

LINEAR RELATIONS BETWEEN CERTAIN SUMS OF RECIPROCAL MODULO p

KARL DILCHER AND LADISLAV SKULA

To Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Les sommes des inverses modulo p prises sur les entiers de N sous-intervalles de longueur égale de l'intervalle $1 \leq j \leq p-1$ sont intimement reliées aux quotients de Fermat. Elles ont été étudiées dans le contexte de la théorie classique du dernier théorème de Fermat. Dans cet article, nous obtenons de nouvelles classes de relations linéaires entre ces sommes dans les cas où N est pair ou impair, et nous prouvons que pour chaque entier pair N , il y a au moins $\lfloor N/4 \rfloor$ relations linéaires indépendantes.

ABSTRACT. The sums of reciprocals modulo p over integers in N subintervals of equal length of the interval $1 \leq j \leq p-1$ are closely related to the Fermat quotients, and they have been studied in connection with the classical theory of Fermat's last Theorem. In this paper, we derive new classes of linear relations between these sums for both even and odd N , and we show that for each even N , there are at least $\lfloor N/4 \rfloor$ linearly independent relations.

1. Introduction

In the classical theory of Fermat's last Theorem, the Fermat quotient of a prime p with integer base a ,

$$q_p(a) := \frac{a^{p-1} - 1}{p}, \quad p \nmid a,$$

has played an important role; see, e.g., Ribenboim's book [6]. In his detailed study of these quotients, Lerch [5] considered the sums

$$(1) \quad s(k, N) := \sum_{j=\lfloor kp/N \rfloor + 1}^{\lfloor (k+1)p/N \rfloor} j^{p-2} \equiv \sum_{\frac{kp}{N} < j < \frac{(k+1)p}{N}} \frac{1}{j} \pmod{p},$$

where $N \geq 1$, $p \nmid N$, and $0 \leq k \leq N-1$. He proved the congruence

$$(2) \quad Nq_p(N) \equiv \sum_{k=0}^{N-1} ks(k, N) \pmod{p}.$$

This generalized the earlier congruence

$$(3) \quad 2q_p(2) \equiv \sum_{\frac{p}{2} < j < p} \frac{1}{j} \equiv s(1, 2) \pmod{p}$$

due to Eisenstein [3]. The sums $s(k, N)$ gained further importance when Vandiver [9] in his extension of earlier criteria of Wieferich and Mirimanoff proved that if the first case of Fermat's last Theorem fails for the prime exponent p , then $q_p(5) \equiv 0 \pmod{p}$ and $s(0, 5) \equiv 0 \pmod{p}$. For other similar criteria, see [6]. Vandiver's criterion concerning the sum $s(0, 5)$ was later extended by Cikánek [1] and the authors [2]. As the definition (1) shows, the sum $s(k, N)$ depends on the given prime p . However, it has been common usage in the literature not to include this dependence in the notation.

It is the purpose of this paper to study linear relations between the sums $s(k, N)$. First of all, it follows from the definition (1) that we have

$$(4) \quad s(k, N) \equiv -s(N - k - 1, N) \pmod{p}, \quad 0 \leq k \leq N - 1.$$

Since

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

because it is a sum over a reduced residue system modulo p , we obviously have

$$(5) \quad \sum_{k=0}^{N-1} s(k, N) \equiv 0 \pmod{p}.$$

For a long time this last congruence was thought to be the only linear congruence between the sums $s(k, N)$, for fixed N , that holds for all primes p , where $p \nmid N$. It came therefore as a surprise when the second author discovered computationally, and was then able to prove in [7], the following congruence for all even N .

Proposition 1.1 (Skula). *If $N = 2M$ and $M \geq 1$ is an integer, then*

$$(6) \quad \sum_{k=0}^{M-1} \left(M - (-1)^k \right) s(k, N) \equiv 0 \pmod{p},$$

for all odd primes p not dividing N .

In addition, it was proved in [7] that

$$(7) \quad s(0, 10) + 2s(1, 10) + s(4, 10) \equiv 0 \pmod{p}.$$

In this paper, we show that the congruence (7) extends to all even N , and that these congruences generalize also in a different direction. Furthermore, we derive a different congruence of the type (6) when N is a multiple of 4. We also show that many of these congruences are linearly independent. All this can be summarized in the following theorem.

Theorem 1.2. *Let p be an odd prime and $N \geq 4$ be an even integer. Then, among the sums $s(0, N), s(1, N), \dots, s(N/2 - 1, N)$, there are at least $\lfloor N/4 \rfloor$ independent linear congruences modulo p that hold for all $p \nmid N$. If $N = 2M$, where M is an odd composite integer and $p > N$, then there is one additional linearly independent congruence modulo p .*

We begin with an auxiliary result in Section 2, which is then used to prove most of the linear congruences in Section 3. In Section 4, we show that $\lfloor N/4 \rfloor$ of these congruences are linearly independent from each other, which imply the first part of Theorem 1.2. The case of odd N is discussed in Section 5 and, as a consequence, we obtain the second part of Theorem 1.2. We conclude this paper with some further congruences in Section 6.

2. An auxiliary result

An essential ingredient in the proof of the congruence (7) in [7] is the existence of the following two congruences due to H.C. Williams [10], [11] (see also [8]), namely

$$(8) \quad \frac{F_{p-\varepsilon}}{p} \equiv \frac{2}{5} \sum_{1 \leq k < \frac{4p}{5}} \frac{(-1)^k}{k} \pmod{p},$$

$$(9) \quad \frac{F_{p-\varepsilon}}{p} \equiv \frac{2}{5} \sum_{\frac{p}{5} < k < \frac{4p}{5}} \frac{1}{k} \pmod{p},$$

for $p \neq 2, 5$, where F_n is the n -th Fibonacci number (that is, $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$) and ε is the Legendre symbol $\varepsilon = (5/p)$. It turns out that this deep connection with the Fibonacci quotients on the left of (8) and (9) is not required. In fact, by direct manipulation of the sums in question, one can derive a vast generalization of the congruence between the right-hand sides of (8) and (9).

For the sake of convenience in the statement and in the proof of the following lemma, as well as in the proof of Proposition 3.1 in the next section, we adopt the following convention. If m_k is any sequence and a, b are integers with $b < a$, then we write

$$(10) \quad \sum_{k=a}^b m_k = - \sum_{k=b}^a m_k.$$

For non-integers a, b with $b \leq a$ we also define

$$\sum_{a < k < b} m_k = - \sum_{b < k < a} m_k.$$

This is consistent with the empty sum being 0, and also with the analogous convention for integrals.

Lemma 2.1. *Let m and N be integers with $m \geq 1$ and $N \geq 4m$, and suppose that p is an odd prime that does not divide N . Then*

$$(11) \quad \sum_{1 \leq k < \frac{N-2m}{N}p} \frac{(-1)^k}{k} \equiv \sum_{\frac{2mp}{N} < k < \frac{N-2m}{2N}p} \frac{1}{k} \pmod{p},$$

where the convention (10) is used if necessary.

Proof. We rewrite the left-hand side of (11) as follows:

$$\begin{aligned} - \sum_{1 \leq k < \frac{N-2m}{N}p} \frac{(-1)^k}{k} &= \sum_{1 \leq k < \frac{N-2m}{N}p} \frac{1}{k} - 2 \sum_{1 \leq j < \frac{N-2m}{2N}p} \frac{1}{2j} \\ &= \sum_{\frac{N-2m}{2N}p \leq k < \frac{N-2m}{N}p} \frac{1}{k}. \end{aligned}$$

Adding the right-hand side of (11) to this and keeping in mind the convention (10), we see that the congruence (11) is equivalent to

$$\sum_{\frac{2mp}{N} < k < \frac{N-2m}{N}p} \frac{1}{k} \equiv 0 \pmod{p}.$$

But this congruence holds for $N \geq 4m$ by symmetry. This is due to the fact that the sum over the whole range from 1 to $p-1$ vanishes modulo p , and $\frac{1}{k} \equiv -\frac{1}{p-k} \pmod{p}$ for all k . $\square$

As an aside, we remark that when $N = 6m$, the right-hand side of (11) vanishes since it is an empty sum. We then immediately obtain the following known congruence (it can be obtained, for instance, from congruences in [4]).

Corollary 2.2. *For any odd prime p we have*

$$\sum_{k=1}^{\lfloor 2p/3 \rfloor} \frac{(-1)^k}{k} \equiv 0 \pmod{p}.$$

3. The linear relations

We begin by stating and proving a generalization of the congruence (7). In fact, for each even N we have $\lfloor N/4 \rfloor$ different congruences.

Proposition 3.1. *Let p be an odd prime, and $N \geq 4$ be an even integer not divisible by p . Then for every integer m , $1 \leq m \leq \lfloor N/4 \rfloor$, we have*

$$(12) \quad \sum_{k=0}^{m-1} s(k, N) + 2 \sum_{k=m}^{2m-1} s(k, N) + \sum_{k=N/2-m}^{N/2-1} s(k, N) \equiv 0 \pmod{p}.$$

Before proving this, we state the cases $m = 1$ and $m = 2$ separately.

Corollary 3.2. *Let $N \geq 4$ be an even integer with $p \nmid N$. Then*

$$(13) \quad s(0, N) + 2s(1, N) + s(N/2 - 1, N) \equiv 0 \pmod{p},$$

and for $N \geq 8$,

$$(14) \quad \begin{aligned} &s(0, N) + s(1, N) + 2s(2, N) + 2s(3, N) \\ &\quad + s(N/2 - 2, N) + s(N/2 - 1, N) \equiv 0 \pmod{p}. \end{aligned}$$

This shows that the congruence (13) is a direct generalization of (7), and that (12) further generalizes (13).

Proof of Proposition 3.1. We begin with the left-hand side of (11) and consider separately the sum over even k and over odd k . First, we have

$$\begin{aligned} \sum_{\substack{1 \leq k < \frac{N-2m}{N}p \\ k \text{ even}}} \frac{1}{k} &= \frac{1}{2} \sum_{1 \leq k < \frac{N-2m}{2N}p} \frac{1}{k} \\ &\equiv \frac{1}{2} (s(0, N) + s(1, N) + \cdots + s(\frac{N}{2} - m - 1, N)) \pmod{p}, \end{aligned}$$

by the definition (1). For the odd k we get, by changing the order of summation,

$$\begin{aligned} \sum_{\substack{1 \leq k < \frac{N-2m}{N}p \\ k \text{ odd}}} \frac{1}{k} &\equiv - \sum_{\substack{1 \leq k < \frac{N-2m}{N}p \\ k \text{ odd}}} \frac{1}{p-k} \pmod{p} \\ &= - \sum_{\substack{\frac{2mp}{N} < k < p \\ k \text{ even}}} \frac{1}{k} \\ &= -\frac{1}{2} \sum_{\frac{mp}{N} < k < \frac{p}{2}} \frac{1}{k} \\ &\equiv -\frac{1}{2} (s(m, N) + s(m+1, N) + \cdots + s(\frac{N}{2} - 1, N)) \pmod{p}. \end{aligned}$$

We now get an expression for the left-hand sum of (11), which we denote by S , if we subtract the odd sum from the even sum. Thus, when $N > 4m$,

$$(15) \quad S \equiv \frac{1}{2} \left(\sum_{k=0}^{m-1} s(k, N) + 2 \sum_{k=m}^{N/2-m-1} s(k, N) + \sum_{k=N/2-m}^{N/2-1} s(k, N) \right) \pmod{p},$$

and when $N = 4m$,

$$(16) \quad S \equiv \frac{1}{2} \left(\sum_{k=0}^{m-1} s(k, N) + \sum_{k=N/2-m}^{N/2-1} s(k, N) \right) \pmod{p}.$$

Moreover, if we express the right-hand side of (11) in terms of the sums $s(k, N)$, we obtain

$$(17) \quad S \equiv \begin{cases} \sum_{k=2m}^{N/2-m-1} s(k, N) \pmod{p} & \text{for } N \geq 6m+2, \\ - \sum_{k=N/2-m}^{2m-1} s(k, N) \pmod{p} & \text{for } N < 6m, \\ 0 & \text{for } N = 6m. \end{cases}$$

Finally, we equate (15) (respectively (16)) and (17), and we immediately get (12) upon multiplying by 2. $\square$

We already remarked that the class of congruences (12) is a generalization of the very simple three-term congruence (13). Another generalization is the following set of congruences which have the advantage of having only four non-zero terms.

Corollary 3.3. *Let p be an odd prime and $N \geq 4$ be an even integer not divisible by p . Then for every integer m , $0 \leq m \leq \lfloor N/4 \rfloor - 1$, we have*

$$(18) \quad -s(m, N) + 2s(2m, N) + 2s(2m+1, N) + s(N/2 - m - 1, N) \equiv 0 \pmod{p}.$$

Proof. For $m = 0$, this is just (13). For $m \geq 1$, we take the congruence (12) with m replaced by $m + 1$ and subtract from it (12) in its original form. The congruence (18) then follows directly. $\square$

Next, we prove a linear congruence that is similar in nature to (6) in that it involves all the sums from $s(0, N)$ to $s(N/2 - 1, N)$.

Proposition 3.4. *Let p be an odd prime and $n \geq 1$ be an integer with $N = 4n$. If p does not divide N , then*

$$(19) \quad \sum_{k=0}^{n-1} s(k, N) + 3 \sum_{k=n}^{2n-1} s(k, N) \equiv 0 \pmod{p}.$$

Proof. By the definition (1), it is clear that

$$(20) \quad s(0, N) + \cdots + s(n-1, N) = s(0, 4),$$

$$(21) \quad s(n, N) + \cdots + s(2n-1, N) = s(1, 4).$$

Using Eisenstein's congruence (3) and the fact that $s(1, 2) \equiv -s(0, 2) \pmod{p}$ by (4), we have

$$(22) \quad -2q_p(2) \equiv s(0, 2) \equiv s(0, 4) + s(1, 4) \pmod{p}.$$

Now we use the *logarithmic property* that also goes back to Eisenstein [3], namely

$$(23) \quad q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p},$$

which is valid for integers a, b not divisible by p . This, together with Lerch's congruence (2), gives us

$$8q_p(2) \equiv 4q_p(4) \equiv s(1, 4) + 2s(2, 4) + 3s(3, 4) \pmod{p}.$$

Using the fact that $s(2, 4) \equiv -s(1, 4) \pmod{p}$ and $s(3, 4) \equiv -s(0, 4) \pmod{p}$, we get

$$(24) \quad 8q_p(2) \equiv -3s(0, 4) - s(1, 4) \pmod{p}.$$

Finally, if we multiply (22) by -4 and equate the result with (24), we obtain

$$s(0, 4) + 3s(1, 4) \equiv 0 \pmod{p}.$$

But this is the same as (19), by (20) and (21). $\square$

For an alternative proof, see Proposition 4.3 in the following section. We included the above proof as an illustration of how Fermat quotients and their logarithmic property can be used in this connection.

4. Linear independence

In this section, we examine the linear dependence and independence of the various linear congruences considered so far. We begin with a definition. Let N be a positive integer and p be a prime not dividing N . Let

$$V_p := \{(a_0, \dots, a_{N-1}) \mid a_0, \dots, a_{N-1} \in \mathbb{F}_p\}$$

be a vector space of dimension N over the finite field $\mathbb{F}_p$, with operations defined component-wise and rational integers also considered as elements of $\mathbb{F}_p$. Furthermore, let

$$U_p := \left\{ (a_0, \dots, a_{N-1}) \in V_p \mid \sum_{k=0}^{N-1} a_k s(k, N) \equiv 0 \pmod{p} \right\}.$$

Then U_p is a subspace of V_p .

Definition 4.1. Let N be a positive integer, p a prime not dividing N , and M a non-negative integer. Then we say that the system of linear congruences

$$\sum_{k=0}^{N-1} a_{m,k} s(k, N) \equiv 0 \pmod{p}, \quad 0 \leq m \leq M,$$

is *linearly independent* (modulo p) if the vectors

$$(a_{m,0}, \dots, a_{m,N-1}) \in U_p, \quad 0 \leq m \leq M,$$

are linearly independent over the field $\mathbb{F}_p$.

Proposition 4.2. For each even integer $N \geq 4$ not divisible by a given odd prime p , the $\lfloor N/4 \rfloor$ congruences given by (18) are linearly independent.

Proof. For $0 \leq m \leq \lfloor N/4 \rfloor - 1$, let

$$(25) \quad T_m(N) := \sum_{k=0}^{N/2-1} a_{m,k} s(k, N)$$

be the left-hand side of the congruence (18). Consider the coefficient matrix $(a_{m,k})$. It is clear that the $\lfloor N/4 \rfloor \times \lfloor N/4 \rfloor$ submatrix consisting of the $\lfloor N/4 \rfloor$ left-most columns is an upper triangular matrix with diagonal $(1, -1, -1, \dots, -1)$. Since the determinant is ± 1 , the matrix $(a_{m,k})$ has full rank modulo any prime p , which means that the congruences (18) are linearly independent. $\square$

This proof and the following result are illustrated by Tables 1 and 2 below. The functions U and V are introduced in Proposition 4.3 below. The coefficients $a_{m,k}$ in (25), for $N/2 \leq k \leq N-1$, are all zero; therefore they are not shown in the following tables.

k	0	1	2	3	4	5	6	7	8
$T_0(18)$	1	2	0	0	0	0	0	0	1
$T_1(18)$	0	-1	2	2	0	0	0	1	0
$T_2(18)$	0	0	-1	0	2	2	1	0	0
$T_3(18)$	0	0	0	-1	0	1	2	2	0
$U(18)$	8	10	8	10	8	10	8	10	8

Table 1: The coefficients $a_{m,k}$ for $N = 18$.

k	0	1	2	3	4	5	6	7	8	9
$T_0(20)$	1	2	0	0	0	0	0	0	0	1
$T_1(20)$	0	-1	2	2	0	0	0	0	1	0
$T_2(20)$	0	0	-1	0	2	2	0	1	0	0
$T_3(20)$	0	0	0	-1	0	0	3	2	0	0
$T_4(20)$	0	0	0	0	-1	1	0	0	2	2
$U(20)$	9	11	9	11	9	11	9	11	9	11
$V(20)$	1	1	1	1	1	3	3	3	3	3

Table 2: The coefficients $a_{m,k}$ for $N = 20$.

Proposition 4.3. For an even $N \geq 4$, let $U(N)$ be the left-hand side of the congruence (6). Then

$$(26) \quad U(N) = \sum_{m=0}^{\lfloor N/4 \rfloor - 1} \left(\frac{N}{2} - 2m - 1 \right) T_m(N).$$

If N is a multiple of 4, let $V(N)$ be the left-hand side of the congruence (19). Then

$$(27) \quad V(N) = \sum_{m=0}^{\lfloor N/4 \rfloor - 1} T_m(N).$$

Proof. Using (25) and changing the orders of summation, it is clear that we need to show

$$(28) \quad U(N) = \sum_{k=0}^{N/2-1} \left(\sum_{m=0}^{\lfloor N/4 \rfloor - 1} \left(\frac{N}{2} - 2m - 1 \right) a_{m,k} \right) s(k, N),$$

$$(29) \quad V(N) = \sum_{k=0}^{N/2-1} \left(\sum_{m=0}^{\lfloor N/4 \rfloor - 1} a_{m,k} \right) s(k, N), \quad \text{when } 4 \mid N.$$

(a) First, fix k with $0 \leq k \leq \lfloor N/4 \rfloor - 1$. Then we see from the left-hand side of (18) that $a_{0,0} = 1$, while

$$(30) \quad a_{k,k} = -1, \quad a_{\lfloor k/2 \rfloor, k} := 2, \quad 1 \leq k \leq \lfloor N/4 \rfloor - 1,$$

and $a_{m,k} = 0$ for all other m , $0 \leq m \leq \lfloor N/4 \rfloor - 1$. This means that the inner sum in (29) is always 1 for all even N , which by (19) proves that (27) is true for the first $\lfloor N/4 \rfloor$ coefficients of the $s(k, N)$.

Next, the inner sum of (28) is $N/2 - 1$ when $k = 0$, and for $1 \leq k \leq \lfloor N/4 \rfloor - 1$ it is, by (30),

$$(31) \quad - \left(\frac{N}{2} - 2k - 1 \right) + 2 \left(\frac{N}{2} - 2 \left\lfloor \frac{k}{2} \right\rfloor - 1 \right) = \frac{N}{2} - 1 + 2 \left(k - 2 \left\lfloor \frac{k}{2} \right\rfloor \right).$$

But $k - 2\lfloor k/2 \rfloor = 0$ when k is even and $k - 2\lfloor k/2 \rfloor = 1$ when k is odd. This, with (6), verifies (26) for the first $\lfloor N/4 \rfloor$ coefficients of the $s(k, N)$.

(b) Now, fix k with $\lfloor \frac{N}{4} \rfloor \leq k \leq \frac{N}{2} - 1$. Then by the left-hand side of (18), we have

$$(32) \quad a_{N/2-1-k,k} = 1, \quad a_{\lfloor k/2 \rfloor, k} := 2,$$

and $a_{m,k} = 0$ for all other m , $0 \leq m \leq \lfloor \frac{N}{4} \rfloor - 1$. If $N/2 - 1 - k = \lfloor k/2 \rfloor$, then we take their combined value to be their sum, namely 3 (see also Table 2, $k = 6$).

If $4 \mid N$, then in the inner sum in (29), both terms (32) occur for all k in the given range, their sum being 3. This, with (19), completes the proof of (27).

Finally, we consider the inner sum in (28). For each k with $\lfloor \frac{N}{4} \rfloor \leq k \leq \frac{N}{2} - 1$; it is, by (32),

$$\left(\frac{N}{2} - 2 \left(\frac{N}{2} - 1 - k \right) - 1 \right) + 2 \left(\frac{N}{2} - 2 \left\lfloor \frac{k}{2} \right\rfloor - 1 \right) = \frac{N}{2} - 1 + 2 \left(k - 2 \left\lfloor \frac{k}{2} \right\rfloor \right).$$

This is the same as the right-hand side of (31), and therefore (26) is verified for the remaining coefficients of the $s(k, N)$. The proof is now complete. $\square$

Remark 4.4. It follows from the first half of part (b) of the above proof that a somewhat more complicated analogue of the congruence (19) holds also for $N \equiv 2 \pmod{4}$. We leave the statement and proof to the reader.

5. The case N odd

It follows from the definition (1) that for all $N \geq 1$ and $0 \leq k \leq N - 1$, we have

$$(33) \quad s(k, N) \equiv s(2k, 2N) + s(2k + 1, 2N) \pmod{p}.$$

This means that any congruence involving the sums $s(k, N)$ immediately leads to a congruence involving the sums $s(k, 2N)$. However, to go in the other direction we require that all pairs $s(2k, 2N)$ and $s(2k + 1, 2N)$ have the same coefficients. This is not the case for any of the congruences proved so far in this paper, so none of these can be reduced to congruences for odd N .

Still, it turns out that at least one such congruence exists for composite odd N . To keep our notation consistent, the parameter N , if it is odd, will be denoted by M in what follows.

Proposition 5.1. *Let M be an odd positive integer and $r, t \geq 3$ be integers such that $M = rt$. If M is not divisible by the odd prime p , then we have*

$$(34) \quad \sum_{k=0}^{\frac{M-3}{2}} \left(\frac{(r-1)(t-1)}{2} + k - r \left\lfloor \frac{k}{r} \right\rfloor - t \left\lfloor \frac{k}{t} \right\rfloor \right) s(k, M) \equiv 0 \pmod{p}.$$

Proof. We use the congruence (2) and rewrite the terms $s(k, M)$ for all k with $(M-1)/2 \leq k \leq M-1$ using (4). Then, we obtain

$$(35) \quad Mq_p(M) \equiv - \sum_{k=0}^{\frac{M-3}{2}} (M-1-2k)s(k, M) \pmod{p}.$$

Moreover, the logarithmic property (23) implies

$$(36) \quad Mq_p(M) \equiv t(rq_p(r)) + r(tq_p(t)) \pmod{p}.$$

Now, we use an immediate extension of (33), namely

$$s(k, r) \equiv s(tk, M) + s(tk+1, M) + \cdots + s(tk+t-1, M) \pmod{p},$$

along with (2), to obtain

$$rq_p(r) \equiv \sum_{k=0}^{r-1} ks(k, r) \equiv \sum_{k=0}^{M-1} \left\lfloor \frac{k}{t} \right\rfloor s(k, M) \pmod{p},$$

and, with (4) again,

$$(37) \quad rq_p(r) \equiv - \sum_{k=0}^{\frac{M-3}{2}} \left(\left\lfloor \frac{M-1-k}{t} \right\rfloor - \left\lfloor \frac{k}{t} \right\rfloor \right) s(k, M) \pmod{p}.$$

To simplify the summand, we let

$$k = tj + l, \quad j = \left\lfloor \frac{k}{t} \right\rfloor, \quad l = 0, 1, \dots, t-1.$$

Then,

$$\begin{aligned} \left\lfloor \frac{M-1-k}{t} \right\rfloor - \left\lfloor \frac{k}{t} \right\rfloor &= \left\lfloor \frac{rt-1-tj-l}{t} \right\rfloor - \left\lfloor \frac{tj+l}{t} \right\rfloor \\ &= \left\lfloor \frac{t(r-j-1)+t-1-l}{t} \right\rfloor - j \\ &= (r-j-1) - j \\ &= r - 2 \left\lfloor \frac{k}{t} \right\rfloor - 1, \end{aligned}$$

so the congruence (37) becomes

$$rq_p(r) \equiv - \sum_{k=0}^{\frac{M-3}{2}} \left(r - 2 \left\lfloor \frac{k}{t} \right\rfloor - 1 \right) s(k, M) \pmod{p},$$

and by symmetry,

$$tq_p(t) \equiv - \sum_{k=0}^{\frac{M-3}{2}} \left(t - 2 \left\lfloor \frac{k}{r} \right\rfloor - 1 \right) s(k, M) \pmod{p}.$$

Finally, if we substitute these last two congruences into (36) and equate the result with (35), we immediately obtain the desired congruence (34). $\square$

Remark 5.2. One may ask whether M can also be a prime. In that case, one of r and t is 1, say $t = 1$. But then the left-hand side of (34) vanishes, and the congruence becomes meaningless.

As mentioned at the beginning of this section, any congruence involving the sums $s(k, M)$ can be rewritten as a congruence involving the sums $s(k, N)$ with $N = 2M$, via (33). If we do this with (34), it turns out that the resulting congruence is linearly independent of the congruences (18).

Proposition 5.3. *Suppose that $N = 2M$, where $M = rt$ is an odd integer, with $r \geq 3$ and $t \geq 3$. Then for all primes $p > N$, the system of congruences (18) together with*

$$(38) \quad \sum_{k=0}^{\frac{N-6}{4}} \left(\frac{(r-1)(t-1)}{2} + k - r \left\lfloor \frac{k}{r} \right\rfloor - t \left\lfloor \frac{k}{t} \right\rfloor \right) (s(2k, N) + s(2k+1, N)) \equiv 0 \pmod{p}$$

is linearly independent (modulo p).

Proof. We augment the coefficient matrix of the expressions (25) by one additional row corresponding to the coefficients in (38). To simplify notation, we set

$$a := (r-1)(t-1)/2.$$

For $0 \leq k \leq (N-6)/4$ and $m = (N-2)/4 = \lfloor N/4 \rfloor$, we put

$$(39) \quad \begin{cases} a_{m,2k} = a_{m,2k+1} := a + k - r \left\lfloor \frac{k}{r} \right\rfloor - t \left\lfloor \frac{k}{t} \right\rfloor, \\ a_{m,k} := 0 \quad \text{for } \frac{N}{2} - 1 \leq k \leq N-1. \end{cases}$$

As in the proof of Proposition 4.2, we will consider only the coefficients $a_{m,k}$ for k with $0 \leq k \leq N/2 - 1$. Thus, we have the integer matrix $A = (a_{m,k})$ of size $(N+2)/4 \times N/2$, where $0 \leq m \leq \frac{N-2}{4}$ and $0 \leq k \leq \frac{N}{2} - 1$. Denote the rows of A by $\mathbf{r}(0), \dots, \mathbf{r}(\frac{N-2}{4})$.

The submatrix corresponding to $0 \leq m, k \leq \frac{N-6}{4}$, which was considered in the proof of Proposition 4.2, is upper triangular with main diagonal $(1, -1, \dots, -1)$. Hence, there exist integer coefficients $c_0 = a, c_1, \dots, c_{\frac{N-6}{4}}$ such that

$$(40) \quad \sum_{m=0}^{\frac{N-6}{4}} c_m \mathbf{r}(m) - \mathbf{r}(\frac{N-2}{4}) := \mathbf{w} = (w(0), \dots, w(\frac{N}{2} - 1)) \pmod{p},$$

where $w(0) \equiv w(1) \equiv \dots \equiv w(\frac{N-6}{4}) \equiv 0 \pmod{p}$.

By (18) and (39), the last column $(N/2 - 1)$ of the matrix A has only zeros as entries, with the exception of the initial entry which is 1 (see Table 1 as an illustration). Therefore, by (40), $w(N/2 - 1) = c_0 = a$. But this means that the matrix consisting of the rows $\mathbf{r}(0), \dots, \mathbf{r}(\frac{N-6}{4})$ and $\mathbf{w}$, and of the columns numbered $0, \dots, \frac{N-6}{4}$ and $\frac{N}{2} - 1$, is nonsingular modulo p . Note that here we have used the fact that $p \nmid a$, which holds by our assumption that $p > N$. This completes the proof. $\square$

6. Further congruences

The congruence (13) is particularly pleasing because it has only three terms, regardless of the size of N . It turns out that there are several more three-term or four-term congruences. However, they are not linearly independent of the congruences in Proposition 4.2.

Corollary 6.1. *Let $N \geq 2$ be an even integer and p an odd prime with $p \nmid N$. Then for $N = 6n + 2$, we have*

$$(41) \quad -s(n, N) + 3s(2n, N) + 2s(2n + 1, N) \equiv 0 \pmod{p},$$

while for $N = 6n + 4$,

$$(42) \quad -s(n, N) + 2s(2n, N) + 3s(2n + 1, N) \equiv 0 \pmod{p},$$

and for $N = 6(n + 1)$,

$$(43) \quad -s(n, N) + 2s(2n, N) + 2s(2n + 1, N) + s(2n + 2, N) \equiv 0 \pmod{p}.$$

Proof. To prove (41) for $n \geq 1$, we use (12) with $N = 6n + 2$ and $m = n + 1$. Then

$$\sum_{k=0}^n s(k, N) + 2 \sum_{k=n+1}^{2n+1} s(k, N) + \sum_{k=2n}^{3n} s(k, N) \equiv 0 \pmod{p}.$$

Similarly, with $m = n$, we get

$$\sum_{k=0}^{n-1} s(k, N) + 2 \sum_{k=n}^{2n-1} s(k, N) + \sum_{k=2n+1}^{3n} s(k, N) \equiv 0 \pmod{p}.$$

If we subtract the second congruence from the first congruence, we immediately obtain (41). For $n = 0$, (41) is true by (5) for $N = 2$. For (42) and (43), we proceed similarly, in both cases taking $m = n + 1$ and $m = n$ again. $\square$

These congruences, as well as the following one, could also be derived with methods similar to those of the proof of Proposition 3.4.

Corollary 6.2. *Let $N = 4n$ and p be an odd prime with $p \nmid N$. Then*

$$(44) \quad -s(n - 1, N) + s(n, N) + 2s(2n - 2, N) + 2s(2n - 1, N) \equiv 0 \pmod{p}.$$

Proof. We use (12) with $N = 4n$ and $m = n - 1$, and rewrite it as

$$\begin{aligned} \sum_{k=0}^{n-2} s(k, N) + 2[s(n - 1, N) + s(n, N)] + 3 \sum_{k=n+1}^{2n-3} s(k, N) \\ + s(2n - 2, N) + s(2n - 1, N) \equiv 0 \pmod{p}. \end{aligned}$$

If we subtract this from (19), we immediately obtain (44). $\square$

Acknowledgements. We are most grateful to Paulo Ribenboim for first bringing us together, and for his encouragement, interest, and generosity shown to both of us over the years. The first author was supported in part by the NSERC. The second author was supported by the Grant Agency of the Czech Republic (Algebraic, Analytic and

Combinatorial Number Theory, 201/07/0191) and the results were obtained while subsidized by the Ministry of Education, Youth and Sports of the Czech Republic (research plan MSM0021630518 "Simulation modelling of mechatronic systems").

REFERENCES

- [1] P. Cikánek, *A special extension of Wieferich's criterion*, Math. Comp. **62**, 1994, no. 206, 923–930.
- [2] K. Dilcher and L. Skula, *A new criterion for the first case of Fermat's last theorem*, Math. Comp. **64**, 1995, no. 209, 363–392.
- [3] G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen welche von zwei Elementen abhaengen und durch gewisse lineare Funktional-Gleichungen definiert werden*. In: Bericht ueber die zur Bekanntmachung geeigneten Verhandlungen der Koenigl. Preuss. Akademie der Wissenschaften zu Berlin, 1850, 36–42. Mathematische Werke (2nd ed.), Gotthold Eisenstein, Band II, Chelsea, New York, 1989, 705–711.
- [4] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **39**, 1938, no. 2, 350–360.
- [5] M. Lerch, *Zur Theorie des Fermatschen Quotienten $(a^{p-1} - 1)/p = q(a)$* , Math. Ann. **60**, 1905, no. 4, 471–490.
- [6] P. Ribenboim, *13 Lectures on Fermat's last theorem*, Springer-Verlag, New York - Heidelberg, 1979, xvi+302 pp.
- [7] L. Skula, *A note on some relations among special sums of reciprocals modulo p* , Math. Slovaca **58**, 2008, no. 1, 5–10.
- [8] Z.H. Sun and Z.W. Sun *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60**, 1992, no. 4, 371–388.
- [9] H.S. Vandiver, *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem*, J. Reine Angew. Math. **144**, 1914, 314–318.
- [10] H.C. Williams, *A note on the Fibonacci quotient $F_{p-\varepsilon}/p$* , Canad. Math. Bull. **25**, 1982, no. 3 366–370.
- [11] H.C. Williams, *Some formulas concerning the fundamental unit of a real quadratic field*, Discrete Math. **92**, 1991, no. 1-3, 431–440.

K. DILCHER, DEPT. OF MATH. AND STAT, DALHOUSIE U., HALIFAX, NOVA SCOTIA, B3H 3J5, CANADA
 dilcher@mathstat.dal.ca

L. SKULA, INSTITUTE OF MATH., FACULTY OF MATHEMATICAL ENGINEERING, U. OF TECHNOLOGY TECHNICKÁ 2, 616 69 BRNO, CZECH REPUBLIC
 skula@fme.vutbr.cz