ACTA ARITHMETICA
204.4 (2022)

Cyclotomic factors of necklace polynomials

by

Trevor Hyde (Chicago, IL)

1. Introduction. The *dth necklace polynomial* $M_d(x)$, for positive integral d, is defined by

$$M_d(x) := \frac{1}{d}\sum_{e|d}\mu(e)x^{d/e},$$

where μ is the number-theoretic Möbius function and the sum is over all positive divisors e of d. Necklace polynomials arise naturally in number theory, combinatorics, dynamics, geometry, representation theory, and algebra. For example, if q is a prime power and $\mathbb{F}_q$ is a finite field with q elements, then $M_d(q)$ is the number of $\mathbb{F}_q$-irreducible monic polynomials of degree d in $\mathbb{F}_q[x]$; if $k \geq 1$ is a natural number, then $M_d(k)$ is the number of aperiodic necklaces comprised of d beads chosen from among k colors.

We begin with the empirical observation that necklace polynomials are highly reducible over $\mathbb{Q}$. For example, if $d = 105$, then

$$\begin{aligned}M_{105}(x) &= \tfrac{1}{105}(x^{105} - x^{35} - x^{21} - x^{15} + x^7 + x^5 + x^3 - x)\\ &= e(x)(x^4+1)(x^2-x+1)(x^2+1)(x^2+x+1)(x+1)(x-1)x,\end{aligned} \tag{1.1}$$

where $e(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of degree 92. With only two exceptions, the irreducible factors of $M_{105}(x)$ are cyclotomic polynomials. Recall that the *mth cyclotomic polynomial* $\Phi_m(x)$ is the $\mathbb{Q}$-minimal polynomial of a primitive mth root of unity. With this notation, (1.1) may be expressed as

$$M_{105}(x) = e(x)\cdot\Phi_8\cdot\Phi_6\cdot\Phi_4\cdot\Phi_3\cdot\Phi_2\cdot\Phi_1\cdot x.$$

2020 *Mathematics Subject Classification*: Primary 11C08; Secondary 11T22, 11T24, 52C35, 68R15.

Key words and phrases: necklace polynomial, cyclotomic polynomial, roots of unity.

Received 4 March 2021; revised 22 October 2021.

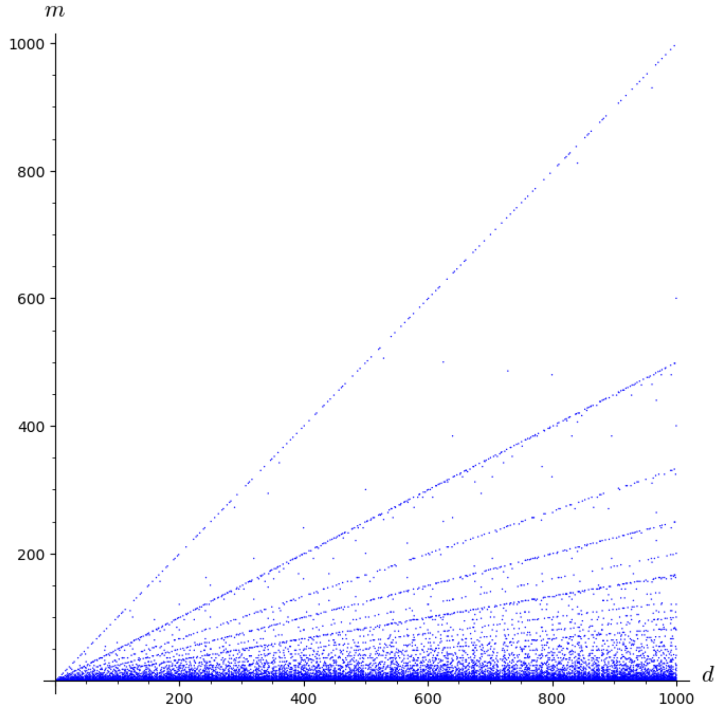
Published online 25 August 2022.

DOI: 10.4064/aa210304-11-5

Here are several more examples: there are irreducible, non-cyclotomic polynomials $f(x), g(x), h(x) \in \mathbb{Q}[x]$ with degrees 148, 212, and 708, respectively, such that

$$\begin{aligned} M_{165}(x) &= \tfrac{1}{165}(x^{165} - x^{55} - x^{33} - x^{15} + x^{11} + x^5 + x^3 - x), \\ &= f(x) \cdot \Phi_{12} \cdot \Phi_{10} \cdot \Phi_5 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \\ M_{231}(x) &= \tfrac{1}{231}(x^{231} - x^{77} - x^{33} - x^{21} + x^{11} + x^7 + x^3 - x) \\ &= g(x) \cdot \Phi_{10} \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_5 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \\ M_{741}(x) &= \tfrac{1}{741}(x^{741} - x^{247} - x^{57} - x^{39} + x^{19} + x^{13} + x^3 - x) \\ &= h(x) \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{12} \cdot \Phi_9 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x. \end{aligned}$$

Since $M_d(x)$ has rational coefficients, $\Phi_m(x)$ dividing $M_d(x)$ is equivalent to $M_d(\zeta_m) = 0$ for some primitive mth root of unity ζ_m. The plot below shows all pairs (d, m) with $1 \le d, m \le 1000$ such that $M_d(\zeta_m) = 0$.



This plot suggests that the preponderance of cyclotomic factors of $M_d(x)$ observed above is not isolated to special values of d, but rather that it occurs to some extent for all d. The primary objectives of this paper are to explain why necklace polynomials have so many cyclotomic factors and to characterize the pairs (d, m) of integers for which $M_d(\zeta_m) = 0$.

A strikingly similar phenomenon occurs for the seemingly unrelated sequence $\Phi_d(x) - 1$ of shifted cyclotomic polynomials. For example,

$$\begin{aligned}
\Phi_{105}(x) - 1 &= \widetilde{e}(x) \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \\
\Phi_{165}(x) - 1 &= \widetilde{f}(x) \cdot \Phi_{10} \cdot \Phi_5 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \\
\Phi_{231}(x) - 1 &= \widetilde{g}(x) \cdot \Phi_{12} \cdot \Phi_{10} \cdot \Phi_6 \cdot \Phi_5 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \\
\Phi_{741}(x) - 1 &= \widetilde{h}(x) \cdot \Phi_{18} \cdot \Phi_{12} \cdot \Phi_9 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x,
\end{aligned}$$

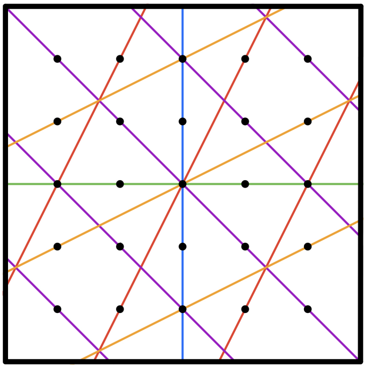
where $\widetilde{e}(x), \widetilde{f}(x), \widetilde{g}(x), \widetilde{h}(x) \in \mathbb{Z}[x]$ are irreducible, non-cyclotomic polynomials of degree 35, 67, 99, and 407, respectively. Note that $\Phi_m(x)$ dividing $\Phi_d(x) - 1$ is equivalent to $\Phi_d(\zeta_m) = 1$ for a primitive mth root of unity ζ_m.

Comparing the factorizations of $M_d(x)$ and $\Phi_d(x) - 1$ in the examples above we see there is a considerable overlap in their cyclotomic factors. The table below illustrates that this is a common occurrence. For each $2 \le d \le 43$, we list all m for which $\Phi_m(x)$ divides both $M_d(x)$ and $\Phi_d(x) - 1$ in plain text, and all m for which $\Phi_m(x)$ divides $M_d(x)$ but not $\Phi_d(x) - 1$ in bold. For d in this range, there are no m for which $\Phi_m(x)$ divides $\Phi_d(x) - 1$ but not $M_d(x)$; the first time this occurs is with $d = 231$ and $m = 4$.

The secondary objectives of this paper are to explain why this qualitatively similar cyclotomic factor phenomenon occurs for the shifted cyclotomic polynomials $\Phi_d(x) - 1$, explain how these factors are related to the factors of $M_d(x)$, and to characterize those pairs of integers (d, m) for which $\Phi_d(\zeta_m) = 1$.

d	m	d	m	d	m
2	$\mathbf{1}$	16	$\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{8}$	30	$1, 2, 4, \mathbf{6}$
3	$\mathbf{1}, 2$	17	$\mathbf{1}, 2, 4, 8, 16$	31	$\mathbf{1}, 2, 3, 5, 6, 10, 15, 30$
4	$\mathbf{1}, \mathbf{2}$	18	$1, \mathbf{2}, 3, \mathbf{6}$	32	$\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{8}, \mathbf{16}$
5	$\mathbf{1}, 2, 4$	19	$\mathbf{1}, 2, 3, 6, 9, 18$	33	$1, 2, 5, 10$
6	$1, \mathbf{2}$	20	$1, 2, \mathbf{4}, 8, \mathbf{12}$	34	$1, 2, 4, \mathbf{6}, 8, 16$
7	$\mathbf{1}, 2, 3, 6$	21	$1, 2, \mathbf{3}, 6, \mathbf{8}$	35	$1, 2, 3, 4, 6$
8	$\mathbf{1}, \mathbf{2}, \mathbf{4}$	22	$1, \mathbf{2}, 5, \mathbf{6}, 10$	36	$1, 2, 3, \mathbf{4}, 6, \mathbf{12}$
9	$\mathbf{1}, 2, \mathbf{3}, 6$	23	$\mathbf{1}, 2, 11, 22$	37	$\mathbf{1}, 2, 3, 4, 6, 9, 12, 18, 36$
10	$1, \mathbf{2}, 4, \mathbf{6}$	24	$1, 2, 4, \mathbf{8}$	38	$1, \mathbf{2}, 3, 6, 9, 18$
11	$\mathbf{1}, 2, 5, 10$	25	$\mathbf{1}, 2, 4, \mathbf{5}, 10, 20$	39	$1, 2, \mathbf{3}, 4, 6, 12$
12	$1, 2, \mathbf{4}$	26	$1, \mathbf{2}, 3, 4, 6, 12$	40	$1, 2, 4, \mathbf{8}, 16, \mathbf{24}$
13	$\mathbf{1}, 2, 3, 4, 6, 12$	27	$\mathbf{1}, 2, \mathbf{3}, 6, \mathbf{9}, 18$	41	$\mathbf{1}, 2, 4, 5, 8, 10, 20, 40$
14	$1, \mathbf{2}, 3, 6$	28	$1, 2, 3, \mathbf{4}, 6, 12$	42	$1, 2, 3, \mathbf{6}$
15	$1, 2, 4$	29	$\mathbf{1}, 2, 4, 7, 14, 28$	43	$\mathbf{1}, 2, 3, 6, 7, 14, 21, 42$

We explain the cyclotomic factors of necklace polynomials $M_d(x)$ and shifted cyclotomic polynomials $\Phi_d(x) - 1$ using the representation theory of finite abelian groups. We trace this phenomenon in both cases to a common source, which we call the *necklace operators*, and show how these operators account for the common cyclotomic factors of $M_d(x)$ and $\Phi_d(x) - 1$. Our analysis reveals a surprising connection between these unexpected cyclotomic factors and arrangements of hyperplanes in finite abelian groups. For example, we will explain how the arrangement of lines covering $\mathbb{Z}/(4) \times \mathbb{Z}/(4)$ pictured below corresponds to the fact that $M_d(\zeta_{65}) = 0$ and $\Phi_d(\zeta_{65}) = 1$ with $d = 9372603371$ (see Example 2.7).



Our terminology and explicit results are detailed in the following section.

1.1. Results. Our first result relates the identities $M_d(\zeta_m) = 0$ and $\Phi_d(\zeta_m) = 1$ and hyperplane arrangements in the group of Dirichlet characters of modulus m. Let $\mathcal{U}_m := (\mathbb{Z}/(m))^\times$ denote the multiplicative group of integers modulo m and let $\widehat{\mathcal{U}}_m := \mathrm{Hom}(\mathcal{U}_m, \mathbb{C}^\times)$ be the group of *Dirichlet characters of modulus* m. Each unit $q \in \mathcal{U}_m$ determines a homomorphism from $\widehat{\mathcal{U}}_m$ to $\mathbb{C}^\times$ by $\chi \mapsto \chi(q)$; let $\mathcal{H}_q \subseteq \widehat{\mathcal{U}}_m$ denote the kernel of this map. We call $\mathcal{H}_q$ the *hyperplane associated to* q,

$$\mathcal{H}_q := \{\chi \in \widehat{\mathcal{U}}_m : \chi(q) = 1\}.$$

Note that with a choice of coordinates for the group $\widehat{\mathcal{U}}_m$—by which we mean some isomorphism between $\widehat{\mathcal{U}}_m$ and a product of cyclic groups $\mathbb{Z}/(n)$—$\mathcal{H}_q$ may be expressed as the vanishing set of an integral linear form, hence the hyperplane terminology (see Remark 2.1).

Theorem 1.1. *Let $d, m > 1$ be coprime integers. If $\widehat{\mathcal{U}}_m \subseteq \bigcup_{p|d} \mathcal{H}_p$, then $x^m - 1$ divides $M_d(x)$ and $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$.*

In other words, if the group $\widehat{\mathcal{U}}_m$ of Dirichlet characters of modulus m is covered by the arrangement of hyperplanes $\{\mathcal{H}_p : p \mid d \text{ is prime}\}$, then $M_d(\zeta_m^k) = 0$ for all $k \geq 0$ and $\Phi_d(\zeta_m^k) = 1$ for all $k \not\equiv 0 \bmod m$.

Remark 1.2. Theorem 1.1 avoids addressing $\Phi_d(1)$, but it is well-known that $\Phi_d(1) = 1$ whenever d is divisible by at least two distinct primes and that $\Phi_{p^r}(1) = p$ for any prime p and $r \geq 1$.

Theorem 1.1 shows that hyperplane arrangements covering $\widehat{\mathcal{U}}_m$ provide one source of common cyclotomic factors of $M_d(x)$ and $\Phi_d(x) - 1$, and that these factors have the property that if $\Phi_m(x)$ is a factor, so is $\Phi_n(x)$ for all $n > 1$ dividing m. Theorem 1.1 empirically accounts for the majority of such common cyclotomic factors. For example, with $1 \leq d \leq 1000$, Theorem 1.1 accounts for all common cyclotomic factors of $M_d(x)$ and $\Phi_d(x) - 1$; for about 88.9% of the cyclotomic factors of $M_d(x)$; and for about 99.7% of the cyclotomic factors of $\Phi_d(x) - 1$.

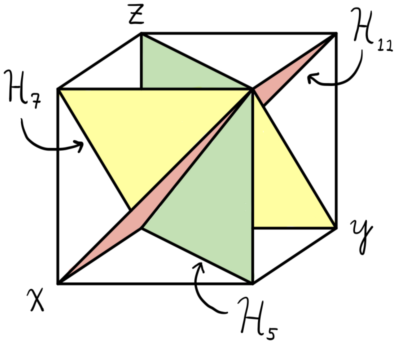
Example 1.3. We illustrate Theorem 1.1 in the case $m = 24$. The Dirichlet characters $\widehat{\mathcal{U}}_{24}$ form a 3-dimensional $\mathbb{F}_2$-vector space. Note that $\mathcal{U}_{24}$ is generated by 13, 17, and 19. Identifying $\mathcal{U}_{24}$ with the dual of $\widehat{\mathcal{U}}_{24}$ we can choose coordinates $\rho : \mathcal{U}_{24} \to \widehat{\mathbb{F}}_2^3$ such that $\rho(13) = x$, $\rho(17) = y$, and $\rho(19) = z$. The pencil of planes containing the line $\langle(1,1,1)\rangle$ covers all of $\mathbb{F}_2^3 \cong \widehat{\mathcal{U}}_{24}$ and consists of

$$\mathcal{H}_{13\cdot 17} : x + y = 0, \qquad \mathcal{H}_{13\cdot 19} : x + z = 0, \qquad \mathcal{H}_{17\cdot 19} : y + z = 0.$$

Since

$$13 \cdot 17 \equiv 5 \bmod 24, \qquad 13 \cdot 19 \equiv 7 \bmod 24, \qquad 17 \cdot 19 \equiv 11 \bmod 24,$$

it follows from Theorem 1.1 with $d = 385 = 5 \cdot 7 \cdot 11$ that $x^{24} - 1$ divides $M_{385}(x)$ and $\frac{x^{24}-1}{x-1}$ divides $\Phi_{385}(x) - 1$.



■

Example 1.4. Let $d, m \geq 1$ and suppose that d is divisible by some prime p such that $p \equiv 1 \bmod m$. In this case, $\mathcal{H}_p = \mathcal{H}_1 = \widehat{\mathcal{U}}_m$ is the degenerate hyperplane, namely the entire group (recall that $\mathcal{H}_d$ is the kernel of the evaluation map $\chi \mapsto \chi(d)$ for χ a Dirichlet character of modulus m). Hence the arrangement $\{\mathcal{H}_p \subseteq \widehat{\mathcal{U}}_m : p \,|\, d \text{ is prime}\}$ trivially covers $\widehat{\mathcal{U}}_m$. Thus Theorem 1.1 implies that $M_d(\zeta_m) = 0$ and $\Phi_d(\zeta_m) = 1$ whenever d is divisible by a prime p such that $p \equiv 1 \bmod m$. In particular, with d fixed, this holds for $m = p-1$ if $\gcd(d, p-1) = 1$. This explains why cyclotomic factors of $M_d(x)$ and $\Phi_d(x) - 1$ are so prevalent: each such prime p dividing d contributes a factor of $\frac{x^{p-1}-1}{x-1}$ to both polynomials. ■

Our second result highlights the structure of the pairs (d, m) with m fixed for which $M_d(\zeta_m) = 0$ or $\Phi_d(\zeta_m) = 1$.

Theorem 1.5. *Let $d, e, m \geq 1$.*

(1) *If $M_d(\zeta_m) = 0$ and e is coprime to m, then $M_{de}(\zeta_m) = 0$.*
(2) *If d and e are coprime to m and if we have an equality of sets of residue classes*

$$\{p \bmod m : p \,|\, d \text{ is prime}\} = \{q \bmod m : q \,|\, e \text{ is prime}\},$$

then $M_d(\zeta_m) = 0$ if and only if $M_e(\zeta_m) = 0$.

Likewise, both assertions hold with $M_d(\zeta_m) = 0$ replaced by $\Phi_d(\zeta_m) = 1$.

Theorem 1.6 characterizes the pairs (d, m) for which $M_d(\zeta_m) = 0$ or $\Phi_d(\zeta_m) = 1$, without the coprime restriction on d and m, in terms of hyperplane arrangements covering certain prescribed subsets of $\widehat{\mathcal{U}_m}$. First, some set-up. If n divides m, then there is a natural injective map $\widehat{\mathcal{U}_n} \to \widehat{\mathcal{U}_m}$ induced by the quotient $\mathcal{U}_m \to \mathcal{U}_n$. We use these maps to identify $\widehat{\mathcal{U}_n}$ with its image in $\widehat{\mathcal{U}_m}$ and say $\widehat{\mathcal{U}_n} \subseteq \widehat{\mathcal{U}_m}$. If $\chi \in \widehat{\mathcal{U}_m}$, then let c_χ be the smallest positive integer n such that $\chi \in \widehat{\mathcal{U}_n}$. Finally, let v_p denote the normalized p-adic valuation.

The precise statement of Theorem 1.6 is technical, but in essence it says that for integers $d, m \geq 1$, there is a subset $\Sigma = \Sigma_{d,m} \subseteq \widehat{\mathcal{U}_m}$ of Dirichlet characters of modulus m such that $M_d(\zeta_m) = 0$ if and only if Σ is covered by the union of hyperplanes $\mathcal{H}_p \subseteq \widehat{\mathcal{U}_m}$ for p a prime dividing d and not m. A similar conclusion holds characterizing the pairs (d, m) such that $\Phi_d(\zeta_m) = 1$, but with a couple of additional arithmetic conditions as well.

Theorem 1.6. *Let $d, e, f, m \geq 1$ be integers and let m' be the product of all primes p such that $v_p(m) = 1$. Suppose that*

(i) *def is squarefree,*
(ii) *d is coprime to m,*
(iii) *e divides m',*
(iv) *f divides m/m'.*

Then:

(1) *If $\Sigma_{f,m} \subseteq \widehat{\mathcal{U}_m}$ is the set of all characters χ such that*

   (a) *$v_p(c_\chi) = v_p(m)$ if $v_p(m) \geq 2$ and $v_p(f) = 0$, and*
   (b) *$v_p(c_\chi) \geq v_p(m) - 1$ if $v_p(m) > 2$ and $v_p(f) = 1$,*

then $M_{def}(\zeta_m) = 0$ *if and only if*

$$\Sigma_{f,m} \subseteq \begin{cases} \bigcup_{p\mid d} \mathcal{H}_p & \text{if } 2 \nmid e, \\ \bigcup_{p\mid d} \mathcal{H}_p \cup \mathcal{H}_2^a & \text{if } 2 \mid e, \end{cases}$$

where $\mathcal{H}_2^a \subseteq \widehat{\mathcal{U}}_m$ *is the affine hyperplane*

$$\mathcal{H}_2^a := \{\chi \in \widehat{\mathcal{U}}_m : \chi(2) = -1\}.$$

(2) *If* m *does not divide* def, *then* $\Phi_{def}(\zeta_m) = 1$ *if and only if*

(a) $\mathcal{H}_{-1} \subseteq \begin{cases} \bigcup_{p\mid md/e} \mathcal{H}_p & \text{if } 3 \nmid e, \\ \bigcup_{p\mid md/e} \mathcal{H}_p \cup \mathcal{H}_3^a & \text{if } 3 \mid e, \end{cases}$

where $\mathcal{H}_3^a \subseteq \widehat{\mathcal{U}}_m$ *is the affine hyperplane*

$$\mathcal{H}_3^a := \{\chi \in \widehat{\mathcal{U}}_m : \chi(3) = -1\},$$

(b) m *divides* $\varphi(def)$, *and*

(c) $\displaystyle\sum_{a\mid def} \lfloor a/m \rfloor \equiv \frac{\varphi(def)}{m} \bmod 2.$

Remark 1.7. We make several comments on Theorem 1.6.

(1) If $d \geq 1$, let d_0 be the product of all distinct primes dividing d and let $e = d/d_0$. Then $dM_d(\zeta_m) = d_0 M_{d_0}(\zeta_m^e)$ and $\Phi_d(\zeta_m) = \Phi_{d_0}(\zeta_m^e)$. Hence we lose no generality in Theorem 1.6 by assuming that def is squarefree.

(2) If $\chi \in \widehat{\mathcal{U}}_m$ is a character, then a common convention is to set $\chi(d) = 0$ whenever d is not coprime to m. Our identification of $\widehat{\mathcal{U}}_n$ with its image in $\widehat{\mathcal{U}}_m$ induced by the quotient map $\mathcal{U}_m \to \mathcal{U}_n$ whenever n divides m suggests a slight natural variant on this convention which we find convenient: If $\chi \in \widehat{\mathcal{U}}_m$ has conductor n and $d \in \mathbb{Z}$, then we set $\chi(d) = 0$ if d is not coprime to n and otherwise set $\chi(d)$ to its non-zero value on the residue class of d modulo n. In particular, the characters on the affine hyperplane $\mathcal{H}_2^a$ defined in Theorem 1.6 must all have conductor dividing $m/2$. See Caution 2.2.

Example 1.8. Theorem 1.6 allows us to account for the cyclotomic factors of $M_d(x)$ not explained by Theorem 1.1. For example, let $m = 8$ and let $e = f = 1$. If d is odd, then Theorem 1.6 implies that $M_d(\zeta_8) = 0$ if and only if

$$\Sigma_{1,8} \subseteq \bigcup_{p\mid d} \mathcal{H}_p.$$

where $\Sigma_{1,8} \subseteq \widehat{\mathcal{U}}_8$ is the set of all characters χ such that $v_2(c_\chi) = 3$, which is to say, $c_\chi = 8$. There are two such characters χ determined by $\chi(3) = \pm 1$ and $\chi(5) = -1$. Hence if $\chi \in \Sigma_{1,8}$, then either $\chi(3) = 1$, or $\chi(3) = -1$ and

$$\chi(7) = \chi(3)\chi(5) = (-1)^2 = 1.$$

Equivalently, $\Sigma_{1,8} \subseteq \mathcal{H}_3 \cup \mathcal{H}_7$.Therefore $M_{21}(\zeta_8) = 0$.

In fact, $M_{21}(x)$ factors as

$$M_{21}(x) = f(x) \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x,$$

where $f(x)$ is irreducible and not cyclotomic. Note that $\Phi_8(x)$ divides $M_{21}(x)$, but $\Phi_4(x)$ does not. This reflects the fact that $\mathcal{H}_3 \cup \mathcal{H}_7$ covers $\Sigma_{1,8}$ but not $\Sigma_{1,4}$, which consists of the character χ such that $\chi(3) = \chi(7) = -1$ and $\chi(5) = 1$. ■

Example 1.9. If $m = 6$, then $\widehat{\mathcal{U}}_6 = \{1, \chi\}$ contains only two characters. The non-trivial character χ has $c_\chi = 3$ and satisfies $\chi(2) = -1$. Thus the affine hyperplane $\mathcal{H}_2^a = \{\chi\}$ consists of the one non-trivial character. Therefore $\bigcup_{p|d} \mathcal{H}_p \cup \mathcal{H}_2^a$ covers $\widehat{\mathcal{U}}_6$ for any $d > 1$ coprime to 6. Theorem 1.6 implies that $M_{2d}(\zeta_6) = 0$ for all d coprime to 6. For example, this explains the $\Phi_6(x)$ factor in $M_{10}(x)$:

$$M_{10}(x) = g(x) \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x,$$

where $g(x) = \frac{1}{10}(x^3 + x^2 - 1)$ is irreducible and not cyclotomic. ■

1.1.1. *Necklace operators.* The connection between the necklace and shifted cyclotomic polynomials traces back to what we call the *necklace operators* φ_d. Let $\mathbb{N}^\circ$ denote the multiplicative semigroup of natural numbers, and let $\mathbb{Z}[\mathbb{N}^\circ]$ be the integral semigroup ring comprised of all integral linear combinations of formal expressions $[m]$ with $m \in \mathbb{N}$ subject only to the relations $[m][n] = [mn]$. The *dth necklace operator* is defined by

$$\varphi_d := \sum_{e|d} \mu(e)[d/e] \in \mathbb{Z}[\mathbb{N}^\circ].$$

The polynomial ring $\mathbb{Q}[x]$ carries a $\mathbb{Z}[\mathbb{N}^\circ]$-module structure where $\alpha = \sum_m a_m[m] \in \mathbb{Z}[\mathbb{N}^\circ]$ acts on $f(x) \in \mathbb{Q}[x]$ by

$$\alpha f(x) := \sum_m a_m f(x^m).$$

Similarly, the non-zero rational functions $\mathbb{Q}(x)^\times$ have a multiplicative action of $\mathbb{Z}[\mathbb{N}^\circ]$ defined on $g(x) \in \mathbb{Q}(x)^\times$ by

$$g(x)^\alpha := \prod_m g(x^m)^{a_m}.$$

With respect to these module structures we have the following expressions for necklace and cyclotomic polynomials in terms of the necklace operator:

$$M_d(x) = \frac{1}{d}\sum_{e|d} \mu(e) x^{d/e} = \frac{1}{d}\sum_{e|d} \mu(e)[d/e]x = \frac{\varphi_d x}{d},$$

$$\Phi_d(x) = \prod_{e|d} (x^{d/e} - 1)^{\mu(e)} = \prod_{e|d} (x-1)^{\mu(e)[d/e]} = (x-1)^{\varphi_d}.$$

In Section 2 we show how the abundance of pairs (d, m) for which $M_d(\zeta_m) = 0$ or $\Phi_d(\zeta_m) = 1$ is ultimately a consequence of the elementary observation that the dth necklace operator has the following factorization in $\mathbb{Z}[\mathbb{N}^\circ]$:

$$\varphi_d = \prod_p [p^{m_p - 1}]([p] - 1) = [d] \prod_{p \mid d} (1 - [p]^{-1}), \tag{1.2}$$

where $d = \prod_p p^{m_p}$ is the prime factorization of d.

If d is coprime to m, then φ_d determines an element of the group ring $\mathbb{Z}[\mathcal{U}_m]$. Hence if v is a vector in a linear $\mathcal{U}_m$-representation V, then $\varphi_d v \in V$. Our analysis of the identities $M_d(\zeta_m) = 0$ and $\Phi_d(\zeta_m) = 1$ hinges on the following result.

THEOREM 1.10. *Let $d, m \geq 1$ be coprime integers and suppose $v \in V$ is an element of a $\mathbb{Q}[\mathcal{U}_m]$-module. Let Σ_v denote the set of Dirichlet characters that occur in the irreducible decomposition of the cyclic $\mathcal{U}_m$-representation generated by v. Then in $\mathbb{C} \otimes V$ we have*

$$\varphi_d v = \sum_{\chi \in \Sigma_v} \chi(d) \prod_{p \mid d} (1 - \overline{\chi(p)}) v_\chi,$$

where v_χ is the χ-isotypic component of the vector v. Thus $\varphi_d v = 0$ if and only if $\Sigma_v \subseteq \bigcup_{p \mid d} \mathcal{H}_p$.

1.2. Related work. As noted above, necklace polynomials have many interpretations. Gauss [10, p. 611] wrote down the necklace polynomials evaluated at a prime p to count irreducible polynomials over $\mathbb{F}_p$ of a prescribed degree, and Schönemann [23, Sec. 48, pp. 319–320] later independently rediscovered this formula. This interpretation accounts for the appearance of necklace polynomials in the Euler product formula for the Hasse–Weil zeta function of the affine line over $\mathbb{F}_q$,

$$\zeta_{\mathbb{A}^1(\mathbb{F}_q)}(t) = \frac{1}{1 - qt} = \prod_{d \geq 1} \left(\frac{1}{1 - t^d} \right)^{M_d(q)}.$$

Necklace polynomials often appear in connection with Euler products. See, for example, Moree [20] and Ettahri, Ramaré, Surel [9], in which the traces of necklace polynomials evaluated at algebraic numbers arise in the study of fast numerical evaluations of Euler products.

The name "necklace polynomial" comes from the combinatorial interpretation of $M_d(k)$ as counting the number of aperiodic necklaces of d beads chosen from among k colors, which Metropolis and Rota [18, p. 95] attribute to the French colonel Moreau; the M in the notation is presumably in his honor. Necklace polynomials also count Lyndon words [2, Sec. 4.2] and the number of periodic orbits of a prescribed length for a generic polynomial of fixed degree [25, Rmk. 4.3]. Metropolis and Rota [18] use necklace polynomials to construct a combinatorial model of the ring of big Witt vectors.

When $g \geq 1$ is an integer, Witt [27, Satz 3] showed that $M_d(g)$ is the dimension of the degree d homogeneous component of the free Lie algebra on g generators. In this context the explicit expression for $M_d(x)$ as a divisor sum is sometimes called Witt's formula [2, p. 1005]. Reutenauer [22, Thm. 4.9, Thm. 5.1] gave a combinatorial proof of this result by constructing an explicit basis for the free Lie algebra from Lyndon words.

Let $\mathrm{PConf}_d(\mathbb{R}^n)$ denote the space of labeled configurations of d distinct points in $\mathbb{R}^n$. The symmetric group S_d acts naturally on this space by permuting labels and this action endows the cohomology $H^*(\mathrm{PConf}_d(\mathbb{R}^n), \mathbb{Q})$ with the structure of an S_d-representation. The character values of these representations are determined by necklace polynomials. See Hyde [13].

In [14], we show that $M_d(1) = \chi_c(\mathrm{Irr}_d(\mathbb{C}))$ and $M_d(-1) = \chi_c(\mathrm{Irr}_d(\mathbb{R}))$, where χ_c is the compactly supported Euler characteristic and $\mathrm{Irr}_d(K)$ is the space of monic, K-irreducible polynomials in $K[x]$ of degree d. In these cases the fundamental theorem of algebra gives a higher level explanation for why $M_d(\pm 1) = 0$ for nearly all d. It would be interesting to find a more conceptual interpretation of the vanishing of $M_d(\zeta_m)$ for $m > 2$, but we are unaware of one at this time.

The Euler characteristic interpretation of $M_d(\pm 1)$ found in [14] extends to the family $M_{d,n}(x)$ of *higher necklace polynomials* introduced by the author in [12] to enumerate the irreducible polynomials over $\mathbb{F}_q$ in $n$variables. Theorem 1.5 in [14] shows that $M_{d,n}(\zeta_p) = 0$ for certain primes p depending on n and nearly all d. However, for $n > 1$, the qualitative behavior of these cyclotomic factors differs from those of $M_d(x)$ and $\Phi_d(x) - 1$, thus we expect the cyclotomic factors of $M_{d,n}(x)$ with $n > 1$ arise for a fundamentally different reason.

Despite the long history of necklace polynomials, the observation of their abundance of cyclotomic factors appears to be new.

The identity $\Phi_d(\zeta_m) = 1$ has received more attention. Note that if $\Phi_d(\zeta_m) = 1$, then

$$1 = \Phi_d(\zeta_m) = \prod_{\gcd(j,d)=1} (\zeta_m - \zeta_d^j). \tag{1.3}$$

Algebraic integral units of the form $\zeta_m - \zeta_n$ are called *cyclotomic units.* Thus (1.3) may be interpreted as a multiplicative relation between cyclotomic units. Such multiplicative relations are of interest in number theory and algebraic K-theory; they have been studied by Bass [1], Conrad [6], Ennola [8], Ramachandra [21], and others. This previous work focuses primarily on finding explicit relations that generate all of the relations amongst the cyclotomic units; our results provide a natural way of generating such relations through the construction of arrangements in $\widehat{\mathcal{U}}_m$ covering a prescribed set.

There is also some literature on classifying the vanishing integral linear combinations of roots of unity of which $M_d(\zeta_m) = 0$ and $\Phi_d(\zeta_m) - 1 = 0$ provide examples. See Christie, Dykema, Klep [5] for a recent reference along with a survey of the previous work on this problem.

Kurshan and Odlyzko [16, 17] made a detailed study of the unit part of $\Phi_d(\zeta_m)$ which included analyzing situations where $\Phi_d(\zeta_m) = 1$. Their work was motivated by problems related to the design of recursive linear digital filters. Our Theorem 1.6(2), characterizing solutions of $\Phi_d(\zeta_m) = 1$, is substantively equivalent to a result they proved in [17]. This can be seen most clearly in their discussion following Proposition 3.4 where they express the condition of $\mathcal{H}_{-1}$ being covered by hyperplanes as a disjunction of conditions on a character χ such that $\chi(-1) = 1$.

For their application, Kurshan and Odlyzko focus on analyzing the case $\Phi_{pm}(\zeta_m)$ with p a prime not dividing m. This case is not covered by Theorem 1.6(2) since we assume that m does not divide def.

Through his study of base b expansions of reciprocal primes $1/p$, Caldwell [4] observed that $\Phi_d(x)-1$ often has an abundance of cyclotomic factors. Caldwell's Theorem 1 gives the necessary condition we state as Theorem 1.6(2b). His Theorems 2, 4, 5 and Corollary 3 gives several sufficient conditions which, from our combinatorial geometry perspective, are equivalent to parametrizing families of hyperplane arrangements in $\widehat{\mathcal{U}}_m$ meeting the conditions in Theorem 1.6(2). As the number of distinct primes dividing d increases, so does the number and complexity of possible arrangements corresponding to cyclotomic factors of $\Phi_d(x) - 1$, hence it will not be possible to find a finite list of such families which account for all $\Phi_m(x)$ dividing $\Phi_d(x) - 1$.

The expression for $\varphi_d v$ given by Theorem 2.5 below generalizes a result of Bzdęga, Herrera-Poyatos, Moree [3, Thm. 1] which is the specialization to the case $v = \zeta_m - 1$ in the $\mathbb{Q}$-linearization of $V = \mathbb{Q}(\zeta_m)^\times$. They use this formula to explicitly evaluate $\Phi_d(\zeta_m)$ for small fixed values of m as a function of d, which in turn they apply to give a new proof of a result of Vaughan on the heights of cyclotomic polynomials.

If $f(x) \in K[x]$ is a polynomial with coefficients in a field K, then the *dth dynatomic polynomial* of f is defined by the product

$$\Phi_{f,d}(x) := \prod_{e|d} (f^e(x) - x)^{\mu(d/e)}, \tag{1.4}$$

where $f^n(x)$ denotes the n-fold iterated composition of $f(x)$ with itself. Recently Doyle, Fili, and Hyde [7] discovered a connection between cyclotomic factors of necklace polynomials and dynatomic factors $\Phi_{f,m}(x)$ of $\Phi_{f,d}(x)-1$.

This connection also arises via the necklace operator φ_d, traces of which can be seen in (1.4).

An earlier version of this paper appeared in the author's dissertation [11, Chp. 4].

1.3. Organization. In Section 2 we develop the theory of the necklace operators and prove Theorem 1.10 as Theorem 2.5, from which we then deduce Theorem 1.1 as Corollary 2.6 and Theorem 1.5 as Corollary 2.8. The first part of Theorems 1.6 is proved in Section 3 as Theorem 3.3 and the second part is proved in Section 4 as Theorem 4.6.

2. Necklace operators. We briefly review the representation theory of finite abelian groups—see Serre [24] for more background. Given a finite (multiplicative) abelian group $\mathcal{U}$, let $\widehat{\mathcal{U}}$ denote the dual group or group of characters $\chi : \mathcal{U} \to \mathbb{C}^\times$. The groups $\mathcal{U}$ and $\widehat{\mathcal{U}}$ are non-canonically isomorphic. Each character $\chi \in \widehat{\mathcal{U}}$ extends linearly to a ring homomorphism $\chi : \mathbb{Z}[\mathcal{U}] \to \mathbb{C}$. If χ_i for $1 \leq i \leq n$ are the distinct characters of $\mathcal{U}$, then the map $\mathbb{Z}[\mathcal{U}] \to \mathbb{C}^n$ given by

$$\alpha \in \mathbb{Z}[\mathcal{U}] \mapsto (\chi_1(\alpha), \ldots, \chi_n(\alpha)) \in \mathbb{C}^n$$

is an embedding of rings. Hence $\alpha \in \mathbb{Z}[\mathcal{U}]$ is zero if and only if $\chi(\alpha) = 0$ for all $\chi \in \widehat{\mathcal{U}}$. A *hyperplane* $\mathcal{H} \subseteq \widehat{\mathcal{U}}$ is defined to be the (multiplicative) kernel of a character of $\widehat{\mathcal{U}}$. The group $\mathcal{U}$ is canonically isomorphic to the dual of $\widehat{\mathcal{U}}$. In particular, if $q \in \mathcal{U}$, then the hyperplane associated to q is

$$\mathcal{H}_q := \ker(q) = \{\chi \in \widehat{\mathcal{U}} : \chi(q) = 1\}.$$

If $q = 1$ is the identity, then $\mathcal{H}_1 = \widehat{\mathcal{U}}$ is the *trivial hyperplane*. If $q \neq 1$, then $\mathcal{H}_q$ is a proper subgroup of $\widehat{\mathcal{U}}$.

Remark 2.1. While we are primarily interested in multiplicative groups of units, the geometric terminology is best understood from an additive perspective. Suppose $\widehat{\mathcal{U}} \cong \mathbb{F}_p^n$ is an n-dimensional vector space over a finite field $\mathbb{F}_p$. If we choose some isomorphism of the pth roots of unity with the additive group of the field $\mathbb{F}_p$, then a character $q : \widehat{\mathcal{U}} \to \mathbb{C}^\times$ of $\widehat{\mathcal{U}}$ is equivalent under this isomorphism to an $\mathbb{F}_p$-linear map $q : \mathbb{F}_p^n \to \mathbb{F}_p$. Thus there is a homogeneous linear form

$$h_q := \sum_{i=1}^{n} a_i x_i$$

with $\mathbb{F}_p$-coefficients such that the hyperplane $\mathcal{H}_q$ is precisely the set of solutions $h_q(x) = 0$ in $\mathbb{F}_p^n$.

Let $\mathcal{U}_m$ denote the group of units modulo m,

$$\mathcal{U}_m := (\mathbb{Z}/(m))^\times.$$

The elements of $\widehat{\mathcal{U}}_m$ are called *Dirichlet characters of modulus* m. If n divides m, then the quotient map $\mathcal{U}_m \to \mathcal{U}_n$ induces an injective map $\widehat{\mathcal{U}}_n \to \widehat{\mathcal{U}}_m$. Identifying $\widehat{\mathcal{U}}_n$ with its image under this map we say $\widehat{\mathcal{U}}_n \subseteq \widehat{\mathcal{U}}_m$. If a character $\chi \in \widehat{\mathcal{U}}_m$ belongs to the subset $\widehat{\mathcal{U}}_n$, then we say χ has *modulus* n. If χ has modulus n, then the values $\chi(k)$ depend only on k modulo n. Note that if χ has modulus n, it also has modulus m for all multiples m of n. The smallest n for which $\chi \in \widehat{\mathcal{U}}_m$ has modulus n is called the *conductor* of χ and denoted c_χ.

Caution 2.2. A common convention in number theory is to distinguish a character $\chi \in \widehat{\mathcal{U}}_n$ from the character it naturally induces in $\widehat{\mathcal{U}}_m$ when $n \mid m$. In particular, the convention is to set $\chi(d) = 0$ for all non-trivial $\chi \in \widehat{\mathcal{U}}_m$ when d is not coprime to m. Since we are identifying $\widehat{\mathcal{U}}_n$ with a subset of $\widehat{\mathcal{U}}_m$ whenever n divides m, we use a slight natural variation on this convention: If $d \in \mathbb{Z}$ and $\chi \in \widehat{\mathcal{U}}_m$ has conductor n, then we set $\chi(d) = 0$ if d is not coprime to n and otherwise set $\chi(d)$ to be the well-defined, non-zero value of χ on the residue class of d modulo n. This gives each character χ a consistent value independent of which group $\widehat{\mathcal{U}}_m$ it is considered to be an element of.

To illustrate, let $m = 10$. Note that $\widehat{\mathcal{U}}_{10} = \widehat{\mathcal{U}}_5$. If $\chi \in \widehat{\mathcal{U}}_{10}$, then the common convention is to say that $\chi(2) = 0$ since 2 divides 10. However, χ has conductor 5 and as an element of $\widehat{\mathcal{U}}_5$ it has a well-defined non-zero value at 2 which we take to be the value of $\chi(2)$.

This convention will prove to be a useful simplification throughout the paper.

If R is a semiring, we let R° denote the multiplicative semigroup of R. Let $\mathbb{Z}[\mathbb{N}^\circ]$ denote the ring generated by the expressions $[m]$ with $m \in \mathbb{N}$ subject to the relations $[m][n] = [mn]$. We define the *dth necklace operator* for $d \geq 1$ to be the element $\varphi_d \in \mathbb{Z}[\mathbb{N}^\circ]$ defined by

$$\varphi_d := \sum_{e|d} \mu(e)[d/e].$$

Remark 2.3. The map $[n] \mapsto n$ determines a ring homomorphism $\mathbb{Z}[\mathbb{N}^\circ] \to \mathbb{Z}$ such that

$$\varphi_d \mapsto \sum_{e|d} \mu(e)(d/e) = \varphi(d),$$

where $\varphi(d)$ is the *Euler totient function*, hence our choice of notation.

Necklace polynomials and cyclotomic polynomials are connected through the necklace operator. Recall from the introduction that with respect to the natural additive and multiplicative actions of $\mathbb{Z}[\mathbb{N}^\circ]$ on $\mathbb{Q}[x]$ and $\mathbb{Q}(x)^\times$, respectively, we have

$$M_d(x) = \frac{\varphi_d x}{d}, \quad \Phi_d(x) = (x-1)^{\varphi_d}.$$

The map $[n]\mapsto[n \bmod m]$ induces a ring homomorphism $\mathbb{Z}[\mathbb{N}^\circ]\to\mathbb{Z}[\mathbb{Z}/(m)^\circ]$. If d is coprime to m, then the image of φ_d under this map belongs to the subring $\mathbb{Z}[\mathcal{U}_m]$. The image of φ_d in $\mathbb{Z}[\mathcal{U}_m]$ factors as

$$\varphi_d = [d]\prod_{p\mid d}(1-[p]^{-1}). \tag{2.1}$$

The factorization (2.1) is equivalent to families of functional identities satisfied by $M_d(x)$ and $\Phi_d(x)$: if p is a prime and $d\ge 1$, then

$$M_{dp}(x)=\begin{cases}\frac{1}{p}(M_d(x^p)-M_d(x)) & p\nmid d,\\ \frac{1}{p}M_d(x^p) & p\mid d,\end{cases}\qquad \Phi_{dp}(x)=\begin{cases}\Phi_d(x^p)/\Phi_d(x) & p\nmid d,\\ \Phi_d(x^p) & p\mid d.\end{cases}$$

The identities for necklace polynomials were observed and given combinatorial interpretations by Metropolis and Rota [18]; the identities for cyclotomic polynomials are well-known.

Remark 2.4. Let d_0 be the product of all distinct primes dividing d. Thus (2.1) implies that $\varphi_d=[d/d_0]\varphi_{d_0}$, hence

$$dM_d(x)=d_0M_{d_0}(x^{d/d_0}),\qquad \Phi_d(x)=\Phi_{d_0}(x^{d/d_0}). \tag{2.2}$$

We use (2.2) to reduce the analysis of $M_d(\zeta_m)$ and $\Phi_d(\zeta_m)$ to the case where d is squarefree.

Let $\mathbb{C}[\mathcal{U}_m]$ denote the group algebra of $\mathcal{U}_m$ over $\mathbb{C}$. If $\chi\in\widehat{\mathcal{U}}_m$ is a character, let $e_\chi\in\mathbb{C}[\mathcal{U}_m]$ denote the corresponding idempotent,

$$e_\chi := \frac{1}{\varphi(m)}\sum_{q\in\mathcal{U}_m}\overline{\chi(q)}[q].$$

We write $v_\chi := e_\chi v$ for the projection of a vector $v\in V$ onto the χ-isotypic component of V. Then

$$v=\sum_{\chi\in\widehat{\mathcal{U}}_m} v_\chi.$$

The *support* of v is the set $\Sigma_v\subseteq\widehat{\mathcal{U}}_m$ of characters χ such that $v_\chi\neq 0$. In particular, $v=0$ if and only if $\Sigma_v=\emptyset$.

Theorem 2.5. *Let $d,m\ge 1$ be coprime integers, let V be a $\mathbb{Q}[\mathcal{U}_m]$-module, and let $v\in V$ be an element with support Σ_v. Then $\varphi_d v$ has the following expression in $\mathbb{C}\otimes V$:*

$$\varphi_d v=\sum_{\chi\in\Sigma_v}\chi(d)\prod_{p\mid d}(1-\overline{\chi(p)})v_\chi.$$

Thus $\varphi_d v=0$ if and only if $\Sigma_v\subseteq\bigcup_{p\mid d}\mathcal{H}_p$. In particular, $\varphi_d=0$ in $\mathbb{Q}[\mathcal{U}_m]$ if and only if $\widehat{\mathcal{U}}_m\subseteq\bigcup_{p\mid d}\mathcal{H}_p$.

Proof. If $\alpha \in \mathbb{C}[\mathcal{U}_m]$ and e_χ is the idempotent associated to a character χ, then $\alpha e_\chi = \chi(\alpha)e_\chi$. Hence

$$\begin{aligned}\varphi_d v &= \sum_{\chi\in\Sigma_v} \varphi_d e_\chi v = \sum_{\chi\in\Sigma_v} \chi(\varphi_d) v_\chi \\ &= \sum_{\chi\in\Sigma_v} \chi(d) \prod_{p\mid d} (1-\overline{\chi(p)}) v_\chi\end{aligned} \tag{2.3}$$

where the final equality follows from (2.1). The factor $1-\overline{\chi(p)}$ vanishes precisely when $\chi \in \mathcal{H}_p$, thus the support of $\varphi_d v$ is $\Sigma_v \setminus \bigcup_{p\mid d}\mathcal{H}_p$. Therefore $\varphi_d v = 0$ if and only if $\Sigma_v \setminus \bigcup_{p\mid d}\mathcal{H}_p = \emptyset$, which is to say, $\Sigma_v \subseteq \bigcup_{p\mid d}\mathcal{H}_p$. Since $\mathbb{Q}[\mathcal{U}_m]$ is cyclic as a module over itself generated by 1, $\Sigma_1 = \widehat{\mathcal{U}}_m$ and it follows that $\varphi_d = \varphi_d 1 = 0$ if and only if $\widehat{\mathcal{U}}_m \subseteq \bigcup_{p\mid d}\mathcal{H}_p$. ■

Theorem 2.5 gives us the following simple sufficient condition for both of the identities $M_d(\zeta_m) = 0$ and $\Phi_d(\zeta_m) = 1$ to hold simultaneously.

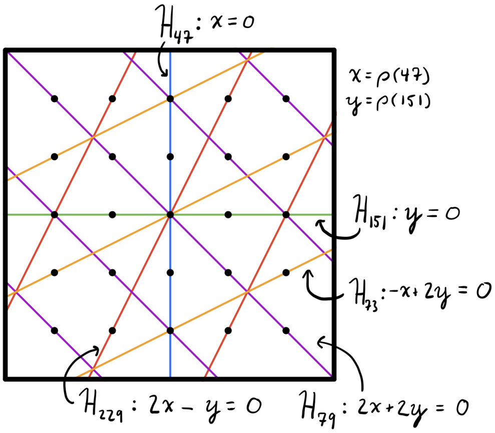
COROLLARY 2.6. *Let $d, m > 1$ be coprime integers. If $\widehat{\mathcal{U}}_m \subseteq \bigcup_{p\mid d}\mathcal{H}_p$, then $x^m - 1$ divides $M_d(x)$ and $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$.*

Proof. If $\widehat{\mathcal{U}}_m \subseteq \bigcup_{p\mid d}\mathcal{H}_p$, then $\varphi_d = 0$ by Theorem 2.5. Thus,

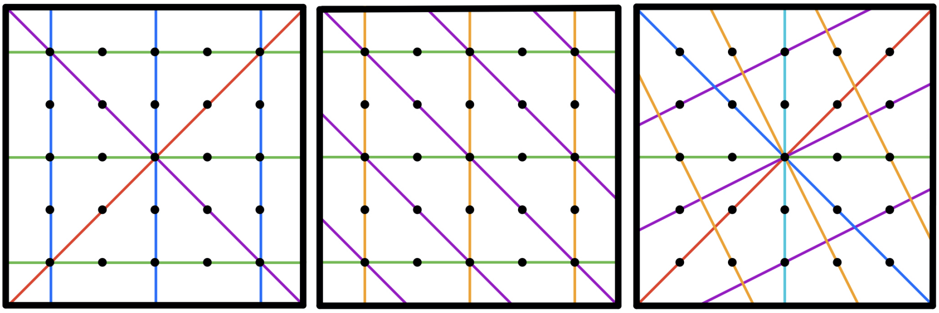
$$M_d(\zeta_m^k) = \frac{\varphi_d \zeta_m^k}{d} = 0, \qquad \Phi_d(\zeta_m^k) = (\zeta_m^k - 1)^{\varphi_d} = 1.$$

The first identity holds for all $k \geq 0$, but in the second identity we need $k \not\equiv 0 \bmod m$ in order to have $\zeta_m^k - 1 \in \mathbb{Q}(\zeta_m)^\times$. Hence $x^m - 1$ divides $M_d(x)$ and $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$. ■

EXAMPLE 2.7. Let $m = 65$ and $d = 9372603371 = 47 \cdot 73 \cdot 79 \cdot 151 \cdot 229$. The group $\widehat{\mathcal{U}}_{65}$ decomposes as $\widehat{\mathcal{U}}_{65} \cong \mathbb{Z}/(4)^2 \times \mathbb{Z}/(3)$, so each hyperplane $\mathcal{H}_p$ factors as $\mathcal{H}_p \cong \mathcal{H}_p^{(4)} \times \mathcal{H}_p^{(3)}$ with $\mathcal{H}_p^{(4)} \subseteq \mathbb{Z}/(4)^2$ and $\mathcal{H}_p^{(3)} \subseteq \mathbb{Z}/(3)$. In this case, each of the hyperplanes $\mathcal{H}_p$ with $p \mid d$ is trivial in the 3-component $\mathcal{H}_p^{(3)} = \mathbb{Z}/(3)$. Thus we can visualize the hyperplanes $\mathcal{H}_p$ via their 4-component $\mathcal{H}_p^{(4)}$ as lines in the “plane” $\mathbb{Z}/(4)^2$. Each of the five primes dividing d corresponds to a different colored line in the diagram below with respect to the choice of coordinates $x = \rho(47)$ and $y = \rho(151)$. Since the five lines $\mathcal{H}_p$ with $p \mid d$ cover all of $\widehat{\mathcal{U}}_{65}$, Corollary 2.6 implies that $M_d(\zeta_{65}^k) = 0$ for all $k \geq 0$ and $\Phi_d(\zeta_{65}^k) = 1$ for all $k \not\equiv 0$ mod 65.


$\mathcal{H}_{47} : x = 0$
$x = \rho(47)$
$y = \rho(151)$
$\mathcal{H}_{151} : y = 0$
$\mathcal{H}_{73} : -x + 2y = 0$
$\mathcal{H}_{229} : 2x - y = 0$
$\mathcal{H}_{79} : 2x + 2y = 0$

By drawing other arrangements of lines covering $\mathbb{Z}/(4)^2$ and then finding primes in the corresponding congruence classes modulo 65 (which exist by Dirichlet's theorem on primes in arithmetic progressions) we can construct several other non-trivial examples of d with $M_d(\zeta_{65}) = 0$ and $\Phi_d(\zeta_{65}) = 1$.



Example values of d for each of these arrangements are, respectively,

$$d_1 = 157 \cdot 181 \cdot 337 \cdot 389,$$
$$d_2 = 79 \cdot 181 \cdot 389,$$
$$d_3 = 47 \cdot 109 \cdot 151 \cdot 157 \cdot 317 \cdot 337. \blacksquare$$

The following corollary of Theorem 2.5 proves Theorem 1.5 from the introduction.

Corollary 2.8. *Let $d, e, m \geq 1$ be integers and let $v \in V$ be an element of a $\mathbb{Q}[\mathcal{U}_m]$-module V.*

(1) *If $\varphi_d v = 0$ and e is coprime to m, then $\varphi_{de} v = 0$.*
(2) *If d and e are coprime to m and*

$$\{p \bmod m : p \,|\, d \text{ is prime}\} = \{q \bmod m : q \,|\, e \text{ is prime}\}, \tag{2.4}$$

then $\varphi_d v = 0$ if and only if $\varphi_e v = 0$.

In particular, if $V = \mathbb{Q}(\zeta_m)$ and $v = \zeta_m$, or if $m > 1$, $V = \mathbb{Q} \otimes \mathbb{Q}(\zeta_m)^\times$, and $v = \zeta_m - 1$, then (1) *and* (2) *hold with $\varphi_d v = M_d(\zeta_m)$ and $\varphi_d v = \varPhi_d(\zeta_m)$, respectively.*

Proof. (1) The product formula (2.1) for the necklace operator implies that φ_d divides φ_{de} in $\mathbb{Z}[\mathbb{N}^\circ]$ and the assumption that e is coprime to m implies that $\varphi_{de}/\varphi_d \in \mathbb{Z}[\mathcal{U}_m]$. Thus,

$$\varphi_{de} v = (\varphi_{de}/\varphi_d)(\varphi_d v) = (\varphi_{de}/\varphi_d)0 = 0.$$

(2) Theorem 2.5 implies that $\varphi_d v = 0$ if and only if $\varSigma_v \subseteq \bigcup_{p|d} \mathcal{H}_p$, where $\varSigma_v$ is the support of v. The hyperplane $\mathcal{H}_p \subseteq \widehat{\mathcal{U}}_m$ depends only on the residue class $p \bmod m$. In other words, the equality in (2.4) is equivalent to $\bigcup_{p|d} \mathcal{H}_p = \bigcup_{q|e} \mathcal{H}_q$. Thus, (2.4) implies $\varphi_d v = 0$ if and only if $\varphi_e v = 0$. ∎

Remark 2.9. A quick computation shows that $M_{10}(\zeta_6) = 0$ but $M_{20}(\zeta_6) \neq 0$. This example shows that the assumption that e is coprime to m is necessary in Corollary 2.8(1).

3. Cyclotomic factors of $M_d(x)$.

In this section we characterize those pairs (d, m) for which $M_d(\zeta_m) = 0$ in terms of an explicit set of Dirichlet characters being covered by an arrangement of hyperplanes. If d is coprime to m, this reduces to determining the support of $\zeta_m \in \mathbb{Q}(\zeta_m)$ by Theorem 2.5. When d and m are not coprime, the situation becomes more complicated and the relevant support depends in a subtle way on the common factors of d and m.

If m is a positive integer, then the *squarefree part* of m, denoted m', is the product of all primes that divide m exactly once. We say a character $\chi \in \widehat{\mathcal{U}}_m$ is *supportive* if m/m' divides the conductor c_χ of χ. Equivalently, χ is supportive if and only if

$$v_p(c_\chi) = v_p(m) \quad \text{for all primes } p \text{ such that } v_p(m) \geq 2. \tag{3.1}$$

Let $\widehat{\mathcal{U}}_m^* \subseteq \widehat{\mathcal{U}}_m$ denote the subset of all supportive characters.

Proposition 3.1. *Let $m \geq 1$ be an integer and let $\chi \in \widehat{\mathcal{U}}_m$ be a character of modulus m. Then χ is in the support of $\zeta_m \in \mathbb{Q}(\zeta_m)$ if and only if χ is supportive.*

Proof. If $m = \prod_p p^{m_p}$ is the prime factorization of m and $\chi \in \widehat{\mathcal{U}}_m$ is a character, then by the Chinese Remainder Theorem there are factorizations

$$\zeta_m = \prod_p \zeta_{p^{m_p}}^{a_p}, \qquad \chi = \prod_p \chi_{p^{m_p}},$$

where $a_p \in \mathcal{U}_{p^{m_p}}$ is a unit and $\chi_{p^{m_p}} \in \widehat{\mathcal{U}}_{p^{m_p}}$ is a character of modulus p^{m_p}. The factorization of χ induces a factorization of idempotents $e_\chi = \prod_p e_{\chi_{p^{m_p}}}$

such that

$$e_\chi \zeta_m = \prod_p e_{\chi_{p^{m_p}}} \zeta_{p^{m_p}}^{a_p}. \tag{3.2}$$

Let Σ_m denote the support of ζ_m in $\mathbb{Q}(\zeta_m)$. Since Σ_m depends only on the cyclic $\mathbb{Q}[\mathcal{U}_m]$-module generated by ζ_m, it follows that Σ_m is the support of ζ_m^a for all $a \in \mathcal{U}_m$. Then (3.2) implies that $\chi \in \Sigma_m$ if and only if $\chi_{p^{m_p}} \in \Sigma_{p^{m_p}}$ for all primes p. The conductor of χ is the product of the conductors of $\chi_{p^{m_p}}$, hence by the definition of supportive characters, $\chi \in \widehat{\mathcal{U}}_m^*$ if and only if $\chi_{p^{m_p}} \in \widehat{\mathcal{U}}_{p^{m_p}}^*$. Thus to prove our claim it suffices to show that $\Sigma_{p^k} = \widehat{\mathcal{U}}_{p^k}^*$ for all primes p and all $k \geq 1$. Note that $\widehat{\mathcal{U}}_{p^k}^* \subseteq \widehat{\mathcal{U}}_{p^k}$ consists of all the primitive characters if $k > 1$ and all characters if $k = 1$.

If $k = 1$, then the identity

$$\sum_{q \in \mathcal{U}_p} \zeta_p^q = -1$$

implies that $\mathbb{Q}(\zeta_p)$ is the cyclic $\mathbb{Q}[\mathcal{U}_p]$-module generated by ζ_p. Therefore $\Sigma_p = \widehat{\mathcal{U}}_p = \widehat{\mathcal{U}}_p^*$.

If $k > 1$, then $\{1, \zeta_{p^k}, \zeta_{p^k}^2, \ldots, \zeta_{p^k}^{p-1}\}$ forms a $\mathbb{Q}(\zeta_{p^{k-1}})$-basis for $\mathbb{Q}(\zeta_{p^k})$. Thus $\mathbb{Q}(\zeta_{p^k})$ decomposes as the direct sum of two $\mathbb{Q}[\mathcal{U}_{p^k}]$-submodules:

$$\mathbb{Q}(\zeta_{p^k}) = \mathbb{Q}(\zeta_{p^{k-1}}) \oplus \sum_{a=1}^{p-1} \mathbb{Q}(\zeta_{p^{k-1}}) \zeta_{p^k}^a =: U \oplus V. \tag{3.3}$$

We claim that V is the cyclic $\mathbb{Q}[\mathcal{U}_{p^k}]$-module generated by ζ_{p^k}. If $q \in \mathcal{U}_{p^k}$, then $q \equiv a + pb \bmod p^k$ for some $1 \leq a \leq p-1$ and some integer b. Consequently, $\zeta_{p^k}^q = \zeta_{p^{k-1}}^b \zeta_{p^k}^a \in \mathbb{Q}(\zeta_{p^{k-1}})\zeta_{p^k}^a$, and elements of this form span V by construction. The normal basis theorem implies that $\mathbb{Q}(\zeta_m) \cong \mathbb{Q}[\mathcal{U}_m]$ as $\mathbb{Q}[\mathcal{U}_m]$-modules for any m. Recall that $\widehat{\mathcal{U}}_{p^{k-1}}$ is identified with its natural image in $\widehat{\mathcal{U}}_{p^k}$ (see Caution 2.2). Hence, taking supports in (3.3) gives us

$$\widehat{\mathcal{U}}_{p^k} = \widehat{\mathcal{U}}_{p^{k-1}} \sqcup \Sigma_{p^k}.$$

Therefore $\Sigma_{p^k} = \widehat{\mathcal{U}}_{p^k} \setminus \widehat{\mathcal{U}}_{p^{k-1}} = \widehat{\mathcal{U}}_{p^k}^*$ consists of the primitive characters of modulus p^k. ∎

Remark 3.2. If $\chi \in \widehat{\mathcal{U}}_m$ is a non-trivial Dirichlet character of modulus m, then the *Gauss sum* of χ is

$$G(\chi) := \sum_{q \in \mathcal{U}_m} \chi(q) \zeta_m^q.$$

Gauss sums are scalar multiples of the isotypic components of $\zeta_m \in \mathbb{Q}(\zeta_m)$.

In particular,

$$G(\chi^{-1}) = \sum_{q \in \mathcal{U}_m} \overline{\chi(q)} \zeta_m^q = \varphi(m) e_\chi \zeta_m = \varphi(m)(\zeta_m)_\chi.$$

Thus the support of ζ_m may be interpreted as the set of all characters χ such that $G(\chi^{-1}) \neq 0$. Since $\widehat{\mathcal{U}}_m^*$ is closed under taking inverses, Proposition 3.1 is equivalent to the assertion

$$\widehat{\mathcal{U}}_m^* = \{\chi \in \widehat{\mathcal{U}}_m : G(\chi) \neq 0\}.$$

This characterization of non-vanishing Gauss sums, and hence of the support of ζ_m, may also be deduced from the classical theory of Gauss sums. In particular, it follows from Theorems 9.7 and 9.10 in Montgomery, Vaughan [19]. We thank Andrew O'Desky for bringing this to our attention.

We now turn to the main result of this section. Note that by Remark 2.4 we lose no generality in assuming that def is squarefree.

THEOREM 3.3. *Let $d, e, f, m \geq 1$ be integers, let m' be the squarefree part of m, and let $\mathcal{H}_2^a \subseteq \widehat{\mathcal{U}}_m$ be the affine hyperplane $\mathcal{H}_2^a := \{\chi \in \widehat{\mathcal{U}}_m : \chi(2) = -1\}$. Suppose that*

(i) *def is squarefree,*
(ii) *d is coprime to m,*
(iii) *e divides m',*
(iv) *f divides m/m'.*

Let $\Sigma_{f,m} \subseteq \widehat{\mathcal{U}}_m$ be the set of all characters χ such that

(1) *$v_p(c_\chi) = v_p(m)$ if $v_p(m) \geq 2$ and $v_p(f) = 0$, and*
(2) *$v_p(c_\chi) \geq v_p(m) - 1$ if $v_p(m) > 2$ and $v_p(f) = 1$.*

Then $M_{def}(\zeta_m) = 0$ if and only if

$$\Sigma_{f,m} \subseteq \begin{cases} \bigcup_{p|d} \mathcal{H}_p & \text{if } e \text{ is odd,} \\ \bigcup_{p|d} \mathcal{H}_p \cup \mathcal{H}_2^a & \text{if } e \text{ is even.} \end{cases}$$

Proof. Since we assume that d, e, f are pairwise coprime, we may express $M_{def}(\zeta_m)$ as

$$M_{def}(\zeta_m) = \frac{1}{def} \varphi_d(\varphi_e \varphi_f \zeta_m).$$

Our strategy is to determine the support of $\varphi_e \varphi_f \zeta_m$ and then apply Theorem 2.5 with $v = \varphi_e \varphi_f \zeta_m$. Note that Theorem 2.5 does not immediately apply with $v = \zeta_m$ because def is not coprime to m.

Observe that

$$\varphi_f \zeta_m = \sum_{b|f} \mu(f/b) \zeta_m^b = \sum_{b|f} \mu(f/b) \zeta_{m/b},$$

where $\zeta_{m/b} := \zeta_m^b$ is a primitive m/bth root of unity and $\mu(f/b) \neq 0$ since f is squarefree. Proposition 3.1 implies that the support of $\zeta_{m/b}$ is $\widehat{\mathcal{U}}_{m/b}^*$.

If b, b' are distinct divisors of f, then by the definition of f there is some prime p such that $v_p(m) \geq 2$ and, say, $1 = v_p(b) > v_p(b') = 0$. Thus if c and c' are the conductors of characters in $\widehat{\mathcal{U}}^*_{m/b}$ and $\widehat{\mathcal{U}}^*_{m/b'}$, respectively, then

$$v_p(c) \leq v_p(m/b) < v_p(m) = v_p(c'),$$

where the last equality follows from Proposition 3.1. In particular, $\widehat{\mathcal{U}}^*_{m/b}$ and $\widehat{\mathcal{U}}^*_{m/b'}$ are disjoint. Therefore the support of $\varphi_f \zeta_m$ is

$$\Sigma_{\varphi_f \zeta_m} = \bigcup_{b|f} \widehat{\mathcal{U}}^*_{m/b}.$$

Let $\Sigma_{f,m} \subseteq \widehat{\mathcal{U}}_m$ be the set of characters defined in the statement of Theorem 3.3. We claim that

$$\Sigma_{f,m} = \bigcup_{b|f} \widehat{\mathcal{U}}^*_{m/b} = \Sigma_{\varphi_f \zeta_m}. \tag{3.4}$$

Suppose $\chi \in \widehat{\mathcal{U}}^*_{m/b}$ for some $b \mid f$. Then (3.1) implies $v_p(c_\chi) = v_p(m/b)$ whenever $v_p(m/b) \geq 2$. Since b is squarefree, there are two cases: if $v_p(b) = 0$, then $v_p(m) = v_p(m/b) \geq 2$ and $v_p(c_\chi) = v_p(m)$; and if $v_p(b) = 1$, then $v_p(m) > 2$ and $v_p(c_\chi) = v_p(m) - 1$. Hence $\chi \in \Sigma_{f,m}$ and thus $\bigcup_{b|f} \widehat{\mathcal{U}}^*_{m/b} \subseteq \Sigma_{f,m}$.

For the reverse inclusion, suppose that $\chi \in \Sigma_{f,m}$. Let b be the product of all primes $p \mid f$ such that $v_p(c_\chi) < v_p(m)$. Then b is a divisor of f, and c_χ divides m/b. If p is a prime such that $v_p(b) = 0$, then $v_p(c_\chi) = v_p(m)$ by construction. If p is a prime such that $v_p(b) = 1$ and $v_p(m/b) > 1$, then $v_p(m) > 2$ and $v_p(c_\chi) \geq v_p(m) - 1$ by the definition of $\Sigma_{f,m}$. On the other hand, $v_p(c_\chi) < v_p(m)$ since p divides b, hence $v_p(c_\chi) = v_p(m) - 1$. In either case we have $v_p(c_\chi) = v_p(m/b)$ when $v_p(m/b) \geq 2$, which is equivalent to $\chi \in \widehat{\mathcal{U}}^*_{m/b}$. Therefore $\Sigma_{f,m} \subseteq \bigcup_{b|f} \widehat{\mathcal{U}}^*_{m/b}$, which finishes the proof of (3.4).

Now suppose p is a prime dividing e, so that $v_p(m) = 1$. Since m/p is coprime to p by assumption, we may write $\zeta_m = \zeta^a_{m/p} \zeta^b_p$ for some $a \in \mathcal{U}_{m/p}$ and $b \in \mathcal{U}_p$. Recall that

$$1 = -\sum_{k=1}^{p-1} \zeta_p^{bk}.$$

For $1 \leq k \leq p-1$, let $c(p,k) \in \mathcal{U}_m$ be the unique unit such that

$$c(p,k) \equiv p \bmod m/p, \qquad c(p,k) \equiv k \bmod p.$$

Then $\zeta_m^{c(p,k)} = \zeta_{m/p}^{ap}\zeta_p^{bk}$. Hence

$$\begin{aligned}\varphi_p\zeta_m &= \zeta_m^p - \zeta_m = \zeta_{m/p}^{ap} - \zeta_m \\ &= -\Big(\zeta_m + \sum_{k=1}^{p-1}\zeta_{m/p}^{ap}\zeta_p^{bk}\Big) = -\Big(1 + \sum_{k=1}^{p-1}[c(p,k)]\Big)\zeta_m =: -\alpha_p\zeta_m.\end{aligned}$$

Recall that any $\chi \in \widehat{\mathcal{U}}_m$ can be factored as $\chi = \chi_{m/p}\chi_p$ with $\chi_n \in \widehat{\mathcal{U}}_n$ (see the proof of Proposition 3.1). Then

$$\chi(c(p,k)) = \chi_{m/p}(p)\chi_p(k).$$

Hence

$$\chi(\alpha_p) = 1 + \chi_{m/p}(p)\sum_{k=1}^{p-1}\chi_p(k).$$

The orthogonality relations for characters imply that

$$\sum_{k=1}^{p-1}\chi_p(k) = \begin{cases} p-1 & \text{if } \chi_p = 1, \\ 0 & \text{if } \chi_p \neq 1. \end{cases}$$

If $\chi_p \neq 1$, then $\chi(\alpha_p) = 1 \neq 0$. If $\chi_p = 1$, then $\chi(\alpha_p) = 0$ is equivalent to

$$0 = \chi(\alpha_p) = 1 + \chi_{m/p}(p)(p-1) \implies \chi_{m/p}(p) = \frac{1}{1-p}.$$

As $\chi_{m/p}(p)$ is a root of unity, it must be the case that $p=2$ and $\chi_{m/p}(2)=-1$. In other words, $\chi(\alpha_p)=0$ if and only if $\chi \in \mathcal{H}_2^a$. Thus $\Sigma_{\varphi_p\zeta_m} = \Sigma_{\zeta_m} = \widehat{\mathcal{U}}_m^*$ for each odd prime $p \mid e$ and $\Sigma_{\varphi_2\zeta_m} = \widehat{\mathcal{U}}_m^* \setminus \mathcal{H}_2^a$. Since e is squarefree, $\varphi_e = \prod_{p|e}\varphi_p$, hence

$$\Sigma_{\varphi_e\varphi_f\zeta_m} = \begin{cases} \Sigma_{f,m} & \text{if } e \text{ is odd}, \\ \Sigma_{f,m} \setminus \mathcal{H}_2^a & \text{if } e \text{ is even}. \end{cases}$$

Thus, invoking Theorem 2.5 makes our proof complete. ∎

Corollary 3.4. *Let $d, e, m \geq 1$ be as in Theorem 3.3. Suppose that m is squarefree and e is odd. If $M_{de}(\zeta_m) = 0$, then $M_{de}(\zeta_m^k) = 0$ for all $k \geq 0$. In other words, $\Phi_m(x)$ divides $M_{de}(x)$ if and only if $x^m - 1$ divides $M_{de}(x)$.*

Proof. If m is squarefree, then $\widehat{\mathcal{U}}_m^* = \widehat{\mathcal{U}}_m$ and $f = 1$ in the notation of Theorem 3.3. Since e is odd, Theorem 3.3 implies that $M_{de}(\zeta_m) = 0$ if and only if $\bigcup_{p|d}\mathcal{H}_p$ covers $\widehat{\mathcal{U}}_m$, and this is equivalent to $\varphi_d = 0$ by Theorem 2.5. Thus for all $k \geq 0$,

$$M_{de}(\zeta_m^k) = \frac{\varphi_d}{d}M_e(\zeta_m^k) = 0. \ ∎$$

Remark 3.5. To see the necessity of the condition that e is odd in Corollary 3.4 consider the factorization

$$M_{10}(x) = g(x)\cdot\Phi_6\cdot\Phi_4\cdot\Phi_2\cdot\Phi_1\cdot x$$

for some non-cyclotomic irreducible polynomial $g(x) \in \mathbb{Q}[x]$. Thus $\Phi_6(x)$ divides $M_{10}(x)$, but $\Phi_3(x)$ does not (here $m = 6$, $d = 5$, $e = 2$).

In Example 1.8 we showed that $M_{21}(\zeta_8) = 0$ but $M_{21}(\zeta_8^2) \neq 0$, which shows the necessity of the assumption that m is squarefree.

4. Cyclotomic factors of $\Phi_d(x) - 1$.

In this section we characterize the pairs (d, m) for which $\Phi_d(\zeta_m) = 1$ in terms of hyperplane arrangements covering explicit subsets of $\widehat{\mathcal{U}}_m$. The structure of this section parallels that of Section 3.

We will make use of the functions of a real variable x with $d \geq 1$ defined by

$$\zeta^x := \exp(2\pi i x), \qquad \varepsilon(x) := 2|\sin(\pi x)|,$$
$$\varphi_d\lfloor x\rfloor := \sum_{e|d} \mu(d/e)\lfloor ex\rfloor \equiv \sum_{e|d} \lfloor ex\rfloor \bmod 2.$$

Thus $\zeta^{k/m} = \zeta_m^k$ and $\varepsilon(x)$ is periodic with period 1 and positive for all non-integral x. If $d \in \mathbb{N}$, let $\varepsilon(x)^{[d]} := \varepsilon(dx)$.

Lemma 4.1. *Let $d > 1$ and let x be a real variable. Then:*

(1) $\zeta^x - 1 = i(-1)^{\lfloor x\rfloor}\zeta^{x/2}\varepsilon(x)$.

(2) $\Phi_d(\zeta^x) = (-1)^{\varphi_d\lfloor x\rfloor}\zeta^{\varphi(d)x/2}\varepsilon(x)^{\varphi_d}$.

Proof. (1) Recall that $2\sin(\pi x) = -i(\zeta^{x/2} - \zeta^{-x/2})$. Thus,

$$\zeta^x - 1 = \zeta^{x/2}(\zeta^{x/2} - \zeta^{-x/2}) = i\zeta^{x/2}(2\sin(\pi x))$$
$$= i(-1)^{\lfloor x\rfloor}\zeta^{x/2}((-1)^{\lfloor x\rfloor}2\sin(\pi x)).$$

The functions $(-1)^{\lfloor x\rfloor}$ and $2\sin(\pi x)$ are both periodic with period 2. Since

$$2\sin(\pi(x+1)) = -2\sin(\pi x), \qquad (-1)^{\lfloor x+1\rfloor} = -(-1)^{\lfloor x\rfloor},$$

it follows that their product has period 1 and

$$(-1)^{\lfloor x\rfloor}2\sin(\pi x) = 2|\sin(\pi x)| = \varepsilon(x).$$

Therefore,

$$\zeta^x - 1 = i(-1)^{\lfloor x\rfloor}\zeta^{x/2}\varepsilon(x).$$

(2) We compute

$$\Phi_d(\zeta^x) = \prod_{e|d}(\zeta^{ex} - 1)^{\mu(d/e)} = \prod_{e|d}(i(-1)^{\lfloor ex\rfloor}\zeta^{ex/2}\varepsilon(ex))^{\mu(d/e)}$$
$$= (-1)^{\sum_{e|d}\mu(d/e)\lfloor ex\rfloor}\zeta^{\sum_{e|d}\mu(d/e)ex/2}\prod_{e|d}\varepsilon(ex)^{\mu(d/e)}$$
$$= (-1)^{\varphi_d\lfloor x\rfloor}\zeta^{\varphi(d)x/2}\varepsilon(x)^{\varphi_d}.$$

Note that the factor of i cancels in the third equality since $\sum_{e|d}\mu(d/e)=0$ for $d>1$. ∎

Setting $x=1/m$ in Lemma 4.1(2) gives us

$$\Phi_d(\zeta_m)=(-1)^{\varphi_d\lfloor 1/m\rfloor}\zeta_{2m}^{\varphi(d)}\varepsilon(1/m)^{\varphi_d}.$$

Therefore $\Phi_d(\zeta_m)=1$ is equivalent to the following two identities holding simultaneously:

$$(-1)^{\varphi_d\lfloor 1/m\rfloor}\zeta_{2m}^{\varphi(d)}=1, \tag{4.1}$$

$$\varepsilon(1/m)^{\varphi_d}=1. \tag{4.2}$$

Equation (4.1) is an arithmetic condition. Satisfying (4.2) requires an analysis of the support of $\varepsilon(1/m)$ in the $\mathbb{Z}[\mathcal{U}_m]$-module $\mathbb{Q}(\zeta_m)^\times$.

It will be simpler to work with additive notation: let $\ell(x):=\log\varepsilon(x)$. We define the *mth cyclotomic module* $\mathcal{C}_m$ to be the $\mathbb{Q}[\mathcal{U}_m]$-module spanned by $\ell(a/m)$ for $a\not\equiv 0 \bmod m$. Let $[q]\ell(a/m):=\ell(qa/m)$ for $q\in\mathcal{U}_m$. Then

$$\varphi_d\ell(1/m)=\log|\Phi_d(\zeta_m)|=\log\varepsilon(1/m)^{\varphi_d}.$$

Since

$$\ell(-x)=\log|\zeta^{-x}-1|=\log|\zeta^{-x}(1-\zeta^x)|=\ell(x),$$

the action of $\mathcal{U}_m$ on $\mathcal{C}_m$ factors through $\mathcal{U}_m/\langle -1\rangle$.

Bass [1, Thm. 2] determined the structure of $\mathcal{C}_m$ as a $\mathbb{Q}[\mathcal{U}_m]$-module. The proof of Theorem 4.2 below is a combination of a Galois equivariant version of the Dirichlet unit theorem and the fact, due to Kummer [15], that the cyclotomic units have finite index in the units $\mathbb{Z}[\zeta_m]^\times$ (see Washington [26, Thm. 8.2] for a modern reference).

THEOREM 4.2 (Bass). *Given $m\geq 1$, let $\omega(m)$ denote the number of distinct prime factors of m, and let $\mathbf{1}$ denote the trivial representation of $\mathcal{U}_m$. Then*

$$\mathcal{C}_m\cong\mathbb{Q}[\mathcal{U}_m/\langle -1\rangle]\oplus\mathbf{1}^{\omega(m)-1}.$$

Therefore the support of $\mathcal{C}_m$ is $\{\chi\in\widehat{\mathcal{U}}_m:\chi(-1)=1\}=\mathcal{H}_{-1}$.

REMARK 4.3. Our definition of the mth cyclotomic module varies slightly from how Bass defines it. Bass' ($\mathbb{Q}$-linearized) cyclotomic module $\mathcal{C}_m'$ is defined as the $\mathbb{Q}$-extension of scalars of the abelian group multiplicatively spanned by ζ_m^a-1 with $a\not\equiv 0 \bmod m$. There is a natural surjective map $\mathcal{C}_m'\to\mathcal{C}_m$ given by $\zeta_m^a-1\mapsto\log|\zeta_m^a-1|=\ell(a/m)$, which we claim is an isomorphism. It suffices to show that if $u=\prod_{a=1}^{m-1}(\zeta_m^a-1)^{b_a}\in\mathcal{C}_m'$ with $b_a\in\mathbb{Z}$ has absolute value 1, then u is a root of unity. Since $\overline{\zeta_m^a-1}=-\zeta_m^{-a}(\zeta_m^a-1)$, we have

$$1=|u|=u\overline{u}=\zeta u^2,$$

for some root of unity ζ. Hence u is a square root of a root of unity, and thus is itself a root of unity. Therefore $\mathcal{C}_m \cong \mathcal{C}'_m$.

The following lemma establishes several useful relations in $\mathcal{C}_m$.

LEMMA 4.4. *Let $m > 1$.*

(1) *If $q > 1$ is a natural number not divisible by m, then*

$$([q]-1)\ell(1/m) := \ell(q/m) - \ell(1/m) = \sum_{b=1}^{q-1} \ell(1/m + b/q).$$

(2) *Let p be a prime and suppose that $q = p^e$ divides m.*

  (a) *If $d < e$, then $\ell(p^d/m) \in \mathbb{Q}[\mathcal{U}_m]\ell(1/m)$.*

  (b) *If q is the largest power of p dividing m and $n = m/q$, then $\varphi_p\ell(1/n) \in \mathbb{Q}[\mathcal{U}_m]\ell(1/m)$.*

Proof. (1) Observe that

$$|\zeta^{qx} - 1| = \prod_{b=0}^{q-1} |\zeta^{x+b/q} - 1|.$$

Evaluating at $x = 1/m$ and taking logarithms (which we can because $m \nmid q$) we find

$$\ell(q/m) = \sum_{b=0}^{q-1} \ell(1/m + b/q).$$

(2a) Part (1) implies that

$$\ell(p^d/m) = \sum_{b=0}^{p^d-1} \ell(1/m + b/p^d) = \sum_{b=0}^{p^d-1} \ell\left(\frac{1 + b(m/p^d)}{m}\right).$$

Since $d < e$, we see that m/p^d is divisible by p. Hence $1 + b(m/p^d)$ is a unit modulo m. Thus $\ell(p^d/m) \in \mathbb{Q}[\mathcal{U}_m]\ell(1/m)$.

(2b) Let $n := m/q$, so that n is coprime to p by assumption. From (1) we have

$$\varphi_p\ell(1/n) = \sum_{b=1}^{p-1} \ell(1/n + b/p) = \sum_{b=1}^{p-1} \ell\left(\frac{p + bn}{np}\right).$$

Since n and p are coprime and b is a unit modulo p, it follows that $p + bn$ is a unit modulo n and modulo p, hence a unit modulo np. Therefore

$$\varphi_p\ell(1/n) \in \mathbb{Q}[\mathcal{U}_m]\ell(1/np) \subseteq \mathbb{Q}[\mathcal{U}_m]\ell(1/m),$$

where the last inclusion is a consequence of part (2a). ∎

Recall that by our convention on extending the domains of Dirichlet characters (see Caution 2.2), if p is a prime dividing m, then $\chi(p)$ has a well-defined, non-zero value if the conductor of χ is not divisible by p, and otherwise $\chi(p) = 0$. If q is the largest power of p dividing m, then we have $\mathcal{H}_p \subseteq \widehat{\mathcal{U}}_{m/q} \subseteq \widehat{\mathcal{U}}_m$.

Proposition 4.5. *Let $m > 1$ be an integer and let $\chi \in \widehat{\mathcal{U}}_m$ be a character of modulus m. Then χ is in the support of $\ell(1/m)$ if and only if*

$$\chi \in \mathcal{H}_{-1} \setminus \bigcup_{p\mid m} \mathcal{H}_p$$
$$= \{\chi \in \widehat{\mathcal{U}}_m : \chi(-1) = 1 \text{ and } \chi(p) \neq 1 \text{ for all primes } p \mid m\}.$$

Proof. Let $m = q_1 \cdots q_k$ be the factorization of m into prime powers where q_i is a power of the prime p_i. If $J \subseteq \{1, \ldots, k\}$ is a subset, let $m_J := \prod_{j\in J} q_j$ and let $n_J := m/m_J$. Lemma 4.4(2b) implies that for each proper subset $J \subset \{1, \ldots, k\}$,

$$\Big(\prod_{p\mid m_J} \varphi_p\Big)\ell(1/n_J) \in \mathbb{Q}[\mathcal{U}_m]\ell(1/m).$$

Let $\widetilde{\Sigma}_m$ denote the support of $\ell(1/m)$. Then the support of the above element is $\widetilde{\Sigma}_{n_J} \setminus \bigcup_{p\mid m_J} \mathcal{H}_p$. Hence

$$\widetilde{\Sigma}_m \supseteq \widetilde{\Sigma}_{n_J} \setminus \bigcup_{p\mid m_J} \mathcal{H}_p.$$

Lemma 4.4(2) shows that $\mathcal{C}_m$ is generated as a $\mathbb{Q}[\mathcal{U}_m]$-module by $\ell(1/n_J)$ as J ranges over all proper subsets of $\{1, \ldots, k\}$ and Theorem 4.2 shows that the support of $\mathcal{C}_m$ is $\mathcal{H}_{-1}$. Thus

$$\mathcal{H}_{-1} = \bigcup_J \widetilde{\Sigma}_{n_J}.$$

Therefore

$$\widetilde{\Sigma}_m \supseteq \bigcup_J \Big(\widetilde{\Sigma}_{n_J} \setminus \bigcup_{p\mid m_J} \mathcal{H}_p\Big) \supseteq \mathcal{H}_{-1} \setminus \bigcup_{p\mid m} \mathcal{H}_p.$$

Now we show the reverse inclusion. Lemma 4.4 implies that for each i,

$$\varphi_{p_i}\ell(1/n_i) = \Big(\sum_{b=1}^{p_i-1} [p_i + bn_i]\Big)\ell(1/n_i p_i) = \Big(\sum_{b=1}^{p_i-1} [p_i + bn_i]\Big)[q_i/p_i]\ell(1/m).$$

If $\chi \in \mathcal{H}_{p_i}$, then by definition χ must have modulus n_i and $\chi(p_i) = 1$. Thus applying the idempotent e_χ to the right hand side of the above identity we find

$$e_\chi\Big(\sum_{b=1}^{p_i-1} [p_i + bn_i]\Big)[q_i/p_i]\ell(1/m) = \sum_{b=1}^{p_i-1} \chi(p_i + bn_i)\chi(q_i/p_i)\ell(1/m)_\chi$$
$$= (p_i - 1)\ell(1/m)_\chi.$$

On the other hand,

$$e_\chi \varphi_{p_i} \ell(1/n_i) = (\chi(p_i) - 1)\ell(1/n_i)_\chi = 0.$$

Therefore $\ell(1/m)_\chi = 0$, which is equivalent to saying that χ does not belong to $\widetilde{\Sigma}_m$. Hence

$$\widetilde{\Sigma}_m \subseteq \mathcal{H}_{-1} \setminus \bigcup_{p|m} \mathcal{H}_p. \ \blacksquare$$

We now prove the main result of this section. Note that by Remark 2.4 we lose no generality by assuming def is squarefree.

Theorem 4.6. *Let $d, e, f \geq 1$ and $m > 1$ be integers, let m' be the squarefree part of m, and let $\mathcal{H}_3^a \subseteq \widehat{\mathcal{U}}_m$ be the affine hyperplane $\mathcal{H}_3^a := \{\chi \in \widehat{\mathcal{U}}_m : \chi(3) = -1\}$. Suppose that*

(i) *m does not divide def,* (ii) *def is squarefree,* (iii) *d is coprime to m,* (iv) *e divides m',* (v) *f divides m/m'.*

Then $\Phi_{def}(\zeta_m) = 1$ if and only if

(1) $\mathcal{H}_{-1} \subseteq \begin{cases} \bigcup_{p|md/e} \mathcal{H}_p & \text{if } 3 \nmid e, \\ \bigcup_{p|md/e} \mathcal{H}_p \cup \mathcal{H}_3^a & \text{if } 3 \mid e, \end{cases}$

(2) *m divides $\varphi(def)$, and*

(3) $\displaystyle\sum_{a|def} \lfloor a/m \rfloor \equiv \frac{\varphi(def)}{m} \bmod 2.$

Proof. As we observed following Lemma 4.1, $\Phi_{def}(\zeta_m) = 1$ is equivalent to the triviality of both the phase (4.1) and the radial (4.2) components of $\Phi_{def}(\zeta_m)$. Suppose that the phase component of $\Phi_{def}(\zeta_m)$ is trivial,

$$(-1)^{\lfloor\varphi\rfloor_{def}(1/m)} \zeta_{2m}^{\varphi(def)} = 1.$$

Thus $\zeta_{2m}^{\varphi(def)} = \pm 1$, which is equivalent to m dividing $\varphi(def)$. If m does divide $\varphi(def)$, then comparing exponents of -1 in the above identity we conclude that

$$\sum_{a|def} \lfloor a/m \rfloor \equiv \frac{\varphi(def)}{m} \bmod 2.$$

Triviality of the radial component of $\Phi_{def}(\zeta_m)$ is equivalent to

$$\varphi_{def}\ell(1/m) = 0.$$

Following the same strategy as in the proof of Theorem 3.3, we determine the support of $\varphi_{ef}\ell(1/m)$ and then appeal to Theorem 2.5.

Let $\chi \in \mathcal{H}_{-1} \subseteq \widehat{\mathcal{U}}_m$ be a character. If $\widetilde{e}$ is the product of all primes p dividing e such that $\chi(p) = 1$ and $\widetilde{n} := m/\widetilde{e}$, then we claim that there is some non-zero constant c such that

$$(4.3)\qquad (\varphi_{ef}\,\ell(1/m))_\chi = \begin{cases} 0 & \text{if } 3 \mid e \text{ and } \chi \in \mathcal{H}_3^a, \\ c\ell(1/\widetilde{n})_\chi & \text{otherwise.} \end{cases}$$

First we finish the proof supposing that we have shown (4.3). Proposition 4.5 implies that $\ell(1/\widetilde{n})_\chi = 0$ if and only if $\chi(p) = 1$ for some prime $p \mid \widetilde{n}$, and any such prime must divide the factor m/e of $\widetilde{n}$ by the definition of $\widetilde{n}$. Therefore, the support Σ of $\varphi_{ef}\,\ell(1/m)$ is

$$\Sigma = \begin{cases} \mathcal{H}_{-1} \setminus \bigcup_{p \mid m/e} \mathcal{H}_p & \text{if } 3 \nmid e, \\ \mathcal{H}_{-1} \setminus (\bigcup_{p \mid m/e} \mathcal{H}_p \cup \mathcal{H}_3^a) & \text{if } 3 \mid e. \end{cases}$$

Thus Theorem 2.5 implies $\varphi_{def}\ell(1/m) = 0$ if and only if

$$\mathcal{H}_{-1} \subseteq \begin{cases} \bigcup_{p \mid dm/e} \mathcal{H}_p & \text{if } 3 \nmid e, \\ \bigcup_{p \mid dm/e} \mathcal{H}_p \cup \mathcal{H}_3^a & \text{if } 3 \mid e. \end{cases}$$

All that remains is to prove (4.3). We use the factorization $\varphi_{ef} = \prod_{p \mid ef} \varphi_p$ (which uses (ii)) to analyze $(\varphi_{ef}\,\ell(1/m))_\chi$ one prime at a time.

Let p be a prime dividing f and let $n := m/p$. Then p divides n by (v). Lemma 4.4(1) implies that

$$\varphi_p\,\ell(1/m) = \sum_{k \in \mathcal{U}_p} [1 + kn]\ell(1/m).$$

If χ has conductor dividing n, then

$$(\varphi_p\,\ell(1/m))_\chi = \sum_{k \in \mathcal{U}_p} \chi(1 + kn)\ell(1/m)_\chi = (p-1)\ell(1/m)_\chi.$$

If the conductor of χ does not divide n, then write $\chi = \chi_n\chi_p$ where χ_n has conductor dividing n and χ_p has conductor p^{m_p} with $m_p = v_p(m) > 1$ (the inequality uses (v)). Thus

$$\begin{aligned} (\varphi_p\,\ell(1/m))_\chi &= \sum_{k \in \mathcal{U}_p} \chi(1 + kn)\ell(1/m)_\chi \\ &= \sum_{k \in \mathcal{U}_p} \chi_p(1 + kp^{m_p - 1})\ell(1/m)_\chi = -\ell(1/m)_\chi, \end{aligned}$$

where the last equality follows from the observation that $\chi_p(1 + kp^{m_p-1})$ ranges over the non-trivial pth roots of unity as k ranges over $\mathcal{U}_p$. Hence in either case there is some non-zero constant c such that

$$(4.4)\qquad (\varphi_p\,\ell(1/m))_\chi = c\ell(1/m)_\chi.$$

Next let p be a prime dividing e, so that $n := m/p$ is coprime to p by (iv) and $n > 1$ by (i). Observe that

$$(\varphi_p\,\ell(1/m))_\chi = \ell(1/n)_\chi - \ell(1/m)_\chi.$$

If the conductor of χ does not divide n, then

$$(\varphi_p\,\ell(1/m))_\chi = -\ell(1/m)_\chi.$$

Suppose the conductor of χ divides n. Lemma 4.4(1) implies that

$$(\chi(p)-1)\ell(1/n)_\chi = (\varphi_p\,\ell(1/n))_\chi = \sum_{k\in\mathcal{U}_p} \chi(p+kn)\ell(1/m)_\chi = \chi(p)(p-1)\ell(1/m)_\chi. \tag{4.5}$$

If $\chi(p) \neq 1$, then

$$(\varphi_p\,\ell(1/m))_\chi = \ell(1/n)_\chi - \ell(1/m)_\chi = \left(\frac{p-1}{1-\overline{\overline{\chi(p)}}} - 1\right)\ell(1/m)_\chi.$$

The coefficient of $\ell(1/m)_\chi$ vanishes if and only if $\chi(p) = 1/(2-p)$. Since $\chi(p)$ is a root of unity, it must be the case that $p = 3$ and $\chi(3) = -1$.

If $\chi(p) = 1$, then $\ell(1/m)_\chi = 0$ by (4.5) and thus

$$(\varphi_p\,\ell(1/m))_\chi = \ell(1/n)_\chi.$$

Hence if $p \,|\, e$ and $n = m/p$, then

(4.6)

$$(\varphi_p\ell(1/m))_\chi = \begin{cases} \ell(1/n)_\chi & \text{if } \chi \in \mathcal{H}_p, \\ 0 & \text{if } p = 3 \text{ and } \chi \in \mathcal{H}_3^a, \\ c\ell(1/m)_\chi & \text{otherwise, for some non-zero constant } c. \end{cases}$$

Together (4.4) and (4.6) prove our claim (4.3). ■

Example 4.7. Let $m = 24$ and suppose we want to find an integer d coprime to 24 such that $\Phi_{3d}(\zeta_{24}) = 1$. The group $\widehat{\mathcal{U}}_{24}$ of Dirichlet characters is a 3-dimensional $\mathbb{F}_2$-vector space. Let $\rho : \mathcal{U}_{24} \to \widehat{\mathbb{F}}_2^3$ be the choice of coordinates such that

$$\rho(13) = x, \qquad \rho(17) = y, \qquad \rho(19) = z.$$

Following Theorem 4.6, we begin by looking for some d such that the plane $\mathcal{H}_{-1} : x + y + z = 0$ is covered by $\mathcal{H}_2$, $\mathcal{H}_3^a$, and the union of the $\mathcal{H}_p$ with $p \,|\, d$. Since $13 \equiv 19 \equiv 1 \bmod 3$ and $17 \equiv 1 \bmod 8$, it follows that $\widehat{\mathcal{U}}_3$ is the subspace $x = z = 0$ and $\widehat{\mathcal{U}}_8$ is the subspace $y = 0$. Then $\mathcal{H}_2 \subseteq \widehat{\mathcal{U}}_3$ consists of the single point $(0,0,0)$, and $\mathcal{H}_3^a \subseteq \widehat{\mathcal{U}}_8$ is the subspace $x = 1$, $y = 0$, which intersects $x + y + z = 0$ at the point $(1,0,1)$. Therefore it suffices for $\bigcup_{p|d} \mathcal{H}_p$ to cover the two points $(1,1,0)$ and $(0,1,1)$. For example, the lines $\mathcal{H}_5 = \mathcal{H}_{13\cdot 17} : x + y = 0$ and $\mathcal{H}_{11} = \mathcal{H}_{17\cdot 19} : y + z = 0$ suffice.

If $d = 55 = 5 \cdot 11$, then $\varphi(3d) = 80$ is not divisible by 24, hence $\Phi_{3 \cdot 5 \cdot 11}(\zeta_{24}) \neq 1$ by Theorem 4.6. On the other hand, if $d = 385 = 5 \cdot 7 \cdot 11$, then $\varphi(3 \cdot 5 \cdot 7 \cdot 11) = 480$ is divisible by 24 and

$$\sum_{a|3d} \lfloor a/m \rfloor = 90 \equiv 20 = \frac{\varphi(3d)}{m} \bmod 2.$$

Thus Theorem 4.6 implies that $\Phi_{3d}(\zeta_m) = \Phi_{3 \cdot 385}(\zeta_{24}) = 1$. ∎

Acknowledgements. We thank Andrew O'Desky for suggesting the connection with Dirichlet characters, for explaining an alternative proof of Proposition 3.1 via Gauss sums (see Remark 3.2), and for extensive feedback on several drafts of this paper. We thank the referee for their feedback and for bringing [4, 9, 20] to our attention. We also thank Weiyan Chen, David Cox, Suki Dasher, Nir Gadish, Jeff Lagarias, Bob Lutz, and Phil Tosteson for their comments and feedback on earlier versions of the paper.

The author is partially supported by the NSF grant DMS-2002176 and the Jump Trading Mathlab Research Fund.

References

[1] H. Bass, *Generators and relations for cyclotomic units*, Nagoya Math. J. 27 (1966), 401–407.

[2] J. Berstel and D. Perrin, *The origins of combinatorics on words*, Eur. J. Combin. 28 (2007), 996–1022.

[3] B. Bzdęga, A. Herrera-Poyatos, and P. Moree, *Cyclotomic polynomials at roots of unity*, Acta Arith. 184 (2018), 215–230.

[4] C. K. Caldwell, *Unique (period) primes and the factorization of cyclotomic polynomials minus one*, Math. Japon. 46 (1997), 189–195.

[5] L. Christie, K. J. Dykema, and I. Klep, *Classifying minimal vanishing sums of roots of unity*, arXiv:2008.11268v1.

[6] M. Conrad, *On explicit relations between cyclotomic numbers*, Acta Arith. 93 (2000), 67–76.

[7] J. R. Doyle, P. Fili, and T. Hyde, *Dynatomic polynomials, necklace operators, and universal relations for dynamical units*, New York J. Math. 28 (2022), 534–556.

[8] V. Ennola, *On relations between cyclotomic units*, J. Number Theory 4 (1972), 236–247.

[9] S. Ettahri, O. Ramaré, and L. Surel, *Fast multi-precision computation of some Euler products*, Math. Comp. 90 (2021), 2247–2265.

[10] C. F. Gauss, *Allgemeine Untersuchungen über die Congruenzen*, in: Untersuchungen über höhere Arithmetik (translated by H. Maser), 2nd ed., Chelsea, New York, 1965.

[11] T. Hyde, *Polynomial statistics, necklace polynomials, and the arithmetic dynamical Mordell–Lang conjecture*, dissertation, Univ. of Michigan, 2019.

[12] T. Hyde, *Liminal reciprocity and factorization statistics*, Algebr. Combin. 2 (2019), 521–539.

[13] T. Hyde, *Polynomial factorization statistics and point configurations in* $\mathbb{R}^3$, Int. Math. Res. Notices 2020, 10154–10179.

[14] T. Hyde, *Euler characteristic of the space of real multivariate irreducible polynomials*, Proc. Amer. Math. Soc. 150 (2022), 2331–2343.

[15] E. Kummer, *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, J. Math. Pures Appl. 16 (1851), 377–498.

[16] R. P. Kurshan and A. M. Odlyzko, *Recursive filters with uniform power distribution*, Electron. Lett. 16 (1980), no. 17, 672–673.

[17] R. P. Kurshan and A. M. Odlyzko, *Values of cyclotomic polynomials at roots of unity*, Math. Scand. 49 (1982), 15–35.

[18] N. Metropolis and G.-C. Rota, *Witt vectors and the algebra of necklaces*, Adv. Math. 50 (1983), 95–125.

[19] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory. I. Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge Univ. Press, Cambridge, 2006.

[20] P. Moree, *Approximation of singular series and automata*, Manuscripta Math. 101 (2000), 385–399.

[21] K. Ramachandra, *On the units of cyclotomic fields*, Acta. Arith. 12 (1966), 165–173.

[22] C. Reutenauer, *Free Lie Algebras*, London Math. Soc. Monogr. 7, Clarendon Press, New York, 1993.

[23] T. Schönemann, *Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist*, J. Reine Angew. Math. 31 (1846), 269–325.

[24] J.-P. Serre, *Linear Representations of Finite Groups*, Grad. Texts in Math. 42, Springer, New York, 1977.

[25] J. H. Silverman, *The Arithmetic of Dynamical Systems*, Grad. Texts in Math. 241, Springer, New York, 2007.

[26] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1982.

[27] E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. 177 (1937), 152–160.

Trevor Hyde
Department of Mathematics
University of Chicago
Chicago, IL 60637, USA
E-mail: tghyde@uchicago.edu