CYCLOTOMIC FACTORS OF NECKLACE POLYNOMIALS

TREVOR HYDE

ABSTRACT. Necklace polynomials $M_d(x)$ play an important role in number theory, combinatorics, dynamics, and representation theory. In this paper we introduce and analyze the *cyclotomic factor phenomenon*: the observation that for all $d \geq 1$ the dth necklace polynomial $M_d(x)$ is highly reducible over $\mathbb{Q}$ with the majority of their irreducible factors being cyclotomic polynomials. We show that this phenomenon extends in two independent directions: to the G-necklace polynomials associated to a finite group G and to the higher necklace polynomials $M_{d,n}(x)$ counting multivariate irreducible polynomials over a finite field. This latter generalization leads to a surprising formula for the Euler characteristic of the moduli space of multivariate irreducible polynomials over $\mathbb{R}$ and $\mathbb{C}$.

1. INTRODUCTION

The d**th necklace polynomial** $M_d(x)$ for $d \geq 1$ an integer is defined by

$$M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}, \tag{1.1}$$

where μ is the number theoretic Möbius function. Necklace polynomials arise naturally in number theory, combinatorics, dynamics, geometry, representation theory, and algebra (see the beginning of Section 2.) 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 of length d one can make with beads in k colors.

We begin with the observation that necklace polynomials are highly reducible over $\mathbb{Q}$.

Example 1.1. Let $d = 3 \cdot 5 \cdot 7 = 105$, then

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

where $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial of degree 92.

With only one exception, the low degree irreducible factors of $M_d(x)$ in Example 1.1 are all cyclotomic polynomials. Recall that the m**th cyclotomic polynomial** $\Phi_m(x)$ is the $\mathbb{Q}$-minimal polynomial of a primitive mth root of unity. More explicitly,

$$\Phi_m(x) = \prod_{n|m} (x^{m/n} - 1)^{\mu(n)}.$$

This preponderance of cyclotomic factors of $M_d(x)$ is not isolated to specific choices of d; it occurs to some extent for all d.

Date: November 20th, 2018.

Example 1.2. There are irreducible, non-cyclotomic polynomials $f(x), g(x), h(x) \in \mathbb{Z}[x]$ with degrees $3, 210, 708$ respectively such that

$$\begin{aligned} 10M_{10}(x) &= x^{10} - x^5 - x^2 + x \\ &= f(x) \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x \\ 243M_{243}(x) &= x^{243} - x^{23} - x^{11} + x \\ &= g(x) \cdot \Phi_{24} \cdot \Phi_{22} \cdot \Phi_{11} \cdot \Phi_{10} \cdot \Phi_8 \cdot \Phi_5 \cdot \Phi_2 \cdot \Phi_1 \cdot x \\ 741M_{741}(x) &= x^{741} - x^{247} - x^{57} - x^{39} + x^{19} + x^{13} + x^3 - x \\ &= h(x) \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{12} \cdot \Phi_9 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x. \end{aligned}$$

We aim to explain why necklace polynomials have cyclotomic factors and to determine the $m, d \geq 1$ such that $\Phi_m(x)$ divides $M_d(x)$. Toward that end our first result is Theorem 1.3. Recall the factorizations

$$x^m - 1 = \prod_{n|m} \Phi_n(x) \qquad x^m + 1 = \prod_{\substack{n|2m \\ n\nmid m}} \Phi_n(x).$$

Theorem 1.3. *Let $m, d \geq 1$ be integers.*

(1) If p is a prime dividing d such that $p \equiv 1 \bmod m$, then $x^m - 1$ divides $M_d(x)$.

(2) If $x^m - 1$ divides $M_d(x)$, then $x^m - 1$ divides $M_{de}(x)$ for all $e \geq 1$.

(3) If $x^m + 1$ divides $M_d(x)$, then $x^m + 1$ divides $M_{de}(x)$ for all odd $e \geq 1$.

*(4) If c is the squarefree part of d (c is the product of all distinct prime factors of d), then all cyclotomic factors of $M_d(x)$ are **induced** from cyclotomic factors of $M_c(x)$ (see Definition 2.8.) In other words, it suffices to determine the cyclotomic factors of $M_d(x)$ for d squarefree.*

(5) If $x^m - 1$ divides $M_d(x)$, then m divides $\varphi(d)$, where φ is the Euler totient function.

Theorem 1.3 describes conditions under which $M_d(x)$ has factors of the form $x^m \pm 1$, which in turn factor as products of cyclotomic polynomials. We conjecture that all cyclotomic factors of necklace polynomials arise in this way.

Conjecture 1.4. *If $\Phi_m(x)$ divides $M_d(x)$ for some $m, d \geq 1$, then either $x^m - 1$ divides $M_d(x)$ or m is even and $x^{m/2} + 1$ divides $M_d(x)$.*

See Section 2.4 for a discussion of Conjecture 1.4 and supporting evidence.

1.1. **Minimal cyclotomic factors.** Assuming Conjecture 1.4 we turn to the problem of characterizing the m and d such that $x^m \pm 1$ divides $M_d(x)$. Theorem 1.3 reduces us to the case where d is squarefree with at least two prime factors such that $x^m \pm 1$ does not divide $M_e(x)$ for any proper factor e of d. Say $x^m \pm 1$ **minimally divides** $M_d(x)$ if $x^m \pm 1$ divides $M_d(x)$ and does not divide $M_e(x)$ for any proper divisor e of d.

A combinatorial encoding of minimal $x^m \pm 1$ factors of necklace polynomials in terms of **primitive necklace systems** (Theorem 2.18) is given in Section 2. As a consequence we parametrize several families of minimal $x^m \pm 1$ factors of necklace polynomials.

Theorem 1.5. *Let $m \geq 1$ be an integer.*

(1) There are no pairs of distinct primes p and q such that $d = pq$ and $x^m - 1$ minimally divides $M_d(x)$.

(2) Suppose that $d = pq$ for distinct primes p and q. Then $x^m + 1$ minimally divides $M_d(x)$ if and only if

$$\begin{aligned} pq &\equiv 1 + m \bmod 2m \\ p &\equiv q + m \bmod 2m \\ p, q &\not\equiv 1 \qquad \bmod 2m. \end{aligned}$$

For example, if $p \equiv m - 1 \bmod 2m$ and $q \equiv -1 \bmod 2m$, then $x^m + 1$ minimally divides $M_{pq}(x)$.

(3) If $d = pqr$ for distinct primes p, q, r such that

$$\begin{aligned} p^2 \equiv q^2 \equiv r^2 &\equiv 1 \bmod m \\ pqr &\equiv 1 \bmod m \\ p, q, r &\not\equiv 1 \bmod m, \end{aligned}$$

then $x^m - 1$ minimally divides $M_d(x)$.

Example 1.6. Let $m = 15$. Then the prime factors of $d = 11 \cdot 19 \cdot 29 = 6061$ satisfy the congruences in Theorem 1.5 (3), hence $x^{15} - 1$ minimally divides $M_{6061}(x)$. In fact

$$\begin{aligned} 6061 M_{6061}(x) &= x^{6061} - x^{551} - x^{319} - x^{209} + x^{29} + x^{19} + x^{11} - x \\ &= f(x) \cdot (x^{15} - 1) \cdot \Phi_{60} \cdot \Phi_{30} \cdot \Phi_{28} \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{14} \cdot \Phi_{12} \\ &\quad \cdot \Phi_{10} \cdot \Phi_9 \cdot \Phi_7 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot x, \end{aligned}$$

where $f(x)$ is an irreducible, non-cyclotomic polynomial of degree 5964.

It would be interesting to know the extent to which minimal $x^m \pm 1$ divisors of necklace polynomials can be classified into infinite families cut out by congruences.

1.2. **Differences of necklace polynomials.** After clearing denominators, the differences between necklace polynomials often have cyclotomic factors.

Example 1.7. There is an irreducible, non-cyclotomic polynomial $f(x) \in \mathbb{Z}[x]$ of degree 83 such that

$$\begin{aligned} 91 M_{91}(x) - 6 M_6(x) &= x^{91} - x^{13} - x^7 - x^6 + x^3 + x^2 \\ &= f(x) \cdot \Phi_5(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \cdot x^2. \end{aligned}$$

This implies, for example, that $91 M_{91}(\zeta_5) = 6 M_6(\zeta_5)$ for any 5th root of unity ζ_5.

In line with Conjecture 1.4 we expect these cyclotomic factors to be accounted for by factors of $dM_d(x) - eM_e(x)$ of the form $x^m \pm 1$. Theorem 1.8 identifies the source of this phenomenon. Say integers d and e are **primewise congruent modulo** m if

$$d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \qquad e = q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$$

for some $k \geq 1$ and primes p_i, q_i such that $e_i = f_i$ and $p_i \equiv q_i \bmod m$ for each i. Then

Theorem 1.8. *Let $d, e \geq 1$ be integers.*

(1) If d and e are primewise congruent modulo m, then

$$dM_d(x) \equiv eM_e(x) \bmod x^m - 1.$$

(2) If d and e are primewise congruent modulo $2m$, then

$$dM_d(x) \equiv eM_e(x) \bmod x^m + 1.$$

Example 1.9. Returning to Example 1.7, note that $91 = 7 \cdot 13$ and $6 = 2 \cdot 3$ are primewise congruent modulo 5. Hence $x^5 - 1$ divides $91 M_{91}(x) - 6 M_6(x)$. The factor of $\Phi_2(x) = x + 1$ appears because $M_d(-1) = 0$ for all $d \geq 2$ (see Theorem 1.15.)

1.3. **Frobenius algebra and functional equations.** Our main tool for analyzing cyclotomic factors of necklace polynomials is the **Frobenius algebra**. The Frobenius algebra, denoted Ψ, is the ring freely generated as an additive abelian group by symbols $[m]$ for $m \in \mathbb{N}$ subject to the multiplicative relations $[m][n] = [mn]$. Equivalently Ψ is the monoid ring $\mathbb{Z}[\mathbb{N}^\times]$ where $\mathbb{N}^\times$ is the multiplicative monoid of natural numbers. There is an action of Ψ on polynomials given by $[m]f(x) := f(x^m)$. Every polynomial in $f(x) = \sum_{k=0}^{d} a_k x^k \in \mathbb{Z}[x]$ has a unique expression as $f(x) = [f]x$ where

$$[f] := \sum_{k=0}^{d} a_k [k].$$

The operator $[M_d]$ associated to a necklace polynomial factors in Ψ according to the prime factorization of d.

Theorem 1.10. *Suppose that $d = \prod_{p|d} p^{e_p}$ is the prime factorization of d. Then*

$$M_d(x) = \frac{1}{d}\varphi[d]x,$$

where

$$\varphi[d] := \prod_{p|d} [p^{e_p}] - [p^{e_p - 1}] \in \Psi.$$

Most cyclotomic factors of necklace polynomials can be traced back to this factorization of the operator $\varphi[d]$. Theorem 1.11 demonstrates a sense in which the cyclotomic factor phenomenon can be associated more generally to the operator $\varphi[d] \in \Psi$.

Theorem 1.11. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial.*

(1) If $x^m - 1$ divides $M_d(x)$, then

$$x^m - 1 \text{ divides } \varphi[d]f(x) = \sum_{e|d} \mu(e) f(x^{d/e}).$$

(2) If $x^m + 1$ divides $M_d(x)$ and $f(x)$ is an odd polynomial, then

$$x^m + 1 \text{ divides } \varphi[d]f(x) = \sum_{e|d} \mu(e) f(x^{d/e}).$$

Example 1.12. In Example 1.2 we saw that $x^{22} - 1$ divides $M_{243}(x)$. It follows that for any polynomial $f(x)$ we have

$$x^{22} - 1 \text{ divides } \varphi[243]f(x) = f(x^{243}) - f(x^{23}) - f(x^{11}) + f(x).$$

1.4. **Cyclotomic factors of $\Phi_d(x) - 1$.** The operator $[f]$ associated to a polynomial $f(x)$ typically does not factor in Ψ. Factorizations of $[f]$ correspond to functional equations satisfied by $f(x)$. For example, the factorization of $[M_d]$ given in Theorem 1.10 is equivalent to $M_d(x)$ satisfying the following relations (see Theorem 2.26.) Let p be a prime integer.

(1) If p does not divide d, then

$$M_{dp}(x) = \frac{1}{p}\big(M_d(x^p) - M_d(x)\big).$$

(2) If p divides d, then

$$M_{dp}(x) = \frac{1}{p}M_d(x^p).$$

These functional equations for $M_d(x)$ were first studied by Metropolis and Rota [27]. Cyclotomic polynomials satisfy a multiplicative version of the same identities. Again let p be a prime integer.

(1) If p does not divide d, then
$$\Phi_{dp}(x) = \frac{\Phi_d(x^p)}{\Phi_d(x)}.$$
(2) If p divides d, then
$$\Phi_{dp}(x) = \Phi_d(x^p).$$

These identities are equivalent to
$$\log \Phi_d(x) = \varphi[d] \log(x-1).$$

Thus Theorem 1.11 suggests that cyclotomic factors of $M_d(x)$ should also divide $\log \Phi_d(x)$, or equivalently $\Phi_d(x)-1$. This does not follow formally from Theorem 1.11 since $\log(x-1)$ is not a polynomial, however we do recover the following result along these lines.

Theorem 1.13. *Suppose that $m, d > 1$ are integers, m does not divide d, and $x^m - 1$ divides $M_d(x)$, then $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$.*

Example 1.14. In Example 1.6 we showed that $x^{15} - 1$ divides $M_{6061}(x)$. Thus Theorem 1.13 implies that $\frac{x^{15}-1}{x-1}$ divides $\Phi_{6061}(x) - 1$. Hence if ζ_{15}^j is any non-trivial 15th root of unity and ζ_{6061} is a primitive 6061th root of unity, then the following product identity holds in $\overline{\mathbb{Q}}$,
$$\prod_{(k,6061)=1} (\zeta_{15}^j - \zeta_{6061}^k) = \Phi_{6061}(\zeta_{15}^j) = 1. \tag{1.2}$$

Since $(15, 6061) = 1$ the difference $\zeta_{15}^j - \zeta_{6061}^k$ is an algebraic unit for each k coprime to 6061. Hence (1.2) is a non-trivial relation satisfied by these units.

1.5. **Trace formula.** A cyclotomic factor $\Phi_m(x)$ of $M_d(x)$ is equivalent to the vanishing $M_d(\zeta_m) = 0$ for any primitive mth root of unity m. Although $M_d(x)$ vanishes at only finitely many roots of unity, Theorem 1.15 shows that $M_d(\zeta_m)$ is approximately zero (in a sense) for all but finitely many m.

Theorem 1.15. *Let $m, d \geq 1$ and let $\mathrm{Tr}_m : \mathbb{Q}(\zeta_m) \to \mathbb{Q}$ be the $\mathbb{Q}$-linear trace map (where $\mathrm{Tr}_m(\alpha)$ is the sum over the orbit of α under $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.) Then*

(1) The trace of $M_d(\zeta_m)$ is given by
$$\mathrm{Tr}_m(M_d(\zeta_m)) = \begin{cases} \mu(m/d) & \text{when } d \text{ divides } m \\ 0 & \text{otherwise.} \end{cases}$$
(2) If d does not divide m and $M_d(\zeta_m)$ is rational, then $M_d(\zeta_m) = 0$.
(3) In particular we have the following evaluations of $M_d(\pm 1)$,
$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & \text{otherwise.} \end{cases}$$

Since $M_1(x) = x$, the trace computation in Theorem 1.15 specializes when $d = 1$ to the well-known formula for the trace of a primitive mth root of unity ζ_m,
$$\mathrm{Tr}_m(\zeta_m) = \mu(m).$$

We view Theorem 1.15 as a generalization of this classic identity. The evaluations of $M_d(\pm 1)$ given in Theorem 1.15 (3) are given geometric interpretations in Section 6.

We show that aspects of the cyclotomic factor phenomenon extend to two independent generalizations of the necklace polynomials $M_d(x)$: the G-necklace polynomials $M_G(x)$ associated to a finite group G, and the higher necklace polynomials $M_{d,n}(x)$ enumerating irreducible polynomials in a multivariate polynomial ring over $\mathbb{F}_q$.

1.6. **G-necklace polynomials.** Let G be a finite group and let X be a finite set. An **X-coloring of G** or a **G-necklace with X colors** is simply a function from G to X. The group G acts on X^G, the set of all X-colorings of G. A **primitive** G-necklace is an element of X^G with trivial stabilizer. If the set X has x elements, then the total number of orbits of primitive G-necklaces with X colors is given by a polynomial $M_G(x)$ in x called the **G-necklace polynomial**. An explicit formula for $M_G(x)$ is given by

$$M_G(x) = \frac{1}{|G|} \sum_{H \subseteq G} \mu(H) x^{|G|/|H|},$$

where $\mu(H)$ is the value of the Möbius function of the subgroup lattice of G on the interval of subgroups between 1 and H (see Section 3.)

When $G = C_d$ is the cyclic group of order d, a C_d-necklace reduces to the usual notion of a necklace of length d and $M_{C_d}(x) = M_d(x)$. Hence $M_G(x)$ is a natural generalization of $M_d(x)$. For certain classes of groups G we observe that $M_G(x)$ exhibits a cyclotomic factor phenomenon similar to the cyclic case.

Example 1.16. Let D_{20} be the dihedral group with 20 elements. Then $M_{D_{20}}(x)$ factors over $\mathbb{Q}$ as

$$20M_{D_{20}}(x) = x^{20} - 11x^{10} + 10x^5 - x^4 + 11x^2 - 10x = f(x)(x^2+1)(x+1)(x-1)x,$$

where $f(x) \in \mathbb{Z}[x]$ is an irreducible, non-cyclotomic polynomial of degree 15.

Dress and Siebeneicher [6] introduced the G-necklace polynomials while constructing an isomorphism between the G-necklace algebra and the G-Burnside-Witt ring. Oh [29] studied the G-necklace polynomials in depth, generalizing the functional identities for the classic necklace polynomials $M_d(x)$ to G-necklace polynomials.

Oh's results provide new insights into these functional equations, highlighting their relation to the structure of the group G. When G is solvable we show that Oh's functional equations for $M_G(x)$ translate into a product formula for $[M_G]$ in the Frobenius algebra. This factorization of $[M_G]$ gives rise to cyclotomic factors of $M_G(x)$.

Theorem 1.17. *Suppose G is a finite group with subgroup K and a chain of normal subgroups*

$$K = N_0 \triangleleft N_1 \triangleleft \dots N_k \triangleleft N_{k+1} = G$$

such N_{i+1}/N_i is cyclic of prime order p_i. Let c_i be the number of non-trivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$.

(1) Let $M_G(x)$ be the G-necklace polynomial, then

$$M_G(x) = \frac{1}{[G:K]} \Big(\prod_{i=0}^{k} [p_i] - c_i[1] \Big) M_K(x).$$

(2) If $c_i = 1$, then $x^{p_i - 1} - 1$ divides $M_G(x)$. If G is solvable and $K = 1$, then $c_0 = 1$ and this implies that $M_G(x)$ has cyclotomic factors.

(3) If $c_i > 1$, then $x^{p_i-1} - 1$ divides $|G| M_G(x)$ in $\mathbb{Z}/(c_i - 1)$.

Example 1.18. The dihedral group D_{20} has a cyclic normal subgroup $C_{10} \triangleleft D_{20}$ of index 2 such that there are 10 non-trivial subgroups in D_{20} which intersect trivially with C_{10}, hence

$$M_{D_{20}}(x) = \frac{1}{2}([2] - 10[1]) M_{10}(x) = \frac{1}{2}(M_{10}(x^2) - 10M_{10}(x)).$$

On the other hand, $M_{D_{20}}(x) = \varphi[10]\frac{1}{2}(x^2 - 10x)$, so Theorem 1.11 implies that $M_{D_{20}}(x)$ is divisible by $x^m - 1$ whenever $M_{10}(x)$ is.

1.7. **Higher necklace polynomials.** Let $\mathbb{F}_q$ be a finite field and let $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ be the set of monic, $\mathbb{F}_q$-irreducible, total degree d polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$. By a monic polynomial in a multivariate polynomial ring we mean an $\mathbb{F}_q^\times$-orbit of polynomials under scaling. Since $\mathbb{F}_q$ is finite, $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a finite set. In [20, Lem. 2.1] we constructed a polynomial $M_{d,n}(x) \in \mathbb{Q}(x)$ such that $M_{d,n}(q) = |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|$ for any prime power q. For $d, n \geq 1$ we call $M_{d,n}(x)$ the **higher necklace polynomials**.

The first (implicit) reference to $M_{d,n}(x)$ we are aware of is due to Carlitz [4, 5] who studied the asymptotic behavior of $M_{d,n}(x)$ as $n \to \infty$. In [20] we analyzed the x-adic asymptotic behavior of $M_{d,n}(x)$, showing that $M_{d,n}(x)$ converges coefficientwise as $n \to \infty$ to a simple rational function related to the classic necklace polynomial $M_d(x)$ in a surprising way.

When $n = 1$ the higher necklace polynomials reduce to the classic case $M_{d,1}(x) = M_d(x)$. If $n > 1$, then there is no known explicit formula for $M_{d,n}(x)$ analogous to the simple expression (1.1) for $M_d(x)$. Furthermore $[M_{d,n}] \in \Psi$ is not known to factor analogously to $[M_d]$ and $[M_G]$ which we used to explain the cyclotomic factor phenomenon in those cases. Nevertheless we observe that $M_{d,n}(x)$ does generally have cyclotomic factors for $d, n \geq 1$.

For each fixed $n > 1$, instead of seeing many different cyclotomic factors of $M_{d,n}(x)$ as we vary d, we see the same factors for all but finitely many d. When $n = 1$ the only cyclotomic factors that divide $M_d(x)$ for all but finitely many d are $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Theorem 1.19 below demonstrates this phenomenon.

Let $b, n \geq 1$ be integers. A **balanced base b expansion of** n is an expression

$$n = b^{k_1} - b^{k_2} + b^{k_3} - \ldots + b^{k_{i-1}} - b^{k_i},$$

where $k_1 > k_2 > k_3 > \ldots > k_i \geq 0$ is a decreasing sequence of integers and the coefficients on the right hand side alternate between ± 1. Equivalently, n has a balanced base b expansion if all of the base b digits of n are 0 or $b - 1$,

$$n = (b-1)b^{\ell_1} + (b-1)b^{\ell_2} + \ldots + (b-1)b^{\ell_j}.$$

In that case, the balanced base b expansion of n is gotten by expanding each $(b-1)b^k = b^{k+1} - b^k$ and collecting coefficients.

Theorem 1.19. *Let $d, n \geq 1$ and suppose p is a prime such that n has the balanced base p expansion*

$$n = \sum_{k=0}^{m} a_k p^k.$$

Let ζ_p be a primitive pth root of unity. Then

$$M_{d,n}(\zeta_p) = \begin{cases} a_k & \text{if } d = p^k \\ 0 & \text{otherwise.} \end{cases}$$

If n has a balanced base p expansion, then $x^p - 1$ divides $M_{d,n}(x)$ for all but finitely many d.

Example 1.20. If $n = 121$, then n has the balanced base 5 expansion

$$121 = 5^3 - 5 + 1.$$

Therefore, if ζ_5 is a primitive 5th root of unity, then

$$M_{d,121}(\zeta_5) = \begin{cases} 1 & d = 1, 125 \\ -1 & d = 5 \\ 0 & \text{otherwise.} \end{cases}$$

Hence $M_{d,121}(x)$ is divisible by $\Phi_5(x)$ for all but finitely many d.

The lack of functional equations or explicit formulas for $M_{d,n}(x)$ requires us to use another method to analyze cyclotomic factors of $M_{d,n}(x)$. The following "combinatorial Euler product formula" gives an indirect way to study the higher necklace polynomials.

Theorem 1.21. *Let $P_{d,n}(x) \in \mathbb{Q}[x]$ be the polynomial such that $P_{d,n}(q)$ is the number of total degree d monic polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$. Then for each $n \geq 1$ the following identity holds in the ring of formal power series with coefficients in $\mathbb{Q}[x]$,*

$$\sum_{d\geq 0} P_{d,n}(x)t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_{j,n}(x)},$$

where exponentiation by $M_{j,n}(x)$ on the right hand side is defined by the binomial theorem,

$$\left(\frac{1}{1-t}\right)^a := \sum_{d\geq 0}(-1)^d\binom{-a}{d}t^d.$$

When $n = 1$ we have $P_{d,1}(x) = x^d$ and Theorem 1.21 specializes to the well-known **cyclotomic identity** [27, Sec. 5],

$$\frac{1}{1-xt} = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_j(x)}.$$

We view Theorem 1.21 as a generalized cyclotomic identity.

1.8. **Geometric interpretations.** We interpret the values $M_{d,n}(\pm 1)$ geometrically as Euler characteristics of the spaces of irreducible polynomials over $\mathbb{R}$ and $\mathbb{C}$. For any field K let $\mathrm{Irr}_{d,n}(K)$ be the space of all monic total degree d irreducible polynomials in $K[x_1, x_2, \ldots, x_n]$. When $K = \mathbb{R}$ or $\mathbb{C}$, $\mathrm{Irr}_{d,n}(K)$ inherits a topology from its inclusion in the projective space $\mathrm{Poly}_{d,n}(K)$ of all total degree d monic polynomials in n variables.

Theorem 1.22. *Let $d, n \geq 1$ and let χ_c be the compactly supported Euler characteristic, then*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad \chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} b_k & \text{if } d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

where $n = \sum_{k\geq 0} b_k 2^k$ is the balanced base 2 expansion of n.

Example 1.23. Suppose $n = 13$. The balanced binary expansion of 13 is

$$13 = 2^4 - 2^2 + 2 - 1.$$

Hence Theorem 1.22 implies

$$\chi_c(\mathrm{Irr}_{d,13}(\mathbb{R})) = \begin{cases} 1 & d = 2, 16 \\ -1 & d = 1, 4 \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 1.22 suggests that the singular cohomology of $\mathrm{Irr}_{d,n}(\mathbb{R})$ depends in a subtle way on the additive structure of the parameter n. It would be interesting to determine the cohomology of this space. Note that the n-dimensional affine general linear group acts on $\mathrm{Irr}_{d,n}(\mathbb{R})$ by linear changes of coordinates and that the quotient by this action can be identified with the moduli space of irreducible degree d real hypersurfaces.

When $n = 1$ we can use our understanding of the irreducible polynomials in $\mathbb{C}[x]$ and $\mathbb{R}[x]$ to compute $M_d(\pm 1)$ geometrically (see Corollary 6.6.) In particular since there are no irreducible polynomials in $\mathbb{C}[x]$ or $\mathbb{R}[x]$ with degree $d > 2$ it follows that $M_d(\pm 1) = 0$ for all such d. This gives an interpretation of the cyclotomic factors $\Phi_1(x)$ and $\Phi_2(x)$ of necklace polynomials $M_d(x)$. We would be interested to know if there are interpretations, geometric or otherwise, of the values $M_{d,n}(\zeta_m)$ for $m > 2$.

1.9. **Organization.** In Section 2 we introduce the Frobenius algebra and use it to explain the cyclotomic factor phenomenon for the classic necklace polynomials $M_d(x)$. Theorem 1.3 is proven as Theorems 2.7, 2.9, 2.13, and 2.15 in Section 2. Section 3 combines these methods with a result of Oh to understand cyclotomic factors of G-necklace polynomials. Theorem 1.17 is proven as Theorem 3.2. Combinatorial Euler products are discussed in Section 4 and then applied in Section 5 to prove Theorem 1.19. Section 6 contains the proof of Theorem 1.22.

1.10. **Acknowledgements.** We thank Suki Dasher andAndrew O'Desky for asking a question that prompted this work. We thank Weiyan Chen, Nir Gadish, Bob Lutz, and Phil Tostesson for helpful conversations and feedback on the manuscript. We thank David Cox for his help on references to the work of Gauss and Schönemann. Finally we thank Jeff Lagarias for his generous advice and encouragement.

2. Necklace polynomials

Necklace polynomials play an important role in several areas of mathematics.

(1) If $x = k$ is a natural number, then $M_d(k)$ counts the number of primitive necklaces (cyclic orderings) formed with d beads in k possible colors. A necklace not invariant under any proper rotation is called **primitive**. This interpretation of $M_d(k)$ gives necklace polynomials their name. Metropolis and Rota [27, Pg. 95] attribute this interpretation of $M_d(x)$ to the French colonel Moreau; the M in the notation is presumably in his honor.

(2) A Lyndon word in a totally ordered alphabet with ℓ letters is a word that is lexicographically minimal among all of its cyclic permutations. The number of Lyndon words of length d formed from ℓ letters is $M_d(\ell)$. See Berstel and Perrin [2, Sec. 4.2].

(3) If $x = q$ is a prime power, then $M_d(q)$ is the number of irreducible monic polynomials in $\mathbb{F}_q[x]$ of degree d. This interpretation was discovered by Gauss [12, Pg. 611] and later independently rediscovered by Schönemann [33, Sec. 48, Pp. 51-52].

(4) If $x = g$ is a natural number, then Witt [40, 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 (1.1) is sometimes called Witt's formula [2, Pg. 1005]. Reutenaur [30, 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.

(5) If $f(x) \in \mathbb{C}[x]$ is a generic degree m polynomial, then the total number of length d periodic orbits of $f(x)$ under iteration is $M_d(m)$. See Silverman [34, Rmk. 4.3].

(6) Metropolis and Rota [27] derived functional equations satisfied by $M_d(x)$ and used them to construct the necklace ring $\mathrm{Nr}(R)$ from any commutative ring R. They proved [27, Prop. 1, Pg. 114] that $\mathrm{Nr}(R)$ is isomorphic to $W(R)$ the ring of big Witt vectors of R whenever R is a **binomial ring** (see Section 4.)

Despite the prevalence of necklace polynomials, the observation of their reducibility and cyclotomic factors seems to have been overlooked. In this section we initiate the study of the cyclotomic factor phenomenon. There are several equivalent ways to approach this problem, all fundamentally reducing to the functional equations discovered by Metropolis and Rota [27]. We reinterpret these relations using the Frobenius algebra defined below.

2.1. **The Frobenius Algebra.** For each integer $n \geq 0$ let $[n]$ be the operator on $\mathbb{Z}[x]$ defined by

$$[n]f(x) := f(x^n).$$

Then $[n]$ is a ring endomorphism of $\mathbb{Z}[x]$ and $[m][n] = [mn]$. We call $[n]$ the n**th Frobenius operator**. The **Frobenius algebra** Ψ is the $\mathbb{Z}$-algebra generated by $[n]$ for $n \geq 0$. The polynomial ring $\mathbb{Z}[x]$ has a

Ψ-module structure. For example, if $\alpha = 3[2] + 5[7] \in \Psi$ and $f(x) \in \mathbb{Z}[x]$ is a polynomial, then

$$\alpha f(x) = (3[2] + 5[7])f(x) = 3f(x^2) + 5f(x^7).$$

Observe that $\mathbb{Z}[x]$ is cyclic as a Ψ-module since if $f(x) = \sum_{i=0}^{j} a_i x^i$, then

$$f(x) = [f]x := \Big(\sum_{i=0}^{j} a_i[i]\Big)x.$$

The Frobenius algebra is canonically isomorphic to the monoid algebra $\mathbb{Z}[\mathbb{N}^\times]$, where $\mathbb{N}^\times$ is the multiplicative monoid of natural numbers. Note that $[1] = 1$ but $[0] \neq 0$ in Ψ since $[0]f(x) = f(x^0) = f(1)$ while $0f(x) = 0$.

Our terminology is inspired by the Frobenius operators in the theory of Witt vectors. Metropolis and Rota [27] construct the necklace ring $\mathrm{Nr}(\mathbb{Z})$ as a combinatorial model of the integral Witt vectors $W(\mathbb{Z})$. In this model they show that the nth Frobenius operator $[n]$ (which they denote F_n) acts on the dth necklace polynomial $M_d(x)$ by $[n]M_d(x) = M_d(x^n)$. The Ψ in the notation for the Frobenius algebra is a reference to the Adams operations ψ_m, which are the name for the Frobenius operators in the context of K-theory. We adopt this notation following Borger [3, Eq. (4.3.1)].

If $m, n \geq 0$ are integers, then $x^m - 1$ divides $x^{mn} - 1$. Hence the ideal $(x^m - 1)$ in $\mathbb{Z}[x]$ is stable under the action of Ψ. It follows that $\mathbb{Z}[x]/(x^m - 1)$ inherits a Ψ-module structure. Let $\Psi[m]$ denote the quotient of Ψ by the annihilator of the module $\mathbb{Z}[x]/(x^m - 1)$. If $\alpha, \beta \in \Psi$ we suggestively write

$$\alpha \equiv \beta \bmod [m]$$

when $\alpha = \beta$ in $\Psi[m]$. Note that if $a \equiv b \bmod m$, then $x^a \equiv x^b \bmod x^m - 1$. It follows that $[a] \equiv [b] \bmod [m]$ whenever $a \equiv b \bmod m$.

We caution that $\Psi[m]$ is **not** the quotient of Ψ by the principal ideal generated by $[m]$; instead it is the quotient by "congruence modulo m inside brackets." To see the difference consider integers a, b such that $a + b \equiv 0 \bmod m$. Then $[a + b] \equiv [0] \bmod [m]$ but generally $[a] + [b] \not\equiv [0]$ or $0 \bmod [m]$.

Suppose that $m, n \geq 0$ are integers and n is odd. The roots of $x^m + 1$ are the mth roots of -1 and in characteristic 0 the polynomial $x^m + 1$ is squarefree. If ζ is a root of $x^m + 1$ and n is odd, then ζ^n is still an mth root of -1, hence $\zeta^{mn} + 1 = 0$. Thus $x^m + 1$ divides $x^{mn} + 1$ whenever n is odd. Let Ψ^{odd} be the subalgebra of Ψ generated by $[n]$ for n odd. Then the ideal $(x^m + 1)$ of $\mathbb{Z}[x]$ is stable under Ψ^{odd} and $\mathbb{Z}[x]/(x^m + 1)$ inherits a Ψ^{odd}-module structure.

Since $x^m + 1$ divides $x^{2m} - 1$ and $x^{b+m} \equiv -x^b \bmod x^m + 1$, it follows that $\mathbb{Z}[x]/(x^m + 1)$ is isomorphic as a Ψ^{odd}-module to the quotient of $\Psi[2m]$ by the relations $[b + m] = -[b]$. Let $\Psi[m]_\pm$ denote this quotient module and for $\alpha, \beta \in \Psi$ write $\alpha \equiv \beta \bmod [m]_\pm$ if $\alpha = \beta$ in $\Psi[m]_\pm$.

Lemma 2.1 shows how the modules $\Psi[m]$ and $\Psi[m]_\pm$ may be used to study factors of polynomials of the form $x^m \pm 1$.

Lemma 2.1. *Let $m \geq 1$ and let $\alpha \in \Psi$.*

(1) If $\alpha \equiv 0 \bmod [m]$, then $x^m - 1$ divides $\alpha f(x)$ for all $f(x) \in \mathbb{Z}[x]$.
(2) If $\alpha \equiv 0 \bmod [m]_\pm$, then $x^m + 1$ divides $\alpha f(x)$ for all odd polynomials $f(x) \in \mathbb{Z}[x]$.

Proof. (1) If $f(x) \in \mathbb{Z}[x]$ is a polynomial, let $[f] \in \Psi$ be the operator such that $f(x) = [f]x$. Then $\alpha[f] \equiv 0 \bmod [m]$, hence

$$\alpha f(x) \equiv (\alpha[f])x \equiv 0x \equiv 0 \bmod x^m - 1.$$

thus $x^m - 1$ divides $\alpha f(x)$.

(2) If $f(x)$ is an odd polynomial, then $[f] \in \Psi^{\mathrm{odd}}$ and $\alpha[f] \equiv 0 \bmod [m]_\pm$. The same calculation as above shows that $x^m + 1$ divides $\alpha f(x)$. □

Example 2.2. We consider a concrete example to illustrate Lemma 2.1 and clarify the notation. Suppose $\alpha = [10] - [7]$. Then for a polynomial $f(x) \in \mathbb{Z}[x]$,

$$\alpha f(x) = ([10] - [7])f(x) = f(x^{10}) - f(x^7).$$

Since $10 \equiv 7 \bmod 3$ it follows that

$$\alpha = [10] - [7] \equiv [1] - [1] = 0 \bmod [3],$$

thus Lemma 2.1 (1) implies that $x^3 - 1$ divides $\alpha f(x)$. On the other hand, $x^{10} \equiv x^7 \equiv x \bmod x^3 - 1$ so we see directly that

$$\alpha f(x) = f(x^{10}) - f(x^7) \equiv f(x) - f(x) = 0 \bmod x^3 - 1.$$

Example 2.3. Lemma 2.1 (2) can fail if $f(x)$ is not an odd polynomial. For example, if $m = 2$ then $\alpha = [2] + [0]$ satisfies $\alpha \equiv 0 \bmod [2]_\pm$ since

$$[2] = [0 + 2] \equiv -[0] \bmod [2]_\pm.$$

If $f(x) = x^2$, then

$$\alpha f(x) = ([2] + [0])x^2 = x^4 + 1 \not\equiv 0 \bmod x^2 + 1.$$

However, if $f(x) = x^3$, then

$$\alpha f(x) = ([2] + [0])x^3 = x^6 + 1 \equiv 0 \bmod x^2 + 1,$$

which is consistent with Lemma 2.1 (2).

Recall that the dth necklace polynomial $M_d(x)$ is defined by

$$M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}. \tag{2.1}$$

Let $S_d(x) := dM_d(x) \in \mathbb{Z}[x]$. The denominator of $M_d(x)$ plays no role in the factorization of this polynomial and adds unnecessary clutter, so we work with $S_d(x)$ for simplicity. In the literature $S_d(x)$ is called the d**th cyclic polynomial** [27, Pg. 97].

Let $\varphi[d]$ denote the operator $[S_d] \in \Psi$. Equation (2.1) gives us the explicit formula

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

Recall the classic identity [28, Pg. 195, (4.1)]

$$\varphi(d) = \sum_{e|d} \mu(e)(d/e), \tag{2.2}$$

where $\varphi(d)$ is the Euler totient function of d, defined as the number of multiplicative units in $\mathbb{Z}/(d)$. The multiplicativity of the Möbius function allows us to factor (2.2) as

$$\varphi(d) = \prod_{p|d} p^{e_p} - p^{e_p - 1}$$

where the product is over prime divisors of d and e_p is the maximum multiplicity of p as a divisor of d. Since the Frobenius operators are multiplicative, it follows that $\varphi[d]$ factors similarly.

Proposition 2.4. *Let $d \geq 1$ and let $\varphi[d] := [S_d] = \sum_{e|d} \mu(e)[d/e] \in \Psi$. Then*

$$\varphi[d] = \prod_{p|d} [p^{e_p}] - [p^{e_p - 1}].$$

Proposition 2.4 justifies the notation $\varphi[d]$ for $[S_d]$. Note that $\varphi[d] \neq [\varphi(d)]$. In Section 2.2 we combine this factorization of $\varphi[d]$ with Lemma 2.1 to characterize factors of $M_d(x)$ of the form $x^m \pm 1$, which conjecturally account for all cyclotomic factors of necklace polynomials (see Section 2.4.)

While discussing the connection between the identity (2.2) and necklace polynomials we record one related observation.

Proposition 2.5. *Let $d \geq 1$ and let $M_d'(x)$ denote the derivative of $M_d(x)$, then*

$$M_d'(1) = \frac{\varphi(d)}{d} = \prod_{p|d} 1 - \frac{1}{p}.$$

Proof. Taking the derivative of (2.1) we have

$$M_d'(x) = \frac{1}{d} \sum_{e|d} \mu(e)(d/e)x^{d/e-1}.$$

Evaluating at $x = 1$ gives

$$M_d'(1) = \frac{1}{d} \sum_{e|d} \mu(e)(d/e) = \frac{\varphi(d)}{d}. \qquad \square$$

Theorem 2.6 shows that the cyclotomic factor phenomenon for $M_d(x)$ is associated more generally to the operator $\varphi[d]$.

Theorem 2.6. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial.*

(1) If $x^m - 1$ divides $M_d(x)$, then $x^m - 1$ divides $\sum_{e|d} \mu(e) f(x^{d/e})$.

(2) If $x^m + 1$ divides $M_d(x)$ and $f(x)$ is an odd polynomial, then $x^m + 1$ divides $\sum_{e|d} \mu(e) f(x^{d/e})$.

Proof. First note that $\varphi[d] := [S_d]$ is 0 in $\Psi[m]$ or $\Psi[m]_\pm$ precisely when $S_d(x) \equiv 0$ modulo $x^m - 1$ or $x^m + 1$ respectively. If $f(x) \in \mathbb{Z}[x]$ is a polynomial, then Lemma 2.1 (1) gives us that $\varphi[d] \equiv 0 \bmod [m]$ implies

$$\varphi[d]f(x) = \sum_{e|d} \mu(e) f(x^{d/e}) \equiv 0 \bmod x^m - 1.$$

Similarly, if $\varphi[d] \equiv 0 \bmod [m]_\pm$ and $f(x)$ is an odd polynomial, then Lemma 2.1 (2) implies that $\varphi[d]f(x) \equiv 0 \bmod x^m + 1$. $\square$

2.2. **Cyclotomic Factors.** Recall that the mth cyclotomic polynomial $\Phi_m(x) \in \mathbb{Z}[x]$ is the monic polynomial defined by

$$\Phi_m(x) := \prod_{n|m} (x^{m/n} - 1)^{\mu(n)}.$$

Equivalently $\Phi_m(x)$ is determined by the identity

$$x^m - 1 = \prod_{n|m} \Phi_n(x). \tag{2.3}$$

Since $x^{2m} - 1 = (x^m - 1)(x^m + 1)$ it follows from (2.3) that

$$x^m + 1 = \prod_{\substack{n|m \\ 2n \nmid m}} \Phi_{2n}(x).$$

The goal of this section is to characterize the pairs of integers (m, d) such that $\Phi_m(x)$ divides $M_d(x)$. Our criteria do not directly address cyclotomic factors of $M_d(x)$ but instead give conditions for when $x^m \pm 1$ divides $M_d(x)$. We conjecture that all cyclotomic factors of $M_d(x)$ may be accounted for in this way (see Conjecture 2.23.)

Theorem 2.7 shows that for a fixed m, the set of all d such that $x^m \pm 1$ divides $M_d(x)$ is closed under scaling.

Theorem 2.7. *Let $m, d \geq 1$.*

(1) If $x^m - 1$ divides $M_d(x)$, then $x^m - 1$ divides $M_{de}(x)$ for all $e \geq 1$.
(2) If $x^m + 1$ divides $M_d(x)$, then $x^m + 1$ divides $M_{de}(x)$ for all odd $e \geq 1$.

Proof. (1) Our assumption that $x^m - 1$ divides $M_d(x)$ is equivalent $\varphi[d] \equiv 0 \bmod [m]$. Proposition 2.4 implies that $\varphi[d]$ divides $\varphi[de]$ in Ψ, hence $\varphi[de] \equiv 0 \bmod [m]$. Thus Lemma 2.1 (1) implies $x^m - 1$ divides $M_{de}(x)$.

(2) Similarly x^m+1 dividing $M_d(x)$ is equivalent to $\varphi[d] \equiv 0 \bmod [m]_\pm$. If e is odd, then $\varphi[de]/\varphi[d] \in \Psi^{\mathrm{odd}}$. Since $\Psi[m]_\pm$ is a Ψ^{odd}-module it follows that $\varphi[de] \equiv 0 \bmod [m]_\pm$. Thus Lemma 2.1 (2) implies $x^m + 1$ divides $M_{de}(x)$. □

Theorem 2.7 allows us to reduce to the case when $x^m \pm 1$ divides $M_d(x)$ and d is minimal with respect to divisibility. Our next result further reduces to the case when d is squarefree.

Definition 2.8. If $f(x) \in \mathbb{Z}[x]$ is a polynomial, then we say a cyclotomic factor $\Phi_m(x)$ of $f(x^e)$ is **induced** from $f(x)$ if $\Phi_n(x)$ divides $f(x)$ for some $n \geq 1$ and $\Phi_m(x)$ divides $\Phi_n(x^e)$.

We claim that all cyclotomic factors of $f(x^m)$ are induced from $f(x)$. If $\Phi_m(x)$ divides $f(x^e)$ and ζ_m is a primitive mth root of unity, then $f(\zeta_m^e) = 0$. Hence ζ_m^e is a root of $f(x)$. Suppose that ζ_m^e is a primitive nth root of unity, then $\Phi_n(x)$ divides $f(x)$. Furthermore $\Phi_m(x)$ divides $\Phi_n(x^e)$.

If c is the squarefree part of d, which is to say that c is the product of the distinct prime factors of d, then Proposition 2.4 implies that

$$\varphi[d] = \prod_{p|d} [p^{e_p}] - [p^{e_p-1}] = \prod_{p|d} [p^{e_p-1}]([p] - [1]) = [d/c]\varphi[c].$$

Hence $S_d(x) = [d/c]S_c(x) = S_c(x^{d/c})$. It follows that all cyclotomic factors of $M_d(x) = \frac{1}{d}S_d(x)$ are induced from cyclotomic factors of $M_c(x)$.

Theorem 2.9. *If c is the squarefree part of d, then all cyclotomic factors of $M_d(x)$ are induced from cyclotomic factors of $M_c(x)$.*

Together Theorems 2.7 and 2.9 further reduce us to considering squarefree d such that $x^m \pm 1$ minimally divides $M_d(x)$. Our final reduction restricts which primes we need to consider.

Definition 2.10. Say positive integers d and e are **primewise congruent modulo** m if

$$d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \qquad e = q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}$$

for some $k \geq 1$ and primes p_i, q_i such that

(1) $e_i = f_i$ for each i,
(2) $p_i \equiv q_i \bmod m$ for each i,
(3) $p_i \neq p_j$ and $q_i \neq q_j$ for each $i \neq j$.

Theorem 2.11. *Let $m, d, e \geq 1$.*

(1) If d and e are primewise congruent modulo m, then

$$S_d(x) \equiv S_e(x) \bmod x^m - 1.$$

(2) If d and e are primewise congruent modulo $2m$, then

$$S_d(x) \equiv S_e(x) \bmod x^m + 1.$$

Proof. If d and e are primewise congruent modulo m, then $\varphi[d] \equiv \varphi[e] \bmod [m]$. It follows that $S_d(x) \equiv S_e(x) \bmod x^m - 1$. If $d \equiv e \bmod 2m$, then $\varphi[d] = \varphi[e]$ in $\Psi[2m]$ hence the same is true in the quotient $\Psi[m]_\pm$. Thus both claims follow from Lemma 2.1, $S_d(x) = \varphi[d]x$, and the fact that x is an odd polynomial. □

Example 2.12. If d and e are primewise congruent modulo m, then $d \equiv e \bmod m$, but primewise congruence is strictly stronger. Theorem 2.11 requires primewise congruence. For example, if $m = 6$ then $7 \equiv 25 \bmod 6$ but $S_7(x) \equiv x^7 - x \equiv 0 \bmod x^6 - 1$ while

$$S_{25}(x) \equiv x^{25} - x^5 \equiv x - x^5 \not\equiv 0 \bmod x^6 - 1.$$

Remark. Suppose p is a prime and d_k is a sequence of natural numbers such that d_k is primewise congruent to d_{k+1} modulo p^k for all $k \geq 1$. Then Theorem 2.11 implies that the sequence $S_{d_k}(x)$ converges in the projective limit $\varprojlim \mathbb{Z}[x]/(x^{p^k} - 1)$ (see Habiro [16].) This limit can be interpreted as an "analytic function on pth power roots of unity." We save the study of these limits for future work.

The next result gives a simple necessary condition for $x^m - 1$ to divide $M_d(x)$.

Theorem 2.13. *If $x^m - 1$ divides $M_d(x)$, then m divides $\varphi(d)$.*

Proof. Consider the $\mathbb{Z}$-module map $\Psi[m] \to \mathbb{Z}/(m)$ determined by $[a] \mapsto a$ for all $a \in \mathbb{N}$. Proposition 2.4 implies that $\varphi[d] \mapsto \varphi(d)$ under this map. Since $x^m - 1$ dividing $M_d(x)$ is equivalent to $\varphi[d] \equiv 0 \bmod [m]$, it follows that $\varphi(d) \equiv 0 \bmod m$ is a necessary condition. □

Example 2.14. Let $d = 15$ and $m = 8$. Then $\varphi(15) = 8$, but

$$S_{15}(x) = x^{15} - x^5 - x^3 + x \equiv x^7 - x^5 - x^3 + x \not\equiv 0 \bmod x^8 - 1.$$

Hence m dividing $\varphi(d)$ is not a sufficient condition.

2.3. **Necklace systems.** We have reduced to studying when $x^m \pm 1$ minimally divides $M_d(x)$ for d squarefree with prime factors only depending on their congruence classes modulo m or $2m$ respectively. The first case to consider is when $d = p$ is prime.

Proposition 2.15. *Let $m, d \geq 1$.*

(1) If d has a prime factor p such that $p \equiv 1 \bmod m$, then $x^m - 1$ divides $M_d(x)$.
(2) $x^m - 1$ minimally divides $M_p(x)$ for a prime p if and only if $p \equiv 1 \bmod m$.

Proof. (1) If $p \equiv 1 \bmod m$, then $[p] \equiv [1] \bmod [m]$ and thus $\varphi[d] \equiv 0 \bmod [m]$ by Proposition 2.4.

(2) Since $S_p(x) = x^p - x = x(x^{p-1} - 1)$ we see that $x^m - 1$ divides $S_p(x)$ if and only if m divides $p - 1$, which is to say that $p \equiv 1 \bmod m$. □

Example 2.16. If $d = 35 = 5 \cdot 7$, then Proposition 2.15 implies that $M_{35}(x)$ is divisible by

$$x^4 - 1 = \Phi_4(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \quad \text{and} \quad x^6 - 1 = \Phi_6(x) \cdot \Phi_3(x) \cdot \Phi_2(x) \cdot \Phi_1(x).$$

In fact we have

$$S_{35}(x) = f(x)\Phi_6(x) \cdot \Phi_4(x) \cdot \Phi_3(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \cdot x,$$

where $f(x) \in \mathbb{Z}[x]$ is an irreducible, non-cyclotomic polynomial of degree 26.

The squarefree d which are a product of more than one prime such that $x^m \pm 1$ minimally divides $M_d(x)$ are more difficult to describe. We can assume that d is squarefree and that no prime divisor of d is congruent to $1 \bmod m$. Theorem 2.11 implies that divisibility by $x^m - 1$ or $x^m + 1$ only depends on the residue classes of the primes dividing d modulo m or $2m$ respectively. We encode these reductions into a combinatorial structure we call a **necklace system** which we show is equivalent to $x^m \pm 1$ dividing $M_d(x)$.

Definition 2.17. Let $m \geq 1$. Note that every residue class modulo m contains either 0, 1, or infinitely many primes. Call a class **empty** if it contains no primes and **isolated** if it contains only one prime. A multiset S of residue classes modulo m is called a **necklace system** (modulo m) if

(1) S contains no empty classes and each isolated class appears at most once.
(2) Under the map $T \mapsto \prod T$ from subsets $T \subseteq S$ to their product residue class in $\mathbb{Z}/(m)$, each class in $a \in \mathbb{Z}/(m)$ is the product $a = \prod T$ for an equal number of T with $|T|$ even and odd.

Note that every congruence class $a \bmod 2m$ has a unique representation as $a \equiv b + cm$ where $0 \leq b < m$ and $c = 0, 1$. Let $c := \operatorname{sgn}(a)$ be the **sign** of a. A multiset S of residue classes modulo m is called a **signed necklace system** (modulo m) if

(1) S contains no empty classes and each isolated class appears at most once.

(2) Under the map $T \mapsto \prod T$ from subsets $T \subseteq S$ to their product residue class in $\mathbb{Z}/(m)$, each class in $a \in \mathbb{Z}/(m)$ is the product $a = \prod T$ for an equal number of T with $|T| + \operatorname{sgn}(\prod T)$ even and odd.

We call a (signed) necklace system S **primitive** if no proper subset of S is a (signed) necklace system.

Theorem 2.18. *Let $m \geq 1$.*

(1) There is a natural equivalence between primitive necklace systems modulo m and primewise congruence classes of minimal d such that $x^m - 1$ divides $M_d(x)$.

(2) There is a natural equivalence between primitive signed necklace systems modulo m and primewise congruence classes of minimal d such that $x^m + 1$ divides $M_d(x)$.

Proof. (1) Suppose that d is squarefree and that $x^m - 1$ divides $M_d(x)$ but not $M_e(x)$ for any proper divisor e of d. Let S be the multiset of congruence classes of the prime divisors of d modulo m. By construction S contains no empty classes and since d is squarefree S contains no isolated class more than once. By Proposition 2.4 and Lemma 2.1 we have

$$\sum_{e|d} \mu(d/e)[e] \equiv \varphi[d] \equiv 0 \bmod [m].$$

Each divisor e of d corresponds to a subset T of S, hence

$$\sum_{T \subseteq S} (-1)^{|S|-|T|} \Big[\prod T\Big] \equiv 0 \bmod [m].$$

The vanishing of this sum is equivalent to the coefficient of $[a]$ being 0 for all congruence classes $a \bmod m$. Each subset T contributes a coefficient of ± 1 according to whether $|T|$ is even or odd. Hence the sum vanishes precisely when for each congruence class $a \bmod m$ there are an equal number of subsets T with $|T|$ even and odd such that $\prod T \equiv a \bmod m$. Thus S is a necklace system modulo m. Since d is assumed to be minimal such that $x^m - 1$ divides $M_d(x)$ it follows that S is primitive.

Given any necklace system S modulo m, the first condition implies that there are distinct primes in each class of S. The above argument shows that $x^m - 1$ divides $M_d(x)$ when d is the product of these primes. If S is primitive, then $x^m - 1$ must minimally divide $M_d(x)$.

(2) We now consider the image of $\varphi[d]$ in $\Psi[m]_\pm$. Recall that $\Psi[m]_\pm$ is $\Psi[2m]$ modulo the relations $[a + m] = -[a]$ for all a. Given a subset T of S the coefficient of $\big[\prod T\big]$ in $\varphi[d] \bmod [m]_\pm$ is $(-1)^{|S|-|T|+\operatorname{sgn}(\prod T)}$, since $\prod T \equiv b + \operatorname{sgn}(\prod T)m \bmod 2m$. The remainder of the argument proceeds as in (1). □

Experimentation leads to many examples of primitive necklace systems, some of which fall into general families. Theorem 2.19 describes several primitive (signed) necklace systems. Note that Proposition 2.15 characterizes all primitive necklace systems with one class.

Theorem 2.19. *Let $m \geq 2$.*

(1) There are no primitive necklace systems S with $|S| = 2$.

(2) If $S = \{a, b\}$ is a primitive signed necklace system modulo m, then

$$\begin{aligned} ab &\equiv 1 + m \bmod 2m \\ a &\equiv b + m \bmod 2m \\ a, b &\not\equiv 1 \qquad \bmod 2m. \end{aligned}$$

For example, $a = m - 1$ and $b = 2m - 1$ is a primitive signed necklace system modulo m.

(3) If $S = \{a, b, c\}$ such that

$$\begin{aligned} a^2 \equiv b^2 \equiv c^2 &\equiv 1 \bmod m \\ abc &\equiv 1 \bmod m \\ a, b, c &\not\equiv 1 \bmod m, \end{aligned}$$

then S is a primitive necklace system modulo m.

Proof. (1) If $S = \{a, b\}$ is a necklace system modulo m, then there has to be a subset T of S with odd cardinality such that $\prod T \equiv 1 \bmod m$ in order to cancel $\prod \emptyset \equiv 1 \bmod m$. That implies either a or b is congruent to $1 \bmod m$. Proposition 2.15 then implies that S is not primitive.

(2) If $S = \{a, b\}$ is a primitive signed necklace system modulo m, then Proposition 2.15 implies that $a, b \not\equiv 1 \bmod 2m$. Thus $T = S$ must be the subset that cancels $\prod \emptyset \equiv 1 \bmod m$. Since $|T| = 2$ is even, we must have $\operatorname{sgn}(ab) = 1$. Hence $ab \equiv 1 + m \bmod 2m$. It follows that $U = \{a\}$ must cancel $V = \{b\}$ which requires that $a \equiv b + m \bmod 2m$. If $a = m - 1$ and $b = 2m - 1$, then these congruence classes are not empty and satisfy the above conditions, hence give a primitive signed necklace system modulo m.

(3) Suppose $S = \{a, b, c\}$ satisfies the congruences

$$\begin{aligned} a^2 \equiv b^2 \equiv c^2 &\equiv 1 \bmod m \\ abc &\equiv 1 \bmod m \\ a, b, c &\not\equiv 1 \bmod m. \end{aligned}$$

Then $abc \equiv 1 \bmod m$ together with

$$\begin{aligned} ab &\equiv c \bmod m \\ ac &\equiv b \bmod m \\ bc &\equiv a \bmod m \end{aligned}$$

imply that S satisfies the second condition for a necklace system. Since all elements of S are units modulo m it follows by Dirichlet's theorem on primes in arithmetic progressions [23, Pg. 167] that these classes contain infinitely many primes. Hence S is a necklace system modulo m. If S were not primitive, then (1) implies that one of a, b, c is $1 \bmod m$. Therefore S is primitive. □

Example 2.20. If $m = 3$, then for any prime $p \equiv 5 \bmod 6$ the set $S = \{2, p\}$ is a primitive signed necklace system modulo 3. This is an example of Theorem 2.19 (2). Hence if $p = 5$, then Theorem 2.18 (2) implies that $x^3 + 1 = \Phi_6(x) \cdot \Phi_2(x)$ divides $S_{10}(x)$. In fact

$$S_{10}(x) = (x^3 + x^2 - 1)\Phi_6(x) \cdot \Phi_4(x) \cdot \Phi_2(x) \cdot \Phi_1(x) \cdot x.$$

Note that $\Phi_6(x)$ divides $S_{10}(x)$ but $x^6 - 1$ does not. This shows that not all cyclotomic factors of necklace polynomials are accounted for by factors of the form $x^m - 1$. Furthermore, if $f(x)$ is any odd polynomial, then Theorem 2.6 implies that

$$x^3 + 1 \text{ divides } f(x^{10}) - f(x^5) - f(x^2) + f(x).$$

Example 2.21. Let $m = 15$. Then $S = \{4, 11, 14\}$ gives an example of the primitive necklace system modulo 15 described in Theorem 2.19 (3). Hence $x^{15} - 1$ divides $M_d(x)$ whenever d is divisible by $6061 = 11 \cdot 19 \cdot 29$.

Example 2.22. Let $m = 10$ and $S = \{3, 13, 19\}$. The following congruences imply that S is a primitive signed necklace system modulo 10,

$$\begin{aligned} 3 \cdot 13 \cdot 19 &\equiv 1 && \bmod 20 \\ 3 &\equiv 3 + 10 && \bmod 20 \\ 19 &\equiv 3 \cdot 13 && \bmod 20 \\ 13 \cdot 19 &\equiv 3 \cdot 19 + 10 && \bmod 20. \end{aligned}$$

This example does not fit into a family described by Theorem 2.19. Theorem 2.18 implies that $x^{10} + 1$ divides $M_d(x)$ whenever d is divisible by $741 = 3 \cdot 13 \cdot 19$.

It would be interesting to know if all primitive (signed) necklace systems can be characterized in some reasonable way. For example, every necklace system can be described in terms of a finite set of

congruences involving m and the elements of S. If we fix the size of S, then there are only finitely many possible congruences describing a necklace system. Which of these have solutions for some m? For infinitely many m? Are there primitive (signed) necklace systems S modulo m with $|S|$ arbitrarily large?

2.4. **Cyclotomic factor conjecture.** Our results in the previous sections show there are structural reasons to expect $M_d(x)$ to have factors of the form $x^m \pm 1$, which in turn give cyclotomic factors of $M_d(x)$. We conjecture that cyclotomic factors of $M_d(x)$ may be accounted for in this way.

Conjecture 2.23. *If $\Phi_m(x)$ divides $M_d(x)$ for some $m, d \geq 1$, then either $x^m - 1$ divides $M_d(x)$ or m is even and $x^{m/2} + 1$ divides $M_d(x)$.*

We have computationally verified Conjecture 2.23 for $1 \leq m \leq 300$ and $1 \leq d \leq 5000$. Theorem 2.9 implies that it suffices to prove Conjecture 2.23 for d squarefree. If $d = p$ is prime, then we can verify Conjecture 2.23 directly: since $S_p(x) = x^p - x$, any cyclotomic factor $\Phi_m(x)$ must divide $x^{p-1} - 1$, hence $x^m - 1$ divides $M_p(x)$. Example 2.20 shows that the $x^{m/2} + 1$ factors are necessary, since $\Phi_6(x)$ divides $M_{10}(x)$ but $x^6 - 1$ does not.

2.5. **Local cyclotomic factors of necklace polynomials.** The product formula for $\varphi[d]$ allows us to determine when $x^m - 1$ divides $S_d(x)$ modulo a prime ℓ. Note that this is equivalent to ℓ dividing $S_d(x)$ modulo $x^m - 1$.

Theorem 2.24. *Let $m \geq 1$ and suppose that $a \bmod m$ has multiplicative order dividing ℓ^k for some prime ℓ and $k \geq 1$. If d has at least $j\ell^k$ distinct prime factors p such that $p \equiv a \bmod m$, then ℓ^j divides $S_d(x) \bmod x^m - 1$.*

Proof. Proposition 2.4 gives the factorization

$$\varphi[d] = \prod_{p|d} [p^{e_p - 1}]([p] - [1]).$$

Our assumption on the divisors of d implies that $\varphi[d]$ has a factor of $([a] - [1])^{j\ell^k}$ modulo $[m]$. Reducing coefficients modulo ℓ we see that

$$([a] - [1])^{\ell^k} \equiv [a^{\ell^k}] - [1] \equiv 0 \bmod \ell.$$

Hence $([a] - [1])^{\ell^k}$ is divisible by ℓ in $\Psi[m]$. Therefore $S_d(x) = \varphi[d]x$ is divisible by ℓ^j modulo $x^m - 1$ by Lemma 2.1 (1). □

Example 2.25. Let $m = 3$ and $\ell = 2$. Consider $d = 2 \cdot 5 \cdot 11 \cdot 17 \cdot 23 \cdot 29 = 1247290$. All six of the prime factors of d are congruent to $-1 \bmod 3$ which has multiplicative order 2. Hence, in the notation of Theorem 2.24, $j = 3$ and it follows that 2^3 divides $S_d(x) \bmod x^3 - 1$. If ω is a primitive 3rd root of unity, then we can also conclude that $S_d(\omega)$ is divisible by 8 in $\mathbb{Z}[\omega]$. The divisibility of Theorem 2.24 is not sharp; for example,

$$S_d(x) \equiv 2^5(x - x^2) \bmod x^3 - 1.$$

2.6. **Functional equations.** The factorization of $\varphi[d]$ given in Proposition 2.4 is equivalent to $S_d(x)$ satisfying a family of functional equations. These identities were discovered by Metropolis and Rota [27, Thm. 3] who proved them combinatorially using necklace interpretation of $M_d(x)$.

Theorem 2.26. *Let $d \geq 1$ and let p be a prime.*

(1) If p does not divide d, then

$$S_{dp}(x) = S_d(x^p) - S_d(x).$$

(2) If p divides d, then

$$S_{dp}(x) = S_d(x^p).$$

Proof. (1) If p does not divide d, then $\varphi[dp] = ([p] - [1])\varphi[d]$. Hence

$$S_{dp}(x) = \varphi[dp]x = ([p] - [1])\varphi[d]x = ([p] - [1])S_d(x) = S_d(x^p) - S_d(x).$$

(2) If p divides d, then $\varphi[dp] = [p]\varphi[d]$. Hence

$$S_{dp}(x) = \varphi[dp]x = [p]\varphi[d]x = [p]S_d(x) = S_d(x^p). \qquad \square$$

Our proof of Theorem 2.26 shows that, more generally, if $f(x) = [f]x$ and $[f] = [g][h]$ factors in Ψ, then $f(x)$ satisfies the functional equation $f(x) = [g]h(x)$.

The two functional equations given in Theorem 2.26 are closely related to functional equations satisfied by cyclotomic polynomials. In particular, let $d \geq 1$ and let p be a prime, then

(1) If p does not divide d, then

$$\Phi_{dp}(x) = \frac{\Phi_d(x^p)}{\Phi_d(x)}.$$

(2) If p divides d, then

$$\Phi_{dp}(x) = \Phi_d(x^p).$$

Taking logarithms we get a sequence $L_d(x) = \log \Phi_d(x)$ of power series satisfying the same functional equations as $S_d(x)$. It follows that

$$\log \Phi_d(x) = \varphi[d] \log \Phi_1(x) = \varphi[d] \log(x - 1). \tag{2.4}$$

To see the connection between $\log \Phi_d(x)$ and $S_d(x)$ more directly recall that

$$S_d(x) = \sum_{e|d} \mu(e) x^{d/e} = \sum_{e|d} \mu(e)[d/e]x.$$

On the other hand

$$\Phi_d(x) = \prod_{e|d} (x^{d/e} - 1)^{\mu(e)},$$

and taking logarithms we find that

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

Theorem 2.6 shows that cyclotomic factors of $M_d(x)$ imply cyclotomic factors of $\varphi[d]f(x)$. This result does not directly apply to $\log \Phi_d(x) = \varphi[d] \log(x-1)$ since $\log(x-1)$ is not a polynomial; convergence issues arise when trying to define the quotient of the power series ring by $x^m - 1$. Nevertheless, we recover the following result.

Theorem 2.27. *Suppose that $m, d > 1$, m does not divide d, and $x^m - 1$ divides $M_d(x)$, then $\frac{x^m-1}{x-1}$ divides $\Phi_d(x) - 1$.*

Proof. If c is the squarefree part of d, then $\Phi_d(x) = \Phi_c(x^{d/c})$ and it follows that all cyclotomic factors of $\Phi_d(x) - 1$ are induced (in the sense of Definition 2.8) from cyclotomic factors of $\Phi_c(x) - 1$. Therefore, by Theorem 2.9, it suffices to prove the result for d squarefree.

Theorem 2.18 implies that $x^m - 1$ dividing $M_d(x)$ is equivalent to the residue classes modulo m of the prime factors of d forming a necklace system S. Since we assume that m does not divide d, all divisors of d are non-zero modulo m. Note that if $a \equiv b \bmod m$, then

$$\frac{x^a - 1}{x - 1} \equiv \frac{x^b - 1}{x - 1} \bmod \frac{x^m - 1}{x - 1}.$$

Consider the product formula for $\Phi_d(x)$ with $d > 1$,

$$\Phi_d(x) = \prod_{e|d} (x^{d/e} - 1)^{\mu(e)} = \prod_{e|d} \left(\frac{x^{d/e} - 1}{x - 1} \right)^{\mu(e)},$$

where the last equality follows from $\sum_{e|d}\mu(e)=0$ whenever $d>1$. Reducing modulo $\frac{x^m-1}{x-1}$ we have

$$\Phi_d(x) \equiv \prod_{1\le a<m}\left(\frac{x^a-1}{x-1}\right)^{n_a} \bmod \frac{x^m-1}{x-1},$$

where for each $1\le a<m$,

$$n_a = \sum_{\substack{e|d \\ d/e\equiv a \bmod m}} \mu(e).$$

The definition of a necklace system implies that $n_a=0$. Therefore $\frac{x^m-1}{x-1}$ divides $\Phi_d(x)-1$. □

Example 2.28. In Example 2.21 we showed that $x^{15}-1$ divides $M_{6061}(x)$. Theorem 2.27 implies that $\frac{x^{15}-1}{x-1}$ divides $\Phi_{6061}(x)-1$.

Example 2.29. Since $\log(x-1)$ is not an odd power series we should not expect factors of $M_d(x)$ of the form x^m+1 to correspond to factors of $\Phi_d(x)-1$. For example, in Example 2.20 we showed that x^3+1 divides $M_{10}(x)$, while $\Phi_{10}(x)-1$ factors as

$$\Phi_{10}(x)-1=(x^2+1)(x-1)x.$$

Theorem 2.27 may be interpreted as giving explicit relations between algebraic units in cyclotomic extensions. If $\frac{x^m-1}{x-1}$ divides $\Phi_d(x)-1$, then

$$\prod_{a\in(\mathbb{Z}/(d))^\times}(\zeta_m-\zeta_d^a)=1,$$

where ζ_m and ζ_d are primitive m and dth roots of unity respectively. For more on cyclotomic units and their relations see Washington [39, Chp. 8] and Sinnott [35].

2.7. **Trace of $M_d(\zeta_m)$.** We conclude this section with a computation of the trace of $M_d(\zeta_m)$, where ζ_m is a primitive mth root of unity. Let $\mathrm{Tr}_m:\mathbb{Q}(\zeta_m)\to\mathbb{Q}$ be the $\mathbb{Q}$-linear trace function defined by $\mathrm{Tr}_m(\alpha):=\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})}\sigma(\alpha)$. Then we define $T(d,m)$ for positive integers $d,m\ge1$ by

$$T(d,m):=\mathrm{Tr}_m(M_d(\zeta_m))\in\mathbb{Q}.$$

Note that $T(d,m)$ is independent of the choice of primitive mth root of unity ζ_m since the trace is invariant under the action of Galois.

Theorem 2.30. *For all $m,d\ge1$ we have*

$$T(d,m):=\mathrm{Tr}_m(M_d(\zeta_m))=\begin{cases}\mu(m/d) & \text{when } d \text{ divides } m\\ 0 & \text{otherwise.,}\end{cases}$$

where μ is the standard Möbius function.

Our proof of Theorem 2.30 uses some results stated in Section 4.

Proof. The cyclotomic identity (see Theorem 4.3) is the following product formula for formal power series with coefficients in $\mathbb{Q}[x]$,

$$\frac{1}{1-xt}=\prod_{d\ge1}\left(\frac{1}{1-t^d}\right)^{M_d(x)}.$$

Substituting $x=\zeta_m^k$ for each k gives

$$\frac{1}{1-t^m}=\prod_{0\le k<m}\frac{1}{1-\zeta_m^k t}=\prod_{0\le k<m}\prod_{d\ge1}\left(\frac{1}{1-t^d}\right)^{M_d(\zeta_m^k)}.$$

Switching the order of the product gives

$$\begin{aligned}\frac{1}{1-t^m} &= \prod_{d\geq 1}\left(\frac{1}{1-t^d}\right)^{\sum_{0\leq k<m} M_d(\zeta_m^k)} \\ &= \prod_{d\geq 1}\left(\frac{1}{1-t^d}\right)^{\sum_{e|m} \mathrm{Tr}_e(M_d(\zeta_e))} \\ &= \prod_{d\geq 1}\left(\frac{1}{1-t^d}\right)^{\sum_{e|m} T(d,e)}.\end{aligned}$$

Lemma 4.2 allows us to compare exponents on both sides of this equation to conclude that

$$\sum_{e|m} T(d,e) = \delta_{d,m},$$

where $\delta_{d,m} = 1$ if and only if $d = m$ and 0 otherwise. Applying Möbius inversion gives our conclusion,

$$T(d,m) = \sum_{e|m} \mu(m/e)\delta_{d,e} = \begin{cases}\mu(m/d) & \text{when } d \text{ divides } m \\ 0 & \text{otherwise.}\end{cases}$$ □

Since $M_d(x)$ is defined over $\mathbb{Q}$, if $M_d(\zeta_m) = 0$ for some primitive mth root of unity ζ_m, then $M_d(x)$ must vanish at all primitive nth roots of unity. Thus, if $\mathrm{Tr}_m(M_d(\zeta_m)) \neq 0$ it follows that $M_d(\zeta_m) \neq 0$. This provides an obstruction for cyclotomic factors of necklace polynomials.

Corollary 2.31. *If d is a divisor of m such that m/d is squarefree, then $M_d(\zeta_m) \neq 0$, or equivalently $\Phi_m(x)$ does not divide $M_d(x)$.*

Proof. If m/d is squarefree, then

$$\mathrm{Tr}_m(M_d(\zeta_m)) = T(d,m) = \mu(m/d) \neq 0.$$

Therefore $M_d(\zeta_m) \neq 0$. □

Theorem 2.30 shows that $M_d(\zeta_m)$ approximately vanishes for all but finitely many d where it presents an obstruction. Corollary 2.32 gives a simple vanishing criterion from Theorem 2.30.

Corollary 2.32. *If d does not divide m and $M_d(\zeta_m)$ is rational, then $M_d(\zeta_m) = 0$.*

Proof. If $M_d(\zeta_m)$ were rational, then $\mathrm{Tr}_m(M_d(\zeta_m)) = \varphi(m)M_d(\zeta_m)$. On the other hand, Theorem 2.30 implies that $\mathrm{Tr}_m(M_d(\zeta_m)) = 0$. Hence $M_d(\zeta_m) = 0$. □

In particular when $m = 1, 2$ the values of $M_d(\pm 1)$ are necessarily rational. Theorem 2.30 specializes in that case to give the following computation.

Corollary 2.33. *Let $M_d(x)$ be the dth necklace polynomial. Then,*

$$M_d(1) = \begin{cases}1 & d = 1 \\ 0 & d > 1.\end{cases} \qquad M_d(-1) = \begin{cases}-1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2.\end{cases}$$

We compute the evaluations $M_d(\pm 1)$ in two other ways as Corollary 4.4 and Corollary 6.6. It is, of course, easy to compute $M_d(\pm 1)$ directly from the explicit formula for $M_d(x)$ (see Lagarias [21, Lem. 2.2] where this evaluation is used in his construction of the z-splitting measure.) These alternative computations of $M_d(\pm 1)$ each offer a new perspective, and in the case of Corollary 6.6 a surprising geometric interpretation.

3. G-NECKLACE POLYNOMIALS

For any finite group G there is a polynomial $M_G(x)$ called the **G-necklace polynomial** such that if $G = C_d$ is the cyclic group of order d, then $M_{C_d}(x) = M_d(x)$ is the classic necklace polynomial. In this section we show that the cyclotomic factor phenomenon studied in Section 2 for $M_d(x)$ extends to $M_G(x)$ for all solvable groups G. Our main result is Theorem 3.2 stated below.

3.1. **Constructing $M_G(x)$.** Let X be a finite set and let X^G be the set of functions from G to X, or equivalently **X-colorings of G**. The group G acts on $f \in X^G$ by $(g \cdot f)(a) := f(g^{-1}a)$. For each subgroup $K \subseteq G$ we define $S_{G,K}(X) \subseteq X^G$ to be the set of colorings with stabilizer K. If K is a subgroup of G, then the subset of all X-colorings of G with stabilizer containing K correspond naturally to X-colorings of the right cosets $K\backslash G$. Thus we have the decomposition G-sets,

$$X^{K\backslash G} \cong \bigsqcup_{K \subseteq H \subseteq G} S_{G,H}(X).$$

If X has x elements, then Möbius inversion with respect to the subgroup lattice of G [37, Prop. 3.7.1] implies that $|S_{G,K}(X)|$ is a polynomial in x which we denote $S_{G,K}(x)$,

$$S_{G,K}(x) := \sum_{K \subseteq H \subseteq G} \mu(K,H) x^{[G:H]}, \tag{3.1}$$

where μ is the Möbius function of the subgroup lattice of G. When $K = 1$ is the trivial subgroup we write $S_G(X) := S_{G,1}(X)$ and

$$S_G(x) := S_{G,1}(x) = \sum_{H \subseteq G} \mu(H) x^{[G:H]}, \tag{3.2}$$

where $\mu(H) := \mu(1,H)$. Let $M_G(X)$ denote the set of G-orbits of elements in $S_G(X)$. The elements of $M_G(X)$ are called **primitive G-necklaces**. Then by the orbit-stabilizer theorem,

$$M_G(x) := |M_G(X)| = \frac{1}{|G|} S_G(x).$$

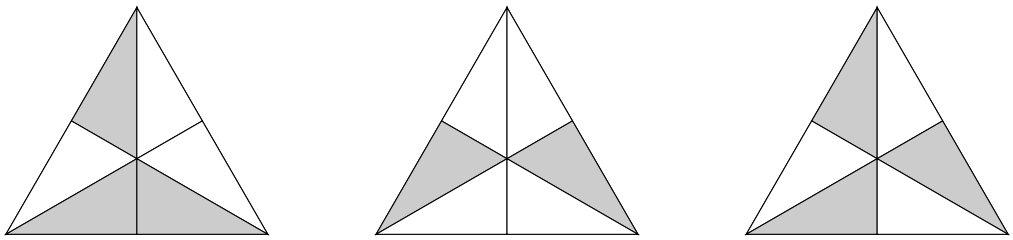
$M_G(x)$ is called the **G-necklace polynomial**. When $G = C_d$ is the cyclic group of order d, (3.2) specializes to the formula for $M_d(x)$

$$M_{C_d}(x) = \frac{1}{|C_d|} \sum_{H \subseteq C_d} \mu(H) x^{[C_d:H]} = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e} = M_d(x).$$

Hence the G-necklace polynomials generalize the classic necklace polynomials and $S_G(x) = |G| M_G(x)$ generalizes $S_d(x) = d M_d(x)$.

Dress and Siebeneicher [6] introduced the G-necklace polynomials in the course of constructing an isomorphism between the G-necklace algebra and the G-Burnside-Witt ring. In their work G is allowed to be any profinite group, but for simplicity we only consider finite groups. Oh [29] studied the G-necklace polynomials in depth, generalizing the functional identities (Theorem 2.26) established by Metropolis and Rota [27] for the classic necklace polynomials $M_d(x)$ to the G-necklace polynomials $M_G(x)$.

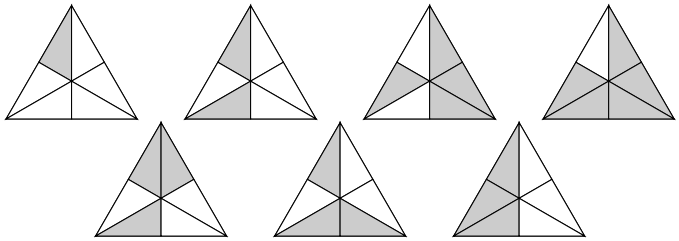
Example 3.1. Let $G = S_3$ be the 3rd symmetric group. If we divide an equilateral triangle into six regions by connecting each edge to the opposite vertex, then S_3 acts acts freely and transitively by reflections on the regions. Hence an X-coloring of the regions gives an element of X^{S_3}. The figure below illustrates 2-colorings of S_3 with stabilizers $H = 1, \langle(12)\rangle, \langle(123)\rangle$ respectively.



Recall that the Möbius function of a poset P is defined so that for each interval $[a, c]$ in P we have $\sum_{a\leq b\leq c} \mu(a, b) = 0$ unless $a = c$ in which case $\mu(a, a) = 1$. These conditions uniquely determine μ if P has finite intervals. Using (3.2) we compute

$$M_{S_3}(x) = \frac{1}{6}(x^6 - 3x^3 - x^2 + 3x).$$

Therefore there are $7 = M_{S_3}(2)$ primitive 2-colorings of S_3. Representatives of these colorings are depicted below.



3.2. **Cyclotomic factors of $M_G(x)$.** Recall the Frobenius algebra Ψ defined in Section 2.1 as the $\mathbb{Z}$-algebra generated by $[m]$ for $m \in \mathbb{N}$ such that $[m][n] = [mn]$. Theorem 3.2 shows how an expression of G as a solvable extension of a subgroup K corresponds to a factorization of $[S_G]$ in Ψ and hence to a functional equation relating $S_G(x)$ and $S_K(x)$.

Theorem 3.2. *Suppose G is a finite group with subgroup K and a chain of subgroups*

$$K = N_0 \lhd N_1 \lhd \dots N_k \lhd N_{k+1} = G$$

such N_{i+1}/N_i is cyclic of prime order p_i. Let c_i be the number of non-trivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$.

(1) Let $S_G(x)$ be the polynomial defined in (3.2)*, then*

$$S_G(x) = \Big(\prod_{i=0}^{k} [p_i] - c_i[1]\Big) S_K(x).$$

(2) If $c_i = 1$, then $x^{p_i-1} - 1$ divides $S_G(x)$. If G is solvable and $K = 1$, then $c_0 = 1$ and this implies that $S_G(x)$ has cyclotomic factors.

(3) If $c_i > 1$, then $S_G(x) \bmod [p_i - 1]$ is divisible by $c_i - 1$.

We first prove Lemma 3.3. This result, due to Oh [29, Thm. 3.6], generalizes an identity for $M_d(x)$ first proved by Metropolis and Rota [27, Thm. 3].

Lemma 3.3. *If $K \subseteq G$ is a subgroup, then*

$$S_K(x^{[G:K]}) = \sum_{K\cap H=1} S_{G,H}(x).$$

Proof. The result follows by counting the elements of the restriction $\mathrm{Res}^G_K(X^G)$ with trivial stabilizer in two ways.

First note that as a left K-set G decomposes into $[G : K]$ copies of K corresponding to the right cosets $K\backslash G$. Hence we have the K-set isomorphisms,

$$\mathrm{Res}^G_K(X^G) \cong (X^K)^{[G:K]} \cong (X^{[G:K]})^K.$$

Therefore the number of elements of $\mathrm{Res}^G_K(X^G) \cong (X^{[G:K]})^K$ with trivial stabilizer is, by definition, $S_K(x^{[G:K]})$.

On the other hand, if f is an element of X^G with stabilizer H, then the stabilizer of f in $\mathrm{Res}^G_K(X^G)$ is $K \cap H$. Thus

$$S_K(x^{[G:K]}) = \sum_{K\cap H=1} S_{G,H}(x). \qquad \square$$

Proof of Theorem 3.2. (1) Applying Lemma 3.3 to $G = N_{i+1}$ with subgroup $K = N_i$ we have

$$S_{N_i}(x^{p_i}) = \sum_{N_i\cap H=1} S_{N_{i+1},H}(x),$$

hence

$$S_{N_{i+1}}(x) = S_{N_i}(x^{p_i}) - \sum_{\substack{N_i\cap H=1\\ H\neq 1}} S_{N_{i+1},H}(x). \tag{3.3}$$

Since $N_i \lhd N_{i+1}$ is a normal subgroup with cyclic quotient of prime order, any nontrivial subgroup $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$ must be cyclic of order p_i. By (3.1) we have

$$S_{N_{i+1},H}(x) = \sum_{H\subseteq J\subseteq N_{i+1}} \mu(H,J)x^{[N_{i+1}:J]}.$$

The second isomorphism theorem for groups [23, Pg. 17] implies that the interval of subgroups between H and N_{i+1} is isomorphic as a lattice to the subgroups of N_i and that $[N_{i+1} : J] = [N_i, N_i \cap J]$. Hence

$$S_{N_{i+1},H}(x) = \sum_{1\subseteq J\subseteq N_i} \mu(J)x^{[N_i:J]} = S_{N_i}(x).$$

If c_i is the number of nontrivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$, then (3.3) simplifies to

$$S_{N_{i+1}}(x) = S_{N_i}(x^{p_i}) - c_i S_{N_i}(x) = ([p_i] - c_i[1])S_{N_i}(x),$$

where $[p_i] - c_i[1] \in \Psi$ is an element of the Frobenius algebra. The product formula then follows by induction on i.

(2) If $c_i = 1$, then the factor $[p_i] - c_i[1]$ in the product formula for $S_G(x)$ vanishes in $\Psi[p_i - 1]$. Hence by Lemma 2.1 (1) it follows that $x^{p_i-1} - 1$ divides $S_G(x)$. If G is solvable and $K = N_0 = 1$, then N_1 is the only nontrivial subgroup of N_1 and $N_0 \cap N_1 = 1$. Hence $c_0 = 1$ and $S_G(x)$ is divisible by $x^{p_i-1}-1$.

(3) This follows from (2) after reducing the coefficients in Ψ modulo $c_i - 1$. $\square$

Example 3.4. If $G = C_{p^e}$ is cyclic of order p^e with $e > 1$ and $1 = N_0 \lhd N_1 \lhd \ldots \lhd N_e = C_{p^e}$ is a composition series, then each $p_i = p$ and $c_i = 0$ for all i except $c_0 = 1$. In this case Theorem 3.2 (1) simplifies to Proposition 2.4,

$$S_{C_{p^e}}(x) = ([p^e] - [p^{e-1}])x = \varphi[p^e]x.$$

Example 3.5. If $G = D_{2d}$ is the dihedral group of order $2d$, then the cyclic group $C_d \lhd D_{2d}$ is a normal subgroup of index 2. There are d elements of order 2 in D_{2d} not contained in C_d, hence Theorem 3.2 (1) implies that

$$S_{D_{2d}}(x) = ([2] - d[1])S_d(x) = S_d(x^2) - dS_d(x) = \sum_{e|d} \mu(e)(x^{2d/e} - dx^{d/e}).$$

Lemma 2.1 (1) implies that $x^m - 1$ divides $S_{D_{2d}}(x)$ whenever $x^m - 1$ divides $S_d(x)$. This does not hold for factors of $S_d(x)$ of the form $x^m + 1$ since 2 is even. For instance, in Example 2.20 we saw that $x^3 + 1$ divides $S_{10}(x)$, but

$$S_{D_{20}}(x) = x^{20} - 11x^{10} + 10x^5 - x^4 + 11x^2 - 10x = f(x)(x^2 + 1)(x + 1)(x - 1)x,$$

where $f(x)$ is an irreducible, non-cyclotomic polynomial of degree 15, hence $S_{D_{20}}(x)$ is not divisible by x^3+1.

Example 3.6. If $G = Q_8$ is the quaternion group, then Q_8 has a cyclic normal subgroup N of order 4 such that there are no nontrivial subgroups of Q_8 which intersect N trivially. Thus Theorem 3.2 (1) and Proposition 2.4 imply that

$$S_{Q_8}(x) = [2]S_4(x) = x^8 - x^4 = x^4(x^2+1)(x+1)(x-1).$$

Example 3.7. If G is a finite abelian group, then G is a direct product of cyclic groups [22, Thm. 8.2],

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}.$$

Combining Theorem 3.2 (1) and Proposition 2.4 we find that

$$S_G(x) = \varphi[d_1]\varphi[d_2]\cdots\varphi[d_k]x,$$

hence if $x^m - 1$ divides $S_{d_i}(x)$ for some i, then $x^m - 1$ divides $S_G(x)$ by Lemma 2.1.

3.3. **Möbius function of a solvable extension.** Combining the explicit formula for $S_G(x)$ in (3.2) with the functional equations in Theorem 3.2 (1) we derive a relation between the value of the Möbius function of a group K and of a solvable extension G of K. An essentially equivalent version of this formula appears in Hawkes, Isaacs, Özaydin [19, Cor. 3.4]. They attribute this formula to Gaschütz [13], however we were unable to find an explicit reference to it in his paper.

Theorem 3.8. *If G is a group with normal subgroup K such that G/K is solvable with composition series*

$$1 = N_0 \lhd N_1 \lhd \ldots \lhd N_{k+1} = G/K,$$

such that $[N_{i+1} : N_i] = p_i$ is prime with c_i non-trivial subgroups $H \subseteq N_{i+1}$ such that $N_i \cap H = 1$, then

$$\mu(G) = (-1)^{k+1}c_0c_1\cdots c_k\mu(K).$$

Proof. Recall the formula (3.2) for $S_G(x)$,

$$S_G(x) = \sum_{H\subseteq G} \mu(H)x^{[G:H]}.$$

The coefficient of the linear term of $S_G(x)$ is $\mu(G)$. On the other hand Theorem 3.2 (1) gives the relation

$$S_G(x) = \Big(\prod_{i=0}^{k}[p_i] - c_i[1]\Big)S_K(x).$$

Comparing linear terms on each side of this equation we get

$$\mu(G) = (-1)^{k+1}c_0c_1\cdots c_k\mu(K). \qquad \square$$

When G is solvable and $K = 1$ Theorem 3.8 simplifies to

$$\mu(G) = (-1)^{k+1}c_0c_1\cdots c_k,$$

which appears in [19, Cor. 3.4].

Numerical experiments suggest that abelian composition factors of a group G account for all the cyclotomic factors of $M_G(x)$. It could be interesting to know what can be said about the factorizations of $M_G(x)$ more generally. One could extend the notion of a necklace system from Definition 2.17 to combinatorially encode cyclotomic factors of $M_G(x)$ for solvable G, but we choose not to pursue that here.

4. Combinatorial Euler Products

Our main tool for the results in Sections 5 and 6 is a product formula for unital formal power series which we call the **combinatorial Euler product**. In this section we review the existence and uniqueness of combinatorial Euler products (Lemma 4.2); discuss their relation to number theory, combinatorics, and Witt vectors; and apply them to the evaluation of necklace polynomials (Corollary 4.4.)

4.1. Existence and uniqueness.

Definition 4.1. A commutative ring R is called a **binomial ring** if

(1) R is torsion free as an abelian group ($ma = 0$ with $m \in \mathbb{Z}$ and $a \in A$ implies $m = 0$ or $a = 0$,) and
(2) For each $a \in R$ and $n \geq 0$, $\binom{a}{n} = \frac{1}{n!}a(a-1)(a-2)\cdots(a-n+1) \in R$.

Binomial rings were defined by Philip Hall [17] in his study of nilpotent groups. See Elliott [7] for an overview and further references on binomial rings. Examples of binomial rings include any localization of $\mathbb{Z}$, any $\mathbb{Q}$-algebra, and the ring of integer valued polynomials in $\mathbb{Q}[x]$.

Let

$$\left(\!\binom{x}{n}\!\right) := \frac{1}{n!}x(x+1)(x+2)\cdots(x+n-1) = \binom{x+n-1}{n}.$$

Recall that $\left(\!\binom{x}{n}\!\right)$ counts the number of subsets of size n chosen from a set of size x with repetition. The second condition of a binomial ring is equivalent to $\left(\!\binom{a}{n}\!\right) \in R$ for each $a \in R$ and $n \geq 0$ by the **combinatorial reciprocity identity** (see Stanley [36],)

$$\left(\!\binom{x}{n}\!\right) = (-1)^n\binom{-x}{n}. \tag{4.1}$$

Let R be a binomial ring and let $\Lambda(R) := 1 + tR[\![t]\!]$ be the set of unital formal power series with coefficients in R. We use $\left(\!\binom{x}{n}\!\right)$ to define an exponential action of R on certain elements of $\Lambda(R)$. In particular,

$$\left(\frac{1}{1-t}\right)^a := \sum_{n\geq 0}\left(\!\binom{a}{n}\!\right)t^n.$$

By (4.1) this identity is equivalent to the binomial theorem.

Lemma 4.2 is well-known in the context of formal power series, symmetric functions, and the theory of Witt vectors but is typically not stated in the generality which we technically require.[1] We prove it here for completeness.

Lemma 4.2. *For any binomial ring R and any sequence $a_d \in R$ for $d \geq 0$ such that $a_0 = 1$ there exists a unique sequence $b_j \in R$ for $j \geq 1$ such that the following identity holds in $\Lambda(R)$.*

$$\sum_{d\geq 0} a_d t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{b_j}. \tag{4.2}$$

Furthermore (4.2) *is equivalent to*

$$a_d = \sum_{\lambda\vdash d} b_\lambda$$

where for a partition $\lambda = (1^{m_1}2^{m_2}\cdots)$

$$b_\lambda := \prod_{j\geq 1}\left(\!\binom{b_j}{m_j}\!\right). \tag{4.3}$$

[1] Metropolis and Rota [27, Sec. 6, Prop. 1] mistakenly state this result for an arbitrary commutative ring; the correct version in terms of binomial rings appears in Elliott [7, Prop. 10.1].

Proof. The right hand side of (4.2) expands as

$$\prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{b_j}=\prod_{j\geq 1}\sum_{m\geq 0}\left(\!\binom{b_j}{m}\!\right)t^{mj}=\sum_{d\geq 0}\sum_{\lambda\vdash d}b_\lambda t^d.$$

We show by induction on d that there exists a uniquely determined sequence b_j such that for all $d\geq 1$,

$$a_d=\sum_{\lambda\vdash d}b_\lambda.$$

For $d=1$ there is only partition λ and thus $a_1=b_1$. Now suppose that $d>1$ and that we have shown b_j is uniquely determined for $j<d$. Then

$$b_d=a_d-\sum_{\substack{\lambda\vdash d\\ \lambda\neq(d)}}b_\lambda.$$

If $\lambda\neq(d)$, then all parts of λ have size $j<d$ hence b_d is uniquely determined by our induction hypothesis. □

We call (4.2) the **combinatorial Euler product** factorization of the series $f(t)=\sum_{d\geq 0}a_dt^d$. This terminology was chosen to highlight a useful analogy which we discuss below.

4.2. **Combinatorial Euler products in number theory.** Classically an Euler product refers to a factorization of a Dirichlet series associated to prime ideals in a ring of integers. The essential example is the Euler product for the Riemann zeta function,

$$\zeta(s):=\sum_{n\geq 1}\frac{1}{n^s}=\prod_p\frac{1}{1-\frac{1}{p^s}}.$$

If V is a variety defined over a finite field $\mathbb{F}_q$, then the Hasse-Weil zeta function $\zeta_V(t)\in\Lambda(\mathbb{Z})$ associated to V is defined by

$$\zeta_V(t):=\exp\left(\sum_{d\geq 1}|V(\mathbb{F}_{q^d})|\frac{t^d}{d}\right)=\sum_{d\geq 0}|\mathrm{Sym}^d(V)(\mathbb{F}_q)|t^d,$$

where $\mathrm{Sym}^d(V)$ is the dth symmetric power of V. The Euler product for $\zeta_V(t)$ takes the form

$$\zeta_V(t)=\prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_j(V)},$$

where $M_j(V)$ is the number of transitive Frobenius orbits on $V(\overline{\mathbb{F}}_q)$ with size j. This Euler product is an example of a combinatorial Euler product and is our motivation for the name.

4.3. **Combinatorial Euler products in combinatorics.** The combinatorial aspect of the combinatorial Euler product relates in part to an analogy between integers and partitions discussed in the paper [14] by Granville and further elaborated in the book [1] by Arratia, Barbour, and Tavaré: Just as every integer has a unique prime factorization, every partition has a unique "factorization" as $\lambda=(1^{m_1}2^{m_2}\cdots)$. The "primes" in this setting are the natural numbers $j\geq 1$. The analog of the Riemann zeta function is the partition generating function; its combinatorial Euler product decomposition is the well-known identity

$$\sum_{d\geq 0}p(d)t^d=\prod_{j\geq 1}\left(\frac{1}{1-t^j}\right),$$

where $p(d)$ is the number of partitions of d.

4.4. **Necklace rings and Witt vectors.** For any commutative ring R Grothendieck [15] defined a ring structure on the unital formal power series $\Lambda(R)$. The addition in $\Lambda(R)$ is multiplication $f(t) \oplus g(t) := f(t)g(t)$ and the product is uniquely determined by

$$\frac{1}{1-at} \otimes \frac{1}{1-bt} := \frac{1}{1-abt},$$

where $a, b \in R$. The ring $\Lambda(R)$ is isomorphic to the ring of big Witt vectors $W(R)$. See the unpublished notes of Lenstra [24] for a nice proof that $\Lambda(R)$ forms a ring with these operations and that $\Lambda(R)$ is canonically isomorphic to $W(R)$ as it is classically defined.

Metropolis and Rota [27, Sec. 6, Prop. 1] use the combinatorial Euler product formula to give an isomorphism between $\Lambda(\mathbb{Z})$ with Grothendieck's ring structure and the *necklace ring* $\mathrm{Nr}(\mathbb{Z})$. Dress and Siebeneicher [6] give a combinatorial construction of the necklace ring $\mathrm{Nr}(\mathbb{Z})$ as the Burnside ring of almost finite C-sets $\widehat{\Omega}(C)$, where C is the infinite cyclic group. A set X with an action of C is called an *almost finite C-set* if for each subgroup C^j of C, the set $M_j(X)$ of orbits with stabilizer C^j is finite. Then the Burnside ring of almost finite C-sets is the complete topological ring generated by classes $[X]$ for each isomorphism class of almost finite C-set X with relations

$$[X \sqcup Y] = [X] + [Y] \qquad [X \times Y] = [X][Y]$$

when X and Y are almost finite C-sets. If $[j] \in \widehat{\Omega}(\mathbb{Z})$ represents the class of the transitive C-set with j elements, then each $[X] \in \widehat{\Omega}(\mathbb{Z})$ has a unique expression as

$$[X] = \sum_{j \geq 1} |M_j(X)|[j].$$

The isomorphism between $\widehat{\Omega}(C)$ and $\Lambda(\mathbb{Z})$ is given by

$$[X] \longmapsto \prod_{j \geq 1} \left(\frac{1}{1-t^j}\right)^{|M_j(X)|}, \tag{4.4}$$

bringing us again to a combinatorial Euler product.

There is a close connection between this interpretation and the Euler product formula for the Hasse-Weil zeta function: if V is a variety over $\mathbb{F}_q$, then $V(\overline{\mathbb{F}}_q)$ is an almost finite C-set, where the cyclic action is given by the Frobenius automorphism of V. Hence $[V(\overline{\mathbb{F}}_q)] \in \widehat{\Omega}(\mathbb{Z})$ and the map (4.4) sends $[V(\overline{\mathbb{F}}_q)]$ to $\zeta_V(t)$.

4.5. **Cyclotomic identity.** The necklace polynomials $M_d(x)$ arise in relation to an important combinatorial Euler product formula known as the **cyclotomic identity**.

Theorem 4.3 (Cyclotomic identity)**.** *The following identity holds in $\Lambda(\mathbb{Q}[x])$,*

$$\frac{1}{1-xt} = \prod_{j \geq 1} \left(\frac{1}{1-t^j}\right)^{M_j(x)}.$$

When $x = q$ is a prime power, Theorem 4.3 reduces to the Euler product formula for Hasse-Weil zeta function of $\mathbb{A}^1$ over $\mathbb{F}_q$. One may interpret this formula as an expression of the unique factorization of polynomials in $\mathbb{F}_q[x]$ into irreducibles. There are many proofs of the cyclotomic identity from different perspectives including number theory [32, Pg. 13], combinatorics [27, Sec. 5], and Lie theory [31, Lem. 3.2].

We close this section by applying the uniqueness of combinatorial Euler products (Lemma 4.2) to give a second computation of the values $M_d(\pm 1)$ for all $d \geq 1$.

Corollary 4.4. *Let $M_d(x)$ be the dth necklace polynomial. Then,*

$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases} \qquad M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$

Proof. (1) Evaluating the cyclotomic identity at $x = 1$ we have

$$\frac{1}{1-t} = \prod_{j \geq 1} \left(\frac{1}{1-t^j} \right)^{M_j(1)}.$$

On the other hand, by Lemma 4.2 we can compare exponents on both sides of this equation to see that

$$M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases}$$

(2) Evaluating the cyclotomic identity at $x = -1$ we have

$$\frac{1}{1+t} = \prod_{j \geq 1} \left(\frac{1}{1-t^j} \right)^{M_j(-1)}.$$

The left hand side can also be written

$$\frac{1}{1+t} = \frac{1-t}{1-t^2} = \left(\frac{1}{1-t} \right)^{-1} \left(\frac{1}{1-t^2} \right).$$

Comparing exponents with Lemma 4.2 we conclude

$$M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$ □

In Section 5 we generalize the cyclotomic identity to a one parameter family of identities associated to the **higher necklace polynomials** $M_{d,n}(x)$. Our proof of Corollary 4.4 generalizes to the evaluation of higher necklace polynomials at certain roots of unity, including ± 1 (see Theorem 5.6.)

5. Higher Necklace Polynomials

Let K be a field and consider the polynomial ring $K[x_1, x_2, \ldots, x_n]$ in n variables.

Definition 5.1. A **monic polynomial** is a $K^\times$-orbit of non-zero polynomials in $K[x_1, x_2, \ldots, x_n]$. Let $\mathrm{Poly}_{d,n}(K)$ be the space of total degree d monic polynomials in $K[x_1, x_2, \ldots, x_n]$. Let $\mathrm{Irr}_{d,n}(K) \subseteq \mathrm{Poly}_{d,n}(K)$ be the subspace of K-irreducible polynomials.

In this section we study $\mathrm{Poly}_{d,n}(K)$ and $\mathrm{Irr}_{d,n}(K)$ when $K = \mathbb{F}_q$ is a finite field. Section 6 considers these spaces when $K = \mathbb{R}$ or $\mathbb{C}$. To keep track of the subscripts d and n note that d stands for the **d**egree of the polynomials and n stands for the **n**umber of variables.

If $K = \mathbb{F}_q$ is a finite field, then $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a finite set. In [20, Lem. 2.1] we showed that the cardinality of $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a polynomial in q with rational coefficients. Note that $n = 1$ corresponds to the space of univariate polynomials and in that case $|\mathrm{Irr}_{d,1}(\mathbb{F}_q)| = M_d(q)$.

Definition 5.2. Suppose that $d, n \geq 1$.

(1) Let $P_{d,n}(x)$ be the polynomial with rational coefficients such that for any prime power q

$$P_{d,n}(q) = |\mathrm{Poly}_{d,n}(\mathbb{F}_q)|.$$

(2) The **higher necklace polynomial** $M_{d,n}(x)$ is the polynomial with rational coefficients such that for any prime power q,

$$M_{d,n}(q) = |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|.$$

The polynomial $P_{d,n}(x)$ is given explicitly by

$$P_{d,n}(x) := \frac{x^{\binom{d+n}{n}} - x^{\binom{d+n-1}{n}}}{x-1}, \tag{5.1}$$

(see [20, Lem. 2.1].) When the number of variables is $n = 1$ the higher necklace polynomials specialize to the classic necklace polynomials

$$M_{d,1}(x) = M_d(x) = \frac{1}{d}\sum_{e|d} \mu(e) x^{d/e}. \tag{5.2}$$

When $n > 1$ there is no known explicit formula for $M_{d,n}(x)$ analogous to (5.2). This makes it challenging to study the higher necklace polynomials directly. Instead we approach $M_{d,n}(x)$ indirectly using the following family of combinatorial Euler products.

Theorem 5.3. *For each $n \geq 1$ the following identity holds in $\Lambda(\mathbb{Q}[x]) := 1 + t\mathbb{Q}[x][\![t]\!]$,*

$$\sum_{d\geq 0} P_{d,n}(x) t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{M_{j,n}(x)}. \tag{5.3}$$

Proof. This identity is equivalent to $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ having unique factorization. More explicitly, for each partition $\lambda = (1^{m_1} 2^{m_2} \cdots)$ of d define $P_{\lambda,n}(x)$ by

$$P_{\lambda,n}(x) := \prod_{j\geq 1} \left(\!\!\binom{M_{j,n}(x)}{m_j}\!\!\right).$$

The degrees of the $\mathbb{F}_q$-irreducible factors of a polynomial $f \in \mathrm{Poly}_{d,n}(\mathbb{F}_q)$ form a partition $\lambda \vdash d$ which we call the **factorization type** of f. Thus $P_{\lambda,n}(q)$ is the number of elements of $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ with factorization type λ. Since every element of $\mathrm{Poly}_{d,n}(\mathbb{F}_q)$ factors uniquely into $\mathbb{F}_q$-irreducibles, we have for each prime power q

$$P_{d,n}(q) = \sum_{\lambda \vdash d} P_{\lambda,n}(q). \tag{5.4}$$

Lemma 4.2 shows that (5.4) is equivalent to

$$\sum_{d\geq 0} P_{d,n}(q) t^d = \prod_{j\geq 1} \left(\frac{1}{1-t^j}\right)^{M_{j,n}(q)}.$$

Finally, since this holds for all prime powers q the identity must hold as polynomials in x. □

Theorem 5.3 appears in the proof of [20, Thm. 2.3] where we used it to study the x-adic convergence of $M_{d,n}(x)$ for d fixed as $n \to \infty$. The advantage of Theorem 5.3 is that it allows us to study the implicitly defined polynomial sequence $M_{d,n}(x)$ by way of the explicitly known polynomial sequence $P_{d,n}(x)$. When $n = 1$, $P_{d,n}(x) = x^d$ and Theorem 5.3 specializes to the classic cyclotomic identity (Theorem 4.3.)

The cyclotomic factor phenomenon studied for $M_d(x)$ in Section 2 extends, in part, to the entire family $M_{d,n}(x)$ of higher necklace polynomials. When $n > 1$ the polynomials $M_{d,n}(x)$ do not appear to satisfy functional equations similar to those satisfied by $M_d(x)$ and $M_G(x)$. This is reflected in the fact that for each fixed $n > 1$ we see fewer distinct cyclotomic factors as d varies. Our main result for this section is Theorem 5.6.

Definition 5.4. Let $b \geq 2$ and $n \geq 1$ be integers. A **balanced base b expansion of** n is an expression

$$n = b^{k_1} - b^{k_2} + b^{k_3} - \ldots + b^{k_{i-1}} - b^{k_i},$$

where $k_1 > k_2 > k_3 > \ldots > k_i \geq 0$ is a decreasing sequence of integers and the coefficients on the right hand side alternate between ± 1. Equivalently, n has a balanced base b expansion if all of the base b digits of n are 0 or $b-1$,

$$n = (b-1)b^{\ell_1} + (b-1)b^{\ell_2} + \ldots + (b-1)b^{\ell_j}.$$

In that case, the balanced base b expansion of n is gotten by expanding each $(b-1)b^k = b^{k+1} - b^k$ and collecting coefficients. Not every $n \geq 1$ has a balanced base b expansion, but when they do exist they are unique.

Example 5.5. Every positive integer has a balanced base 2 expansion. For example the balanced base 2 expansion of $n = 13$ is

$$13 = 2^4 - 2^2 + 2^1 - 1.$$

Theorem 5.6. *Let p be a prime and let $n \geq 1$ be an integer such that*

$$n = \sum_{k \geq 0} b_k p^k$$

is the balanced base p expansion of n. If ζ_p is a primitive pth root of unity, then

$$M_{d,n}(\zeta_p) = \begin{cases} b_k & \text{if } d = p^k \\ 0 & \text{otherwise.} \end{cases}$$

Thus it follows that $\Phi_p(x)$ divides $M_{d,n}(x)$ for all but finitely many $d \geq 1$ whenever n has a balanced base p expansion.

Before proving Theorem 5.6 we prove two lemmas. If $m \geq 0$ is an integer, let

$$[m]_x := \frac{x^m - 1}{x - 1} = x^{m-1} + x^{m-2} + \ldots + x + 1.$$

Lemma 5.7. *If ζ is a non-trivial nth root of unity, then $[m]_\zeta$ depends only on m modulo n.*

Proof. If ζ is a nontrivial nth root of unity, then

$$[n]_\zeta = \zeta^{n-1} + \zeta^{n-2} + \ldots + \zeta + 1 = 0.$$

If $m = an + b$, then

$$\begin{aligned} [m]_x &= \frac{x^{an+b} - 1}{x - 1} \\ &= x^b \cdot \frac{x^{an} - 1}{x - 1} + \frac{x^b - 1}{x - 1} \\ &= x^b \cdot \frac{x^{an} - 1}{x^n - 1} \cdot \frac{x^n - 1}{x - 1} + \frac{x^b - 1}{x - 1} \\ &= x^b [a]_{x^n} [n]_x + [b]_x. \end{aligned}$$

Evaluating at $x = \zeta$ gives

$$[m]_\zeta = [b]_\zeta.$$

□

Lemma 5.8 is known as Lucas' congruence, due to Èdouard Lucas [25]. See Fine [11] for a slick modern proof.

Lemma 5.8. *If p is a prime and*

$$\begin{aligned} m &= a_k p^k + a_{k-1} p^{k-1} + \ldots + a_1 p + a_0 \\ n &= b_k p^k + b_{k-1} p^{k-1} + \ldots + b_1 p + b_0 \end{aligned}$$

are the base p expansions of the natural numbers m and n (without assuming the leading coefficients are non-zero), then

$$\binom{m}{n} \equiv \binom{a_k}{b_k}\binom{a_{k-1}}{b_{k-1}}\cdots\binom{a_1}{b_1}\binom{a_0}{b_0} \bmod p.$$

We now prove Theorem 5.6.

Proof of Theorem 5.6. The polynomial $P_{d,n}(x)$ may be expressed as

$$P_{d,n}(x) = \frac{x^{\binom{d+n}{n}} - x^{\binom{d+n-1}{n}}}{x-1} = \left[\binom{d+n}{n}\right]_x - \left[\binom{d+n-1}{n}\right]_x. \tag{5.5}$$

Suppose that n has a balanced base p expansion and let ζ be a non-trivial pth root of unity. Then by Theorem 5.3,

$$\sum_{d\geq 0} P_{d,n}(\zeta)t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_{j,n}(\zeta)}. \tag{5.6}$$

We evaluate $M_{d,n}(\zeta)$ by expressing the left hand side of (5.6) as a combinatorial Euler product in another way and then using the uniqueness of Lemma 4.2. Towards that end, let $Q(t) \in \Lambda(\mathbb{Q}(\zeta))$ be defined by

$$Q(t) := \sum_{d\geq 0}\left[\binom{d+n}{n}\right]_\zeta t^d.$$

Then by (5.5)

$$\begin{aligned}
\sum_{d\geq 0} P_{d,n}(\zeta)t^d &= \sum_{d\geq 0}\left(\left[\binom{d+n}{n}\right]_\zeta - \left[\binom{d+n-1}{n}\right]_\zeta\right)t^d \\
&= \sum_{d\geq 0}\left[\binom{d+n}{n}\right]_\zeta t^d - t\sum_{d\geq 1}\left[\binom{d+n-1}{n}\right]_\zeta t^{d-1} \\
&= Q(t) - tQ(t) \\
&= (1-t)Q(t).
\end{aligned}$$

Next we determine the coefficients of $Q(t)$. Say positive integers d and n are *p-complementary* if there is no p^k with a non-zero coefficient in the base p expansions of both d and n. If d and n are not p-complementary, suppose p^k is the smallest power of p common to the base p expansions of d and n. Then the coefficient of p^k in $d+n$ is 0 since

(1) the coefficient of p^k in n is $p-1$ by our assumption that n has a balanced base p expansion,
(2) the coefficient of p^k in d is at least 1, and
(3) the minimality of k implies there are no carries for smaller power p in the sum.

Thus Lucas' congruence (Lemma 5.8) implies that if d and n are not p-complementary, then

$$\binom{d+n}{n} \equiv 0 \bmod p$$

since the factor corresponding to p^k will be 0. Therefore, if d and n are not p-complementary, then by Lemma 5.7 we have

$$\left[\binom{d+n}{n}\right]_\zeta = 0.$$

Suppose d and n are p-complementary. Then for each k, the coefficient of p^k in the base p expansion of n is either 0 or $p-1$ by the assumption that n has a balanced base p expansion. In the first case the

factor corresponding to p^k in Lucas' congruence is $\binom{d_k}{0} = 1$ where d_k is the coefficient of p^k in the base p expansion of d. In the latter case, note that if $0 \leq a < p$, then

$$\binom{a}{p-1} = \begin{cases} 0 & \text{if } a < p-1 \\ 1 & \text{if } a = p-1 \end{cases}. \tag{5.7}$$

Then Lucas' congruence and (5.7) imply that when d and n are p-complementary,

$$\binom{d+n}{n} \equiv 1 \bmod p.$$

Hence by Lemma 5.7,

$$\left[\binom{d+n}{n}\right]_\zeta = 1.$$

Combining these computations we have

$$Q(t) = \sum_{d\geq 0} \left[\binom{d+n}{n}\right]_\zeta t^d = \sum_{\substack{d \text{ is } p\text{-comp.} \\ \text{to } n}} t^d.$$

The existence and uniqueness of base p expansions of natural numbers is equivalent to the following product formula,

$$\frac{1}{1-t} = \sum_{d\geq 0} t^d = \prod_{k\geq 1} \sum_{a=0}^{p-1} t^{ap^k} = \prod_{k\geq 1} \frac{1-t^{p^{k+1}}}{1-t^{p^k}},$$

where the factor of $\frac{1-t^{p^{k+1}}}{1-t^{p^k}}$ contributes to the coefficient of t^d precisely when d is not p-complementary to p^k. If $n = (p-1)p^{k_1} + (p-1)p^{k_2} + \ldots + (p-1)p^{k_s}$ is the base p expansion of n, then

$$Q(t) = \sum_{\substack{d \text{ is } p\text{-comp.} \\ \text{to } n}} t^d = \frac{1}{1-t} \prod_{i=1}^{s} \frac{1-t^{p^{k_i}}}{1-t^{p^{k_i+1}}}.$$

Therefore

$$\sum_{d\geq 0} P_{d,n}(\zeta) t^d = (1-t)Q(t) = \prod_{i=1}^{s} \frac{1-t^{p^{k_i}}}{1-t^{p^{k_i+1}}} = \prod_{j\geq 1} \left(\frac{1}{1-t^{p^k}}\right)^{b_k},$$

where $n = b_\ell p^\ell + b_{\ell-1}p^{\ell-1} + \ldots + b_1 p + b_0$ is the balanced base p expansion of n. The uniqueness of combinatorial Euler products (Lemma 4.2) implies that $M_{p^k,n}(\zeta) = b_k$ and $M_{d,n}(\zeta) = 0$ when d is not a power of p. □

For a fixed n there are finitely many primes p for which n has a balanced base p expansion. Theorem 5.6 tells us that for each such prime p there are only finitely many d such that $M_{d,n}(\zeta_p) \neq 0$ for ζ_p a primitive pth root of unity. The only prime p for which $n = 1$ has a balanced base p expansion is $p = 2$ and this reflects the fact that $M_{d,1}(\zeta_p) = 0$ for all but finitely many d if and only if $p = 2$ (Corollary 4.4.)

For any integer $m \geq 1$ we have $[m]_0 = 1$. Thus (5.5) implies $P_{d,n}(0) = 0$ for all $d, n \geq 1$, hence $M_{d,n}(0) = 0$. Setting $x = 1$ gives $[m]_1 = m$, hence by (5.5)

$$P_{d,n}(1) = \binom{d+n}{n} - \binom{d+n-1}{n} = \binom{d+n-1}{d} = \left(\!\!\binom{n}{d}\!\!\right).$$

Therefore

$$\sum_{d\geq 0} P_{d,n}(1) t^d = \sum_{d\geq 0} \left(\!\!\binom{n}{d}\!\!\right) t^d = \left(\frac{1}{1-t}\right)^n.$$

Thus $M_{1,n}(1) = n$ and $M_{d,n}(1) = 0$ for $d > 1$. We record these computations in Proposition 5.9.

Proposition 5.9. *For all $d, n \geq 1$, $M_{d,n}(0) = 0$ and*

$$M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases}$$

In Section 6 we interpret the values of $M_{d,n}(\pm 1)$ as Euler characteristics.

We finish this section with a result on the family of formal power series

$$Z_n(x,t) := \sum_{d \geq 0} P_{d,n}(x) t^d$$

appearing in the generalized cyclotomic identity.

Theorem 5.10. *If $n \geq 1$, then the formal power series*

$$Z_n(x,t) = \sum_{d \geq 0} P_{d,n}(x) t^d$$

is a rational function in t with coefficients in $\mathbb{Q}[x]$ if and only if $n = 1$. However, for every root of unity ζ, $Z(\zeta, t)$ is a rational function in t with coefficients in $\mathbb{Q}(\zeta)$.

Proof. When $n = 1$ the series $Z_n(x,t)$ specializes to

$$Z_1(x,t) = \frac{1}{1 - xt}.$$

If $n > 1$ and $Z_n(x,t)$ were a rational function in t with coefficients in $\mathbb{Q}[x]$, then the coefficient of t^d in $Z_n(x,t)$ would have leading term x^{cd} for some constant c. However, (5.1) shows that $P_{d,n}(x)$ has leading term of the form x^{cd^n} which for $n > 1$ implies that $Z_n(x,t)$ is not rational.

If $x = \zeta$ is an mth root of unity, then

$$P_{d,n}(\zeta) = \left[\binom{d+n}{n} \right]_\zeta - \left[\binom{d+n-1}{n} \right]_\zeta,$$

and by Lemma 5.7 the values of $P_{d,n}(\zeta)$ only depend on $\binom{d+n}{n}$ and $\binom{d+n-1}{n}$ modulo m. Hence the values of $P_{d,n}(\zeta)$ are periodic as functions of d. All formal power series with periodic coefficients are rational. □

6. Necklace values as Euler characteristics

Recall from Definition 5.1 the space $\mathrm{Poly}_{d,n}(K)$ of all total degree d monic polynomials in $K[x_1, x_2, \ldots, x_n]$ and the subspace $\mathrm{Irr}_{d,n}(K)$ of K-irreducible polynomials. When $K = \mathbb{R}$ or $\mathbb{C}$ the space $\mathrm{Poly}_{d,n}(K)$ has a natural topology inherited from the ambient affine space of all polynomials in $K[x_1, x_2, \ldots, x_n]$ with degree at most d, and thus $\mathrm{Irr}_{d,n}(K) \subseteq \mathrm{Poly}_{d,n}(K)$ inherits a subspace topology.

Definition 6.1. Say a topological space X is **tame** if the compactly supported singular cohomology $H_c^k(X, \mathbb{Q})$ (see Hatcher [18, Pg. 243]) is defined for all $k \geq 0$ and vanishes for all but finitely many k. If X is tame, then the **compactly supported Euler characteristic** $\chi_c(X)$ is

$$\chi_c(X) := \sum_{k \geq 0} (-1)^k \dim_{\mathbb{Q}} H_c^k(X, \mathbb{Q}).$$

When $K = \mathbb{R}$ or $\mathbb{C}$, the space $\mathrm{Irr}_{d,n}(K)$ may be constructed from projective spaces by cut-and-paste relations and is therefore tame. The main result of this section is Theorem 6.2 which shows that $\chi_c(\mathrm{Irr}_{d,n}(K))$ when $K = \mathbb{R}$ or $\mathbb{C}$ is given by $M_{d,n}(\pm 1)$.

Theorem 6.2. *Let $d, n \geq 1$ and let $M_{d,n}(x)$ be the higher necklace polynomial as defined in Definition 5.2. Then*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad \chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} b_k & \text{if } d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

where $n = \sum_{k \geq 0} b_k 2^k$ is the balanced binary expansion of n (see Definition 5.4.)

Remark. When one has a space V which can be defined over any field K such that the size of $V(\mathbb{F}_q)$ is given by a polynomial $F(x)$ evaluated at $x = q$, one hopes that the compactly supported Euler characteristic of $V(K)$ when $K = \mathbb{R}$ or $\mathbb{C}$ should be given by evaluating $F(x)$ at $x = \pm 1$. If V is a variety defined over $\mathbb{Z}$ this heuristic can be made precise by working the Grothendieck ring of varieties (see Farb, Wolfson [8, 9, 10] or Vakil's notes [38].) Theorem 6.2 shows that this is the case for the space $\mathrm{Irr}_{d,n}$, although $\mathrm{Irr}_{d,n}$ is not a variety or even constructible in the Zariski topology, which presents a technical difficulty. If one could identify the proper Grothendieck ring in which to define the class of $\mathrm{Irr}_{d,n}$, then Theorem 6.2 could potentially be generalized to the motivic identity

$$[\mathrm{Irr}_{d,n}] = M_{d,n}(\mathbb{L}),$$

where $\mathbb{L} := [\mathbb{A}^1]$ is the class of the affine line.

We first prove several lemmas. Lemma 6.3 describes the geometry of the space $\mathrm{Poly}_{d,n}(K)$.

Lemma 6.3. *Let K be a field. Then for all $d, n \geq 1$,*

(1) If $\mathrm{Poly}_{\leq d,n}(K)$ is the space of all non-zero monic polynomials in $K[x_1, x_2, \ldots, x_n]$ with degree at most d, then $\mathrm{Poly}_{\leq d,n}(K) \cong \mathbb{P}^{\binom{d+n}{n}-1}(K)$. The space $\mathrm{Poly}_{\leq d-1,n}(K)$ sits naturally inside of $\mathrm{Poly}_{\leq d,n}(K)$ and $\mathrm{Poly}_{d,n}(K)$ is the complement,

$$\mathrm{Poly}_{d,n}(K) = \mathbb{P}^{\binom{d+n}{n}-1}(K) \setminus \mathbb{P}^{\binom{d+n-1}{n}-1}(K).$$

(2) If λ is a partition, let $m_j(\lambda)$ denote the number of parts of λ of size j. Unique factorization of polynomials over a field gives the decomposition

$$\mathrm{Poly}_{d,n}(K) = \bigsqcup_{\lambda \vdash d} \prod_{j \geq 1} \mathrm{Sym}^{m_j(\lambda)}(\mathrm{Irr}_{j,n}(K)).$$

Proof. (1) Consider the K-vector space spanned by all monomials in n variables of degree at most d. By the classic stars-and-bars counting argument this space has dimension $\binom{d+n}{n}$. The projectivization of this vector space is, by definition, the space of all non-zero monic degree at most d polynomials in $K[x_1, x_2, \ldots, x_n]$. Hence $\mathrm{Poly}_{\leq d,n}(K) \cong \mathbb{P}^{\binom{d+n}{n}-1}(K)$.

(2) This follows immediately from the fact that any finitely generated polynomial ring over a field has unique factorization. □

Remark. Some caution is needed when interpreting the symmetric powers in Lemma 6.3 (2). That is, $\mathrm{Sym}^m(\mathrm{Irr}_{d,n}(K))$ should not be interpreted as $(\mathrm{Sym}^m \mathrm{Irr}_{d,n})(K)$ in the sense of scheme theory. For example, the irreducible degree one polynomials over K correspond to points on the affine line $\mathrm{Irr}_{1,1}(K) \cong \mathbb{A}^1(K)$. On one hand $\mathrm{Sym}^2 \mathbb{A}^1$ is a scheme defined over $\mathbb{Z}$ and as such is isomorphic to $\mathbb{A}^2$, hence $(\mathrm{Sym}^2 \mathrm{Irr}_{1,1})(\mathbb{R}) = \mathbb{A}^2(\mathbb{R})$ is the space of all degree 2 monic polynomials over $\mathbb{R}$. However $\mathrm{Sym}^2(\mathrm{Irr}_{1,1}(\mathbb{R}))$ is the collection all reducible quadratic polynomials of the form $(x - a)(x - b)$ with $a, b \in \mathbb{R}$.

Theorem 6.4, due to MacDonald [26], allows us to compute the Euler characteristic of a symmetric power of a space X in terms of the Euler characteristic of X. See Vakil's notes [38, Thm. 2.3] for a nice one line proof.

Theorem 6.4 (MacDonald)**.** *If X is a tame space, then so is $\mathrm{Sym}^m X$ and*

$$\chi_c(\mathrm{Sym}^m X) = \left(\!\!\binom{\chi_c(X)}{m}\!\!\right).$$

Equivalently, in $\Lambda(\mathbb{Z})$ we have

$$\sum_{d\geq 0} \chi_c(\mathrm{Sym}^d X)t^d = \left(\frac{1}{1-t}\right)^{\chi_c(X)}.$$

Finally Lemma 6.5 recalls some important well-known properties of the compactly supported Euler characteristic (see [38].) Note that property (2) fails for the non-compactly supported Euler characteristic.

Lemma 6.5. *Suppose that X and Y are tame spaces. Then*

(1) $\chi_c(X \sqcup Y) = \chi_c(X) + \chi_c(Y)$,

(2) $\chi_c(X \times Y) = \chi_c(X)\chi_c(Y)$,

(3) $\chi_c(\mathbb{R}) = -1$ *and* $\chi_c(\mathbb{C}) = 1$,

(4) If $K = \mathbb{R}$ or $\mathbb{C}$, then $\chi_c(\mathbb{P}^{n-1}(K)) = [n]_{\chi_c(K)}$.

Proof. The first three properties are well-known. To compute the Euler characteristic of projective space we use

$$\mathbb{P}^{n-1}(K) = K^{n-1} \sqcup K^{n-2} \sqcup \ldots \sqcup K \sqcup 1,$$

where $1 = K^0$ is the one point space. Taking χ_c when $K = \mathbb{R}$ or $\mathbb{C}$ we have

$$\chi_c(\mathbb{P}^{n-1}(K)) = \chi_c(K)^{n-1} + \chi_c(K)^{n-2} + \ldots + \chi_c(K) + 1 = [n]_{\chi_c(K)}. \qquad \square$$

We now prove Theorem 6.2.

Proof of Theorem 6.2. Let $K = \mathbb{R}$ or $\mathbb{C}$. Then by Lemma 6.3 (2), Lemma 6.5, and MacDonald's Theorem 6.4 we have

$$\begin{aligned}\chi_c(\mathrm{Poly}_{d,n}(K)) &= \sum_{\lambda\vdash d}\prod_{j\geq 1} \chi_c(\mathrm{Sym}^{m_j}(\mathrm{Irr}_{j,n}(K))) \\ &= \sum_{\lambda\vdash d}\prod_{j\geq 1} \left(\!\!\binom{\chi_c(\mathrm{Irr}_{j,n}(K))}{m_j}\!\!\right).\end{aligned}$$

Lemma 4.2 implies that this is equivalent to

$$\sum_{d\geq 0} \chi_c(\mathrm{Poly}_{d,n}(K))t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{\chi_c(\mathrm{Irr}_{j,n}(K))}.$$

On the other hand, Lemma 6.3 (1) and Lemma 6.3 show that

$$\begin{aligned}\chi_c(\mathrm{Poly}_{d,n}(K)) &= \chi_c(\mathbb{P}^{\binom{n+d}{n}-1}(K)) - \chi_c(\mathbb{P}^{\binom{n+d-1}{n}-1}(K)) \\ &= \left[\binom{n+d}{n}\right]_{\chi_c(K)} - \left[\binom{n+d-1}{n}\right]_{\chi_c(K)} \\ &= P_{d,n}(\chi_c(K)).\end{aligned}$$

The generalized cyclotomic identity (Theorem 5.3) gives

$$\sum_{d\geq 0} P_{d,n}(\chi_c(K))t^d = \prod_{j\geq 1}\left(\frac{1}{1-t^j}\right)^{M_{j,n}(\chi_c(K))}.$$

Hence by the uniqueness of combinatorial Euler products we conclude that for all $d, n \geq 1$,

$$\chi_c(\mathrm{Irr}_{d,n}(K)) = M_{d,n}(\chi_c(K)).$$

Our result then follows from Lemma 6.5 (3), Proposition 5.9, and Theorem 5.6. □

6.1. **Geometric computations of necklace values.** Theorem 6.2 gives a geometric interpretation of $M_{d,n}(\pm 1)$. When $n = 1$ this leads to a "geometric computation" of $M_d(\pm 1)$.

Corollary 6.6. *Let $M_d(x)$ be the dth necklace polynomial. Then,*

$$M_d(1) = \begin{cases} 1 & \text{if } d = 1 \\ 0 & \text{otherwise.} \end{cases} \qquad M_d(-1) = \begin{cases} -1 & \text{if } d = 1 \\ 1 & \text{if } d = 2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (1) Theorem 6.2 implies that $M_d(1) = \chi_c(\mathrm{Irr}_{d,1}(\mathbb{C}))$. Since $\mathbb{C}$ is algebraically closed, there are no $\mathbb{C}$-irreducible polynomials of degree $d > 1$. Hence $M_d(1) = 0$ for $d > 1$. On the other hand, every degree one polynomial is irreducible and thus $\mathrm{Irr}_{1,1}(\mathbb{C}) \cong \mathbb{C}$. Therefore $M_1(1) = \chi_c(\mathbb{C}) = 1$.

(2) Theorem 6.2 implies that $M_d(-1) = \chi_c(\mathrm{Irr}_{d,1}(\mathbb{R}))$. Since $\mathbb{C}/\mathbb{R}$ is a degree 2 extension and $\mathbb{C}$ is algebraically closed, it follows that there are no $\mathbb{R}$-irreducible polynomials of degree $d > 2$. Thus $M_d(-1) = \chi_c(\mathrm{Irr}_{d,1}(\mathbb{R})) = 0$ for $d > 2$. As noted above, $\mathrm{Irr}_{1,1}(\mathbb{R}) \cong \mathbb{R}$ and thus $M_1(-1) = \chi_c(\mathbb{R}) = -1$.

Finally, there is a homeomorphism $\mathrm{Poly}_{2,1}(\mathbb{R}) \cong \mathbb{R}^2$ given by $x^2+bx+c \mapsto (b, c)$ and $\mathrm{Irr}_{2,1}(\mathbb{R})$ corresponds to the open subspace $b^2 - 4c < 0$ with Euler characteristic 1. Hence $M_2(-1) = \chi_c(\mathrm{Irr}_{2,1}(\mathbb{R})) = 1$. □

As another example of this type of argument consider the space of degree 1 irreducible polynomials $\mathrm{Irr}_{1,n}(K)$. The space of monic linear polynomials is $\mathbb{P}^n$ minus a point $\mathbb{P}^0$ corresponding to the constant monic function 1. Since every degree 1 polynomial is irreducible, we have

$$\chi_c(\mathrm{Irr}_{1,n}(\mathbb{C})) = \chi_c(\mathbb{P}^n(\mathbb{C})) - \chi_c(\mathbb{P}^0(\mathbb{C})) = (n + 1) - 1 = n.$$

This agrees with Proposition 5.9 where we found that $M_{1,n}(1) = n$. On the other hand

$$\chi_c(\mathrm{Irr}_{1,n}(\mathbb{R})) = \chi_c(\mathbb{P}^n(\mathbb{R})) - \chi_c(\mathbb{P}^0(\mathbb{R})) = \frac{1 + (-1)^n}{2} - 1 = \begin{cases} 0 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

This agrees with the evaluation of $M_{1,n}(-1)$ from Theorem 5.6 since the coefficient of 1 in the balanced binary expansion of n is 0 if n is even and -1 if n is odd.

Theorem 6.2 connects the evaluation of $M_{d,n}(x)$ at the second roots of unity to the geometry of the space $\mathrm{Irr}_{d,n}(K)$ of irreducible polynomials. When $n = 1$ our understanding of these spaces for $K = \mathbb{R}$ or $\mathbb{C}$ gives a geometric reason for cyclotomic factors $\Phi_m(x)$ of $M_d(x)$ with $m = 1, 2$. It would be interesting to know if there is some geometric or otherwise "motivic" explanation for the rest of the cyclotomic factors of $M_d(x)$.

REFERENCES

[1] R. Arratia, A. D. Barbour, S. Tavaré, Logarithmic combinatorial structures: a probabilistic approach, *European Mathematical Society*, **1**, (2003).

[2] J. Berstel, D. Perrin, The origins of combinatorics on words, *European J. Combin.*, **28**, (2007), 996-1022, DOI: 10.1016/j.ejc.2005.07.019.

[3] J. Borger, Witt vectors, semirings, and total positivity, *preprint*, (2015), arXiv: 1310.3013v2.

[4] L. Carlitz, The distribution of irreducible polynomials in several indeterminates, *Illinois J. Math.*, **7**, no. 3, (1963), 371-375.

[5] L. Carlitz, The distribution of irreducible polynomials in several indeterminates II, *Canad. J. Math.*, **17**, (1965), 261-266.

[6] A. W. M. Dress, C. Siebeneicher, The Burnside ring of the infinite cyclic group and its relation to the necklace algebra, λ-rings, and the universal ring of Witt vectors, *Adv. Math.*, **78**, no. 1, (1989), 1-41, DOI: 10.1016/0001-8708(89)90027-3.

[7] J. Elliott, Binomial rings, integer-valued polynomials, and λ-rings, *J. Pure Appl. Algebra*, **207**, no. 1, (2006), 165-185, DOI: 10.1016/j.jpaa.2005.09.003.
[8] B. Farb, J. Wolfson, Étale homological stability and arithmetic statistics, *Quart. J. Math*, **69**, no. 3, (2018), 951-974, DOI: 10.1093/qmath/hay009.
[9] B. Farb, J. Wolfson, Topology and arithmetic of resultants, I, *New York J. Math.*, **22**, (2016), 801-821, available at http://nyjm.albany.edu/j/2016/22-37.html.
[10] B. Farb, J. Wolfson, Topology and arithmetic of resultants, II: the resultant 1 hypersurface, *Algebraic Geometry*, **4**, no. 3, (2017), 337-352, DOI: 10.14231/AG-2017-019.
[11] N. J. Fine, Binomial coefficients modulo a prime, *Am. Math. Monthly*, **54**, no. 10, (1947), 589-592, DOI: 10.2307/2304500.
[12] C. F. Gauss, Allgemeine Untersuchungen über die Congruenzen, in *Untersuchungen über höhere Arithmetik* (translated by H. Maser), 2nd edn. *Chelsea Publishing Co.*, New York, (1965).
[13] W. Gaschütz, Die Eulersche Funktion Endlicher Auflösbarer Gruppen, *Ill. J. Math.*, **3**, no. 4, (1959), 469-476.
[14] A. Granville, The anatomy of the integers, *preprint*, available at `http://www.dms.umontreal.ca/~andrew/MSI/AnatomyForTheBook.pdf`.
[15] A. Grothendieck, La théorie des classes de Chern, *Bull. Soc. Math. France*, **86**, no. 2, (1958), 137-154, DOI: 10.24033/bsmf.1501.
[16] K. Habiro, Cyclotomic completions of polynomial rings, *Publications of the Research Institute for Mathematical Sciences*, **40**, no. 4, (2004), 1127-1146, DOI: 10.2977/prims/1145475444.
[17] P. Hall, The Edmonton Notes on Nilpotent Groups, *Queen Mary College Mathematics Notes*, Mathematics Department, Queen Mary College, London, (1969).
[18] A. Hatcher, Algebraic topology, *Cambridge University Press*, (2002), available at http://pi.math.cornell.edu/ hatcher/AT/AT.pdf.
[19] T. Hawkes, I. M. Isaacs, M. Özaydin, On the Möbius function of a finite group, *Rocky Mt. J. of Math.*, **19**, no. 4, (1989), 1003-1034, available at https://www.jstor.org/stable/44237284.
[20] T. Hyde, Liminal reciprocity and factorization statistics, to appear in *Alg. Comb.*, (2018), arXiv: 1803.08438.
[21] J. C. Lagarias, A family of measures on symmetric groups and the field with one element, *J. Number Theory*, **161**, (2016), 311-342, DOI: 10.1016/j.jnt.2015.09.003.
[22] S. Lang, Algebra, **211**, *Springer Science & Business Media*, (2002).
[23] S. Lang, Algebraic number theory, **110**, *Springer Science & Business Media*, (1986).
[24] H. W. Lenstra, Construction of the ring of Witt vectors, *preprint*, available at `http://pub.math.leidenuniv.nl/~lenstrahw/PUBLICATIONS/witt.pdf`.
[25] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Am. J. Math.*, **1**, no. 4, (1878), 289-321, DOI: 10.2307/2369373.
[26] I. G. MacDonald, The Poincaré polynomial of a symmetric product, *Math. Proc. Camb. Philos. Soc.*, **58**, no. 4, (1962), DOI: 10.1017/S0305004100040573.
[27] N. Metropolis, G.-C. Rota, Witt vectors and the algebra of necklaces, *Adv. Math.*, **50**, no. 2, (1983), 95-125, DOI: 10.1016/0001-8708(83)90035-X.
[28] I. Niven, H. S. Zuckerman, H. L. Montgomery, An introduction to the theory of numbers, *John Wiley & Sons*, (2013).
[29] Y.-T. Oh, Group-theoretical generalization of necklace polynomials, *J. Algebr. Comb.*, **35**, (2012), 389-420, DOI: 10.1007/s10801-011-0307-3.
[30] C. Reutenauer, Free Lie algebras, **7**, *London Mathematical Society Monographs*, (1993).
[31] C. Reutenauer, On symmetric functions related to Witt vectors and the free Lie algebra, *Adv. Math.*, **110**, (1995), 234-246, DOI: 10.1006/aima.1995.1009.
[32] M. Rosen, Number theory in function fields, **210**, *Spring Science & Business Media*, (2002).
[33] T. Schönemann, Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, *J. Reine Angew. Math.*, **31**, (1846), 269-325.
[34] J. H. Silverman, The arithmetic of dynamical systems, **241**, *Springer Science & Business Media*, (2007).
[35] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. Math.*,**108**, no. 1, (1978), 107-134, DOI: 10.2307/1970932.
[36] R. P. Stanley, Combinatorial reciprocity theorems, *Combinatorics*, **16**, Springer, Dordrecht, (1975), 307-318.
[37] R. P. Stanley, Enumerative combinatorics volume I, second edition, *Cambridge University Press*, (2011).
[38] R. Vakil, Arizona winter school notes, available at `http://swc.math.arizona.edu/aws/2015/2015VakilNotes.pdf`.
[39] L. C. Washington, Introduction to cyclotomic fields, **83**, *Springer Science & Business Media*, (1997).
[40] E. Witt, Treue Darstellung Liescher Ringe, *J. Reine Angew. Math*, **177**, (1937), 152-160, DOI: 10.1515/crll.1937.177.152.

DEPT. OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109-1043,
E-mail address: `tghyde@umich.edu`