SOME ENUMERATIVE APPLICATIONS OF CYCLOTOMIC POLYNOMIALS

RICHARD P. STANLEY

Abstract. We begin with three formulas involving integer partitions, polynomials over $\mathbb{F}_q$, and Dirichlet series that have strong similarities. These formulas can be unified and extended by a general result involving factorization in a free monoid. The key fact underlying this approach is that for certain subsets S (called *cyclotomic sets*) of the positive integers, the numerator and denominator of a certain rational function $G_S(x)$ are products of cyclotomic polynomials. We then investigate properties of cyclotomic sets and conclude with a connection between certain cyclotomic sets and commutative algebra.

1. Introduction

We begin by stating three formulas. A glance at them makes it obvious that there is some connection among them. The main goal of this paper is to explain and extend this connection. It is stated in terms of free monoids, so in Section 2 we develop the necessary background information on free monoids. In Section 3 we give a general formula (Theorem 3.1) involving free monoids and cyclotomic polynomials. This formula is the main result of this paper; what follows are applications and enhancements. The key fact underlying Theorem 3.1 is that for certain subsets S (called *cyclotomic sets*) of the positive integers, both the numerator and denominator of a certain rational function $G_S(x)$ are products of cyclotomic polynomials. We explain in Section 4 the connection with the three formulas and how they can be generalized. In Section 5 we investigate properties of cyclotomic sets, and finally in Section 6 we discuss a connection between certain cyclotomic sets and commutative algebra.

First formula. By a *partition* λ of an integer $n \geq 0$, we mean a sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ of integers λ_i satisfying $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ and $\sum \lambda_i = n$. Thus $\lambda_i = 0$ for all but finitely many i. A nonzero λ_i is a *part* of λ. Let $f(n)$ denote the number of partitions of n for which no part appears exactly once, i.e., for each $k \geq 1$ there is not exactly

Date: January 17, 2025.

one i for which $\lambda_i = k$. For instance, when $n = 8$ there are six such partitions: 44, 3311, 2222, 22211, 221111, 11111111. MacMahon [8, p. 54] proved the following formula (in a dual form):

$$\sum_{n\geq 0} f(n)x^n = \prod_{k\geq 1} \frac{1-x^{6k}}{(1-x^{2k})(1-x^{3k})}. \tag{1.1}$$

Second formula. Let $f(n)$ denote the number of monic polynomials $H(t)$ over the finite field $\mathbb{F}_q$ such that when $H(t)$ is factored into irreducible factors over $\mathbb{F}_q$, no irreducible factor occurs with multiplicity one. Such polynomials are called *powerful*. Then [10][15]

$$\sum_{n\geq 0} f(n)x^n = \frac{1-qx^6}{(1-qx^2)(1-qx^3)}. \tag{1.2}$$

Third formula. Let S denote the set of positive integers m such that no prime p divides m with multiplicity one, i.e., if $p|m$ then $p^2|m$. Such integers are called *powerful*, in analogy to powerful polynomials. (The irreducible factors in both cases have multiplicity at least two.) Let $\zeta(s)$ denote the Riemann zeta function, i.e., $\zeta(s) = \sum_{n\geq 1} n^{-s}$ (when the real part of s exceeds 1). Then [4, (10)]

$$\sum_{n\in S} n^{-s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}. \tag{1.3}$$

Obviously the three formulas are related in some way. The next section develops a general result (Theorem 3.1) which we use in Section 4 to explain the three formulas.

2. A free monoid

Let $\mathbb{N} = \{0, 1, 2, \dots\}$, and let $\mathfrak{M}$ denote a free commutative monoid with countably infinitely many generators. In other words, $\mathfrak{M}$ is isomorphic to the monoid $\mathbb{N}^\infty$ consisting of all infinite sequences $u = (u_1, u_2, \dots)$, where $u_i \in \mathbb{N}$ and only finitely many $u_i \neq 0$, under the operation of componentwise addition. The monoid $\mathfrak{M}$ has a unique *basis* $B = \{v(1), v(2), \dots\}$, where $v(i)$ is the ith unit coordinate vector, i.e., $v(i)_i = 1$ while $v(i)_j = 0$ for $j \neq i$. Every $u \in \mathfrak{M}$ can be uniquely written $u = c_1v(1) + c_2v(2) + \cdots$, where $c_i \in \mathbb{N}$ and all but finitely many $c_i = 0$. We call c_i the *multiplicity* of $v(i)$ in u, denoted $c_i = \mu_u(v(i))$. Let

$$\omega\colon \mathfrak{M} \to \mathbb{N}^m \tag{2.1}$$

be a monoid homomorphism, where $m \in \mathbb{P} := \{1, 2, 3, \dots\}$ or $m = \infty$. We call ω a *weight* on $\mathfrak{M}$ if $\omega^{-1}(\alpha)$ is finite for all $\alpha \in \mathbb{N}^m$. In this

situation we will associate with the pair $(\mathfrak{M}, \omega)$ and a set $S \subseteq \mathbb{P}$ a certain generating function $F_S(\boldsymbol{x})$. In some situations involving cyclotomic polynomials, $F_S(\boldsymbol{x})$ has a simple expression in terms of $F_\emptyset(\boldsymbol{x})$, as explained in the next section. In subsequent sections we give three applications by suitable choices of $(\mathfrak{M}, \omega)$, corresponding to the three formulas of Section 1.

If $\alpha = (\alpha_1, \alpha_2, \dots) \in \mathbb{N}^m$ we use the multivariate notation $\boldsymbol{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots$. Regarding $(\mathfrak{M}, \omega)$ as fixed, consider the formal series

$$F(\boldsymbol{x}) = \sum_{u \in \mathfrak{M}} \boldsymbol{x}^{\omega(u)}.$$

Because for each $\alpha \in \mathbb{N}^m$ the set $\omega^{-1}(\alpha)$ is finite, the series $F(\boldsymbol{x})$ is well-defined, i.e., has finite coefficients. Clearly from the definition of a free commutative monoid and the fact that ω is a homomorphism, we have

$$\begin{aligned} F(\boldsymbol{x}) &= \prod_{v \in B} \left(1 + \boldsymbol{x}^{\omega(v)} + \boldsymbol{x}^{2\omega(v)} + \cdots\right) \\ &= \prod_{v \in B} (1 - \boldsymbol{x}^{\omega(v)})^{-1}, \end{aligned} \tag{2.2}$$

where B is the unique basis for $\mathfrak{M}$. Now let $S \subseteq \mathbb{P}$, and define

$$F_S(\boldsymbol{x}) = \sum_{\substack{u \in \mathfrak{M} \\ v \in B \Rightarrow \mu_u(v) \notin S}} \boldsymbol{x}^{\omega(u)}. \tag{2.3}$$

Thus the sum is over all elements $u \in \mathfrak{M}$ such that no basis element $v \in B$ appears in u with multiplicity belonging to S. In particular, $F(\boldsymbol{x}) = F_\emptyset(\boldsymbol{x})$.

Since the multiplicities $\mu_u(v)$ can be chosen independently, we obtain as a generalization of equation (2.2) the identity

$$F_S(\boldsymbol{x}) = \prod_{v \in B} \left(\sum_{j \in \mathbb{N} - S} \boldsymbol{x}^{j\omega(v)} \right). \tag{2.4}$$

Example 2.1. Consider the case $S = \{1\}$. In other words, in equation (2.3) we are summing over all elements $u \in \mathfrak{M}$ for which no basis element has multiplicity one. We could call such elements u *powerful*.

Then equation (2.4) becomes

$$\begin{aligned} F_{\{1\}}(\boldsymbol{x}) &= \prod_{v\in B}\left(1+\boldsymbol{x}^{2\omega(v)}+\boldsymbol{x}^{3\omega(v)}+\boldsymbol{x}^{4\omega(v)}+\cdots\right) \\ &= \prod_{v\in B}\left(1+\frac{\boldsymbol{x}^{2\omega(v)}}{1-\boldsymbol{x}^{\omega(v)}}\right) \\ &= \prod_{v\in B}\left(\frac{1-\boldsymbol{x}^{\omega(v)}+\boldsymbol{x}^{2\omega(v)}}{1-\boldsymbol{x}^{\omega(v)}}\right). \end{aligned}$$

The key observation is that for an indeterminate z,

$$\frac{1-z+z^2}{1-z}=\frac{1-z^6}{(1-z^2)(1-z^3)}. \tag{2.5}$$

Hence

$$\begin{aligned} F_{\{1\}}(\boldsymbol{x}) &= \prod_{u\in B}\frac{1-\boldsymbol{x}^{6\omega(v)}}{(1-\boldsymbol{x}^{2\omega(v)})(1-\boldsymbol{x}^{3\omega(v)})} \\ &= \frac{F(\boldsymbol{x}^2)F(\boldsymbol{x}^3)}{F(\boldsymbol{x}^6)}, \end{aligned} \tag{2.6}$$

We would like to find other sets $S\subseteq\mathbb{P}$ that yield formulas similar to equation (2.6). We discuss such sets in the next section.

3. Cyclotomic polynomials and cyclotomic sets

In order to generalize equation (2.6) we introduce cyclotomic polynomials. Let $n\geq 1$. The *cyclotomic polynomial* $\Phi_n(x)$ (which we normalize to have constant term 1) is the polynomial over the rationals $\mathbb{Q}$ with constant term 1 whose zeros are the primitive nth roots of 1. Thus $\Phi_1(x)=1-x$ and

$$\Phi_n(x)=\prod_{\substack{1\leq r\leq n\\ \gcd(n,r)=1}}\left(x-e^{2\pi ir/n}\right),\ n\geq 2,$$

and

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

By a simple Möbius inversion argument, we obtain the well-known formula

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

where μ denotes the usual number-theoretic Möbius function. In particular, a polynomial $P(x) \in \mathbb{Q}[x]$ is a product of cyclotomic polynomials if and only if it can be written in the form

$$P(x) = \frac{(1-x^{a_1})\cdots(1-x^{a_s})}{(1-x^{b_1})\cdots(1-x^{b_t})}$$

for some positive integers $a_1, \ldots, a_s, b_1, \ldots, b_t$.

NOTE. Usually $\Phi_n(x)$ is normalized to be monic. This only makes a difference when $n = 1$. According to our definition $\Phi_1(n) = 1 - x$, while traditionally $\Phi_1(x) = x - 1$.

Let $S \subseteq \mathbb{P}$, and define the generating function

$$G_S(x) = \frac{1}{1-x} - \sum_{j \in S} x^j. \tag{3.1}$$

We say that S is a *cyclotomic set* if $G_S(x)$ can be written as a rational function whose numerator and denominator are finite products of cyclotomic polynomials. Equivalently, there exist positive integers $a_1, \ldots, a_s$ and $b_1, \ldots, b_t$ for which

$$G_S(x) = \frac{\prod_{i=1}^{r}(1-x^{a_i})}{\prod_{j=1}^{t}(1-x^{b_j})}. \tag{3.2}$$

Note that if S is any *finite* subset of $\mathbb{P}$, then we can write

$$G_S(x) = \frac{N_S(x)}{1-x},$$

where

$$N_S(x) = 1 - (1-x)\sum_{j \in S} x^j \in \mathbb{Z}[x]. \tag{3.3}$$

Moreover, S is cyclotomic if and only if $N_S(x)$ is a (finite) product of cyclotomic polynomials. By a well-known theorem of Kronecker [7], this condition is equivalent to $N_S(x)$ having all its zeros α on the unit circle ($|\alpha| = 1$).

We come to the main result of this paper. The next section explains how our three formulas in Section 1 are special cases. The original proofs of the first and third formulas at [8, p. 54] and [4, (10)] are essentially specializations of our proof of the next result (Theorem 3.1). The first published proof [15] of the second formula (1.2) does not follow this paradigm, unlike the later proof at [13, p. 152].

Theorem 3.1. *Suppose that S is cyclotomic, and let $G_S(x)$ be as in equation* (3.1)*. Thus as in equation* (3.2) *we can write*

$$G_S(x) = \frac{\prod_{i=1}^r (1-x^{a_i})}{\prod_{j=1}^t (1-x^{b_j})}$$

for certain positive integers a_i and b_j. Then

$$F_S(\boldsymbol{x}) = \frac{\prod_{j=1}^t F(\boldsymbol{x}^{b_j})}{\prod_{i=1}^r F(\boldsymbol{x}^{a_i})}.$$

Proof. The argument is a direct generalization of Example 2.1. We have

$$F_S(\boldsymbol{x}) = \prod_{v\in B}\left(\frac{1}{1-\boldsymbol{x}^{\omega(v)}} - \sum_{j\in S}\boldsymbol{x}^{j\omega(v)}\right).$$

But

$$\frac{1}{1-\boldsymbol{x}^{\omega(v)}} - \sum_{j\in S}\boldsymbol{x}^{j\omega(v)} = \frac{\prod_{i=1}^r (1-\boldsymbol{x}^{a_i\omega(v)})}{\prod_{j=1}^t (1-\boldsymbol{x}^{b_j\omega(v)})}.$$

Hence

$$F_S(\boldsymbol{x}) = \prod_{v\in B}\left(\frac{\prod_{i=1}^r (1-\boldsymbol{x}^{a_i\omega(v)})}{\prod_{j=1}^t (1-\boldsymbol{x}^{b_j\omega(v)})}\right).$$

Comparing with equation (2.2) completes the proof. □

Like many general results in enumerative combinatorics, such as the Möbius inversion formula [11, Prop. 3.7.1] and the Exponential Formula [12, Cor. 5.1.6], Theorem 3.1 per se is rather simple and unassuming. It is the applications that make it interesting. We will give three such applications in Section 4 that explain the three formulas in Section 1.

Example 3.2. (a) Equation (2.5) shows that the set $S = \{1\}$ is cyclotomic.

(b) The set $S = \{1, 2, 3, 5, 7, 11\}$ is cyclotomic. Indeed,

$$\begin{aligned} G_S(x) &= \frac{\Phi_6(x)\Phi_{12}(x)\Phi_{18}(x)}{\Phi_1(x)} \\ &= \frac{(1-x^{12})(1-x^{18})}{(1-x^4)(1-x^6)(1-x^9)}. \end{aligned} \tag{3.4}$$

(c) For any integer $k \geq 1$, the infinite set $S = \{k, k+1, k+2, \dots\}$ is cyclotomic. Indeed,

$$G_S(x) = 1 + x + \cdots + x^{k-1} = \prod_{\substack{d|k \\ d\neq 1}} \Phi_d(x) = \frac{1-x^k}{1-x}. \tag{3.5}$$

It is natural to ask whether cyclotomic sets can be classified or whether they have any interesting properties in addition to being cyclotomic. These questions will be the subject of Section 5.

4. The three formulas redux

4.1. **MacMahon's partition formula.** Let Par denote the set of all partitions of all integers $n \geq 0$. We make Par into a monoid by the operation of multiset union of parts, denoted $\lambda \cup \mu$. That is, if $m_i(\lambda)$ is the number of parts of λ equal to i, then $m_i(\lambda \cup \mu) = m_i(\lambda) + m_i(\mu)$. Clearly Par is a free commutative monoid whose basis elements are the partitions $(i, 0, 0, \dots)$ with only one part $i > 0$. We define the weight function $\omega\colon \mathrm{Par} \to \mathbb{N}$ by $\omega(\lambda) = n$ if λ is a partition of n. Note that $\omega(\lambda \cup \mu) = \omega(\lambda) + \omega(\mu)$, so ω is a monoid homomorphism. Then $F(\boldsymbol{x}) = \sum_{n \geq 0} p(n) x^n$, where $p(n)$ denotes the number of partitions of n. Equation (2.2) becomes

$$F(x) = \prod_{i \geq 1} (1 - x^i)^{-1},$$

the familiar generating function for $p(n)$ going back to Leibniz and Euler. Finally Theorem 3.1 specializes to the following result.

Corollary 4.1. *Suppose that S is a cyclotomic set so that equation* (3.1) *holds for certain positive integers a_i and b_j. Let $p_S(n)$ denote the number of partitions of n none of whose part multiplicities belong to S. Then*

$$\begin{aligned} \sum_{n \geq 0} p_S(n) x^n &= \frac{F(x^{b_1}) \cdots F(x^{b_t})}{F(x^{a_1}) \cdots F(x^{a_r})} \\ &= \frac{\prod_{i=1}^{r} (1 - x^{a_i})(1 - x^{2a_i})(1 - x^{3a_i}) \cdots}{\prod_{j=1}^{t} (1 - x^{b_j})(1 - x^{2b_j})(1 - x^{3b_j}) \cdots}. \end{aligned}$$

Example 4.2. Let $S = \{1\}$, a cyclotomic set (Example 3.2(a)). Thus $p_S(n)$ is the number of partitions of n for which no part appears exactly once, denoted $f(n)$ in equation (1.1). We obtain from equation (2.5) and Corollary 4.1 that

(4.1)
$$F_S(x) = \frac{(1 - x^6)(1 - x^{12})(1 - x^{18}) \cdots}{(1 - x^2)(1 - x^4)(1 - x^6) \cdots (1 - x^3)(1 - x^6)(1 - x^9) \cdots},$$

where x is a single variable because $m = 1$ in equation (2.1). Hence we have proved our first formula (1.1) as a consequence of Theorem 3.1.

The above formula illustrates a special feature of the monoid Par, namely, we obtain quotients of infinite products that we can try to simplify by cancelling common factors in the numerator and denominator. The denominator factors $1-x^k$ in equation (4.1) have exponents k that are multiples of 2 or 3. Multiples of 6 appear twice, once as multiples of 2 and once as multiples of 3. The numerator factor exponents are multiples of 6, so they cancel one of the two such denominator factors. We are left with 1 in the numerator, and factors $1-x^k$ in the denominator, each with multiplicity one, where k is divisible by 2 or 3. Equivalently, $k \not\equiv \pm 1 \pmod 6$. In other words,

$$F_S(x) = \prod_{k \not\equiv \pm 1 \,(\mathrm{mod}\, 6)} (1-x^k)^{-1}.$$

We conclude that $p_S(n)$ (the number of partitions of n with no part appearing exactly once) is equal to the number of partitions of n into parts not congruent to ± 1 modulo 6. MacMahon [8, p. 54] was aware that

$$\prod_{k \not\equiv \pm 1 \,(\mathrm{mod}\, 6)} (1-x^k)^{-1} = \prod_{k \geq 1} \frac{1-x^{6k}}{(1-x^{2k})(1-x^{3k})}.$$

Let us call a cyclotomic set S *clean* (continuing to assume $\mathfrak{M} = \mathrm{Par}$) if we can write

$$F_S(x) = \prod_{k \in T} (1-x^k)^{-1} \tag{4.2}$$

for some $T \subseteq \mathbb{P}$. Thus $\{1\}$ is clean. We consider equation (4.2) to be a "clean" partition identity—the coefficient of x^n in the expansion of the right-hand side has the simple interpretation of counting partitions of n whose parts belong to T. For any particular cyclotomic set S it is easy to determine whether it is clean, but we don't have a general theory of cleanness. Some examples are given below.

Example 4.3. We stated in Example 3.2(b) that the set $\{1, 2, 3, 5, 7, 11\}$ is cyclotomic. This set turns out to be clean. We have

$$F_S(x) = \prod_i (1-x^i)^{-1},$$

where

$$i \equiv 0, 4, 6, 8, 9, 12, 16, 18, 20, 24, 27, 28, 30, 32 \,(\mathrm{mod}\, 36). \tag{4.3}$$

Thus we obtain the following new result.

Theorem 4.4. *For all $n \geq 0$, the number of partitions of n such that no part occurs exactly 1,2,3,5,7 or 11 times equals the number of partitions of n into parts i satisfying equation* (4.3).

Example 4.5. The infinite set $S = \{2, 3, 4, \dots\}$ is cyclotomic and clean:

$$\frac{1}{1-x} - (x^2 + x^3 + x^4 + \cdots) = \frac{1-x^2}{1-x} = 1 + x. \tag{4.4}$$

We obtain the famous theorem of Euler that the number of partitions of n into distinct parts equals the number of partitions of n into odd parts.

Example 4.6. An example of a set that is cyclotomic but not clean is $S = \{1, 5, 7, 8, 9, 11\}$, for which

$$\frac{1}{1-x} - \sum_{j \in S} x^j = \frac{(1-x^5)(1-x^6)(1-x^{30})}{(1-x^2)(1-x^3)(1-x^{10})(1-x^{15})}.$$

After canceling all possible numerator and denominator factors, we obtain

$$F_S(x) = \frac{\prod_i (1-x^i)}{\prod_j (1-x^j)},$$

where i ranges over all positive integers satisfying

$$i \equiv \pm 5 \pmod{30},$$

while j ranges over all positive integers satisfying

$$j \equiv \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \pm 12, \pm 14, 15 \pmod{30}.$$

4.2. **Finite fields.** Fix a prime power q. Let Pol denote the set of all monic polynomials $H(t) \in \mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field of order q. We make Pol into a free commutative monoid by the operation of ordinary polynomial multiplication. The identity element is the constant polynomial 1. The unique basis B for Pol consists of those polynomials in Pol that are irreducible over $\mathbb{F}_q$. For $H \in \text{Pol}$ define $\omega(H) = \deg H$. Clearly ω is a weight on Pol (with $m = 1$ in equation (2.1)).

The series $F(x)$ (where x is a single variable since $m = 1$) is given by $\sum_{n \geq 0} f(n) x^n$, where $f(n)$ is the number of monic polynomials of degree n over $\mathbb{F}_q$. Since such a polynomial has n coefficients which can be chosen independently from $\mathbb{F}_q$, we have $f(n) = q^n$. Hence

$$F(x) = \sum_{n \geq 0} q^n x^n = \frac{1}{1-qx}.$$

For $S \subseteq \mathbb{P}$, the coefficient $f_S(n)$ of x^n in $F_S(x)$ is equal to the number of monic polynomials of degree n over $\mathbb{F}_q$ for which no irreducible factor

has multiplicity $j \in S$. If S is a cyclotomic set and equation (3.2) holds, then

$$F_S(x) = \frac{\prod_{i=1}^{r}(1-qx^{a_i})}{\prod_{j=1}^{t}(1-qx^{b_j})}. \tag{4.5}$$

Thus $F_S(x)$ is a rational function of x and q. We can expand this rational function by partial fractions with respect to q and obtain in principle an explicit formula for $f_S(n)$. This formula will depend on the congruence class of n modulo some integer N. For example, in Example 4.8 below we have $N = 6$, and it is fortuitous that $f_S(n)$ can be written in the condensed form (4.6).

Example 4.7. Let $S = \{2, 3, 4, \dots\}$. Then $f_S(n)$ is equal to the number of squarefree monic polynomials of degree n over $\mathbb{F}_q$. By the case $k = 2$ of Example 3.2(c) there follows

$$\begin{aligned} F_S(x) &= \frac{1-qx^2}{1-qx} \\ &= 1 + qx + \sum_{n\geq 2}(q-1)q^{n-1}x^n, \end{aligned}$$

whence $f_S(n) = (q-1)q^{n-1}$ for $n \geq 2$, a well-known result going back at least to Carlitz [2]. (Carlitz in a footnote on page 41 gives a reference to a proof by Landau in 1919 when q is prime.) Comparing with Example 4.5 shows that the formula for $f_S(n)$ is a kind of "finite field analogue" (but not a q-analogue in the usual sense of this term [11, pp. 30–31]) of the result of Euler given in Example 4.5.

Example 4.8. Let $S = \{1\}$, so $f_S(n)$ is the number of monic polynomials of degree n over $\mathbb{F}_q$ such that every irreducible factor has multiplicity at least two. Such polynomials are called *powerful*. From equation (2.5) there follows (in analogy to equation (1.1))

$$F_S(x) = \frac{1-qx^6}{(1-qx^2)(1-qx^3)},$$

which is our second formula (1.2). The partial fraction decomposition of $F_S(x)$ with respect to q is given by

$$F_S(x) = \frac{1+x+x^2+x^3}{1-qx^2} - \frac{x(1+x+x^2)}{1-qx^3}.$$

From this formula it is not difficult to show that

$$f_S(n) = q^{\lfloor n/2\rfloor} + q^{\lfloor n/2\rfloor - 1} - q^{\lfloor (n-1)/3\rfloor}. \tag{4.6}$$

This formula for $f_S(n)$ first appeared as a problem in [10], with a published solution by Stong [15]. The analogy between equation (1.1)

and the present example was noted by Stanley [13, p. 152]. In fact, it was this analogy that inspired the present paper.

Example 4.9. Let $S = \{1, 2, 3, 5, 7, 11\}$. From equation (3.4) we get the following new result:

$$\begin{aligned} F_S(x) &= \frac{(1-qx^{12})(1-qx^{18})}{(1-qx^4)(1-qx^6)(1-qx^9)} \\ &= \frac{\Phi_2\Phi_4\Phi_8\Phi_7\Phi_{14}}{\Phi_5(1-qx^4)} + \frac{\Phi_3\Phi_9\, x^8}{\Phi_5(1-qx^9)} \\ &\quad - \frac{\Phi_2\Phi_3\Phi_4\Phi_6^2\Phi_{12}\, x^2}{1-qx^6}, \end{aligned}$$

where $\Phi_j = \Phi_j(x)$. A formula for $f_S(n)$ will involve the congruence class of n modulo 36 (the least common multiple of 4, 6, and 9).

4.3. **Dirichlet series.** Perhaps the most familiar monoid that is isomorphic to $\mathfrak{M}$ is the set $\mathbb{P}$ of positive integers under multiplication. The basis elements are the prime numbers. What can we do with this choice of $\mathfrak{M}$?

If $n = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}\cdots$ is the prime power factorization of n (so all but finitely many $\alpha_i = 0$) then define $\omega\colon \mathbb{P} \to \mathbb{N}^\infty$ by $\omega(n) = (\alpha_1, \alpha_2, \alpha_3, \dots)$, clearly a weight on $\mathbb{P}$ (with $m = \infty$ in equation (2.1)). If p_i is the ith prime (so $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc.), then change the indeterminate x_i into p_i^{-s}, where s is an indeterminate. The "variables" p_i^{-s} remain algebraically independent, so there is no loss of information in making this change of notation. The power series $\sum_{\alpha\in\mathbb{N}^\infty} f(\alpha)\boldsymbol{x}^\alpha$ is converted into the *Dirichlet series* $\sum_{n\geq 1} g(n)n^{-s}$, where $n = 2^{\alpha_1}3^{\alpha_2}\cdots$ and $g(n) = f(\alpha)$.

Writing $\widetilde{F}(s)$ for $F(\boldsymbol{x})$ and $\widetilde{F}_S(s)$ for $F_S(\boldsymbol{x})$ after the above change of variables, we thus have

$$\widetilde{F}(s) = \sum_{n\geq 1} \frac{1}{n^s},$$

the Riemann zeta function $\zeta(s)$. For $S \subseteq \mathbb{P}$ we have

$$\widetilde{F}_S(s) = \sum_{n\in T} \frac{1}{n^s},$$

where T is the set of all $n \in \mathbb{P}$ such that no prime factor of n has multiplicity $j \in S$. When S is cyclotomic and equation (3.2) holds, we obtain from Theorem 3.1 that

$$\widetilde{F}_S(s) = \frac{\zeta(b_1 s)\cdots\zeta(b_t s)}{\zeta(a_1 s)\cdots\zeta(a_r s)}.$$

Example 4.10. Let $S = \{2, 3, 4, \dots\}$. Then T is the set of squarefree positive integers. From equation (4.4) there follows the well-known formula

$$\sum_{\substack{n\geq 1\\ n \text{ squarefree}}} \frac{1}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

Example 4.11. Let $S = \{1\}$. Integers for which no prime factor has multiplicity 1 are called *powerful* [4][9]. We consider 1 to be powerful. From equation (2.5) we obtain [4, (10)]

$$\sum_{\substack{n\geq 1\\ n \text{ powerful}}} \frac{1}{n^s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}, \tag{4.7}$$

which is our third formula (1.3).

As a somewhat frivolous application, it is well-known that

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(12) = \frac{691\pi^{12}}{638512875}.$$

Hence putting $s = 1$ and $s = 2$ in equation (4.7) gives [4, (13)]

$$\sum_{\substack{n\geq 1\\ n \text{ powerful}}} \frac{1}{n} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} = \frac{315\zeta(3)}{2\pi^4} = 1.943596\cdots$$

and

$$\sum_{\substack{n\geq 1\\ n \text{ powerful}}} \frac{1}{n^2} = \frac{\zeta(4)\zeta(6)}{\zeta(12)} = \frac{15015}{1382\pi^2} = 1.100823\cdots.$$

5. Properties of cyclotomic sets

We have succeeded in our main goal of providing a unified explanation for the three formulas of Section 1 that allows substantial generalization. One obvious question remains: what can we say about the cyclotomic sets themselves? In general, the classification of cyclotomic sets, even the finite ones, is wide open. Some properties of finite cyclotomic sets are given by the next two results. For a finite set $S \subset \mathbb{P}$, write $\max(S)$ for the maximum element of S.

Theorem 5.1. *Let S be a finite cyclotomic set and $d = \max(S)$. Then for all $0 \leq j \leq d$, exactly one of j and $d - j$ belongs to S. Hence $\#S = (d + 1)/2$, so in particular d is odd.*

Proof. First note that when we write $N_S(x)$ as a minimal product of cyclotomic polynomials, the polynomial $\Phi_1(x) = 1 - x$ cannot appear

as a factor. Otherwise, if we set $x = 1$ in equation (3.3) then the left-hand side becomes 0 while the right-hand side becomes 1.

For $n \geq 2$, it's easy to see that

$$x^{\phi(n)}\Phi_n(1/x) = \Phi_n(x), \tag{5.1}$$

where $\phi(n) = \deg \Phi_n(x)$. (It is irrelevant here that ϕ is the Euler phi function.)

The left-hand side of equation (3.3) has degree $d+1$. Since it is a product of cyclotomic polynomial $\Phi_n(x)$ for $n \geq 2$, we have by equation (5.1),

$$x^{d+1}\left(1 - \left(1 - \frac{1}{x}\right)\sum_{j\in S} x^{-j}\right) = 1 - (1-x)\sum_{j\in S} x^j.$$

This equation simplifies to

$$1 + x + x^2 + \cdots + x^d = \sum_{j\in S} x^j + \sum_{j\in S} x^{d-j},$$

and the proof follows. □

Theorem 5.2. *Let S be a finite cyclotomic set. When $N_S(x)$ is written as a minimal product of cyclotomic polynomials $\Phi_n(x)$, then $n \neq 1$ and $n \neq p^k$, where p is prime and $k \geq 1$.*

Proof. We saw in the previous proof that $n \neq 1$. Now put $x = 1$ in equation (3.3). Since $\Phi_{p^r}(1) = p$, the left-hand side is divisible by p while the right-hand side is 1, a contradiction. □

For any finite $S \subset \mathbb{P}$, define $N_S(x)$ to be *palindromic* if $x^{d+1}N_S(1/x) = N_S(x)$, where $d = \max(S) = \deg N_S(x) - 1$. Hence by equation (5.1), a necessary condition for S to be cyclotomic is that $N_S(x)$ is palindromic. There are $2^{(d-1)/2}$ sets S with $\max(S) = d$, where d is odd, for which $N_S(x)$ is palindromic. Let $c(d)$ be the number of these that are cyclotomic. Here is a table of $c(d)$ for $d \leq 29$.

d	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
$c(d)$	1	2	3	5	5	9	10	12	18	22	22	37	39	41	54

Note that $c(d)$ seems to grow much more slowly than $2^{(d-1)/2}$, perhaps a little faster than linearly. A very crude upper bound on $c(d)$ is the total number $g(d)$ of polynomials of degree $d+1$ that are products of cyclotomic polynomials. Kotěšovec [6] obtained the asymptotic formula

$$\log g(d) \sim \frac{1}{\pi}\sqrt{105\zeta(3)d},$$

where ζ denotes the Riemann zeta function. Thus at least we know that $c(d)$ has subexponentional growth.

The cyclotomic sets S with $\max(S) \leq 9$ are the following, where we we abbreviate e.g. $\{1,2,5\}$ as 125.

$$\begin{gathered} 1 \\ 13, 23 \\ 125, 135, 345 \\ 1237, 1247, 1357, 2367, 4567 \\ 12359, 12569, 13579, 14679, 56789 \end{gathered}$$

Some infinite families are clear, such as $1, 23, 345, 4567, 56789, \ldots$.

Aside. The palindromic polynomials of the form

$$N_S(x) = 1 - (1-x)\sum_{j \in S} x^j,$$

where S is a finite subset of $\mathbb{P}$, seem to have many zeros α on the unit circle ($|\alpha| = 1$). There are 2^b such polynomials when $\max(S) = 2b+1$. For instance, when $b = 16$, the proportion of zeros that are on the unit circle of the $2^{16} = 65536$ polynomials is

$$\frac{751153}{1081344} = 0.69464\cdots.$$

No reason is currently known. Some further discussion appears on MathOverflow [14].

6. Numerical semigroups

We conclude this paper by explaining a connection between certain cyclotomic sets and commutative algebra. A *numerical semigroup* is a submonoid M of $\mathbb{N}$ (under addition) such that $\mathbb{N} - M$ is finite. Thus M is closed under addition and contains 0. The condition that $\mathbb{N} - M$ is finite entails no loss of generality, since every submonoid of $\mathbb{N}$ is either $\{0\}$ or of the form kM, where $k \geq 1$ and M is a numerical semigroup. It is well known that a numerical semigroup is finitely-generated.

Note. It would be more logical to use the term "numerical monoid" instead of "numerical semigroup." However, "numerical semigroup" is what appears in the literature, so we have adhered to this terminology.

Given a numerical semigroup M, define

$$A_M(x) = \sum_{i \in M} x^i,$$

the *Hilbert series* of M. Note that

$$A_M(x) = \frac{1}{1-x} - \sum_{i \in \mathbb{N} - M} x^i.$$

Following Ciolan, García-Sánchez, and Moree [3], define a numerical semigroup to be *cyclotomic* if the product $(1-x)A_M(x)$ is a product of cyclotomic polynomials. Thus a numerical semigroup M is cyclotomic if and only if $\mathbb{N}-M$ is a cyclotomic set. The set $\mathbb{N}-M$, in addition to being cyclotomic, has the further property that its complement M is closed under addition.

Example 6.1. (a) Let M be generated by $a, b \geq 2$, denoted $M = \langle a, b\rangle$, with $\gcd(a, b) = 1$. Then M is cyclotomic, and

$$A_M(x) = \frac{1-x^{ab}}{(1-x^a)(1-x^b)}.$$

(b) Let $M = \langle 4, 6, 7\rangle = \mathbb{N} - \{1, 2, 3, 5, 9\}$. Then M is cyclotomic with

$$A_M(x) = \frac{(1-x^{12})(1-x^{14})}{(1-x^4)(1-x^6)(1-x^7)}.$$

(c) Let $M = \langle 5, 6, 7\rangle = \mathbb{N} - \{1, 2, 3, 4, 8, 9\}$. Then M is not cyclotomic.

Example 6.4 below is a continuation of the previous example.

There is an interesting connection between cyclotomic semigroups and commutative algebra. Let K be a field ($\mathbb{Q}$ will do) and M a numerical semigroup. The *semigroup algebra* $K[M]$ is the subalgebra of the polynomial ring $K[z]$ generated by all monomials z^i for $i \in M$. Thus these monomials in fact form a K-basis for M. Let $M = \langle g_1, \ldots, g_m\rangle$. We say that M is a *complete intersection* if all relations among the generators $z^{g_1}, \ldots, z^{g_m}$ of $K[M]$ (as a K-algebra) are a consequence of $m-1$ of them (the minimum possible). This condition is independent of the choice of generators. Our definition of complete intersection is a special case of a more general definition from commutative algebra that we won't give here.

A relation among the generators z^{g_i} will have the form

$$(z^{g_1})^{c_1} \cdots (z^{g_m})^{c_m} = (z^{g_1})^{d_1} \cdots (z^{g_m})^{d_m}$$

for nonnegative integers $c_1, \ldots, c_m, d_1, \ldots, d_m$. The *degree* of the relation is the integer $\sum g_i c_i = \sum g_i d_i$. If M is a complete intersection with $M = \langle g_1, \ldots, g_m\rangle$, and if the minimal relations have degrees $e_1, \ldots, e_{m-1}$, then it follows from elementary commutative algebra that

$$A_M(x) = \frac{(1-x^{e_1})\cdots(1-x^{e_{m-1}})}{(1-x^{g_1})\cdots(1-x^{g_m})}.$$

Hence if $K[M]$ is a complete intersection, then M is cyclotomic. Whether the converse holds is a central open problem in the theory of cyclotomic numerical semigroups [3, Conj. 1].

Conjecture 6.2. *If M is a cyclotomic numerical semigroup, then $K[M]$ is a complete intersection.*

Example 3.2(a) shows that Conjecture 6.2 is true when M is generated by two elements. Herzog [5, Thm. 3.10] showed that it is also true when M is generated by three elements. In fact, he showed the following stronger result (the fourth condition only implicitly).

Theorem 6.3. *Let the numerical semigroup M be generated by three elements. The following four conditions are equivalent.*

- *M is cyclotomic.*
- *$K[M]$ is a complete intersection.*
- *If $S = \mathbb{N} - M$, then the polynomial $1 - (1-x)\sum_{j\in S} x^j$ is palindromic.*
- *(for readers familiar with commutative algebra) $K[M]$ is a Gorenstein ring.*

Example 6.4. (a) Let $M = \langle a, b\rangle$, with $a, b \geq 2$ and $\gcd(a,b) = 1$. Then $K[M]$ is a complete intersection. The unique minimal relation is $(z^a)^b = (z^b)^a$, of degree ab, in agreement with Example 3.2(a).

(b) The numerical semigroup $M = \langle 4, 6, 7\rangle = \mathbb{N} - \{1, 2, 3, 5, 9\}$ is cyclotomic. Setting $a = z^4$, $b = z^6$, and $c = z^7$, the minimal relations are $a^3 = b^2$ and $a^2b = c^2$, so $K[M]$ is a complete intersection. The degrees of the relations are 12 and 14, so

$$A_M(x) = \frac{(1-x^{12})(1-x^{14})}{(1-x^4)(1-x^6)((1-x^7)}.$$

Note that there are many more relations among the generators, e.g., $a^7 = c^4$, but they are all consequences of the minimal relations. For instance, squaring the second gives $c^4 = (a^2b)^2 = a^4b^2$. Substituting $b^2 = a^3$ (the first relation) gives $c^4 = a^4a^3 = a^7$.

(c) The numerical semigroup $\langle 5, 6, 7\rangle = \mathbb{N} - \{1, 2, 3, 4, 8, 9\}$ is not cyclotomic. Setting $a = z^5$, $b = z^6$, and $c = z^7$, the minimal relations are $a^4 = bc^2$, $b^2 = ac$, and $c^3 = a^3b$. Note that if we multiply the first relation by b, obtaining $a^4b = b^2c^2$, then substitute $b^2 = ac$ (the second relation) to get $a^4b = ac^3$, and then divide by a, we get $a^3b = c^3$ (the third relation). So why isn't the third relation a consequence of the first two, so we have only two minimal relations? The answer is that dividing by a is not allowed; we are only allowed to use algebra operations (linear combinations and multiplication) on the relations.

ACKNOWLEDGMENT. I am grateful to the referees for their helpful suggestions that have greatly improved the elucidation of this paper.

REFERENCES

[1] G. E. Andrews, Generalization of a partition theorem of MacMahon, *J. Combinatorial Theory* **3** (1967), 100–101.
[2] L. Carlitz, The arithmetic of polynomials in a Galois field, *Amer. J. Math.* **54** (1932), 39–50.
[3] E.-A. Ciolan, P. A. García-Sánchez, and P. Moree, Cyclotomic numerical semigroups, *SIAM J. Discrete Math.* **30** (2016), 650–668.
[4] S. W. Golomb, Powerful numbers, *Amer. Math. Monthly* **77** (1970), 848–852.
[5] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, *Manuscripta Math.* **3** (1970), 175–193.
[6] V. Kotěšovec, in A120963, OEIS Foundation Inc. (2024), The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.
[7] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.* **53** (1857), 173–175.
[8] P. A. MacMahon, *Combinatory Analysis*, vol. 2, Cambridge University Press, Cambridge, 1916; reprinted by Chelsea, New York, 1960.
[9] Powerful number, *Wikipedia*, Wikimedia Foundation, 3 April 2024, en.wikipedia.org/wiki/Powerful_number.
[10] R. Stanley, Problem 11348, *Amer. Math. Monthly* **115** (2008), 262.
[11] R. Stanley, *Enumerative Combinatorics*, vol. 1, second edition, Cambridge University Press, 2012.
[12] R. Stanley, *Enumerative Combinatorics*, vol. 2, second edition, Cambridge University Press, New York/Cambridge, 2023.
[13] R. Stanley, *Conversational Problem Solving*, American Mathematical Society, Providence, RI, 2020.
[14] R. Stanley, Polynomials with many zeros of absolute value 1, URL (version: 2024-01-29): https://mathoverflow.net/q/461829.
[15] R. Stong, Solution to 11348, *Amer. Math. Monthly* **117** (2010), 87–88.

Email address: `rstan@math.mit.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MIAMI, CORAL GABLES, FL 33124