polynomials with cyclotomic polynomials.

Lemma 34 (Kronecker, 1857; cf. [6])**.** *If f is a Kronecker polynomial with $f(0) \neq 0$, then all roots of f are actually on the unit circle and f factorizes over the rationals as a product of cyclotomic polynomials.*

By this result and the fact that cyclotomic polynomials are monic and irreducible we can factorize a Kronecker polynomial $f(x)$ into irreducibles as

$$f(x) = x^e \prod_{d\in\mathcal{D}} \Phi_d(x)^{e_d}, \tag{14}$$

with $e \geq 0$, $\mathcal{D}$ a finite set and each $e_d \geq 1$.

Corollary 35. *Let f be a Kronecker polynomial with $f(0) \neq 0$. Let k be such that $\Phi_1^k \parallel f$. If k is even, then f is self-reciprocal, otherwise f is anti self-reciprocal.*

Proof. Recall that Φ_1 is anti self-reciprocal and Φ_d is self-reciprocal for $d \geq 2$. □

In light of Corollary 35 one can apply the results of Section 2.6 to Kronecker polynomials.

Proposition 36. *Let f be a Kronecker polynomial with $f(0) \neq 0$. Then*
a) $f(1) \geq 0$.
b) *If $f(1) \neq 0$, then $f(-1) \geq 0$. Furthermore, if $f(-1) > 0$, then $f(x) > 0$ for all $x \in \mathbb{R}$.*

Proof.
a) We have $f(1) \geq 0$ by (14) and Lemma 4.
b) If $f(1) \neq 0$, then $1 \notin \mathcal{D}$. We have $\Phi_n(-1) \geq 0$ for every $n > 1$ by Lemma 7. Hence we obtain $f(-1) \geq 0$. Furthermore, if $f(-1) > 0$, then $2 \notin \mathcal{D}$. Let $x \in \mathbb{R}$. We have $\Phi_n(x) > 0$ for every $n > 2$ and, consequently, $f(x) > 0$. □

Using Lemma 34 and the results of Section 5 one can obtain some information about the factorization and the values of Kronecker polynomials.

Lemma 37. *Let $m \in \{1, 2, 3, 4, 6\}$. Suppose that f is of the form* (14) *and, moreover, satisfies $\min \mathfrak{D} > m$. Then*

$$|f(\xi_m)| = \prod_{\substack{d \in \mathfrak{D} \\ m|d,\ \Lambda(d/m) \neq 0}} |\Phi_d(\xi_m)|^{e_d} = \exp\Big(\sum_{d \in \mathfrak{D},\ m|d} e_d \Lambda(d/m) \Big) \in \mathbb{Z}_{>0}.$$

The following result is a reformulation of the latter, but with $\mathfrak{D}$ assumed to be unknown.

Lemma 38. *Let f be a Kronecker polynomial and $m \in \{1, 2, 3, 4, 6\}$. Let us also assume that $f(\zeta_d) \neq 0$ for every $d \leq m$. Then $|f(\xi_m)|$ is an integer and each of its prime factors q is contributed by a divisor Φ_d of f with $d = mq^t$ for some $t \geq 1$.*

These lemmas are easily proved on using Lemma 26 and weaker versions of them have already been applied to cyclotomic numerical semigroups [4].

`Acknowledgement`. We acknowledge helpful discussions with Peter Stevenhagen (mathematical content, presentation) and Lola Thompson (presentation, English) of earlier versions of this paper. In particular, Peter Stevenhagen sketched the third author how to compute the resultant of two cyclotomic polynomials by purely algebraic number theoretical means. In this paper we presented another proof staying closer to the basic definitions (Theorem 9). We also thank Hendrik Lenstra for pointing out some glitches in an earlier version.

A substantial part of this paper was written during a one month internship in the autumn of 2016 of the second author at the Max Planck Institute for Mathematics in Bonn. He would like to thank the third author for the opportunity given and the staff for their hospitality. He would also like to acknowledge the third author and Pedro A. García-Sánchez for their teachings and guidance.

References

[1] F. Amoroso, Algebraic numbers close to 1 and variants of Mahler's measure, *J. Number Theory* **60** (1996), 80–96.
[2] T.M. Apostol, Resultants of cyclotomic polynomials, *Proc. Amer. Math. Soc.* **24** (1970), 457–462.
[3] B. Bzdęga, On a generalization of Beiter Conjecture, *Acta Arith.* **173** (2016), 133–140.
[4] E.-A. Ciolan, P. García-Sánchez, and P. Moree, Cyclotomic numerical semigroups, *SIAM J. Discrete Math.* **30** (2016), 650–668.

[5] H. Cremer, *Carmina mathematica und andere poetische Jugendsünden.* 7. Aufl., Aachen: Verlag J. A. Mayer (1982).
[6] P.A. Damianou, Monic polynomials in $\mathbb{Z}[x]$ with roots in the unit disc, *Amer. Math. Monthly,* **108** (2001), 253–257. *Amer. Math. Monthly* **109** (2002), 217–234.
[7] F.-E. Diederichsen, Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetisher Äquivalenz, *Abh. Math. Sem. Hansischen Univ.* **13** (1940), 357–412.
[8] G. Dresden, Resultants of cyclotomic polynomials, *Rocky Mountain J. Math.* **42** (2012), 1461–1469.
[9] R.P. Kurshan and A.M. Odlyzko, Values of cyclotomic polynomials at roots of unity, *Mathematica Scandinavica* **49** (1981), 15–35.
[10] S. Lang, *Cyclotomic fields I and II.* Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics **121**, Springer-Verlag, New York, 1990.
[11] S. Lang, *Algebraic number theory.* Second edition. Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1994.
[12] E. Lehmer, A numerical function applied to cyclotomy, *Bull. Amer. Math. Soc.* **36** (1930), 291–298.
[13] S. Louboutin, Resultants of cyclotomic polynomials, *Publ. Math. Debrecen* **50** (1997), 75–77.
[14] K. Motose, On values of cyclotomic polynomials. VIII, *Bull. Fac. Sci. Technol. Hirosaki Univ.* **9** (2006), 15–27.
[15] R. Sivaramakrishnan, *Classical theory of arithmetic functions*, Monographs and Textbooks in Pure and Applied Mathematics **26**, Marcel Dekker, Inc., New York, 1989.
[16] R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, 311–322.
[17] R.C. Vaughan, Bounds for the coefficients of cyclotomic polynomials, *Michigan Math. J.* **21** (1975), 289–295.

Bartłomiej Bzdęga
Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznan, Poland.
e-mail: exul@amu.edu.pl

Andrés Herrera-Poyatos
Faculty of Science, University of Granada, Avenida de la Fuente Nueva, 18071 Granada, Spain.
e-mail: andreshp9@gmail.com

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