#A22 INTEGERS 24 (2024)

REGULAR PRIMES, NON-WIEFERICH PRIMES, AND FINITE MULTIPLE ZETA VALUES OF LEVEL N

Shin-ichiro Seki[1]

Department of Mathematical Sciences, Aoyama Gakuin University, Sagamihara, Japan

seki@math.aoyama.ac.jp

Received: 11/1/23, Accepted: 2/8/24, Published: 2/19/24

Abstract

We introduce finite multiple zeta values of general levels and discuss the relationship between the non-zeroness of these values and regular or non-Wieferich primes. Because it is challenging to prove the infinitude of these kinds of primes, we suggest tackling several related problems more promptly.

1. Introduction

The following two old conjectures about prime numbers are still open.

Conjecture 1. There exist infinitely many regular primes.

Conjecture 2. There exist infinitely many non-Wieferich primes.

For a prime p, we call p *regular* when p is odd and the class number of the pth cyclotomic field is not divisible by p. We call p *non-Wieferich* when $2^{p-1} - 1$ is not divisible by p^2. These kinds of primes are each associated with the following theorems related to Fermat's last theorem.

Theorem 1 (Kummer [21]). *If p is a regular prime, then Fermat's last theorem for the exponent p is correct.*

Theorem 2 (Wieferich [33]). *If p is a non-Wieferich prime, then the first case of Fermat's last theorem for the exponent p is correct.*

In addition to the pure interest in the distribution of primes, historically, one of the motivations to resolve Conjectures 1 and 2 can be attributed to Fermat's last theorem. If Conjecture 2 is true, then it ensures that the first case of Fermat's

DOI: 10.5281/zenodo.10680412

[1] This research was supported by JSPS KAKENHI Grant Number 21K13762.

last theorem holds for infinitely many prime exponents. Similarly, if Conjecture 1 is true, then it ensures that Fermat's last theorem holds for infinitely many prime exponents. It should be noted that for the first case, it has been shown by Adleman–Heath-Brown [1] to hold for infinitely many prime exponents without relying on Conjecture 2. As is well known, since Fermat's last theorem was fully resolved by Wiles [34], this motivation can be said to have vanished.

In this decade, there has been a focus on the study of finite multiple zeta values and Conjecture 1 is related to the non-vanishing nature of these values. Furthermore, in this note, we define a generalization of finite multiple zeta values to general levels and explore their relationship with Conjecture 2. From the study of these values, a new and compelling motivation has arisen to resolve Conjectures 1 and 2 after the work by Wiles. In Section 5, we discuss problems that are believed to be resolved before these conjectures.

2. Finite Multiple Zeta Values of Level N

2.1. Finite Multiple Zeta Values

The finite multiple zeta values, which are analogues of multiple zeta values (periods of mixed Tate motives over $\mathbb{Z}$), were defined as elements of the ring

$$\mathcal{A} := \left(\prod_{p\in\mathcal{P}} \mathbb{Z}/p\mathbb{Z}\right) \Bigg/ \left(\bigoplus_{p\in\mathcal{P}} \mathbb{Z}/p\mathbb{Z}\right)$$

by Kaneko–Zagier. Here, $\mathcal{P}$ denotes the set of all prime numbers. This ring $\mathcal{A}$, termed the ring of integers modulo infinitely large primes, is not an integral domain but a reduced ring. Through the diagonal embedding, $\mathcal{A}$ possesses a $\mathbb{Q}$-algebra structure. Elements of $\mathcal{A}$ are actually determined as equivalence classes, but they are often represented by their representative elements $(a_p)_{p\in\mathcal{P}}$ in $\prod_{p\in\mathcal{P}}\mathbb{Z}/p\mathbb{Z}$. In this context, even if a_p is not defined for a finite number of primes p, it remains well-defined as an element of $\mathcal{A}$ and poses no problem. We call a tuple of positive integers $\boldsymbol{k} = (k_1, \ldots, k_r)$ an *index*. Its *depth* is given by r, and its *weight* by $k_1 + \cdots + k_r$. We consider the empty set $\varnothing$ as an index with both depth and weight being 0, and refer to it as the *empty index*. For each prime p and for non-empty index $\boldsymbol{k} = (k_1, \ldots, k_r)$, we define $\zeta_p(\boldsymbol{k}) \in \mathbb{Z}_{(p)}$ as follows:

$$\zeta_p(\boldsymbol{k}) := \sum_{0<m_1<\cdots<m_r<p} \frac{1}{m_1^{k_1}\cdots m_r^{k_r}}.$$

Using the natural isomorphism $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$, we define the *finite multiple zeta value* $\zeta_{\mathcal{A}}(\boldsymbol{k}) \in \mathcal{A}$ by $\zeta_{\mathcal{A}}(\boldsymbol{k}) := (\zeta_p(\boldsymbol{k}) \bmod p)_{p\in\mathcal{P}}$. Put $\zeta_{\mathcal{A}}(\varnothing) := 1$. There are many

$\mathbb{Q}$-linear relations among finite multiple zeta values. For example, the relation

$$2\zeta_{\mathcal{A}}(1,2,3)+\zeta_{\mathcal{A}}(1,2,1,2)+\zeta_{\mathcal{A}}(1,2,2,1)+\zeta_{\mathcal{A}}(1,1,1,3)=0 \tag{1}$$

holds, as explained in [26, Section 3.7]. For an index $\boldsymbol{k}$ of weight k, we shall refer to $\zeta_{\mathcal{A}}(\boldsymbol{k})$ as the finite multiple zeta value of weight k. For a non-negative integer k, we denote the $\mathbb{Q}$-vector space spanned by all finite multiple zeta values of weight k as $\mathcal{Z}_{\mathcal{A},k}$, and set $\mathcal{Z}_{\mathcal{A}} := \sum_{k=0}^{\infty}\mathcal{Z}_{\mathcal{A},k}$. By the so-called harmonic (stuffle) product formula, it is understood that $\mathcal{Z}_{\mathcal{A}}$ is a $\mathbb{Q}$-subalgebra of $\mathcal{A}$. Research on the algebraic structure of $\mathcal{Z}$, the $\mathbb{Q}$-subalgebra of $\mathbb{R}$ spanned by all multiple zeta values, has been ongoing for many years. Similarly, the investigation of the algebraic structure of $\mathcal{Z}_{\mathcal{A}}$ is both fascinating and extensive. Furthermore, a surprising algebraic isomorphism $\mathcal{Z}_{\mathcal{A}} \simeq \mathcal{Z}/\zeta(2)\mathcal{Z}$ is conjectured to exist, which is known as the Kaneko–Zagier conjecture. This implies a connection between "prime numbers" and "zeta" in a form entirely different from the Euler product formula, making it a highly intriguing conjecture. For a detailed correspondence, refer to [18, Conjecture 9.5].

2.2. Finite Multiple Zeta Values of Level N

Recently, the finite multiple zeta value of level two, $\zeta_{\mathcal{A}}^{(2)}(\boldsymbol{k})$, was introduced by Kaneko, Murakami, and Yoshihara in [19]. In this context, we define finite multiple zeta values of higher levels. Let N be a positive integer. Elements of $\mathbb{Z}/N\mathbb{Z}$ are considered as equivalence classes with respect to the equivalence relation of congruence modulo N in the usual way. Furthermore, the equivalence class to which an integer a belongs will be denoted by $\overline{a}$. For each prime p, non-empty index $\boldsymbol{k}=(k_1,\dots,k_r)$, and $\boldsymbol{\alpha}:=(\alpha_1,\dots,\alpha_r)\in(\mathbb{Z}/N\mathbb{Z})^r$, we define $\zeta_{p,N}^{\boldsymbol{\alpha}}(\boldsymbol{k})\in\mathbb{Z}_{(p)}$ as follows:

$$\zeta_{p,N}^{\boldsymbol{\alpha}}(\boldsymbol{k}) := \sum_{\substack{0<m_1<\cdots<m_r<p\\ m_i\in\alpha_i \text{ for all } 1\le i\le r}} \frac{1}{m_1^{k_1}\cdots m_r^{k_r}}.$$

For the case $\boldsymbol{k}=\varnothing$, there is only one element of $(\mathbb{Z}/N\mathbb{Z})^r$ $(r=0)$, which we denote as $\bullet$. For convenience, we set $\zeta_{p,N}^{\bullet}(\varnothing):=1$ and for every index $\boldsymbol{k}$, $\zeta_{p,N}^{\boxtimes}(\boldsymbol{k}):=0$.

Definition 1. We call a map $c\colon(\mathbb{Z}/N\mathbb{Z})^\times\to(\mathbb{Z}/N\mathbb{Z})^r\cup\{\boxtimes\}$ a *color map.* We define $\zeta_{\mathcal{A},N}^{c}(\boldsymbol{k})\in\mathcal{A}$, referred to as a *finite multiple zeta value of level N with color map c*, by $\zeta_{\mathcal{A},N}^{c}(\boldsymbol{k}):=(\zeta_{p,N}^{c(\overline{p})}(\boldsymbol{k}) \bmod p)_{p\in\mathcal{P}}$.

Note that since there are only finitely many prime numbers p for which $c(\overline{p})$ is not defined, $\zeta_{\mathcal{A},N}^{c}(\boldsymbol{k})\in\mathcal{A}$ is well-defined. These values are finite analogues of the multiple zeta values of level N with color defined by Yuan–Zhao in [35, Section 2].

Remark 1. After the original draft of this paper was completed, Masataka Ono kindly informed the author of analogues of finite multiple zeta values defined by

Tasaka using $\zeta^{\boldsymbol{\alpha}}_{p,N}(\boldsymbol{k})$ in [30, Section 6.4]. While these values are defined in modified rings, not in the ring $\mathcal{A}$, they differ from ours but are closely related. Regardless, further research on these values is expected in the future.

For later use, we give the following definition here: for each integer j satisfying $0 \leq j < N$, we define a map $[j]$ by $[j](\alpha) \coloneqq (-j\alpha, \ldots, -j\alpha) \in (\mathbb{Z}/N\mathbb{Z})^r$ for any $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$. Although this definition depends on both N and r, it poses no issues when used in contexts where N and r are specified, as in $\zeta^{[j]}_{\mathcal{A},N}(\boldsymbol{k})$. When $r = 0$, $[j](\alpha) = \bullet$. For an index $\boldsymbol{k}$ of weight k, let $\zeta^{(N)}_{\mathcal{A}}(\boldsymbol{k}) \coloneqq N^k \zeta^{[0]}_{\mathcal{A},N}(\boldsymbol{k})$. Then, we have $\zeta^{(1)}_{\mathcal{A}}(\boldsymbol{k}) = \zeta_{\mathcal{A}}(\boldsymbol{k})$ and $\zeta^{(2)}_{\mathcal{A}}(\boldsymbol{k})$ coincides with the value defined in [19].

For each non-negative integer k, we define a $\mathbb{Q}$-vector space $\mathcal{Z}_{\mathcal{A},k}(N)$ by

$$\mathcal{Z}_{\mathcal{A},k}(N) \coloneqq \sum_{\boldsymbol{k}\colon \text{ index of weight } k} \; \sum_{c\colon (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^{\text{depth of } \boldsymbol{k}} \cup \{\boxtimes\}} \mathbb{Q} \cdot \zeta^{c}_{\mathcal{A},N}(\boldsymbol{k}).$$

We set $\mathcal{Z}_{\mathcal{A}}(N) \coloneqq \sum_{k=0}^{\infty} \mathcal{Z}_{\mathcal{A},k}(N)$. This $\mathcal{Z}_{\mathcal{A}}(N)$ is the space spanned by all finite multiple zeta values of level N. A natural generalization of the harmonic product formula holds, and it should be almost obvious that $\mathcal{Z}_{\mathcal{A}}(N)$ possesses the structure of a $\mathbb{Q}$-subalgebra of $\mathcal{A}$ such that $\mathcal{Z}_{\mathcal{A},k_1}(N) \cdot \mathcal{Z}_{\mathcal{A},k_2}(N) \subset \mathcal{Z}_{\mathcal{A},k_1+k_2}(N)$. For example, we have

$$\begin{aligned}\zeta^{f}_{\mathcal{A},N}(k_1,k_2)\zeta^{g}_{\mathcal{A},N}(l) = \zeta^{h_1}_{\mathcal{A},N}(l,k_1,k_2) + \zeta^{h_2}_{\mathcal{A},N}(k_1,l,k_2) + \zeta^{h_3}_{\mathcal{A},N}(k_1,k_2,l) \\ + \zeta^{h_4}_{\mathcal{A},N}(k_1+l,k_2) + \zeta^{h_5}_{\mathcal{A},N}(k_1,k_2+l),\end{aligned}$$

where for each $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, if $f(\alpha)$ or $g(\alpha)$ equals $\boxtimes$, we set $h_1(\alpha) = \cdots = h_5(\alpha) \coloneqq \boxtimes$; otherwise, writing $f(\alpha) = (f_1(\alpha), f_2(\alpha)) \in (\mathbb{Z}/N\mathbb{Z})^2$, we define

$$\begin{aligned}&h_1(\alpha) \coloneqq (g(\alpha), f_1(\alpha), f_2(\alpha)), \quad h_2(\alpha) \coloneqq (f_1(\alpha), g(\alpha), f_2(\alpha)), \\ &h_3(\alpha) \coloneqq (f_1(\alpha), f_2(\alpha), g(\alpha)), \\ &h_4(\alpha) \coloneqq \begin{cases} f(\alpha) & \text{if } f_1(\alpha) = g(\alpha), \\ \boxtimes & \text{otherwise} \end{cases}, \quad h_5(\alpha) \coloneqq \begin{cases} f(\alpha) & \text{if } f_2(\alpha) = g(\alpha), \\ \boxtimes & \text{otherwise.} \end{cases}\end{aligned}$$

Not only the harmonic product formula, but we also provide natural generalizations of the reversal formula for finite multiple zeta values (Hoffman [13, Theorem 4.5], Zhao [36, Lemma 3.3]; see also [26, Proposition 2.6]) and a formula

$$\zeta_{\mathcal{A}}(k_1,\ldots,k_r) = \sum_{i=0}^{r} (-1)^{k_{i+1}+\cdots+k_r} \zeta^{(2)}_{\mathcal{A}}(k_1,\ldots,k_i)\zeta^{(2)}_{\mathcal{A}}(k_r,\ldots,k_{i+1})$$

obtained by Kaneko, Murakami, and Yoshihara [19, Equation (6)].

Lemma 1. *Let $\boldsymbol{k} = (k_1, \dots, k_r)$ be an index of weight k. Let j be an integer satisfying $0 \leq j < N$. Then,*

$$\left(\sum_{\frac{jp}{N} < m_1 < \cdots < m_r < \frac{(j+1)p}{N}} \frac{1}{m_1^{k_1} \cdots m_r^{k_r}} \bmod p \right)_{p \in \mathcal{P}} = N^k \zeta_{\mathcal{A},N}^{[j]}(\boldsymbol{k})$$

holds in $\mathcal{A}$.

Proof. Take $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ and a prime p belonging to α. By putting $m_i' = Nm_i$, we have

$$\sum_{\frac{jp}{N} < m_1 < \cdots < m_r < \frac{(j+1)p}{N}} \frac{1}{m_1^{k_1} \cdots m_r^{k_r}} = N^k \sum_{\substack{jp < m_1' < \cdots < m_r' < (j+1)p \\ m_i' \equiv 0 \pmod{N} \text{ for all } 1 \leq i \leq r}} \frac{1}{{m'}_1^{k_1} \cdots {m'}_r^{k_r}},$$

and by putting $n_i = m_i' - jp$, we have

$$\sum_{\substack{jp < m_1' < \cdots < m_r' < (j+1)p \\ m_i' \equiv 0 \pmod{N} \text{ for all } 1 \leq i \leq r}} \frac{1}{{m'}_1^{k_1} \cdots {m'}_r^{k_r}} \equiv \sum_{\substack{0 < n_1 < \cdots < n_r < p \\ n_i \in -j\alpha \text{ for all } 1 \leq i \leq r}} \frac{1}{n_1^{k_1} \cdots n_r^{k_r}} \pmod{p}.$$

This gives a proof. □

Proposition 1. *Let $\boldsymbol{k} = (k_1, \dots, k_r)$ be an index of weight k.*

i) Let $\overleftarrow{\boldsymbol{k}} := (k_r, \dots, k_1)$. For a color map c, we define $\overleftarrow{c}$ as follows: when $c(\alpha) = (\alpha_1, \dots, \alpha_r) \in (\mathbb{Z}/N\mathbb{Z})^r$, set $\overleftarrow{c}(\alpha) := (\alpha - \alpha_r, \dots, \alpha - \alpha_1)$, and when $c(\alpha) = \boxtimes$, set $\overleftarrow{c}(\alpha) := \boxtimes$. Then, we have

$$\zeta_{\mathcal{A},N}^{c}(\boldsymbol{k}) = (-1)^k \zeta_{\mathcal{A},N}^{\overleftarrow{c}}(\overleftarrow{\boldsymbol{k}}).$$

ii) For each tuple of integers $(i_1, \dots, i_{N-1})$ satisfying $0 \leq i_1 \leq \cdots \leq i_{N-1} \leq r$ and each integer j satisfying $0 \leq j < N$, set $\boldsymbol{k}_{(i_1,\dots,i_{N-1});j} := (k_{i_j+1}, \dots, k_{i_{j+1}})$. Here, we set $i_0 := 0$, $i_N := r$, and if $i_j = i_{j+1}$, then $\boldsymbol{k}_{(i_1,\dots,i_{N-1});j} = \varnothing$. Then, we have

$$\zeta_{\mathcal{A}}(\boldsymbol{k}) = N^k \sum_{0 \leq i_1 \leq \cdots \leq i_{N-1} \leq r} \prod_{j=0}^{N-1} \zeta_{\mathcal{A},N}^{[j]}(\boldsymbol{k}_{(i_1,\dots,i_{N-1});j}).$$

Proof. The first formula can be proved using a standard substitution trick $n_i = p - m_{r+1-i}$. For the second one, it suffices to use the partitioning of the sum range

$$\sum_{0 < m_1 < \cdots < m_r < p} = \sum_{0 \leq i_1 \leq \cdots \leq i_{N-1} \leq r} \sum_{\substack{0 < m_1 < \cdots < m_{i_1} < \frac{p}{N} \\ \frac{p}{N} < m_{i_1+1} < \cdots < m_{i_2} < \frac{2p}{N} \\ \cdots \\ \frac{(N-1)p}{N} < m_{i_{N-1}+1} < \cdots < m_r < p}}$$

and Lemma 1. Note that if a prime p does not divide N, then for any $j = 1, 2, \ldots, N-1$, jp/N is not an integer, and therefore, the above partitioning holds true for all but a finite number of primes p. □

The following basic fact will be used later in the proof of Proposition 4.

Lemma 2. *Let N be a positive integer and M a positive multiple of N. Then, for any non-negative integer k, $\mathcal{Z}_{\mathcal{A},k}(N) \subset \mathcal{Z}_{\mathcal{A},k}(M)$ holds.*

Proof. This easily follows from the following partitioning of the sum range:

$$\sum_{\substack{0<m_1<\cdots<m_r<p \\ m_i \equiv a_i \pmod{N} \text{ for all } 1\le i\le r}} = \sum_{0\le j_1,\ldots,j_r<\frac{M}{N}} \sum_{\substack{0<m_1<\cdots<m_r<p \\ m_i \equiv a_i+j_iN \pmod{M} \text{ for all } 1\le i\le r}},$$

where p is a prime number and $a_1, \ldots, a_r$ are integers. □

While investigating $\mathbb{Q}$-linear relations among finite multiple zeta values of level N seems to be an interesting subject, we will not pursue it further in this note.

2.3. Non-Zeroness

Researchers of finite multiple zeta values face a significant issue. Namely, not a single finite multiple zeta value corresponding to a non-empty index has been proved to be non-zero. In other words, Equation (1) might imply

$$2 \times 0 + 0 + 0 + 0 = 0.$$

There is a possibility that all linear relations that researchers of finite multiple zeta values have proved could be trivial! (It is crucial to note, however, that this only applies when viewing the relations in $\mathcal{A}$; in most cases, they have indeed shown non-trivial results.) This is an extremely frustrating situation, but based on the initial conjectures, the following can be said.

Proposition 2. (*i*) *If Conjecture* 1 *is true, then for every positive integer k that is not equal to* 1*,* 2*, or* 4*, there exists at least one non-zero finite multiple zeta value of weight k.*

(*ii*) *If Conjecture* 2 *is true, then for every even positive integer N and every positive integer k, there exists at least one non-zero finite multiple zeta value of level N and weight k.*

It is known that $\mathcal{Z}_{\mathcal{A},1} = \mathcal{Z}_{\mathcal{A},2} = \mathcal{Z}_{\mathcal{A},4} = 0$ (see [26] for details). The proofs of (i) and (ii) will be given in Section 3 and Section 4, respectively. For a result regarding odd levels greater than two, see Proposition 4.

3. Bernoulli–Seki Numbers

For a non-negative integer n, B_n denotes the nth *Bernoulli–Seki number*;

$$\frac{te^t}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n.$$

Here, the inclusion of "Seki" in the name emphasizes that Takakazu Seki independently discovered this sequence alongside Jacob Bernoulli. Kummer's criterion asserts that $p \geq 5$ is regular if and only if p does not divide any of B_2, B_4, $\ldots$, B_{p-3}. Thus, Conjecture 1 implies the following.

Conjecture 3. Let $k \geq 3$ be an odd integer. Then, there exist infinitely many primes p greater than k such that p does not divide B_{p-k}.

Let $k \geq 2$ be an integer, and define an element of $\mathcal{A}$ from the Bernoulli–Seki numbers as follows:

$$\mathfrak{Z}(k) := \left(\frac{B_{p-k}}{k} \bmod p\right)_{p\in\mathcal{P}}.$$

If k is even, then $\mathfrak{Z}(k) = 0$. If Conjecture 3 is true, then for odd $k \geq 3$, we have $\mathfrak{Z}(k) \neq 0$. Here, regarding the special values of finite multiple zeta values, the following is well-known (Vandiver, Hoffman, and Zhao [13, Theorem 6.1], [36, Theorem 3.1]; see also [18, Equation (7.2)], [26, Proposition 2.3]):

$$\zeta_{\mathcal{A}}(k_1,k_2) = (-1)^{k_2}\binom{k_1+k_2}{k_1}\mathfrak{Z}(k_1+k_2), \quad k_1,k_2 \geq 1. \tag{2}$$

Thus, the validity of Proposition 2 (i) for the case where the weight is an odd integer greater than one is established. This has been pointed out in several references and is likely well-known (cf. [17]). In the following, we will discuss the case where the weight is an even integer greater than four.

Proof of Proposition 2 (i). Let $k \geq 6$ be an even integer. In this case, there exist odd integers k_1 and k_2, both greater than one, such that we can decompose k as $k = k_1 + k_2$. If p is a regular prime greater than both k_1 and k_2, then by Kummer's criterion, p does not divide either B_{p-k_1} or B_{p-k_2}. Hence, if Conjecture 1 is true, we have $\mathfrak{Z}(k_1)\mathfrak{Z}(k_2) \neq 0$. From Equation (2), $\mathfrak{Z}(k_1) \in \mathcal{Z}_{\mathcal{A},k_1}$ and $\mathfrak{Z}(k_2) \in \mathcal{Z}_{\mathcal{A},k_2}$. By the harmonic product formula, $\mathfrak{Z}(k_1)\mathfrak{Z}(k_2) \in \mathcal{Z}_{\mathcal{A},k}$, and this product can be expressed as a $\mathbb{Q}$-linear combination of finite multiple zeta values of weight k. Therefore, at least one finite multiple zeta value of weight k must be non-zero. □

Although not used later, we provide here two curious formulas for values of level twelve.

Proposition 3. *Let $k \geq 3$ be an odd integer. Then, we have*

$$2\zeta^{[2]}_{\mathcal{A},12}(k) = (2^{-k} - 3^{-k} - 4^{-k} + 12^{-k})\mathfrak{Z}(k),$$
$$2\zeta^{[3]}_{\mathcal{A},12}(k) = (3^{-k} - 4^{-k} - 6^{-k} + 12^{-k})\mathfrak{Z}(k).$$

Proof. Let n be a positive integer and $p \geq 5$ a prime such that $p - 1 \nmid 2n$. From Vandiver's congruence [32, Equation (7)], we can derive the following two well-known congruences:

$$\frac{3^{p-2n} + 4^{p-2n} - 6^{p-2n} - 1}{4n} B_{2n} \equiv \sum_{\frac{p}{6} < m < \frac{p}{4}} m^{2n-1} \pmod{p},$$
$$\frac{2^{p-2n} + 3^{p-2n} - 4^{p-2n} - 1}{4n} B_{2n} \equiv \sum_{\frac{p}{4} < m < \frac{p}{3}} m^{2n-1} \pmod{p}.$$

The first one is also given in [29, Equation (9)]. Setting $2n = p - k$ and varying p, we obtain the desired formulas by Lemma 1. □

4. Fermat Quotients

Let N be a positive integer and p a prime number that does not divide N. We define the *Fermat quotient with base N* by

$$q_p(N) := \frac{N^{p-1} - 1}{p}.$$

For an integer j satisfying $0 \leq j < N$, we set $s_p(j, N)$ as

$$s_p(j, N) := \sum_{\frac{jp}{N} < m < \frac{(j+1)p}{N}} \frac{1}{m}.$$

In 1850, Eisenstein [9] proved that $2q_p(2) \equiv -s_p(0, 2) \pmod{p}$. We use the following generalization due to Skula, Dobson, and Ichimura.

Theorem 3 (Skula [28], Dobson [8], Ichimura [15])**.** *For every positive integer N, we have*

$$(N + 1)q_p(2) \equiv - \sum_{0 \leq j < \frac{N}{2}} s_p(2j, 2N) \pmod{p}.$$

Here, we define the logarithm function $\log_{\mathcal{A}} : \mathbb{Q}^{\times} \to \mathcal{A}$ as $\log_{\mathcal{A}}(N) := (q_p(N) \bmod p)_{p \in \mathcal{P}}$. (The Fermat quotient can be defined similarly even when N is not a positive integer.) The reason for the name is that the logarithmic law can be derived from the congruence $q_p(NM) \equiv q_p(N) + q_p(M) \pmod{p}$. Theorem 3 derives

$$\log_{\mathcal{A}}(2) = -\frac{2N}{N+1} \sum_{0 \le j < \frac{N}{2}} \zeta^{[2j]}_{\mathcal{A},2N}(1) \tag{3}$$

using Lemma 1, and in particular it is shown that $\log_{\mathcal{A}}(2) \in \mathcal{Z}_{\mathcal{A},1}(2N)$ for every N.

Proof of Proposition 2 *(ii)*. We assume that Conjecture 2 is true. By this assumption, there exist infinitely many primes p that do not divide $q_p(2)$ and hence $\log_{\mathcal{A}}(2) \neq 0$. By Equation (3), there exists an integer j satisfying $0 \le j < N/2$ (fix one such j) such that $\zeta^{[2j]}_{\mathcal{A},2N}(1) \neq 0$. Let k be an arbitrary positive integer. Since $\mathcal{A}$ is a reduced ring, we have $\zeta^{[2j]}_{\mathcal{A},2N}(1)^k \neq 0$. Since $\zeta^{[2j]}_{\mathcal{A},2N}(1)^k \in \mathcal{Z}_{\mathcal{A},k}(2N)$ and this value can be expressed as a $\mathbb{Q}$-linear combination of finite multiple zeta values of level $2N$ and weight k, we see that at least one finite multiple zeta value of level $2N$ and weight k must be non-zero. □

By using Lerch's congruence instead of Skula, Dobson, and Ichimura's congruence, we can obtain the following proposition through a similar argument.

Theorem 4 (Lerch [23, Equation (8)]). *For $N \ge 2$, we have*

$$Nq_p(N) \equiv \sum_{j=1}^{N-1} js_p(j,N) \pmod{p}.$$

This theorem derives

$$\log_{\mathcal{A}}(N) = \sum_{j=1}^{N-1} j \cdot \zeta^{[j]}_{\mathcal{A},N}(1) \in \mathcal{Z}_{\mathcal{A},1}(N).$$

In particular, by Lemma 2, we see that $\log_{\mathcal{A}}(N) \in \mathcal{Z}_{\mathcal{A},1}(M)$ for any positive integer M that is a multiple of N.

Proposition 4. *Let $N \ge 2$ be an integer. Assume that there exist infinitely many primes p that do not divide $q_p(N)$. Let M be any positive multiple of N. Then, for every positive integer k, there exists at least one non-zero finite multiple zeta value of level M and weight k.*

Remark 2. Proposition 4 is an extension of Proposition 2 (ii), and thanks to Lemma 2, to obtain Proposition 2 (ii), Eisenstein's congruence is sufficient, while Skula, Dobson, and Ichimura's congruence is not necessary. However, Equation (3) demonstrates a fact that is stronger than the mere $\log_{\mathcal{A}}(2) \in \mathcal{Z}_{\mathcal{A},1}(2N)$, making it worth mentioning due to the fact that it restricts the types of color maps used in zeta values to the form of $[2j]$.

5. Problems

Conjecture 1 has been shown to imply the existence of non-zero zeta values for each weight. However, in the current state where not a single non-zero value is known to exist, it is crucial to prove the existence of at least one. To achieve this, it is sufficient to address the following problem, which is weaker than Conjecture 3.

Problem 1. Show that there exists at least one odd integer $k \geq 3$ such that there are infinitely many primes $p > k$ that do not divide B_{p-k}.

If this problem is resolved in the affirmative, it implies that at least one non-zero finite multiple zeta value exists. From the perspective of the Kaneko–Zagier conjecture, $\mathfrak{Z}(k)$ can be considered as a counterpart to the Riemann zeta value $\zeta(k)$. In a sense, this problem aims for a result analogous to Ball–Rivoal [3] and Zudilin [37]'s outstanding works for Riemann zeta values, albeit in a slightly weaker form. For every odd integer $k \geq 3$, it is conjectured that $\mathfrak{Z}(k)$ is not only non-zero but also irrational. More strongly, it is expected to be a non-zero zero divisor.

Regarding Conjecture 2 and the assumption of Proposition 4, several conditional results are known. One of the most famous results is due to Silverman [27], asserts the correctness of these conjectures under the ABC conjecture. It should be noted that the author lacks the expertise to comprehend the claimed proof of the ABC conjecture by Mochizuki [25]. On a related note, it is worth mentioning about Artin's primitive root conjecture, which is a well-known conjecture about a different kind of prime numbers. It states that for any integer g that is neither -1 nor a square integer, there exist infinitely many primes p for which g is a primitive root modulo p. This conjecture was proved for all values of g by Hooley [14] under the generalized Riemann hypothesis. On the other hand, there exist unconditional results, which state that the conjecture holds for at least one value of g, as shown by Gupta–Ram Murty [11] and Heath-Brown [12]. In particular, according to Heath-Brown's result, Artin's conjecture is true for at least one of the values $g = 2$, 3, or 5. Expecting a similar progress for the case of Fermat quotients, an unconditional solution to the following problem is desired.

Problem 2. Show that there exists at least one integer $N \geq 2$ such that there are infinitely many primes p which do not divide $q_p(N)$.

If this problem is resolved in the affirmative, it implies that for at least one (therefore infinitely many) $N \geq 2$, there exists a non-zero finite multiple zeta value of level N for each weight.

For each odd prime p, ℓ_p denotes the least positive integer N for which p does not divide $q_p(N)$. There have been several studies providing upper bounds for ℓ_p. An early result by Lenstra Jr. [22] gives $\ell_p \leq 4(\log p)^2$. One of more recent improvements is $\ell_p \leq (\log p)^{463/252+o(1)}$ as $p \to \infty$, proved by Bourgain, Ford, Konyagin, and Shparlinski [4]. We aim to eliminate the dependence on p in these upper bounds.

Problem 3 ([10, Conjecture 9])**.** Show that there exists an integer M such that $\ell_p \leq M$ holds for every odd prime p.

If Problem 3 is resolved affirmatively, it is clear that Problem 2 follows in the affirmative as well. Let us provide an alternative formulation of the statement in Problem 3. For each N, we set

$$W(N) \coloneqq \{p \in \mathcal{P} : N^{p-1} - 1 \equiv 0 \pmod{p^2}\}, \quad W^{\mathrm{c}}(N) \coloneqq \mathcal{P} \setminus W(N).$$

Lemma 3. *A positive resolution of Problem 3 is equivalent to the validity of the following statement: there exists an integer $M \geq 3$ such that the intersection $\bigcap_{N=2}^{M} W(N)$ is finite.*

Proof. Let $M \geq 3$ be an integer and we note that $\ell_p < p$. We can easily check that the following equivalences hold: for all primes $p \geq 3$, $\ell_p \leq M$ if and only if $\mathcal{P} = \bigcup_{N=2}^{M} W^{\mathrm{c}}(N)$, which in turn holds if and only if $\bigcap_{N=2}^{M} W(N) = \varnothing$. Assume that $\bigcap_{N=2}^{M} W(N)$ is a non-empty finite set and write it $\{p_1, \ldots, p_k\}$ by enumeration. Let L be defined as $L \coloneqq \max\{\ell_{p_1}, \ldots, \ell_{p_k}\}$. Then, we have $\bigcap_{N=2}^{L} W(N) = \varnothing$. □

Let us define $\eth_p$ as the Bernoulli–Seki number analogue of ℓ_p.

Definition 2. Let $p \geq 5$ be a prime. We define $\eth_p$ as the least odd integer $k \geq 3$ for which p does not divide B_{p-k}.

Proposition 5. *For every prime $p \geq 11$, we have*

$$\eth_p \leq \begin{cases} \frac{p-3}{2} & \text{if } p \equiv 1 \pmod{4}, \\ \frac{p-5}{2} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Let $i(p)$ denote the index of irregularity defined by $i(p) \coloneqq \#\{2k : p \mid B_{2k}, 2 \leq 2k \leq p-3\}$. Since a trivial inequality $\eth_p \leq 2i(p) + 3$ holds, it suffices to provide an appropriate upper bound for $i(p)$. Let h_p^- denote the first factor of the class number of the pth cyclotomic field. We then have the inequality $i(p) \leq \log(h_p^-)/\log p$ from Vandiver's result [31]. Since an elementary inequality $p^{\frac{p+3}{4}} 2^{-\frac{p-1}{4}} \leq p^{\frac{p-8}{4}}$ holds for $p \geq 71$, we can obtain the desired bound from Carlitz's inequality $h_p^- < p^{\frac{p+3}{4}} 2^{-\frac{p-1}{4}}$ ([7, Equation (21)]). Here, note that $\eth_p = 3$ for all $p < 16843$. □

Remark 3. When $p \equiv 3 \pmod{4}$, it is known from the congruence due to Cauchy (see [5, Equation (5.2)]) that $B_{\frac{p+1}{2}} \not\equiv 0 \pmod{p}$, leading to $\eth_p \leq \frac{p-1}{2}$. When $p \equiv 1 \pmod{4}$, it is conjectured that $B_{\frac{p-1}{2}} \not\equiv 0 \pmod{p}$ by the congruence due to Kiselev [20] and the Ankeny, Artin, and Chowla conjecture [2], leading to $\eth_p \leq \frac{p+1}{2}$. While the proposition above provides better bounds than those derived from these considerations, it would be desirable to obtain more non-trivial bound, for example, $\eth_p \leq p^{1-\varepsilon}$ for some positive ε.

It is conjectured that $\sup_{p\in\mathcal{P}} i(p) = \infty$, but on the other hand, $\eth_p$ is expected to be bounded. (Does $\eth_p \leq 5$ always hold?)

Problem 4. Show that there exists an integer M such that $\eth_p \leq M$ holds for every prime $p \geq 5$.

If Problem 4 is resolved affirmatively, it is clear that Problem 1 follows in the affirmative as well. For each odd integer $k \geq 3$, we set $I(k) := \{p \in \mathcal{P} : p \mid B_{p-k}\}$. By a similar argument as in the proof of Lemma 3, we can prove the following.

Lemma 4. *A positive resolution of Problem* 4 *is equivalent to the validity of the following statement*: *there exists an integer* $M \geq 5$ *such that the intersection* $\bigcap_{3\leq k\leq M,\ k\text{: odd}} I(k)$ *is finite.*

Conjecture 1 remains open; however, the infinitude of irregular primes has been proved (Jensen [16], Carlitz [6]). Furthermore, the following lower bound has been obtained by Luca, Pizarro-Madariaga, and Pomerance [24]:

$$\#\{p \leq x : p \text{ is an irregular prime}\} \geq (1+o(1))\frac{\log\log x}{\log\log\log x}, \quad \text{as } x \to \infty.$$

The relative density of the set of irregular primes in the set of all prime numbers is conjectured to be $1 - e^{-\frac{1}{2}}$. On the contrary, the relative density of the set of Wieferich primes in the set of all prime numbers is conjectured to be zero, and proving the infinitude of Wieferich primes may be highly challenging. If this infinitude is true, then $\log_{\mathcal{A}}(2)$ would become a zero divisor.

Acknowledgements. The author thanks Professors Masanobu Kaneko, Toshiki Matsusaka, Pieter Moree, Masataka Ono, and Shingo Saito for their valuable comments. The author is also grateful to Hanamichi Kawamura for discussions.

References

[1] L. M. Adleman and D. R. Heath-Brown, The first case of Fermat's last theorem, *Invent. Math.* **79** (1985), 409-416.

[2] N. C. Ankeny, E. Artin, and S. Chowla, The class-number of real quadratic fields, *Ann. of Math. (2)* **56** (1952), 479-493.

[3] K. Ball and T. Rivoal, Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs, *Invent. Math.* **146** (2001), 193-207.

[4] J. Bourgain, K. Ford, S. V. Konyagin, and I. E. Shparlinski, On the divisibility of Fermat quotients, *Michigan Math. J.* **59** (2010), 313-328.

[5] L. Carlitz, The class number of an imaginary quadratic field, *Comment. Math. Helv.* **27** (1953), 338-345.

[6] L. Carlitz, Note on irregular primes, *Proc. Amer. Math. Soc.* **5** (1954), 329-331.

[7] L. Carlitz, A generalization of Maillet's determinant and a bound for the first factor of the class number, *Proc. Amer. Math. Soc.* **12** (1961), 256-261.

[8] J. B. Dobson, On Lerch's formula for the Fermat quotient, preprint, `arXiv: 1103.3907v6`.

[9] G. Eisenstein, Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden, *Ber. K. Preuss. Akad. Wiss. Berlin* **15** (1850), 36-42.

[10] A. Granville, Some conjectures related to Fermat's last theorem, in *Number theory* (Banff, Alberta, 1988), 177-192, Walter de Gruyter, Berlin 1990.

[11] R. Gupta and M. Ram Murty, A remark on Artin's conjecture, *Invent. Math.* **78** (1984), 127-130.

[12] D.R. Heath-Brown, Artin's conjecture for primitive roots, *Q. J. Math.* **37** (1986), 27-38.

[13] M. E. Hoffman, Quasi-symmetric functions and mod p multiple harmonic sums, *Kyushu J. Math.* **69** (2015), 345-366.

[14] C. Hooley, Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209-220.

[15] H. Ichimura, Note on a congruence for the Fermat quotient with base 2, *Kyushu J. Math.* **73** (2019), 115-121.

[16] K. L. Jensen, Om talteoretiske Egenskaber ved de Bernoulliske Tal, *Nyt Tidsskr. Math. B* **26** (1915), 73-83.

[17] M. Kaneko, Finite multiple zeta values (in Japanese), in *Various aspects of multiple zeta values*, *RIMS Kôkyûroku Bessatsu* **B68** (2017), 175-190.

[18] M. Kaneko, An introduction to classical and finite multiple zeta values, *Publications mathématiques de Besançon, Algèbre et théorie des nombres* 2019/1, 103-129.

[19] M. Kaneko, T. Murakami, and A. Yoshihara, On finite multiple zeta values of level two, *Pure Appl. Math. Q.* **19** (2023), 267-280.

[20] A. A. Kiselev, An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers, *Dokl. Akad. Nauk* **61** (1948), 777-779.

[21] E. E. Kummer, Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factoren nicht vorkommen, *J. Reine Angew. Math.* **40** (1850), 131-138.

[22] H. W. Lenstra Jr., Miller's primality test, *Inform. Process. Lett.* **8** (1979), 86-88.

[23] M. Lerch, Zur Theorie des Fermatschen Qutienten $\frac{a^{p-1}-1}{p} = q(a)$, *Math. Ann.* **60** (1905), 471-490.

[24] F. Luca, A. Pizarro-Madariaga, and C. Pomerance, On the counting function of irregular primes, *Indag. Math. (N.S.)* **26** (2015), 147-161.

[25] S. Mochizuki, Inter-universal Teichmüller theory IV: Log-volume computations and set-theoretic foundations, *Publ. Res. Inst. Math. Sci.* **57** (2021), 627-723.

[26] S. Saito, Numerical tables of finite multiple zeta values, in *Various aspects of multiple zeta values*, *RIMS Kôkyûroku Bessatsu* **B68** (2017), 191-208.

[27] J. H. Silverman, Wieferich's criterion and the *abc*-conjecture, *J. Number Theory* **30** (1988), 226-237.

[28] L. Skula, A note on some relations among special sums of reciprocals modulo p, *Math. Slovaca* **58** (2008), 5-10.

[29] E. Stafford and H. S. Vandiver, Determination of some properly irregular cyclotomic fields, *Proc. Natl. Acad. Sci. USA* **16** (1930), 139-150.

[30] K. Tasaka, Finite and symmetric colored multiple zeta values and multiple harmonic q-series at roots of unity, *Selecta Math. (N.S.)* **27**, 21 (2021), 34 pp.

[31] H. S. Vandiver, On the first factor of the class number of a cyclotomic field, *Bull. Amer. Math. Soc.* **25** (1919), 458-461.

[32] H. S. Vandiver, On Bernoulli's numbers and Fermat's last theorem, *Duke Math. J.* **3** (1937), 569-584.

[33] A. Wieferich, Zum letzten Fermatschen Theorem, *J. Reine Angew. Math.* **136** (1909), 293-302.

[34] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), 443-551.

[35] H. Yuan and J. Zhao, Double shuffle relations of double zeta values and the double Eisenstein series at level N, *J. Lond. Math. Soc. (2)* **92** (2015), 520-546.

[36] J. Zhao, Wolstenholme type theorem for multiple harmonic sums, *Int. J. Number Theory* **4** (2008), 73-106.

[37] V. V. Zudilin [W. Zudilin], One of the numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational, *Uspekhi Mat. Nauk* **56** (2001), 149-150.