SOME ENUMERATIVE APPLICATIONS OF CYCLOTOMIC POLYNOMIALS

RICHARD P. STANLEY

Abstract. Euler showed that the number of partitions of n into distinct parts is equal to the number of partitions of n into odd parts. MacMahon showed that the number of partitions of n for which no part occurs exactly once is equal to the number of partitions of n into parts divisible by 2 or 3. Both these results are instances of a general phenomenon based on the fact that certain polynomials are the product of cyclotomic polynomials. After discussing this assertion, we explain how it can be extended to such topics as counting certain polynomials over finite fields and obtaining Dirichlet series generating functions for certain classes of integers.

1. Introduction

Our story begins with a partition identity of MacMahon [8, p. 54]. We then consider to what extent this result can be generalized using the same basic proof technique. 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 $m_j = m_j(\lambda)$ be the number of parts of λ equal to j, called the *multiplicity* of j in λ. For a set $S \subseteq \mathbb{P} = \{1, 2, \dots\}$, let $p^S(n)$ be the number of partitions of λ such that $m_j(\lambda) \notin S$ for every $j \geq 1$. Thus the elements of S are the disallowed part multiplicities. The following theorem is a standard result in the theory of partitions.

Theorem 1.1. *For $S \subseteq \mathbb{P}$ we have*

$$\sum_{n \geq 0} p^S(n) x^n = \prod_{k \geq 1} \left(\sum_{\substack{j \geq 0 \\ j \notin S}} x^{jk} \right).$$

Proof. To expand the product on the right, choose a term $x^{j_k k}$ from the factor indexed by k, with all but finitely many $j_k = 0$. These terms

---

Date: April 28, 2024.

multiply to give the term

$$x^{\sum_{k\geq 1} j_k k}.$$

This term corresponds to the partition of $n = \sum_k j_k k$ which has j_k parts equal to k. Hence the coefficient of x^n in the expansion of the product is $p^S(n)$. ☐

By completely analogous reasoning we obtain a similar result when we restrict the *value* of the parts, rather than the multiplicity of the parts.

Theorem 1.2. *Let $T \subseteq \mathbb{P}$. Let $p_T(n)$ denote the number of partitions λ of n for which every part λ_i satisfies $\lambda_i \in T$. Then*

$$\sum_{n\geq 0} p_T(n)x^n = \prod_{j\in T}(1-x^j)^{-1}.$$

We can now state and prove the result of MacMahon.

Theorem 1.3. *Let $n \geq 0$. Then the number of partitions of n for which every part appears at least twice is equal to the number of partitions λ of n for which every part satisfies $\lambda_i \not\equiv \pm 1 \pmod 6$. Equivalently, λ_i is divisible by 2 or 3 (or both).*

Proof. Let $S = \{1\}$, so $p^S(n)$ is the number of partitions of n for which every part appears at least twice. By Theorem 1.1,

$$\begin{aligned} \sum_{n\geq 1} p^S(n)x^n &= \prod_{k\geq 1}(1+x^{2k}+x^{3k}+x^{4k}+\cdots) \\ &= \prod_{k\geq 1}\left(\frac{1}{1-x^k} - x^k\right). \end{aligned}$$

Now note that

$$\frac{1}{1-x} - x = \frac{1-x+x^2}{1-x} = \frac{1-x^6}{(1-x^2)(1-x^3)}. \tag{1.1}$$

We can replace x by x^k for any $k \geq 1$ without affecting the validity of the equation, so

$$\sum_{n\geq 1} p^S(n)x^n = \prod_{k\geq 1} \frac{1-x^{6k}}{(1-x^{2k})(1-x^{3k})}. \tag{1.2}$$

The denominator factors are of the form $1-x^m$ where $m \not\equiv \pm 1 \pmod 6$, with $1-x^{6k}$ appearing twice. The numerator factors cancel out one of the $1-x^{6k}$ factors in the denominator, leaving us with

$$\prod_{n\not\equiv \pm 1 \pmod 6} (1-x^n)^{-1},$$

and the proof follows from Theorem 1.2. □

2. Cyclotomic polynomials and cyclotomic sets

The crucial fact underlying the proof of Theorem 1.3 is the identity (1.1). To generalize it, it is convenient to introduce cyclotomic polynomials.

Let $n \geq 1$. The *cyclotomic polynomial* $\Phi_n(x)$ is the monic polynomial over the rationals $\mathbb{Q}$ whose zeros are the primitive nth roots of 1. Since we will be dealing with power series with constant term 1, it is convenient to normalize cyclotomic polynomials to have constant term 1. This makes no difference when $n \geq 2$ since $\Phi_n(0) = 1$ for $n \geq 2$. But for the purposes of this paper, we redefine $\Phi_1(x) = 1 - x$. Thus

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

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

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

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

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

$$G_S(x) = \frac{1}{1-x} - \sum_{j \in S} x^j. \tag{2.1}$$

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 $a_1, \ldots, a_r$ and $b_1, \ldots, b_t$ for which

$$G_S(x) = \frac{\prod_{i=1}^r (1 - x^{a_i})}{\prod_{j=1}^t (1 - x^{b_j})}. \tag{2.2}$$

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

$$N_S(x) = 1 - (1-x)\sum_{j\in S} x^j \in \mathbb{Z}[x]. \tag{2.3}$$

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 ($|\alpha| = 1$).

Example 2.1. (a) Equation (1.1) shows that the set $S = \{1\}$ is cyclotomic.

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

$$\begin{aligned} G_S(x) &= \frac{\Phi_6(x)\Phi_{12}(x)\Phi_{18}(x)}{\Phi_1(x)} \\ &= \frac{(1-x^{12})(1-x^{18})}{(1-x^4)(1-x^6)(1-x^9)}. \end{aligned} \tag{2.4}$$

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

$$G_S(x) = 1 + x + \cdots + x^{k-1} = \prod_{\substack{d|k \\ d\neq 1}} \Phi_d(x) = \frac{1-x^k}{1-x}. \tag{2.5}$$

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 2.2. *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 (2.3) then the left-hand side becomes 0 while the right-hand side becomes 1.

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

$$x^{\phi(n)}\Phi_n(1/x) = \Phi_n(x), \tag{2.6}$$

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

The left-hand side of equation (2.3) has degree $d+1$. Since it is a product of cyclotomic polynomial $\Phi_n(x)$ for $n \geq 2$, we have by equation (2.6),

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

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. $\square$

Theorem 2.3. *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 (2.3). Since $\Phi_{p^r}(1) = p$, the left-hand side is divisible by p while the right-hand side is 1, a contradiction. $\square$

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 (2.6), 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 $f(d)$ be the number of these that are cyclotomic. Here is a table of $f(d)$ for $d \leq 29$.

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

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

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

where ζ denotes the Riemann zeta function.

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 $1, 23, 345, 4567, 56789, \dots$.

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 lots of zeros α on the unit circle ($|\alpha| = 1$). There are 2^m such polynomials when $\max(S) = 2m+1$. For instance, when $n = 33$, the average number of zeros 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 [13].

3. Numerical semigroups

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.

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 $A_M(x)(1-x)$ 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 3.1. (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 3.4 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 $M = \langle g_1,\dots,g_m\rangle$. We say that M is a *complete intersection* if all relations among the generators $z^{g_1},\dots,z^{g_m}$ are a consequence of $m-1$ of them (the minimum possible). Our definition of complete intersection is a special case of a more general definition from commutative algebra.

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 $c_1,\dots,c_m,d_1,\dots,d_m$. The *degree* of the relation is the integer $\sum g_ic_i = \sum g_id_i$. If M is a complete intersection with $M = \langle g_1,\dots,g_m\rangle$, and if the minimal relations have degrees $e_1,\dots,e_{m-1}$, 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 3.2. *If M is a cyclotomic numerical semigroup, then $K[M]$ is a complete intersection.*

Example 2.1(a) shows that Conjecture 3.2 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 3.3. *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 3.4. (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 2.1(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.

4. Generating functions

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 sequences $\alpha = (\alpha_1, \alpha_2, \dots)$, where $\alpha_i \in \mathbb{N}$ and only finitely many $\alpha_i \neq 0$, under the operation of componentwise addition. The monoid $\mathfrak{M}$ has a unique *basis* $B = \{u_1, u_2, \dots\}$, such that (writing the binary operation on $\mathfrak{M}$ multiplicatively) every $v \in \mathfrak{M}$ can be uniquely written $v = u_1^{c_1}u_2^{c_2}\cdots$ where $c_i \in \mathbb{N}$ and all but finitely many $c_i = 0$. We call c_i the *multiplicity* of u_i in v, denoted $c_i = \mu_v(u_i)$. Let $\omega\colon \mathfrak{M} \to \mathbb{N}^k$ be a monoid homomorphism, where $k \in \mathbb{P}$ or $k = \infty$. We call ω a *weight* on $\mathfrak{M}$ if $\omega^{-1}(\alpha)$ is finite for all $\alpha \in \mathbb{N}^k$. In this situation we will associate with the pair $(\mathfrak{M}, \omega)$ and a set $S \subseteq \mathbb{P}$ a certain generating function that is especially simple when S is a cyclotomic set. In subsequent sections we give three applications by suitable choices of $(\mathfrak{M}, \omega)$.

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

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

Because each set $\omega^{-1}(\alpha)$ is finite, the series $F(x)$ 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

$$F(x) = \prod_{u \in B} (1 - x^{\omega(u)})^{-1}, \tag{4.1}$$

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

$$F_S(x) = \sum_{\substack{v \in \mathfrak{M} \\ u \in B \Rightarrow \mu_v(u) \notin S}} x^{\omega(v)}. \tag{4.2}$$

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

The main result of this section (really a simple observation) is that $F_S(x)$ can be expressed in term of $F(x)$ when S is a cyclotomic set.

Theorem 4.1. *Suppose that S is cyclotomic, and let $G_S(x)$ be as in equation* (2.1)*. Thus as in equation* (2.2) *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

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

Proof. We have, in analogy with Theorem 1.1, that

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

But

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

Hence

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

Comparing with equation (4.1) completes the proof. □

Like many general results in enumerative combinatorics, Theorem 4.1 per se is rather simple and unassuming. It is the applications that make it interesting. The next three sections are devoted to applications of Theorem 4.1.

5. Integer partitions

Let $\mathfrak{F}$ denote the set of all partitions of all integers $n \geq 0$, with the operation $\cup$ defined by $m_j(\lambda \cup \mu) = m_j(\lambda) + m_j(\mu)$ for all j, where m_j is defined at the beginning of Section 1. If we identify a partition with the multiset (set with repeated elements) of its parts, then the operation $\cup$ is just multiset union. Then $\mathfrak{F}$ is a monoid isomorphic to $\mathbb{N}^\infty$. The unique basis for $\mathfrak{F}$ consists of the partitions $(i, 0, 0, \dots)$ with only one part. If λ is a partition of n, then define $\omega(\lambda) = n$. Clearly ω is a weight on $\mathfrak{F}$.

The series $F(x)$ becomes the well-known generating function (going back to Leibniz and Euler) for the number $p(n)$ of partitions of n,

$$\sum_{n \geq 0} p(n) x^n = \prod_{i \geq 1} (1 - x^i)^{-1},$$

also the special case $S = \emptyset$ of Theorem 1.1 or $T = \mathbb{P}$ of Theorem 1.2. Moreover, $F_S(x)$ is just the series $\sum_{n \geq 0} p^S(n) x^n$ of Theorem 1.1. If S is a cyclotomic set and equation (2.2) holds, then

$$F_S(x) = \prod_{i \geq 1} \frac{(1 - x^{ia_1}) \cdots (1 - x^{ia_r})}{(1 - x^{ib_1}) \cdots (1 - x^{ib_t})}. \tag{5.1}$$

For instance, when $S = \{1\}$ we obtain equation (1.2).

In general, we can uniquely write

$$F_S(x) = \prod_{i \geq 1} (1 - x^i)^{-d_i} \tag{5.2}$$

for $d_i \in \mathbb{Z}$. The nicest situation occurs when each d_i is 0 or 1, so

$$F_S(x) = \prod_{i \in X} (1 - x^i)^{-1}.$$

for some set $X \subseteq \mathbb{P}$. The coefficient of x^n in $F_S(x)$ is then the number of partitions of n whose parts belong to X. When this situation occurs we call S a *clean* set because we obtain a "clean" partition identity of the form: for all $n \geq 0$, the number of partitions of n for which no part occurs exactly j times when $j \in S$ is equal to the number of partitions of n into parts belonging to T. This is what happened for Theorem 1.3.

Consider the coefficient of x^n in the general case of equation (5.2). Rather than just counting partitions λ whose parts belong to a set X, when $d_i \geq 2$ then we have to "color" each part of λ equal to i with one of d_i colors. When $d_i < 0$ then each part equal to i is colored with one of $-d_i$ colors, but each color can occur at most once for each i. Moreover, each part equal to i (with some color) is weighted by a multiplicative factor of -1. We still get a partition identity, but it is "messy."

Example 5.1. Let $S = \{1, 2, 3, 5, 7, 11\}$ as in Example 3.1(b). This set turns out to be clean. We have

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

where

$$i \equiv 0, 4, 6, 8, 9, 12, 16, 18, 20, 24, 27, 28, 30, 32 \pmod{36}. \tag{5.3}$$

Thus we obtain the following result.

Theorem 5.2. *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* (5.3).

Example 5.3. The set $S = \{2, 3, 4, \dots\}$ is cyclotomic and clean:

$$\frac{1}{1-x} - (x^2 + x^3 + x^4 + \cdots) = 1 + x = \frac{1-x^2}{1-x}. \tag{5.4}$$

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

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

We have

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

where i ranges over all positive integers satisfying

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

while j ranges over all positive integers satisfying

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

Example 5.5. The set $\mathbb{N} - M$, where M is the numerical semigroup $\langle a, b \rangle$ of Example 3.1(a), is cyclotomic and clean. We obtain the following straightforward generalization of MacMahon's Theorem 1.3. For a different generalization of MacMahon's theorem, see Andrews [1].

Theorem 5.6. *Let $a, b \geq 2$ and $\gcd(a, b) = 1$. Then for every $n \geq 0$, the number of partitions of n whose part multiplicities belong to the numerical semigroup $\langle a, b \rangle$ is equal to the number of partitions of n whose parts are multiples of a or b (or both).*

Although it is easy to determine for any specific cyclotomic set S, and for those belonging to some infinite classes such as that given in Example 5.5, whether or not it is clean, we don't know of any significant general results concerning clean sets.

6. Polynomials over $\mathbb{F}_q$

Let $\mathfrak{Q}$ denote the set of all monic polynomials $P(t)$ over the finite field $\mathbb{F}_q$. Under the operation of multiplication, $\mathfrak{Q}$ is a monoid isomorphic to $\mathbb{N}^\infty$. The unique basis B for $\mathfrak{Q}$ consists of those polynomials in $\mathfrak{Q}$ that are irreducible. For $P \in \mathfrak{Q}$ define $\omega(P) = \deg P$. Clearly ω is a weight on $\mathfrak{Q}$.

The series $F(x)$ 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 (2.2) holds, then

$$F_S(x) = \frac{\prod_{i=1}^{r} (1 - q x^{a_i})}{\prod_{j=1}^{t} (1 - q x^{b_j})}. \tag{6.1}$$

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 6.2 below we have $N = 6$, and it is fortuitous that $f_S(n)$ can be written in the condensed form (6.2).

Example 6.1. Let $S = \{2, 3, 4, \ldots\}$. 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 2.1(c) there follows

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

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 5.3 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 by Example 5.3.

Example 6.2. 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 (1.1) there follows (in analogy to Theorem 1.3)

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

The partial fraction decomposition 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

$$f_S(n) = q^{\lfloor n/2 \rfloor} + q^{\lfloor n/2 \rfloor - 1} - q^{\lfloor (n-1)/3 \rfloor}. \tag{6.2}$$

This formula for $f_S(n)$ first appeared as a problem in [10], with a published solution by Stong [14]. The analogy between Theorem 1.3 and the present example was noted by Stanley [12, p. 152]. In fact, it was this analogy that inspired the present paper.

Example 6.3. Let $S = \{1, 2, 3, 5, 7, 11\}$. From equation (2.4) we get

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

where $\Phi_j = \Phi_j(x)$.

7. Dirichlet series

Perhaps the most familiar monoid isomorphic to $\mathbb{N}^\infty$ is the set $\mathbb{P}$ of positive integers under the operation of multiplication. The unique basis B is the set of prime numbers. 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 $\mathbb{P}$. 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 $\sum_{\alpha\in\mathbb{N}^\infty} f(\alpha)x^\alpha$ 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 $F(x)$ and $\widetilde{F}_S(s)$ for $F_S(x)$ 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 (2.2) holds, we obtain

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

Example 7.1. Let $S = \{2, 3, 4, \dots\}$. Then T is the set of squarefree positive integers. From equation (5.4) there follows the well-known formula

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

Example 7.2. Let $S = \{1\}$. Integers for which no prime factor has multiplicity 1 are called *powerful* [4][9]. From equation (1.1) we obtain [4, (10)]

$$\sum_{\substack{n\geq 1\\ n \text{ powerful}}} \frac{1}{n^s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}. \tag{7.1}$$

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 (7.1) 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

$$\sum_{\substack{n\geq 1\\ n \text{ powerful}}} \frac{1}{n^2} = \frac{\zeta(4)\zeta(6)}{\zeta(12)} = \frac{15015}{1382\pi^2} = 0.100823\cdots.$$

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. Kotesovec, 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, *Conversational Problem Solving*, American Mathematical Society, Providence, RI, 2020.

[13] R. Stanley, Polynomials with many zeros of absolute value 1, URL (version: 2024-01-29): https://mathoverflow.net/q/461829.

[14] 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