This is to certify that the

dissertation entitled

Generating Function Proofs
of Identities and Congruences

presented by

Szu-En Cheng

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics

Major professor

Date April 28, 2003

GENERATING FUNCTION PROOFS OF IDENTITIES AND CONGRUENCES

By

Szu-En Cheng

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

2003

ABSTRACT

GENERATING FUNCTION PROOFS OF IDENTITIES AND CONGRUENCES

By

Szu-En Cheng

In this study, we combine some ideas from formal power series and symmetric functions to provide a uniform framework for proving congruences and identities. This setting permits us to uniformly explain relationships between Waring's Formulas, Newton's Identity, symmetric functions, and linear recurrence relations.

We have several different applications. In the first application, we use the cycle indicator C_n of the symmetric group and the Lagrange Inversion Theorem to derive various identities connecting several famous combinatorial sequences. In the second application, we discuss the relationship between the number of periodic points in a dynamical system, linear recurrence relations, and the power sum symmetric function in the characteristic roots of the recurrence relation. In the final application, we use our results to give explicit formulas for universal polynomials of universal λ-rings. Moreover, we provide a connection of our work with ghost rings, necklace rings, and Witt vectors.

ACKNOWLEDGEMENTS

I felt that I was in a dream when I passed my thesis defense, not only because I came back to MSU from Taiwan just one day before the defense, but also I finished my dissertation with such a busy schedule. Hence, I would like to express my deepest gratitude to my advisor, Professor Bruce E. Sagan, for his useful instruction, patient guidance, and enormous help during my graduate career.

Thanks also go to members of my thesis committee, Professors Jonathan I. Hall, Tien-Yien Li, Susan E. Schuur, and Peter Magyar, for their time and participation. Professors Susan E. Schuur and Peter Magyar proofread this thesis – I owe them a sincere debt of gratitude. I want to thank Professors Tien-Yien Li and Jonathan I. Hall for guidance and support.

I would also like to express appreciation for the support of my friends, especially Chih-Hsiung Tsai for sharing a lot of good times and hard times together in the Mathematics Department. Daniel Selahi Durusoy has shared his talents for being a mathematician and runner – we had a lot of fun running together. Thanks go to Mei-Yu Tsai for her wisdom and kindly help. Leah C. Howard is a very special friend at MSU; I will remember that we exchanged many things about culture and life experience as well as a trip to Taiwan.

Finally, it is with greatest pleasure that I thank my wife, Chia-Lin, for her understanding and confidence in me. Of course, I would like to thank my parents for their support and encouragement. There are still many people I need to thank. So, thanks again for all who love me and support me. Without them I could not make my dream come true!

TABLE OF CONTENTS

Chapter 0

Introduction

Formal power series (or generating functions) and symmetric functions are powerful tools in algebraic combinatorics. In this study, we combine some ideas from both to provide a uniform framework for proving congruences and identities. Specifically, let $R(z) = 1 + a_1 z + a_2 z^2 + \cdots$ be a fixed formal power series in $\mathbb{C}[[z]]$. Since the constant term of $R(z)$ is 1, $1/R(z)$ is still a formal power series over $\mathbb{C}$ with constant term 1. So, we can define

$$H(z) = 1 + h_1 z + h_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]],$$

$$E(z) = 1 + e_1 z + e_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]],$$

and

$$P(z) = p_1 z + p_2 z^2 + \cdots \in z\mathbb{C}[[z]]$$

by the equations

$$H(z) = \frac{1}{R(z)},$$

$$E(z) = R(-z),$$

and

$$P(z) = -z\frac{R'(z)}{R(z)} = z\frac{H'(z)}{H(z)}.$$

We then factor $R(z)$ as

$$R(z) = \prod_{n\geq 1}(1 + R_n(z))^{C_n},$$

where the $R_n(z)$ are formal power series in $\mathbb{C}[[z]]$ having z^n as the smallest power with nonzero coefficient. By using the following four types of factorizations:

$$\begin{array}{ll}
\text{Type I} & R(z) = \prod_{n\geq 1}(1-z^n)^{M_n}, \\
\text{Type II} & R(z) = \prod_{n\geq 1}\left(1+z^n+\cdots+z^{(q-1)n}\right)^{N_n}, \\
\text{Type III} & R(z) = \prod_{n\geq 1}\left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{O_n}, \\
\text{Type IV} & R(z) = \prod_{n\geq 1}(1-Q_n z^n)
\end{array}$$

where $q \geq 2$ is a positive integer, we derive various congruences and identities.

In the special case where $R(z)$ is a polynomial, $H(z)$, $E(z)$, and $P(z)$ become the generating functions for the complete homogeneous, elementary, and power sum symmetric functions in the inverses of the roots of $R(z)$. This setting permits us to uniformly explain relationships between Waring's Formulas, Newton's Identity, symmetric functions, and linear recurrence relations.

We also give some characterizations of those coefficient sequences $\{p_n\}_{n\geq 1}$ of $P(z)$ which satisfy

$$\sum_{d|n} \mu(d) p_{n/d} \equiv 0 \pmod{n}$$

or

$$\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} \equiv 0 \pmod{q^t n}$$

where q is a prime and t is a positive integer. Moreover, using our model, we settle several conjectures in the literature and generalize some known theorems.

We have several different applications. In the first, we use the cycle indicator, C_n, of the symmetric group

$$C_n(t_1, t_2, \cdots, t_n) = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{1}{k_1!k_2!\cdots k_n!}\left(\frac{t_1}{1}\right)^{k_1}\left(\frac{t_2}{2}\right)^{k_2}\cdots\left(\frac{t_n}{n}\right)^{k_n}$$

to express relationships between $R(z)$, $H(z)$, $E(z)$ and $P(z)$. Moreover, we use the cycle indicator and the Lagrange Inversion Theorem to derive various identities connecting several famous combinatorial sequences.

In the second application, we discuss the relationship between the number of periodic points in a dynamical system, linear recurrence relations, and the power sum symmetric function in the characteristic roots of the recurrence relation. Moreover, we prove the conjectures of Du in [15, 16, 17] and give algebraic proofs of some of his theorems.

In the final application, we use our results to give explicit formulas for universal polynomials of universal λ-rings. Moreover, we provide a connection of our work with ghost rings, necklace rings, and Witt vectors.

Chapter 1

Preliminaries

We use the following notation: $\mathbb{P}$ is the positive integers, $\mathbb{N}$ is the nonnegative integers, $\mathbb{Z}$ is the integers, $\mathbb{Q}$ is the rational numbers, $\mathbb{R}$ is the real numbers, and $\mathbb{C}$ is the complex numbers.

1.1 Formal power series

We recall some definitions and properties of formal power series. Details can be found in [24, 61].

Definition 1.1.1. The *algebra of formal power series* in z over $\mathbb{C}$ is

$$\mathbb{C}[[z]] = \left\{ \sum_{n\geq 0} a_n z^n \;\middle|\; a_n \in \mathbb{C} \quad \text{for all } n \geq 0 \right\}.$$

$\mathbb{C}[[z]]$ is an algebra under the operations:

Addition: $$\left(\sum_{n\geq 0} a_n z^n\right) + \left(\sum_{n\geq 0} b_n z^n\right) = \sum_{n\geq 0} (a_n + b_n) z^n.$$

Product: $$\left(\sum_{n\geq 0} a_n z^n\right)\left(\sum_{n\geq 0} b_n z^n\right) = \sum_{n\geq 0} c_n z^n \quad \text{where } c_n = \textstyle\sum_{i=0}^{n} a_i b_{n-i}.$$

Scalar multiplication: $$c\left(\sum_{n\geq 0} a_n z^n\right) = \sum_{n\geq 0} (c a_n) z^n \quad \text{where } c \in \mathbb{C}.$$ ■

If $F(z)$ and $G(z)$ are elements of $\mathbb{C}[[z]]$ satisfying $F(z)G(z) = 1$, then we write $G(z) = F(z)^{-1}$.

Theorem 1.1.2. *Let* $F(z) = \sum_{n\geq 0} a_n z^n \in \mathbb{C}[[z]]$. *Then* $F(z)^{-1}$ *exists if and only if* $a_0 \neq 0$.

■

We commonly write $a_0 = F(0)$, even through $F(z)$ is not considered to be a function of z.

We need to deal with infinite sums and products in $\mathbb{C}[[z]]$. Hence, we need the concept of *convergence*. For that, we need the following definition.

Definition 1.1.3. The *order* of nonzero $F(z) \in \mathbb{C}[[z]]$ is

$$\mathrm{ord}F(z) = \text{the smallest } n \text{ such that } z^n \text{ has nonzero coefficient in } F(z).$$

The *leading coefficient* of $F(z)$ is the coefficient of $z^{\mathrm{ord}F(z)}$. ■

Definition 1.1.4. Let $F_n(z) \in \mathbb{C}[[z]]$ for $n \geq 0$. Then the limit $\lim\limits_{n\to\infty} F_n(z) = F(z)$ exists if $\lim\limits_{n\to\infty} \mathrm{ord}(F(z) - F_n(z)) = \infty$. ■

Now, we can define infinite sums and products.

Definition 1.1.5. Let $F_n(z) \in \mathbb{C}[[z]]$ for $n \geq 0$.

(i) The *sum* $F(z) = \sum_{n\geq 0} F_n(z)$ exists in $\mathbb{C}[[z]]$ if and only if $F(z) = \lim\limits_{n\to\infty} S_n(z)$ exists where $S_n(z) = F_0(z) + F_1(z) + \cdots + F_n(z)$.

(ii) The *product* $F(z) = \prod_{n\geq 0} F_n(z)$ exists in $\mathbb{C}[[z]]$ if and only if $F(z) = \lim\limits_{n\to\infty} P_n(z)$ exists where $P_n(z) = F_0(z)F_1(z)\cdots F_n(z)$. ■

Proposition 1.1.6.

(i) *Let* $F_n(z) \in \mathbb{C}[[z]]$ *for* $n \geq 0$. *Then* $\sum_{n\geq 0} F_n(z)$ *converges if and only if* $\lim\limits_{n\to\infty} \mathrm{ord}F_n(z) = \infty$.

(*ii*) *Let* $F_n(z) \in \mathbb{C}[[z]]$ *with* $F_n(0) = 0$ *for* $n \geq 0$. *Then* $\prod_{n\geq 0}(1 + F_n(z))$ *converges if and only if* $\lim\limits_{n\to\infty} \operatorname{ord} F_n(z) = \infty$. ■

We can now define the important composition operation.

Definition 1.1.7. Let $F(z) = \sum_{n\geq 0} a_n z^n$, $G(z) = \sum_{n\geq 0} b_n z^n$ with $b_0 = 0$, then we can define the *composition* $F(G(z)) := \sum\limits_{n\geq 0} a_n G(z)^n$. Note that $b_0 = 0$ guarantees the convergence of the sum for $F(G(z))$. ■

We will need the following particular series and operations in the next chapters.

Definition 1.1.8. We define the following formal power series.

(*i*) *Exponential*

$$\exp(z) := 1 + z + \frac{z^2}{2!} + \cdots$$

(*ii*) *Logarithm*

$$\log(1+z) := z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots$$ ■

Definition 1.1.9. Let $F(z) = \sum_{n\geq 0} a_n z^n \in \mathbb{C}[[z]]$. Then $F(z)$ has

(*i*) *formal derivative*

$$F'(z) := \sum_{n\geq 0}(n+1)a_{n+1}z^n.$$

(*ii*) *formal integral*

$$\int_0^z F(x)dx := \sum_{n\geq 1} \frac{a_{n-1}}{n} z^n.$$ ■

Definition 1.1.10. Let $F(z) = \sum_{n\geq 0} a_n z^n$, $G(z) = \sum_{n\geq 0} b_n z^n \in \mathbb{C}[[z]]$. Then the *Hadamard product* of $F(z)$ and $G(z)$ is defined by

$$F(z) \odot G(z) := \sum_{n\geq 0} a_n b_n z^n.$$ ■

1.2 Arithmetic functions

We also recall some definitions and properties of arithmetic functions (see e.g [2, 28]).

Definition 1.2.1. A complex-valued function defined on the positive integers is called an *arithmetic function.* ■

Definition 1.2.2. Let α and β be two arithmetic functions. The *Dirichlet product* (or *Dirichlet convolution*) of α and β is defined by

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(d)\beta(n/d). \qquad ■$$

We have some algebraic properties of the Dirichlet product.

Proposition 1.2.3. *For any arithmetic functions α, β and γ we have*

$$\begin{aligned} \alpha * \beta &= \beta * \alpha \\ (\alpha * \beta) * \gamma &= \alpha * (\beta * \gamma). \end{aligned}$$

That is, the Dirichlet product is commutative and associative. ■

Definition 1.2.4. The arithmetic function I given by

$$I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

is called the *identity function.*

The identity function I is the identity element for the Dirichlet product.

If α and β are arithmetic functions satisfying $\alpha * \beta = I$, then we write $\beta = \alpha^{-1}$ and call β the *Dirichlet inverse* of α. ■

Theorem 1.2.5. *Let α be an arithmetic function. Then α^{-1} exists if and only if $\alpha(1) \neq 0$.*

■

Definition 1.2.6. We define the unit function u to be the arithmetic function such that $u(n) = 1$ for all $n \geq 1$. ■

We have the celebrated Möbius function and Möbius Inversion Theorem.

Definition 1.2.7. The *Möbius function* $\mu(n)$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k, \\ 0 & \text{otherwise.} \end{cases}$$

Note that u and μ are the Dirichlet inverses of each other. ■

Möbius Inversion Theorem. *Let $\alpha(n)$ and $\beta(n)$ be arithmetic functions. Then*

$$\alpha(n) = \sum_{d|n} \beta(d), \qquad \textit{for all } n \geq 1.$$

if and only if

$$\beta(n) = \sum_{d|n} \mu(d)\alpha(n/d), \qquad \textit{for all } n \geq 1.$$ ■

We also need the definition of the following function.

Definition 1.2.8. The *Euler totient* $\phi(n)$ is defined to be the number of positive integers $\leq n$ which are relatively prime to n. ■

Proposition 1.2.9. *We have*

$$\sum_{d|n} \phi(d) = n.$$ ■

In order to get congruences and identities in the next chapter, we need the following notation.

Definition 1.2.10. We use the notation $F(z) \equiv G(z) \pmod{z^n}$ where $F(z), G(z) \in \mathbb{C}[[z]]$ to mean $F(z) - G(z) \in z^n\mathbb{C}[[z]]$.

If $q \in \mathbb{P}$, we also use the notation $F(z) \equiv G(z) \pmod{q}$ to mean that $F(z) - G(z) \in q\mathbb{Z}[[z]]$. In other words, for each power of z, the difference between the corresponding coefficients of $F(z)$ and $G(z)$ is an integral multiple of q (even though the coefficients themselves may be complex). ■

Other definitions will be introduced as needed.

Chapter 2

Main Results

In this chapter, we use formal power series to obtain some general results for proving identities and congruences.

2.1 The types

Let $R(z) = 1 + a_1 z + a_2 z^2 + \cdots$ be a fixed formal power series in $\mathbb{C}[[z]]$. Since the constant term of $R(z)$ is 1, $1/R(z)$ is still a formal power series over $\mathbb{C}$ with constant term 1. So, we can define

$$H(z) = 1 + h_1 z + h_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]],$$

$$E(z) = 1 + e_1 z + e_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]],$$

and

$$P(z) = p_1 z + p_2 z^2 + \cdots \in z\mathbb{C}[[z]]$$

by the equations

$$H(z) = \frac{1}{R(z)}, \tag{2.1}$$

$$E(z) = R(-z), \tag{2.2}$$

and

$$P(z) = -z\frac{R'(z)}{R(z)} = z\frac{H'(z)}{H(z)}. \tag{2.3}$$

It is useful to write equation (2.3) as

$$R(z) = \exp\left(-\int_0^z \frac{P(x)}{x}dx\right) = \exp\left(-\sum_{n\geq 1} \frac{p_n}{n} z^n\right). \tag{2.4}$$

As we will see in Subsection 2.5.1, if $R(z)$ is a polynomial then $H(z), E(z)$ and $P(z)$ are just the generating functions for the complete homogeneous, elementary, and power sum symmetric functions in the reciprocals of the roots of $R(z)$.

We will be interested in how various factorizations of $R(z)$ translate in terms of $H(z)$, $E(z)$ and $P(z)$. But first we need some preliminary results.

Theorem 2.1.1. *If $R_n(z)$, for all $n \geq 1$ are formal power series in $\mathbb{C}[[z]]$ with* $\operatorname{ord} R_n(z) = n$, *then there are unique $C_n \in \mathbb{C}, n \geq 1$, with*

$$R(z) = \prod_{n\geq 1}(1+R_n(z))^{C_n}.$$

Proof: Notice that

$$(1+R_n(z))^{C_n} = 1 + r_n C_n z^n + \cdots$$

where $r_n \neq 0$ is the leading coefficient of $R_n(z)$. Also multiplying any formal power series by $1 + R_n(z)$ changes only the z^j terms for $j \geq n$. So, it is enough to show that we can find $C_1, C_2, \cdots$ so that

$$R(z) \equiv 1 + a_1 z + \cdots + a_n z^n \equiv \prod_{j=1}^{n}(1+R_j(z))^{C_j} \pmod{z^{n+1}},$$

for all $n \in \mathbb{P}$.

We prove this by induction on n. For $n = 1$, let

$$C_1 = \frac{a_1}{r_1}.$$

We have

$$R(z) \equiv 1 + a_1 z \equiv (1+R_1(z))^{C_1} \pmod{z^2}.$$

Assume that there exist unique C_j, for $1 \leq j \leq n-1$ such that

$$R(z) \equiv 1 + a_1 z + \cdots + a_{n-1} z^{n-1} \equiv \prod_{j=1}^{n-1}(1+R_j(z))^{C_j} \pmod{z^n}.$$

Write

$$\prod_{j=1}^{n-1}(1+R_j(z))^{C_j} = 1+a_1z+\cdots+a_{n-1}z^{n-1}+\tilde{a}_nz^n+\cdots,$$

and let

$$C_n = \frac{a_n-\tilde{a}_n}{r_n}. \tag{2.5}$$

Then

$$\begin{aligned}\prod_{j=1}^{n}(1+R_j(z))^{C_j} &= (1+a_1z+\cdots+a_{n-1}z^{n-1}+\tilde{a}_nz^n+\cdots)(1+R_n(z))^{C_n}\\ &= (1+a_1z+\cdots+a_{n-1}z^{n-1}+\tilde{a}_nz^n+\cdots)(1+(a_n-\tilde{a}_n)z^n+\cdots)\\ &= 1+a_1z+\cdots+a_nz^n+\cdots\end{aligned}$$

So,

$$R(z) \equiv 1+a_1z+\cdots+a_nz^n \equiv \prod_{j=1}^{n}(1+R_j(z))^{C_j} \pmod{z^{n+1}}$$

Therefore, by induction, we are done. ■

We need the following lemma and corollary to prove various integer congruences.

Lemma 2.1.2. *Let $q,t \in \mathbb{P}$. If $R(z) \in qz\mathbb{Z}[[z]]$, then*

$$(1+R(z))^{q^{t-1}} \equiv 1 \pmod{q^t}.$$

Proof: Induct on t. For $t=1$, the result is trivial.

Assume the lemma is true for $t-1 \geq 1$, that is

$$(1+R(z))^{q^{t-2}} = 1+q^{t-1}\tilde{R}(z)$$

for some $\tilde{R}(z) \in z\mathbb{Z}[[z]]$. Then

$$\begin{aligned}(1+R(z))^{q^{t-1}} &= \left((1+R(z))^{q^{t-2}}\right)^q\\ &= \left(1+q^{t-1}\tilde{R}(z)\right)^q\\ &= \left(1+qq^{t-1}\tilde{R}(z)+\binom{q}{2}\left(q^{t-1}\tilde{R}(z)\right)^2+\cdots+\left(q^{t-1}\tilde{R}(z)\right)^q\right)\\ &\equiv 1 \pmod{q^t}\end{aligned}$$

since $(q^{t-1})^i = q^{(t-1)i}$ and $(t-1)i \geq t$, for $i \geq 2, t \geq 2$. ■

Corollary 2.1.3. *Let $q, t \in \mathbb{P}$. Given $R_n(z)$, for all $n \geq 1$ as in Theorem 2.1.1 with $R_n(z) \in qz^n(\pm 1 + z\mathbb{Z}[[z]])$ for all $n \geq 1$. Then*

$$R(z) \in 1 + q^t z\mathbb{Z}[[z]]$$

if and only if

$$C_n \in q^{t-1}\mathbb{Z} \quad \textit{for all } n \geq 1.$$

Proof: ($\Leftarrow$) This follows from Lemma 2.1.2.

($\Rightarrow$) We proceed by induction on n as in the proof of Theorem 2.1.1. It is clear that $C_1 \in q^{t-1}\mathbb{Z}$. Assume that $C_j \in q^{t-1}\mathbb{Z}$, for $1 \leq j \leq n-1$, then $\tilde{a}_n \in q^t\mathbb{Z}$ by Lemma 2.1.2. Therefore, by equation (2.5), $C_n \in q^{t-1}\mathbb{Z}$ since $a_n \in q^t\mathbb{Z}$ and $r_n = \pm q$. ■

We will now introduce the four types of factorization that will concern us for the rest of this thesis.

2.1.1 Type I

Let

$$R_n(z) = -z^n \quad \forall n \geq 1.$$

Using these polynomials, we have the next theorem.

Theorem 2.1.4. *Let $R(z) = 1 + a_1 z + a_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]]$. There are unique $M_n \in \mathbb{C}, n \geq 1$, with*

$$R(z) = \prod_{n \geq 1} (1 - z^n)^{M_n}. \tag{2.6}$$

Moreover, we have

$$p_n = \sum_{d|n} dM_d \quad \forall n \geq 1 \tag{2.7}$$

and

$$M_n = \frac{1}{n} \sum_{d|n} \mu(d) p_{n/d} \quad \forall n \geq 1. \tag{2.8}$$

Proof: The first statement is clear because of Theorem 2.1.1.

Now taking the logarithmic derivative on both sides of (2.6), and multiplying by $-z$ gives

$$-z\frac{R'(z)}{R(z)} = \sum_{n\geq 1} nM_n \frac{z^n}{1-z^n}.$$

That is,

$$P(z) = \sum_{n\geq 1} nM_n(z^n + z^{2n} + \cdots).$$

Comparing the coefficients on both sides, we get

$$p_n = \sum_{d|n} dM_d \quad \forall n \geq 1.$$

Finally, equation (2.8) follows by applying the Möbius Inversion Theorem to (2.7). ■

We can now obtain the Cyclotomic Identity (see e.g. [40]) which has important applications in combinatorics.

Corollary 2.1.5 (Cyclotomic Identity). *If* $\alpha \in \mathbb{P}$, *then we have*

$$\frac{1}{1-\alpha z} = \prod_{n\geq 1}\left(\frac{1}{1-z^n}\right)^{M_n} \quad \textit{where} \quad M_n = \frac{1}{n}\sum_{d|n}\mu(d)\alpha^{n/d}.$$

Proof: Let $R(z) = 1 - \alpha z$. We get $p_n = \alpha^n$ from equation (2.3). Hence, by equation (2.6) and (2.8), we have the desired result. ■

Remark: It is worth noting that $M_n = \frac{1}{n}\sum_{d|n}\mu(d)\alpha^{n/d}$ is the number of primitive necklaces with n beads and α colors.

2.1.2 Type II

Let $q > 1$ be a positive integer and let

$$R_n(z) = z^n + \cdots + z^{(q-1)n} \quad \forall n \geq 1.$$

Before we can state the analog of Theorem 2.1.4 in this context, we need the following definition and lemma.

Definition 2.1.6. Let $q > 1$ be a positive integer. If $n = mq^s$, where $q \nmid m$, then we define $\operatorname{ord}_q(n) = s$.

Lemma 2.1.7. *Let $\{\alpha_n\}_{n\geq 1}$ and $\{\beta_n\}_{n\geq 1}$ be two sequences. Let $q > 1$ be a positive integer and c be a constant. Then*

$$\beta_n = \begin{cases} \sum_{d|n} \alpha_d & \text{if } q \nmid n, \\ \sum_{d|n} \alpha_d - c\sum_{d|\frac{n}{q}} \alpha_d & \text{if } q \mid n \end{cases} \tag{2.9}$$

if and only if

$$\alpha_n = \sum_{d|n} \mu(d)\beta_{\frac{n}{d}} + c\sum_{d|\frac{n}{q}} \mu(d)\beta_{\frac{n}{qd}} + \cdots + c^s \sum_{d|\frac{n}{q^s}} \mu(d)\beta_{\frac{n}{q^s d}}$$

where $s = \operatorname{ord}_q(n)$.

Proof: Using equation (2.9), we define

$$\begin{aligned} B(n) &:= \sum_{i=0}^{ord_q(n)} c^i \beta_{n/q^i} \\ &= \beta_n + c\beta_{n/q} + \cdots + c^s \beta_{n/q^s} \\ &= \left(\sum_{d|n} \alpha_d - c\sum_{d|\frac{n}{q}} \alpha_d\right) + c\left(\sum_{d|\frac{n}{q}} \alpha_d - c\sum_{d|\frac{n}{q^2}} \alpha_d\right) + \cdots + c^s \sum_{d|\frac{n}{q^s}} \alpha_d \\ &= \sum_{d|n} \alpha_d \,. \end{aligned}$$

Hence, we have

$$\beta_n = \begin{cases} B(n) & \text{if } q \nmid n, \\ B(n) - cB(n/q) & \text{if } q \mid n. \end{cases}$$

Now, by Möbius Inversion Theorem, we obtain

$$\begin{aligned}
\alpha_n &= \sum_{d|n} \mu(n/d) B(d) \\
&= \sum_{d|n} \mu(n/d) \sum_{i=0}^{ord_q(d)} c^i \beta_{d/q^i} \\
&= \sum_{i=0}^{ord_q(n)} \sum_{d|\frac{n}{q^i}} \mu\left(\frac{n}{q^i d}\right) c^i \beta_d \\
&= \sum_{i=0}^{ord_q(n)} \sum_{d|\frac{n}{q^i}} \mu(d) c^i \beta_{\frac{n}{q^i d}} \\
&= \sum_{d|n} \mu(d) \beta_{\frac{n}{d}} + c \sum_{d|\frac{n}{q}} \mu(d) \beta_{\frac{n}{qd}} + \cdots + c^s \sum_{d|\frac{n}{q^s}} \mu(d) \beta_{\frac{n}{q^s d}}.
\end{aligned}$$

This establishes the result. ■

Theorem 2.1.8. *Let* $R(z) = 1 + a_1 z + a_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]]$. *There are unique* $N_n \in \mathbb{C}, n \geq 1$, *with*

$$R(z) = \prod_{n \geq 1} \left(1 + z^n + \cdots + z^{(q-1)n}\right)^{N_n}. \tag{2.10}$$

Moreover,

$$p_n = \begin{cases} -\sum_{d|n} d N_d & \text{if } q \nmid n, \\ -\sum_{d|n} d N_d + q \sum_{d|\frac{n}{q}} d N_d & \text{if } q \mid n \end{cases} \tag{2.11}$$

and

$$N_n = -\frac{1}{n} \left(\sum_{d|n} \mu(d) p_{n/d} + q \sum_{d|\frac{n}{q}} \mu(d) p_{\frac{n}{qd}} + \cdots + q^s \sum_{d|\frac{n}{q^s}} \mu(d) p_{\frac{n}{q^s d}} \right) \tag{2.12}$$

where $s = \mathrm{ord}_q(n)$.

Proof: The first statement is clear because of Theorem 2.1.1.

We may rewrite

$$R(z) = \prod_{n \geq 1} \left(1 + z^n + \cdots + z^{(q-1)n}\right)^{N_n} = \prod_{n \geq 1} \left(\frac{1 - z^{qn}}{1 - z^n}\right)^{N_n}. \tag{2.13}$$

Now taking the logarithmic derivative on both sides of (2.13), and multiplying by $-z$ gives

$$-z\frac{R'(z)}{R(z)} = \sum_{n\geq 1} N_n \left(\frac{qnz^{qn}}{1-z^{qn}} - \frac{nz^n}{1-z^n}\right).$$

That is,

$$P(z) = \sum_{n\geq 1} qnN_n(z^{qn}+z^{2qn}+\cdots) - \sum_{n\geq 1} nN_n(z^n+z^{2n}+\cdots).$$

Comparing the coefficients on both sides, we get equation (2.11). Finally, by Lemma 2.1.7 (using $\alpha_n = -nN_n$, $\beta_n = p_n$ and $c = q$), we have the last conclusion. ■

2.1.3 Type III

Let $q > 1$ be a positive integer and

$$R_n(z) = \frac{(1-z^n)^q}{1-z^{qn}} - 1 \quad \forall n \geq 1.$$

Using these R_n, we obtain the next theorem. Its proof is similar to that of Theorem 2.1.8 and so is omitted.

Theorem 2.1.9. *Let $R(z) = 1 + a_1 z + a_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]]$. There are unique $O_n \in \mathbb{C}, n \geq 1$, with*

$$R(z) = \prod_{n\geq 1} \left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{O_n}. \tag{2.14}$$

Moreover,

$$p_n = \begin{cases} q\sum_{d|n} dO_d & \text{if } q \nmid n, \\ q\left(\sum_{d|n} dO_d - \sum_{d|\frac{n}{q}} dO_d\right) & \text{if } q \mid n \end{cases} \tag{2.15}$$

and

$$O_n = \frac{1}{qn}\left(\sum_{d|n} \mu(d) p_{n/d} + \sum_{d|\frac{n}{q}} \mu(d) p_{\frac{n}{qd}} + \cdots + \sum_{d|\frac{n}{q^s}} \mu(d) p_{\frac{n}{q^s d}}\right) \tag{2.16}$$

where $s = \mathrm{ord}_q(n)$. ■

The following corollary will be needed to establish the fundamental congruence for Type III in Theorem 2.3.4.

Corollary 2.1.10. *If q is a prime, we can write*

$$O_n = \frac{1}{qn} \sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d}.$$

Proof: We have

$$\begin{aligned}
\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} &= \sum_{d|n} \mu(d) p_{n/d} - \sum_{\substack{d|n \\ q|d}} \mu(d) p_{n/d} \\
&= \sum_{d|n} \mu(d) p_{n/d} - \sum_{d|\frac{n}{q}} \mu(qd) p_{\frac{n}{qd}} \\
&= \sum_{d|n} \mu(d) p_{n/d} - \mu(q) \sum_{\substack{d|\frac{n}{q} \\ q\nmid d}} \mu(d) p_{\frac{n}{qd}} \\
&= \sum_{d|n} \mu(d) p_{n/d} + \sum_{\substack{d|\frac{n}{q} \\ q\nmid d}} \mu(d) p_{\frac{n}{qd}} \\
&= \sum_{d|n} \mu(d) p_{n/d} + \sum_{d|\frac{n}{q}} \mu(d) p_{\frac{n}{qd}} + \cdots + \sum_{d|\frac{n}{q^s}} \mu(d) p_{\frac{n}{q^s d}}
\end{aligned}$$

where $s = \text{ord}_q(n)$. Comparing this equation with equation (2.16) gives the result. ■

2.1.4 Type IV

In the subsection, we will study a different way to factor $R(z)$. Rather than fixing $R_n(z)$ and finding the corresponding exponents, the exponents will all equal one and this will determine appropriate $R_n(z)$.

Theorem 2.1.11. *Let* $R(z) = 1 + a_1 z + a_2 z^2 + \cdots \in 1 + z\mathbb{C}[[z]]$. *There are unique* $Q_n \in \mathbb{C}, n \geq 1$, *with*

$$R(z) = \prod_{n \geq 1} (1 - Q_n z^n). \tag{2.17}$$

Moreover, we have

$$p_n = \sum_{d|n} d Q_d^{n/d} \quad \forall n \geq 1. \tag{2.18}$$

Proof: Comparing the coefficients on both sides of (2.17), we have

$$\begin{aligned} a_n &= \sum_{\substack{k_1+k_2+\cdots+k_r=n \\ 1\leq k_1<k_2<\cdots<k_r\leq n}} (-1)^r Q_{k_1} Q_{k_2} \cdots Q_{k_r} \\ &= \left(\sum_{\substack{k_1+k_2+\cdots+k_r=n \\ 1\leq k_1<k_2<\cdots<k_r<n}} (-1)^r Q_{k_1} Q_{k_2} \cdots Q_{k_r} \right) - Q_n. \end{aligned}$$

Thus, we can recursively determine $Q_1, Q_2, \cdots$.

Now, taking the logarithmic derivative on both sides of (2.17), and multiplying by $-z$ gives

$$-z\frac{R'(z)}{R(z)} = \sum_{n\geq 1} n \frac{Q_n z^n}{1-Q_n z^n}.$$

That is,

$$P(z) = \sum_{n\geq 1} n(Q_n z^n + Q_n^2 z^{2n} + \cdots).$$

Comparing the coefficients on both sides, we get equation (2.18). ■

Remark: In this situation the p_n are called the ghost components of the Q_n (see e.g. [33, p.330]). We will discuss them in more detail in Section 3.3.

The analogue of Corollary 2.1.3 in this context is as follows.

Corollary 2.1.12. *Let* $q \in \mathbb{P}$ *and* $R(z) \in 1 + z\mathbb{R}[[z]]$. *Then*

$$R(z) \in 1 + qz\mathbb{Z}[[z]]$$

if and only if

$$Q_n \in q\mathbb{Z} \quad \forall n \geq 1.$$

Proof: ($\Leftarrow$) This direction is obvious.

($\Rightarrow$) In the proof of Theorem 2.1.11, it is easy to see that if $Q_j \in q\mathbb{Z}$, for $1 \leq j \leq n-1$ then $Q_n \in q\mathbb{Z}$. Hence, we are done by induction. ■

2.2 Some operations

We wish to express the relationships between the exponents in the Type I, II and III factorizations. Let $q > 1$ be a positive integer. If

$$\begin{aligned} R(z) &= \prod_{n\geq 1}(1-z^n)^{M_n} \\ &= \prod_{n\geq 1}\left(1+z^n+\cdots+z^{(q-1)n}\right)^{N_n} \\ &= \prod_{n\geq 1}\left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{O_n} \end{aligned}$$

then we have the following relations.

Corollary 2.2.1. *If* $s = \operatorname{ord}_q(n)$ *then*

(i) $N_n = -\left(M_n + M_{n/q} + \cdots + M_{n/q^s}\right)$,

(ii) $O_n = \frac{1}{q}\left(M_n + \frac{1}{q}M_{n/q} + \cdots + \frac{1}{q^s}M_{n/q^s}\right)$,

(iii) $M_n = \begin{cases} -N_n & \text{if } q \nmid n, \\ -N_n + N_{n/q} & \text{if } q \mid n. \end{cases}$

Proof: Equations (i) and (ii) follow from Theorems 2.1.4, 2.1.8, and 2.1.9. Equation (iii) follows directly from (i). ■

It will be necessary to see how various operations on power series $R(z)$ translate to the corresponding $P(z)$ series. We will start with product, quotient, and substitution.

Proposition 2.2.2. *Suppose* $\tilde{R}(z), \hat{R}(z) \in 1 + z\mathbb{C}[[z]]$.

(i) We have

$$R(z) = \tilde{R}(z)\hat{R}(z)$$

if and only if

$$P(z) = \tilde{P}(z) + \hat{P}(z)$$

where $\tilde{P}(z)$ *and* $\hat{P}(z)$ *are related to* $\tilde{R}(z)$ *and* $\hat{R}(z)$ *as in equation* (2.3).

(ii) Similarly, we have

$$R(z) = \tilde{R}(z)/\hat{R}(z)$$

if and only if

$$P(z) = \tilde{P}(z) - \hat{P}(z).$$

(iii) Let $r \in \mathbb{P}$ and $\tilde{R}(z) \in 1 + z\mathbb{C}[[z]]$. We have

$$R(z) = \tilde{R}(z^r)$$

if and only if

$$P(z) = r\tilde{P}(z^r).$$

Proof: (i) $(\Rightarrow)$ By equation (2.3), we have

$$\begin{aligned} P(z) &= -z\frac{R'(z)}{R(z)} \\ &= -z\frac{\tilde{R}'(z)\hat{R}(z) + \tilde{R}(z)\hat{R}'(z)}{\tilde{R}(z)\hat{R}(z)} \\ &= -z\frac{\tilde{R}'(z)}{\tilde{R}(z)} - z\frac{\hat{R}'(z)}{\hat{R}(z)} \\ &= \tilde{P}(z) + \hat{P}(z). \end{aligned}$$

$(\Leftarrow)$ By (2.4), we obtain

$$\begin{aligned} R(z) &= \exp\left(-\int_0^z \frac{P(x)}{x}dx\right) \\ &= \exp\left(-\int_0^z \left(\frac{\tilde{P}(x) + \hat{P}(x)}{x}\right)dx\right) \\ &= \exp\left(-\int_0^z \frac{\tilde{P}(x)}{x}dx\right)\exp\left(-\int_0^z \frac{\hat{P}(x)}{x}dx\right) \\ &= \tilde{R}(z)\hat{R}(z). \end{aligned}$$

(ii) and (iii) are proved similarly. ■

We now consider an operation that will give the Hadamard product. We use $[i, j]$ to denote the least common multiple of i and j and (i, j) to the great common divisor of i and j.

Proposition 2.2.3. *Let* $\tilde{R}(z)$ *and* $\hat{R}(z) \in 1 + z\mathbb{C}[[z]]$. *We have*

$$R(z) = \prod_{n\geq 1}(1 - z^n)^{M_n},$$

where

$$M_n = \sum_{[i,j]=n} (i, j)\tilde{M}_i\hat{M}_j$$

and $\tilde{M}_n$ *and* $\hat{M}_n$ *are related to* $\tilde{p}_n$ *and* $\hat{p}_n$ *as in equation* (2.7),*or equivalently* (2.8), *if and only if*

$$P = \tilde{P} \odot \hat{P}.$$

Proof: ($\Leftarrow$) From the definition of Hadamard product, we have $p_n = \tilde{p}_n\hat{p}_n$. Hence, by (2.7) and (2.8), we have

$$\begin{aligned}
M_n &= \frac{1}{n}\sum_{d|n}\mu(d)p_{n/d} \\
&= \frac{1}{n}\sum_{d|n}\mu(n/d)p_d \\
&= \frac{1}{n}\sum_{d|n}\mu(n/d)\tilde{p}_d\hat{p}_d \\
&= \frac{1}{n}\sum_{d|n}\mu(n/d)\sum_{i|d}i\tilde{M}_i\sum_{j|d}j\hat{M}_j \qquad \text{(by (2.7))} \\
&= \frac{1}{n}\sum_{i,j|n}i\tilde{M}_ij\hat{M}_j\sum_{d|\frac{n}{[i,j]}}\mu\left(\frac{n}{d[i,j]}\right) \\
&= \frac{1}{n}\sum_{[i,j]=n} ij\tilde{M}_i\hat{M}_j \\
&= \sum_{[i,j]=n}(i,j)\tilde{M}_i\hat{M}_j \qquad (\text{since } ij = [i,j](i,j)).
\end{aligned}$$

($\Rightarrow$) Using the above calculation, we know

$$\begin{aligned}
M_n &= \sum_{[i,j]=n}(i,j)\hat{M}_i\tilde{M}_j \\
&= \frac{1}{n}\sum_{d|n}\mu(n/d)\tilde{p}_d\hat{p}_d \quad \forall n \geq 1.
\end{aligned}$$

Hence, by Möbius Inversion Theorem and (2.7), we have

$$p_n = \sum_{d|n} dM_d = \tilde{p}_n \hat{p}_n \quad \forall n \geq 1.$$

In this way we obtain the desired result. ■

2.3 Congruences

In this section, we will use Types I-IV to derive the fundamental congruences for use in our examples and applications.

2.3.1 Type I

The next result is equivalent to various results of Carlitz [7, 8] in number theory and of Dold [13] in dynamical systems.

Theorem 2.3.1. *The following three conditions are equivalent*

(i) $R(z) \in 1 + z\mathbb{Z}[[z]]$,

(ii) $M_n \in \mathbb{Z} \quad \forall n \geq 1$,

(iii) $\sum_{d|n} \mu(d) p_{n/d} \equiv 0 \pmod{n} \quad \forall n \geq 1$.

Proof: $(i) \Leftrightarrow (ii)$ follows from Corollary 2.1.3 with $q = t = 1$.

$(ii) \Leftrightarrow (iii)$ is clear from (2.8). ■

Remark: It is important to note that in this result and others like it to follow, even though the individual terms in the sum could be complex numbers, the sum itself is an integer and divisible by the modulus.

As a special case, we obtain Fermat's famous Little Theorem.

Corollary 2.3.2 (Fermat's Little Theorem). *Let $a \in \mathbb{Z}$ and q be a prime, then*

$$a^q \equiv a \pmod{q}.$$

Proof: Let $R(z) = 1 - az$. We obtain $p_n = a^n$ from equation (2.3). Hence, by Theorem (2.3.1) we have

$$\sum_{d|q} \mu(d) p_{q/d} = a^q - a \equiv 0 \pmod{q}. \qquad \blacksquare$$

2.3.2 Type II

Theorem 2.3.3. *Let $q > 1$ be a positive integer. Then the following three conditions are equivalent*

(i) $R(z) \in 1 + z\mathbb{Z}[[z]]$,

(ii) $N_n \in \mathbb{Z} \quad \forall n \geq 1$,

(iii) $\sum_{d|n} \mu(d) p_{n/d} + q \sum_{d|\frac{n}{q}} \mu(d) p_{\frac{n}{qd}} + \cdots + q^s \sum_{d|\frac{n}{q^s}} \mu(d) p_{\frac{n}{q^s d}} \equiv 0 \pmod{n} \quad \forall n \geq 1$,
where $s = \text{ord}_q(n)$.

Proof: $(i) \Leftrightarrow (ii)$ follows from Theorem 2.3.1 and Corollary 2.2.1. Since

$$R(z) \in 1 + z\mathbb{Z}[[z]] \Leftrightarrow M_n \in \mathbb{Z} \quad \forall n \geq 1 \Leftrightarrow N_n \in \mathbb{Z} \quad \forall n \geq 1.$$

$(ii) \Leftrightarrow (iii)$ is clear from equation (2.12). ■

2.3.3 Type III

Theorem 2.3.4. *Let q be a prime and t be a positive integer. Then the following three conditions are equivalent*

(i) $R(z) \in 1 + q^t z\mathbb{Z}[[z]]$,

(ii) $O_n \in q^{t-1}\mathbb{Z} \quad \forall n \geq 1$,

(iii) $\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} \equiv 0 \pmod{q^t n} \quad \forall n \geq 1$.

Proof: $(i) \Leftrightarrow (ii)$ follows by noticing that if q is prime then

$$(1-z^n)^q \equiv 1-z^{qn} \pmod{q}.$$

That is,

$$\frac{(1-z^n)^q}{1-z^{qn}} \in 1+qz\mathbb{Z}[[z]].$$

Now, if

$$R(z) = \prod_{n\geq 1} \left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{O_n},$$

then the result follows from Corollary 2.1.3.

$(ii) \Leftrightarrow (iii)$ is from Corollary 2.1.10. ∎

The next theorem is similar to Dieudonné-Dwork's Lemma for p-adic numbers. See, for example, [50, 32].

Theorem 2.3.5. *Let q be a prime. Then*

$$R(z) \in 1+z\mathbb{Z}[[z]]$$

if and only if

$$\frac{R(z)^q}{R(z^q)} \in 1+qz\mathbb{Z}[[z]].$$

Proof: Write

$$R(z) = \prod_{n\geq 1} (1-z^n)^{M_n},$$

and let

$$\tilde{R}(z) = \frac{R(z)^q}{R(z^q)} = \prod_{n\geq 1} \left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{M_n}.$$

Then, we have $\tilde{O}_n = M_n$ for all $n \geq 1$. Hence,

$$\begin{aligned} R(z) \in 1+z\mathbb{Z}[[z]] &\Leftrightarrow M_n \in \mathbb{Z} \quad \forall n \geq 1 \quad \text{(By Theorem 2.3.1)} \\ &\Leftrightarrow \tilde{O}_n \in \mathbb{Z} \quad \forall n \geq 1 \\ &\Leftrightarrow \tilde{R}(z) = \frac{R(z)^q}{R(z^q)} \in 1+qz\mathbb{Z}[[z]] \quad \text{(By Theorem 2.3.4).} \end{aligned}$$

This completes the proof. ∎

To use Theorem 2.3.4 in practice, we need to recast it in the following way.

Proposition 2.3.6. *Let q be a prime and $t \in \mathbb{P}$. Suppose $\tilde{R}(z), \hat{R}(z) \in 1 + z\mathbb{C}[[z]]$. Then*

$$\tilde{R}(z) \equiv \hat{R}(z) \pmod{q^t}$$

if and only if

$$\sum_{\substack{d|n \\ q\nmid d}} \mu(d)\tilde{p}_{n/d} \equiv \sum_{\substack{d|n \\ q\nmid d}} \mu(d)\hat{p}_{n/d} \pmod{q^t n} \quad \forall n \geq 1.$$

Proof: Let

$$R(z) = \tilde{R}(z)/\hat{R}(z).$$

Then

$$\begin{aligned}
&\tilde{R}(z) \equiv \hat{R}(z) \pmod{q^t} \\
&\quad \Leftrightarrow R(z) = \tilde{R}(z)/\hat{R}(z) \equiv 1 \pmod{q^t} \\
&\quad \Leftrightarrow \sum_{\substack{d|n \\ q\nmid d}} \mu(d)p_{n/d} \equiv 0 \pmod{q^t n} \quad \forall n \geq 1 \quad \text{(By Theorem 2.3.4)} \\
&\quad \Leftrightarrow \sum_{\substack{d|n \\ q\nmid d}} \mu(d)\tilde{p}_{n/d} \equiv \sum_{\substack{d|n \\ q\nmid d}} \mu(d)\hat{p}_{n/d} \pmod{q^t n} \quad \forall n \geq 1.
\end{aligned}$$

The last equivalence is because of Proposition 2.2.2. ■

The next two corollaries give examples of how Proposition 2.3.6 can be used.

Corollary 2.3.7. *Fix a positive integer l.*

(i) For the prime 2,

$$R(z) \equiv 1 + z^l \pmod{2}$$

if and only if

$$\sum_{\substack{d|n \\ 2\nmid d}} \mu(d)p_{n/d} \equiv \begin{cases} l \pmod{2n} & \textit{for } n = l2^k, \quad k \geq 0, \\ 0 \pmod{2n} & \textit{otherwise.} \end{cases}$$

(ii) Let $q \neq 2$ be a prime. Then

$$R(z) \equiv 1 + z^l \pmod{q}$$

if and only if

$$\sum_{\substack{d|n\\ q\nmid d}} \mu(d) p_{n/d} \equiv \begin{cases} -l \pmod{qn} & \textit{for } n = lq^k, \quad k \geq 0, \\ 2l \pmod{qn} & \textit{for } n = 2lq^k, \quad k \geq 0, \\ 0 \pmod{qn} & \textit{otherwise.} \end{cases}$$

Proof: (i) Let $\tilde{R}(z) = 1 - z^l \equiv R(z) \pmod 2$. It is easy to see that $\tilde{M}_i = \delta_{il}$.

Now Corollary 2.2.1 shows that

$$2n\tilde{O}_n = n\tilde{M}_n + \frac{n}{2}\tilde{M}_{n/2} + \cdots + \frac{n}{2^s}\tilde{M}_{n/2^s}$$

where $s = \mathrm{ord}_2(n)$. Moreover, $2n\tilde{O}_n$ has nonzero value if and only if $\tilde{M}_l$ appears on the right-hand side of the above equation.

Hence, by Corollary 2.1.10, we get

$$\sum_{\substack{d|n\\ 2\nmid d}} \mu(d) \tilde{p}_{n/d} = 2n\tilde{O}_n \equiv \begin{cases} l \pmod{2n} & \text{for } n = l2^k, \quad k \geq 0, \\ 0 \pmod{2n} & \text{otherwise.} \end{cases}$$

Finally, by Proposition 2.3.6, we get the desired equivalence.

(ii) Let $\tilde{R}(z) = 1 + z^l = (1 - z^l)^{-1}(1 - z^{2l})$. It is easy to see that

$$\tilde{M}_n = \begin{cases} -1 & \text{if } n = l, \\ 1 & \text{if } n = 2l, \\ 0 & \text{otherwise.} \end{cases}$$

Now Corollary 2.2.1 shows that

$$qn\tilde{O}_n = n\tilde{M}_n + \frac{n}{q}\tilde{M}_{n/q} + \cdots + \frac{n}{q^s}\tilde{M}_{n/q^s}$$

where $s = \mathrm{ord}_q(n)$. Moreover, $qn\tilde{O}_n$ has nonzero value if and only if $\tilde{M}_l$ or $\tilde{M}_{2l}$ appear on the right-hand side of the above equation.

Hence, by Corollary 2.1.10, we get

$$\sum_{\substack{d|n\\ q\nmid d}} \mu(d) \tilde{p}_{n/d} = qn\tilde{O}_n \equiv \begin{cases} -l \pmod{qn} & \text{for } n = lq^k, \quad k \geq 0, \\ 2l \pmod{qn} & \text{for } n = 2lq^k, \quad k \geq 0, \\ 0 \pmod{qn} & \text{otherwise.} \end{cases}$$

Again, we use Proposition 2.3.6 to get the desired equivalence. ■

Corollary 2.3.8. *Let q be a prime.*

(i) Suppose $l \geq 2$ and $l \neq q^s$ for any $s \geq 1$. Then

$$R(z) \equiv 1 + z + \cdots + z^{l-1} \pmod{q}$$

if and only if

$$\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} \equiv \begin{cases} -1 \pmod{qn} & \text{for } n = q^k, \quad k \geq 0, \\ l \pmod{qn} & \text{for } n = lq^k, \quad k \geq 0, \\ 0 \pmod{qn} & \text{otherwise.} \end{cases}$$

(ii) Suppose $l \geq 2$ and $l = q^s$ for some $s \geq 1$. Then

$$R(z) \equiv 1 + z + \cdots + z^{l-1} \pmod{q}$$

if and only if

$$\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} \equiv \begin{cases} -1 \pmod{qn} & \text{for } n = q^k, \quad 0 \leq k < s, \\ l-1 \pmod{qn} & \text{for } n = q^k, \quad k \geq s, \\ 0 \pmod{qn} & \text{otherwise.} \end{cases}$$

Proof: Let $\tilde{R}(z) = 1 + z + \cdots + z^{l-1} = (1-z)^{-1}(1-z^l)$. It is easy to see that

$$\tilde{M}_n = \begin{cases} -1 & \text{if } n = 1, \\ 1 & \text{if } n = l, \\ 0 & \text{otherwise.} \end{cases}$$

Now the proof is finished in the same manner as in previous corollary. ∎

2.3.4 Type IV

Theorem 2.3.9. *Let $q, t \in \mathbb{P}$. If $R(z) \in 1 + q^t z\mathbb{Z}[[z]]$, then*

$$p_{mq^s} \equiv 0 \pmod{q^{t+s}}$$

for all $m \in \mathbb{P}$ and $s \in \mathbb{N}$.

Proof: For $q = 1$ the result follows from the definition of $P(z)$. Assume $q \geq 2$. Notice that, by Corollary 2.1.12, we have $q^t \mid Q_n$, for all n.

Let d be a divisor of mq^s. If $\operatorname{ord}_q(d) = i$ and $\operatorname{ord}_q(mq^s) = j$ then

$$\begin{aligned}
\operatorname{ord}_q\left(dQ_d^{mq^s/d}\right) &\geq \operatorname{ord}_q(d) + \operatorname{ord}_q\left(Q_d^{mq^s/d}\right) \\
&\geq i + tq^{j-i} \qquad (\text{because } q^t \mid Q_d) \\
&\geq i + t(j-i+1) \qquad (\text{because } q \geq 2) \\
&= i + tj - ti + t \\
&= (t-1)(j-i) + t + j \\
&\geq t + s \qquad (\text{because } t \geq 1,\ j \geq i \text{ and } j \geq s).
\end{aligned}$$

Therefore, by Theorem 2.1.11

$$p_{mq^s} = \sum_{d \mid mq^s} dQ_d^{mq^s/d} \equiv 0 \pmod{q^{t+s}}$$

for all $m \in \mathbb{P}$ and $s \in \mathbb{N}$. ■

Remark: The converse of the above theorem is not true in general. For example, let $t = 1$ and

$$p_n = \begin{cases} q^{s+1} & \text{if } n = q^s, \quad s \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then the p_n satisfy the condition in the above theorem. Now let $\tilde{q}$ be a prime not dividing q. We have

$$\sum_{d \mid \tilde{q}} \mu(d) p_{\tilde{q}/d} = p_{\tilde{q}} - p_1 = 0 - q \not\equiv 0 \pmod{\tilde{q}}.$$

Therefore, by Theorem 2.3.1, $R(z) \notin 1 + z\mathbb{Z}[[z]]$. Hence, $R(z) \notin 1 + qz\mathbb{Z}[[z]]$.

However, in the next subsection, we will show that by adding one condition, the converse will become true.

Proposition 2.3.10. *Let* $q, t \in \mathbb{P}$. *If* $R(z) \equiv \tilde{R}(z) \pmod{q^t}$ *then*

$$p_{mq^s} \equiv \tilde{p}_{mq^s} \pmod{q^{t+s}}$$

for all $m \in \mathbb{P}$, $s \in \mathbb{N}$.

Proof: Since

$$\frac{R(z)}{\tilde{R}(z)} \equiv 1 \pmod{q'}.$$

The conclusion follows by Theorem 2.3.9 and Proposition 2.2.2. ■

2.3.5 Some characterizations

In this subsection, we will give some characterizations for $\{p_n\}_{n\geq 1}$, the sequence of coefficients of $P(z)$. First, we need the following two results.

Lemma 2.3.11. *Let α, β be arithmetic functions with integer values.*

(i) Let $q \in \mathbb{P}$. If $\alpha(n) \equiv 0 \pmod{n}$ and $\beta(n) \equiv 0 \pmod{qn}$ for all $n \geq 1$, then $(\alpha * \beta)(n) \equiv 0 \pmod{qn}$ for all $n \geq 1$.

(ii) If $\alpha(1) = \pm 1$ and $\alpha(n) \equiv 0 \pmod{n}$ for all $n \geq 1$, then $\alpha^{-1}(n) \equiv 0 \pmod{n}$ for all $n \geq 1$. Where α^{-1} is the Dirichlet inverse of α.

Proof:

(i) We have

$$\begin{aligned}(\alpha * \beta)(n) &= \sum_{d|n} \alpha(d)\beta(n/d) \\ &= \sum_{d|n} dk_d q \frac{n}{d} k'_{n/d} \quad \text{for some } k_d \text{ and } k'_{n/d} \in \mathbb{Z} \\ &= \sum_{d|n} qnk_d k'_{n/d} \\ &\equiv 0 \pmod{qn}.\end{aligned}$$

(ii) Let $\bar{\alpha}(n) = \alpha(n)/n$ which is integer-valued. Since $\bar{\alpha}(1) = \pm 1$, $\bar{\alpha}^{-1}$ exists and is still integer-valued. So, $\alpha^{-1}(n) = n\bar{\alpha}^{-1}(n) \equiv 0 \pmod{n}$. ■

The next theorem is a generalization of Jarden's result in [30], here we give a simpler proof.

Theorem 2.3.12. *Let α, β be arithmetic functions with $\alpha(1) = \pm 1$ and for all $n \geq 2$ $\sum_{d|n} \alpha(d) \equiv 0 \pmod{n}$. Then*

$$\sum_{d|n} \mu(d)\beta(n/d) \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1$$

if and only if

$$\sum_{d|n} \alpha(d)\beta(n/d) \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1.$$

Proof: "$\Rightarrow$" We are given $(\alpha * u)(n) \equiv 0 \pmod{n}$ and $(\mu * \beta)(n) \equiv 0 \pmod{n}$ for all $n \geq 1$. Therefore, by Lemma 2.3.11(i), we have

$$(\alpha * \beta)(n) = (\alpha * u) * (\mu * \beta)(n) \equiv 0 \pmod{n} \quad \text{for all } n \geq 1.$$

"$\Leftarrow$" Since $(\alpha * u)(n) \equiv 0 \pmod{n}$ for all $n \geq 1$, by Lemma 2.3.11(ii) we have

$$(\alpha * u)^{-1}(n) \equiv 0 \pmod{n} \quad \text{for all } n \geq 1.$$

Again, by Lemma 2.3.11(i) and $(\alpha * \beta)(n) \equiv 0 \pmod{n}$ for all $n \geq 1$, we get

$$((\alpha * u)^{-1} * (\alpha * \beta))(n) \equiv 0 \pmod{n} \quad \text{for all } n \geq 1.$$

On the other hand,

$$\begin{aligned}(\alpha * u)^{-1} * (\alpha * \beta) &= (u^{-1} * \alpha^{-1}) * (\alpha * \beta)\\ &= (\mu * \alpha^{-1}) * (\alpha * \beta)\\ &= \mu * \beta.\end{aligned}$$

That is $(\mu * \beta)(n) \equiv 0 \pmod{n}$ for all $n \geq 1$. ■

Remark: In particular, we may choose α to be Euler's totient ϕ function or Jordan's totient J_k function since $\sum_{d|n} \phi(d) = n$ and $\sum_{d|n} J_k(d) = n^k$. However α need not be a multiplicative function. For example, in [30] Jarden used this result on the function defined by $\alpha(1) = 1$, $\sum_{d|n} \alpha(d) = -n$ for $n > 1$. Now $\alpha(2) = -3$, and $\alpha(3) = -4$, $\alpha(6) = 0$, showing that the conditions on α in Theorem 2.3.12 do not imply that α is multiplicative.

Now, we have the following characterizations for $\{p_n\}_{n\geq 1}$.

Theorem 2.3.13. *The following are equivalent:*

(i) $\exp\left(\sum_{n\geq 1}\frac{p_n}{n}z^n\right) \in 1+z\mathbb{Z}[[z]]$,

(ii) $\sum_{d|n}\mu(d)p_{n/d} \equiv 0 \pmod{n}$ *for all* $n \geq 1$,

(iii) $\sum_{d|n}\alpha(d)p_{n/d} \equiv 0 \pmod{n}$ *for all* $n \geq 1$, *where* α *is an arithmetic function with* $\alpha(1) = \pm 1$ *and* $\sum_{d|n}\alpha(d) \equiv 0 \pmod{n}$ *for all* $n \geq 2$,

(iv) $p_{mq^s} \equiv p_{mq^{s-1}} \pmod{q^s}$ *for all primes* q *and* $m, s \in \mathbb{P}$.

Proof: $(i) \Leftrightarrow (ii)$ Note that

$$R(z) = \exp\left(-\sum_{n\geq 1}\frac{p_n}{n}z^n\right) \in 1+z\mathbb{Z}[[z]]$$

if and only if

$$\exp\left(\sum_{n\geq 1}\frac{p_n}{n}z^n\right) \in 1+z\mathbb{Z}[[z]].$$

Now we can apply Theorem 2.3.1 to get the result.

$(ii) \Leftrightarrow (iii)$ follows by writing $p(n) = p_n$ and applying Theorem 2.3.12.

$(iv) \Rightarrow (ii)$ If $q \mid n$, we can write $n = mq^s$ where $s = \mathrm{ord}_q(n)$. Thus

$$\begin{aligned}\sum_{d|n}\mu(d)p_{n/d} &= \sum_{\substack{d|n\\ q\nmid d}}\mu(d)p_{n/d} + \sum_{\substack{d|n\\ q|d}}\mu(d)p_{n/d}\\ &= \sum_{d|m}\mu(d)p_{mq^s/d} + \sum_{d|m}\mu(qd)p_{mq^{s-1}/d}\\ &= \sum_{d|m}\mu(d)\left(p_{mq^s/d} - p_{mq^{s-1}/d}\right)\\ &\equiv 0 \pmod{q^s} \qquad \text{(by } (iv)).\end{aligned}$$

Since the above congruence is true for any prime $q \mid n$, we have established (ii).

$(i) \Rightarrow (iv)$ Let

$$\tilde{R}(z) = \frac{R(z)^q}{R(z^q)}$$

which is in $1+qz\mathbb{Z}[[z]]$ by Theorem 2.3.5. Hence, by Theorem 2.3.9

$$\tilde{p}_{mq^s} \equiv 0 \pmod{q^{s+1}}$$

for all $m, s \in \mathbb{P}$.

On the other hand, by Proposition 2.2.2, we have

$$\tilde{P}(z) = qP(z) - qP(z^q).$$

That is

$$\tilde{p}_{mq^s} = q(p_{mq^s} - p_{mq^{s-1}}) \equiv 0 \pmod{q^{s+1}}$$

for all $m, s \in \mathbb{P}$. Thus we have (iv). ■

Remark: $(i) \Leftrightarrow (iv)$ has been proved by Beukers [5]. Stanley [62, p.72] also give a proof of the equivalence of $(i), (ii)$ and (iv) for $1 \le n \le N$, where N is a fixed positive integer.

We have an analogous characterization using Type III. Before we can state the result, we need some another definition and a couple of results.

Definition 2.3.14. Let α, β be arithmetic functions and q be a prime. We define $\alpha *_q \beta$ as follows.

$$(\alpha *_q \beta)(n) = (\alpha * \beta)(n) + (\alpha * \beta)(n/q) + \cdots + (\alpha * \beta)(n/q^s)$$

where $s = \operatorname{ord}_q(n)$.

Lemma 2.3.15. *We have*

$$\alpha * (\beta *_q \gamma) = (\alpha * \beta) *_q \gamma.$$

Proof: This follows directly from the definitions. ■

We now have an analogue of Theorem 2.3.12 for Type III.

Theorem 2.3.16. *Let q be a prime and $t \in \mathbb{P}$. Let α, β be arithmetic functions with $\alpha(1) = \pm 1$ and $\sum_{d|n} \alpha(d) \equiv 0 \pmod{n}$ for all $n \ge 2$. Then*

$$(\mu *_q \beta)(n) \equiv 0 \pmod{q^t n} \quad \text{for all } n \ge 1$$

if and only if

$$(\alpha *_q \beta)(n) \equiv 0 \pmod{q^t n} \quad \textit{for all } n \geq 1.$$

Proof: ”⇒” Since $(\alpha * u)(n) \equiv 0 \pmod{n}$ and $(\mu *_q \beta)(n) \equiv 0 \pmod{q^t n}$ for all $n \geq 1$. By Lemmas 2.3.11(i) and 2.3.15, we have

$$(\alpha *_q \beta)(n) = (\alpha * u) * (\mu *_q \beta)(n) \equiv 0 \pmod{q^t n} \quad \text{for all } n \geq 1.$$

”⇐” We know

$$(\alpha * u)^{-1}(n) \equiv 0 \pmod{n} \quad \text{for all } n \geq 1.$$

Again by Lemma 2.3.11(i) and $(\alpha *_q p)(n) \equiv 0 \pmod{q^t n}$ for all $n \geq 1$, we get

$$\Big((\alpha * u)^{-1} * (\alpha *_q \beta)\Big)(n) \equiv 0 \pmod{q^t n} \quad \text{for all } n \geq 1.$$

On the other hand,

$$\begin{aligned}(\alpha * u)^{-1} * (\alpha *_q \beta) &= (u^{-1} * \alpha^{-1}) * (\alpha *_q \beta)\\ &= (\mu * \alpha^{-1}) * (\alpha *_q \beta)\\ &= \mu *_q \beta \qquad \text{(by Lemma 2.3.15).}\end{aligned}$$

That is $(\mu *_q \beta)(n) \equiv 0 \pmod{q^t n}$ for all $n \geq 1$. ∎

Now we have the following characterization.

Theorem 2.3.17. *Let q be a prime and $t \in \mathbb{P}$. The following are equivalent:*

(i) $\exp\left(\sum_{n\geq 1} \frac{p_n}{n} z^n\right) \in 1 + q^t z\mathbb{Z}[[z]]$,

(ii) $\sum_{\substack{d|n\\ q\nmid d}} \mu(d) p_{n/d} \equiv 0 \pmod{q^t n}$ *for all $n \geq 1$,*

(iii) $(\alpha *_q p)(n) \equiv 0 \pmod{q^t n}$ *for all $n \geq 1$, where $p(n) = p_n$ and α is an arithmetic function with $\alpha(1) = \pm 1$ and $\sum_{d|n} \alpha(d) \equiv 0 \pmod{n}$ for all $n \geq 2$,*

(iv) $p_{m\tilde{q}^s} \equiv p_{m\tilde{q}^{s-1}} \pmod{\tilde{q}^s}$ *and* $p_{mq^s} \equiv 0 \pmod{q^{t+s}}$ *for all primes $\tilde{q}$ other than q and $m, s \in \mathbb{P}$.*

Proof: $(i) \Leftrightarrow (ii)$ Note that

$$\exp\left(\sum_{n\geq 1} \frac{p_n}{n} z^n\right) \in 1 + q^t z\mathbb{Z}[[z]].$$

if and only if

$$\exp\left(-\sum_{n\geq 1} \frac{p_n}{n} z^n\right) \in 1 + q^t z\mathbb{Z}[[z]].$$

Now we can apply Theorem 2.3.4 to get the result.

$(ii) \Leftrightarrow (iii)$ follows by noticing that

$$(\mu *_q \beta)(n) = \sum_{\substack{d|n \\ q\nmid d}} \mu(d)\beta(n/d)$$

from the proof of Corollary 2.1.10. Now apply Theorem 2.3.16.

$(iv) \Rightarrow (ii)$ Let $\tilde{q}$ ba a prime other than q. If $\tilde{q} \mid n$, we can write $n = m\tilde{q}^s$ where $s = \operatorname{ord}_{\tilde{q}}(n)$. Thus

$$\begin{aligned}
\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} &= \sum_{\substack{d|n \\ q\nmid d,\ \tilde{q}\nmid d}} \mu(d) p_{n/d} + \sum_{\substack{d|n \\ q\nmid d,\ \tilde{q}|d}} \mu(d) p_{n/d} \\
&= \sum_{\substack{d|m \\ q\nmid d}} \mu(d) p_{m\tilde{q}^s/d} + \sum_{\substack{d|m \\ q\nmid d}} \mu(\tilde{q}d) p_{m\tilde{q}^{s-1}/d} \\
&= \sum_{\substack{d|m \\ q\nmid d}} \mu(d) \left(p_{m\tilde{q}^s/d} - p_{m\tilde{q}^{s-1}/d}\right) \\
&\equiv 0 \pmod{\tilde{q}^s} \qquad \text{(by } (iv)).
\end{aligned}$$

For q, if $q \mid n$ then we can write $n = mq^s$ where $s = \operatorname{ord}_q(n)$. Hence

$$\begin{aligned}
\sum_{\substack{d|n \\ q\nmid d}} \mu(d) p_{n/d} &= \sum_{d|m} \mu(d) p_{mq^s/d} \\
&\equiv 0 \pmod{q^{t+s}} \qquad \text{(by } (iv)).
\end{aligned}$$

Combining the above two congruences, we establish (ii).

$(i) \Rightarrow (iv)$ Since $R(z) \in 1 + q^t z\mathbb{Z}[[z]] \subset 1 + z\mathbb{Z}[[z]]$, Theorems 2.3.13 and 2.3.9 combine to give $p_{m\tilde{q}^s} \equiv p_{m\tilde{q}^{s-1}} \pmod{\tilde{q}^s}$ and $p_{mq^s} \equiv 0 \pmod{q^{t+s}}$ for all primes $\tilde{q}$ and $m, s \in \mathbb{P}$. ∎

2.4 Basic identities

In this section, we will show how equations (2.3) and (2.4) lead to generalizations for various famous identities.

First, we have an identity which generalizes Newton's power sum formula from his book "Arithmetica Universalis" ([44, pp. 107–108] [46, pp. 361–362]) and which follows easily from equation (2.3).

Theorem 2.4.1. *We have*

$$P(z)R(z) + zR'(z) = 0.$$

Equivalently,

$$p_n + a_1 p_{n-1} + \cdots + a_{n-1} p_1 + n a_n = 0 \quad \forall n \geq 1. \qquad \blacksquare$$

Newton did not actually prove his formula. There are many different proofs in the literature (e.g. [4, 39, 69]) but this is arguably the shortest and easiest.

Second, we obtain three identities which generalizes Waring's Formulas [67]. See also [10, 11, 38].

Theorem 2.4.2. *We have*

$$p_n = \sum_{k_1+2k_2+\cdots+nk_n=n} (-1)^{k_1+\cdots+k_n} \frac{n}{k_1+\cdots+k_n} \binom{k_1+\cdots+k_n}{k_1,\ldots,k_n} a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}, \tag{2.19}$$

$$p_n = \sum_{k_1+2k_2+\cdots+nk_n=n} (-1)^{k_1+\cdots+k_n-1} \frac{n}{k_1+\cdots+k_n} \binom{k_1+\cdots+k_n}{k_1,\ldots,k_n} h_1^{k_1} h_2^{k_2} \cdots h_n^{k_n}, \tag{2.20}$$

$$p_n = \sum_{k_1+2k_2+\cdots+nk_n=n} (-1)^{k_2+k_4+\cdots} \frac{n}{k_1+\cdots+k_n} \binom{k_1+\cdots+k_n}{k_1,\ldots,k_n} e_1^{k_1} e_2^{k_2} \cdots e_n^{k_n}. \tag{2.21}$$

Proof: To obtain the first expression for p_n, use equation (2.4) to get

$$\begin{aligned}
\sum_{n\geq 1} \frac{p_n}{n} z^n &= -\log(R(z)) \\
&= -\log\left(1 + (a_1 z^1 + a_2 z^2 + \cdots)\right) \\
&= \sum_{i\geq 1} \frac{(-1)^i}{i} \left(a_1 z^1 + a_2 z^2 + \cdots\right)^i.
\end{aligned}$$

The conclusion follows by comparing the coefficients of z^n on both sides.

The other two identities are obtained similarly. ■

Next, we can use equation (2.4) to obtain some identities which are inverses to our generalizations of Waring's Formulas.

Theorem 2.4.3. *We have*

$$a_n = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{(-1)^{k_1+k_2+\cdots+k_n}}{1^{k_1}k_1!2^{k_2}k_2!\cdots n^{k_n}k_n!} p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \tag{2.22}$$

$$h_n = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{1}{1^{k_1}k_1!2^{k_2}k_2!\cdots n^{k_n}k_n!} p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \tag{2.23}$$

$$e_n = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{(-1)^{k_2+k_4+\cdots}}{1^{k_1}k_1!2^{k_2}k_2!\cdots n^{k_n}k_n!} p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}. \tag{2.24}$$

Proof: By equation (2.4),

$$\begin{aligned}\sum_{n\geq 1} a_n z^n &= \exp\left(-\sum_{n\geq 1} \frac{p_n}{n} z^n\right) \\ &= \sum_{i\geq 0} \left(-\sum_{n\geq 1} \frac{p_n}{n} z^n\right)^i \Big/ i! \\ &= \sum_{i\geq 0} \frac{(-1)^i}{i!} \left(\frac{p_1}{1} z^1 + \frac{p_2}{2} z^2 + \cdots\right)^i.\end{aligned}$$

The conclusion follows by comparing the coefficients of z^n on both sides.

Again, the other two identities are obtained similarly. ■

We can simplify the notation in the previous two theorems by using partitions. A *partition* of n, denoted $\lambda \vdash n$, is a sequence of positive integers

$$\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_l)$$

with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_l$ and $\sum \lambda_i = n$. We also write $\lambda = (1^{k_1}2^{k_2}\cdots n^{k_n})$ where k_i is the multiplicity of i in λ.

The *length* of λ is the number of parts of λ,

$$l(\lambda) = k_1 + k_2 + \cdots + k_n.$$

The *weight* of λ is

$$|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_l = k_1 + 2k_2 + \cdots + nk_n = n.$$

We also use the following notation:

$$z_\lambda = 1^{k_1} k_1! 2^{k_2} k_2! \cdots n^{k_n} k_n!,$$
$$\mu_\lambda = \frac{l(\lambda)!}{k_1! k_2! \cdots k_n!}$$

and

$$\epsilon_\lambda = (-1)^{|\lambda| - l(\lambda)}.$$

For $f = a, h, e$ or p and $\lambda \vdash n$, we write

$$f_\lambda = f_{\lambda_1} f_{\lambda_2} \cdots f_{\lambda_l} = f_1^{k_1} f_2^{k_2} \cdots f_n^{k_n}.$$

Thus, we can rewrite Theorems 2.4.2 and 2.4.3 in a manner that will be familiar to the reader conversant with symmetric functions.

Theorem 2.4.4. *We have*

$$p_n = \sum_{\lambda \vdash n} (-1)^{l(\lambda)} \frac{n}{l(\lambda)} \mu_\lambda a_\lambda, \tag{2.25}$$
$$p_n = \sum_{\lambda \vdash n} (-1)^{l(\lambda)-1} \frac{n}{l(\lambda)} \mu_\lambda h_\lambda, \tag{2.26}$$
$$p_n = \sum_{\lambda \vdash n} \epsilon_\lambda \frac{n}{l(\lambda)} \mu_\lambda e_\lambda. \qquad \blacksquare$$

Theorem 2.4.5. *We have*

$$a_n = \sum_{\lambda \vdash n} (-1)^{l(\lambda)} z_\lambda^{-1} p_\lambda, \tag{2.27}$$
$$h_n = \sum_{\lambda \vdash n} z_\lambda^{-1} p_\lambda,$$
$$e_n = \sum_{\lambda \vdash n} \epsilon_\lambda z_\lambda^{-1} p_\lambda. \qquad \blacksquare$$

The next two theorems contain other relations between the coefficients of our power series.

Theorem 2.4.6. *We have*

$$h_n + a_1 h_{n-1} + \cdots + a_{n-1} h_1 + a_n = 0 \quad \forall n \geq 1, \tag{2.28}$$

and

$$h_n = \sum_{\lambda \vdash n} (-1)^{l(\lambda)} \mu_\lambda a_\lambda .$$

Proof: Since $R(z)H(z) = 1$, we have the first identity.

From $H(z) = R(z)^{-1}$, we get

$$\begin{aligned} 1 + h_1 z + h_2 z^2 + \cdots &= \left(1 + (a_1 z^1 + a_2 z^2 + \cdots)\right)^{-1} \\ &= \sum_{i \geq 0} (-1)^i (a_1 z^1 + a_2 z^2 + \cdots)^i \end{aligned}$$

Now compare the coefficients of z^n on both sides to get the second identity. ■

Theorem 2.4.7. *We have*

(i) $p_n = -(a_1 h_{n-1} + 2a_2 h_{n-2} + \cdots + (n-1) a_{n-1} h_1 + n a_n) \quad \forall n \geq 1,$

(ii) $p_n = h_1 a_{n-1} + 2h_2 a_{n-2} + \cdots + (n-1) h_{n-1} a_1 + n h_n \quad \forall n \geq 1.$

Proof: These follow directly by writing equation (2.3) as

$$P(z) = -zR'(z)H(z),$$

and

$$P(z) = zH'(z)R(z).$$

■

Combining equation (2.25) with our previous results, we can get expressions for the Type I and III exponents in terms of the coefficients of $R(z)$.

Theorem 2.4.8. *We have*

$$M_n = \sum_{d|n} \frac{\mu(d)}{d} \sum_{\lambda \vdash \frac{n}{d}} (-1)^{l(\lambda)} \frac{\mu_\lambda}{l(\lambda)} a_\lambda,$$

and if q is a prime then

$$O_n = \frac{1}{q} \sum_{\substack{d|n \\ q\nmid d}} \frac{\mu(d)}{d} \sum_{\lambda \vdash \frac{n}{d}} (-1)^{l(\lambda)} \frac{\mu_\lambda}{l(\lambda)} a_\lambda.$$

Proof: By equation (2.8), we have

$$\begin{aligned} M_n &= \frac{1}{n} \sum_{d|n} \mu(d) p_{n/d} \\ &= \frac{1}{n} \sum_{d|n} \mu(d) \sum_{\lambda \vdash \frac{n}{d}} (-1)^{l(\lambda)} \frac{n}{d} l(\lambda)^{-1} \mu_\lambda a_\lambda \qquad \text{(by (2.25))} \\ &= \sum_{d|n} \frac{\mu(d)}{d} \sum_{\lambda \vdash \frac{n}{d}} (-1)^{l(\lambda)} l(\lambda)^{-1} \mu_\lambda a_\lambda. \end{aligned}$$

Hence, we get the first identity. The second one is also obtained similarly using Corollary 2.1.10. ■

We conclude this section by giving one simple example for demonstration. More examples will be given in Section 2.6.

Example 2.4.9. Let $R(z) = 1 - z$. Then by equations (2.1)–(2.3) we have

$$\begin{aligned} H(z) &= 1 + z + z^2 + \cdots \\ E(z) &= 1 + z \\ P(z) &= z + z^2 + \cdots \end{aligned}$$

Hence, by Theorem 2.4.5 we have

$$0 = \sum_{\lambda \vdash n} (-1)^{l(\lambda)} z_\lambda^{-1} \quad \text{for } n > 1, \tag{2.29}$$

$$1 = \sum_{\lambda \vdash n} z_\lambda^{-1}, \tag{2.30}$$

and

$$0 = \sum_{\lambda \vdash n} \epsilon_\lambda z_\lambda^{-1} \quad \text{for } n > 1.$$

Identity (2.29) is Cayley's Identity [9] and identity (2.30) is well-known as Cauchy's Identity [49].

Moreover, by equation (2.26) we have

$$1 = \sum_{\lambda \vdash n} (-1)^{l(\lambda)-1} \frac{n}{l(\lambda)} \mu_\lambda, \quad \text{for } n > 0.$$

This is equivalent to an identity in [10, 59]. ■

2.5 Symmetric functions, linear recurrence relations and matrices

In this section, we will discuss the case when $R(z)$ is a polynomial.

2.5.1 Symmetric functions

When $R(z) = 1 + a_1 z^1 + \cdots + a_r z^r$ is a polynomial of degree r in $\mathbb{C}[z]$, there is a connection with symmetric functions. First, define

$$F(z) = z^r R\left(\frac{1}{z}\right).$$

That is,

$$F(z) = z^r + a_1 z^{r-1} + \cdots + a_{r-1} z + a_r.$$

Assume that $\alpha_1, \alpha_2, \cdots, \alpha_r \in \mathbb{C}$ are the roots of $F(z)$. We can write

$$F(z) = \prod_{i=1}^{r} (z - \alpha_i),$$

or equivalently

$$R(z) = \prod_{i=1}^{r} (1 - \alpha_i z). \tag{2.31}$$

Now define the following symmetric functions:

The *nth complete homogeneous symmetric function* in the roots of $F(z)$ is

$$h_n := \sum_{1 \le i_1 \le \cdots \le i_n \le r} \alpha_{i_1} \cdots \alpha_{i_n}.$$

The *nth elementary symmetric function* in the roots of $F(z)$ is

$$e_n := \sum_{1 \le i_1 < \cdots < i_n \le r} \alpha_{i_1} \cdots \alpha_{i_n}.$$

The *nth power sum symmetric function* in the roots of $F(z)$ is

$$p_n := \sum_{i=1}^{r} \alpha_i^n.$$

The corresponding generating functions are

$$\begin{aligned}
H(z) &:= \sum_{n \ge 0} h_n z^n = \prod_{i=1}^{k} \frac{1}{1-\alpha_i z}, \\
E(z) &:= \sum_{n \ge 0} e_n z^n = \prod_{i=1}^{k} (1+\alpha_i z), \\
P(z) &:= \sum_{n \ge 1} p_n z^n = \sum_{n \ge 1} \sum_{i=1}^{k} \alpha_i^n z^n \\
&= \sum_{i=1}^{k} \sum_{n \ge 1} (\alpha_i z)^n \\
&= \sum_{i=1}^{k} \frac{\alpha_i z}{1-\alpha_i z}.
\end{aligned}$$

Comparing these last three equations with (2.31), we see that $H(z), E(z), P(z)$ and $R(z)$ satisfy the equations (2.1)–(2.3) and so all of the results from the previous sections apply. Specializing Theorem 2.4.1 to this case where $a_n = 0$ for $n > r$, we immediately have Newton's original power sum formula.

Theorem 2.5.1. *We have*

$$p_n + a_1 p_{n-1} + \cdots + a_{n-1} p_1 + n a_n = 0 \qquad \text{if } 1 \le n \le r,$$

and

$$p_n + a_1 p_{n-1} + \cdots + a_r p_{n-r} = 0 \qquad \text{if } n > r. \tag{2.32}$$

■

In the same manner, Theorem 2.4.4 gives Waring's formulas. For example,

Theorem 2.5.2. *We have*

$$p_n = \sum_{\substack{\lambda \vdash n \\ \lambda_1 \leq r}} (-1)^{l(\lambda)} \frac{n}{l(\lambda)} \mu_\lambda a_\lambda. \tag{2.33}$$

■

Similarly, Theorem 2.4.6 specializes to the following theorem.

Theorem 2.5.3. *We have*

$$h_n + a_1 h_{n-1} + \cdots + a_{n-1} h_1 + a_n = 0 \qquad \text{if } 1 \leq n \leq r,$$

$$h_n + a_1 h_{n-1} + \cdots + a_r h_{n-r} = 0 \qquad \text{if } n > r \tag{2.34}$$

and

$$h_n = \sum_{\substack{\lambda \vdash n \\ \lambda_1 \leq r}} (-1)^{l(\lambda)} \mu_\lambda a_\lambda. \tag{2.35}$$

■

The next example will be used in Subsection 3.2.2.

Example 2.5.4. Fix a positive integer $r \geq 2$ and $a, b \in \mathbb{C}$. Let

$$R(z) = 1 - az - bz^r.$$

By Theorem 2.5.2 we have

$$
\begin{aligned}
p_n &= \sum_{k_1+2k_2+\cdots+rk_r=n} (-1)^{k_1+\cdots+k_r} \frac{n}{k_1+\cdots+k_r} \binom{k_1+\cdots+k_r}{k_1,\ldots,k_r} (-a)^{k_1} 0^{k_2} \cdots 0^{k_{r-1}} (-b)^{k_r} \\
&= \sum_{k_1+rk_r=n} (-1)^{k_1+k_r} \frac{n}{k_1+k_r} \binom{k_1+k_r}{k_r} (-a)^{k_1} (-b)^{k_r} \\
&= \sum_{k_1+rk_r=n} \frac{n}{k_1+k_r} \binom{k_1+k_r}{k_r} a^{k_1} b^{k_r} \\
&= \sum_{k_r=0}^{\lfloor \frac{n}{r} \rfloor} \frac{n}{(n-rk_r)+k_r} \binom{(n-rk_r)+k_r}{k_r} a^{n-rk_r} b^{k_r} \\
&= \sum_{k=0}^{\lfloor \frac{n}{r} \rfloor} \frac{n}{n-(r-1)k} \binom{n-(r-1)k}{k} a^{n-rk} b^{k}.
\end{aligned}
$$

In particular, we have

$$
p_n = \begin{cases} a^n & \text{for } 1 \le n < r, \\ a^n + na^{n-r}b & \text{for } r \le n < 2r. \end{cases}
$$

■

2.5.2 Linear recurrence relations

Given a linear recurrence relation

$$
A_n + a_1 A_{n-1} + \cdots + a_r A_{n-r} = 0 \qquad \text{for } n > r
$$

with initial conditions $A_1, A_2, \cdots, A_r$, where $a_i \in \mathbb{C}$, $1 \le i \le r$. The *characteristic polynomial* of the recurrence relation is

$$
F(z) = z^r + a_1 z^{r-1} + \cdots + a_r,
$$

and its roots $\alpha_1, \alpha_2, \cdots, \alpha_r \in \mathbb{C}$ are called the *characteristic roots*. Note that the solution of the recurrence relation is determined uniquely by the initial conditions $A_1, A_2, \cdots, A_r$.

We wish to see what initial conditions must be imposed so that the solution to our recurrence will just be the nth power sum of the characteristic roots $\alpha_1, \alpha_2, \cdots, \alpha_r$. Combining Newton's Formula (2.32) (for the recurrence relation) and Waring's Formula (2.33) (for the initial conditions), we get the desired constraints.

Theorem 2.5.5. *The solution of the recurrence relation*

$$A_n + a_1 A_{n-1} + \cdots + a_n A_{n-r} = 0 \qquad \text{for } n > r$$

with initial conditions

$$\begin{aligned} A_1 &= -a_1 \\ A_2 &= a_1^2 - 2a_2 \\ \vdots &= \vdots \\ A_r &= \sum_{\substack{\lambda \vdash n \\ \lambda_1 \leq r}} (-1)^{l(\lambda)} \frac{n}{l(\lambda)} \mu_\lambda a_\lambda \end{aligned}$$

is

$$A_n = \alpha_1^n + \alpha_2^n + \cdots + \alpha_r^n$$

where the α_i are the characteristic roots of the recurrence relation. ■

Similarly, combining equation (2.34) (for the recurrence relation) and equation (2.35) (for the initial conditions), we get the initial conditions and recurrence relation for the nth complete homogeneous symmetric function in the characteristic roots $\alpha_1, \alpha_2, \cdots, \alpha_r$.

Theorem 2.5.6. *The solution of the recurrence relation*

$$A_n + a_1 A_{n-1} + \cdots + a_n A_{n-r} = 0 \qquad \text{for } n > r$$

with initial conditions

$$\begin{aligned} A_1 &= -a_1 \\ A_2 &= a_1^2 - a_2 \\ \vdots &= \vdots \\ A_r &= \sum_{\substack{\lambda \vdash n \\ \lambda_1 \leq r}} (-1)^{l(\lambda)} \mu_\lambda a_\lambda \end{aligned}$$

is

$$A_n = \sum_{1 \leq i_1 \leq \cdots \leq i_n \leq r} \alpha_{i_1} \cdots \alpha_{i_n}$$

where the α_i are the characteristic roots of the recurrence relation. ■

Just as in Proposition 2.2.2, we will need to know how to handle addition and substraction of power sums of the characteristic roots. Here, we provide a more general result.

Theorem 2.5.7. *Let* $\{\tilde{A}_n\}_{n\geq 1}$ *be the solution of the recurrence relation*

$$\tilde{A}_n + \tilde{a}_1\tilde{A}_{n-1} + \cdots + \tilde{a}_r\tilde{A}_{n-r} = 0 \qquad \textit{for } n > r \tag{2.36}$$

with initial conditions $\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_r$*. Also, let* $\{\hat{A}_n\}_{n\geq 1}$ *be the solution of the recurrence relation*

$$\hat{A}_n + \hat{a}_1\hat{A}_{n-1} + \cdots + \hat{a}_s\hat{A}_{n-s} = 0 \qquad \textit{for } n > s \tag{2.37}$$

with initial conditions $\hat{A}_1, \hat{A}_2, \cdots, \hat{A}_s$*. Then the solution of the recurrence relation*

$$A_n + a_1A_{n-1} + \cdots + a_{r+s}A_{n-(r+s)} = 0 \qquad \textit{for } n > r+s \tag{2.38}$$

where $a_i = \tilde{a}_i + \tilde{a}_{i-1}\hat{a}_1 + \cdots + \tilde{a}_1\hat{a}_{i-1} + \hat{a}_i$*, with initial conditions*

$$A_n = \beta\tilde{A}_n + \gamma\hat{A}_n \qquad \textit{for } 1 \leq n \leq r+s \textit{ and } \beta, \gamma \in \mathbb{C},$$

is

$$A_n = \beta\tilde{A}_n + \gamma\hat{A}_n \qquad \textit{for } n \geq 1.$$

Proof: The characteristic polynomial of the recurrence relation (2.38) is

$$(z^r + \tilde{a}_1z^{r-1} + \cdots + \tilde{a}_r)(z^s + \hat{a}_1z^{s-1} + \cdots + \hat{a}_s).$$

Since $z^r + \tilde{a}_1z^{r-1} + \cdots + \tilde{a}_r$ is the characteristic polynomial of (2.36) and $z^s + \hat{a}_1z^{s-1} + \cdots + \hat{a}_s$ is the characteristic polynomial of (2.37), we have $\{\tilde{A}_n\}_{n\geq 1}$ and $\{\hat{A}_n\}_{n\geq 1}$ are the solutions of the recurrence relation (2.38) with initial conditions $\tilde{A}_n$, $1 \leq n \leq r+s$ and $\hat{A}_n$, $1 \leq n \leq r+s$ respectively. Therefore, by the superposition principle, we obtain the desired result. ■

The next theorem will be used in proving some conjectures of Du in Subsection 3.2.2.

Theorem 2.5.8. *Factor* $R(z) = 1 + a_1z + \cdots + a_{r+s}z^{r+s}$ *as* $R(z) = \tilde{R}(z)\hat{R}(z)$ *for polynomials* $\tilde{R}(z)$, $\hat{R}(z)$ *of degree* r *and* s*. Then the solution of the recurrence relation*

$$A_n + a_1A_{n-1} + \cdots + a_{r+s}A_{n-(r+s)} = 0 \qquad \textit{for } n > r+s$$

with initial conditions

$$A_n = \tilde{p}_n - \hat{p}_n \qquad \text{for } 1 \leq n \leq r+s$$

is

$$A_n = \tilde{p}_n - \hat{p}_n \qquad \text{for all } n \geq 1.$$

Proof: This follows directly from the previous theorem with $\tilde{A}_n = \tilde{p}_n$, $\hat{A}_n = \hat{p}_n$, $\beta = 1$, and $\gamma = -1$. ∎

2.5.3 Matrices

We can also connect our work with the determinant and the trace of a matrix.

Let X be a matrix in $\mathcal{M}_{r\times r}(\mathbb{C})$. The *characteristic polynomial* of X is

$$F(z) = \det(zI - X).$$

Paralleling the development in Subsection 2.5.1, define

$$R(z) := z^r F\left(\frac{1}{z}\right) = \det(I - zX).$$

Let $\alpha_1, \alpha_2, \cdots, \alpha_r$ be the roots of $F(z)$. It is a well-known result that

$$p_n = \sum_{i=1}^{r} \alpha_i^n = \operatorname{tr}(X^n).$$

Therefore, we have

$$P(z) = \sum_{n\geq 1} p_n z^n = \sum_{n\geq 1} \operatorname{tr}(X^n) z^n. \tag{2.39}$$

Hence, we have the following theorem which connects the determinant and the trace of a matrix.

Theorem 2.5.9. *We have*

$$\det(I - zX)^{-1} = \exp\left(\sum_{n\geq 1} \frac{\operatorname{tr}(X^n)}{n} z^n\right). \tag{2.40}$$

Proof: This follows from equation (2.39) and (2.4). ∎

Corollary 2.5.10. *Let $\tilde{X}$ be a matrix in $\mathcal{M}_{r\times r}(\mathbb{C})$ and $\hat{X}$ in $\mathcal{M}_{s\times s}(\mathbb{C})$. We have*

$$\det(I - z\tilde{X} \otimes \hat{X})^{-1} = \exp\left(\sum_{n\geq 1} \frac{\operatorname{tr}(\tilde{X}^n)\operatorname{tr}(\hat{X}^n)}{n} z^n\right) \tag{2.41}$$

where $\otimes$ is the tensor product.

Proof: Let

$$X = \tilde{X} \otimes \hat{X}.$$

Then we have

$$\operatorname{tr}(X^n) = \operatorname{tr}(\tilde{X}^n)\operatorname{tr}(\hat{X}^n) \qquad \text{for all } n \geq 1.$$

Hence, by Theorem 2.5.9 we are done. ■

2.6 Various examples

In this section, we use our techniques to derive various congruences and identities, some of which have appeared in the literature.

2.6.1 Congruences

The next example follows immediately from Theorem 2.3.4, Proposition 2.3.6, and Corollaries 2.3.7–2.3.8.

Example 2.6.1. We have the following results.

(*i*)

$$R(z) \equiv 1 \pmod 2$$

if and only if

$$\sum_{\substack{d|n\\ 2\nmid d}} \mu(d) p_{n/d} \equiv 0 \pmod{2n}.$$

(ii)

$$R(z) \equiv 1+z \pmod 2$$

if and only if

$$\sum_{\substack{d|n \\ 2\nmid d}} \mu(d) p_{n/d} \equiv \begin{cases} 1 \pmod{2n} & \text{for } n = 2^k, \quad k \geq 0, \\ 0 \pmod{2n} & \text{otherwise.} \end{cases}$$

(iii)

$$R(z) \equiv 1+z^2 \pmod 2$$

if and only if

$$\sum_{\substack{d|n \\ 2\nmid d}} \mu(d) p_{n/d} \equiv \begin{cases} 2 \pmod{2n} & \text{for } n = 2^k, \quad k \geq 1, \\ 0 \pmod{2n} & \text{otherwise.} \end{cases}$$

(iv)

$$R(z) \equiv 1+z+z^2 \pmod 2$$

if and only if

$$\sum_{\substack{d|n \\ 2\nmid d}} \mu(d) p_{n/d} \equiv \begin{cases} -1 \pmod{2n} & \text{for } n = 2^k, \quad k \geq 0, \\ 3 \pmod{2n} & \text{for } n = 3 \cdot 2^k, \quad k \geq 0. \\ 0 \pmod{2n} & \text{otherwise.} \end{cases}$$

■

A conjecture of P. Filipponi

The following two examples generalize the results in [1, 21].

In [21], P. Filipponi defined a sequence $\{A_n\}_{n\geq 0}$ by

$$A_n - A_{n-1} - cA_{n-2} = 0 \qquad \text{for } n \geq 2 \tag{2.42}$$

with initial conditions $A_0 = 2$ and $A_1 = 1$, where $c \geq 1$ is a natural number. He showed that if $c = q$ where q is an odd prime then

$$A_{q^s} \equiv 1 \pmod{q^s} \qquad \text{for all } s \in \mathbb{P}.$$

Moreover, he conjectured that if $c = q-1$ and $q \geq 5$ is a prime then the above congruence is also true.

Later, in [1], R. André-Jeannin proved the above conjecture and also generalized it as follows.

If $q \geq 1$ is a natural number and $c \equiv 0 \pmod{q}$ then

$$A_{q^s} \equiv 1 \pmod{q^{s+1}} \qquad \text{for all } s \in \mathbb{N}.$$

And, if $q \geq 5$ is a prime and $c \equiv -1 \pmod{q}$ then

$$A_{q^s} \equiv 1 \pmod{q^{s+1}} \qquad \text{for all } s \in \mathbb{N}.$$

In order to use our results and techniques to get congruences, we need to use A_1 and A_2 as the initial conditions. Since from (2.42) we know $A_2 = 1+2c$, we get the initial conditions $A_1 = 1$ and $A_2 = 1+2c$. Now, by Theorem 2.5.5, we obtain

$$A_n = p_n \qquad \text{for all } n \geq 1$$

where p_n is the n-th power sum in the characteristic roots of the recurrence relation (2.42). Note also that (2.42) corresponds to

$$R(z) = 1 - z - cz^2.$$

So the next theorem has André-Jeannin's first congruence as the special case when $t = m = 1$.

Theorem 2.6.2. *Let $q, t \in \mathbb{P}$. If $R(z) \equiv 1 - z \pmod{q^t}$ then*

$$p_{mq^s} \equiv 1 \pmod{q^{t+s}}$$

for all $m \in \mathbb{P}$, $s \in \mathbb{N}$.

Proof: Let $\tilde{R}(z) = 1 - z$. Then from (2.3)

$$\tilde{P}(z) = \frac{z}{1-z} = z + z^2 + \cdots$$

So, $\tilde{p}_n = 1$ for all $n \in \mathbb{P}$. We now apply Proposition 2.3.10 to get the conclusion. ■

Similarly André-Jeannin's second congruence follows from the next result when $t = 1$ because if $q \geq 5$ is prime then $q \equiv \pm 1 \pmod 6$.

Theorem 2.6.3. *Let $q, t \in \mathbb{P}$. If $R(z) \equiv 1 - z + z^2 \pmod{q^t}$ then*

$$p_{q^s} \equiv \begin{cases} 2 \pmod{q^{s+t}} & \textit{if } q \equiv 0 \pmod 6, \\ 1 \pmod{q^{s+t}} & \textit{if } q \equiv \pm 1 \pmod 6, \\ -1 \pmod{q^{s+t}} & \textit{if } q \equiv \pm 2 \pmod 6, \\ -2 \pmod{q^{s+t}} & \textit{if } q \equiv 3 \pmod 6 \end{cases}$$

for all $s \in \mathbb{P}$.

Proof: Let $\tilde{R}(z) = 1 - z + z^2$. Since

$$\tilde{R}(z) = 1 - z + z^2 = \frac{1+z^3}{1+z}.$$

We have, using (2.3),

$$\tilde{P}(z) = \frac{-3z^3}{1+z^3} + \frac{z}{1+z} = 3(-z^3 + z^6 - \cdots) + (z - z^2 + \cdots).$$

So,

$$\tilde{p}_n = \begin{cases} 2 & \text{if } n \equiv 0 \pmod 6, \\ 1 & \text{if } n \equiv \pm 1 \pmod 6, \\ -1 & \text{if } n \equiv \pm 2 \pmod 6, \\ -2 & \text{if } n \equiv 3 \pmod 6. \end{cases}$$

Notice that $\pm q^s \equiv \pm q \pmod 6$ for all $q, s \in \mathbb{P}$. Again, we apply Proposition 2.3.10 to get the desired result. ■

2.6.2 Identities

We can use our machinery to get interesting factorizations of exponentials.

Theorem 2.6.4. *Let $q > 1$ be a positive integer.*

(*i*) $\displaystyle\prod_{n \geq 1} (1 - z^n)^{\mu(n)/n} = \exp(-z)$,

$$(ii)\ \prod_{n\geq 1}\left(1+z^n+\cdots+z^{(q-1)n}\right)^{\mu(n)/n} = \exp(z-z^q),$$

$$(iii)\ \prod_{n\geq 1}\left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{\mu(n)/n} = \exp(-qz+z^q).$$

Proof: (i) Let

$$R(z)=\prod_{n\geq 1}(1-z^n)^{\mu(n)/n}.$$

By equation (2.7)

$$p_n=\sum_{d|n} d\,\frac{\mu(d)}{d}=\sum_{d|n}\mu(d)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore, $P(z)=z$. Hence, by equation (2.4), we have the desired result.

(ii) Let

$$\tilde{R}(z)=\prod_{n\geq 1}\left(1+z^n+\cdots+z^{(q-1)n}\right)^{\mu(n)/n}$$

Using the result in (i), we get

$$\tilde{R}(z)=\frac{R(z^q)}{R(z)}=\frac{\exp(-z^q)}{\exp(-z)}=\exp(z-z^q).$$

(iii) Let

$$\hat{R}(z)=\prod_{n\geq 1}\left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{\mu(n)/n}$$

Again, using the result in (i), we obtain

$$\hat{R}(z)=\frac{R(z)^q}{R(z^q)}=\frac{\exp(-z)^q}{\exp(-z^q)}=\exp(-qz+z^q).$$ ■

Theorem 2.6.5. *Let $q>1$ be a positive integer.*

$$(i)\ \prod_{n\geq 1}(1-z^n)^{\phi(n)/n}=\exp\left(\frac{-z}{1-z}\right),$$

$$(ii)\ \prod_{n\geq 1}\left(1+z^n+\cdots+z^{(q-1)n}\right)^{\phi(n)/n}=\exp\left(\frac{z}{1-z}-\frac{z^q}{1-z^q}\right),$$

$$(iii)\ \prod_{n\geq 1}\left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{\phi(n)/n}=\exp\left(\frac{-qz}{1-z}+\frac{z^q}{1-z^q}\right).$$

Proof: (i) Let

$$R(z) = \prod_{n\geq 1}(1-z^n)^{\phi(n)/n}.$$

By equation (2.7)

$$p_n = \sum_{d|n} d\,\frac{\phi(d)}{d} = \sum_{d|n}\phi(d) = n.$$

Therefore,

$$P(z) = z + 2z^2 + 3z^3 + \cdots$$

Hence, by equation (2.4), we have

$$R(z) = \exp\left(-z - z^2 - z^3 - \cdots\right) = \exp\left(\frac{-z}{1-z}\right).$$

(ii) and (iii) follow by the same method as in Theorem 2.6.4. ■

For the next result, we recall the definition of Liouville's function and one of its properties from number theory (see, e.g. [2]).

Definition 2.6.6. *Liouville's function* $\lambda(n)$ is defined by

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{a_1+\cdots+a_k} & \text{if } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. \end{cases}$$ ■

Proposition 2.6.7. *We have*

$$\sum_{d|n}\lambda(d) = \begin{cases} 1 & \textit{if } n \textit{ is a square,} \\ 0 & \textit{otherwise.} \end{cases}$$ ■

Theorem 2.6.8. *Let $q > 1$ be a positive integer.*

$$(i)\ \prod_{n\geq 1}(1-z^n)^{\lambda(n)/n} = \exp\left(-\sum_{n\geq 1}\frac{z^{n^2}}{n^2}\right),$$

$$(ii)\ \prod_{n\geq 1}\left(1+z^n+\cdots+z^{(q-1)n}\right)^{\lambda(n)/n} = \exp\left(\sum_{n\geq 1}\frac{z^{n^2}}{n^2} - \sum_{n\geq 1}\frac{z^{qn^2}}{n^2}\right),$$

$$(iii)\ \prod_{n\geq 1}\left(\frac{(1-z^n)^q}{1-z^{qn}}\right)^{\lambda(n)/n} = \exp\left(-\sum_{n\geq 1}\frac{qz^{n^2}}{n^2} + \sum_{n\geq 1}\frac{z^{qn^2}}{n^2}\right).$$

Proof: Let

$$R(z)=\prod_{n\geq 1}(1-z^n)^{\lambda(n)/n}.$$

By Equation (2.7)

$$p_n=\sum_{d|n}d\,\frac{\lambda(d)}{d}=\sum_{d|n}\lambda(d)=\begin{cases}1 & \text{if } n \text{ is a square,}\\ 0 & \text{otherwise.}\end{cases}$$

Therefore,

$$P(z)=z+z^4+z^9+\cdots$$

Hence, by equation (2.4), we have

$$R(z)=\exp\left(-\sum_{n\geq 1}\frac{z^{n^2}}{n^2}\right).$$

(ii) and (iii) follow by the same method as in Theorem 2.6.4. ■

Theorem 2.6.9. *Let $q>1$ be a prime. We have*

$$(i)\ \prod_{\substack{n\geq 1\\ q\nmid n}}(1-z^n)^{-\mu(n)/n}=\exp\left(\sum_{s\geq 0}\frac{z^{q^s}}{q^s}\right),$$

$$(ii)\ \prod_{\substack{n\geq 1\\ q\nmid n}}(1-z^n)^{-\phi(n)/n}=\exp\left(\sum_{n\geq 1}\frac{z^n}{q^{\mathrm{ord}_q(n)}}\right),$$

$$(iii)\ \prod_{\substack{n\geq 1\\ q\nmid n}}(1-z^n)^{-\lambda(n)/n}=\exp\left(\sum_{s\geq 0}\sum_{\substack{m\geq 1\\ q\nmid m}}\frac{z^{m^2q^s}}{m^2q^s}\right).$$

Proof: Let

$$R(z)=\prod_{\substack{n\geq 1\\ q\nmid n}}(1-z^n)^{-\mu(n)/n}.$$

By equation (2.7)

$$p_n=-\sum_{\substack{d|n\\ q\nmid d}}d\,\frac{\mu(d)}{d}=-\sum_{\substack{d|n\\ q\nmid d}}\mu(d).$$

However,

$$\sum_{\substack{d|n \\ q\nmid d}} \mu(d) = \sum_{d|\frac{n}{q^s}} \mu(d) \qquad \text{where } s = \operatorname{ord}_q(n).$$

That is,

$$\sum_{\substack{d|n \\ q\nmid d}} \mu(d) = \begin{cases} 1 & \text{if } n = q^s, \quad s \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$P(z) = -z - z^q - z^{q^2} + \cdots$$

Hence, by equation (2.4), we have the desired result.

(ii) and (iii) follow by noting that

$$\sum_{\substack{d|n \\ q\nmid d}} \phi(d) = \sum_{d|\frac{n}{q^s}} \phi(d) = \frac{n}{q^s} \qquad \text{where } s = \operatorname{ord}_q(n).$$

and

$$\sum_{\substack{d|n \\ q\nmid d}} \lambda(d) = \sum_{d|\frac{n}{q^s}} \lambda(d) = \begin{cases} 1 & \text{if } \frac{n}{q^s} \text{ is a square, where } s = \operatorname{ord}_q(n), \\ 0 & \text{otherwise.} \end{cases}$$

Now apply the same method as in (i). ■

Note that (i) is so-called the *Artin-Hasse exponential* (see e.g [32, 50]).

Example 2.6.10. Let

$$R(z) = (1-z)^c,$$

where $c \in \mathbb{C}$. Then, by equation (2.3) we have

$$P(z) = cz + cz^2 + \cdots$$

Hence, by Theorem 2.4.5, we have

$$(-1)^n \binom{c}{n} = \sum_{\lambda \vdash n} (-c)^{l(\lambda)} z_\lambda^{-1}, \tag{2.43}$$

$$\binom{c+n-1}{n} = \sum_{\lambda \vdash n} c^{l(\lambda)} z_\lambda^{-1}, \tag{2.44}$$

$$\binom{c}{n} = \sum_{\lambda \vdash n} \epsilon_\lambda c^{l(\lambda)} z_\lambda^{-1}. \tag{2.45}$$

Note that identity (2.44) is Sylvester's Identity [63].

If c is a positive integer, then from (2.43) and (2.45) we get

$$0 = \sum_{\lambda \vdash n} (-c)^{l(\lambda)} z_\lambda^{-1} \quad \text{for } n > c,$$

and

$$0 = \sum_{\lambda \vdash n} \epsilon_\lambda c^{l(\lambda)} z_\lambda^{-1} \quad \text{for } n > c.$$

■

Example 2.6.11. Let

$$R(z) = 1 - cz - cz^2 - \cdots = (1-z)^{-1}(1-(c+1)z),$$

where $c \in \mathbb{C}$. Then, by Proposition 2.2.2, we have

$$P(z) = \sum_{n \geq 1} ((c+1)^n - 1) z^n.$$

Hence, by Theorem 2.4.4, we get

$$(c+1)^n - 1 = \sum_{\lambda \vdash n} c^{l(\lambda)} \frac{n}{l(\lambda)} \mu_\lambda.$$

If $c = 1$, then the previous identity becomes

$$2^n - 1 = \sum_{\lambda \vdash n} \frac{n}{l(\lambda)} \mu_\lambda$$

which is an identity in [10]. ■

Example 2.6.12. Let $q > 1$ be a positive integer and

$$R(z) = (1-z)^q / (1-z^q).$$

By Proposition 2.2.2, we get

$$p_n = \begin{cases} 0 & \text{if } q \mid n, \\ q & \text{otherwise.} \end{cases}$$

Moreover, from

$$R(z) = (1-z)^q(1-z^q)^{-1} = (1-z)^q(1+z^q+z^{2q}+\cdots)$$

we have

$$a_n = \begin{cases} 0 & \text{if } q \text{ odd and } n \equiv 0 \pmod{q}, \quad n \geq 1, \\ 2 & \text{if } q \text{ even and } n \equiv 0 \pmod{q}, \quad n \geq 1, \\ (-1)^{n'}\binom{q}{n'} & \text{otherwise, where } n' = n - q\lfloor n/q \rfloor. \end{cases}$$

And from

$$H(z) = (1-z^q)(1-z)^{-q} = (1-z)^{-q} - z^q(1-z)^{-q}$$

we get

$$h_n = \binom{q+n-1}{q-1} - \binom{n-1}{q-1}.$$

Hence, by Theorem 2.4.5, we obtain

$$\sum_\lambda \frac{(-q)^{l(\lambda)}}{z_\lambda} = \begin{cases} 0 & \text{if } q \text{ odd and } n \equiv 0 \pmod{q}, \quad n \geq 1, \\ 2 & \text{if } q \text{ even and } n \equiv 0 \pmod{q}, \quad n \geq 1, \\ (-1)^{n'}\binom{q}{n'} & \text{otherwise, where } n' = n - q\lfloor n/q \rfloor \end{cases} \tag{2.46}$$

$$\sum_\lambda \frac{q^{l(\lambda)}}{z_\lambda} = \binom{q+n-1}{q-1} - \binom{n-1}{q-1}, \tag{2.47}$$

and

$$\sum_\lambda \epsilon_\lambda \frac{q^{l(\lambda)}}{z_\lambda} = \begin{cases} 0 & \text{if } q \text{ odd and } n \equiv 0 \pmod{q}, \quad n \geq 1, \\ 2 & \text{if } q \text{ even and } n \equiv 0 \pmod{q}, \quad n \geq 1, \\ \binom{q}{n'} & \text{otherwise, where } n' = n - q\lfloor n/q \rfloor \end{cases} \tag{2.48}$$

where the summation is over all partitions λ of n into parts are not divisible by q.

Note that identity (2.47) is an identity in [41]. In particular, if $q = 2$ then we get Schur's Identity [56, 57]

$$\sum_\lambda \frac{2^{l(\lambda)}}{z_\lambda} = 2,$$

where the summation is over all partitions λ of n into odd parts. ■

Chapter 3

Applications

Now we apply our results in the previous chapter to several different problems.

3.1 Cycle indicators and combinatorial sequences

In this section,we will study the connection with cycle indicators and combinatorial sequences. We start with the definition of cycle indicators.

Definition 3.1.1. The *cycle indicator* C_n of the nth symmetric group is

$$C_n(t_1, t_2, \cdots, t_n) = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{1}{k_1!k_2!\cdots k_n!} \left(\frac{t_1}{1}\right)^{k_1} \left(\frac{t_2}{2}\right)^{k_2} \cdots \left(\frac{t_n}{n}\right)^{k_n}. \qquad \blacksquare$$

We wish to express the relationships between $R(z)$, $H(z)$, $E(z)$ and $P(z)$ in terms of C_n. Using our results in Section 2.4, we can get the following expressions.

Theorem 3.1.2. *We have*

$$a_n = C_n(-p_1, -p_2, \cdots, -p_n), \tag{3.1}$$

$$h_n = C_n(p_1, p_2, \cdots, p_n), \tag{3.2}$$

$$e_n = C_n(p_1, -p_2, \cdots, (-1)^{n-1}p_n) \tag{3.3}$$

and

$$\sum_{n\geq 0} C_n(-p_1,-p_2,\cdots,-p_n)z^n = \exp\left(-\sum_{n\geq 1}\frac{p_n}{n}z^n\right), \tag{3.4}$$

$$\sum_{n\geq 0} C_n(p_1,p_2,\cdots,p_n)z^n = \exp\left(\sum_{n\geq 1}\frac{p_n}{n}z^n\right), \tag{3.5}$$

$$\sum_{n\geq 0} C_n(p_1,-p_2,\cdots,(-1)^{n-1}p_n)z^n = \exp\left(\sum_{n\geq 1}(-1)^{n-1}\frac{p_n}{n}z^n\right). \tag{3.6}$$

Proof: These identities are obtained directly from Theorem 2.4.3, equations (2.4), (2.1) and (2.2). ■

Note that equation (3.5) is a well-know expression in algebraic combinatorics (see e.g [23, 27, 49, 62]).

There are many interesting specialization of Theorem 3.1.2 related to combinatorial sequences and special polynomials. For instance, Gessel [23], Hsu and Shiue [26, 27], and Riordan [49] had some identities which can be expressed in terms of C_n. Our machinery can easily be applied to reprove these and get various others.

For example, we can rewrite equations (2.43)–(2.45) in Example 2.6.10 as

$$\begin{aligned}(-1)^n\binom{c}{n} &= C_n(-c,-c,\cdots,-c),\\ \binom{c+n-1}{n} &= C_n(c,c,\cdots,c),\\ \binom{c}{n} &= C_n\left(c,-c,\cdots,(-1)^{n-1}c\right)\end{aligned}$$

where $c \in \mathbb{C}$.

Similarly, by equations (2.46)–(2.48) in Example 2.6.12, we have

$$C_n(-q,\cdots,-q,\underset{\underset{q}{\uparrow}}{0},-q,\cdots,-q,\underset{\underset{2q}{\uparrow}}{0},-q,\cdots)$$
$$=\begin{cases} 0 & \text{if } q \text{ odd and } n\equiv 0 \pmod{q} \quad n\geq 1,\\ 2 & \text{if } q \text{ even and } n\equiv 0 \pmod{q} \quad n\geq 1,\\ (-1)^{n'}\binom{q}{n'} & \text{otherwise, where } n'=n-q\lfloor n/q\rfloor,\end{cases}$$

$$C_n(q,\cdots,q,\underset{\underset{q}{\uparrow}}{0},q,\cdots,q,\underset{\underset{2q}{\uparrow}}{0},q,\cdots)=\binom{q+n-1}{q-1}-\binom{n-1}{q-1},$$

$$C_n(q,\cdots,(-1)^{q-2}q,\underset{\underset{q}{\uparrow}}{0},(-1)^{q}q,\cdots,(-1)^{2q-2}q,\underset{\underset{2q}{\uparrow}}{0},(-1)^{2q}q,\cdots)$$
$$=\begin{cases} 0 & \text{if } q \text{ odd and } n\equiv 0 \pmod{q} \quad n\geq 1,\\ 2 & \text{if } q \text{ even and } n\equiv 0 \pmod{q} \quad n\geq 1,\\ \binom{q}{n'} & \text{otherwise, where } n'=n-q\lfloor n/q\rfloor.\end{cases}$$

The definitions of the combinatorial sequences and their generating functions in the following examples can be found in [12, 49, 61, 62].

Theorem 3.1.3 ([26, 27]). *Let F_n and L_n be the Fibonacci and Lucas numbers, respectively. We have*

$$F_n = C_n(L_1,L_2,\cdots,L_n).$$

Proof: The generating function for the Fibonacci numbers F_n is

$$\sum_{n\geq 0} F_n z^n = \frac{1}{1-z-z^2},$$

and the generating function of the Lucas numbers L_n is

$$\sum_{n\geq 1} L_n z^n = \frac{z+2z^2}{1-z-z^2}.$$

Now, let $H(z)=(1-z-z^2)^{-1}=\sum_{n\geq 0}F_n z^n$. Then, by equation (2.3), we have

$$P(z)=\frac{z+2z^2}{1-z-z^2}=\sum_{n\geq 1}L_n z^n.$$

Hence, by equation (3.2), we obtain the desired result. ∎

Note that in the next few examples, we will use exponential generating functions instead of ordinary generating functions. Hence, factorial factors will appear in our identities.

Theorem 3.1.4 ([26, 27]). *Let BE_n be the Bell numbers. We have*

$$BE_n = n!\, C_n\left(\frac{1}{0!}, \frac{1}{1!}, \cdots, \frac{1}{(n-1)!}\right).$$

Proof: Recall that the exponential generating function of the Bell numbers is

$$\sum_{n\geq 0} \frac{BE_n}{n!} z^n = \exp(\exp(z) - 1).$$

Now, let $H(z) = \exp(\exp(z) - 1) \in 1 + z\mathbb{C}[[z]]$. Hence, by equation (2.3), we have

$$P(z) = z\exp(z) = z + \frac{z^2}{1!} + \frac{z^3}{2!} + \cdots$$

The result now follows from equation (3.2). ■

Theorem 3.1.5. *Let E_n and T_n be the Euler and tangent numbers, respectively. We have*

$$E_n = n!\, C_n\left(\frac{T_0}{0!}, \frac{T_1}{1!}, \frac{T_2}{2!}, \cdots, \frac{T_{n-1}}{(n-1)!}\right).$$

Proof: Note that the exponential generating functions of the Euler and tangent numbers are

$$\sum_{n\geq 0} \frac{E_n}{n!} z^n = \sec(z) \qquad \text{and} \qquad \sum_{n\geq 0} \frac{T_n}{n!} z^n = \tan(z).$$

Let

$$H(z) = \sec(z) \in 1 + z\mathbb{C}[[z]].$$

Then, by equation (2.3), we have

$$P(z) = z\tan(z).$$

Hence, by Theorem 3.1.2, we get the desired result. ■

Remark: There are alternate Euler numbers and tangent numbers defined by

$$\sum_{n\geq 0} \frac{E_n^*}{n!} z^n = \frac{2\exp(z)}{\exp(2z)+1} = \operatorname{sech}(z),$$

and

$$\sum_{n\geq 0} \frac{T_n^*}{n!} z^n = \frac{\exp(2z)-1}{\exp(2z)+1} = \tanh(z).$$

In this case, we have

$$E_n^* = n!\, C_n\left(\frac{-T_0^*}{0!}, \frac{-T_1^*}{1!}, \frac{-T_2^*}{2!}, \cdots, \frac{-T_{n-1}^*}{(n-1)!}\right).$$

Theorem 3.1.6 ([23]). *Let D_n be the derangement numbers. We have*

$$D_n = n!\, C_n\,(0, 1, \cdots, 1).$$

Proof: The exponential generating function of the derangement number is

$$\sum_{n\geq 0} \frac{D_n}{n!} z^n = \frac{\exp(-z)}{1-z}.$$

The result now follows by using the usual techniques. ■

Theorem 3.1.7. *Let B_n be the Bernoulli numbers. We have*

$$B_n = n!\, C_n\left(\frac{B_1}{1!}, \frac{-B_2}{2!}, \frac{-B_3}{3!}, \cdots, \frac{-B_n}{n!}\right)$$

and

$$B_n = n!\, C_n\left(\frac{B_1}{1!}, -\frac{B_2}{2!}, \cdots, (-1)^{n+1}\frac{B_n}{n!}\right).$$

Proof: Note that the exponential generating function of the Bernoulli numbers is

$$\sum_{n\geq 0} \frac{B_n}{n!} z^n = \frac{z}{\exp(z)-1}.$$

Let

$$H(z) = \frac{z}{\exp(z)-1} \in 1 + z\mathbb{C}[[z]].$$

Then, by equation (2.3), we have

$$P(z) = 1 - \frac{z\exp(z)}{\exp(z)-1} = 1 - z - \frac{z}{\exp(z)-1} = 1 - z - H(z).$$

Hence, by equation (3.2)

$$B_n = n!\, C_n\left(\frac{-B_1-1}{1!}, \frac{-B_2}{2!}, \frac{-B_3}{3!}, \cdots, \frac{-B_n}{n!}\right)$$

or equivalently,

$$B_n = n!\, \mathcal{C}_n\left(\frac{B_1}{1!}, \frac{-B_2}{2!}, \cdots, \frac{-B_n}{n!}\right)$$

since $B_1 = \frac{-1}{2}$ and $-B_1 - 1 = \frac{-1}{2} = B_1$.

Moreover, if we write

$$P(z) = 1 - \frac{z\exp(z)}{\exp(z)-1} = 1 - \frac{-z}{\exp(-z)-1} = 1 - H(-z),$$

Then we get the second identity. ■

3.1.1 The Lagrange Inversion Theorem

In order to obtain more interesting identities, we utilize the remarkable Lagrange Inversion Theorem to calculate the coefficients in a formal power series.

We recall the Lagrange Inversion Theorem and one of its corollaries (see e.g. [12, 24, 62, 68]).

Lagrange Inversion Theorem. *Let $G(z) \in [[z]]$ with $G(0) \neq 0$, and let $F(z)$ be defined by*

$$F(z) = zG(F(z)).$$

Then

$$n[z^n]F(z)^k = k[z^{n-k}]G(z)^n$$

where $k, n \in \mathbb{Z}$.

Note that if $k < 0$ then $F(z)^k$ is the Laurent series of the form

$$\sum_{n \geq k} a_n z^n.$$

Corollary 3.1.8. *Let $L(z), G(z) \in \mathbb{C}[[z]]$ with $G(0) \neq 0$, and let $F(z)$ be defined by*

$$F(z) = zG(F(z)).$$

Then we have

$$n[z^n]L(F(z)) = [z^{n-1}]L'(z)G(z)^n$$

and

$$n[z^n]\log\left(\frac{F(z)}{z}\right) = [z^n]G(z)^n. \qquad \blacksquare$$

Theorem 3.1.9. *We have*

$$\begin{aligned}
-(n-1)^{n-1} &= n!\,C_n\left(-\frac{1}{1!}, -\frac{4}{2!}, \cdots, -\frac{n^n}{n!}\right),\\
(n+1)^{n-1} &= n!\,C_n\left(\frac{1}{1!}, \frac{4}{2!}, \cdots, \frac{n^n}{n!}\right),\\
(1-n)^{n-1} &= n!\,C_n\left(\frac{1}{1!}, -\frac{4}{2!}, \cdots, (-1)^{n-1}\frac{n^n}{n!}\right).
\end{aligned}$$

Proof: Consider the functional equation

$$F(z) = z\exp(F(z)).$$

By using the Lagrange Inversion Theorem, we have

$$F(z)^k = \sum_{n\geq k} \frac{kn^{n-k-1}}{(n-k)!} z^n$$

where $k \in \mathbb{Z}$.

Now, let $R(z) = \exp(-F(z)) \in 1 + z\mathbb{C}[[z]]$. Then we have

$$\begin{aligned}
R(z) &= \exp(-F(z)) = zF(z)^{-1} = \sum_{n\geq 0} \frac{-(n-1)^{n-1}}{n!} z^n,\\
H(z) &= \exp(F(z)) = z^{-1}F(z) = \sum_{n\geq 0} \frac{(n+1)^{n-1}}{n!} z^n,\\
E(z) &= \exp(-F(-z)) = -zF(-z)^{-1} = \sum_{n\geq 0} \frac{(1-n)^{n-1}}{n!} z^n,\\
P(z) &= zF'(z) = \sum_{n\geq 1} \frac{n^n}{n!} z^n.
\end{aligned}$$

The result now follows by applying Theorem 3.1.2. ■

Remark: The number $(n+1)^{n-1}$ is the number of labelled trees on $n+1$ vertices [49, 62].

Theorem 3.1.10. *Let*

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

be the nth Catalan number. We have

$$\begin{aligned}
-C_{n-1} &= c_n\left(-\binom{1}{0}, -\binom{3}{1}, \cdots, -\binom{2n-1}{n-1}\right), \\
C_n &= c_n\left(\binom{1}{0}, \binom{3}{1}, \cdots, \binom{2n-1}{n-1}\right), \\
(-1)^{n-1}C_{n-1} &= c_n\left(\binom{1}{0}, -\binom{3}{1}, \cdots, (-1)^{n-1}\binom{2n-1}{n-1}\right).
\end{aligned}$$

Proof: Note that the generating function of the Catalan numbers

$$C(z) := C_0 + C_1 z + C_2 z^2 + \cdots$$

satisfies

$$C(z) = 1 + zC(z)^2. \tag{3.7}$$

Now, let $H(z) = C(z) \in 1 + z\mathbb{C}[[z]]$. By equation (3.7), we have

$$1 = C(z)^{-1} + zC(z).$$

Hence,

$$\begin{aligned}
R(z) &= C(z)^{-1} = 1 - zC(z), \\
E(z) &= R(-z) = 1 + zC(-z),
\end{aligned}$$

and

$$\begin{aligned}
a_n &= -C_{n-1} \quad \text{for } n \geq 1, \\
e_n &= (-1)^{n-1}C_{n-1} \quad \text{for } n \geq 1.
\end{aligned}$$

Also,

$$\begin{aligned}
P(z) &= z\frac{C'(z)}{C(z)} \\
&= z\frac{C(z)^2 + z2C(z)C'(z)}{C(z)} \\
&= zC(z) + 2z^2C'(z).
\end{aligned}$$

So,

$$\begin{aligned} p_n &= C_{n-1} + 2(n-1)C_{n-1} \\ &= (2n-1)\frac{1}{n}\binom{2n-2}{n-1} \\ &= \binom{2n-1}{n-1}. \end{aligned}$$

Therefore, by Theorem 3.1.2, we obtain the desired result. ■

We conclude this section by giving one more application.

Theorem 3.1.11. *Let*

$$MO_n = \frac{1}{n+1}\sum_i \binom{n+1}{i}\binom{n+1-i}{i+1}$$

be the Motzkin numbers. We have

$$\begin{aligned} -MO_{n-2} &= C_n\left(-1, -3, \cdots, -\sum_i \binom{n}{i}\binom{n-i}{i}\right), \\ MO_n &= C_n\left(1, 3, \cdots, \sum_i \binom{n}{i}\binom{n-i}{i}\right), \\ (-1)^{n-1}MO_{n-2} &= C_n\left(1, -3, \cdots, (-1)^{n-1}\sum_i \binom{n}{i}\binom{n-i}{i}\right) \end{aligned}$$

for $n \geq 2$.

Proof: Note that the generating function of the Motzkin numbers

$$MO(z) := MO_0 + MO_1 z + MO_2 z^2 + \cdots$$

satisfies

$$MO(z) = 1 + zMO(z) + z^2 MO(z)^2. \tag{3.8}$$

Let $\widetilde{MO}(z) = zMO(z)$. Then equation (3.8) becomes

$$\widetilde{MO}(z) = z(1 + \widetilde{MO}(z) + \widetilde{MO}(z)^2).$$

So, to use the Lagrange Inversion Theorem, we will need the expansion

$$\begin{aligned}(1+z+z^2)^n &= \sum_{i\geq 0}\binom{n}{i}(z+z^2)^{n-i}\\ &= \sum_{i\geq 0}\binom{n}{i}z^{n-i}(1+z)^{n-i}\\ &= \sum_{i\geq 0}\binom{n}{i}z^{n-i}\sum_{j\geq 0}\binom{n-i}{j}z^j\\ &= \sum_{i,j\geq 0}\binom{n}{i}\binom{n-i}{j}z^{n-i+j}.\end{aligned}$$

Now, let $H(z) = MO(z) = z^{-1}\widetilde{MO}(z) \in 1+z\mathbb{C}[[z]]$. Then

$$R(z) = MO(z)^{-1} = z\widetilde{MO}(z)^{-1},$$

and

$$\begin{aligned}a_n &= [z^n]MO(z)^{-1}\\ &= [z^{n-1}]\widetilde{MO}(z)^{-1}\\ &= \frac{-1}{n-1}[z^n](1+z+z^2)^{n-1} && \text{(by Lagrange Inversion)}\\ &= \frac{-1}{n-1}\sum_i\binom{n-1}{i}\binom{n-1-i}{i-1} && \text{(by the expansion)}\\ &= -MO_{n-2}\end{aligned}$$

for $n \geq 2$.

Also, rewrite equation (2.3) as

$$\log(H(z)) = \sum_{n\geq 1}\frac{p_n}{n}z^n,$$

we have

$$\begin{aligned}p_n &= n[z^n]\log(H(z))\\ &= n[z^n]\log\left(\frac{\widetilde{MO}(z)}{z}\right)\\ &= [z^n](1+z+z^2)^n && \text{(by Corollary 3.1.8)}\\ &= \sum_i\binom{n}{i}\binom{n-i}{i} && \text{(by the expansion).}\end{aligned}$$

Again, we apply Theorem 3.1.2 to establish the formulas. ■

3.2 Dynamical Systems

There is a strong connection between number theory and dynamical systems. In particular, the number of periodic points in a dynamical system satisfies a congruence relation, (3.12) below. Various authors have applied (3.12) to get congruences for dynamical systems [6, 15, 16, 17, 22, 34, 35, 36, 47].

Du [15, 16, 17] has obtained several interesting results about counting the periodic points using linear recurrence relations. Moreover, he made extensive use of the computer to formulate conjectures about congruences for these sequences which he could not prove using dynamical-systems techniques. He also asked if number-theoretic proofs were possible for his theorems. At the first glance, there is no obvious way to obtain a relationship between the initial conditions and the recurrence relations in Du's theorems and conjectures. However, we are able to prove Du's conjectures and theorems using our techniques.

3.2.1 Introduction

In this subsection,we recall some basic definitions and results from dynamical systems (see e.g. [16, 47]).

For a map $T : X \to X$ on a set X, we denote the nth iterate of T by T^n. We call a point $x \in X$ a *periodic point of period n* under T if

$$T^n(x) = x,$$

for some $n \geq 1$. Call x a *periodic point of least period n* under T if

$$T^n(x) = x \quad \text{and} \quad T^k(x) \neq x \quad \text{for } 1 \leq k < n.$$

We denote the number of points of period n under T by

$$\mathrm{Per}_n(T) = \#\{x \in X \mid T^n(x) = x\},$$

and the number of points of least period n under T by

$$\mathrm{LPer}_n = \#\{x \in X \mid T^n(x) = x \text{ and } T^k(x) \neq x \text{ for } 1 \leq k < n\}.$$

We assume $\mathrm{Per}_n(T)$ is finite for all $n \geq 1$.

It is easy to see that x is a periodic point of n if and only if x is a periodic point of least period d for some $d \mid n$. Hence we have

$$\mathrm{Per}_n = \sum_{d|n} \mathrm{LPer}_d. \tag{3.9}$$

Furthermore, if x is a periodic point of least period n under T, then the points x, $T(x)$, $\cdots$, $T^{n-1}(x)$ are all distinct and are all periodic points of least period n. We call the set

$$\{T^k(x) \mid k \geq 0\} = \{x, T(x), \cdots, T^{n-1}(x)\}$$

the *(periodic) orbit* of x under T. Then the number of orbits of length n under T is

$$\mathrm{Orb}_n(T) = \frac{1}{n}\mathrm{LPer}_n(T). \tag{3.10}$$

Hence, by (3.9) and (3.10), we have

$$\mathrm{Per}_n = \sum_{d|n} d\mathrm{Orb}_d \quad \forall n \geq 1.$$

Then, by the Möbius Inversion Theorem, we get

$$\mathrm{Orb}_n = \frac{1}{n}\sum_{d|n} \mu(d)\mathrm{Per}_{n/d} \quad \forall n \geq 1. \tag{3.11}$$

Since Orb_n is a nonnegative integer, we get the following congruence

$$\sum_{d|n} \mu(d)\mathrm{Per}_{n/d} \equiv 0 \pmod{n} \quad \forall n \geq 1. \tag{3.12}$$

3.2.2 Du's Theorems and Conjectures

In this section, we will show that the initial conditions and recurrence relations in Du's conjectures and theorems are connected with the power sums in the characteristic roots of the recurrence relations. Hence, we are able to prove these congruences by using Theorem 2.3.1. First, we give some examples which algebraically prove theorems which Du demonstrated using the theory of dynamical systems. We then use the same techniques to prove Du's conjectures in [16, 17].

The next two examples deal with linear recurrence relations of order 2 and order 3.

Example 3.2.1. Let a_1 and a_2 be integers and $\{A_n\}$ satisfy the recurrence relation

$$A_n + a_1 A_{n-1} + a_2 A_{n-2} = 0 \qquad \text{for } n > 2$$

with initial conditions

$$A_1 = -a_1 \quad \text{and} \quad A_2 = a_1^2 - 2a_2.$$

So, by Theorem 2.5.5, A_n is the nth power sum in the roots of $F(z) = z^2 + a_1 z + a_2$. Hence, by Theorem 2.3.1, we have

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \text{for all } n \geq 1. \qquad \blacksquare$$

Remark: When $a_1 = -1, a_2 = -1$, we get

$$A_1 = 1, A_2 = 3, A_3 = 4, A_4 = 7, A_5 = 11, \cdots$$

so that $A_n = L_n$, the nth Lucas number (see e.g [19, 65]).

Example 3.2.2. Let a_1, a_2 and a_3 be integers and $\{A_n\}$ satisfy the recurrence relation

$$A_n + a_1 A_{n-1} + a_2 A_{n-2} + a_3 A_{n-3} = 0 \qquad \text{for } n > 3$$

with initial conditions

$$A_1 = -a_1, \quad A_2 = a_1^2 - 2a_2 \quad \text{and} \quad A_3 = -a_1^3 + 3a_1 a_2 - 3a_3.$$

So, by Theorem 2.5.5, A_n is the nth power sum of the roots of $F(z) = z^3 + a_1 z^2 + a_2 z + a_3$. Hence, by Theorem 2.3.1, we have

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \text{for all } n \geq 1. \qquad \blacksquare$$

Remark: This example generalizes the result in [16, Theorem 4], and also gives the explicit initial conditions that Du was asking for.

Du's Theorems

We now give algebraic proofs of Du's theorems.

Theorem 3.2.3 ([15, Theorem 3]). *Fix $r \geq 1$ and let*

$$A_n - A_{n-1} - A_{n-2} - \cdots - A_{n-r} = 0 \qquad \textit{for } n > r$$

with initial conditions

$$A_n = 2^n - 1, \quad \textit{for } 1 \leq n \leq r.$$

Then

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1.$$

Proof: We will show that A_n is the nth power sum in the roots of the characteristic polynomial

$$F(z) = z^r - z^{r-1} - z^{r-2} - \cdots - 1.$$

To prove this, let

$$\begin{aligned} R(z) &= 1 - z - z^2 - \cdots - z^r \\ &= (1 - 2z + z^{r+1})/(1 - z). \end{aligned}$$

Now, let $\tilde{R}(z) = 1 - 2z + z^{r+1}$ and $\hat{R}(z) = 1 - z$. It follows easily from Example 2.5.4 that

$$\tilde{p}_n = 2^n \quad \text{and} \quad \hat{p}_n = 1 \qquad \text{for } 1 \leq n \leq r.$$

Thus, by Proposition 2.2.2, we get $p_n = 2^n - 1$ for $1 \leq n \leq r$. Now Theorem 2.5.5 shows that p_n and A_n satisfy the same initial conditions and recurrence relation. Hence they must be equal for all $n \geq 1$. Therefore, by Theorem 2.3.1, we have

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \text{for all } n \geq 1. \qquad \blacksquare$$

Theorem 3.2.4 ([15, Theorem 4], [16, Theorem 3]). *Fix integer $r \geq 1$ and let*

$$A_n - A_{n-1} - \sum_{i=2}^{2r} (-1)^i A_{n-i} = 0 \qquad \textit{for } n > 2r$$

with initial conditions

$$\begin{array}{rcll} A_{2n-1} & = & 1 & \textit{for } 1 \leq n \leq r, \\ A_{2n} & = & 2^{n+1} - 1 & \textit{for } 1 \leq n \leq r. \end{array}$$

Then

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1.$$

Proof: We will show that A_n is the nth power sum in the roots of the characteristic polynomial

$$F(z) = z^{2r} - z^{2r-1} - \sum_{i=2}^{2r} (-1)^i z^{2r-i}.$$

To show this, let

$$\begin{aligned} R(z) &= 1 - z - \sum_{i=2}^{2r} (-1)^i z^i \\ &= (1 - 2z^2 - z^{2r+1})/(1+z). \end{aligned}$$

Now, let $\tilde{R}(z) = 1 - 2z^2 - z^{2r+1}$ and $\hat{R}(z) = 1 + z$. By a method similar to Example 2.5.4, we have

$$\begin{array}{rcll} \tilde{p}_{2n-1} & = & 0 & \text{for } 1 \leq n \leq r, \\ \tilde{p}_{2n} & = & 2^{n+1} & \text{for } 1 \leq n \leq r. \end{array}$$

Also, $\hat{p}_n = (-1)^n$, for all $n \geq 1$. Hence, by Proposition 2.2.2, we get

$$\begin{array}{rcll} p_{2n-1} & = & 1 & \text{for } 1 \leq n \leq r, \\ p_{2n} & = & 2^{n+1} - 1 & \text{for } 1 \leq n \leq r. \end{array}$$

Arguing as in the previous proof, $p_n = A_n$ for all $n \geq 1$. Therefore, by Theorem 2.3.1, we have

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \text{for all } n \geq 1. \qquad \blacksquare$$

Remark: In [15], Du used a more complicated recurrence relation for the sequence in this theorem. Later, he discovered a simpler recurrence relation in [16]. Here, we have simplified the recurrence relation even further.

Theorem 3.2.5 ([16, Theorem 2]). *Fix $r \geq 2$ and let*

$$A_n - 3A_{n-1} + A_{n-2} + \cdots + A_{n-r} = 0 \qquad \textit{for } n > r$$

with initial conditions

$$A_n = 2^{n+1} - 1, \quad \textit{for } 1 \leq n \leq r.$$

Then

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1.$$

Proof: We will show that A_n is the nth power sum in the roots of the characteristic polynomial

$$F(z) = z^r - 3z^{r-1} + z^{r-2} + \cdots + 1.$$

To show this, let

$$\begin{aligned} R(z) &= 1 - 3z + z^2 + \cdots + z^r \\ &= (1 - 4z + 4z^2 - z^{r+1})/(1-z). \end{aligned}$$

Now, let $\tilde{R}(z) = 1 - 4z + 4z^2 - z^{r+1}$ and $\hat{R}(z) = 1 - z$. From Theorem 2.5.2 it follows that for $n \leq r$ then nth power sum in the roots of $\tilde{R}(z)$ are the same as that sum for $1 - 4z + 4z^2$. So

$$\tilde{p}_n = 2^{n+1} \quad \text{and} \quad \hat{p}_n = 1 \qquad \text{for } 1 \leq n \leq r.$$

Thus, by Proposition 2.2.2, we get $p_n = 2^{n+1} - 1$ for $1 \leq n \leq r$. The proof is finished in the usual manner. ∎

Theorem 3.2.6 ([17, Theorem 5]). *Fix $r \geq 2$ and let*

$$A_n - \sum_{i=1}^{r} (2i-1) A_{n-i} - \sum_{i=r+1}^{2r-1} (4r - 2i - 1) A_{n-i} = 0 \qquad \textit{for } n \geq 2r$$

with initial conditions

$$A_n = \begin{cases} 3^n - 2 & \textit{for } 1 \leq n \leq r, \\ 3^n - 4n \cdot 3^{n-r-1} - 2 & \textit{for } r < n < 2r. \end{cases}$$

Then

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1.$$

Proof: The reader will be familiar with the method by now, so we will only provide the main steps. Let

$$\begin{aligned} R(z) &= 1 - \sum_{i=1}^{r}(2i-1)z^i - \sum_{i=r+1}^{2r-1}(4r-2i-1)z^i \\ &= (1 - 3z + 4z^{r+1} - z^{2r} - z^{2r+1})/(1-z)^2. \end{aligned}$$

Now, let $\tilde{R}(z) = 1 - 3z + 4z^{r+1} - z^{2r} - z^{2r+1}$ and $\hat{R}(z) = (1-z)^2$. From Theorem 2.5.2, the power sums for $\tilde{R}(z)$ and $1 - 3z + 4z^{r+1}$ are the same for $n < 2r$. So by Example 2.5.4

$$\tilde{p}_n = \begin{cases} 3^n & \text{for } 1 \leq n \leq r, \\ 3^n - 4n \cdot 3^{n-r-1} & \text{for } r < n < 2r. \end{cases}$$

Also, $\hat{p}_n = 2$, for all $n \geq 1$. Thus, by Proposition 2.2.2, we get

$$p_n = \begin{cases} 3^n - 2 & \text{for } 1 \leq n \leq r, \\ 3^n - 4n \cdot 3^{n-r-1} - 2 & \text{for } r < n < 2r. \end{cases}$$

Since $A_n = p_n$ for all $n \geq 1$, we are done. ■

Du's Conjectures

Using the same methods, we can prove Du's conjectures in [16, 17] which he could not obtain using dynamical-systems techniques.

The next theorem resolves the conjecture in [16].

Theorem 3.2.7. *Fix* $r \geq 2$ *and let*

$$A_n - 3A_{n-1} + A_{n-2} + \cdots + A_{n-2r+1} = 0 \qquad \textit{for } n \geq 2r$$

with initial conditions

$$A_n = \begin{cases} 1 & \textit{for } 1 \leq n < r, \\ 2n \cdot 2^{n-r} + 1 & \textit{for } r \leq n < 2r. \end{cases}$$

Then

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \textit{for all } n \geq 1.$$

Proof: Notice that the characteristic polynomial of the recurrence relation is

$$\begin{aligned} & z^{2r-1} - 3z^{2r-2} + z^{2r-3} + \cdots + 1 \\ &= (z^r - 2z^{r-1} - 1)(z^{r-1} - z^{r-2} - \cdots - 1). \end{aligned}$$

We will show that A_n is difference of the nth power sums in the roots of

$$z^r - 2z^{r-1} - 1 \quad \text{and} \quad z^{r-1} - z^{r-2} - \cdots - 1.$$

So, let

$$\tilde{R}(z) = 1 - 2z - z^r$$

and

$$\begin{aligned} \hat{R}(z) &= 1 - z - \cdots - z^{r-1} \\ &= (1 - 2z + z^r)/(1 - z). \end{aligned}$$

It follows easily from Example 2.5.4 and Proposition 2.2.2 that

$$\tilde{p}_n = \begin{cases} 2^n & \text{for } 1 \le n < r, \\ 2^n + n \cdot 2^{n-r} & \text{for } r \le n < 2r. \end{cases}$$

and

$$\hat{p}_n = \begin{cases} 2^n - 1 & \text{for } 1 \le n < r, \\ 2^n - n \cdot 2^{n-r} - 1 & \text{for } r \le n < 2r. \end{cases}$$

Thus, we have

$$\tilde{p}_n - \hat{p}_n = \begin{cases} 1 & \text{for } 1 \le n < r, \\ 2n \cdot 2^{n-r} + 1 & \text{for } r \le n < 2r. \end{cases}$$

Now applying Theorem 2.5.8 we obtain $A_n = \tilde{p}_n - \hat{p}_n$ for all $n \ge 1$. Since by Theorem 2.3.1 both $\tilde{p}_n$ and $\hat{p}_n$ satisfy the desired congruence, so does their difference. ■

The next theorem proves the conjecture in [17]

Theorem 3.2.8. *Fix $r \ge 2$ and let*

$$A_n - \sum_{i=1}^{r}(2i-1)A_{n-i} - \sum_{i=r+1}^{2r-1}(4r-2i-1)A_{n-i} = 0 \qquad \textit{for } n \ge 2r$$

with initial conditions

$$A_n = \begin{cases} 3^n & \textit{for } 1 \le n < r, \\ 3^r - 2r & \textit{for } n = r, \\ 3^n - 4n \cdot 3^{n-r-1} & \textit{for } r < n < 2r. \end{cases}$$

Then

$$\sum_{d|n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \textit{for all } n \ge 1.$$

Proof: Notice that the characteristic polynomial of the recurrence relation is

$$z^{2r-1} - \sum_{i=1}^{r} (2i-1) z^{2r-1-i} - \sum_{i=r+1}^{2r-1} (4r-2i-1) z^{2r-1-i}$$
$$= (z^r - 2z^{r-1} - 2z^{r-2} - \cdots - 2z - 1)(z^{r-1} + z^{r-2} + \cdots + 1).$$

We will show that A_n is difference of the powers sum of the roots of

$$z^r - 2z^{r-1} - 2z^{r-2} - \cdots - 2z - 1$$

and

$$z^{r-1} + z^{r-2} + \cdots + 1.$$

So, let

$$\tilde{R}(z) = 1 - 2z - 2z^2 - \cdots - 2z^{r-1} - z^r$$
$$= (1 - 3z + z^r + z^{r+1})/(1-z)$$

and

$$\hat{R}(z) = 1 + z + z^2 + \cdots + z^{r-1}$$
$$= (1 - z^r)/(1-z).$$

Using the usual techniques we get

$$\tilde{p}_n = \begin{cases} 3^n - 1 & \text{for } 1 \le n < r, \\ 3^n - r - 1 & \text{for } n = r, \\ 3^n - 4n \cdot 3^{n-r-1} - 1 & \text{for } r < n < 2r. \end{cases}$$

and

$$\hat{p}_n = \begin{cases} r-1 & \text{for } r \mid n, \\ -1 & \text{otherwise.} \end{cases}$$

Thus, we get

$$\tilde{p}_n - \hat{p}_n = \begin{cases} 3^n & \text{for } 1 \le n < r, \\ 3^n - 2r & \text{for } n = r, \\ 3^n - 4n \cdot 3^{n-r-1} & \text{for } r < n < 2r. \end{cases}$$

Now we are done as in the proof of the previous theorem. ■

Actually, Du in [16, 17] used dynamical systems to prove that the sequences $\{A_n\}_{n\geq 1}$ in Theorems 3.2.7 and 3.2.8 satisfy the following congruences.

$$\sum_{\substack{d \mid n \\ d:\ \text{odd}}} \mu(d) A_{n/d} \equiv \begin{cases} 1 \pmod{2n} & \text{for } n = 2^k, \quad k \geq 0, \\ 0 \pmod{2n} & \text{otherwise.} \end{cases} \tag{3.13}$$

Recently, Du, Huang and Li [18] used a different approach to prove the congruences

$$\sum_{d \mid n} \mu(d) A_{n/d} \equiv 0 \pmod{n} \quad \text{for all } n \geq 1.$$

from (3.13).

3.3 Universal λ-rings, ghost rings, necklace rings, and Witt vectors

The main purpose of this section is to give explicit formulas for universal polynomials of universal λ-rings and to give a connection of our viewpoint with ghost rings, necklace rings, and Witt vectors.

Universal λ-rings [14, 25, 31] are an important tool from commutative algebra, and have numerous applications to several areas of mathematics [3, 14, 25, 31, 40, 52]. In the literature the construction of universal λ-rings is by universal polynomials. However, to the best of our knowledge, no explicit formulas for universal polynomials have been established in the literature. Since universal polynomials are the building blocks of universal λ-rings, it would be helpful to have such formulas for them. We will derive such expressions shortly.

Since we have already been working over $\mathbb{C}$, we will continue to do so in this section. However, these results remain true over suitable commutative rings.

We first consider a ring structure on $z\mathbb{C}[[z]]$. We use the usual addition operation but Hadamard product $\odot$ for the multiplication. This ring is called the *ghost ring* $Gh(\mathbb{C})$ [33, 40, 52].

We define the *ghost map*

$$gh: 1+z\mathbb{C}[[z]] \to z\mathbb{C}[[z]]$$

by

$$gh(R(z)) = -z\frac{R'(z)}{R(z)} = P(z).$$

We wish to define the ring structure on $1+z\mathbb{C}[[z]]$ for which the ghost map becomes an isomorphism of rings. By Proposition 2.2.2, we must define addition in $1+z\mathbb{C}[[z]]$ to be the usual multiplication of formal power series. Now, we define the multiplication $*$ on $1+z\mathbb{C}[[z]]$ by

$$\tilde{R}(z) * \hat{R}(z) = gh^{-1}\left(gh\left(\tilde{R}(z)\right) \odot gh\left(\hat{R}(z)\right)\right).$$

where

$$gh^{-1}(P(z)) = \exp\left(-\int_0^z \frac{P(x)}{x}dx\right) = \exp\left(-\sum_{n\geq 1}\frac{p_n}{n}z^n\right).$$

This ring structure on $1+z\mathbb{C}[[z]]$ is called the *universal λ-ring*.

Suppose $\tilde{R}(z) = 1+\tilde{a}_1z+\tilde{a}_2z^2+\cdots$ and $\hat{R}(z) = 1+\hat{a}_1z+\hat{a}_2z^2+\cdots$. Let $R(z) = \tilde{R}(z) * \hat{R}(z) = 1+a_1z+a_2z^2+\cdots$. Then there exist polynomials

$$S_n[x_1,\cdots,x_n;y_1,\cdots,y_n]$$

such that

$$a_n = S_n[\tilde{a}_1,\cdots,\tilde{a}_n;\hat{a}_1,\cdots,\hat{a}_n].$$

These polynomials, S_n, are called the *universal polynomials* of the universal λ-ring. No explicit formulas for universal polynomials has been given in the literature. However, we can get a_n (and thus S_n) by applying our results in Section 2.4.

Theorem 3.3.1. *We have*

$$a_n = \sum_{\nu=(1^{k_1}2^{k_2}\cdots n^{k_n})\vdash n} \frac{(-1)^{l(\nu)}}{z_\nu} \prod_{i=1}^{n} \left(\left(\sum_{\lambda \vdash i} (-1)^{l(\lambda)} \frac{n}{l(\lambda)} \mu_\lambda \tilde{a}_\lambda \right) \left(\sum_{\lambda' \vdash i} (-1)^{l(\lambda')} \frac{n}{l(\lambda')} \mu_{\lambda'} \hat{a}_{\lambda'} \right) \right)^{k_i}.$$

Proof: By equation (2.27),

$$\begin{aligned} a_n &= \sum_{\nu=(1^{k_1}2^{k_2}\cdots n^{k_n})\vdash n} (-1)^{l(\nu)} z_\nu^{-1} p_\nu \\ &= \sum_{\nu=(1^{k_1}2^{k_2}\cdots n^{k_n})\vdash n} (-1)^{l(\nu)} z_\nu^{-1} \tilde{p}_\nu \hat{p}_\nu . \end{aligned}$$

Now applying equation (2.25) finishes the proof. ∎

The first few examples are

$$\begin{aligned} a_1 &= -\tilde{a}_1 \hat{a}_1 \\ a_2 &= \tilde{a}_1^2 \hat{a}_2 + \tilde{a}_2 \hat{a}_1^2 - 2\tilde{a}_2 \hat{a}_2 \\ a_3 &= -\tilde{a}_1^3 \hat{a}_3 - \tilde{a}_3 \hat{a}_1^3 + 3\tilde{a}_1 \tilde{a}_2 \hat{a}_3 + 3\tilde{a}_3 \hat{a}_1 \hat{a}_2 - \tilde{a}_1 \tilde{a}_2 \hat{a}_1 \hat{a}_2 - 3\tilde{a}_3 \hat{a}_3 . \end{aligned}$$

Since, $R(z) \in 1 + z\mathbb{C}[[z]]$ can write as

$$R(z) = \prod_{n \geq 1} (1 - z^n)^{M_n}.$$

Hence, we can define a ring structure on the *necklace vector* $(M_1, M_2, \cdots) \in \mathbb{C}^{\mathbb{P}}$ [14, 40]. Addition is the usual componentwise addition and the multiplication is defined by

$$M_n = \sum_{[i,j]=n} (i,j) \tilde{M}_i \hat{M}_j$$

which we already used in Proposition 2.2.3. This ring is called the *necklace ring* $Nr(\mathbb{C})$ [14, 40].

Similarly, write $R(z) \in 1 + z\mathbb{C}[[z]]$ as

$$R(z) = \prod_{n \geq 1} (1 - Q_n z^n).$$

We can define a ring structure on the *Witt vector* $(Q_1, Q_2, \cdots) \in \mathbb{C}^{\mathbb{P}}$ [33, 40]. However, we are unable to give explicit definitions of addition and multiplication for Witt vectors.

Chapter 4

Open problems

In this thesis, we obtained our results from generalizations of the elementary, complete homogeneous, and power sum symmetric functions. However, there are still serval important bases for the algebra of symmetric functions, for example Schur symmetric functions [37, 55], which we have not yet considered. We predict that by similarly generalizing Schur symmetric functions and other bases, we will obtain more results in the future. We also intend to investigate multivariate analogues and q-analogues of our results

In the following, we will outline some questions which arise naturally in our work.

In Theorem 2.1.11 we showed

$$p_n = \sum_{d|n} d Q_d^{n/d}, \quad \forall n \geq 1.$$

But now we can not apply the Möbius Inversion Theorem directly to write down Q_n in terms of p_n. Because of this, in Section 3.3 the ring structure of Witt vectors $(Q_1, Q_2, \cdots)$ is still a mystery. It would be wonderful to find an explicit formula to help in understanding this structure.

Question 1. What is an explicit formula for Q_n in terms of p_n?

In Theorem 2.3.1, we proved

$$\sum_{d|n} \mu(d) p_{n/d} \equiv 0 \pmod{n}.$$

The number $\frac{1}{n}\sum_{d|n}\mu(d)p_{n/d}$ counts objects arising in combinatorics, dynamical systems and finite fields. Hence, we would like to find condition(s) on p_n such that

$$\frac{1}{n}\sum_{d|n}\mu(d)p_{n/d}\in\mathbb{N}. \tag{4.1}$$

In Theorems 2.3.1 and 2.3.13 we gave conditions which guarantee $\frac{1}{n}\sum_{d|n}\mu(d)p_{n/d}\in\mathbb{Z}$.

Question 2. What condition(s) would characterize those sequences $\{p_n\}_{n\geq 1}$ satisfying (4.1)?

Similarly, in Theorem 2.3.4, we have

$$\sum_{\substack{d|n\\ q\nmid d}}\mu(d)p_{n/d}\equiv 0 \pmod{q^t n}.$$

However, we do not know of a combinatorial interpretation for the numbers

$$\frac{1}{q^t n}\sum_{\substack{d|n\\ q\nmid d}}\mu(d)p_{n/d}$$

except in the special case when $R(z)=1-q^t z$ this sum counts the number of irreducible polynomials of degree n over $GF(q^t)$ with given nonzero trace [54].

Question 3. Do the numbers $\frac{1}{q^t n}\sum_{\substack{d|n\\ q\nmid d}}\mu(d)p_{n/d}$ count anything?

We also have the analogue of our second question in this context.

Question 4. What condition(s) would characterize those sequences $\{p_n\}_{n\geq 1}$ satisfying

$$\frac{1}{q^t n}\sum_{\substack{d|n\\ q\nmid d}}\mu(d)p_{n/d}\in\mathbb{N}?$$

In Section 2.3, we derived various congruences involving the power sum symmetric functions. It seems that this method might work for other symmetric functions. The Witt symmetric functions (see [64]) are defined by

$$l_n=\frac{1}{n}\sum_{d|n}\mu(d)p_d^{n/d}.$$

Rota and Sagan [53] use group actions to get congruences for some special Witt symmetric functions.

Question 5. What identities and congruences for Witt symmetric functions can be obtained using our methods?

In Section 3.1, we used cycle indicators to relate combinatorial sequences. We can also apply these techniques to special functions such as the Hermite and Gegenbauer Polynomials [12]. But that work will appear elsewhere.

BIBLIOGRAPHY

[1] Richard André-Jeannin, On a conjecture of Piero Filipponi, *Fibonacci Quart.*, **32** (1994), no. 1, 11–14.

[2] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976.

[3] M. F. Atiyah and D. O. Tall, Group representations, λ-rings and the J-homomorphism, *Topology*, **8** (1969), 253–297.

[4] Elwyn R. Berlekamp, *Algebraic coding theory*, McGraw-Hill Book Co., New York, 1968.

[5] F. Beukers, Some congruences for the Apéry numbers, *J. Number Theory*, **21** (1985), no.2, 141–155.

[6] Jozef Bobok and Lúbomír Snoha, Periodic points and little Fermat theorem, *Nieuw Arch. Wisk. (4)*, **10** (1992), no.1-2, 33–35.

[7] Leonard Carlitz, Note on a paper of Dieudonné, *Proc. Amer. Math. Soc.*, **9** (1958), 32–33.

[8] Leonard Carlitz, A note on power series with integral coefficients, *Boll. Un. Mat. Ital. (3)*, **19** (1964), 1-3.

[9] Arthur Cayley, Note on the theory of Determinants, *The London, Edinburgh and Dublin Philosophical Magazine and Journal of Science*, 4th series, **21** (1861), 180–185.

[10] William Y. C. Chen, Ko-Wei Lih, and Yeong Nan Yeh, Cyclic tableaux and symmetric functions, *Studies in Applied Mathematics*, **94** (1995), no. 3, 327–339.

[11] William Y. C. Chen and James D. Louck, The combinatorial power of the companion matrix, *Linear Algebra and its Applications*, **232** (1996), 261–278.

[12] Louis Comtet, *Advanced combinatorics*, D. Reidel Publishing Co., Dordrecht, enlarged edition, 1974.

[13] A. Dold, Fixed point indices of iterated maps, *Inventiones Mathematicae*, **74** (1983), no. 3, 419–435.

[14] Andreas W. M. Dress and Christian Siebeneicher, The Burnside ring of the infinite cyclic group and its relations to the necklace algebra, λ-rings, and the universal ring of Witt vectors. *Adv. Math.*, **8** (1989), no.1, 1–41.

[15] Bau-Sen Du, A simple method which generates infinitely many congruence identities, *Fibonacci Quart.*, **27** (1989), no.2, 116–124.

[16] Bau-Sen Du, Congruence identities arising from dynamical systems, *Appl. Math. Lett.*, **12** (1999), no.5, 115–119.

[17] Bau-Sen Du, Obtaining new dividing formulas $n \mid Q(n)$ from the known ones, *Fibonacci Quart.*, **38** (2000), no.3, 217–222.

[18] Bau-Sen Du, Sen-Shan Huang, and Ming-Chia Li, Generalized Fermat, double Fermat and Newton sequences, *Journal of Number Theory*, **98** (2003), no.1, 172–183.

[19] Richard A. Dunlap, *The golden ratio and Fibonacci numbers*, World Scientific Publishing Co. Inc., River Edge, NJ, 1997.

[20] G. Everest, A. J. van der Poorten, Y. Puri, and T. Ward, Integer sequences and periodic points, *J. Integer Seq.*, **5** (2002), no. 2, Article 02.2.3, 10 pp. (electronic).

[21] Piero Filipponi, A note on a class of Lucas sequences, *Fibonacci Quart.*, **29** (1991), no. 3, 256–263.

[22] Michael Frame, Brenda Johnson, and Jim Sauerberg, Fixed points and Fermat: a dynamical systems approach to number theory, *Amer. Math. Monthly*, **107** (2000), no.5, 422–428.

[23] Ira M. Gessel, Combinatorial proofs of congruences, *Enumeration and design*, Academic Press, Toronto, ON, 1984, 157–197.

[24] I. P. Goulden and D. M. Jackson, *Combinatorial enumeration*, John Wiley & Sons Inc., New York, 1983.

[25] Michiel Hazewinkel, *Formal groups and applications*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[26] L. C. Hsu and Peter J. S. Shiue, Representation of various special polynomials via the cycle indicator of symmetric group, In *Combinatorics and graph theory '95, Vol. 1 (Hefei)*, World Sci. Publishing, River Edge, NJ, 1995, 157–162.

[27] Leetsch C. Hsu and Peter Jau-Shyong Shiue, Cycle indicators and special functions, *Annals of Combinatorics*, **5** (2001), no. 2, 179–196.

[28] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, second edition, 1990.

[29] Von W. Jänichen, Über die Verallgemeinerung einer Gauss'schen formal aus der theorie der höheren kongruenzen, *Sitzungsberichte der Berliner Mathematischen Gesellschaft*, **20** (1921), 23–29.

[30] Dov Jarden, Arithmetical properties of sums of powers, *Amer. Math. Monthly*, **56** (1949), 457–461.

[31] Donald Knutson, *λ-rings and the representation theory of the symmetric group*, Springer-Verlag, Berlin, 1973.

[32] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd Edition, Springer-Verlag, New York, 1984.

[33] Serge Lang, *Algebra*, Springer-Verlag, New York, third edition, 2002.

[34] Lionel Levine, Fermat's little theorem: a proof by function iteration, *Math. Mag.*, **72** (1999), no.4, 308–309.

[35] Chyi-Lung Lin, Obtaining dividing formulas $n \mid Q(n)$ from iterated maps, *Fibonacci Quart.*, **36** (1998), no.2, 118–124.

[36] Chyi-Lung Lin, A unified way for obtaining dividing formulas $n \mid Q(n)$, *Taiwanese J. Math.*, **2** (1998), no.4, 469–481.

[37] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1995.

[38] Percy A. MacMahon, *Combinatory analysis*, 2 vols, Cambridge Univ. Press, Cambridge, England, 1915–16; reprinted in one volume by Chelsea Publishing Co., New York, 1960.

[39] D. G. Mead, Newton's identities, *The American Mathematical Monthly*, **99** (1992), no. 8, 749–751.

[40] N. Metropolis and Gian-Carlo Rota, Witt vectors and the algebra of necklaces, *Adv. in Math.*, **50** (1983), no.2, 95–125.

[41] Alun O. Morris, Generalizations of the Cauchy and Schur identities, *J. Combinatorial Theory Ser. A*, **11** (1971), 163–169.

[42] R. F. Muirhead, Some proofs of Newton's theorem on sums of powers of roots, *Proceedings of the Edinburgh Mathematical Society*, **23** (1904), 66–70.

[43] R. F. Muirhead, A proof of Waring's expression for $\sum a^r$ in terms of the coefficients of an equation, *Proceedings of the Edinburgh Mathematical Society*, **23** (1904), 71–74.

[44] Isaac Newton, *The mathematical works of Isaac Newton* Vol. II, Assembled with an introduction by Derek T. Whiteside, Johnson Reprint Corp., New York, 1967.

[45] Isaac Newton, *The mathematical papers of Isaac Newton* Vol. I: 1664–1666, Edited by D. T. Whiteside, Cambridge University Press, London, 1967.

[46] Isaac Newton, *The mathematical papers of Isaac Newton* Vol V: 1683–1684, Edited by D. T. Whiteside, Cambridge University Press, New York, 1972.

[47] Yash Puri and Thomas Ward, A dynamical property unique to the Lucas sequence, *Fibonacci Quart.*, **39** (2001), no 5, 398–402.

[48] Yash Puri and Thomas Ward, Arithmetic and growth of periodic orbits, *J. Integer Seq.*, **4** (2001), no. 2, Article 01.2.1, 18 pp. (electronic).

[49] John Riordan, *An introduction to combinatorial analysis*, John Wiley & Sons Inc., New York, 1958.

[50] Alain M. Robert, *A course in p-adic analysis*, Springer-Verlag, New York, 2000.

[51] Fred S. Roberts, *Applied combinatorics*, Prentice Hall Inc., Englewood Cliffs, NJ, 1984.

[52] Leslie G. Roberts, The ring of Witt vectors, In *The Curves Seminar at Queen's, Vol. XI (Kingston, ON, 1997)*, volume 105 of *Queen's Papers in Pure and Appl. Math.*, Queen's Univ., Kingston, ON, 1997, 2–36.

[53] Gian-Carlo Rota and Bruce Sagan, Congruences derived from group action, *European J. Combin.*, **1** (1980), 67–76.

[54] F. Ruskey, C. R. Miers, and J. Sawada, The number of irreducible polynomials and Lyndon words with given trace, *SIAM J. Discrete Math.*, **14** (2001), no. 2, 240–245.

[55] Bruce E. Sagan, *The symmetric group*, Springer-Verlag, New York, second edition, 2001.

[56] I. Schur, Über die Darstellung der symmetrischen und der alterniерenden Gruppen durch gebrochene lineare substitutionen, *J. Reine Angew. Math.*, **139** (1911), 155–250.

[57] I. Schur, On the representation of the symmetric and alternating groups by fractional linear substitutions, *Internat. J. Theoret. Phys.*, **40** (2001), no. 1, 413–458. Translated from the German [J. Reine Angew. Math. **139** (1911), 155–250] by Marc-Felix Otto.

[58] Issai Schur, Arithmetische Eigenschaften der potenzsummen einer algebraischen Gleichung, *Compositio Math.*, **4** (1937), 432–444.

[59] J. Sheehan, An identity, *Amer. Math. Monthly*, **77** (1970), 168.

[60] C. J. Smyth, A coloring proof of a generalisation of Fermat's little theorem, *The American Mathematical Monthly*, **93** 1986, no. 6, 469–471.

[61] Richard P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge University Press, Cambridge, 1997.

[62] Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, Cambridge University Press, Cambridge, 1999.

[63] J. J. Sylvester, On a generalization of a theorem of Cauchy, *The London, Edinburgh and Dublin Philosophical Magazine and Journal of Science*, 4th series, **22** (1861), 378–382.

[64] Jean-Yves Thibon, The cycle enumerator of unimodal permutations, *Ann. Comb.*, **5** (2001), no.3-4, 493–500.

[65] S. Vajda, *Fibonacci & Lucas numbers, and the golden section: Theory and applications*, Ellis Horwood Ltd., Chichester, 1989.

[66] François Viète, Albert Girard, and Florimond de Beaune, *The early theory of equations: on their nature and constitution*, Translations of three treatises from the Latin and French by Robert Schmidt and Ellen Black, Golden Hind Press, Fairfield, CT, 1986.

[67] Edward Waring, *Meditationes algebraicæ*, edited and translated from the Latin by Dennis Weeks, American Mathematical Society, Providence, RI, 1991.

[68] Herbert S. Wilf, *Generatingfunctionology*, Academic Press Inc., Boston, MA, second edition, 1994.

[69] Doron Zeilberger, A combinatorial proof of Newton's identities, *Discrete Mathematics*, **49** (1984), no. 3, 319.