The Arithmetic of Multiple Harmonic Sums

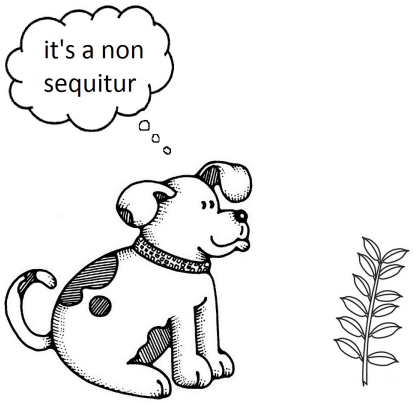
by

Julian H. Rosen

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in the University of Michigan
2013

Doctoral Committee:

Professor Jeffrey C. Lagarias, Chair
Professor Fred C. Adams
Associate Professor Kartik Prasanna
Professor Karen E. Smith
Professor Michael E. Zieve


it's a non
sequitur

To four people who taught me math when I was small:

Ed McLain — Bill Knight — Kris Warloe — Wayne Jackson

Acknowledgements

I thank my advisor, Jeff Lagarias, for providing mathematical insights, career advice, and lots of help producing a readable document. I also thank Jeff for introducing me to the problem that eventually became this thesis.

I thank all of the grad students at the University of Michigan who talked to me about math. Particularly, I thank Hunter Brooks and Jordan Watkins for numerous mathematical discussions.

I thank Daniel Fiorilli and Mike Zieve for career advice. I also thank Mike for several mathematical collaborations.

I thank Patricia Klein for enormous emotional support during the writing of this thesis.

I thank my Mom and Dad for always being there.

I thank Michael Johnson keeping me sane.

The work that went into this thesis was supported in part by NSF grants DMS-0943832 and DMS-1101373.

Table of Contents

List of Tables

Table

Chapter 1

Introduction

Over the past two decades, there has been a renewal of interest in a family of real numbers called multiple zeta values. Multiple zeta values are a generalization of the values the Riemann zeta function takes at positive integers. This thesis concerns the arithmetic of a family of rational numbers called multiple harmonic sums, which are finite analogs of multiple zeta values. There are many similarities between the two families. The theory of multiple zeta values is further developed, so we begin there.

1.1 Multiple zeta values

The Riemann zeta function, defined by the series

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

has a long history. Although it bears the name of the 19th century German mathematician Bernhard Riemann (who considered it as a function of a complex variable and provided an analytic continuation), study of this function predates Riemann by 200 years. Of particular interest prior to Riemann's work were the values of the zeta function at positive integers.

In 1735 Euler [9] computed $\zeta(2) = \frac{\pi^2}{6}$, solving what was then known as the Basel problem, first posed in 1644 by Pietro Mengoli. Euler's computation actually works for all even positive integers, and we have

$$\zeta(2n) = \frac{(2\pi)^{2n}(-1)^{n+1}B_{2n}}{2(2n)!},$$

where B_n are the Bernoulli numbers, defined by the power series

$$\frac{x}{e^x - 1} = \sum \frac{B_n}{n!} x^n.$$

The Bernoulli numbers are rational, so for each positive integer n, $\zeta(2n)$ is a rational multiple of π^{2n}.

Surprisingly little is known about $\zeta(n)$ for n odd. For example, none of these values are known to be transcendental, although it is conjectured that they are algebraically independent over $\mathbb{Q}(\pi)$. Apéry [1] provided a first step by proving in 1976 that $\zeta(3)$ is irrational. A result of Rivoal [29] from 2000 shows that for any $\epsilon > 0$, there exists an integer $A_0 > 0$ such that for all odd integers $a > A_0$, the dimension of the $\mathbb{Q}$ vector space spanned by $\zeta(3), \zeta(5), \ldots, \zeta(a)$ is at least $\frac{1-\epsilon}{1+\log(2)} \log(a)$. This implies that infinitely many odd zeta values are irrational. In 2004 Zudilin [42] proved that at least one of the four numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, or $\zeta(11)$ is irrational.

The multiple zeta function generalizes $\zeta(s)$ to a function of more than one variable. For k a positive integer, the *multiple zeta function of depth* k is the function of k complex variables defined by the series

$$\zeta(s_1, \ldots, s_k) = \sum_{n_1 > \ldots > n_k \geq 1} \frac{1}{n_1^{s_1} \ldots n_k^{s_k}}.$$

This series converges provided that $\mathrm{Re}(s_1) > 1$ and $\mathrm{Re}(s_i) > 0$ for $i = 2, 3, \ldots, k$ (see [15]). In depth 1 this is just the ordinary Riemann zeta function. A value of the multiple zeta function at integer arguments is called a multiple zeta value. Many interesting algebraic relations among multiple zeta values are known. As a particularly simple example, Euler knew that $\zeta(2,1) = \zeta(3)$.

Recall that a *composition* is a finite ordered list of positive integers. If $\mathbf{s} = (s_1, \ldots, s_k)$ is a composition, we define the *weight* and *depth* of $\mathbf{s}$ to be $w(\mathbf{s}) = s_1 + \ldots + s_k$ and $\ell(\mathbf{s}) = k$, respectively. We can think of ζ as a function that takes as input a composition $\mathbf{s} = (s_1, \ldots, s_k)$ and returns the multiple zeta value $\zeta(\mathbf{s}) := \zeta(s_1, \ldots, s_k)$.

Kontsevich [38] noted that multiple zeta values could be represented as iterated integrals of rational functions. This iterated integral is known as the Drinfeld integral, as it was studied earlier by Drinfeld [8] in connection with the absolute Galois group of $\mathbb{Q}$. The integral representation means that multiple zeta values are examples of

periods. Loosely speaking, a period is a complex number that arises from integrating a rational function with rational coefficients over a rationally defined domain. The set of periods forms a ring that contains all algebraic numbers. We will discuss the specific iterated integral construction in the next section.

1.1.1 Hoffman's algebra

In order to study multiple zeta values, Hoffman [15] considered the following non-commutative rings:

Definition 1.1.1. Set $\mathfrak{H}_{\mathbb{Q}} := \mathbb{Q}\langle x, y\rangle$, the non-commutative polynomial algebra in two variables, and the two subalgebras $\mathfrak{H}^1_{\mathbb{Q}} := \mathbb{Q} + \mathfrak{H}_{\mathbb{Q}}y$, $\mathfrak{H}^0_{\mathbb{Q}} := \mathbb{Q} + x\mathfrak{H}_{\mathbb{Q}}y$.

A basis for $\mathfrak{H}^1_{\mathbb{Q}}$ consists of words in the non-commuting symbols $z_1, z_2, \ldots$, where $z_n = x^{n-1}y$. A basis for $\mathfrak{H}^0_{\mathbb{Q}}$ consists of those words $z_{s_1} \ldots z_{s_n}$ with $s_1 \geq 2$. There is a $\mathbb{Q}$-linear "evaluation map" $\zeta : \mathfrak{H}^0_{\mathbb{Q}} \to \mathbb{R}$, taking the word $z_{s_1} \ldots z_{s_k} \in \mathfrak{H}^0_{\mathbb{Q}}$ to the multiple zeta value $\zeta(s_1, \ldots, s_k) \in \mathbb{R}$.

Hoffman also defined a commutative product, called the stuffle product, on $\mathfrak{H}^1_{\mathbb{Q}}$. The stuffle product $*$ is defined recursively. First we set

$$1 * \alpha = \alpha * 1 = \alpha$$

for every $\alpha \in \mathfrak{H}^1_{\mathbb{Q}}$. Next, if $k_1, k_2 \in \mathbb{Z}_{>0}$ and $\alpha_1, \alpha_2 \in \mathfrak{H}^1_{\mathbb{Q}}$, then

$$(z_{k_1}\alpha_1) * (z_{k_2}\alpha_2) = z_{k_1}(\alpha_1 * (z_{k_2}\alpha_2)) + z_{k_2}((z_{k_1}\alpha_1) * \alpha_2) + z_{k_1+k_2}(\alpha_1 * \alpha_2).$$

The multiplication $*$ restricts to give a commutative multiplication on $\mathfrak{H}^0_{\mathbb{Q}}$. The stuffle product is constructed to reflect multiplication of nested sums over integers, and we have

$$\zeta(\alpha_1 * \alpha_2) = \zeta(\alpha_1)\zeta(\alpha_2)$$

for all $\alpha_1, \alpha_2 \in \mathfrak{H}^0_{\mathbb{Q}}$.

The utility of using words in the symbols x and y (as opposed to the symbols $z_1, z_2, \ldots$) comes from Kontsevich's representation of a multiple zeta value as an iterated integral. Let $\alpha = u_1 \ldots u_k \in \mathfrak{H}^0_{\mathbb{Q}}$ be a word, with $u_i \in \{x, y\}$. We have an equality

$$\zeta(\alpha) = \iint\limits_{1 \geq t_1 > \ldots > t_k \geq 0} \omega_{u_1}(t_1)\omega_{u_2}(t_2) \ldots \omega_{u_k}(t_k)\, dt_1 dt_2 \ldots dt_k,$$

where $\omega_x(t) = \frac{1}{t}$, $\omega_y(t) = \frac{1}{1-t}$. To reflect this iterated integral expression, we define a second commutative product, called the shuffle product, on $\mathfrak{H}_{\mathbb{Q}}$. The shuffle product ш is defined recursively. First we set

$$1 ш \alpha = \alpha ш 1 = \alpha$$

for every $\alpha \in \mathfrak{H}_{\mathbb{Q}}$. Next, if $t_1, t_2 \in \{x, y\}$ and $\alpha_1, \alpha_2 \in \mathfrak{H}_{\mathbb{Q}}$, then

$$(t_1\alpha_1) ш (t_2\alpha_2) = t_1(\alpha_1 ш (t_2\alpha_2)) + t_2((t_1\alpha_1) ш \alpha_2).$$

The multiplication ш restricts to give commutative multiplications on $\mathfrak{H}^0_{\mathbb{Q}}$ and $\mathfrak{H}^1_{\mathbb{Q}}$. The shuffle product is constructed to reflect multiplication of iterated integrals, and we have

$$\zeta(\alpha_1 ш \alpha_2) = \zeta(\alpha_1)\zeta(\alpha_2)$$

for all $\alpha_1, \alpha_2 \in \mathfrak{H}^0_{\mathbb{Q}}$.

1.1.2 Relations among multiple zeta values

A major goal of the theory of multiple zeta values is classifying the algebraic relations over $\mathbb{Q}$ among multiple zeta values. We have already seen that $\zeta(2n)$ is a rational multiple of π^{2n} for each positive integer n. This means that $\zeta(2n)$ is a rational multiple of $\zeta(2)^n$ for all n, so we have, e.g., the relation $5\zeta(4) = 2\zeta(2)^2$. Lindemann's theorem of 1882 shows that π is a transcendental number, so we have a complete understanding of the algebraic structure of the field $\mathbb{Q}(\zeta(2), \zeta(4), \ldots)$: it is a purely transcendental extension of $\mathbb{Q}$ of transcendence degree 1, generated by π^2. This means we completely understand the stucture of algebraic relations among the values $\zeta(2), \zeta(4), \ldots$.

Our first example of a relation involving a multiple zeta value of depth 2 was the equality $\zeta(2,1) = \zeta(3)$. A more exotic relation is

$$66\zeta(13,3) + 375\zeta(11,5) + 686\zeta(9,7) + 675\zeta(7,9) + 396\zeta(5,11) = \frac{78967}{3617}\zeta(16),$$

which was discovered by Gangl, Kaneko, and Zagier [10] in their investigation of modular forms.

In view of either of the product representations given in the previous section, it will suffice to consider *linear* equations over $\mathbb{Q}$ satisfied by multiple zeta values.

Using the framework of the evaluation map $\zeta : \mathfrak{H}^0_{\mathbb{Q}} \to \mathbb{R}$, the problem of classifying algebraic relations among multiple zeta values reduces to describing the kernel of ζ. There are several known methods of producing elements of $\ker(\zeta)$. We describe a few of these methods below.

The stuffle and shuffle products give us two different ways to express a product of multiple zeta values as a $\mathbb{Z}$-linear combination of multiple zeta values. This implies that for all $\alpha_1, \alpha_2 \in \mathfrak{H}^0_{\mathbb{Q}}$, $\alpha_1 * \alpha_2 - \alpha_1 \text{ш} \alpha_2 \in \ker(\zeta)$. This is known as the *double shuffle relation* (see the work of Ihara, Kaneko, and Zagier [17] for an introduction). The double shuffle relation can be generalized to allow $\alpha_1, \alpha_2 \in \mathfrak{H}^1_{\mathbb{Q}}$, using a regularization process. Regularization leads to the so-called *extended double shuffle relations*.

Another method of producing linear relations among multiple zeta values is the Duality Theorem, conjectured by Hoffman [14] and proven by Kontsevich [38]. We first define an anti-automorphism $\tau : \mathfrak{H}_{\mathbb{Q}} \to \mathfrak{H}_{\mathbb{Q}}$ which interchanges x and y. The map τ restricts to an anti-automorphism of $\mathfrak{H}^0_{\mathbb{Q}}$. The Duality Theorem for multiple zeta values is the statement that

$$\zeta(\alpha) = \zeta(\tau(\alpha)) \text{ for all } \alpha \in \mathfrak{H}^0_{\mathbb{Q}}.$$

In other words, $\tau(\alpha) - \alpha \in \ker(\zeta)$.

There is a map $D : \mathfrak{H}_{\mathbb{Q}} \to \mathfrak{H}_{\mathbb{Q}}$, determined by $D(x) = 0$, $D(y) = xy$, and the condition that D is a $\mathbb{Q}$-derivation. The derivation D restricts to a derivation on the subalgebra $\mathfrak{H}^0_{\mathbb{Q}}$. If we set $\overline{D} := \tau D \tau$ (where τ is the anti-involution defined above), then a result of Hoffman [14] implies that

$$\overline{D}(\alpha) - D(\alpha) \in \ker(\zeta) \text{ for all } \alpha \in \mathfrak{H}^0_{\mathbb{Q}}.$$

This was later generalized by Ohno [26]. A further generalization was given by Ihara, Kaneko, and Zagier [17].

The kernel of ζ is conjectured to be a homogeneous ideal. Indeed, all known relations among multiple zeta values can be decomposed into homogeneous relations (that is, relations involving compositions of fixed weight). Define d_n to be the $\mathbb{Q}$-dimension of the image of the n-th graded piece of $\mathfrak{H}^0_{\mathbb{Q}}$ under ζ. In other words, d_n is the number of linearly independent multiple zeta values of weight n. Using known methods for constructing relations among multiple zeta values, the conjectural values

of d_n for $n \leq 10$ are given in the following table:

n	2	3	4	5	6	7	8	9	10
d_n	1	1	1	2	2	3	4	5	7

Numerology suggests that $d_n = A_n$, where A_n is defined to be the sequence satisfying the linear recurrence relation $A_n = A_{n-2} + A_{n-3}$, with initial values $A_2 = A_3 = A_4 = 1$. This was conjectured by Zagier [38] in 1994, and the upper bound $d_n \leq A_n$ was proven by Terasoma [32] in 2002. Zagier's conjecture led Hoffman [15] to conjecture in 1997 that multiple zeta values of the form $\zeta(s_1, \ldots, s_k)$ with $s_i \in \{2, 3\}$ form a basis for the space of multiple zeta values (it can be checked that the number a_n of compositions $\mathbf{s} = (s_1, \ldots, s_k)$ with $s_i \in \{2, 3\}$ and $w(\mathbf{s}) = n$ satisfies the conjectured recurrence, and has the same initial values). Brown [6] showed in 2012 that multiple zeta values $\zeta(s_1, \ldots, s_k)$ with $s_i \in \{2, 3\}$ span the space of multiple zeta values, proving one part of Hoffman's conjecture.

1.2 Multiple harmonic sums

The work of this thesis is on multiple harmonic sums, which are values of a finite truncation of the multiple zeta function.

Definition 1.2.1. Let $\mathbf{s} = (s_1, s_2, \ldots, s_k)$ be a composition, n a non-negative integer. The *multiple harmonic sum* is given by

$$H_n(\mathbf{s}) = H_n(s_1, \ldots, s_k) := \sum_{n \geq n_1 > n_2 > \ldots > n_k \geq 1} \frac{1}{n_1^{s_1} \ldots n_k^{s_k}}.$$

We will denote by $\{s_1, \ldots, s_k\}^a$ the composition

$$(\underbrace{s_1, \ldots, s_k}, \underbrace{s_1, \ldots, s_k}, \ldots, \underbrace{s_1, \ldots, s_k}),$$

consisting of a concatenated copies of $(s_1, \ldots, s_k)$.

Unlike what is conjectured to be the case for multiple zeta values, multiple harmonic sums are rational numbers, and we are interested in their arithmetic properties. We will take $n = p - 1$, p a prime, and study p-adic congruence properties of the multiple harmonic sums $H_{p-1}(\mathbf{s})$ for various compositions $\mathbf{s}$.

1.2.1 Modulo p multiple harmonic sums

Hoffman [16] and Zhao [40] independently studied the residues of the multiple harmonic sums $H_{p-1}(\mathbf{s})$ modulo p, p a prime. Multiple harmonic sums satisfy many congruences modulo powers of p, the most familiar of which is probably Wolstenholme's theorem, stating that $H_{p-1}(1) \equiv 0 \mod p^2$ for all primes $p \geq 5$.

Congruences modulo p for multiple harmonic sums fail to hold for certain small primes. One way to account for this is to consider the ring

$$\mathcal{A} := \left(\prod_p \mathbb{Z}/p\mathbb{Z}\right) / \left(\bigoplus_p \mathbb{Z}/p\mathbb{Z}\right).$$

An element of $\mathcal{A}$ is a tuple (a_p) with $a_p \in \mathbb{Z}/p\mathbb{Z}$, where we identify (a_p) and (a'_p) if $a_p = a'_p$ for all but finitely many primes p. The ring $\mathcal{A}$ is a $\mathbb{Q}$-algebra. This formulation is discussed in [30], building upon an idea in [19]. In the theory of modulo p multiple harmonic sums, the analog of the the numbers d_n (which count the number of linearly independent multiple zeta values of weight n) is the dimension (over $\mathbb{Q}$) of the span of the elements

$$(H_{p-1}(\mathbf{s})) \in \mathcal{A},$$

where $\mathbf{s}$ runs over compositions of weight n. For example, there is only one composition of weight 1, and Wolstenholme's theorem says that this sum is divisible by p (in fact, p^2) for sufficiently large primes p, so $c_1 = 0$. Likewise, there are two sums of weight two, and it is known that

$$H_{p-1}(2) \equiv H_{p-1}(1,1) \equiv 0 \pmod{p} \text{ for } p \geq 5,$$

so that $c_2 = 0$. In weight 3, there are four sums to consider. It is known [16, 40] that

$$H_{p-1}(1,1,1) \equiv H_{p-1}(3) \equiv 0$$

$$H_{p-1}(2,1) \equiv -H_{p-1}(1,2) \mod p,$$

so that $c_3 = 1$.

The structure of modulo p multiple harmonic sums has been studied by several other authors. Tauraso [31] studied a modulo p analog of Apéry's series' for $\zeta(2)$

and $\zeta(3)$. Pilehrood and Pilehrood [27] extended this to series for $\zeta(4)$ and $\zeta(5)$. Pilehrood, Pilehrood, and Tauraso [28] computed a modulo p analog of Zagier's computation [39] of $\zeta(2,\ldots,2,3,2\ldots,3)$. Very recent work of Saito and Wakabayashi [30] establishes a modulo p analog of a theorem of Bowman and Bradley [4] on relations between multiple zeta values of a certain shape.

The best known upper bounds for c_n (which are conjectured to be the true values) are given in [28]:

n	1	2	3	4	5	6	7	8	9
c_n	0	0	1	0	1	1	1	2	2

No formula for c_n has been conjectured.

1.2.2 Congruences modulo higher powers of p

Our departure from the theory of modulo p multiple harmonic sums begins by considering congruences modulo higher powers of p. As a motivating example, we have the congruence

$$2H_{p-1}(1) \equiv pH_{p-1}(2) \mod p^3 \text{ for } p \geq 7,$$

extending Wolstenholme's theorem. Unlike the congruences arising from the study of multiple harmonic sums modulo p, our congruence involves multiple harmonic sums of two different weights. We also have a factor of p appearing as the coefficient of $H_{p-1}(2)$. It will turn out to be more convenient if we multiply through by p to obtain

$$2pH_{p-1}(1) \equiv p^2H_{p-1}(2) \mod p^4. \tag{1.1}$$

This congruence involves terms of the form $p^{w(\mathbf{s})}H_{p-1}(\mathbf{s})$, where $\mathbf{s}$ is a composition and p is a prime. We refer to these terms as *weighted* multiple harmonic sums. The coefficients of the weighted sums will be rational numbers independent of p.

The congruence (1.1) can be extended. If $N \geq 2$ is an integer, we have the congruence

$$2pH_{p-1}(1) \equiv \sum_{n=2}^{N}(-1)^n p^n H_{p-1}(n) \begin{cases} \mod p^{N+2} \text{ if } 2|N \\ \mod p^{N+1} \text{ if } 2 \nmid N. \end{cases}$$

Letting $N \to \infty$, we get the identity

$$2pH_{p-1}(1) = \sum_{n=2}^{\infty} (-1)^n p^n H_{p-1}(n), \tag{1.2}$$

where the sum is p-adically convergent for all primes p. We call equation (1.2) an *asymptotic relation among weighted multiple harmonic sums*, or an *asymptotic relation* for short.

1.3 Statement of results

This section summarizes the main results of the thesis. Our results involve multiple harmonic sums $H_{p-1}(\mathbf{s})$, where p is a prime and $\mathbf{s}$ a composition. More specifically, we study linear congruences involving the weighted multiple harmonic sums $p^{w(\mathbf{s})}H_{p-1}(\mathbf{s})$, whose coefficients are rational numbers independent of p.

1.3.1 Binomial coefficient congruences

Wolstenholme's theorem, stated above, is the congruence $H_{p-1}(1) \equiv 0 \pmod{p^2}$, holding for all primes $p \geq 5$. In Chapter 2 we consider generalizations of Wolstenholme's theorem in two directions.

In the first direction, we observe that an equivalent form of Wolstenholme's theorem involves binomial coefficients, and gives the congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ for all $p \geq 5$. The two forms of Wolstenholme's theorem can be combined in the congruence

$$\binom{2p-1}{p-1} \equiv 1 - 2pH_{p-1}(1) \pmod{p^5},$$

due to van Hamme [34], which holds for $p \geq 7$. A stronger congruence was recently given by Meštrović [22], who showed that

$$\binom{2p-1}{p-1} \equiv 1 + 2pH_{p-1}(1) - 4p^2H_{p-1}(1,1) \pmod{p^7}$$

holds for $p \geq 11$. Our result involves the *elementary symmetric multiple harmonic sums* $H_{p-1}(\{1\}^n)$.

In the second direction, we generalize the binomial coefficient that appears. An example of this kind of generalization was given by Glaisher [12], who showed that

$$\binom{kp-1}{p-1} \equiv 1 \pmod{p^3}$$

holds for all primes $p \geq 5$ and all positive integers k. Our result is a common generalization of the preceding results. The coefficients in our congruences are given by polynomials in k. We make the following definition.

Definition 1.3.1. For integers $0 \leq j \leq n$, let $b_{j,n}(T) \in \mathbb{Q}[T]$ be the unique polynomial of degree at most $2n+1$ satisfying

- $b_{j,n}(T) \equiv (T-1)^j \mod (T-1)^{n+1}$
- $b_{j,n}(T) \equiv (-1)^j T^j \mod T^{n+1}$

The polynomials $b_{j,n}(T)$ are called *extremal polynomials*.

Now we can state our general family of congruences for $\binom{kp-1}{p-1}$ in terms of multiple harmonic sums.

Theorem 1.3.2 (Optimized Binomial Congruences)**.** *Fix a non-negative integer n. The polynomials $b_{j,n}(T)$ have integer coefficients for $j = 0, 1, \ldots, n$, and the following hold:*

1. *For every prime $p \geq 2n+5$ and every integer k:*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k)\, p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}. \tag{1.3}$$

2. *If $p = 2n+3$ is prime, then for every integer k, the above congruence holds modulo p^{2n+2}.*

3. *For every prime $3 \leq p \leq 2n+1$ and every integer k, the above congruence is an equality:*

$$\binom{kp-1}{p-1} = \sum_{j=0}^{n} b_{j,n}(k)\, p^j H_{p-1}(\{1\}^j).$$

Theorem 1.3.2 has four important features:

1. The coefficients $b_{j,n}(k)$ appearing in the congruence (1.3) are independent of the prime p.

2. There are a large number of congruences for $\binom{kp-1}{p-1}$ holding modulo p^{2n+3}, which involve the multiple harmonic sums $H_{p-1}(\{1\}^j)$ for $1 \leq j \leq 2n$ (see Theorem 2.3.3). The congruences (1.3) are extremal among these in only containing the terms $H_{p-1}(\{1\}^j)$ for $1 \leq j \leq n$.

3. The restriction of the theorem to exclude certain small primes, depending on n, is necessary. The congruences may fail to hold modulo p^{2n+3} for $p = 2n+3$ (when $2n+3$ is prime), and generally also fail for $p = 2$.

4. The extremal polynomials $b_{j,n}(T)$ depend on n, and for fixed j their values at integers $b_{j,n}(k)$ (which are the coefficients in the congruences) do *not* stabilize as $n \to \infty$ (with the exception of $b_{0,n}(k)$; see the tables in 2.1.2). However they do satisfy many interesting congruences as n varies, which we address in Section 2.6.

We also provide a classification of those triples (n, p, k) for which the extremal congruence (1.3) holds modulo an extra power of p.

Theorem 1.3.3 (Exceptional Congruences)**.** *Let the polynomials $b_{j,n}(T)$ be as in the statement of Theorem 1.3.2.*

1. *For every prime $p \geq 2n+5$ and every integer $k \geq 1$, the congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=1}^{n} b_{j,n}(k)\, p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+4}}$$

holds if and only if either $k \equiv 0, 1 \mod p$ or p divides the numerator of the Bernoulli number B_{p-2n-3}.

2. *If $p = 2n+3$ is prime and k is any integer, then the congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=1}^{n} b_{j,n}(k)\, p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}$$

holds if and only if $k \equiv 0, 1 \mod p$.

To prove these theorems, we make use of the following family of asymptotic relations among the elementary symmetric multiple harmonic sums.

Theorem 1.3.4 (Asymptotic Relations for Elementary Symmetric Sums)**.** *Let n be a non-negative integer. For all odd primes p, we have*

$$p^n H_{p-1}(\{1\}^n) + \sum_{j \geq n} (-1)^{j+1} \binom{j}{n} p^j H_{p-1}(\{1\}^j) = 0.$$

This identity follows from Proposition 2.2.1 in Chapter 2. The summation above is finite, as $H_{p-1}(\{1\}^j) = 0$ for $j > p-1$, but the length of the sum depends on p. We further investigate this family of asymptotic relations in Chapter 5.

Uniqueness of binomial congruences

We believe that our congruences are the only ones of shape (1.3). Although we cannot prove this unconditionally, we can show that it follows from the following conjecture.

Conjecture 1.3.5 (Linear Bernoulli Nondegeneracy Conjecture)**.** *Fix an odd integer $k \geq 3$. There are infinitely many primes p for which p does not divide the numerator of the Bernoulli number B_{p-k}.*

Our uniqueness statement has the following form:

Theorem 1.3.6 (Uniqueness of Optimized Congruences)**.** *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. Let n, k be integers with $n \geq 0$, and suppose $b_0, \ldots, b_n \in \mathbb{Q}$ are such that the congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}$$

holds for all sufficiently large primes p. Then we have $b_j = b_{j,n}(k)$, where $b_{j,n}(T)$ are the extremal polynomials defined in the statement of Theorem 1.3.2.

A similar uniqueness statment for L-value congruences is given as Theorem 1.3.11, which also depends on the Linear Bernoulli Nondegeneracy Conjecture.

1.3.2 Congruences for p-adic L-function values

In Chapter 3, we study congruences for values $L_p(k, \omega^{1-k})$ of the Kubota-Leopold p-adic L-function, where k is a positive integer. We begin with a brief introduction to p-adic L-functions.

The Riemann zeta function takes rational values at the negative integers. More generally, if χ is any Dirichlet character, the values of the Dirichlet L-function $L(s, \chi)$ at negative integers are algebraic numbers, and in fact lie in the number field generated by the values of χ. These algebraic numbers can be written explicitly in terms of generalized Bernoulli numbers.

Let p be a prime, χ a primitive Dirichlet character. Fix, once and for all, embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\mathbb{C}_p$. We will identify elements of $\mathbb{C}$ algebraic over $\mathbb{Q}$ with elements of $\mathbb{C}_p$. In 1851 Kummer showed that the generalized Bernoulli numbers

satisfy certain congruence properties modulo powers of p, which imply that the restriction of $L(s,\chi)$ to the negative integers in a fixed residue class modulo $p-1$ is p-adically continuous. Kubota and Leopoldt [20] used Kummer's congruences to define a p-adic L-function L_p. For any Dirichlet character $\chi \neq 1$, the Kubota-Leopoldt p-adic L-function $L_p(s,\chi)$ is the unique continuous function $\mathbb{Z}_p \to \mathbb{C}_p$ whose values agree with the Dirichlet L-function $L(s,\chi)$ when s is a negative integer congruent to 1 modulo $p-1$. When $\chi = 1$, $L_p(s,\chi)$ has a simple pole at $s = 1$. Kubota and Leopoldt go further, showing that $L_p(s,\chi)$ is analytic, not just continuous.

The Teichmüller character $\omega = \omega_p$ is the Dirichlet character of conductor p taking a positive integer n not divisible by p to the unique $(p-1)$-th root of unity in $\mathbb{C}_p$ that is congruent to n modulo p (remember that we are identifying $\overline{\mathbb{Q}} \subset \mathbb{C}$ with $\overline{\mathbb{Q}} \subset \mathbb{C}_p$). We consider the values $L_p(k,\omega^{1-k})$ where $k \geq 3$ is an odd integer (this function vanishes when $k \geq 2$ is even). These values are p-adic analogs of values of the Riemann zeta function, and some authors write $\zeta_p(k)$ for $L_p(k,\omega^{1-k})$.

Washington [36] gave expressions for the modified harmonic sums

$$H_{pn}^{(p)}(r) := \sum_{\substack{j=1 \\ (j,p=1}}^{pn} \frac{1}{j^r},$$

with r a positive integer, in terms of these p-adic L-function values. Note that $H_p^{(p)}(r) = H_{p-1}(r)$. This generalizes a result of Boyd [5], but a special case appeared in earlier work of Morita [24, 25]. The precise expression is given here:

Proposition 1.3.7 (Modified Harmonic Sum Values)**.** *Let r, n be positive integers, p an odd prime. Then:*

$$H_{np}^{(p)}(r) = -\sum_{j=1}^{\infty} \binom{-r}{j} L_p(r+j, \omega^{1-j-r})(pn)^j,$$

where the infinite sum is p-adically convergent.

We use this to derive the following expression for the values $L_p(k,\omega^{1-k})$ in terms of the power sum multiple harmonic sums.

Theorem 1.3.8 (p-adic L-values and Multiple Harmonic Sums)**.** *Let $k \geq 2$ be an*

negative integer, and p an odd prime. Then

$$p^k L_p(k, \omega^{1-k}) = \sum_{n \geq k-1} \frac{(-1)^{n+k+1}}{n} \binom{n}{k-1} B_{n+k+1}\, p^n H_{p-1}(n).$$

where the right side is p-adically convergent.

This is proven in Chapter 3 as Theorem 3.2.5. Our main theorem is a congruence for the values $L_p(k, \omega^{1-k})$ in terms of multiple harmonic sums.

Theorem 1.3.9 (Extremal p-adic L-value Congruences)**.** *Let $k \geq 3$ be an odd integer, n a non-negative integer. There exist explicitly computable rational constants $b_j(k, n)$, $j = 0, 1, \ldots$, such that the congruence*

$$pL_p(k, \omega_p^{1-k}) \equiv \sum_{j=0}^{n} b_j(k, n) p^j H_{p-1}(k - 1 + j) \pmod{p^{2n+3}} \tag{1.4}$$

holds for all sufficiently large primes p.

This is proven in Chapter 3 as Theorem 3.4.1. The proof makes use of the following family of asymptotic relations among the power sum multiple harmonic sums.

Theorem 1.3.10 (Asymptotic Relations for Power Sums)**.** *Let n be a non-negative integer. For all primes p, we have*

$$(-1)^n p^{n+1} H_{p-1}(n+1) + \sum_{i \geq n} \binom{i}{n} p^{i+1} H_{p-1}(i+1) = 0,$$

where the above sum converges in $\mathbb{Q}_p$ for every n.

This is proven as Proposition 3.3.1. Note that the sum above is actually infinite. We further investigate this family of asymptotic relations in Chapter 5.

Uniqueness of L-value congruences

As was the case with Theorem 1.3.2, we can establish uniqueness of our congruences for L-values if we assume the Linear Bernoulli Nondegeneracy Conjecture.

Theorem 1.3.11 (Uniqueness of Optimized L-value Congruences)**.** *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. Then the constants $b_j(k, n)$ appearing in the statement of Theorem 1.3.9 are uniquely determined by the condition that the congruence (1.4) holds for all sufficiently large primes p.*

This is proven as Corollary 3.5.3.

1.3.3 Asymptotic relations

In Chapter 4, we examine a family of identities related to the identity

$$2pH_{p-1}(1) = \sum_{n=2}^{\infty}(-1)^n p^n H_{p-1}(n)$$

given previously, which is an example of an *asymptotic relation*. To study asymptotic relations, we will use a completion of the graded ring $\mathfrak{H}^1_{\mathbb{Q}}$ defined by Hoffman. For technical reasons[1], we work over $\mathbb{Z}[\frac{1}{2}]$ instead of over $\mathbb{Q}$.

Definition 1.3.12. Let $\mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]} := \mathbb{Z}[\frac{1}{2}]\langle x, y\rangle$, the polynomial algebra over $\mathbb{Z}[\frac{1}{2}]$ in non-commuting variables x and y, and two subalgebras $\mathfrak{H}^1_{\mathbb{Z}[\frac{1}{2}]} := \mathbb{Z}[\frac{1}{2}] + \mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]}y$, $\mathfrak{H}^0_{\mathbb{Z}[\frac{1}{2}]} := \mathbb{Z}[\frac{1}{2}] + x\mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]}y$. Let $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ be the completion of the ring $\mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]}$ with respect to the grading given by degree. If we set $z_n := x^{n-1}y$ for $n \geq 0$, an element of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ is a formal infinite sum

$$\alpha = \sum_{\mathbf{s}=(s_1,\ldots,s_k)} \alpha_{\mathbf{s}} z_{s_1} \ldots z_{s_k}, \tag{1.5}$$

where the summation is taken over all compositions $\mathbf{s}$, and the coefficients $\alpha_{\mathbf{s}}$ are in $\mathbb{Z}[\frac{1}{2}]$. The topology on $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ has a neighborhood basis consisting of the sets

$$\mathbb{I}_n := \left\{ \sum_{\mathbf{s}} \alpha_{\mathbf{s}} z_{s_1} \ldots z_{s_k} : \alpha_{\mathbf{s}} = 0 \text{ when } s_1 + \ldots + s_k < n \right\}.$$

The stuffle product $*$ gives a (continuous) commutative multiplication on $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$.

For each non-negative integer n, $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}/\mathbb{I}_n$ is free and finitely-generatedl as a module over $\mathbb{Z}[\frac{1}{2}]$. We denote by $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ the set $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ viewed as a commutative topological ring with the stuffle product. The ring $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ is isomorphic to the completion of the ring of quasi-symmetric functions over $\mathbb{Z}[\frac{1}{2}]$; see [16] for a discussion of quasi-symmetric functions and the proof of this fact.

The element α given by (1.5) represents the (infinite) formal sum

$$\sum_{\mathbf{s}} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}) \tag{1.6}$$

[1] Another possibility is discussed in the Appendix

of weighted multiple harmonic sums, with p an unspecified prime. Elements of $\mathbb{I}_n$ represent sums of the form (1.6) that are formally divisibly by p^n.

The following formalism is new.

Definition 1.3.13.

- For each prime $p \geq 3$, define $\phi_p : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \mathbb{Z}_p$,

$$\left(\sum_{\mathbf{s}=(s_1,\ldots,s_k)} \alpha_{\mathbf{s}} z_{s_1} \ldots z_{s_k} \right) \mapsto \sum_{\mathbf{s}=(s_1,\ldots,s_k)} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(s_1, \ldots, s_k).$$

  It is a continuous ring homomorphism.

- We let $\phi : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \prod_{p\geq 3} \mathbb{Z}_p$ be the product of the maps ϕ_p, and we call ϕ the *universal evaluation map.*

- For each non-negative integer n, we define

$$\mathbb{J}_n := \{\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} : p^n | \phi_p(\alpha) \text{ for all sufficiently large primes } p\}.$$

The closed ideal $\ker(\phi)$ plays the same role for us that $\ker(\zeta) \subset \mathfrak{H}^0_{\mathbb{Q}}$ plays in the study of multiple zeta values. Unlike what is conjectured to be the case for $\ker(\zeta)$, the ideal $\ker(\phi)$ is not homogeneous. Particularly, the identity (1.2) shows that the non-homogeneous element $2y - xy + x^2y - \ldots = y + (1+x)^{-1}y$ is in $\ker(\phi)$, and its degree one homogeneous component $2y$ is not.

We have the containment $\ker(\phi) + \mathbb{I}_n \subset \mathbb{J}_n$, which is the statement that an asymptotic relation can be truncated to give a congruence holding for all but finitely many primes. In many known examples, a converse holds: if we have a congruence for weighted multiple harmonic sums, we can find an asymptotic relation with the congruence as a truncation. We make the following conjecture.

Conjecture 1.3.14. *Let n be a positive integer, and suppose $\alpha \in \mathbb{J}_n$. Then there exists an integer $r > 0$ such that $r\alpha \in \ker(\phi) + \mathbb{I}_n$.*

The statement of this conjecture can we simplified if adopt the asymptotic evaluation map described in the Appendix.

Remark 1.3.15. A complete undertstanding of the ideals $\mathbb{J}_n$ would suffice to determine the structure modulo p of the multiple harmonic sums of a given weight n. The set of formal $\mathbb{Z}[\frac{1}{2}]$-linear combinations of multiple harmonic sums of weight n is $\mathbb{I}_n/\mathbb{I}_{n+1}$, and the number of linearly independent sums in this weight is $\operatorname{rank}_{\mathbb{Z}[\frac{1}{2}]}(\mathbb{I}_n/(\mathbb{J}_{n+1}\cap\mathbb{I}_n))$.

There is an anti-automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ which squares to the identity, namely taking $z_{s_1}\dots z_{s_k}$ to

$$\overline{z_{s_1}\dots z_{s_k}} := z_{s_k}\dots z_{s_1}.$$

This can also be viewed as an involution on the set of compositions, where we set $\overline{(s_1,\dots,s_k)} = s_k\dots s_1$. Hoffman ([16], Theorem 4.5) shows that for every composition $\mathbf{s}$, we have the congruence

$$H_{p-1}(\mathbf{s}) \equiv (-1)^{w(\mathbf{s})} H_{p-1}(\overline{\mathbf{s}}) \pmod{p}$$

for all primes p. The following is an asymptotic extension of this congruence.

Theorem 1.3.16 (Asymptotic Reflection Theorem)**.** *Let $\mathbf{s}=(s_1,\dots,s_k)$ be a composition. For all primes p we have a convergent p-adic series equality*

$$H_{p-1}(\mathbf{s}) = (-1)^{w(\mathbf{s})} \sum_{\substack{\mathbf{b}=(b_1,\dots,b_k)\\ b_1,\dots,b_k\geq 0}} \prod_{j=1}^{k} \binom{s_j+b_j-1}{s_j-1} p^{b_1+\dots+b_k} H_{p-1}(\overline{\mathbf{s}}+\mathbf{b}),$$

where $\mathbf{s}+\mathbf{b} = (s_1+b_1,\dots,s_k+b_k)$.

We can state the Asymptotic Reflection Theorem in terms of the derivation $\overline{d}$ defined by Ihara, Kaneko, and Zagier ([17], Table 2):

Theorem 1.3.17 (Asymptotic Reflection Theorem, short form)**.** *Let $\overline{d}$ be the derivation on $\widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]}$ given by $x\mapsto x^2$, $y\mapsto xy$, and let $R:\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}\to\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ be the anti-involution sending $z_{s_1}\dots z_{s_k}$ to $(-1)^{s_1+\dots+s_k} z_{s_k}\dots z_{s_1}$. Then $\exp(\overline{d})$ is an automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, and for any $\alpha\in\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$,*

$$\exp\left(\overline{d}\right)(\alpha) - \mathrm{R}(\alpha) \in \mathbb{J}_\infty.$$

In [16] Hoffman also proves a duality theorem (Theorem 4.6). To state this theorem, we need a definition. For n a non-negative integer and $\mathbf{s}=(s_1,\dots,s_k)$ a composition, we let

$$S_n(\mathbf{s}) := \sum_{n\geq n_1\geq n_2\geq\dots\geq n_k\geq 1} \frac{1}{n_1^{s_1}\dots n_k^{s_k}}.$$

This sum can be expressed in terms of multiple harmonic sums:

$$S_n(\mathbf{s}) = \sum_{\mathbf{t} \preceq \mathbf{s}} H_n(\mathbf{t}),$$

where $\mathbf{t} \preceq \mathbf{s}$ means the composition $\mathbf{t}$ can be obtained from $\mathbf{s}$ by combining some of its parts.

Compositions $\mathbf{s} = (s_1, \ldots, s_k)$ of weight n are in bijection with subsets of $\{1, 2, \ldots, n-1\}$ by the map

$$\varphi : (s_1, \ldots, s_k) \mapsto \{s_1, s_1 + s_2, \ldots, s_1 + s_2 + \ldots + s_{k-1}\}. \tag{1.7}$$

The dual $\mathbf{s}^*$ is the composition corresponding under (1.7) to the complement of $\varphi(\mathbf{s})$. The operation $\mathbf{s} \mapsto \mathbf{s}^*$ squares to the identity. Hoffman's result states that for all compositions $\mathbf{s}$, the congruence

$$S_{p-1}(\mathbf{s}) + S_{p-1}(\mathbf{s}^*) \equiv 0 \pmod{p}$$

holds for all primes p. This was later extended by Zhao, who showed that for all odd primes p,

$$S_{p-1}(\mathbf{s}) + S_{p-1}(\mathbf{s}^*) + p \left(\sum_{\mathbf{t} \preceq \mathbf{s}} H_{p-1}((1) \sqcup \mathbf{t}) \right) \equiv 0 \pmod{p^2},$$

where $(1) \sqcup (t_1, \ldots, t_k) = (1, t_1, \ldots, t_k)$. These congruences can be expressed in a different way. Define a continuous involution $\psi : \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]}$, $x \mapsto x + y$, $y \mapsto -y$. This restricts to a map $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, which we also denote ψ. Hoffman [16] shows that the duality theorem is equivalent to the congruence

$$H_{p-1}(\psi(\mathbf{s})) - H_{p-1}(\mathbf{s}) \equiv 0 \pmod{p}.$$

Our asymptotic extension of the above congruences is stated in terms of two automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$: ψ (described by Hoffman in [16]) and $\Phi_{(-y)}$ (described by Ihara, Kaneko, and Zagier in [17]).

Theorem 1.3.18 (Asymptotic Duality Theorem)**.** *Let $\psi : \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]}$ be the automorphism $x \mapsto x + y$, $y \mapsto -y$, and $\Phi_{(-y)} : \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ the automorphism*

$\alpha \mapsto (1+y)\left(\frac{1}{1+y} * \alpha\right)$. *Then* ψ *restricts to an automorphism of* $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, *and for all* $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, *we have*

$$\Phi_{(-y)}(\alpha) - \psi(\alpha) \in \mathbb{J}_\infty.$$

Proofs of the Asymptotic Reflection Theorem and the Asymptotic Duality Theorem are given in Chapter 4.

1.3.4 Asymptotic relations for symmetrized multiple harmonic sums

Chapter 5 concerns *symmetrized* multiple harmonic sums, which we now define. Suppose $\mathbf{s} = (s_1, \ldots, s_k)$, $\mathbf{t} = (t_1, \ldots, t_k)$ are two compositions of equal length. We write $\mathbf{s} \sim \mathbf{t}$ if there exists a permutation $\sigma \in S_k$ such that $s_i = t_{\sigma(i)}$ for $i = 1, 2, \ldots, k$.

Definition 1.3.19. Let $\mathbf{s}$ be a partition of length k, N a positive integer. We define the *symmetrized multiple harmonic sum* by

$$\mathscr{H}_N(\mathbf{s}) = \sum_{\mathbf{t} \sim \mathbf{s}} H_N(\mathbf{t}).$$

We have the special cases $\mathscr{H}_N(\{1\}^k) = H_N(\{1\}^k)$ and $\mathscr{H}_N(k) = H_N(k)$, $k, n \in \mathbb{N}$. If $\mathbf{s} \sim \mathbf{t}$, then $\mathscr{H}_N(\mathbf{s}) = \mathscr{H}_N(\mathbf{t})$, so that we may restrict our attention to the case that $\mathbf{s}$ is a partition (i.e., $\mathbf{s} = (s_1, \ldots, s_k)$ with $s_1 \geq \ldots \geq s_k$).

To study asymptotic relation involving symmetrized multiple harmonic sums, we use a completion of the ring of symmetric functions over $\mathbb{Z}[\frac{1}{2}]$, which has the form

$$\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} = (\mathbb{Z}[\frac{1}{2}])[[e_1, e_2, \ldots]],$$

where e_n is the n-th elementary symmetric function. We think of e_n as representing the expression $p^n \mathscr{H}_{p-1}(\{1\}^n)$, with p an unspecified odd prime. We identify $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ with the closed $\mathbb{Z}[1/2]$-subalgebra of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ generated by the elements $z_1, z_2, \ldots$, identifying $e_n \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ with $y^n \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$.

For each odd prime p, there is a continuous ring homomorphism

$$\varphi_p : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to \mathbb{Z}_p,$$

taking e_n to $p^n \mathscr{H}_{p-1}(\{1\}^n)$. We denote by $\varphi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to \prod_{p \geq 3} \mathbb{Z}_p$ the product of these maps. This map φ is just the restriction of the universal evaluation map

$\phi : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \prod_{p\geq 3} \mathbb{Z}_p$ to $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \subset (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$. For $n \in \mathbb{Z}_{>0}$, we get an ideal

$$\mathscr{J}_n := \{\alpha \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} : \varphi_p(\alpha) \in p^n \mathbb{Z}_p \text{ for all sufficiently large primes } p\}.$$

Our first result is a description of the ideals $\ker(\varphi)$ and $\mathscr{J}_n$ for $n = 0, 1, 2, \ldots$. The following definition is used in our description of $\mathscr{J}_n$.

Definition 1.3.20. We define a non-Archimedean valuation v on $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ to be trivial on $\mathbb{Z}\left[\frac{1}{2}\right]$, and given by

$$v(e_n) = \begin{cases} n+1 & \text{if } n \text{ even}, \\ n+2 & \text{if } n \text{ odd}, \end{cases}$$

extended multiplicatively to monomials. Denote by $\mathscr{I}_n$ the ideal consisting of those $\alpha \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ for which $v(\alpha) \geq n$. The ideals $\mathscr{I}_n$ form a neighborhood basis of 0 for the topology on $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$.

The valuation v is motivated by congruences for multiple harmonic sums (given below as Proposition 2.3.1), which imply that for $n \geq 0$, $v_p(p^n \mathscr{H}(\{1\}^n)) \geq v(e_n)$ holds for all sufficiently large primes p.

We can now describe a large class of elements in the ideals $\ker(\varphi)$ and $\mathscr{J}_n$.

Theorem 1.3.21. *For $n = 0, 1, 2, \ldots$, let*

$$\alpha_n := e_n + \sum_{k\geq n} (-1)^{k+1} \binom{k}{n} e_k \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}.$$

Then $\alpha_n \in \ker(\varphi)$, and we have

$$\ker(\varphi) \supset \overline{(\alpha_0, \alpha_1, \ldots)}.$$

For all $n \geq 0$, we have

$$\mathscr{J}_n \supset (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n.$$

This is proven as Theorem 5.2.2. The elements α_n come from the asymptotic relations given by Theorem 1.3.4, for $n \geq 0$ and $p \geq 3$:

$$p^n \mathscr{H}_{p-1}(\{1\}^n) + \sum_{j\geq n} (-1)^j \binom{j}{n} p^j \mathscr{H}_{p-1}(\{1\}^j) = 0.$$

Conditionally upon a conjecture of Zhao [41] concerning Bernoulli numbers, the containments of ideals Theorem 1.3.21 are actualy equalities. We state Zhao's conjecture here.

Conjecture 1.3.22 (Nonlinear Bernoulli Nondegeneracy Conjecture)**.** *Let*

$$f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$$

be a homogenous polynomial, where we set $\deg(x_i) = 2i + 1$*. If* f *is non-zero, then there exist infinitely many primes* p *such that* p *does not divide the numerator of*

$$f(B_{p-3}, B_{p-5}, \ldots, B_{p-2n-1}).$$

We show the following:

Theorem 1.3.23. *The Nonlinear Bernoulli Nondegeneracy Conjecture is true if and only if for all* $n \geq 0$*, the second containment is equality:*

$$\mathscr{J}_n = (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n \text{ for all } n \geq 0.$$

These conditions imply that $\ker(\varphi) = \overline{(\alpha_0, \alpha_1, \ldots)}$.

This is proven as Theorem 5.2.4. The generators α_n of $\ker(\varphi)$ come from certain asymptotic relations among the elementary symmetric multiple harmonic sums. The Asymptotic Reflection Theorem 1.3.17 implies a similar family of p-adic identities among the power sum multiple harmonmic sums. Particularly, for n a non-negative integer, setting $\alpha = x^n y$ gives the identity

$$(-1)^n p^{n+1} \mathscr{H}_{p-1}(n+1) + \sum_{k \geq n} \binom{k}{n} p^{k+1} \mathscr{H}_{p-1}(k+1) = 0,$$

which holds for all primes p (these identities were given above as Theorem 1.3.10). To write down the corresponding elements of $\ker(\varphi)$, we make the following definition.

Definition 1.3.24. Let $\mathbf{s} = (s_1, \ldots, s_m)$ be a composition. The elementary symmetric functions generate the ring of symmetric functions, and we define $\theta_{\mathbf{s}}(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$ to be the unique polynomial such that

$$\sum_{(t_1, \ldots, t_k) \sim \mathbf{s}} \left(\sum_{i_1 > \ldots > i_k} x_{i_1}^{t_1} \ldots x_{i_k}^{t_k} \right) = \theta_{\mathbf{s}}(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x})),$$

where $e_n(\mathbf{x})$ is the n-th the elementary symmetric function in $\mathbf{x} = (x_1, x_2, \ldots)$. We set

$$h(\mathbf{s}) = \theta_{\mathbf{s}}(e_1, \ldots, e_n) \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}.$$

Now, Theorem 1.3.17 implies that the elements

$$\beta_n := (-1)^n h(n+1) + \sum_{k \geq n} \binom{k}{n} h(k+1)$$

are in $\ker(\varphi)$ for $n = 0, 1, \ldots$.

The next result of Chapter 5, which is combinatorial in nature, says that the elements $\alpha_n \in \ker(\varphi)$ (and by Theorem 1.3.21, all of $\ker(\varphi)$) can be obtained, in an appropriate sense, from the elements β_n. In particular, this implies that the relations given by the Asymptotic Reflection Theorem 1.3.17 are sufficient to generate the ideal

$$\ker(\varphi) = \ker(\phi) \cap \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}.$$

To make this assertion precise, we give the following definition.

Definition 1.3.25. An ideal $I \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is called *absolutely closed* if I is closed, and for all $r \in \mathbb{Z}_{>0}$ and $\alpha \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, we have $r\alpha \in I \Rightarrow \alpha \in I$. If $I \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is any ideal, we define $\widetilde{I}$ to be the intersection of all absolutely closed ideals containing I, and call $\widetilde{I}$ the *absolute closure* of I. It is an asbolutely closed ideal.

We can now state our result.

Theorem 1.3.26. *For $n = 0, 1, \ldots$, let $\alpha_n, \beta_n \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ be given by*

$$\alpha_n = e_n + \sum_{k \geq n} (-1)^{k+1} \binom{k}{n} e_k,$$

$$\beta_n = (-1)^n h(n+1) + \sum_{k \geq n} \binom{k}{n} h(k+1).$$

Let J_α, $J_\beta \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ be the ideals generated by the α_n and β_n, respectively. Then we have

$$\widetilde{J_\alpha} = \widetilde{J_\beta}.$$

This is proven as Theorem 5.2.7. This Theorem implies that $\alpha_n \in \widetilde{J_\beta}$ for all n, and assuming the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture, that $\ker(\varphi) = \widetilde{J_\beta}$ (as $\ker(\varphi)$ is absolutely closed).

Chapter 2

Elementary Symmetric Sums and Wolstenholme's Theorem

In this chapter, we give a family a congruences for the binomial coefficient $\binom{kp-1}{p-1}$, with k an integer and p a prime. Our congruences involve multiple harmonic sums, and hold modulo arbitrary large powers of p. The general congruence in our family, which depends a parameter n, involves n elementary symmetric multiple harmonic sums, and holds modulo p^{2n+3}. These congruences are actually part of a much larger collection of congruences for $\binom{kp-1}{p-1}$ in terms of the elementary symmetric multiple harmonic sums. Congruences in our family have been optimized, in that they involve the fewest multiple harmonic sums among those congruences holding modulo the same power of p. The coefficients in our congruences are given by polynomials in k.

2.1 Introduction

In 1862 Wolstenhome [37] noted the congruence that for all primes $p \geq 5$,

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

This result is now known as Wolstenholme's theorem. I was later found that the related congruence on harmonic numbers $H_n := \sum_{j=1}^{n} \frac{1}{j}$, stating that for all primes $p \geq 5$,

$$H_{p-1} \equiv 0 \pmod{p^2},$$

which was discovered earlier (by E. Waring [35] in 1782 and again by C. Babbage [2] in 1819), is in fact equivalent to Wolstenholme's result.

In the following 150 years, Wolstenholme's congruence has been generalized in many directions (see Meštrović [23] for a survey). In this chapter we consider generalizations in two directions. The first direction treats a larger set of binomial

coefficients, replacing $2p-1$ with $kp-1$. In 1900 Glaisher [12] showed that for all integers $k \geq 2$,

$$\binom{kp-1}{p-1} \equiv 1 \pmod{p^3}$$

holds for all $p \geq 5$.

The second direction obtains congruences modulo higher powers of p, by adding extra terms to the right hand side of Wolstenholme's congruence. In 2000 van Hamme [34] proved a result implying that for all primes $p \geq 7$,

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{j=1}^{p-1} \frac{1}{j} \pmod{p^5}, \tag{2.1}$$

where $H_n := \sum_{j=1}^{n} \frac{1}{j}$ are the harmonic numbers. Recently Meštrović [22] showed that for any prime $p \geq 11$,

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{j=1}^{p-1} \frac{1}{j} + 4p^2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} \pmod{p^7} \tag{2.2}$$

This congruence involves the additional expression

$$\sum_{1 \leq i < j \leq p-1} \frac{1}{ij},$$

which is an example of a multiple harmonic sum, defined below.

The main result of this chapter is a simultaneous generalization and unification of these results, giving congruences for $\binom{kp-1}{p-1}$ to arbitrary powers of p.

2.1.1 Main result

A *composition* is a finite ordered list $(s_1, \ldots, s_k)$ of positive integers. For ease of notation, we will denote by $\{s_1, \ldots, s_k\}^a$ the composition

$$(\underbrace{s_1, \ldots, s_k}, \underbrace{s_1, \ldots, s_k}, \ldots, \underbrace{s_1, \ldots, s_k})$$

consisting of a concatenated copies of $(s_1, \ldots, s_k)$.

Definition 2.1.1. For $\mathbf{s} = (s_1, \ldots, s_k)$ a composition and n a positive integer, we define the *multiple harmonic sum*

$$H_n(\mathbf{s}) := \sum_{n \geq n_1 > \ldots > n_k \geq 1} \frac{1}{n_1^{s_1} \cdot \ldots \cdot n_k^{s_k}}.$$

By convention, we set $H_n(\mathbf{s}) = 0$ if $k > n$.

It has long been known (see e.g. [21]) that the binomial coefficient $\binom{kp-1}{p-1}$ (for k an integer) can be written as a linear combination of 'elementary symmetric' multiple harmonic sums $H_{p-1}(\{1\}^j)$:

$$\binom{kp-1}{p-1} = \sum_{j=0}^{p-1} (k-1)^j p^j H_{p-1}(\{1\}^j).$$

For a fixed non-negative integer n, we may truncate this equation after the $2n$-th term and use known results on the p-adic valuation of the multiple harmonic sums $H_{p-1}(\{1\}^j)$ to obtain the congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{2n} (k-1)^j p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}} \tag{2.3}$$

which holds for all primes $p \geq 2n+5$.

In Section 2 we derive a family of identities involving the multiple harmonic sums $H_{p-1}(\{1\}^j)$. We use these identities to cancel terms appearing in (2.3). Our main result, like equation (2.3), gives for each non-negative integer n a congruence for the binomial coefficient $\binom{kp-1}{p-1}$ mod p^{2n+3}, involving multiple harmonic sums. However, our congruence uses only n elementary symmetric multiple harmonic sums, instead of the $2n$ used in equation (2.3).

The coefficients in our congruences are polynomials in k. We make the following definition.

Definition 2.1.2. Let $0 \leq j \leq n$ be integers. The *extremal polynomial* $b_{j,n}(T) \in \mathbb{Q}[T]$ is the unique polynomial of degree at most $2n+1$ satisfying:

(C1) $b_{j,n}(T) \equiv (T-1)^j \mod (T-1)^{n+1}$

(C2) $b_{j,n}(T) \equiv (-1)^j T^j \mod T^{n+1}$

A table of the extremal polynomials $b_{j,n}(T)$ for $0 \leq j \leq n \leq 3$ can be found in Section 2.1.2. Now we can state our main result:

Theorem 2.1.3. (Optimized Congruences) *Let $n \geq 0$ be a fixed integer. The extremal polynomials $b_{j,n}(T)$ $(0 \leq j \leq n)$ have integer coefficients, and for every prime*

$p \geq 2n+5$ and every integer $k \geq 1$:

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k)\, p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}. \tag{2.4}$$

This congruence holds mod p^{2n+2} for $p = 2n+3$, and is equality for $3 \leq p \leq 2n+5$.

Wolstenholme's congruence is the case $n = 0, k = 2$ of Theorem 2.1.3. As another example, taking $n = k = 3$ gives the congruence

$$\binom{3p-1}{p-1} \equiv 1 + 402pH_{p-1}(1) - 396p^2 H_{p-1}(1,1) + 216p^3 H_{p-1}(1,1,1) \mod p^9.$$

Theorem 2.1.3 has four important features:

1. The coefficients $b_{j,n}(k)$ in the congruence (2.4) are independent of the prime p.
2. There are a large number of congruences for $\binom{kp-1}{p-1}$ holding mod p^{2n+3}, which involve the multiple harmonic sums $H_{p-1}(\{1\}^j)$ for $1 \leq j \leq 2n$ (see Theorem 2.3.3). The congruences (2.4) are optimized among these in only containing the terms $H_{p-1}(\{1\}^j)$ for $1 \leq j \leq n$.
3. The congruences may fail to hold (mod p^{2n+3}) for $p = 2n+3$ (when $2n+3$ is prime), and also fail to hold for $p = 2$.
4. The extremal polynomials $b_{j,n}(T)$ depend on n, and for fixed j their values at integers $b_{j,n}(k)$, which are the coefficients in the congruences, do *not* stabilize as $n \to \infty$ (with the exception of $b_{0,n}(k)$; see the tables in Section 2.1.2).

One may ask whether the coefficients $b_{j,n}(k)$ appearing in the extremal congruences (2.4) are uniquely characterized by (2.4) holding for all sufficiently large primes p; we discuss this in Section 2.1.3, where we show that an affirmative answer would follow from the conjecture that there exist infinitely many regular primes.

An *exceptional congruence* will be a triple (k, n, p) such that the corresponding congruence given in Theorem 2.1.3 holds modulo an extra power of p. We characterize exceptional congruences for primes $p \geq 2n+3$ as follows.

Theorem 2.1.4. (Exceptional Congruences) *Let n be a non-negative integer, $p \geq 2n+5$ a prime. For all $k \in \mathbb{Z}$, the exceptional congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+4}}$$

holds if and only if either $k \equiv 0, 1 \pmod{p}$ *or* p *divides the numerator of the Bernoulli number* B_{p-2n-3}.

We obtain Theorem 2.1.3 as a special case of a much more general family $\mathcal{F}_{N,k}$ of generalized Wolstenholme congruences, given in Theorem 2.3.3, and with the $\mathcal{F}_{N,k}$ specified in Definition 2.3.4. The general congruence in the family $\mathcal{F}_{N,k}$ (which will hold for all sufficiently large primes p) is of the form

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{N} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{N+1+\epsilon}}$$

where $\epsilon \in \{1, 2\}$ is chosen so that $\epsilon \equiv N \pmod 2$, and the coefficients b_j are rational numbers. Each congruence in this general family is derived from (2.3), using linear combinations of identities among multiple harmonic sums (these identities are stated as Theorem 2.2.2). The optimized congruence (2.4) is distinguished as the unique congruence in the family $\mathcal{F}_{2n,k}$ satisfying $b_{n+1} = b_{n+2} = \ldots = b_{2n} = 0$.

2.1.2 The extremal polynomials $b_{j,n}(T)$

In Section 2.6 we prove some interesting properties of the extremal polynomials $b_{j,n}(T)$. Below we present data on these polynomials for small j, n.

Table 2.1: Extremal polynomials $b_{j,n}(T)$

$n\backslash j$	0	1	2	3
0	1			
1	1	$T^2 - T$		
2	1	$-T^4 + 2T^3 - T$	$T^4 - 2T^3 + T^2$	
3	1	$2T^6 - 6T^5 + 5T^4 - T + 1$	$-2T^6 + 6T^5 - 5T^4 + T^2$	$T^6 - 3T^5 + 3T^4 - T^3$

This table illustrates that $b_{0,n}(T) = 1$ for all n (this will be established in Section 2.6). While the definition of $b_{j,n}(T)$ given earlier shows that it has degree at most $2n + 1$, in fact its degree is at most $2n$ (see Theorem 2.4.6).

We next consider the coefficients $b_{j,n}(k)$ appearing in the extremal congruences given in Theorem 2.1.3. Values of the coefficients for $k = 2$ are given in the table below.

Table 2.2: Extremal coefficients $b_{j,n}(k)$ for $k = 2$

$n\backslash j$	0	1	2	3	4	5
0	1					
1	1	2				
2	1	-2	4			
3	1	14	-12	8		
4	1	-66	68	-40	16	
5	1	382	-380	248	-112	32

This table shows that $b_{1,2}(2) = -2$, $b_{2,2}(2) = 4$, so that Theorem 2.1.3 reduces to Meštrović's result (2.2) in the case $n = k = 2$.

2.1.3 Uniqueness issues

The statement of Theorem 2.1.3 raises an issue concerning whether the coefficients $b_{j,n}(k)$ above are uniquely determined by the condition that the congruences (2.4) hold for all sufficiently large primes p. We cannot prove this unconditionally. However, we will show that it would follow from a conjecture concerning Bernoulli numbers, which we state here:

Conjecture 2.1.5 (Linear Bernoulli Nondegeneracy Conjecture)**.** *For all odd integers $k \geq 3$, there exist infinitely many primes p for which p does not divide the numerator of the Bernoulli number B_{p-k}.*

Recall that a prime p is called *regular* if p does not divide the numerators of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. It is believed that there are infinitely many regular primes; this would imply Conjecture 2.1.5. A stronger version of this conjecture was given by Zhao [41].

Theorem 2.1.6 (Uniqueness of Optimized Congruences)**.** *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. Let n, k be integers with $n \geq 0$, and suppose $b_0, \ldots, b_n \in \mathbb{Q}$ are such that the congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}$$

holds for all sufficiently large primes p. Then we have $b_j = b_{j,n}(k)$, where $b_{j,n}(T)$ are the extremal polynomials given by Definition 2.1.2.

2.1.4 Related results

The literature contains a vast collection of identities and congruences involving multiple harmonic sums and related sums, starting with work of Euler on harmonic numbers. Some of these involve binomial coefficient congruences (see Granville [13] for a survey).

A number of congruences are known for the elementary symmetric multiple harmonic sums $H_n(\{1\}^r)$ considered in this chapter. In 1900 Glaisher [11] proved that for all odd $r \geq 5$ and all primes $p \geq 7$,

$$S_r(p) := \frac{pr}{2} H_{p-1}(\{1\}^r) - H_{p-1}(\{1\}^{r-1}) \equiv 0 \pmod{p^4}.$$

In 1953 Carlitz [7] sharpened the congruence of Glaisher to show for all odd $r \geq 5$ and prime $p \geq 7$,

$$S_r(p) \equiv p^4 \frac{(p-r)(p-r-1)(p-r-2)}{24(p-r-3)(p-1)!} B_{p-3} \pmod{p^5},$$

giving a relation with Bernoulli numbers. Along similar lines, Tauraso [31] shows that for any prime $p \geq 7$,

$$\begin{aligned} H_{p-1}(1) &\equiv -\frac{1}{2} p H_{p-1}(1,1) - \frac{1}{6} p^2 H_{p-1}(1,1,1) \\ &\equiv p^2 \left(\frac{B_{2p-5}}{3p-5} - 3\frac{B_{2p-4}}{2p-4} + 3\frac{B_{p-3}}{p-3} \right) + p^4 \frac{B_{p-5}}{p-5} \pmod{p^5}. \end{aligned}$$

Hoffman [16] and Zhao [40] independently investigated congruence properties of multiple harmonic sums mod p (and sometimes mod p^2). The theory of multiple harmonic sums (and particular, their values mod p) is analogous to the study of multiple zeta values. Relations among multiple zeta values have been studied extensively. A very general method for generating relations is given by Ihara, Kaneko, and Zagier [17].

The appearance of Bernoulli numbers is congruences suggest a connection with p-adic zeta functions. Indeed, Morita [24, 25] demonstrated a relations between the power sum multiple harmonic sums $H_{p-1}(n)$ and the Kubota-Leopoldt p-adic L-function. More recent result along these lines are given by Washington [36]. In Chapter 3, we provide a family of congruences for $\zeta_p(k)$ in terms of the multiple

harmonic sums $H_{p-1}(n)$. These congruences exploit relations among the power sum multiple harmonic sums, and are similar the the congruences in this chapter. In Chapter 5, we investigate the structure underlying these relations.

2.2 Representing binomial coefficients in terms of multiple harmonic sums

Let n be a positive integer, and define a polynomial

$$f_n(T) = \sum_{j=0}^{n} (n+1)^j H_n(\{1\}^j) T^j \in \mathbb{Q}[T]. \tag{2.5}$$

The coefficients of $f_n(T)$ are the elementary symmetric functions in $\frac{n+1}{1}, \frac{n+1}{2}, \ldots, \frac{n+1}{n}$, so there is a factorization

$$f_n(T) = \prod_{j=1}^{n} \left(1 + \frac{n+1}{j} T\right) = \frac{1}{n!} \prod_{j=1}^{n} \Big((n+1)T + j\Big). \tag{2.6}$$

This factorization shows that f_n satisfies the functional equation $f_n(-1-T) = (-1)^n f_n(T)$. This gives the equality

$$\begin{aligned}
\sum_{j\geq 0} (n+1)^j H_n(\{1\}^j) T^j &= (-1)^n \sum_{j\geq 0} (n+1)^j H_n(\{1\}^j)(-1-T)^j \\
&= \sum_{j\geq 0} (-1)^{n+j} (n+1)^j H_n(\{1\}^j) \sum_{0\leq i\leq j} \binom{j}{i} T^i \\
&= \sum_{i\geq 0} \left(\sum_{j\geq i} \binom{j}{i} (-1)^{n+j} (n+1)^j H_n(\{1\}^j) \right) T^i,
\end{aligned}$$

holding identically in T. Equating the coefficient of T^j on each side and rearranging gives the following identity.

Proposition 2.2.1. *For all non-negative integers n, j, we have*

$$(n+1)^j H_n(\{1\}^j) + \sum_{i\geq j} (-1)^{n+i+1} \binom{i}{j} (n+1)^i H_n(\{1\}^i) = 0. \tag{2.7}$$

The sum above is finite, as the terms corresponding to $i > n$ vanish. We thus have a family of linear equations (indexed by j) satisfied by the quantities $(n+1)^i H_n(\{1\}^i)$, $i = 0, 1, \ldots, n$.

Next we obtain a general set of identities expressing binomial coefficients in terms of the $H_n(\{1\}^j)$.

Proposition 2.2.2. *Let n be a non-negative integer, k, $c_0, c_1, \ldots$ indeterminates, and define*

$$b_j = (k-1)^j + c_j + (-1)^{n+j+1} \sum_{i=0}^{j} \binom{j}{i} c_i.$$

Then the equation

$$\binom{k(n+1)-1}{n} = \sum_{j=0}^{\infty} b_j (n+1)^j H_n(\{1\}^j), \tag{2.8}$$

holds identically in the indeterminates k, $c_0, c_1, \ldots$. Here the right side of (2.8) is a finite sum, since $H_n(\{1\}^j) = 0$ for $j > n$.

Proof. We begin by using equations (2.5) and (2.6) to write

$$\begin{aligned} \binom{k(n+1)-1}{n} &= f_n(k-1) \\ &= \sum_{j \geq 0} (k-1)^j (n+1)^j H_n(\{1\}^j). \end{aligned}$$

We add to this equation a linear combination of equations (2.7) (where c_j is the coefficient of the equation indexed by j) to obtain the general formula. □

Remark 2.2.3. By making suitable choices of the parameters c_i in Proposition 2.2.2, we can arrange to have $b_j = 0$ for many j. Theorem 2.4.1 is obtained by optimizing this process.

2.3 Congruences for $\binom{kp-1}{p-1}$ modulo powers of p

To obtain congruences for $\binom{kp-1}{p-1}$, we will truncate the expansion of Proposition 2.2.2, with k an integer and $n = p-1$, p an odd prime. To establish a bound on the error due to truncation, we need some congruence properties of multiple harmonic sums.

2.3.1 Congruence properties of multiple harmonic sums

Zhao ([40], Theorem 1.6) gives the following congruence involving multiple harmonic sums $H_{p-1}(\{1\}^j)$ and Bernoulli numbers:

Proposition 2.3.1. *Let p be a fixed odd prime, and j an integer with $1 \leq j \leq p-3$. Then we have*

$$H_{p-1}(\{1\}^j) \equiv \begin{cases} \frac{-B_{p-1-j}}{j+1} p \pmod{p^2} & \text{if } j \equiv 0 \mod 2 \\ \left(\frac{-(j+1)}{2(j+2)} B_{p-2-j}\right) p^2 \pmod{p^3} & \text{if } j \equiv 1 \mod 2 \end{cases}$$

We prove an additional congruence for $H_{p-1}(\{1\}^j))$ for those j which are not covered by Proposition 2.3.1:

Proposition 2.3.2. *Let p be a fixed odd prime, and j a positive integer.*

(i) If $j = p-2$ we have $H_{p-1}(\{1\}^j) \equiv \frac{1}{2}p \pmod{p^2}$.

(ii) If $j = p-1$ we have $H_{p-1}(\{1\}^j)) \equiv -1 \pmod{p}$.

(iii) If $j \geq p$ we have $H_{p-1}(\{1\}^j) = 0$.

Proof. (i) We have

$$\begin{aligned} H_{p-1}(\{1\}^{p-2}) &= \sum_{i=1}^{p-1} \frac{1}{1 \cdots \hat{i} \cdots (p-1)} \\ &= \frac{1}{(p-1)!} \sum_{i=1}^{p-1} i \\ &= \frac{1}{(p-1)!} \frac{p(p-1)}{2} \\ &\equiv \frac{p}{2} \pmod{p^2}. \end{aligned}$$

In the last line, we used Wilson's theorem, stating that $(p-1)! \equiv -1 \pmod{p}$.

(ii) We have

$$\begin{aligned} H_{p-1}(\{1\}^{p-1}) &= \frac{1}{(p-1)!} \\ &\equiv -1 \pmod{p} \end{aligned}$$

(iii) For $j \geq p$ the defining sum is empty.

□

2.3.2 A general family of congruences

We can now obtain our general family of congruences for $\binom{kp-1}{p-1}$. The congruences are obtained from Proposition 2.2.2 by truncation. We take some care to express the error due to truncation in terms of Bernoulli numbers.

Theorem 2.3.3 (General Wolstenholme-like Congruence)**.** *Let k be an integer. Let $c_0, c_1, \ldots \in \mathbb{Q}$ be given, and take $b_j \in \mathbb{Q}$ to be*

$$b_j := (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i. \tag{2.9}$$

Fix an odd prime p not dividing the denominator of any c_i, and let N be a non-negative integer. Define

$$E_N := \binom{kp-1}{p-1} - \sum_{j=0}^{N} b_j p^j H_{p-1}(\{1\}^j).$$

(i) *If $0 \le N \le p-4$, then*

$$E_N \equiv \begin{cases} \frac{-B_{p-3-N}}{N+3} \left(\frac{N+2}{2} b_{N+1} + b_{N+2}\right) p^{N+3} & \pmod{p^{N+4}} \text{ if } N \text{ is even} \\ \frac{-B_{p-2-N}}{N+2} b_{N+1}\, p^{N+2} & \pmod{p^{N+3}} \text{ if } N \text{ is odd} \end{cases}.$$

(ii) *If $N = p-3$, then $E_N \equiv \left(\frac{b_{N+1}}{2} - b_{N+2}\right) p^{N+2} \pmod{p^{N+3}}$.*

(iii) *If $N = p-2$, then $E_N \equiv -b_{N+1} p^{N+1} \pmod{p^{N+2}}$.*

(iv) *If $N \ge p-1$, then $E_N = 0$.*

In particular, we get the congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{N} b_j p^j H_{p-1}(\{1\}^j) \begin{cases} \bmod p^{N+3} \text{ if } N \le p-4,\ N \text{ even} \\ \bmod p^{N+2} \text{ if } N \le p-4,\ N \text{ odd} \\ \bmod p^{N+2} \text{ if } N = p-3 \\ \bmod p^{N+1} \text{ if } N = p-2 \\ \bmod 0 \text{ if } N \ge p-1 \end{cases} \tag{2.10}$$

(Congruence mod 0 means equality)

Proof. We apply Proposition 2.2.2 with $n = p-1$ to obtain the equality

$$\binom{kp-1}{p-1} = \sum_{j=0}^{\infty} b_j p^j H_{p-1}(\{1\}^j).$$

Because $n = p-1$ is even, the values of b_i do not depend on p. The b_j are p-integral (because we assume the c_j to be p-integral), as are the multiple harmonic sums $H_{p-1}(\{1\}^j)$, so we have

$$E_N \equiv \sum_{j=N+1}^{N+3} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{N+4}}.$$

Case (i-a): Suppose $0 \leq N \leq p-5$ and N is even. Propositions 2.3.1 and 2.3.2 imply $H_{p-1}(\{1\}^{N+1}) \equiv \frac{-(N+2)}{2(N+3)} B_{p-3-N} p^2 \pmod{p^3}$, $H_{p-1}(\{1\}^{N+2}) \equiv \frac{-1}{N+3} B_{p-N-3} p \pmod{p}$, and $H_{p-1}(\{1\}^{N+3}) \equiv 0 \pmod{p}$. This implies

$$E_N \equiv \frac{-B_{p-3-N}}{N+3} \left(\frac{N+2}{2} b_{N+1} + b_{N+2} \right) p^{N+3} \pmod{p^{N+4}}.$$

Case (i-b): Suppose $1 \leq N \leq p-4$ and N is odd. Proposition 2.3.1 implies $H_{p-1}(\{1\}^{N+1}) \equiv \frac{-1}{N+2} B_{p-2-N} p \pmod{p^2}$ and $H_{p-1}(\{1\}^{N+2}) \equiv 0 \pmod{p}$. This implies

$$E_N \equiv \frac{-B_{p-2-N}}{N+2} b_{N+1} p^{N+2} \pmod{p^{N+3}}.$$

Case (ii): Suppose $N = p-3$. Proposition 2.3.2 implies $H_{p-1}(\{1\}^{p-2}) \equiv \frac{p}{2} \pmod{p^2}$, $H_{p-1}(\{1\}^{p-1}) \equiv -1 \pmod{p}$, so

$$E_N \equiv \left(\frac{b_{N+1}}{2} - b_{N+2} \right) p^{N+2} \pmod{p^{N+3}}.$$

Case (iii): Suppose $N = p-2$. Proposition 2.3.2 implies $H_{p-1}(\{1\}^{p-1}) \equiv -1 \pmod{p}$, so

$$E_N \equiv -b_{N+1} p^{N+1} \pmod{p^{N+2}}.$$

Case (iv): Suppose $N \geq p-1$. Then E_N is given by an empty sum, so $E_N = 0$.

□

Definition 2.3.4. We call the congruence (2.10) the *generalized Wolstenholme congruence* associated with the data

$$[k, (c_0, c_1, \ldots), N],$$

and we will say that $b_0, \ldots, b_N$ are the *generalized Wolstenholme coefficients* associated with this data. We let $\mathcal{F}_{N,k}$ denote the family of all generalized Wolstenholme congruences above, where N, k are fixed and the other data varies.

Assuming the truth of the Linear Bernoulli Nondegeneracy Conjecture 2.1.5, we can show that our family contains *all* congruences of this form.

Theorem 2.3.5 (Strong Uniqueness)**.** *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture 2.1.5. If k, m are integers with $m \geq 0$, and $a_0, \ldots, a_n \in \mathbb{Q}$ are such that*

$$\binom{kp-1}{p-1} \equiv a_0 + a_1 pH(\{1\}^1) + \ldots + a_n p^n H(\{1\}^n) \pmod{p^m}$$

holds for all but finitely many p, then this congruence arises from Theorem 2.3.3, in the following sense: there are constants $c_0, c_1, \ldots \in \mathbb{Q}$ such that, if $b_0, b_1, \ldots$ are defined by (2.9), then we have $a_i = b_i$ for $i = 0, 1, \ldots, \psi(m)$, where $\psi(m) = m-2$ if m is even and $\psi(m) = m-3$ if m is odd.

Proof. Suppose, to the contrary, that there is a congruence of the form

$$\binom{kp-1}{p-1} \equiv a_0 + a_1 pH(\{1\}^1) + \ldots + a_n p^n H(\{1\}^n) \pmod{p^m},$$

holding for sufficiently large p, which does not arise from Theorem 2.3.3. Subracting the identity

$$\binom{kp-1}{p-1} = \sum_{j \geq 0} (k-1)^j p^j H_{p-1}(\{1\}^j)$$

from this congruence gives us a congruence of the form

$$\sum_{j \geq 0} c_j p^j H_{p-1}(\{1\}^j) \equiv 0 \pmod{p^m}, \tag{2.11}$$

which by hypothesis does not arise from truncating a linear combination of the identities (2.7). We may choose (2.11) so that $j_0 := \min\{j : c_j \neq 0\}$ is maximized among all congruences of this shape not arising from a truncation of a linear combinations of the identities (2.7). This implies that j_0 is even, for if j_0 were odd, we could add $\frac{-1}{2} c_j$ times the identity (2.7) with $j = j_0$, cancelling the lowest order term and

contradicting the maximality of j_0. By hypothesis, we also have $m \geq j_0 + 2$, so by reducing (2.11) mod p^{j_0+2}, we get

$$c_{j_0} p^{j_0} H_{p-1}(\{1\}^{j_0}) \equiv 0 \pmod{p^{j_0+2}}$$

for all sufficiently large primes p. Using Proposition 2.3.1, we get

$$\frac{c_{j_0}}{j_0+1} p^{j_0+1} B_{p-1-j_0} \equiv 0 \pmod{p^{j_0+2}}$$

for all sufficiently large p. Since $c_{j_0} \neq 0$, this contradicts the Linear Bernoulli Non-degeneracy Conjecture. □

Remark 2.3.6. For fixed k, N, the family $\mathcal{F}_{N,k}$ has the structure of an affine linear space over $\mathbb{Q}$ in the following way: if $B = (b_0, \ldots, b_N)$ and $B' = (b'_0, \ldots, b'_N)$ are the coefficients associated with the data $[k, (c_0, c_1, \ldots), N]$, $[k, (c'_0, c'_1, \ldots), N]$ respectively, and $t \in \mathbb{Q}$, then

$$tB + (1-t)B' = (tb_0 + (1-t)b'_0,\ \ldots,\ tb_N + (1-t)b'_N),$$

where the numbers on right hand side are the generalized Wolstenholme coefficients associated with the data

$$[k, (tc_0 + (1-t)c'_0,\ tc_1 + (1-t)c'_1,\ \ldots), N].$$

In the next section we will focus exclusively on the case where $N = 2n$ is even. We will determine that the affine space of generalized Wolstenholme coefficients, for arbitrary k and $N = 2n$, has dimension n.

Now we consider some special cases of Theorem 2.3.3. In what follows we will write $(c_0, \ldots, c_m)$ for the sequence $(c_0, \ldots, c_m, 0, 0, \ldots)$.

As one example, fix a positive integer k and take the data $[k, ((k-1)^2), 2]$. This gives $(b_0, b_1, b_2, b_3, b_4) = (1, k(k-1), 0)$, so we get the congruence

Corollary 2.3.7. *For all integers k and all primes $p \neq 2, 5$, we have*

$$\binom{kp-1}{p-1} \equiv 1 + k(k-1)pH_{p-1}(1) \pmod{p^5}$$

This is a generalization of van Hamme's result (2.1).

Taking the data $[2, (49, -18, 4), 6]$ gives
$(b_0, b_1, \ldots, b_6) = (1, 14, -12, 8, 0, 0, 0)$, so we get the identity

Corollary 2.3.8. *For all odd primes p, we have*

$$\binom{2p-1}{p-1} \equiv 1 + 14pH_{p-1}(1) - 12p^2 H_{p-1}(1,1) + 8p^3 H_{p-1}(1,1,1) \pmod{p^9}$$

Corollaries 2.3.7 and 2.3.8 are special cases of Theorem 2.3.3.

2.4 Optimized binomial congruences

We now state a version of our main result (Theorem 2.1.3). We show that when $N = 2n$ is even, it is always possible to choose the data $(c_0, c_1, \ldots)$ so that $b_{n+1} = b_{n+2} = \ldots = b_{2n} = 0$. Moreover, this condition will uniquely determine the values of b_j for $0 \le j \le n$. We will derive this result using Theorem 2.3.3.

Theorem 2.4.1 (Optimized Binomial Congruences)**.** *Let integers k, n be given, with $n \ge 0$, and set $N = 2n$. There is a unique generalized binomial congruence whose coefficients $b_0, \ldots, b_{2n}$ satisfy $b_{n+1} = b_{n+2} = \ldots = b_{2n} = 0$. This congruence has $b_0, b_1, \ldots, b_n \in \mathbb{Z}$.*

In other words, for $N = 2n$, Theorem 2.3.3 produces a unique congruence of the form

$$\binom{kp-1}{p-1} \equiv b_0 + b_1 pH(1) + \ldots + b_n p^n H(\{1\}^n) \pmod{p^{2n+3}}. \tag{2.12}$$

with $b_i \in \mathbb{Z}$, which holds for all odd primes $p \neq 2n+3$. This congruence holds mod p^{2n+2} when $p = 2n+3$, and is equality for $3 \le p \le 2n+1$.

Before giving the proof, we remark that this theorem, combined with Theorem 2.3.5, implies the uniqueness statement Theorem 2.1.6.

For the proof of Theorem 2.4.1, we need some preliminaries.

Definition 2.4.2. Fix integers N, k, with $N \ge 0$. Define $V_{N,k} \subset \mathbb{Z}^{N+1}$ to be the set

$$V_{N,k} := \left\{ (b_0, \ldots, b_N) : \exists c_0, c_1, \ldots \in \mathbb{Z} \text{ s.t. } b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \right\}.$$

In other words $V_{N,k}$ is the set of *generalized Wolstenholme coefficients* corresponding to integer data. We similarly define $V_{N,k}^{\mathbb{Q}} \subset \mathbb{Q}^{N+1}$ to be

$$V_{N,K}^{\mathbb{Q}} := \left\{ (b_0, \ldots, b_N) : \exists c_0, c_1, \ldots \in \mathbb{Q} \text{ s.t. } b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \right\},$$

the set of generalized Wolstenholme coefficients corresponding to rational data.

The inclusion $V_{N,k} \hookrightarrow V_{N,k}^{\mathbb{Q}}$ induces an isomorphism

$$V_{N,k} \otimes \mathbb{Q} \cong V_{N,k}^{\mathbb{Q}}$$

of affine spaces over $\mathbb{Q}$. We have that $V_{N,k}$ is a coset of the subgroup

$$\hat{V}_N := \left\{ (b_0, \ldots, b_N) : \exists c_0, c_1, \ldots \in \mathbb{Z} \text{ s.t. } b_j = c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \right\} \subseteq \mathbb{Z}^N,$$

which does not depend on k. We then have the following:

Proposition 2.4.3. *For all integers N, k, with $N \geq 0$, we have $V_{N,k} = V_{N,1-k}$.*

Proof. As $V_{N,k}$ and $V_{N,1-k}$ are cosets of the same subgroup $\hat{V}_N \leq \mathbb{Z}^{N+1}$, equality will follow if we can show $V_{N,k} \cap V_{N,1-k} \neq \phi$.

Taking $c_0 = c_1 = \ldots = 0$, we see $(1, (-k), (-k)^2, \ldots, (-k)^N) \in V_{N,1-k}$. To see that this element is also in $V_{N,k}$, set $c_j = -(k-1)^j$. Then

$$\begin{aligned} b_j &= (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \\ &= (k-1)^j - (k-1)^j + (-1)^j \sum_{i=0}^{j} \binom{j}{i} (k-1)^i \\ &= (-k)^j. \end{aligned}$$

□

Lemma 2.4.4. *For positive integers b, n, $n \times n$ matrix*

$$M_{n,b} := \left(\binom{b+i}{j} \right)_{0 \leq i,j < n}$$

has determinant 1.

Proof. Define $n \times n$ matrices $L_n = (\binom{i}{j})$, $U_{n,b} = (\binom{b}{j-i})$. L_n is unipotent lower-triangular and $U_{n,b}$ is unipotent upper-triangular, so both have determinant 1. It follows from the Vandermonde convolution identity that $M_{n,b} = L_n U_{n,b}$, so that $\det M_{n,b} = (\det L_n)(\det U_{n,b}) = 1$. □

Lemma 2.4.5. *For all non-negative integers n, $\hat{V}_{2n}$ is a free $\mathbb{Z}$-module of rank n, and the map $\pi : \hat{V}_{2n} \to \mathbb{Z}^n$, $(b_0, \ldots, b_{2n}) \mapsto (b_{n+1}, \ldots, b_{2n})$ is an isomorphism*

Proof. Here $(b_0, \ldots, b_{2n}) \in \hat{V}_{2n}$ is determined by the values of c_j for $0 \leq j \leq 2n$. We therefore have a surjective map $\varphi_n : \mathbb{Z}^{2n+1} \to \hat{V}_{2n} \leq \mathbb{Z}^{2n+1}$, taking $(c_0, \ldots, c_{2n})$ to $(a_0, \ldots, a_{2n})$ with

$$a_j = c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i.$$

With respect to the standard basis on $\mathbb{Z}^{2n+1}$, φ_n is given by the matrix

$$A_n := \left(\delta_{i,j} + (-1)^{j+1} \binom{j}{i} \right)_{0 \leq i,j \leq 2n}.$$

Let us identify column vectors of length $2n+1$ with the set of polynomials of degree at most $2n$ via the identification $(a_0, \ldots, a_{2n}) \leftrightarrow a_0 + a_1 T + \ldots + a_{2n} T^{2n}$. The j-th column of A_n is identified with the polynomial $T^j - (-1 - T)^j$. This means that the column span of A_n is contained in the set of polynomials $f(T)$ satisfying $f(T) = -f(-1 - T)$. Such polynomials can be written as $\mathbb{Q}$-linear combinations of $T + \frac{1}{2}, (T + \frac{1}{2})^3, \ldots, (T + \frac{1}{2})^{2n-1}$. It follows that $\operatorname{rank}(\hat{V}_{2n}) = \operatorname{rank}(A_n) \leq n$.

Next let $i : \mathbb{Z}^n \to \mathbb{Z}^{2n+1}$, $(x_0, \ldots, x_{n-1}) \mapsto (x_0, \ldots, x_{n-1}, 0, \ldots, 0)$. We have $\pi \circ \varphi_n \circ i(x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1})$, where

$$y_j = (-1)^{n+j} \sum_{i=0}^{n-1} \binom{n+1+j}{i} x_i.$$

Lemma 2.4.4 implies this map is bijective. It follows that π is surjective. Since $\operatorname{rank}(\hat{V}_{2n}) \leq n = \operatorname{rank}(\mathbb{Z}^n)$, we must have that $\operatorname{rank}(\hat{V}_{2n}) = n$, and π is bijective. □

Proof of Theorem 2.4.1. We need to show that there is a unique element of the form $(b_0, \ldots, b_n, 0, \ldots, 0)$ in $V_{2n,k}^{\mathbb{Q}}$, and that $b_0, \ldots, b_n \in \mathbb{Z}$. It suffices to show there is a unique element of this form in $V_{2n,k}$. Because $V_{2n,k} = (1, (k-1), \ldots, (k-1)^{2n}) + \hat{V}_{2n}$,

this is equivalent to the existence of a unique element

$$\underline{a} = (a_0, \ldots, a_n, -(k-1)^{n+1}, \ldots, -(k-1)^{2n})$$

in $\hat{V}_{2n}$. This follows from Lemma 2.4.5, which implies there is a unique $\underline{a} \in \hat{V}_{2n}$ with $\pi(\underline{a}) = (-(k-1)^{n+1}, \ldots, -(k-1)^{2n})$.

That the values $b_{j,n}(k)$ agree with a polynomial in k will follow from Theorem 2.4.6 below. □

We summarize the recipe for constructing the coefficients $b_{j,n}(k)$ given in Theorem 2.4.1. It will follow that these coefficients are interpolated by a polynomial $b_{j,n}(T)$.

Theorem 2.4.6. *The coefficients $b_{j,n}(k)$ given in Theorem 2.4.1 are values of a polynomial $b_{j,n}(T)$ at $T = k$, having integer coefficients and degree at most $2n$. This polynomial can be computed explicitly as follows.*
Let M_n be the $n \times n$ matrix

$$M_n = \left[(-1)^{n+i} \binom{n+1+i}{j} \right]_{0 \le i,j \le n-1}.$$

Let D_n be the $(n+1) \times n$ matrix

$$D_n = \left[(-1)^{i+1} \binom{i}{j} + \delta_{i,j} \right]_{\substack{0 \le i \le n \\ 0 \le j \le n-1}}$$

where $\delta_{i,j}$ is the Kronecker delta. Then M_n is invertible over the integers, and we have the matrix equation

$$\begin{pmatrix} b_{0,n}(k) \\ b_{1,n}(k) \\ \vdots \\ b_{n,n}(k) \end{pmatrix} = \begin{pmatrix} (k-1)^0 \\ (k-1)^1 \\ \vdots \\ (k-1)^n \end{pmatrix} - D_n \cdot M_n^{-1} \cdot \begin{pmatrix} (k-1)^{n+1} \\ (k-1)^{n+2} \\ \vdots \\ (k-1)^{2n} \end{pmatrix}$$

Definition 2.4.7. For integers j, n, k, with $j, n \ge 0$, we let $b_{j,n}(k)$ denote the coefficients arising from Theorem 2.4.1. We call these *extremal coefficients*. We also denote by $b_{j,n}(T)$ the polynomial giving these coefficients, and call these *extremal polynomials*. By convention, we take $b_{j,n}(T) = 0$ for $n+1 \le j \le 2n$, and we say that $b_{j,n}(T)$ is not defined for $j \ge 2n+1$.

Proposition 2.4.3 says that $V_{2n,k} = V_{2n,1-k}$, so we observe that $b_{j,n}(k) = b_{j,n}(1-k)$. Combined with Theorem 2.4.6, this observation gives the following characterization of the extremal polynomials $b_{j,n}(T)$:

Proposition 2.4.8. *Fix integers j, n, with $j \leq 2n$. The extremal polynomial $b_{j,n}(T) \in \mathbb{Z}[T]$ is the unique polynomial of degree at most $2n$ satisfying the following conditions:*

(i) $b_{j,n}(T) \equiv (T-1)^j \mod (T-1)^{n+1}$,

(ii) $b_{j,n}(T) \equiv (-T)^j \mod T^{n+1}$.

Theorem 2.1.3, stated in the introduction, now follows from the combination of Theorem 2.4.1, Theorem 2.4.6, and Proposition 2.4.8.

2.5 Exceptional congruences and Bernoulli numbers

We now investigate the situations under which our congruences hold modulo some larger power of p than given by Theorem 2.4.1. We term these *exceptional congruences*. In the case of Wolstenholme's theorem, the exceptional congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$$

holds if and only if p divides the numerator of the Bernoulli number B_{p-3}; this follows from results of van Hamme [34] and Glaisher [11]. We establish a similar result, which shows that the congruence (2.12) hold modulo an extra power of p if and only if either $p|B_{p-2n-3}$, or $p|k(k-1)$.

Fix non-negative integers n, k, and let $c_0, c_1, \ldots \in \mathbb{Z}$ be chosen so that the generalized Wolstenholme congruence associated with the data $[k, (c_0, c_1, \ldots), 2n]$ is the optimal one, given by Theorem 2.4.1. The c_i are not uniquely determined by this condition. Let $b_0, b_1, \ldots, b_{2n+2}$ be given by (2.9), so that $b_j = b_{j,n}(k)$ for $j = 0, 1, \ldots, n$, and $b_j = 0$ for $j = n+1, n+2, \ldots, 2n$. The values of b_{2n+1} and b_{2n+2} will depend on the choice of the c_i.

Lemma 2.5.1. *Independent of the choice of c_i, we have*

$$(n+1)b_{2n+1} + b_{2n+2} = k^{n+1}(k-1)^{n+1}.$$

Proof. First we show that the value of $C_n(k)$ depends only on n and k, but not the choice of c_i. Let $\pi : V_{2n+2,k} \to V_{2n,k}$, $(b_0, \ldots, b_{2n+2}) \mapsto (b_0, \ldots, b_{2n})$ be the projection map, which is surjective (where $V_{\cdot,k}$ is given by Definition 2.4.2). Lemma 2.4.5 implies that $\operatorname{rank}(V_{2n+2,k}) = n+1$, $\operatorname{rank}(V_{2n,k}) = n$, so that $U := \pi^{-1}(b_0, b_1, \ldots, b_n, 0, \ldots, 0)$ is a $\mathbb{Z}$-torsor. We will be done if we can exhibit $(b'_0, \ldots, b'_{2n+2}) \neq (b_0, \ldots, b_{2n+2}) \in U$ such that $(n+1)b'_{2n+1} + b'_{2n+2} = (n+1)b_{2n+1} + b_{2n+2}$.

If we take $c'_i = c_i$ for $i \neq 2n+1$, and $c'_{2n+1} = c_{2n+1} + 1$, we will have that $b'_i = b_i$ for $i \leq 2n$, $b'_{2n+1} = b_{2n+1} + \binom{2n+1}{1}$, and $b'_{2n+2} = b_{2n+2} - \binom{2n+2}{2}$. It follows directly that $(n+1)b'_{2n+1} + b'_{2n+2} = (n+1)b_{2n+1} + b_{2n+2}$.

Next we show that $C_n(k)$ agrees with a polynomial in k. Using the same process as in Corollary 2.4.6, we may solve for the data $c_0, \ldots, c_{2n}$ to give the extremal congruence. We will use this data (with $c_i = 0$ for $i \geq 2n+1$). We can then compute b_{2n+1}, b_{2n+2} in the following way:
Let M_n be the $n \times n$ matrix

$$M_n = \left[(-1)^{n+i} \binom{n+1+i}{j} \right]_{0 \leq i,j \leq n-1}.$$

Let A_n be the $2 \times n$ matrix

$$A_n = \left[(-1)^{i+1} \binom{i}{j} + \delta_{i,j} \right]_{\substack{2n+1 \leq i \leq 2n+2 \\ 0 \leq j \leq n-1}}.$$

Then M_n is invertible over the integers, and we have the matrix equation

$$\begin{pmatrix} b_{2n+1} \\ b_{2n+2} \end{pmatrix} = \begin{pmatrix} (k-1)^{2n+1} \\ (k-1)^{2n+2} \end{pmatrix} - A_n \cdot M_n^{-1} \cdot \begin{pmatrix} (k-1)^{n+1} \\ (k-1)^{n+2} \\ \vdots \\ (k-1)^{2n} \end{pmatrix}.$$

This shows that b_{2n+1}, b_{2n+2} are polynomials in k. Moreover, b_{2n+1} is equal to $(k-1)^{2n+1}$ plus a $\mathbb{Z}$-linear combination of $(k-1)^{n+1}, \ldots, (k-1)^{2n}$, so that b_{2n+1} is monic in k, of degree $2n+1$, and $(k-1)^{n+1} | b_{2n+1}$. Similarly, b_{2n+2} is monic of degree $2n+2$, and $(k-1)^{n+1} | b_{2n+2}$. It follows that $C_n(k) = (n+1)b_{2n+1} + b_{2n+2}$ is monic of degree $2n+2$, with $(k-1)^{2n+1} | C_n(k)$. The polynomial $C_n(k)$ is determined by the set $V_{2n+2,k}$, and Lemma 2.4.3 says that $V_{2n+2,k} = V_{2n+2,1-k}$. We may therefore make the

substitution $k \leftrightarrow 1-k$ to get the $k^{n+1}|C_n(k)$. By the Chinese remainder theorem, $k^{n+1}(k-1)^{n+1}|C_n(k)$. The only monic polynomial of degree $2n+2$ which is divisible by $k^{n+1}(k-1)^{n+1}$ is $k^{n+1}(k-1)^{n+1}$, so we conclude $C_n(k) = k^{n+1}(k-1)^{n+1}$. □

We now consider the possibility of extra powers of p in the congruence (2.12). For all integers k, n with $n \geq 0$, and all odd primes p, define

$$E(k,n,p) := \binom{kp-1}{p-1} - \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j).$$

Proposition 2.5.2. *Suppose $p \geq 2n+5$. Then*

$$E(k,n,p) \equiv \frac{-B_{p-3-2n}}{2n+3} k^{n+1}(k-1)^{n+1} p^{2n+3} \pmod{p^{2n+4}}.$$

Proof. By Theorem 2.3.3 and Proposition 2.3.1, we have

$$\begin{aligned}
E(k,n,p) &\equiv b_{2n+1} p^{2n+1} H_{p-1}(\{1\}^{2n+1}) + b_{2n+2} p^{2n+2} H_{p-1}(\{1\}^{2n+2}) \\
&\equiv -b_{2n+1} p^{2n+3} \frac{2n+2}{2(2n+3)} B_{p-3-2n} - b_{2n+2} p^{2n+3} \frac{B_{p-3-2n}}{2n+3} \\
&\equiv \frac{-B_{p-3-2n}}{n+3} \left((n+1) b_{2n+1} - b_{2n+2}\right) \\
&\equiv \frac{-B_{p-3-2n}}{n+3} k^{n+1}(k-1)^{n+1} \pmod{p^{2n+4}}.
\end{aligned}$$

□

Proposition 2.5.3. *Suppose $p = 2n+3$. Then*

$$E(k,n,p) \equiv -k^{n+1}(k-1)^{n+1} p^{2n+2} \pmod{p^{2n+3}}.$$

Proof. Using Theorem 2.3.3 and Proposition 2.3.1, we have

$$\begin{aligned}
E(k,n,p) &= b_{2n+1} p^{2n+1} H_{p-1}(\{1\}^{2n+1}) + b_{2n+2} p^{2n+2} H_{p-1}(\{1\}^{2n+2}) \\
&\equiv \frac{b_{2n+1}}{2} p^{2n+2} - b_{2n+2} p^{2n+2} \\
&\equiv \left(-\frac{(p-1) b_{2n+1}}{2} - b_{2n+1} \right) p^{2n+2} \\
&\equiv -\left((n+1) b_{2n+1} + b_{2n+2}\right) \\
&\equiv -k^{n+1}(k-1)^{n+1} p^{2n+2} \pmod{p^{2n+3}}.
\end{aligned}$$

□

We can now state the precise conditions under which the congruence in Theorem 2.4.1 holds modulo an extra power of p. Our next theorem is an immediate consequence of the preceding two propositions:

Theorem 2.5.4. *Let $n \geq 0$, k be integers, p an odd prime, and $b_{j,n}(T)$ the extremal polynomials (characterized by Proposition 2.4.8).*

(i) Suppose $p \geq 2n+5$. The congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+4}}$$

holds if and only if either $p | B_{p-3-2n}$ or $k \equiv 0, 1 \pmod{p}$.

(ii) Suppose $p = 2n+3$. The congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}$$

holds if and only if $k \equiv 0, 1 \pmod{p}$.

2.6 Properties of the extremal polynomials

The extremal polynomials $b_{j,n}(T)$ satisfy many arithmetic conditions. The following proposition records some of these, which follow from Proposition 2.4.8.

Proposition 2.6.1. *The extremal polynomials $b_{j,n}(T)$ satisfy the properties:*

(i) For all non-negative integers n, $b_{0,n}(T) = 1$ and $b_{n,n}(T) = T^n(T-1)^n$.

(ii) For all non-negative integers $j \leq 2n$, $T^j(T-1)^j$ divides $b_{j,n}(T)$.

For fixed j, the polynomials $b_{j,n}(T)$ depend on n. One exception to this is that $b_{0,n}(T) = 1$ for all non-negative integers n. Examining the table in Section 1.2, we see that $b_{1,n}(T)$ does indeed depend on n. However, $b_{1,n}(T) + b_{2,n}(T) = T^2 - T$ for all n. This is the first in a family of equations giving linear combinations of the extremal polynomials $b_{j,n}(T)$ which are independent of n.

Proposition 2.6.2. *Let m be a non-negative integer. Suppose $f(T) = \sum_{j=0}^{m} a_j T^j \in \mathbb{Q}[T]$ satisfying $f(T) = f(-1-T)$. Then for all non-negative integers n with $2n \geq m$, we have*

$$\sum_{j=0}^{m} a_j b_{j,n}(T) = f(T-1).$$

Proof. Define $g(T) = \sum_{j=0}^{m} a_j b_{j,n}(T)$. By Proposition 2.4.8, $b_{j,n}(T) \equiv (T-1)^j \pmod{(T-1)^{n+1}}$, so that $g(T) \equiv f(T-1) \mod (T-1)^{n+1}$. Similarly, by Proposition 2.4.8, $b_{j,n}(T) \equiv (-T)^j \pmod{T^{n+1}}$, so that $g(T) \equiv f(-T) \equiv f(T-1) \mod T^{n+1}$. This means $g(T)$ and $f(T-1)$ agree mod $T^{2n+1}(T-1)^{2n+1}$. Since these polynomials both have degree at most $2n+1$, they must be equal. $\square$

Chapter 3

Power Sums and p-adic L-function Values at Positive Integers

3.1 Introduction

We express the values of p-adic L-functions at positive integers as a p-adically convergent infinite sum involving the power sum multiple harmonic sums $\sum_{n=1}^{p-1} \frac{1}{n^k}$, with k varying. Truncating this expression gives congruences for thes p-adic L-values. We derive a family of linear relations among the power sum multiple harmonic sums, and use these relations to eliminate terms in our congruences. For all positive integers n, we can optimize this process to obtain a congruence for a p-adic L-value mod p^{2n+2}, involving $n+1$ multiple harmonic sums.

3.1.1 Statement of results

The main result of this chapter is a family of congruences for values of the Kubota-Leopoldt p-adic L-function at positive integers. The congruences in our family hold modulo arbitrarily large powers of p, and involve power sum multiple harmonic sums.

Fix an odd prime p, and let $\omega_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p$ be the Teichmüller character: for $(n,p) = 1$, $\omega_p(n)$ is the unique $(p-1)$-st root of 1 in $\mathbb{Q}_p$ with $\omega_p(n) \equiv n \mod p$. Our congruences involve the values $L_p(k, \omega^{1-k})$ for k an odd positive integer, which is the p-adic analog of the real number $\zeta(k)$.

Theorem 3.1.1. *Let $k \geq 3$ be an odd integer, n a non-negative integer. There exist explicitly computable rational constants $b_j(k,n)$, $j = 0, 1, \ldots$, such that the congruence*

$$pL_p(k, \omega_p^{1-k}) \equiv \sum_{j=0}^{n} b_j(k,n) p^j H_{p-1}(k-1+j) \pmod{p^{2n+3}} \tag{3.1}$$

holds for all sufficiently large primes p.

We give a table of the coefficients $b_j(k,n)$ for $k=3$ here:

Table 3.1: Coefficients $b_j(3,n)$ in L-value congruences

$n\backslash j$	0	1	2	3	4	5
0	1/2					
1	1/2	1/3				
2	1/2	7/15	1/5			
3	1/2	13/21	3/7	16/105		
4	1/2	1	1	64/105	4/21	
5	1/2	97/33	43/11	512/165	52/33	32/77

As an example, taking $k=3$, $n=2$ gives

$$pL_p(3,\omega^{-2}) \equiv \frac{1}{2}H_{p-1}(2) + \frac{7}{15}pH_{p-1}(3) + \frac{1}{5}p^2H_{p-1}(4) \pmod{p^7}.$$

Theorem 3.1.1 is a special case of a much more general family of congruences. The general congruence in this family, which holds for all sufficiently large primes p, is of the form

$$pL_p(k,\omega^{-2}) \equiv \sum_{j=0}^{n} b_j p^j H_{p-1}(k-1+j) \pmod{p^{n+1+\epsilon}}, \tag{3.2}$$

where $\epsilon \in \{0,1\}$ is chosen so that $\epsilon \equiv n \pmod 2$.

This general family contains a unique congruence of shape (3.2) which holds mod p^{2n+3}. In this sense, the coefficients $b_j(k,n)$ are uniquely determined. It is reasonable to expect that the congruence (3.1) holding for sufficiently large primes uniquely determines the coefficients $b_j(k,n)$. We cannot prove this unconditionally, but we show that it follows from the Weak Regularity Conjecture.

Theorem 3.1.2. *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture 1.3.5. Then the constants $b_j(k,n)$ appearing in the statement of Theorem 3.1.1 are uniquely determined by the condition that the congruence (3.1) holds for all sufficiently large primes p.*

3.2 Representing p-adic L-function values in terms of power sums

Our congruences are obtained by truncating an infinite series for $L_p(k,\omega^{1-k})$, involving power sum multiple harmonic sums. This series gives an actual equality with $L_p(k,\omega_p^{1-k})$.

3.2.1 Construction of the p-adic L-function

We begin by recalling the construction of the Kubota-Leopoldt p-adic L-function. Fix a prime p. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, $\mathbb{C}_p$ the completion of an algebraic closure of $\mathbb{Q}_p$. Fix an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, and also in $\mathbb{C}_p$. Let $\omega : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}_p$ be the Teichmüller character, defined previously. Via our chosen embeddings of $\overline{\mathbb{Q}}$, we may identify ω with a complex Dirichlet character. If χ is an arbitrary Dirichlet character, we define χ_n to be the primitive character inducing the product $\chi\omega^{-n}$.

Dirichlet L-functions take algebraic values at non-positive integers. A surprising fact is that, if we remove the Euler factor at p and restrict to a particular residue class mod $p-1$, these algebraic values are p-adically continuous. Because the non-positive integers in any residue class mod $p-1$ are dense in $\mathbb{Z}_p$, we can obtain a continuous function on $\mathbb{Z}_p$ (this function even turns out to be analytic).

Proposition 3.2.1 ([18], p. 29)**.** *Let p be a fixed prime, and define*

$$q = \begin{cases} p & \text{if } p \text{ odd} \\ 4 & \text{if } p = 2 \end{cases}.$$

Let χ be a primitive Dirichlet character. There exists a unique p-adic meromorphic function $L_p(s,\chi)$ with the following properties:

1. *$L_p(s,\chi)$ has a Laurent series expansion*

$$L_p(s,\chi) = \sum_{n=-1}^{\infty} a_n(s-1)^n, \qquad a_n \in \mathbb{C}_p,$$

   where $a_{-1} = 1 - \frac{1}{p}$ if χ is the trivial character, $a_{-1} = 0$ otherwise. This series converges for $s \in \mathbb{C}_p$ with $|s-1| < r$, where $r = |p|^{\frac{1}{p-1}}|q|^{-1} > 1$. In particular, the series converges for $s \in \mathbb{Z}_p$.

2. *For all positive integers n,*

$$L_p(1-n,\chi) = (1 - \chi_n(p)p^{n-1})L(1-n,\chi_n).$$

In the case $\chi = \omega^n$, condition (2) in Proposition 3.2.1 gives

$$L_p(1-n,\omega^n) = \left(1 - p^{n-1}\right)^{-1}\zeta(1-n).$$

For k a positive integer we consider $L_p(k, \omega^{1-k})$ to be the p-adic analog of the real number $\zeta(k)$ (for this reason the quantity $L_p(s, \omega^{1-n})$ is sometimes denoted $\zeta_{p,k}(k)$). The values $L_p(k, \omega^{1-k})$ appear in our congruences.

3.2.2 Power sums

For n is a positive integer, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. More generally, for any non-negative integer k, the expression $1^k + 2^k + \ldots + n^k$ is given by a polynomial in n of degree $k+1$. The exact form of this polynomial is given by Faulhaber's formula, which says

$$\sum_{j=0}^{n-1} j^k = \frac{1}{k+1} \sum_{j=1}^{k+1} \binom{k+1}{j} B_{k+1-j}\, n^j.$$

We have changed the upper limit of summation from n to $n-1$ for convenience.

It is reasonable to ask for an analogous formula when k is negative (in this case, the formula cannot be a polynomial in n). There are two main options. First, if we are interested is studying $\sum_{j=1}^{n} \frac{1}{j^k}$ (for k a positive integer) over the real numbers, we can write

$$\sum_{j=1}^{n} \frac{1}{j^k} = \zeta(k) + (-1)^{k-1} \frac{\psi^{(k-1)}(1+n)}{(k-1)!}, \tag{3.3}$$

where $\psi^{(n)}(s) = \left(\frac{d}{ds}\right)^n \frac{\Gamma'}{\Gamma}(s)$ is the polygamma function. In the case $k = 1$, we must replace the term $\zeta(1)$ by Euler's constant γ (which is the constant term in the Laurent expansion of $\zeta(s)$ at $s = 1$).

A second option is available if we wish to study the power sums $\sum_{j=1}^{n-1} \frac{1}{j^k}$ p-adically. In order that this sum be well-behaved, we have to modify the problem slightly, and consider instead the sums

$$\sum_{\substack{j=1 \\ (j,p)=1}}^{n-1} \frac{1}{j^k}.$$

For m a positive integer, we have

$$\sum_{\substack{j=1 \\ (j,p)=1}}^{n-1} \frac{1}{j^k} \equiv \sum_{\substack{j=1 \\ (j,p)=1}}^{n-1} j^{\varphi(p^m)-k} \pmod{p^m}.$$

If we choose m large enough that $\varphi(p^m) - k \geq m$, then we can use Faulhaber's formula and write

$$\begin{aligned}
\sum_{\substack{j=1 \\ (j,p)=1}}^{n-1} \frac{1}{j^k} &\equiv \sum_{\substack{j=1 \\ (j,p)=1}}^{n-1} j^{\varphi(p^m)-k} \\
&\equiv \sum_{j=1}^{n-1} j^{\varphi(p^m)-k} \\
&\equiv \frac{1}{\varphi(p^m)+1-k} \sum_{j=1}^{\varphi(p^m)+1-k} \binom{\varphi(p^m)+1-k}{j} B_{\varphi(p^m)+1-k-j} n^j \\
&\equiv \sum_{j\geq 1} c_j^{(m,k)} n^j \pmod{p^m},
\end{aligned}$$

where we have written

$$c_j^{(m,k)} = \begin{cases} \binom{\varphi(p^m)+1-k}{j} \frac{B_{\varphi(p^m)+1-k-j}}{\varphi(p^m)+1-k}, \text{ if } 1 \leq j \leq \varphi(p^m)+1-k, \\ 0, \text{ otherwise.} \end{cases}$$

We now prove a lemma.

Lemma 3.2.2. *Let j, k be positive integers, p an odd prime, and let the rational numbers $c_j^{(m,k)}$ be as above. For any integer n, we have the p-adic limit*

$$\lim_{m\to\infty} c_j^{(m,k)} n^j = -\binom{-k}{j} L_p(k+j, \omega^{1-k-j}) n^j.$$

If additionally p divides n, then the above limit is uniform in j (holding k fixed).

Proof. We denote by ϵ the Dirchlet character taking the value 1 at all positive integers. The statement that

$$\lim_{m\to\infty} c_j^{(m,k)} n^j = -\binom{-k}{j} L_p(k+j, \omega^{1-k-j}) n^j.$$

follows from the well known formula $\zeta(1-a) = L(1-a,\epsilon) = -\frac{B_a}{a}$ for $a \geq 1$. For the claim of uniformity in j when $p|n$, we observe that the parts not converging uniformly in j are the binomial coefficient (which introduces a factor of $j!$ in the denominator), and the value of the L-function $L_p(k+j, \omega^{1-k-j})$ (which grows at worst like $p^{\lfloor \log(j) \rfloor}$). Both of these problems are dominated by the factor of p^j due to the term n^j, so we get uniform convergence in this case. □

We have therefore shown the following.

Proposition 3.2.3. *Let k, n be positive integers, p an odd prime. Suppose $p|n$. Then:*

$$\sum_{\substack{j=1 \\ (j,p)=1}}^{np} \frac{1}{j^k} = -\sum_{j=1}^{\infty} \binom{-k}{j} L_p(k+j, \omega^{1-j-k})(pn)^j, \tag{3.4}$$

where the infinite sum is p-adically convergent.

We may think of this formula as a p-adic analog of Equation (3.3), in the following way. Over the complex numbers, we have a power series expansion

$$\zeta(k) + (-1)^{k-1} \frac{\psi^{(k-1)}(1+s)}{(k-1)!} = -\sum_{j \geq 1} \binom{-k}{j} \zeta(k+j) s^j,$$

convergent for $|s| < 1$. If we begin with Equation (3.3), replace the expression on the right hand side with its power series expansion (ignoring issues of convergence), replace each zeta value $\zeta(k)$ with the analogous p-adic value $L_p(k, \omega^{1-k})$, and evaluate at $s = np$, we obtain Equation (3.4).

The preceding discussion suggests defining a p-adic polygamma function (for k a positive integer) by

$$\psi_p^{(k)}(1+s) = (-1)^{k+1} k! \sum_{n \geq 0} \binom{-k-1}{n} L_p(1+k+n, \omega^{-k-n}) s^n, \tag{3.5}$$

which converges for $|s| < 1$. Morita [24], [25] constructed a p-adic analog of $\log(\Gamma(1+s))$, but arrived at the same series expansion (3.5).

For $n = p$, we can state Proposition 3.2.3 in terms of multiple harmonic sums.

Corollary 3.2.4. *Let k be a non-negative integer, p an odd prime. Then*

$$p^{k+1} H_{p-1}(k+1) = \sum_{n \geq k+2} (-1)^{n+k} \binom{n-1}{k} p^n L_p(n, \omega^{1-n}),$$

where the sum converges in $\mathbb{C}_p$.

3.2.3 p-adic L-function values in terms of multiple harmonic sums

Corollary 3.2.4 expresses power multiple harmonic sums as (infinite) linear combinations of p-adic L-function values at positive integers. We invert this linear system, solving for the L-values in terms of the power multiple harmonic sums.

Theorem 3.2.5. *Let $k \geq 2$ be an negative integer, and p an odd prime. Then*

$$p^k L_p(k, \omega^{1-k}) = \sum_{n \geq k-2} (-1)^{n+k} \binom{n}{k-2} \frac{B_{n+2-k}}{k-1} p^{n+1} H_{p-1}(n+1), \tag{3.6}$$

where the right side is p-adically convergent.

Proof. Using Corollary 3.2.4, we compute

$$\begin{aligned}
&\frac{1}{k-1} \sum_{n \geq k-2} (-1)^{n+k} \binom{n}{k-2} B_{n+2-k} p^{n+1} H_{p-1}(\{n+1\}; p-1) \\
=&\frac{1}{k-1} \sum_{n \geq k} (-1)^{n+k} \binom{n-1}{k-1} B_{n-k} \sum_{j \geq n} (-1)^{j+n} \binom{j+1}{n} p^{j+2} L_p(j+2, \omega^{-j-1}) \\
=&\frac{1}{k-1} \sum_{j \geq k} (-1)^{j+k} p^{j+2} L_p(j+2, \omega^{-j-1}) \left(\sum_{n=k}^{j} B_{n-k} \binom{n}{k} \binom{j+1}{n} \right) \\
=&\frac{1}{k-1} \sum_{j \geq k} (-1)^{j+k} \binom{j+1}{k} p^{j+2} L_p(j+2, \omega^{-j-1}) \left(\sum_{n=k}^{j} B_{n-k} \binom{j+1-k}{n-k} \right) \\
=&\frac{1}{k-1} \sum_{j \geq k} (-1)^{j+k} \binom{j+1}{k} p^{j+2} L_p(j+2, \omega^{-j-1}) \left(\sum_{n=0}^{j-k} B_n \binom{j+1-k}{n} \right) \\
=&\frac{1}{k-1} \sum_{j \geq k} (-1)^{j+k} \binom{j+1}{k} p^{j+2} L_p(j+2, \omega^{-j-1}) \delta_{j,k} \\
=&p^k L_p(k, \omega^{1-k}).
\end{aligned}$$

□

In the next section we will truncate (3.6) to obtain a congruence for $L_p(k, \omega^{1-k})$. We derive a family of relations among the power sum multiple harmonic sums, and use these relations to modify our congruences. This process will be optimized in Section 3.4.

3.3 Congruences for p-adic L-values

3.3.1 Relations among multiple harmonic sum

We now derive a family of linear relations among the power sum multiple harmonic sums $H_{p-1}(n)$.

Proposition 3.3.1. *Let p be an odd prime. For every non-negative integer n,*

$$(-1)^n p^{n+1} H_{p-1}(n+1) + \sum_{i \geq n} \binom{i}{n} p^{i+1} H_{p-1}(i+1) = 0, \tag{3.7}$$

where the infinite sum converges in $\mathbb{Q}_p$.

Proof. We consider the rational function

$$g_{p-1}(T) := \sum_{i=1}^{p-1} \frac{1}{T + \frac{i}{p}}.$$

This function satisfies a functional equation relating T and $-1-T$. We can compute

$$\begin{aligned} g_{p-1}(-1-T) &= \sum_{i=1}^{p-1} \frac{1}{-1-T+\frac{i}{p}} \\ &= \sum_{i=1}^{p-1} \frac{1}{-T-\frac{p-i}{p}} \\ &= -\sum_{j=1}^{p-1} \frac{1}{T+\frac{j}{p}} \\ &= -g_{p-1}(T). \end{aligned}$$

(In the third line above, we have made the substitution $j = p - i$.)

We can also expand $g_{p-1}(T)$ as a power series. We have

$$\begin{aligned} g_{p-1}(x) &= \sum_{i=1}^{p-1} \frac{1}{T+\frac{i}{p}} \\ &= \sum_{i=1}^{p-1} \frac{p}{j} \frac{1}{1+\frac{p}{j}T} \\ &= \sum_{i=1}^{p-1} \sum_{n\geq 0} (-1)^n \frac{p^{n+1}}{i^{n+1}} T^n \\ &= \sum_{n\geq 0} (-1)^n p^{n+1} \left(\sum_{i=1}^{p-1} \frac{1}{i^{n+1}} \right) T^n \\ &= \sum_{n\geq 0} (-1)^n p^{n+1} H_{p-1}(n+1) T^n. \end{aligned}$$

The multiple harmonic sum $H_{p-1}(n)$ is p-integral for all n, so over the field $\mathbb{C}_p$, the above series converges whenever $v_p(T) > v_p(\frac{1}{p})$. In particular, for such T, the functional equation for $g_{p-1}(T)$ gives

$$\begin{aligned} \sum_{n\geq 0} (-1)^n p^{n+1} H_{p-1}(n+1) T^n &= -\sum_{n\geq 0} (-1)^n p^{n+1} H_{p-1}(n+1)(-1-T)^n \\ &= -\sum_{n\geq 0} p^{n+1} H_{p-1}(n+1) \sum_{i=0}^{n} \binom{n}{i} T^i \\ &= -\sum_{i\geq 0} \left(\sum_{n\geq i} \binom{n}{i} p^{n+1} H_{p-1}(n+1) \right) T^i. \end{aligned}$$

Equating the coefficients of T^n on both sides of the above equation gives the desired result. □

In Chapter 2 we derived a similar family of relations for the elementary symmetric multiple harmonic sums $H_{p-1}(\{1\}^n)$. There we consider the generating function

$$f_{p-1}(T) := \prod_{n=1}^{p-1} \left(1 + \frac{p}{n} T\right) = \sum_{n=0}^{p-1} p^j H_{p-1}(\{1\}^n) T^n.$$

The connection between these two families of relations will be discussed in Chapter 5.

3.3.2 A general family of congruences for $L_p(k, \omega^{1-k})$

Now we derive a general family of congruences for $L_p(k, \omega^{1-k})$. The congruences are obtained by truncating (3.6) and adding a linear combination of the relations given by Proposition 3.3.1. To control the error due to truncation, we need to the following result describing the power of p dividing $H_{p-1}(n)$:

Proposition 3.3.2 ([40]). *Let n be a positive integer. For any prime $p \geq n+3$,*

$$H_{p-1}(n) \equiv 0 \begin{cases} \bmod p^2 & \text{if } n \text{ is odd,} \\ \bmod p & \text{if } n \text{ is even.} \end{cases}$$

Setting $n = 1$ in the above Proposition gives

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod{p^2},$$

which is equivalent to Wolstenholme's theorem. We may view the more general result as a natural generalization of Wolstenholme's Theorem.

We now give our general family of congruences for $L_p(k, \omega^{1-k})$:

Theorem 3.3.3. *Fix integers $k \geq 2$, $N \geq 0$. Let $c_0, c_1, \ldots, c_{N-1} \in \mathbb{Q}$, and define*

$$b_n = \frac{(-1)^{n+k}}{k-1}\binom{n}{k-2} B_{n+2-k} + (-1)^n c_n + \sum_{j=0}^{n} \binom{n}{j} c_j.$$

For all sufficiently large primes p, we have the congruence

$$p^k L_p(k, \omega^{1-k}) \equiv \sum_{n=0}^{N-1} b_n p^{n+1} H_{p-1}(n+1) \begin{cases} \pmod{p^{N+2}} & \text{if } N \text{ odd,} \\ \pmod{p^{N+3}} & \text{if } N \text{ even.} \end{cases} \tag{3.8}$$

Proof. We begin with Equation (3.6), and add a linear combination of the identities (3.7), where c_j is the coefficient of the equation indexed by j. We truncate at the N-th term. We use Proposition 3.3.2 to control the error, which gives the desired result for all primes $p \geq N+3$ not dividing the denominator of any c_j. □

Definition 3.3.4. We call (3.8) the *generalized harmonic congruence* associated with the data $[k, (c_0, \ldots, c_{N-1}), N]$, and we call $(b_0, \ldots, b_{N-1})$ the *generalized harmonic coefficients* associated with this data.

3.4 Optimized congruences

In this section, we optimize the application of Theorem 3.3.3 with $N = 2n+k-1$ ($k \geq 3$ odd). We choose the coefficients $c_0, c_1, \ldots, c_{N-1}$ in such a way that we get $b_0 = b_1 = \ldots = b_{k-3} = 0 = b_{k+n-1} = b_{k+n} = \ldots = b_{2n+k-2}$.

Theorem 3.4.1. *Let $k \geq 3$ be an odd integer, n a non-negative integer. There are unique constants $b_j(k,n) \in \mathbb{Q}$ ($j = 0, 1, \ldots, n$) with the following property:*

There exist $c_0, c_1, \ldots, c_{2n-1} \in \mathbb{Q}$ such that the generalized harmonic coefficients $(b_0, \ldots, b_{2n})$ satisfy $b_0 = b_1 = \ldots = b_{k-3} = 0$, $b_j = b_j(k,n)$ for $k-2 \leq j \leq k+n-2$, and $b_{k+n-1} = b_{k+n} = \ldots = 0$. In other words, we get a congruence

$$pL_p(k, \omega^{1-k}) \equiv \sum_{j=0}^{n} b_j(k,n) p^j H_{p-1}(k-1+j) \pmod{p^{2n+3}}, \tag{3.9}$$

which holds for all sufficiently large primes p.

We will need several preliminary facts before we can prove this theorem.

Definition 3.4.2. Let $\varphi_N : \mathbb{Q}^N \to \mathbb{Q}^N$ be the linear map

$$\varphi_N(c_0, \ldots, c_{N-1}) = (b_0, \ldots, b_{N-1}),$$

with b_j given by

$$b_j = (-1)^j c_j + \sum_{i=0}^{j} \binom{j}{i} c_i.$$

For $S \subset \{0, 1, \ldots, N-1\}$, we define

$$\pi_{S,N} : \mathbb{Q}^N \to \mathbb{Q}^{|S|}$$

to be projection onto the coordinates given by S, and

$$i_{S,N} : \mathbb{Q}^{|S|} \to \mathbb{Q}^N$$

the inclusion into the coordinates given by S. If the value of N is clear, we will abbreviate $\pi_{S,N}$ and $i_{S,N}$ by π_S, i_S respectively.

In what follows, let $n \geq 0$, $k \geq 3$ be integers with k odd, and set $N = 2n+k-1$ be an even integer.

Proposition 3.4.3. *We have rank*$(\varphi_N) = n + \frac{k-1}{2}$.

Proof. With respect to the standard basis, the matrix for φ_N is lower triangular. The diagonal entries of even index are non-zero, implying that $\text{rank}(\varphi_N) \geq n + \frac{k-1}{2}$. For the reverse inequality, consider the row span of φ_N. If we identify row vectors of length N with polynomials in an indeterminate T of degree at most $N-1$, via $(a_0, \ldots, a_{N-1}) \leftrightarrow \sum_{j=0}^{N-1} a_j T^j$, then one checks that every row vector of φ_N is identified with a polynomial $f(T)$ satisfying $f(T) = f(-1-T)$. Such polynomials can be expanded in odd powers of $(T + \frac{1}{2})$, so their span is of dimension at most $n + \frac{k-1}{2}$. □

Proposition 3.4.4. *Set* $S = \{k-2, k-1, \ldots, N-1\}$, $R = \{n+k-1, n+k, \ldots, N-1\}$. *Then the map*

$$f \;:=\; \pi_R|_{Im(i_S)\cap Im(\varphi_N)} : Im(i_S) \cap Im(\varphi_N) \to \mathbb{Q}^n$$

is a linear isomorphism.

Proof. We begin by proving surjectivity of f. Taking $T = \{k-2, k-1, \ldots, k+n-3\}$, it can be seen from the definition of φ_N that

$$\varphi_N(\text{Im}(i_T)) \subset \text{Im}(i_S).$$

Surjectivity will therefore follow if we can show

$$\pi_R \circ \varphi_N \circ i_T : \mathbb{Q}^{h-m} \to \mathbb{Q}^{h-m}$$

is surjective. We can directly compute that the matrix representing $\pi_R \circ \varphi_N \circ i_T$ (with respect to the standard basis on $\mathbb{Q}^{h-m}$) is

$$\left(\binom{j+h+m}{i+2m-1}\right)_{0\leq i,j\leq h-m-1}.$$

That the determinant of this square matrix is non-zero follows from a theorem of Tonne ([33], p. 18, Theorem 2).

Given surjectivity, to prove injectivity it will suffice to show

$$\dim(\mathrm{Im}(i_S) \cap \mathrm{Im}(\varphi_N)) \leq n.$$

Define $T' = \{0, 2, 4, \ldots, k-3\}$. We have $\mathrm{Im}(i_S) \subset \ker(\pi_{T'})$, so it is sufficient to prove $\dim(\ker(\pi_{T'}) \cap \mathrm{Im}(\varphi_N)) \leq n$. This will follow from Proposition 3.4.3 if we can show $\mathrm{rank}(\pi_{T'} \circ \varphi_N) \geq \frac{k-1}{2}$. We will show that in fact $\mathrm{rank}(\pi_{T'} \circ \varphi_n \circ i_{T'}) = \frac{k-1}{2}$. With respect to the standard bases, the matrix for $\pi_{T'} \circ \varphi_N \circ i_{T'}$ has the form

$$\left(\binom{2j}{2i} + \delta_{i,j} \right)_{0 \leq i,j \leq \frac{k-1}{2}}.$$

This matrix is lower triangular, with every diagonal entry equal to 2, so the result follows □

Proof of Theorem 3.4.1. We are given integers $n \geq 0$, $k \geq 3$ with k odd. Set $N = 2nk - 1$. Define $\underline{a} = (a_0, \ldots, a_{N-1}) \in \mathbb{Q}^N$ by

$$a_j = \frac{(-1)^{j+1}}{k+1} \binom{j}{k} B_{j-k}.$$

The set of coefficients $(b_0, b_1, \ldots, b_{N-1}) \in \mathbb{Q}^N$ arising from Proposition 3.3.3 is precisely

$$\underline{a} + \mathrm{Im}(\varphi_N).$$

The statement of Theorem 3.4.1 is therefore equivalent to the statement that there exists a unique element $\underline{d} = (d_0, \ldots, d_{N-1}) \in \mathrm{Im}(\varphi_N)$ with $d_j = -a_j$ for $0 \leq j \leq k-3$ and for $n + k - 1 \leq j \leq 2n + k - 2$. Note that $a_j = 0$ for $j \leq k - 1$. This forces $\underline{d} \in \mathrm{Im}(i_S)$, where S is as defined in Proposition 3.4.4. By Proposition 3.4.4, there is a unique $\underline{d} \in \mathrm{Im}(i_S) \cap \mathrm{Im}(\varphi_N)$ with $d_j = -a_j$ for $n + k - 1 \leq j \leq 2n + k - 2$. This completes the proof. □

3.5 Uniqueness

We believe the coefficients $b_j(k, n)$ appearing in Theorem 3.4.1 are uniquely determined by the condition that the congruence (3.9) holds for all sufficiently large primes. We do not establish this unconditionally. However, we will show that it follows from the following conjecture concerning Bernoulli numbers.

Conjecture 3.5.1 (Linear Bernoulli Nondegeneracy Conjecture)**.** *Fix an odd integer $k \geq 3$. There are infinitely many primes p for which p does not divide the numerator of the Bernoulli number B_{p-k}.*

Now we can state our uniqueness result.

Theorem 3.5.2 (Uniqueness of Optimized L-value Congruences)**.** *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. If k, m are integers with $m \geq 0$, and $a_1, \ldots, a_n \in \mathbb{Q}$ are such that*

$$p^k L_p(k, \omega^{1-k}) \equiv \sum_{j=0}^{n-1} a_j p^{j+1} H_{p-1}(j+1) \pmod{p^m}$$

holds for all but finitely many p, then this congruence arises from Theorem 3.4.1, in the following sense: there are constants $c_0, c_1, \ldots \in \mathbb{Q}$ such that, if $b_0, b_1, \ldots$ are defined by (2.9), then we have $a_i = b_i$ for $i = 0, 1, \ldots, \psi(m)$, where $\psi(m) = m - 2$ if m is even and $\psi(m) = m - 3$ if m is odd.

Proof. Suppose, to the contrary, that there is a congruence of the form

$$p^k L_p(k, \omega^{1-k}) \equiv \sum_{j=0}^{n-1} a_j p^{j+1} H_{p-1}(j+1) \pmod{p^m}$$

holding for sufficiently large p, which does not arise from Theorem 2.3.3. Subracting the identity

$$p^k L_p(k, \omega^{1-k}) = \sum_{n \geq k-2} (-1)^{n+k} \binom{n}{k-2} \frac{B_{n+2-k}}{k-1} p^{n+1} H_{p-1}(n+1)$$

from this congruence gives us a congruence of the form

$$\sum_{j \geq 0} c_j p^j H_{p-1}(j) \equiv 0 \pmod{p^m}, \tag{3.10}$$

which by hypothesis does not arise from truncating a linear combination of the identities (3.7). We may choose (3.10) so that $j_0 := \min\{j : c_j \neq 0\}$ is maximized among all congruences of this shape not arising from a truncation of a linear combinations of the identities (3.7). This implies that j_0 is even, for if j_0 were odd, we could add $\frac{-1}{2} c_j$ times the identity (3.7) with $j = j_0$, cancelling the lowest order term and

contradicting the maximality of j_0. By hypothesis, we also have $m \geq j_0 + 2$, so by reducing (3.10) mod p^{j_0+2}, we get

$$c_{j_0} p^{j_0} H_{p-1}(j_0) \equiv 0 \pmod{p^{j_0+2}}$$

for all sufficiently large primes p. Since j_0 is even, we have the congruence

$$H_{p-1}(j_0) \equiv \frac{j_0}{j_0+1} B_{p-j_0-1} p \mod p^2$$

for $p \geq j_0 + 3$ (see [40], Theorem 1.6). This implies

$$\frac{j_0 c_{j_0}}{j_0+1} p^{j_0+1} B_{p-1-j_0} \equiv 0 \pmod{p^{j_0+2}}$$

for all sufficiently large p. Since $c_{j_0} \neq 0$, this contradicts the Linear Bernoulli Nondegeneracy Conjecture. □

Theorems 3.4.1 and 3.5.2 now immediately imply the following:

Corollary 3.5.3 (Uniqueness of Extremal p-adic L-value Congruences)**.** *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. Then the constants $b_j(k,n)$ appearing in the statement of Theorem 3.4.1 are uniquely determined by the condition that the congruence (3.9) holds for all sufficiently large primes p.*

Chapter 4

Formal p-adic Identities Among Multiple Harmonic Sums

In this chapter we set up a general framework for constructing and classifying identities involving weighted multiple harmonic sums $p^{w(\mathbf{s})}H_{p-1}(\mathbf{s})$, where $\mathbf{s} = (s_1, \ldots, s_k)$ is a composition and p a prime. Our framework is in many ways similar to a framework used in the study of multiple zeta values (see, e.g., [15, 17, 26], and many others). We begin with a brief outline of the theory of multiple zeta values.

4.1 Multiple zeta values

For k a positive integer, the *multiple zeta function of depth k* is the function of k complex variables defined by the series

$$\zeta(s_1, \ldots, s_k) = \sum_{n_1 > n_2 > \ldots > n_k \geq 1} \frac{1}{n_1^{s_1} \ldots n_k^{s_k}}.$$

This series converges provided that $\mathrm{Re}(s_1) > 1$ and $\mathrm{Re}(s_i) > 0$ for $i = 2, 3, \ldots, k$ (see [15]).

Recall that a *composition* is a finite ordered list of positive integers. If $\mathbf{s} = (s_1, \ldots, s_k)$ is a composition, we define the *weight* and *depth* of $\mathbf{s}$ to be $w(\mathbf{s}) = s_1 + \ldots + s_k$ and $\ell(\mathbf{s}) = k$, respectively. We can think of ζ as a function that takes as input a composition $\mathbf{s} = (s_1, \ldots, s_k)$ and returns the multiple zeta value $\zeta(\mathbf{s}) = \zeta(s_1, \ldots, s_k)$.

4.1.1 Hoffman's algebra

To study multiple zeta values, Hoffman [15] used $\mathfrak{H}_{\mathbb{Q}} := \mathbb{Q}\langle x, y\rangle$, the non-commutative polynomial algebra in two variables over the integers, and the two

subalgebras $\mathfrak{H}^1_{\mathbb{Q}} := \mathbb{Q} + \mathfrak{H}y$, $\mathfrak{H}^0_{\mathbb{Q}} := \mathbb{Q} + x\mathfrak{H}y$. A basis of $\mathfrak{H}^1_{\mathbb{Q}}$ consists of words in the non-commuting symbols $z_1, z_2, \ldots$, where $z_k = x^{k-1}y$. A basis for $\mathfrak{H}^0_{\mathbb{Q}}$ consists of those words $z_{s_1} \ldots z_{s_n}$ with $s_1 \geq 2$. There is a $\mathbb{Q}$-linear map $\zeta : \mathfrak{H}^0_{\mathbb{Q}} \to \mathbb{R}$, taking the word $z_{s_1} \ldots z_{s_k} \in \mathfrak{H}^0_{\mathbb{Q}}$ to the multiple zeta value $\zeta(s_1, \ldots, s_k) \in \mathbb{R}$.

The ring $\mathfrak{H}^1_{\mathbb{Q}}$ can be given a commutative product, called the stuffle product and denoted $*$. The stuffle product is defined recursively. First we set

$$1 * \alpha = \alpha * 1 = \alpha$$

for every $\alpha \in \mathfrak{H}^1_{\mathbb{Q}}$. Next, if $k_1, k_2 \in \mathbb{Z}_{>0}$ and $\alpha_1, \alpha_2 \in \mathfrak{H}^1_{\mathbb{Q}}$, then

$$(z_{k_1}\alpha_1) * (z_{k_2}\alpha_2) = z_{k_1}(\alpha_1 * (z_{k_2}\alpha_2)) + z_{k_2}((z_{k_1}\alpha_1) * \alpha_2) + z_{k_1+k_2}(\alpha_1 * \alpha_2).$$

This restricts to give a commutative product on $\mathfrak{H}^0_{\mathbb{Q}}$. The stuffle product is constructed to reflect multiplication of nested sums over integers, and we have

$$\zeta(\alpha_1 * \alpha_2) = \zeta(\alpha_1)\zeta(\alpha_2)$$

for all $\alpha_1, \alpha_2 \in \mathfrak{H}^0_{\mathbb{Q}}$. The commutative ring $(\mathfrak{H}^1_{\mathbb{Q}}, *)$ is isomorphic to $\mathrm{QSym}_{\mathbb{Q}}$, the ring of quasi-symmetric functions over $\mathbb{Q}$ (see [16] for a construction of $\mathrm{QSym}_{\mathbb{Q}}$ and proof of this fact).

The utility of using words in the symbols x and y (as opposed to the symbols $z_1, z_2, \ldots$) comes from Kontsevich's representation of a multiple zeta value as an iterated integral. Let $\alpha = u_1 \ldots u_k \in \mathfrak{H}^0_{\mathbb{Q}}$ be a word, with $u_i \in \{x, y\}$. We have an equality

$$\zeta(\alpha) = \iint\limits_{1 \geq t_1 > t_2 > \ldots > t_k \geq 0} \omega_{u_1}(t_1)\omega_{u_2}(t_2) \ldots \omega_{u_k}(t_k)\ dt_1 dt_2 \ldots dt_k,$$

where $\omega_x(t) = \frac{1}{t}$, $\omega_y(t) = \frac{1}{1-t}$. To reflect this iterated integral expression, we define second commutative product, called the shuffle product, on $\mathfrak{H}_{\mathbb{Q}}$. The shuffle product ш is defined recursively. First we set

$$1 ш \alpha = \alpha ш 1 = \alpha$$

for every $\alpha \in \mathfrak{H}_{\mathbb{Q}}$. Next, if $t_1, t_2 \in \{x, y\}$ and $\alpha_1, \alpha_2 \in \mathfrak{H}_{\mathbb{Q}}$, then

$$(t_1\alpha_1) ш (t_2\alpha_2) = t_1(\alpha_1 ш (t_2\alpha_2)) + t_2((t_1\alpha_1) ш \alpha_2).$$

The multiplication ш restricts to give commutative multiplications on $\mathfrak{H}^0_{\mathbb{Q}}$ and $\mathfrak{H}^1_{\mathbb{Q}}$. The shuffle product is constructed to reflect multiplication of iterated integrals, and we have

$$\zeta(\alpha_1 ш \alpha_2) = \zeta(\alpha_1)\zeta(\alpha_2)$$

for all $\alpha_1, \alpha_2 \in \mathfrak{H}^1_{\mathbb{Q}}$.

4.1.2 Relations among multiple zeta values

A major goal of the theory of multiple zeta values is classifying the algebraic relations over $\mathbb{Q}$ among multiple zeta values. In view of either of the product representation given in the previous section, it will suffice to consider *linear* equations over $\mathbb{Q}$ satisfied by multiple zeta values. Using the framework of the evaluation map $\zeta : \mathfrak{H}^0_{\mathbb{Q}} \to \mathbb{R}$, the problem of classifying algebraic relations among multiple zeta values reduces to describing the kernel of ζ. There are several known methods of producing elements of $\ker(\zeta)$. We describe a few of these methods below.

1. It was observed above that for all $\alpha_1, \alpha_2 \in \mathfrak{H}^0_{\mathbb{Q}}$, $\zeta(\alpha_1 * \alpha_2) = \zeta(\alpha_1)\zeta(\alpha_2) = \zeta(\alpha_1 ш \alpha_2)$. It follows that $\alpha_1 * \alpha_2 - \alpha_1 ш \alpha_2 \in \ker(\zeta)$. This is the *double shuffle relation*, which was investigated by Ihara, Kaneko, and Zagier [17]. The double shuffle relation can be generalized to allow $\alpha_1, \alpha_2 \in \mathfrak{H}^1_{\mathbb{Q}}$, using a regularization process. Regularization leads to the so-called *extended double shuffle relations*. These relations conjecturally generate $\ker(\zeta)$.

2. Another method of producing linear relations among multiple zeta values is the Duality Theorem, conjectured by Hoffman [14] and proven by Kontsevich [38]. We first define an anti-automorphism $\tau : \mathfrak{H}_{\mathbb{Q}} \to \mathfrak{H}_{\mathbb{Q}}$ which interchanges x and y. The map τ restricts to an anti-automorphism of $\mathfrak{H}^0_{\mathbb{Q}}$. The Duality Theorem for multiple zeta values is the statement that $\zeta(\alpha) = \zeta(\tau(\alpha))$ for all $\alpha \in \mathfrak{H}^0_{\mathbb{Q}}$. In other words, $\tau(\alpha) - \alpha \in \ker(\zeta)$.

3. There is a map $D : \mathfrak{H}_{\mathbb{Q}} \to \mathfrak{H}_{\mathbb{Q}}$, determined by $D(x) = 0$, $D(y) = xy$, and the condition that D is a $\mathbb{Q}$-derivation. The derivation D restricts to a derivation on the subalgebra $\mathfrak{H}^0_{\mathbb{Q}}$. If we set $\overline{D} := \tau D \tau$ (where τ is the anti-involution defined above), then a result of Hoffman [14] implies that $\overline{D}(\alpha) - D(\alpha) \in \ker(\zeta)$ for all $\alpha \in \mathfrak{H}^0_{\mathbb{Q}}$. This was later generalized by Ohno [26]. A further generalization was given by Ihara, Kaneko, and Zagier [17].

The ring $\mathfrak{H}^0_{\mathbb{Q}}$ is graded by degree, and the kernel of ζ is conjectured to be a homogenous ideal. Indeed, all known relations among multiple zeta values can be decomposed into homogenous relations (that is, relations involving compositions of fixed weight). Define d_n to be the $\mathbb{Q}$-dimension of the image of the n-th graded piece of $\mathfrak{H}^0_{\mathbb{Q}}$ under ζ. In other words, d_n is the number of linearly independent multiple zeta values of weight n. Using known methods for constructing relations among multiple zeta values, the values of d_n for $n \leq 10$ are believed to be

n	2	3	4	5	6	7	8	9	10
d_n	1	1	1	2	2	3	4	5	7

Numerology suggests that numbers d_n satisfy the linear recurrence relation $d_n = d_{n-2} + d_{n-3}$; this was conjectured by Zagier [38]. Zagier's conjecture led Hoffman [15] to conjecture that multiple zeta values of the form $\zeta(s_1, \ldots, s_k)$ with $s_i \in \{2, 3\}$ form a basis for the space of multiple zeta values (it can be checked that the number a_n of compositions $\mathbf{s} = (s_1, \ldots, s_k)$ with $s_i \in \{2, 3\}$ and $w(\mathbf{s}) = n$ satisfies the conjectured recurrence, and has the same initial values).

4.2 Multiple harmonic sums

In this section we investigate p-adic relations among *weighted* multiple harmonic sums $p^{w(\mathbf{s})}H_{p-1}(\mathbf{s})$, where $\mathbf{s}$ is a composition and p is an unspecified prime. We will work over the ring $\mathbb{Z}[\frac{1}{2}]$, so we consider the non-commutative algebras $\mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]} := \mathbb{Z}[\frac{1}{2}]\langle x, y\rangle$, and the two subalgebras $\mathfrak{H}^1_{\mathbb{Z}[\frac{1}{2}]} := \mathbb{Z}[\frac{1}{2}] + \mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]}y$, $\mathfrak{H}^0_{\mathbb{Z}[\frac{1}{2}]} := \mathbb{Z}[\frac{1}{2}] + x\mathfrak{H}_{\mathbb{Z}[\frac{1}{2}]}y$. The stuffle product $*$ gives a commutative multiplication on $\mathfrak{H}^1_{\mathbb{Z}[\frac{1}{2}]}$.

As above, we set $z_n := x^{n-1}y$. We will actually use the completion $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ of the ring $\mathfrak{H}^1_{\mathbb{Z}[\frac{1}{2}]}$.

Definition 4.2.1. Denote by $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ the completion of $\mathfrak{H}^1_{\mathbb{Z}[\frac{1}{2}]}$ with respect the degree grading. An element of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ is a formal infinite sum

$$\alpha = \sum_{\mathbf{s}=(s_1,\ldots,s_k)} \alpha_{\mathbf{s}} z_{s_1} \ldots z_{s_k} \tag{4.1}$$

in the non-commuting variables $z_1, z_2, \ldots$, where the summation is taken over all compositions $\mathbf{s} = (s_1, \ldots, s_k)$, and the coefficients $\alpha_{\mathbf{s}}$ are in $\mathbb{Z}[\frac{1}{2}]$. The topology on

$\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ has a neighborhood basis consisting of the sets

$$\mathbb{I}_n := \left\{ \sum_{\mathbf{s}} \alpha_{\mathbf{s}} z_{s_1} \dots z_{s_k} : \alpha_{\mathbf{s}} = 0 \text{ when } s_1 + \dots + s_k < n \right\}.$$

The stuffle product $*$ gives a (continuous) commutative multiplication on $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$.

We will write $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ when we mean the set $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, viewed as a commutative ring with multiplication given by $*$. We have that $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ is isomorphic as a topological ring to the completion of the ring os quasi-symmetric functions over $\mathbb{Z}[\frac{1}{2}]$ (see[]). The $\mathbb{I}_n$ are ideals of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$, and for each non-negative integer n, $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}/\mathbb{I}_n$ is a finitely-generated and free as a module over $\mathbb{Z}[\frac{1}{2}]$.

Remark 4.2.2. Most of what we do could be done over $\mathbb{Z}$ instead of over $\mathbb{Z}[\frac{1}{2}]$. The consequence of this would be that several of our theorems would have more complicated statements. In some ways it would be most desirable to work over $\mathbb{Q}$ instead, but this raises technical problems; see the Appendix for a possible resolution.

We view the element $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ given by (4.1) as representing the (infinite) formal sum

$$\sum_{\mathbf{s}} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}) \tag{4.2}$$

of weighted multiple harmonic sums, with p an unspecified prime. Elements of $\mathbb{I}_n$ represent sums of the form (4.2) that are formally divisibly by p^n.

The following definition is new.

Definition 4.2.3. For each prime $p \geq 3$, define $\phi_p : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \mathbb{Z}_p$,

$$\left(\sum \alpha_{\mathbf{s}} z_{s_1} \dots z_{s_k} \right) \mapsto \sum_{\mathbf{s}} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}).$$

It is a continuous ring map. We let $\phi : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \prod_{p \geq 3} \mathbb{Z}_p$ be the product of these maps, and we call ϕ the *universal evaluation map*. For each non-negative integer n, we define

$$\mathbb{J}_n = \{\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} : p^n | \phi_p(\alpha) \text{ for all sufficiently large primes } p\}.$$

We think of an element of $\mathbb{J}_n$ as a formal congruence

$$\sum_{\mathbf{s}} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}) \equiv 0 \mod p^n \mathbb{Z}_p$$

with $a_{\mathbf{s}} \in \mathbb{Z}[\frac{1}{2}]$, such that the series converges in $\mathbb{Q}_p$ and the congruence holds for all $p \geq 3$. We think of an element of $\ker(\phi)$ as a formal equality

$$\sum_{\mathbf{s}} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}) = 0,$$

holding (and p-adically convergent) for all $p \geq 3$. We call such an expression a *formal p-adic identity*. We view the map ϕ as an analogue of $\zeta : \mathfrak{H}^0 \to \mathbb{R}$.

Our goal is to understand the ideals $\ker(\phi)$ and $\mathbb{J}_n$ as well as possible. We prove some basic properties below.

Definition 4.2.4. An ideal $I \subset (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ is called *absolutely closed* if I is closed, and for all $r \in \mathbb{Z}_{>0}$ and $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, we have $r\alpha \in I \Rightarrow \alpha \in I$. If $I \subset (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ is any ideal, we define $\widetilde{I}$ to be the intersection of all absolutely closed ideals containing I, and call $\widetilde{I}$ the *absolute closure* of I. It is an asbolutely closed ideal.

Proposition 4.2.5. *For all $n \geq 0$, $\mathbb{J}_n$ is an ideal of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$. We have $\ker(\phi) + \mathbb{I}_n \subset \mathbb{J}_n$, so that the ideals $\mathbb{J}_n$ are open. Additionally, $\mathbb{J}_n$ and the kernel of ϕ are absolutely closed.*

Proof. The first statement follows from the general fact that the preimage of an ideal under a ring map is an ideal. It is clear from the definitions that $\mathbb{J}_\infty$ and $\mathbb{I}_n$ are contained in $\mathbb{J}_n$, which implies $\mathbb{J}_n$ is open. The final statement is immediate from the definition of absolute closure. □

Remark 4.2.6. The absolutely closed ideal $\ker(\phi) \subset (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ plays the same role for us that $\ker(\zeta) \subset (\mathfrak{H}^0, *)$ plays in the study of multiple zeta values. Unlike what is conjectured to be the case for $\ker(\zeta)$, the ideal $\ker(\phi)$ is not homogeneous. Particularly, the identity

$$2pH_{p-1}(1) = \sum_{n=2}^{\infty} (-1)^n p^n H_{p-1}(n),$$

which follows from Corollary 4.3.3, shows that the non-homogeneous element $2y - xy + x^2y - \ldots = y + (1+x)^{-1}y$ is in $\ker(\phi)$. The degree one homogeneous component $2y$ is not, as $pH_{p-1}(1) \neq 0$ for all p.

At the moment, all known elements of $\mathbb{J}_n$ come from the following, which is an immediate corollary of Proposition 4.2.5:

Corollary 4.2.7. *The ideal $\mathbb{J}_n$ is contained in the absolute closure of* $\ker(\phi) + \mathbb{I}_n$.

Corollary 4.2.7 is the statement that an asymptotic relation can be truncated to give a congruence holding for all but finitely many primes. In many known examples, a converse holds: if we have a congruence for weighted multiple harmonic sums, we can find an asymptotic relation with the congruence as a truncation. We make the following conjecture.

Conjecture 4.2.8. *For all integers $n \geq 0$, $\mathbb{J}_n$ is the absolute closure of* $\ker(\phi) + \mathbb{I}_n$.

In Chapter 5, we consider the closed subalgebra $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \subset (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ consisting of symmetric elements (see Definition 5.1.1). Conditionally on a conjecture involving Bernoulli numbers, we produce a sequence of elements of $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ that generate an ideal with absolute closure $\ker(\phi) \cap \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$. We show that a suitable modification of the converse of Corollary 4.2.7 is true for $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$.

Remark 4.2.9. The ideals $\mathbb{J}_n$ determine the set of mod p congruences among multiple harmonic sums of a given weight n, which hold for all suffieciently large primes p. The set of formal $\mathbb{Z}[\frac{1}{2}]$-linear combinations of multiple harmonic sums of weight n is $\mathbb{I}_n/\mathbb{I}_{n+1}$, and the number of mod p linearly independent sums in this weight is the rank of $(\mathbb{I}_n/(\mathbb{J}_{n+1} \cap \mathbb{I}_n))$.

4.3 Some elements in the kernel of the universal evaluation map

Two useful techniques for producing mod p relations among multiple harmonic sums are due to Hoffman [16]. In this chapter we provide analogous recipes for producing elements of $\ker(\phi)$. These elements correspond to formal p-adic identities extending the mod p congruences of Hoffman.

4.3.1 The p-adic reflection theorem

There is an anti-automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ which squares to the identity, taking $z_{s_1} \dots z_{s_k}$ to $\overline{z_{s_1} \dots z_{s_k}} := z_{s_k} \dots z_{s_1}$. This can also be viewed as an involution on the set of compositions, where $\overline{(s_1, \dots, s_k)} = s_k \dots s_1$. Hoffman ([16], Theorem 4.5)

shows that for every composition $\mathbf{s}$, we have the congruence

$$H_{p-1}(\mathbf{s}) \equiv (-1)^{w(\mathbf{s})} H_{p-1}(\overline{\mathbf{s}}) \pmod{p}$$

for all primes p. The following is an p-adic extension of this congruence.

Theorem 4.3.1 (p-adic Reflection Theorem)**.** *Let $\mathbf{s} = (s_1, \ldots, s_k)$ be a composition. For all primes p we have a convergent p-adic series equality*

$$H_{p-1}(\mathbf{s}) = (-1)^{w(\mathbf{s})} \sum_{\substack{\mathbf{b}=(b_1,\ldots,b_k) \\ b_1,\ldots,b_k \geq 0}} \prod_{j=1}^{k} \binom{s_j + b_j - 1}{b_j} p^{b_1+\ldots+b_k} H_{p-1}(\overline{\mathbf{s}} + \mathbf{b}),$$

where $\mathbf{s} + \mathbf{b} = (s_1 + b_1, \ldots, s_k + b_k)$.

Proof. First, for $1 \leq m \leq p-1$ an integer, the binomial theorem gives

$$\begin{aligned} \frac{1}{(p-m)^s} &= \frac{(-1)^s}{n^s} \left(1 - \frac{p}{m}\right)^s \\ &= (-1)^s \sum_{b \geq 0} \binom{s+b-1}{b} p^j m^{-s-b}, \end{aligned}$$

which converges p-adically. We then make the substitutions $n_i \leftrightarrow p - m_i$ in the definition of the multiple harmonic sum, giving

$$\begin{aligned} H_{p-1}(\mathbf{s}) &= \sum_{p-1 \geq n_1 > \ldots > n_k \geq 1} \frac{1}{n_1^{s_1} \ldots n_k^{s_k}} \\ &= \sum_{p-1 \geq m_k > \ldots > m_1 \geq 1} \frac{1}{(p-m_1)^{s_1} \ldots (p-m_k)^{s_k}} \\ &= (-1)^{w(\mathbf{s})} \sum_{p-1 \geq m_k > \ldots > m_1 \geq 1} \sum_{b_1,\ldots,b_k \geq 0} \prod_{j=1}^{k} \binom{s_j + b_j - 1}{b} p^j m_j^{-s_j - b_j} \\ &= (-1)^{w(\mathbf{s})} \sum_{b_1,\ldots,b_k \geq 0} \prod_{j=1}^{k} \binom{s_j + b_j - 1}{b} p^j H_{p-1}(s_k + b_1, \ldots, s_1 + b_k) \end{aligned}$$

□

We can state the p-adic Reflection Theorem in terms of the derivation $\overline{d}$ defined by Ihara, Kaneko, and Zagier ([17], Table 2):

Corollary 4.3.2 (p-adic Reflection Theorem, short form)**.** *Let $\overline{d}$ be the derivation on $\widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]}$ given by $x \mapsto x^2$, $y \mapsto xy$, and let $R : \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ be the anti-involution sending $z_{s_1} \dots z_{s_k}$ to $(-1)^{s_1+\dots+s_k} z_{s_k} \dots z_{s_1}$. Then $\exp(\overline{d})$ is an automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, and for any $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$,*

$$\exp\left(\overline{d}\right)(\alpha) - \mathrm{R}(\alpha) \in \ker(\phi).$$

Proof. By linearity, it suffices to consider $\alpha = z_{s_1} \dots z_{s_k}$. It is shown in [17], Proposition 7, that $\exp(\overline{d})$ is an automorphism of $\widehat{\mathfrak{H}}^0_{\mathbb{Z}[\frac{1}{2}]}$ satisfying $\exp(\overline{d})(x) = (1-x)^{-1}x$ and $\exp(\overline{d})(y) = (1-x)^{-1}y$. Now we compute

$$\begin{aligned}
\exp(\overline{d})(\alpha) &= \prod_{j=1}^{k} \exp(\overline{d})(x^{s_j-1}y) \\
&= \prod_{j=1}^{k} (1-x)^{-s_j} x^{s_j-1} y \\
&= \prod_{j=1}^{k} \sum_{b_j \geq 0} \binom{s_j + b_j - 1}{b_j} x^{s_j-1+b} y \\
&= \sum_{b_1,\dots,b_k \geq 0} z_{s_1+b_1} \dots z_{s_k+b_k}
\end{aligned}$$

The result now follows from Theorem 4.3.1 and the definition of $R(z_{s_1} \dots z_{s_k})$. □

Taking $\alpha = x^n y \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, we get the following:

Corollary 4.3.3. *For all $n \geq 0$, the convergent p-adic identity*

$$(-1)^n p^{n+1} H_{p-1}(n+1) + \sum_{k \geq n} \binom{k}{n} p^{k+1} H_{p-1}(k+1) = 0$$

holds for all primes p. Equivalently, we have

$$(-1)^n p^{n+1} x^n y + \sum_{k \geq n} \binom{k}{n} x^k y \in \ker(\phi).$$

This corollary will be used in Chapter 5 to show that Theorem 4.3.1 suffices to determine the intersection of $\ker(\phi)$ with the closed subalgebra of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ generated by the elements y^n.

Proof. Every term appearing in $\exp(\overline{d})(x^n y)$ is of the form $x^k y$ for some $m \geq n$. The coefficient of $x^k y$ is the number of ordered $(n+1)$-tuples of non-negative integers

with sum $k-n$. By a standard combinatorial argument, this number is $\binom{k}{n}$. The result now follows. □

4.3.2 The p-adic duality theorem

In [16] Hoffman also proves a duality theorem (Theorem 4.6). To state this theorem, we need a definition. For n a non-negative integer and $\mathbf{s} = (s_1, \ldots, s_k)$ a composition, we let

$$S_n(\mathbf{s}) := \sum_{n \geq n_1 \geq n_2 \geq \ldots \geq n_1 \geq 1} \frac{1}{n_1^{s_1} \ldots n_k^{s_k}}.$$

This sum can be expressed in terms of multiple harmonic sums:

$$S_n(\mathbf{s}) = \sum_{\mathbf{t} \preceq \mathbf{s}} H_n(\mathbf{t}),$$

where $\mathbf{t} \preceq \mathbf{s}$ means the composition $\mathbf{t}$ can be obtained from $\mathbf{s}$ by combining some of its parts. When $\mathbf{s} = (s_1, \ldots, s_k)$ is a composition, we denote by $\mathfrak{z}(\mathbf{s})$ the element

$$\sum_{\substack{\mathbf{t}=(t_1,\ldots,t_m) \\ \mathbf{t} \preceq \mathbf{s}}} z_{t_1} \ldots z_{t_m} \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}.$$

We extend $\mathfrak{z}$ to a $\mathbb{Z}[\frac{1}{2}]$-linear map $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, taking $z_{s_1} \ldots z_{s_k}$ to $\mathfrak{z}(s_1, \ldots, s_k)$ for each composition $\mathbf{s} = (s_1, \ldots, s_k)$. In [16] an inverse to $\mathfrak{z}$ is constructed using the Möbius inversion formula.

Compositions $\mathbf{s} = (s_1, \ldots, s_k)$ of weight n are in bijection with subsets of $\{1, 2, \ldots, n-1\}$ by the map

$$\phi : (s_1, \ldots, s_k) \mapsto \{s_1, s_1 + s_2, \ldots, s_1 + s_2 + \ldots + s_{k-1}\}. \tag{4.3}$$

The dual $\mathbf{s}^*$ is the composition corresponding under (4.3) to the complement of $\phi(\mathbf{s})$. The operation $\mathbf{s} \mapsto \mathbf{s}^*$ squares to the identity. We extend this operation to an automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, $(z_{s_1} \ldots z_{s_k})^* := z_{t_1} \ldots z_{t_{k'}}$, where $(t_1, \ldots, t_{k'}) = (s_1, \ldots, s_k)^*$. Hoffman's result states that for all compositions $\mathbf{s}$, the congruence

$$S_{p-1}(\mathbf{s}) + S_{p-1}(\mathbf{s}^*) \equiv 0 \pmod{p}$$

holds for all primes p .This was later extended by Zhao, who showed that for all odd primes p,

$$S_{p-1}(\mathbf{s}) + S_{p-1}(\mathbf{s}^*) + p\left(\sum_{\mathbf{t}\preceq\mathbf{s}} H_{p-1}((1)\sqcup\mathbf{t})\right) \equiv 0 \pmod{p^2},$$

where $(1)\sqcup(t_1,\ldots,t_k) = (1,t_1,\ldots,t_k)$. These congruences can be expressed in a different way. Define an involution $\psi : \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]}$, $x \mapsto x+y$, $y \mapsto -y$. This restricts to a map $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, which we also denote ψ. Hoffman [16] shows that the duality theorem is equivalent to the congruence

$$H_{p-1}(\psi(\mathbf{s})) - H_{p-1}(\mathbf{s}) \equiv 0 \pmod{p}.$$

Our p-adic extension of the above congruences is stated in terms of two automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$: ψ (described by Hoffman in [16]) and $\Phi_{(-y)}$ (described by Ihara, Kaneko, and Zagier in [17]).

Theorem 4.3.4 (p-adic Duality Theorem)**.** *Let $\psi : \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}_{\mathbb{Z}[\frac{1}{2}]}$ be the automorphism $x \mapsto x+y$, $y \mapsto -y$, and $\Phi_{(-y)} : \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ the automorphism $\alpha \mapsto (1+y)\left(\frac{1}{1+y} * \alpha\right)$. Then ψ restricts to an automorphism of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, and for all $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, we have*

$$\Phi_{(-y)}(\alpha) - \psi(\alpha) \in \ker(\phi).$$

Proof. By linearity, it suffices to consider $\alpha = z_{s_1}\ldots z_{s_k}$. We may assume p is odd, as this is the case for all but finitely many p. First we compute a p-adic representation of $\binom{p}{n}$, n fixed. We have

$$\begin{aligned}\binom{p}{n} &= \frac{p(p-1)\ldots(p-n+1)}{n!} \\ &= (-1)^{n+1}\frac{p}{n}\left(1-\frac{p}{1}\right)\left(1-\frac{p}{2}\right)\ldots\left(1-\frac{p}{n-1}\right) \\ &= (-1)^{n+1}\frac{p}{n}\sum_{j\geq 0}(-1)^j p^j H_{n-1}(\{1\}^j).\end{aligned}$$

The work of Hoffman ([16], Theorem 4.2 and the proof of Theorem 4.6) shows that for any composition $\mathbf{s}$,

$$-S_{p-1}(\mathbf{s}^*) = \sum_{n=1}^{p}\binom{p}{n}(-1)^{n+1}S_{n-1}(\mathbf{s}).$$

Multiplying through by $p^{w(\mathbf{s})} = p^{w(\mathbf{s}^*)}$ and using our p-adic representation of $\binom{p}{n}$, we have

$$\begin{aligned} -p^{w(\mathbf{s}^*)} S_{p-1}(\mathbf{s}^*) &= \sum_{n=1}^{p} \binom{p}{n} (-1)^{n+1} p^{w(\mathbf{s})} S_{n-1}(\mathbf{s}) \\ &= p^{w(\mathbf{s})} S_{p-1}(\mathbf{s}) + \sum_{n=1}^{p-1} \frac{p}{n} p^{2(\mathbf{s})} S_{n-1}(\mathbf{s}) \sum_{j\geq 0} (-1)^j p^j H_{n-1}(\{1\}^j) \\ &= p^{w(\mathbf{s})} S_{p-1}(\mathbf{s}) + \sum_{j\geq 0} (-1)^j p^{w(\mathbf{s})+j+1} \sum_{n=1}^{p-1} \frac{1}{n} S_{n-1}(\mathbf{s}) H_{n-1}(\{1\}^j) \end{aligned}$$

The left hand side above is $\phi_p(-\mathfrak{z}(\mathbf{s}^*))$. The bottom right is

$$\phi_p\left(\mathfrak{z}(\mathbf{s}) + \sum_{j\geq 0} (-1)^j y(\mathfrak{z}(\mathbf{s}) * y^j)\right) = \phi_p\left(\mathfrak{z}(\mathbf{s}) + y\left(\frac{1}{1+y} * \mathfrak{z}(\mathbf{s})\right)\right).$$

It follows that

$$\mathfrak{z}(\mathbf{s}^*) + \mathfrak{z}(\mathbf{s}) + y\left(\frac{1}{1+y} * \mathfrak{z}(\mathbf{s})\right) \in \ker(\phi)$$

for all compositions $\mathbf{s}$. Since this expression is linear in $\mathbf{s}$, the formula holds when $\mathbf{s}$ is replaced by any element of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$. If we choose the element $\mathfrak{z}^{-1}(\alpha)$ for some $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, we get

$$-\psi(\alpha) + \alpha + y\left(\frac{1}{1+y} * \alpha\right) \in \mathbb{J}_\infty, \tag{4.4}$$

using the relation $-\mathfrak{z}(\mathbf{s}^*) = \psi(\mathfrak{z}(\mathbf{s}))$ ([16], Theorem 3.2).

Next, we note that the asymptotic relation

$$\sum_{n\geq 1} (-1)^{n+1} p^n H_{p-1}(\{1\}^n) = 0,$$

which follows from Proposition 2.2.1 with $n = p-1$, $j = 0$, implies that $y - y^2 + y^3 - \ldots = \frac{y}{1+y} \in \mathbb{J}_\infty$. The set $\mathbb{J}_\infty$ is an ideal of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$, so $\frac{1}{1+y} * \alpha - \alpha \in \mathbb{J}_\infty$. Combining this with (4.4) gives

$$(1+y)\left(\frac{1}{1+y} * \alpha\right) - \psi(\alpha) \in \mathbb{J}_\infty.$$

This completes the proof. □

Remark 4.3.5. The ring $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ is filtered by the ideals $\mathbb{I}_n$, and is in fact graded. As we discussed in Remark 4.2.9, the study of mod p multiple harmonic sums amounts to the study the sets $\mathbb{I}_n/(\mathbb{J}_{n+1} \cap \mathbb{I}_n)$. We can reinterpret this as the study of the ideal

$$\bigoplus_{n\geq 0} (\mathbb{J}_{n+1} \cap \mathbb{I}_n)/\mathbb{I}_{n+1} \subset \bigoplus_{n\geq 0} \mathbb{I}_n/\mathbb{I}_{n+1}$$

in the associated graded ring of $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ [16].

The automorphisms R and ψ in Theorems 4.3.1 and 4.3.4 preserve the grading. The automorphism $\exp(\overline{d})$ and $\Phi_{(-y)}$ preserve the filtration but not the grading. In fact, $\exp(\overline{d})$ and $\Phi_{(-y)}$ induce the identity map on the associated graded ring, so our Theorems 4.3.1, 4.3.4 reduce to the duality and reflection theorems for mod p sums (Theorems 4.5 and 4.6 of [16]) when we pass to the associated graded ring. It is perhaps accurate to say that the study of asymptotic relations among multiple harmonic sums is the study of the ring $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ and universal evaluation map $\phi : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \prod_{p\geq 3} \mathbb{Z}_p$, whereas the study of mod p multiple harmonic sums is the study of the associated graded ring and morphism, where $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ is filtered by the ideals $\mathbb{I}_n$, and $\prod_{p\geq 3} \mathbb{Z}_p$ is filtered by the ideals $\prod_{p\geq 3} p^n \mathbb{Z}_p$.

Chapter 5

Formal p-adic Identities for Symmetrized Sums

In this chapter we consider *symmetrized multiple harmonic sums*, which are variations of multiple harmonic sums. Symmetrized multiple harmonic sums include the elementary symmetric multiple harmonic sums $H_n(\{1\}^k)$ and the power sum multiple harmonic sums $H_n(k)$. We provide a classification of congruences among weighted symmetrized multiple harmonic sums, which is conditional upon a conjecture of Zhao [41] regarding Bernoulli numbers.

5.1 Introduction

Suppose $\mathbf{s} = (s_1, \ldots, s_k)$, $\mathbf{t} = (t_1, \ldots, t_k)$ are two compositions of equal length. We write $\mathbf{s} \sim \mathbf{t}$ if there exists a permutation $\sigma \in S_k$ such that $s_i = t_{\sigma(i)}$ for $i = 1, 2, \ldots, k$.

Definition 5.1.1. Let $\mathbf{s}$ be a partition of length k, N a positive integer. We define the *symmetrized multiple harmonic sum* by

$$\mathscr{H}_N(\mathbf{s}) = \sum_{\mathbf{t} \sim \mathbf{s}} H_N(\mathbf{t}).$$

We have the special cases $\mathscr{H}_N(\{1\}^k) = H_N(\{1\}^k)$ and $\mathscr{H}_N(k) = H_N(k)$, $k, n \in \mathbb{N}$; in these cases, we will prefer the notation $\mathscr{H}$ to emphasize that the sums are symmetrized. If $\mathbf{s} \sim \mathbf{t}$, then $\mathscr{H}_N(\mathbf{s}) = \mathscr{H}_N(\mathbf{t})$, so that we may restrict our attention to the case $\mathbf{s}$ is a partition (i.e., $\mathbf{s} = (s_1, \ldots, s_k)$ with $s_1 \geq \ldots \geq s_k$).

Our study of symmetrized multiple harmonic sums uses the completion of the ring of symmetric functions over $\mathbb{Z}[\frac{1}{2}]$ (see Remark 4.2.2 for a dicussion of this choice of base ring).

Definition 5.1.2. Let $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ denote the completion of the ring of symmetric functions over $\mathbb{Z}[\frac{1}{2}]$ with respect to the degree grading. By the fundamental theorem of elementary symmetric functions, we have an identification

$$\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} = \left(\mathbb{Z}\left[\frac{1}{2}\right]\right)[[e_1, e_2, \ldots]],$$

where e_n is the n-th elementary symmetric function. The topology on this power series ring comes from completing the polynomial ring $\mathbb{Z}[\frac{1}{2}][e_1, e_2, \ldots]$ with respect to the grading $\deg(e_n) = n$. An element of $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is a formal infinite sum

$$\sum_I a_I e^I$$

over multi-indices $I = (i_1, \ldots, i_k, 0, 0, \ldots)$, where $e^I := e_1^{i_1} \ldots e_k^{i_k}$. The topology has a neighborhood basis of 0 consisting of the ideals

$$\left\{ \sum_I a_I e^I : a_I = 0 \text{ if } i_1 + 2i_2 + \ldots + ki_k < n \right\}.$$

Recall that in Chapter 4, we considered $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, which is the set of formal infinite sums

$$\sum_{\mathbf{s}=(s_1,\ldots,s_k)} \alpha_{\mathbf{s}} z_{s_1} \ldots z_{s_k},$$

where the summation is taken over all compositions $\mathbf{s}$, and the coefficients $\alpha_{\mathbf{s}}$ are in $\mathbb{Z}[\frac{1}{2}]$. We also defined, in Section 4.1.1, a commutative product $*$ on $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, called the stuffle product, so that the commutative ring $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ is ismorphic to the completion of the ring of quasi-symmetric functions over $\mathbb{Z}[\frac{1}{2}]$. The fundamental theorem of elementary symmetric functions implies that we can identify $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ with the closed subring of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) = \mathrm{QSym}_{\mathbb{Z}[\frac{1}{2}]}$ consisting of the symmetric functions, where $e_n \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is identified with $z_1^n \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$.

Definition 5.1.3. For each odd prime p, define a continuous ring map

$$\begin{aligned} \varphi_p : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} &\to \mathbb{Z}_p \\ e_n &\mapsto p^n \mathscr{H}(\{1\}^n). \end{aligned}$$

We let $\varphi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to \prod_{p\geq 3} \mathbb{Z}_p$ be the product of these maps, and we call φ the *symmetric universal evaluation map*. This map is just the restriction to $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \subset \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$ of the universal evaluation map ϕ defined in Chapter 4. For $n \in \mathbb{Z}_{>0}$, we get an ideal

$$\mathscr{J}_n := \{\alpha \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} : \varphi_p(\alpha) \in p^n\mathbb{Z}_p \text{ for all sufficiently large primes } p\}.$$

5.2 Results

In this section we state our results concerning symmetrized multiple harmonic sums. These results are proven later in this chapter. We have two main results.

5.2.1 Description of the ideals $\ker(\varphi)$ and $\mathscr{J}_n$

Our first result is a description of the ideals $\ker(\varphi)$ and $\mathscr{J}_n$, for $n = 0, 1, 2, \ldots$. The following definition is used in our description of $\mathscr{J}_n$.

Definition 5.2.1. We define a non-Archimedean valuation v on $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ to be trivial on $\mathbb{Z}\left[\frac{1}{2}\right]$, and given by

$$v(e_n) = \begin{cases} n+1 & \text{if } n \text{ even}, \\ n+2 & \text{if } n \text{ odd}, \end{cases}$$

extended multiplicatively to monomials. Denote by $\mathscr{I}_n$ the ideal consisting of those $\alpha \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ for which $v(\alpha) \geq n$.

This valuation is motivated by the congruences for multiple harmonic sums given as Proposition 2.3.1, which imply that for $n \geq 0$, $v_p(p^n\mathscr{H}(\{1\}^n)) \geq v(e_n)$ holds for all sufficiently large primes p. The topology on $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is generated by v.

We can now describe a large class of elements in the ideals $\ker(\varphi)$ and $\mathscr{J}_n$.

Theorem 5.2.2. *For $n = 0, 1, 2, \ldots$, let*

$$\alpha_n := e_n + \sum_{k\geq n} (-1)^{k+1} \binom{k}{n} e_k \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}.$$

Then $\alpha_n \in \ker(\varphi)$, and we have

$$\ker(\varphi) \supset \overline{(\alpha_0, \alpha_1, \ldots)}.$$

For all $n \geq 0$, we have

$$\mathscr{J}_n \supset (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n.$$

Conditionally upon a conjecture of Zhao [41] concerning Bernoulli numbers, the containments of ideals Theorem 1.3.21 are actualy equalities. We state Zhao's conjecture here.

Conjecture 5.2.3 (Nonlinear Bernoulli Nondegeneracy Conjecture)**.** *Let*

$$f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$$

be a homogenous polynomial, where we set $\deg(x_i) = 2i + 1$*. If* f *is non-zero, then there exist infinitely many primes* p *such that* p *does not divide the numerator of*

$$f(B_{p-3}, B_{p-5}, \ldots, B_{p-2n-1}).$$

We show the following:

Theorem 5.2.4. *The Nonlinear Bernoulli Nondegeneracy Conjecture is true if and only if for all* $n \geq 0$*, the second containment is equality:*

$$\mathscr{J}_n = (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n \text{ for all } n \geq 0.$$

These conditions imply that $\ker(\varphi) = \overline{(\alpha_0, \alpha_1, \ldots)}$.

This means, assuming the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture, we have a recipe for writing down *all* congruences among weighted, symmetrized multiple harmon sums, which hold for all sufficiently large primes p. We would like to have a similar description of the kernel of $\phi : \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} \to \prod_{p \geq 3} \mathbb{Z}_p$, and of the ideals $\mathbb{J}_n \subset \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, discussed in Chapter 4.

The elements $\alpha_n \in \ker(\varphi)$ come from the identities

$$p^n \mathscr{H}_{p-1}(\{1\}^n) + \sum_{k \geq n} (-1)^{k+1} \binom{j}{n} p^k \mathscr{H}_{p-1}(\{1\}^k) = 0,$$

holding for all primes $p \geq 3$. This identity was proven in Chapter 2 (it follows from Proposition 2.2.1), where it was used to construct binomial coefficient congruences. This is given below as Proposition 5.3.1.

5.2.2 Elementary symmetric identities and power sum identities

The generators α_n of $\ker(\varphi)$ given in Theorem 5.2.2 come from asymptotic relation among the elementary symmetric multiple harmonic sums. The Asymptotic Reflection Theorem 4.3.1 implies a similar family of asymptotic relation among the power sum multiple harmonmic sums. Particularly, for n a non-negative integer, taking $\alpha = x^n y$ in Corollary 4.3.3 gives the identity

$$(-1)^n p^{n+1} \mathscr{H}_{p-1}(n+1) + \sum_{k \geq n} \binom{k}{n} p^{k+1} \mathscr{H}_{p-1}(k+1) = 0,$$

which holds for all primes p. To write down the corresponding elements of $\ker(\varphi)$, we make the following definition.

Definition 5.2.5. Let $\mathbf{s} = (s_1, \ldots, s_m)$ be a composition. The elementary symmetric functions generate the ring of symmetric functions, and we define $\theta_{\mathbf{s}}(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$ to be the unique polynomial such that

$$\sum_{(t_1,\ldots,t_k)\sim \mathbf{s}} \left(\sum_{i_1 > \ldots > i_k} x_{i_1}^{t_1} \ldots x_{i_k}^{t_k} \right) = \theta_{\mathbf{s}}(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x})),$$

where $e_n(\mathbf{x})$ is the n-th the elementary symmetric in $\mathbf{x} = (x_1, x_2, \ldots)$. We set

$$h(\mathbf{s}) = \theta_{\mathbf{s}}(e_1, \ldots, e_n) \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}.$$

Now, Corollary 4.3.3 implies that the elements

$$\beta_n := (-1)^n h(n+1) + \sum_{k \geq n} \binom{k}{n} h(k+1)$$

are in $\ker(\varphi)$ for $n = 0, 1, \ldots$.

The second result of this chapter, which is combinatorial in nature, says that the elements $\alpha_n \in \ker(\varphi)$ can be obtained, in an appropriate sense, from the elements β_n. In particular, this implies that if the Nonlinear Bernoulli Nondegeneracy Conjecture is true, the p-adic Reflection Theorem 4.3.1 is sufficient to determine $\ker(\varphi) = \ker(\phi) \cap \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$. To make this precise, we give the following definition.

Definition 5.2.6. An ideal $I \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is called *absolutely closed* if I is closed, and for all $r \in \mathbb{Z}_{>0}$ and $\alpha \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, we have $r\alpha \in I \Rightarrow \alpha \in I$. If $I \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is any ideal, we

define $\widetilde{I}$ to be the intersection of all absolutely closed ideals containing I, and call $\widetilde{I}$ the *absolute closure* of I. It is an asbolutely closed ideal.

We can now state our next result.

Theorem 5.2.7. *For $n = 0, 1, \ldots$, let $\alpha_n, \beta_n \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ be given by*

$$\alpha_n = e_n + \sum_{k \geq n} (-1)^{k+1} \binom{k}{n} e_k,$$

$$\beta_n = (-1)^n h(n+1) + \sum_{k \geq n} \binom{k}{n} h(k+1).$$

Let J_α, $J_\beta \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ be the ideals generated by the α_n and β_n, respectively. Then we have

$$\widetilde{J_\alpha} = \widetilde{J_\beta}.$$

This Theorem implies that $\alpha_n \in \widetilde{J_\beta}$ for all n, and assuming the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture, that $\ker(\varphi) = \widetilde{J_\beta}$.

5.3 Identities and congruences for elementary symmetric sums

In this section, we consider the elementry symmetric multiple harmonic sums $\mathscr{H}_{p-1}(\{1\}^n)$, with p and odd prime and n a positive integer. We have the following family of identities among these sums, which were used extensively in Chapter 2. These identities follow from Proposition 2.2.1.

Proposition 5.3.1. *Let p be an odd prime. For every non-negative integer n, we have:*

$$p^n \mathscr{H}_{p-1}(\{1\}^n) + \sum_{i \geq n} (-1)^{i+1} \binom{i}{n} p^i \mathscr{H}_{p-1}(\{1\}^i) = 0.$$

The above sum is finite (terms vanish when $i \geq p$).

We also recall the following congruences for the elementary symmetric sums $\mathscr{H}_{p-1}(\{1\}^n)$ in terms of Bernoulli numbers, given by Zhao in [40]:

Proposition 5.3.2. *Let p be a fixed odd prime, and n an integer with $1 \leq n \leq p-3$. Then we have*

$$\mathscr{H}_{p-1}(\{1\}^n) \equiv \begin{cases} \frac{-1}{n+1} B_{p-1-n}\ p & (\text{mod } p^2) \text{ if } n \text{ is even,} \\ \frac{-(n+1)}{2(n+2)} B_{p-2-n}\ p^2 & (\text{mod } p^3) \text{ if } n \text{ is odd.} \end{cases}$$

5.4 Generation of the ideals $\ker(\varphi)$ and $\mathscr{J}_n$

In this section, we prove Theorems 5.2.2 and 5.2.4. We begin with two lemmas.

Lemma 5.4.1. *Let n be a positive integer. Define a grading on the polynomial ring $\mathbb{Z}[\frac{1}{2}][x_1, \ldots, x_n]$ by $\deg(x_i) = 2i + 1$. Suppose $f(x_1, \ldots, x_n) \neq 0 \in \mathbb{Z}[\frac{1}{2}][x_1, \ldots, x_n]$ is homogeneous of degree d. Then*

$$v_p(\phi_p(f(e_2, e_4, \ldots, e_{2n}))) \geq d$$

for all sufficiently large primes p. If we assume the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture, then equality holds for infinitely many p.

Proof. By Proposition 5.3.2 and the definition of v, we have

$$\phi_p(f(e_2, \ldots, e_{2n})) \equiv p^d f\left(\frac{-B_{p-3}}{3}, \ldots, \frac{-B_{p-2n-1}}{2n+1}\right) \mod p^{d+1}$$

for $p \geq 2n + 3$. The result now follows by applying the Nonlinear Bernoulli Nondegeneracy Conjecture to

$$f\left(\frac{-x_1}{3}, \frac{-x_2}{5}, \ldots, \frac{-x_n}{2n+1}\right).$$

□

Lemma 5.4.2. *Let n be a positive integer. Then $\varphi_p(Is_n) \subset p^n\mathbb{Z}_p$ for all primes $p \geq 3n$.*

Proof. Suppose $\alpha \in \mathscr{I}_n$. We put a grading on the polynomial ring $\mathbb{Z}[\frac{1}{2}][x_1, x_2, \ldots]$ as in the statement of Lemma 5.4.1. Extracting terms of low degree, we find that there are polynomials $f_n, f_{n+1}, \ldots, f_{3n-1} \in \mathbb{Z}[\frac{1}{2}][x_1, x_2, \ldots]$ with $\deg(f_i) = i$, so that

$$\alpha = \sum_{i=n}^{3n-1} f_i(e_1, e_2, \ldots) + \alpha',$$

with $\alpha' \in \mathscr{I}_{3n}$. For $n \leq i \leq 3n - 1$, the fact that $\varphi_p(f_i) \in p^n\mathbb{Z}_p$ for sifficiently large p follows from Lemma 5.4.1. The fact that $\varphi_p(\alpha') \in p^n\mathbb{Z}_p$ for all p follows from the definition of φ_p and the fact that

$$v(e_1^{a_1} \cdot \ldots \cdot e_k^{a_k}) \geq 3n \Rightarrow 1 \cdot a_1 + \ldots + k \cdot a_k \geq n.$$

□

Proof of Theorem 5.2.2. First we show that $\mathscr{J}_n \supset (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$ for all $n \geq 0$. This follows from the fact that the elements α_i are in $\ker(\phi)$ by Proposition 5.3.1, and $\mathscr{I}_n \subset \mathscr{J}_n$ by Lemma 5.4.2.

As the kernel of a continuous map, $\ker(\varphi)$ is closed. Along with the fact that $\alpha_n \in \ker(\varphi)$ for all n, this implies

$$\ker(\varphi) \supset \overline{(\alpha_0, \alpha_1, \ldots)}.$$

□

Proof of Theorem 5.2.4. First we show that the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture implies $\mathscr{J}_n = (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$ for all $n \geq 0$. Suppose, for the sake of contradiction, there is some $\gamma \in \mathscr{J}_n$ such that $\gamma \notin (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$. We will chose a coset representative for $\gamma \mod (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$. Since $\mathscr{I}_n$ contains all terms of high degree, we can choose our representative to be a polynomial in $e_1, e_2, \ldots, e_n$. For every non-negative integer m, we have

$$\frac{\alpha_{2m+1}}{2} = e_{2m+1} + \sum_{k \geq 2m+2} \frac{(-1)^{k+1}}{2} \binom{k}{2m+1} e_k.$$

Using this, we can choose a coset representative which does not involve e_k for k odd. This means that we can find a polynomial $f(x_1, x_2, \ldots) \in \mathbb{Z}[\frac{1}{2}][x_1, x_2, \ldots]$ satisfying

$$\gamma \equiv f(e_2, e_4, \ldots) \mod (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n.$$

We have already concluded that $(\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n \subset \mathscr{J}_n$, so this implies $f(e_2, e_4, \ldots) \in \mathscr{J}_n$. The hypothesis on γ implies $f(e_2, e_4, \ldots) \notin \mathscr{I}_n$. Let us grade the polynomial ring $\mathbb{Z}[\frac{1}{2}][x_1, x_2, \ldots]$ by $\deg(x_i) = 2i + 1$. For $k = 0, 1, \ldots$, write $f_k(x_1, x_2, \ldots)$ for the homogeneous componenet of f of degree k. Let d be minimal with the property that $f_d \neq 0$; we have that $d \leq n - 1$. Now, assuming the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture, Lemma 5.4.1 implies that

$$v_p(f(e_2, e_4, \ldots)) = v_p(f_d(e_2, e_4, \ldots)) = d < n$$

for infinitely many primes p, contradicting the fact that $f(e_2, e_4, \ldots) \in \mathscr{J}_n$. This completes the proof of the fact that the Nonlinear Bernoulli Nondegeneracy Conjecture implies $\mathscr{J}_n = (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$ for all $n \geq 0$.

Next, we show that $\mathscr{J}_n = (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$ implies the truth of the Nonlinear Bernoulli Nondegeneracy Conjecture. Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$ be non-zero and homogeneous of degree n as in the statement of the Nonlinear Bernoulli Nondegeneracy Conjecture (where we set $\deg(x_i) = 2i + 1$. The coset representative γ above was unique, which implies that

$$f(e_2, e_4, \ldots) \notin (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_{n+1}.$$

By hypothesis, this means $f(e_2, \ldots) \notin \mathscr{J}_n$, so that

$$p^{n+1} \nmid f(p^2 H_{p-1}(\{1\}^2, p^4 H_{p-1}(\{1\}^4), \ldots)$$

for infinitely many primes p. It follows from Proposition 5.3.2 that

$$p \nmid f(B_{p-3}, B_{p-5}, \ldots)$$

for infinitely many primes p.

Finally we show that $\mathscr{J}_n = (\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n$ for all n implies $\ker(\varphi) = \overline{(\alpha_0, \alpha_1, \ldots)}$. We have

$$(\alpha_0, \alpha_1, \ldots) \subset \ker(\varphi) \subset \bigcap_{n=0}^{\infty} \mathscr{J}_n = \bigcap_{n=0}^{\infty} \Big((\alpha_0, \alpha_1, \ldots) + \mathscr{I}_n \Big) = \overline{(\alpha_0, \alpha_1, \ldots)},$$

where the last equality holds because the $\mathscr{I}_n$ are a neighborhood basis of 0. Now the fact that $\ker(\varphi)$ is closed completes the proof. □

5.5 A category of complete topological rings

We now move towards the proof of Theorem 5.2.7. We will need to establish some facts about $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$. The ring $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is a complete topological $\mathbb{Z}[\frac{1}{2}]$-algebra. We define a category in which $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ is an object.

Definition 5.5.1. Let cRing denote the category whose class of objects consists of commutative topological $\mathbb{Z}[\frac{1}{2}]$-algebras R that satisfy the following properties:

1. Every Cauchy sequence in R has a unique limit.

2. There is a countable neighborhood basis of 0 in R consisting of open ideals.

3. R is torsion-free as a $\mathbb{Z}\left[\frac{1}{2}\right]$-module.

Morphisms in cRing are continuous $\mathbb{Z}\left[\frac{1}{2}\right]$-algebra maps.

To verify condition 2 for the ring $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, we note that $\mathscr{I}_n$ $(n = 0, 1, \ldots)$ are a neighborhood basis of 0. We also make the following definition regarding formal power series over a ring $R \in$ cRing:

Definition 5.5.2. Let $R \in$ cRing be given. A formal power series

$$f(T) = \sum_{n \geq 0} r_n T^n \in R[[T]]$$

is called *quasi-acceptable* if the following conditions hold:

1. r_n is topologically nilpotent for all $n \geq 1$ (that is, for each n, $r_n^j \to 0$ as $j \to \infty$).
2. $r_n \to 0$ as $n \to \infty$.
3. $r_0 - 1$ is topologically nilpotent

The series $f(T)$ is called *acceptable* if in place of (3) we have the stronger condition

(3') $r_0 = 1$.

Let $\tilde{F} :$ cRing $\to$ Set be the functor taking a ring R to the set of quasi-acceptable power series over R. Likewise, let $F :$ cRing $\to$ Set take R to the set of acceptable power series over R.

We remark that, for any $R \in$ cRing, both $\tilde{F}(R)$ and $F(R)$ are *subgroups* of $R[[T]]^\times$. Next we show that the functor F is represented by $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$.

Proposition 5.5.3. *There is a natural isomorphism of functors* $\mathrm{Hom}(\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}, \_\_) \to F$*, taking a continuous morphism* $\psi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ *to the series*

$$f_\psi(T) := 1 + \sum_{n \geq 1} \psi(e_n) T^n \in F(R).$$

Proof. Let $\psi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ be given, and set $r_n = \psi(e_n)$, $n = 1, 2, \ldots$. Now, for every $n \geq 1$, $\lim_i e_n^i = 0$ in $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, so by continuity $\lim_i r_n^i = 0$ in R, i.e., r_n is topologically nilpotent. Additionally, $\lim_n e_n = 0$ in $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, so $\lim_n r_n = 0$ in R. This proves that

$$1 + \sum_{n \geq 1} r_n T^n \in F(R)$$

To show that this natural transformation is in fact an isomorphism, we construct its inverse. Let

$$1 + \sum_{n \geq 1} r_n T^n \in F(R)$$

be given. Define a map $\psi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ as follows: for $\alpha = \sum_I a_I x^I \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, set

$$\psi(\alpha) = \sum_I a_I r^I,$$

where $r^I = r_1^{i_1} r_2^{i_2} \dots$ and the sum suns over multi-indices $I = (i_1, i_2, \dots)$. The fact that the r_i are topologically nilpotent and that $r_n \to 0$ implies that $r^I \to 0$ (in the sense that, for any neighborhood U of 0 in R, $r^I \in U$ for all but finitely-many I). The completeness of R, along with the fact that the topology on R has a basis consisting of $\mathbb{Z}[\frac{1}{2}]$-submodules (in fact, ideals) now implies that the above sum converges, so ψ is well-defined. It is evident that ψ is a morphism of topological rings, and by construction we have $\psi(e_i) = r_i$. Finally, to see that the association $\psi \leftrightarrow 1 + \sum_{n \geq 1} r_n T^n$ is bijective, we note that if two morphisms $\psi, \psi' : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ satisfy $\psi(e_i) = \psi'(e_i)$ for all i, then ψ and ψ' agree on the dense subring $\mathbb{Z}\left[\frac{1}{2}\right][e_1, e_2, \dots]$ of $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$, and hence are identical. □

We make the following definition:

Definition 5.5.4. For $R \in \mathrm{cRing}$ and $f(T) \in F(R)$, we will write ψ_f for the corresponding morphism $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$. Similarly, if $\psi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$, we will write $f_\psi(T)$ for the corresponding element of $F(R)$.

Remark 5.5.5. For any ring $R \in \mathrm{cRing}$, the set $F(R)$ of acceptable power series over R is a abelian group under multiplication. This abelian group structure comes from a co-commutative Hopf algebra structure on the ring of symmetric functions. The ring of quasi-symmetric functions also has a Hopf algebra structure, which is not co-commutative. See [16] for a description.

Consider the product ring

$$R_2 := \prod_{p \text{ odd}} \mathbb{Z}_p.$$

This ring is a $\mathbb{Z}[\frac{1}{2}]$-algebra which is complete with respect to the topology generated

a neighborhood basis of 0 consisting of the ideals

$$\prod_{3\leq p\leq n} p^n\mathbb{Z}_p \times \prod_{p>n} \mathbb{Z}_p \subset R_2,$$

so $R_2 \in \mathrm{cRing}$. We can identify R_2 with the profinite completion of $\mathbb{Z}\left[\frac{1}{2}\right]$.

By Proposition 5.5.3, the symmetric universal evaluation map $\varphi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R_2$ gives an acceptable power series $f_\varphi \in R_2[[T]]$. Our investigation of formal p-adic relations among symmetrized multiple harmonic sums will hinge on the study of the series f_φ. In particular, we will show that f_φ satisfies a functional equation.

5.5.1 Operations on power series

The functional equation for $f_\varphi(T)$ relates T and $-1-T$ (and is therefore symmetric about $T = \frac{-1}{2}$). To motivate our next definition, we take $R \in \mathrm{cRing}$, $f(T) \in R[[T]]$, and we formally compute $f(-1-T)$:

$$\begin{aligned} f(-1-T) &= \sum_{n\geq 0} r_n(-1-T)^n \\ &= \sum_{n\geq 0}(-1)^n r_n \sum_{j=0}^{n} \binom{n}{j} T^j \\ &= \sum_{j\geq 0} a_j T^j, \end{aligned}$$

where

$$a_n = \sum_{j\geq n}(-1)^j \binom{j}{n} r_j. \tag{5.1}$$

If $r_n \to 0$, the the sum giving a_n converges in R, and we only define $f(-1-T)$ if this is the case. We make the following definitions:

Definition 5.5.6. Suppose $R \in \mathrm{cRing}$. We denote by $R\{T\}$ the set of power series

$$f(T) = \sum_{n\geq 0} r_n T^n \in R[[T]]$$

satisfying $r_n \to 0$. We topologize $R\{T\}$ by taking as a neighborhood basis of 0 sets of the for $U\{T\}$, where U is a neighborhood of 0 in R. For $f(T) \in R\{T\}$, we define a power series

$$(Sf)(T) = \sum_{n\geq 0} a_n T^n \in R[[T]]$$

by

$$a_n = \sum_{j \geq n} (-1)^j \binom{j}{n} r_j$$

When no ambiguity can arrise, we will abbreviate $(Sf)(T)$ by $f(-1-T)$.

Next, we prove some basic properties about the series $f(-1-T)$.

Proposition 5.5.7. *Let $R \in \mathrm{cRing}$, $f(T) = \sum r_n T^n \in R[[T]]$ be given, with $r_n \to 0$. Then:*

1. *The map $S : R\{T\} \to R\{T\}$ is an involution of R-algebras.*
2. *If $f(T) \in R\{T\}$, then $f'(T) \in R\{T\}$, and*

$$\left(\frac{d}{dT}\right)(Sf)(T) = -(Sf')(T)$$

3. *If $f(T)$ is acceptable, then $f(-1-T)$ is quasi-acceptable.*

Proof. (1,2) To begin, we first note that S is additive. Next, if $r_n \to 0$, then

$$a_n = \sum_{j \geq n} (-1)^j \binom{j}{n} r_j \to 0,$$

so that S takes $R\{T\}$ to $R\{T\}$. Next, we note that S is continuous: if $U \subset R$ is an open ideal containing 0, then $S^{-1}(U\{T\}) \supset U\{T\}$. Since such $U\{T\}$ are a local basis at 0, it follows that S is continuous. Now, statements (1) and (2) of the proposition obviously hold for the restriction of S to $R[T]$. Finally, $R[T]$ is dense in $R\{T\}$, so we are done.

(3) Clear from the definition of (quasi-)acceptable

□

5.5.2 Computations involving the elements α_n and β_n

The polynomials $\theta_{[n]}$ given in Definition 5.2.5 have an explicit description, which we give here.

Proposition 5.5.8. *Define a formal power series*

$$f(T) = 1 + \sum_{n \geq 1} y_n T^n,$$

with $y_1, y_2, \ldots$ indeterminates. Then, we have

$$\frac{f'(T)}{f(T)} = \sum_{n\geq 0}(-1)^n \theta_{n+1}(y_1, \ldots, y_{n+1})T^n$$

Proof. By the definition of θ_{n+1}, it suffices to show that if $f(T) = 1 + \sum_{n\geq 1} e_n T^n$ as a power series over the ring of symmetric functions (in the variables $x_1, x_2, \ldots$, say), then

$$\frac{f'(T)}{f(T)} = \sum_{n\geq 0}(-1)^n p_{n+1} T^n,$$

where e_n and p_n are the elementary and power sum symmetric functions, respectively. We have a factorization

$$f(T) = \prod_{n=1}^{\infty}(1 + x_n T),$$

from which we can compute

$$\begin{aligned}
\frac{f'(T)}{f(T)} &= \sum_{n=1}^{\infty} \frac{x_n}{1 + x_n T} \\
&= \sum_{n=1}^{\infty} x_n - x_n^2 T + x_n^4 T^2 - \ldots \\
&= \sum_{k=0}^{\infty}(-1)^k p_{k+1} T^k.
\end{aligned}$$

□

The following Proposition gives a concise way of describing the elements α_n, $\beta_n \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$. We consider the 'universal' acceptable series $f_{\mathrm{Id}} \in F(\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]})$, given by

$$f_{\mathrm{Id}}(T) = 1 + \sum_{n\geq 1} e_n T^n.$$

When $g(T)$ is an arbitrary power series, we denote by $[g(T)]_n$ the coefficient of T^n in g.

Proposition 5.5.9. *Let $f_{\mathrm{Id}}(T) \in F(\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]})$ be as above. Then, we have*

$$\alpha_n = \left[\tilde{f}(T) - \tilde{f}(-1 - T)\right]_n$$

and

$$\beta_n = \left[\frac{\tilde{f}'}{\tilde{f}}(T) + \frac{\tilde{f}'}{\tilde{f}}(-1 - T)\right]_n$$

The first few values of $\theta_{[n]}$ are:

$$\begin{aligned}
\theta_1(y_1) &= y_1 \\
\theta_2(y_1, y_2) &= y_1^2 - 2y_2 \\
\theta_3(y_1, y_2, y_3) &= y_1^3 - 3y_1y_2 + 3y_3 \\
\theta_4(y_1, y_2, y_3, y_4) &= y_1^4 - 4y_1^2y_2 + 4y_1y_3 + 2y_2^2 - 4y_4
\end{aligned}$$

As an example, we can use the above to compute the first few terms of β_0:

$$\begin{aligned}
\beta_0 &\equiv 2h(1) + h(2) + h(3) + h(4) \mod \mathscr{I}_7 \\
&\equiv 2e_1 + e_1^2 - 2e_2 - 3e_1e_2 + 2e_2^2 + 3e_3 - 4e_4 \mod \mathscr{I}_7
\end{aligned}$$

and of β_1:

$$\begin{aligned}
\beta_1 &\equiv 2h(3) + 3h(4) \mod \mathscr{I}_7 \\
&= -6e_1e_2 + 6e_2^2 + 6e_3 - 12e_4 \mod \mathscr{I}_7
\end{aligned}$$

5.6 More on complete topological rings

Recall that an ideal $I \subset R$, with $R \in \mathrm{cRing}$, is called *absolutely closed* if I is closed, and for all $\alpha \in R$, $r \in \mathbb{Z}_{>0}$, we have $r\alpha \in I \to \alpha \in I$. We denote by $\widetilde{I}$ the intersection of all absolutely closed ideals containing I.

Proposition 5.6.1. *We have the following:*

1. *If $R \in \mathrm{cRing}$, $I \subset R$, then $\widetilde{I}$ is absolutely closed, and it is the smallest absolutely closed ideal containing I.*
2. *If $R, S \in \mathrm{cRing}_0$, and $f : R \to S$ is a morphism, then $\ker(f)$ is absolutely closed*
3. *If $R \in \mathrm{cRing}$, and $I \subset R$ is closed, then $R/I \in \mathrm{cRing}$. If I is absolutely closed, then $R/I \in \mathrm{cRing}$.*

Proof. 1. This follows immediately from the fact that intersections of closed (resp. relatively $\mathbb{Z}$-divisible) ideals is closed (resp. relatively $\mathbb{Z}$-divisible).

2. First, we have $\ker(f) = f^{-1}(\{0\})$ is closed. Also, if $r \in R$, $n \in \mathbb{Z}_{>0}$ satisfy $nr \in \ker(f)$, then $f(nr) = nf(r) = 0$. Because S is torsion-free, this implies $f(r) = 0$, i.e., $r \in \ker(f)$.

3. Ler $\pi : R \to R/I$ be the projection map. Clearly R/I is a commutative topological $\mathbb{Z}\left[\frac{1}{2}\right]$-algebra (in the quotient topology). Let $U_1, U_2, \ldots \subset R$ be a countable neighborhood basis of 0 consisting of open ideals. Suppose $\tilde{r}_1, \tilde{r}_2, \ldots \in R/I$ is a Cauchy sequence. For each positive integer i, $\pi(U_i + I)$ is an open neighborhood of 0 in R/I, so we can find a sequence $N_1 < N_2 < \ldots$ of positive integers such that $\tilde{r}_n - \tilde{r}_{n+1} \in \pi(U_i + I)$ for all $n > N_i$. Choose $r_1, r_2, \ldots \in R$ such that $\pi(\tilde{r}_n) = r_n$. For n a positive integer, define

$$i(n) = \max\{i : N_i < n\}$$

Now, for each n, $\tilde{r}_{n+1} - \tilde{r}_n \in U_{i(n)} + I$, so we may choose $u_n \in U_{i(n)}$, $j_n \in I$ with $\tilde{r}_{n+1} - \tilde{r}_n = u_n + j_n$. Define

$$s_n = \tilde{r}_n - \sum_{i=1}^{n-1} j_i$$

We then check that $s_{n+1} - s_n = u_n \to 0$ in R. Because the U_i are closed under addition, this implies that s_n is a Cauchy sequence in R, which must converges to some $s \in R$. Because π is continuous, it follows that $\tilde{r}_n \to \pi(s)$. This shows that every Cauchy sequence in R/I has a limit. Because I is closed, $\{0\}$ is closed in R/I. In any topological group, the identity is closed if and only if the group is Hausdorff. This implies that the limit of a Cauchy sequence in R/I is unique.

□

5.6.1 Sets of acceptable power series defined by ideals

Recall that F : cRing $\to$ Set is the functor taking $R \in$ cRing to the set of acceptable power series over R.

Definition 5.6.2. Let $I \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ be any ideal. If R is an object of cRing, we define $\mathbb{V}(I)(R) \subset F(R)$ by

$$\mathbb{V}(I)(R) = \{f(T) \in F(R) : I \subset \ker(\psi_f)\},$$

where $\psi_f : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ which corresponds (via the isomorphism of Proposition 5.5.3) to the set of morphisms $\psi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ with $I \subset \ker(\psi)$.

Our next proposition shows the extent to which to functor $R \mapsto \mathbb{V}(I)(R)$ determines the ideal I.

Proposition 5.6.3. *Let I_1, $I_2 \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ be ideals. Then, we have*

$$\mathbb{V}(I_1)(R) \subset \mathbb{V}(I_2)(R) \text{ for all } R \in \mathrm{cRing} \Leftrightarrow \widetilde{I_1} \supset \widetilde{I_2},$$

Interchanging the roles of I_1 and I_2, we also have

$$\mathbb{V}(I_1)(R) = \mathbb{V}(I_2)(R) \text{ for all } R \in \mathrm{cRing} \Leftrightarrow \widetilde{I_1} = \widetilde{I_2}$$

Proof. The kernel of any morphism in cRing is absolutely closed, so for every $R \in$ cRing, we can identify maps $\psi : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]} \to R$ satisfying $I_i \subset \ker(\psi)$ with maps $\psi' : \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}/I_i \to R$. In other words, the ring $\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}/\widetilde{I_i}$ represents the functor $\mathbb{V}(I_i)(\_\_) : \mathrm{cRing} \to \mathrm{Set}$. Now, using the Yoneda lemma, we have

$$\begin{aligned}
\forall R : \mathbb{V}(I_1)(R) \subset \mathbb{V}(I_2)(S) \quad &\Leftrightarrow \quad \exists \eta : \mathbb{V}(I_1)(__) \to \mathbb{V}(I_2)(__) \\
&\qquad \text{commuting with } \mathbb{V}(I_i)(__) \to F(__) \\
&\Leftrightarrow \quad \exists \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}\text{-algebra morphism } \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}/\widetilde{I_2} \to \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}/\widetilde{I_1} \\
&\Leftrightarrow \quad \widetilde{I_1} \supset \widetilde{I_2}
\end{aligned}$$

□

5.7 Proof of Theorem 5.2.7

Recall that, for $n = 0, 1, \ldots$, we defined elements $\alpha_n, \beta_n \in \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ by

$$\alpha_n = e_n + \sum_{k \geq n} (-1)^{k+1} \binom{k}{n} e_k,$$

$$\beta_n = (-1)^n h(n+1) + \sum_{k \geq n} \binom{k}{n} h(k+1).$$

We also defined ideals J_α, $J_\beta \subset \hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ to be generated by the α_n and β_n, respectively. The assertion of Theorem 5.2.7 is then that

$$\widetilde{J_\alpha} = \widetilde{J_\beta}.$$

We begin with a lemma.

Lemma 5.7.1. *Let $R \in$ cRing, $f(T) \in F(R)$ be given. Then $f(T) = f(-1-T)$ if and only if*

$$\frac{f'}{f}(T) = -\frac{f'}{f}(-1-T).$$

Proof of Theorem 5.2.7. By Proposition 5.6.3, it suffices to show that $\mathbb{V}(J_\alpha)(R) = \mathbb{V}(J_\beta)(R)$ for all $R \in$ cRing.

Suppose $f(T) = \sum_n r_n T^n \in F(R)$. We can express the condition $f(T) \in \mathbb{V}(J_\alpha)(R)$ as relation between $f(T)$ and $f(-1-T)$:

$$\begin{aligned} f(T) \in \mathbb{V}(J_\alpha)(R) &\Leftrightarrow \alpha_n \in \ker(\psi_f)\ \forall n \\ &\Leftrightarrow s_n + \sum_{j \geq n} (-1)^{j+1} \binom{j}{n} r_j = 0\ \forall n \\ &\Leftrightarrow f(T) = f(-1-T) \end{aligned}$$

We also have a similar relation for $\mathbb{V}(B)(S)$. Using Proposition 5.5.8, we have

$$\frac{f'}{f}(-1-T) = \sum_{n \geq 0} a_n T^n,$$

where

$$a_n = \sum_{j \geq n} \binom{j}{n} \theta_{[n+1]}(r_1, \ldots, r_{n+1})$$

or equivalently,

$$a_{n-1} = \sum_{j \geq n} \binom{j-1}{n-1} \theta_{[n]}(s_1, \ldots, s_n)$$

Now, we can say:

$$\begin{aligned} f(T) \in \mathbb{V}(B)(S) &\Leftrightarrow \beta_n \in \ker(\psi_f)\ \forall n \\ &\Leftrightarrow \theta_{[n]}(r_1, \ldots, r_n) + (-1)^{n+1} \sum_{j \geq n} \binom{j-1}{n-1} \theta_{[j]}(r_1, \ldots, r_j = 0)\ \forall n \\ &\Leftrightarrow \frac{f'}{f}(T) = -\frac{f'}{f}(-1-T) \end{aligned}$$

To finish the proof, we only need to show that, for acceptable $f(T)$, we have

$$f(T) = f(-1-T) \Leftrightarrow \frac{f'}{f}(T) = -\frac{f'}{f}(-1-T)$$

Proposition 5.5.7 implies that.

$$f(T) = f(-1-T) \Rightarrow \frac{f'}{f}(T) = -\frac{f'}{f}(-1-T)$$

For the reverse implication, we first show that, for $g(T)$, $h(T) \in R[[T]]$ quasi-acceptable, we have

$$\frac{g'}{g}(T) = \frac{h'}{h}(T) \Rightarrow \frac{g(T)}{g(0)} = \frac{h(T)}{h(0)}$$

As a formal power series, we define

$$\log(1+x) = \sum_{n\geq 1}(-1)^{n+1}\frac{x^n}{n} \in \mathbb{Q}[[x]]$$

Given a power series $g(T) \in R[[T]]$ with constant term 1, we can evaluate $\log(g(T))$ using the above series for log. We will introduce some denominators, so $\log(g(T))$ will actually be a formal power series over the ring $R \otimes \mathbb{Q}$. Note that, in general, $R \otimes \mathbb{Q}$ will no longer be complete. Additionally, $\log(g(T))$ will have constant term 0.

We also have the exponential function, given by the power series

$$\exp(x) = \sum_{n\geq 0}\frac{x^n}{n!} \in \mathbb{Q}[[x]]$$

Given $h(T) \in R[[T]]$ with constant term 0, we can evaluate $\exp(h(T))$, which will be a power series over $S \otimes \mathbb{Q}$ with constant term 1. For $g(T) \in R[[T]]$, we will write $\overline{g}(T)$ for the image of $g(T)$ in $(R \otimes \mathbb{Q})[[T]]$. The fact that $\exp(\log(1+x)) = 1+x$ as power series gives us that, for $g(T) \in R[[T]]$ with constant term 1:

$$\exp(\log(g(T)) = \overline{g}(T) \tag{5.2}$$

Suppose $\frac{g'}{g}(T) = \frac{h'}{h}(T)$. If we take the image of the first equation in $(R \otimes \mathbb{Q})[[T]]$ and rewrite, we get

$$\frac{d}{dT}\log(g(T)/g(0)) = \frac{d}{dT}\log(h(T)/h(0))$$

Since $S \otimes \mathbb{Q}$ is torsion-free, the only power series with derivative 0 are constants, so we get

$$\log(g(T)/g(0)) = \log(h(T)/h(0)) + C \tag{5.3}$$

for some $C \in R \otimes \mathbb{Q}$. Comparing the constant terms on both sides of the equation above, we get that $C = 0$. Exponentiating both sides of (5.3) gives

$$\overline{\left(\frac{g(T)}{g(0)}\right)} = \overline{\left(\frac{h(T)}{h(0)}\right)}$$

Finally, R is torsion-free, so the natural map $R \to R \otimes \mathbb{Q}$ is injective. This implies $\frac{g(T)}{g(0)} = \frac{h(T)}{h(0)}$, as desired.

Now, suppose $\frac{f'}{f}(T) = -\frac{f'}{f}(-1-T)$. Applying the above claim, we conclude that (remembering that $f(0) = 1$):

$$f(T) = \frac{f(-1-T)}{f(-1)}$$

Making the substitution $T \leftrightarrow -1 - T$, we find that

$$f(-1-T) = \frac{f(T)}{f(-1)},$$

so that $f(-1)^2 = 1$. This implies that $\frac{1-f(-1)}{2}$ is idempotent , so that

$$\frac{1-f(-1)}{2} = \left(\frac{1-f(-1)}{2}\right)^n$$

for all $n \geq 1$ (here it is essential that R is a $\mathbb{Z}\left[\frac{1}{2}\right]$-algebra, not just a $\mathbb{Z}$-algebra). Fianlly, Proposition 5.5.7 says that $\frac{1-f(-1)}{2}$ is topologically nilpotent, so we must have $\frac{1-f(-1)}{2} = 0$, i.e., $f(-1) = 1$. We therefore have

$$f(T) = f(-1-T)$$

This completes the proof. $\square$

Appendix

The Ring of Asymptotic Numbers

In this appendix, we define a topological ring $\mathcal{R}_{\mathbb{Q}}$, which we term *the ring of asymptotic numbers*; it is a $\mathbb{Q}$-algebra, and the topology comes from a non-Archimedean metric extending the discrete (trivial) metric on $\mathbb{Q}$. Although we think $\mathcal{R}_{\mathbb{Q}}$ is an interesting ring in its own right, the purpose of this appendix is to discuss the possibility of using $\mathcal{R}_{\mathbb{Q}}$ as a replacement for the ring $\prod_{p\geq 3}\mathbb{Z}_p$ appearing as the target of the (symmetric or not) universal evaluation maps, given in Definitions 4.2.3 and 5.1.3. This replacement will be accompanied by passing from $\mathbb{Z}[\frac{1}{2}]$ coefficients to $\mathbb{Q}$ coefficients in the source ring ($\hat{\Lambda}_{\mathbb{Z}[\frac{1}{2}]}$ or $\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$).

Although we will not make use of it here, it is possible to give a similar definition with $\mathbb{Q}$ replaced by any global field.

A.1 Introduction

In Section 4.2 we utilize the complete topological ring $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$, which we identify with the completion of the ring of quasi-symmetric functions over $\mathbb{Z}[\frac{1}{2}]$. The universal evaluation map, given by Definition 4.2.3, is a continuous ring map

$$\phi : (\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *) \to \prod_{p\geq 3}\mathbb{Z}_p.$$

Under the identification of $(\widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}, *)$ with the ring of quasi-symmetric functions, this map of $\mathbb{Z}[\frac{1}{2}]$-algebras is the product of the maps ϕ_p, where ϕ_p takes the monomial quasi-symmetric function

$$M_{(s_1,\ldots,s_k)} := \sum_{i_1>\ldots>i_k} t_{i_1}^{s_1}\ldots t_{i_k}^{s_k}$$

to the element

$$p^{s_1+\ldots+s_k} H_{p-1}(s_1, \ldots, s_k) \in \mathbb{Z}_p.$$

In Chapter 4 we investigate the kernel of ϕ, as well as the ideals

$$\mathbb{J}_n := \{\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]} : \phi_p(\alpha)) \in p^n \mathbb{Z}_p \text{ for all sufficiently large primes } p\}.$$

Although the universal evaluation map does not extend to $\widehat{\mathfrak{H}}^1_{\mathbb{Q}}$, it is possible to give an ad hoc definition of analogous ideals $\tilde{\mathbb{J}}_n \subset \widehat{\mathfrak{H}}^1_{\mathbb{Q}}$:

$$\tilde{\mathbb{J}}_n := \left\{ \sum_{\mathbf{s}} \alpha_{\mathbf{s}} z_{s_1} \ldots z_{s_k} : \sum_{w(\mathbf{s})<n} \alpha_{\mathbf{s}} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}) \in p^n \mathbb{Z}_p \text{ for all sufficiently large } p \right\}.$$

Below, we define a topological ring $\mathcal{R}_{\mathbb{Q}}$, and we propose an *asymptotic evaluation map* $\tilde{\phi} : \widehat{\mathfrak{H}}^1_{\mathbb{Q}} \to \mathcal{R}_{\mathbb{Q}}$, which is a continuous ring map. The ring $\mathcal{R}_{\mathbb{Q}}$ has a countable neighborhood basis $\mathcal{R} = I_0 \supset I_1 \supset \ldots$ consisting of ideals, with the property that $\tilde{\phi}^{-1}(I_n) = \tilde{\mathbb{J}}_n$. It is also the case that

$$\ker(\tilde{\phi}) = \bigcap_{n=0}^{\infty} \tilde{\mathbb{J}}_n.$$

We can similarly define a *symmetric asymptotic evaluation map*, related to the symmetric universal evaluation map defined in Chapter 5.

A.2 The ring of asymptotic numbers

We consider the metric spaces $\mathbb{Z}_p$ as p ranges through the primes. We normalize our distance functions $d_p : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}_{\geq 0}$ by $d_p(x, y) = \left(\frac{1}{2}\right)^{v_p(x-y)}$. Let $R = \prod \mathbb{Z}_p$, on which we put the uniform topology: the ideals $I_n := \prod (p^n \mathbb{Z}_p)$ form a neighborhood basis of 0. The topology on R is generated by the metric

$$d((a_p), (b_p)) := \sup_p d_p(a_p, b_p).$$

We call two elements $(a_p), (b_p) \in R$ *asymptotic* if $d_p(a_p, b_p) \to 0$ as $p \to \infty$. The set of elements asymptotic to 0 is a closed ideal of R, which we denote J. We define *the ring of asymptotic numbers* $\mathcal{R}_{\mathbb{Q}} := R/J$ as a ring, on which we put the quotient

topology. We denote by $[(a_p)]$ the class of a sequence $(a_p) \in R$ in the quotient ring $\mathcal{R}$. There is a ring map $\mathbb{Q} \to \mathcal{R}_\mathbb{Q}$, $r \mapsto [(a_p)]$, where

$$a_p = \begin{cases} r : v_p(r) \geq 0, \\ 0 : v_p(r) < 0. \end{cases}$$

Proposition A.2.1. *The ring $\mathcal{R}_\mathbb{Q}$ enjoys the following properties:*

1. *The topology on $\mathcal{R}_\mathbb{Q}$ comes from a metric d, discrete on $\mathbb{Q}$, given by*

$$d([(a_p)], [(b_p)]) = \limsup_{p \to \infty} d_p(a_p, b_p).$$

2. *$\mathcal{R}_\mathbb{Q}$ is complete but not locally compact.*

Proof. 1. The ideals $I_n \subset R$ are a neighborhood basis of 0 for the topology on R, so a neighborhood basis of 0 for the topology on $\mathcal{R}_\mathbb{Q}$ is the images of $I_n + J$ under the quotient map $R \to \mathcal{R}_\mathbb{Q}$. It is straightforward to verify that the open d-ball of radius $\left(\frac{1}{2}\right)^{n-1}$ centered at 0 in $\mathcal{R}_\mathbb{Q}$ is the image of $I_n + J$.

2. This follows from the general fact that the quotient of a complete metrizable topological group by a closed subgroup is complete (see [3], TG IX.25, Proposition 4).

□

A.3 The asymptotic evaluation map

Here we define the *asymptotic evaluation map*, which is a continuous ring map $\tilde{\phi} : (\widehat{\mathfrak{H}}^1_\mathbb{Q}, *) \to \mathcal{R}_\mathbb{Q}$. Let

$$\alpha = \sum_{\mathbf{s}=(s_1,\ldots,s_k)} \alpha_\mathbf{s} z_{s_1} \ldots z_{s_k} \in \widehat{\mathfrak{H}}^1_\mathbb{Q}$$

be given. For each positive integer, we define an element $[(a_p^n)] \in \mathcal{R}_\mathbb{Q}$ by

$$a_p^n := \sum_{w(\mathbf{s})<n} a_\mathbf{s} p^{w(\mathbf{s})} H_{p-1}(\mathbf{s}) \in \mathbb{Z}_p.$$

A direct computation shows that

$$d\left([(a_p^n)],[(a_p^m)]\right) \leq \left(\frac{1}{2}\right)^{\min(m,n)}$$

for positive integers m, n, so that $[(a_p^n)]$ is a Cauchy sequence. We define

$$\tilde{\phi}(\alpha) = \lim_{n\to\infty}[(a_p^n)] \in \mathcal{R}_{\mathbb{Q}}.$$

It is simple to check that $\tilde{\phi}$ is a ring homomorphism, and that

$$\alpha \in \mathbb{I}_n \Rightarrow d\left(\tilde{\phi}(\alpha), 0\right) \leq \left(\frac{1}{2}\right)^n,$$

so that $\tilde{\phi}$ is continuous.

Remark A.3.1. A similar construction yields *symmetric asymptotic evaluation map* $\tilde{\phi} : \hat{\Lambda}_{\mathbb{Q}} \to \mathcal{R}_{\mathbb{Q}}$. The details are omitted.

A.4 Usefulness of the ring of asymptotic numbers

There are two main advantages to using the ring of asymptotic numbers, as opposed to $\prod_{p\geq 3}\mathbb{Z}_p$, as the target of the universal evaluation maps. We discuss these advantages below.

A.4.1 Passage from $\mathbb{Z}[\frac{1}{2}]$ to $\mathbb{Q}$

Our representation of values of p-adic L-function values at positive integers naturally lives in $\widehat{\mathfrak{H}}^1_{\mathbb{Q}}$. More specifically, the identity

$$p^k L_p(k,\omega^{1-k}) = \sum_{n\geq k-2}(-1)^{n+k}\binom{n}{k-2}\frac{B_{n+2-k}}{k-1}p^{n+1}H_{p-1}(n+1),$$

given in Chapter 3 as Equation (3.6), can now be interpretted as the statement that

$$\tilde{\phi}\left(\alpha\right) = \left(p^k L_p(k,\omega^{1-k})\right)_p \in \mathcal{R}_{\mathbb{Q}},$$

where $\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Q}}$ is given by

$$\alpha = \sum_{n\geq k-2}(-1)^{n+k}\binom{n}{k-2}\frac{B_{n+2-k}}{k-1}x^n y.$$

Since $\alpha \notin \widehat{\mathfrak{H}}^1_{\mathbb{Z}[\frac{1}{2}]}$, we have no way of formulating this statement in terms of the universal evaluation map. In fact, the denominator of terms in α contain all primes, so this problem cannot be remedied simply by replacing $\mathbb{Z}[\frac{1}{2}]$ with $\mathbb{Z}[\frac{1}{N}]$ for some integer N.

Using $\mathbb{Q}$ coefficients also simplifies the statements of some theorems and conjectures appearing earlier.

A.4.2 Exclusion of finitely-many primes

As an abstract ideal, $\ker(\varphi)$ is quite complicated. It likely cannot be generated by countably many elements. One saving grace is that this ideal is closed, and there is hope that it is the *closure* of a countably generated ideal (as was the case for the kernel of the symmetric universal evaluation map ϕ; see Theorem 5.2.2).

We have seen the identity

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

which holds for $p \geq 3$ but fails for $p = 2$. Although we do not have examples, there may be identities failing for a larger finite set of primes. If there were such identities, then instead of examining $\ker(\phi)$, the right object to study would instead be

$$J := \left\{\alpha \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}} : \phi_p(\alpha) = 0 \text{ for all but finitely many primes } p\right\}.$$

Unlike $\ker(\tilde{\phi})$, J need not be closed.

Proposition A.4.1. *Suppose $p_1 < p_2 < \ldots$ is an infinite sequence of primes, and that $\alpha_{p_1}, \alpha_{p_2}, \ldots \in \widehat{\mathfrak{H}}^1_{\mathbb{Z}}$ satisfy the conditions:*

- *$\phi_p(\alpha_{p_n}) = 0$ for all but finitely many primes p.*
- *$\phi_{p_n}(\alpha_{p_n}) \neq 0$.*

Then the ideal $J \subset (\widehat{\mathfrak{H}}^1_{\mathbb{Z}}, *)$ is not closed.

Proof. Replacing p_n with a larger prime if necessary, we may assume that $\phi_p(\alpha_{p_n}) = 0$ for $p > p_n$. The elements $\alpha_{p_1}, \alpha_{p_2}, \ldots$ are in J by hypothesis, but one checks that

$$\sum_{n\geq 1} y^{p_n - 1} * \alpha_{p_n}$$

is in the closure of J, but not in J itself. □

References

[1] Roger Apéry. Interpolation de fractions continues et irrationalité de certaines constantes. In *Mathematics*, CTHS: Bull. Sec. Sci., III, pages 37–53. Bib. Nat., Paris, 1981.

[2] Charles Babbage. Demonstration of a theorem relating to prime numbers. *The Edinburgh Philosophical Journal*, 1:46–49, 1819.

[3] Nicolas Bourbaki. *Éléments de mathématique. VIII. Première partie: Les structures fondamentales de l'analyse. Livre III: Topologie générale. Chapitre IX: Utilisation des nombres réels en topologie générale.* Actualités Sci. Ind., no 1045. Hermann et Cie., Paris, 1948.

[4] Douglas Bowman and David M. Bradley. The algebra and combinatorics of shuffles and multiple zeta values. *J. Combin. Theory Ser. A*, 97(1):43–61, 2002.

[5] David W. Boyd. A p-adic study of the partial sums of the harmonic series. *Experiment. Math.*, 3(4):287–302, 1994.

[6] Francis Brown. Mixed Tate motives over $\mathbb{Z}$. *Ann. of Math. (2)*, 175(2):949–976, 2012.

[7] Leonard Carlitz. Note on a theorem of Glaisher. *J. London Math. Soc.*, 28:245–246, 1953.

[8] Vladimir Drinfeld. On quasitriangular quasi-Hopf algebras and on a group that is closely connected with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Algebra i Analiz*, 2(4):149–181, 1990.

[9] Leonhard Euler. De summis serierum reciprocarum. *Commentarii academiae scientiarum Petropolitanae*, 7:123–134, 1740.

[10] Herbert Gangl, Masanobu Kaneko, and Don Zagier. Double zeta values and modular forms. In *Automorphic forms and zeta functions*, pages 71–106. World Sci. Publ., Hackensack, NJ, 2006.

[11] J. W. L. Glaisher. Congruences relating to the sums of products of the first n numbers and to other sums and products. *Quart. J. Math.*, 31:2–35, 1899.

[12] J. W. L. Glaisher. On the residues of the sums of the inverse powers of numbers in arithmetical progression. *Quart. J. Math.*, 32:271–288, 1900.

[13] Andrew Granville. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. In *Organic mathematics (Burnaby, BC, 1995)*, volume 20 of *CMS Conf. Proc.*, pages 253–276. Amer. Math. Soc., Providence, RI, 1997.

[14] Michael E. Hoffman. Multiple harmonic series. *Pacific J. Math.*, 152(2):275–290, 1992.

[15] Michael E. Hoffman. The algebra of multiple harmonic series. *J. Algebra*, 194(2):477–495, 1997.

[16] Michael E. Hoffman. Quasi-symmetric functions and mod p multiple harmonic sums. 2004.

[17] Kentaro Ihara, Masanobu Kaneko, and Don Zagier. Derivation and double shuffle relations for multiple zeta values. *Compos. Math.*, 142(2):307–338, 2006.

[18] Kenkichi Iwasawa. *Lectures on p-adic L-functions*. Princeton University Press, Princeton, N.J., 1972. Annals of Mathematics Studies, No. 74.

[19] Masanobu Kaneko and Don Zagier. Finite multiple zeta values. *in preparation*.

[20] Tomio Kubota and Heinrich-Wolfgang Leopoldt. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.*, 214/215:328–339, 1964.

[21] Emma Lehmer. On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson. *Ann. of Math. (2)*, 39(2):350–360, 1938.

[22] Romeo Meštrović. On the mod p^7 determination of $\binom{2p-1}{p-1}$. *Rocky Mountain Journal of Mathematics*, 2012.

[23] Romeo Meštrović. Wolstenholme's theorem: its generalization and extensions in the last hundred and fifty years (1862-2012). 2012.

[24] Yasuo Morita. A p-adic analogue of the Γ-function. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 22(2):255–266, 1975.

[25] Yasuo Morita. A p-adic integral representation of the p-adic L-function. *J. Reine Angew. Math.*, 302:71–95, 1978.

[26] Yasuo Ohno. A generalization of the duality and sum formulas on the multiple zeta values. *J. Number Theory*, 74(1):39–43, 1999.

[27] Khodabakhsh Hessami Pilehrood and Tatiana Hessami Pilehrood. Congruences arising from apéry-type series for zeta values. 2011.

[28] Khodabakhsh Hessami Pilehrood, Tatiana Hessami Pilehrood, and Roberto Tauraso. New properties of multiple harmonic sums modulo p and p-analogues of leshchiner's series. 2013.

[29] Tanguy Rivoal. Séries hypergéométriques et irrationalité des valeurs de la fonction zêta de Riemann. *J. Théor. Nombres Bordeaux*, 15(1):351–365, 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[30] Shingo Saito and Noriko Wakabayashi. The bowman-bradley type theorem for finite multiple zeta values. 2013.

[31] Roberto Tauraso. More congruences for central binomial coefficients. *J. Number Theory*, 130(12):2639–2649, 2010.

[32] Tomohide Terasoma. Mixed Tate motives and multiple zeta values. *Invent. Math.*, 149(2):339–369, 2002.

[33] Philip C. Tonne. A regular determinant of binomial coefficients. *Proc. Amer. Math. Soc.*, 41:17–23, 1973.

[34] Lucien Van Hamme. Some congruences involving the p-adic gamma function and some arithmetical consequences. In *p-adic functional analysis (Ioannina, 2000)*, volume 222 of *Lecture Notes in Pure and Appl. Math.*, pages 133–138. Dekker, New York, 2001.

[35] Edward Waring. *Meditationes algebraicæ*. American Mathematical Society, Providence, RI, 1991. Translated from the Latin, edited and with a foreword by Dennis Weeks, With an appendix by Franz X. Mayer, translated from the German by Weeks.

[36] Lawrence C. Washington. p-adic L-functions and sums of powers. *J. Number Theory*, 69(1):50–61, 1998.

[37] Joseph Wolstenholme. On certain properties of prime numbers. *The Quarterly Journal of Pure and Applied Mathematics*, 5:35–39, 1862.

[38] Don Zagier. Values of zeta functions and their applications. In *First European Congress of Mathematics, Vol. II (Paris, 1992)*, volume 120 of *Progr. Math.*, pages 497–512. Birkhäuser, Basel, 1994.

[39] Don Zagier. Evaluation of the multiple zeta values $\zeta(2,\dots,2,3,2,\dots,2)$. *Ann. of Math. (2)*, 175(2):977–1000, 2012.

[40] Jianqiang Zhao. Wolstenholme type theorem for multiple harmonic sums. *Int. J. Number Theory*, 4(1):73–106, 2008.

[41] Jianqiang Zhao. Mod p structure of alternating and non-alternating multiple harmonic sums. *J. Théor. Nombres Bordeaux*, 23(1):299–308, 2011.

[42] Wadim Zudilin. On the irrationality of the values of the Riemann zeta function. *Izv. Ross. Akad. Nauk Ser. Mat.*, 66(3):49–102, 2002.