An analog of Wolstenholme's theorem

Boaz Cohen[*]

Department of Computer Science, The Academic College of Tel-Aviv, Rabenu Yeruham St., P.O.B. 8401 Yaffo, 6818211, Israel

Received August 26, 2022; accepted March 29, 2023

Abstract. In this paper, we shall prove an analogous version of Wolstenholme's theorem, namely, given a prime number $p \geqslant 2$ and positive integers a, b, m such that $p \nmid m$, we shall determine the maximal prime power p^e, which divides the numerator of the fraction

$$\frac{1}{m} + \frac{1}{m+p^b} + \frac{1}{m+2p^b} + \ldots + \frac{1}{m+(p^a-1)p^b},$$

when written in reduced form, with the exception of one case, where $p = 2$, $b = 1$, $m > 1$ and $2^a \| m-1$. In this exceptional case, a lower bound for e is given.

AMS subject classifications: 11A05, 11A07, 11A41
Keywords: Wolstenholme's theorem, Bauer's theorem, congruences, primes

1. Introduction

The classical Wolstenholme's theorem states that if $p > 3$ is a prime number, then the numerator of the fraction

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}$$

is divisible by p^2. The proof can be found in [3, pp. 112–114]. Let us illustrate this result. For $p = 13$, we have

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} = \frac{86021}{27720},$$

and here indeed $13^2 \mid 86021$. We remark that for some primes, the numerator in Wolstenholme's theorem can be divisible by p^3, even if the fraction is written in reduced form. These prime numbers, which satisfy a stronger version of Wolstenholme's theorem, are called Wolstenholme primes. The only Wolstenholme primes known so far are 16843 and 2124679, though it is conjectured that their number is infinite. Wolstenholme's theorem has many generalizations and extensions. One of them is due to L. Carlitz [1] and it asserts as follows: if m is an arbitrary integer, then for each prime $p > 3$, the numerator of the fraction

$$\frac{1}{mp+1} + \frac{1}{mp+2} + \ldots + \frac{1}{mp+(p-1)}$$

[*] Corresponding author. *Email address:* `arctanx@gmail.com` (Boaz Cohen)

is divisible by p^2. Further generalization can be found in [5].

In this paper, we shall prove the following analog of Wolstenholme's theorem: if p is an odd prime number and a, b, m are positive integers such that $p \nmid m$, then the numerator of the fraction

$$\frac{1}{m} + \frac{1}{m+p^b} + \frac{1}{m+2p^b} + \ldots + \frac{1}{m+(p^a-1)p^b},$$

when written in reduced form, is divisible by p^a but not by p^{a+1}. For example, for $p = 3$, $a = 2$, $b = 1$ and $m = 2$, we obtain that

$$\frac{1}{2} + \frac{1}{5} + \frac{1}{8} + \frac{1}{11} + \frac{1}{14} + \frac{1}{17} + \frac{1}{20} + \frac{1}{23} + \frac{1}{26} = \frac{3688785}{3131128},$$

and here indeed $3^2 \| 3688785$.

In the case of the prime $p = 2$ one needs to distinguish cases according to whether $b \geqslant 2$ or $b = 1$: Suppose that a, b, m are positive integers such that $2 \nmid m$. If $b \geqslant 2$, then the numerator of the fraction

$$\frac{1}{m} + \frac{1}{m+2^b} + \frac{1}{m+2\cdot 2^b} + \frac{1}{m+3\cdot 2^b} + \ldots + \frac{1}{m+(2^a-1)2^b},$$

when written in reduced form, is divisible by 2^a but not by 2^{a+1}. For example, for $a = 4$, $b = 2$ and $m = 1$, we obtain that

$$1 + \frac{1}{5} + \frac{1}{9} + \frac{1}{13} + \frac{1}{17} + \ldots + \frac{1}{61} = \frac{42155877944972752}{24142663793423175},$$

and here indeed $2^4 \| 42155877944972752$.

When $b = 1$, the results depend upon the value of m. If $m = 1$, then the numerator of the fraction

$$1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots + \frac{1}{1+2(2^a-1)}$$

when written in reduced form, is divisible by 2^{2a} but not by 2^{2a+1}. For example, for $a = 4$, we obtain that

$$1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \ldots + \frac{1}{31} = \frac{10686452707072}{4512611027925},$$

and here indeed $2^8 \| 10686452707072$.

If $m > 1$ and c is the positive integer such that $2^c \| m-1$, then the maximal prime power 2^e which divides the numerator of the fraction

$$\frac{1}{m} + \frac{1}{m+2} + \frac{1}{m+4} + \frac{1}{m+6} + \ldots + \frac{1}{m+2(2^a-1)},$$

when written in reduced form, is either $2^{a+\min\{a,c\}}$ if $a \neq c$, or at least 2^{2a+1} if $a = c$. As an example, for $a = 4$ and $m = 9$, we obtain that

$$\frac{1}{9} + \frac{1}{11} + \frac{1}{13} + \frac{1}{15} + \ldots + \frac{1}{39} = \frac{134154786738304}{166966608033225}.$$

In this case, $2^3 \| m-1$, so $c = 3$, and indeed $2^7 \| 134154786738304$.

2. Preliminaries

We begin with a brief overview of several concepts concerning elementary symmetric polynomials. Recall that the kth elementary symmetric function in n variables is defined by

$$e_k(x_1, x_2, \ldots, x_n) = \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} x_{i_1}x_{i_2}\cdots x_{i_k}.$$

For example, the elementary symmetric functions in 4 variables are:

$$\begin{aligned}
e_1(x_1,x_2,x_3,x_4) &= x_1+x_2+x_3+x_4\\
e_2(x_1,x_2,x_3,x_4) &= x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4\\
e_3(x_1,x_2,x_3,x_4) &= x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4\\
e_4(x_1,x_2,x_3,x_4) &= x_1x_2x_3x_4.
\end{aligned}$$

It is convenient to define $e_0(x_1, x_2, \ldots, x_n) = 1$. Note that the kth elementary symmetric function is homogenous of degree k, that is,

$$e_k(\lambda x_1, \lambda x_2, \ldots, \lambda x_n) = \lambda^k e_k(x_1, x_2, \ldots, x_n)$$

for every λ.

If we expand the product $(z-x_1)(z-x_2)\cdots(z-x_n)$ into a polynomial in the variable z, we get the following relation:

$$(z-x_1)(z-x_2)\cdots(z-x_n) = \sum_{k=0}^{n}(-1)^k e_k(x_1, x_2, \ldots, x_n)z^{n-k}.$$

We continue with the following result, which will helpful in the sequel.

Proposition 1. *Suppose that p is a prime number and let t be a positive integer such that $p \nmid t$. If a, b are integers such that $0 \leqslant b \leqslant a$ and $t \leqslant p^{a-b}$, then*

$$p^{a-b}\| \binom{p^a}{p^b t}.$$

Proof. If $a = b$, then $t = 1$ and the result certainly holds. So assume that $a > b$. For a positive number n define $\nu_p(n)$ to be the multiplicity of p in n, namely $\nu_p(n)$ is the non-negative integer such that $p^{\nu_p(n)}\|n$. By [4, pp. 90–91], we know that

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Here the lower square-bracket notation $\lfloor x \rfloor$ denotes the largest integer not exceeding the real number x. Hence

$$\begin{aligned}
\nu_p((p^b t)!) &= \left\lfloor \frac{p^b t}{p} \right\rfloor + \left\lfloor \frac{p^b t}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{p^b t}{p^b} \right\rfloor + \left\lfloor \frac{p^b t}{p^{b+1}} \right\rfloor + \left\lfloor \frac{p^b t}{p^{b+2}} \right\rfloor + \ldots\\
&= (p^{b-1} + p^{b-2} + \ldots + p + 1)t + \left\lfloor \frac{t}{p} \right\rfloor + \left\lfloor \frac{t}{p^2} \right\rfloor + \ldots\\
&= t\frac{p^b - 1}{p-1} + \nu_p(t!).
\end{aligned}$$

Now, for a real number x and an integer n, we have $\lfloor n+x\rfloor = n+\lfloor x\rfloor$ and $\lfloor -x\rfloor = -1-\lfloor x\rfloor$ if x is not an integer (see [4, p. 90]). Therefore, as $a>b$, we get

$$\begin{aligned}\nu_p((p^{a-b}-t)!) &= \left\lfloor \frac{p^{a-b}-t}{p}\right\rfloor + \left\lfloor \frac{p^{a-b}-t}{p^2}\right\rfloor + \ldots + \left\lfloor \frac{p^{a-b}-t}{p^{a-b}}\right\rfloor \\ &= (p^{a-b-1}+\ldots+p+1) + \left\lfloor -\frac{t}{p}\right\rfloor + \left\lfloor -\frac{t}{p^2}\right\rfloor + \ldots + \left\lfloor -\frac{t}{p^{a-b}}\right\rfloor \\ &= \frac{p^{a-b}-1}{p-1} - \underbrace{(1+1+\ldots+1)}_{a-b \text{ times}} - \left(\left\lfloor \frac{t}{p}\right\rfloor + \left\lfloor \frac{t}{p^2}\right\rfloor + \ldots + \left\lfloor \frac{t}{p^{a-b}}\right\rfloor\right) \\ &= \frac{p^{a-b}-1}{p-1} - (a-b) - \nu_p(t!).\end{aligned}$$

Observe that the third equality follows from the fact that $p\nmid t$. From the first formula we deduce that

$$\nu_p((p^a)!) = 1\cdot\frac{p^a-1}{p-1} + \nu_p(1) = \frac{p^a-1}{p-1},$$

and the first and the second formula yield:

$$\begin{aligned}\nu_p((p^a-p^bt)!) &= \nu_p((p^b(p^{a-b}-t))!) \\ &= (p^{a-b}-t)\frac{p^b-1}{p-1} + \nu_p((p^{a-b}-t)!) \\ &= (p^{a-b}-t)\frac{p^b-1}{p-1} + \frac{p^{a-b}-1}{p-1} - (a-b) - \nu_p(t!).\end{aligned}$$

Hence

$$\nu_p\left(\binom{p^a}{p^bt}\right) = \nu_p((p^a)!) - \nu_p((p^bt)!) - \nu_p((p^a-p^bt)!) = a-b,$$

and the proof is complete. □

3. The value of $e_k(0,1,2,\ldots,p^a-1)$ modulo p^a

Let p be a prime number and a a positive integer. Our aim in this section is to compute the values of the expressions $e_k(0,1,2,\ldots,p^a-1)$ modulo p^a, where e_k denotes the kth elementary symmetric function. As we shall see, the values of these expressions will play an important role in our analysis. To do so, we shall use a specific generalization of Lagrange's Indeterminate Congruence Theorem. Recall that Lagrange's Indeterminate Congruence Theorem claims that

$$x(x-1)(x-2)\cdots(x-p+1) \equiv x^p - x \pmod{p},$$

where the congruence indicates that the corresponding coefficients of the polynomials are congruent modulo p. A generalization of Lagrange's Indeterminate Congruence Theorem was given by Bauer (see theorems 126 and 127 of [3]) and later by Vandiver. Equations (8') and (9') of [6], listed below, are the ones we need for our analysis:

Theorem 1 (Vandiver [6]). *Let p be a prime number and let a be a positive integer.*

(a) *If $p > 2$, then*

$$x(x-1)(x-2)\cdots(x-(p^a-1)) \equiv (x^p - x)^{p^{a-1}} \pmod{p^a}.$$

(b) *If $p = 2$ and $a \geqslant 2$, then*

$$x(x-1)(x-2)\cdots(x-(2^a-1)) \equiv \big((x^2-x)^2 - 2(x^2-x)\big)^{2^{a-2}} \pmod{2^a}.$$

Proposition 2. *Suppose that p is an odd prime number, a is a positive integer and $0 \leqslant k \leqslant p^a$ is an integer. Then*

$$e_k(0,1,2,\ldots,p^a-1) \equiv (-1)^k(-1)^{k/(p-1)}\binom{p^{a-1}}{\frac{k}{p-1}} \pmod{p^a}$$

if $p-1 \mid k$ and $0 \leqslant k \leqslant p^a - p^{a-1}$, and $e_k(0,1,2,\ldots,p^a-1) \equiv 0 \pmod{p^a}$ otherwise.

Proof. On the one hand, by Theorem 1(a)

$$\begin{aligned} x(x-1)(x-2)\cdots(x-(p^a-1)) &\equiv (x^p-x)^{p^{a-1}} \\ &= \sum_{i=0}^{p^{a-1}}\binom{p^{a-1}}{i}(x^p)^{p^{a-1}-i}(-x)^i \\ &= \sum_{i=0}^{p^{a-1}}\binom{p^{a-1}}{i}(-1)^i x^{p^a-i(p-1)} \pmod{p^a}, \end{aligned}$$

so the powers of x in the sum are of the form x^{p^a-k}, where $p-1 \mid k$ and $0 \leqslant k \leqslant (p-1)p^{a-1} = p^a - p^{a-1}$. On the other hand,

$$x(x-1)(x-2)\cdots(x-(p^a-1)) = \sum_{k=0}^{p^a}(-1)^k e_k(0,1,2,\ldots,p^a-1)x^{p^a-k}.$$

Now, comparing the corresponding exponents yields

$$e_k(0,1,2,\ldots,p^a-1) \equiv (-1)^k(-1)^{k/(p-1)}\binom{p^{a-1}}{\frac{k}{p-1}} \pmod{p^a}$$

if $p-1 \mid k$ and $0 \leqslant k \leqslant p^a - p^{a-1}$, and $e_k(0,1,2,\ldots,p^a-1) \equiv 0 \pmod{p^a}$ otherwise, as required. □

Proposition 3. *Suppose that $a \geqslant 3$ and $0 \leqslant k \leqslant 2^a$ are integers. Then*

$$e_k(0,1,2,\ldots,2^a-1) \equiv \begin{cases} 1, & \text{if } k=0 \\ 2^{a-1}, & \text{if } k=1 \\ 2^{a-2}, & \text{if } k=2 \\ 0, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is odd} \\ \binom{2^{a-1}}{k} & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is even} \\ 2^{a-1}, & \text{if } 2^{a-1}<k\leqslant 2^{a-1}+2 \\ 0, & \text{if } 2^{a-1}+2<k\leqslant 2^a \end{cases} \pmod{2^a}.$$

Proof. Set $f(x) = x(x-1)(x-2)\cdots(x-(2^a-1))$. Note that by Theorem 1(b)

$$f(x) \equiv \big((x^2-x)^2 - 2(x^2-x)\big)^{2^{a-2}} = \sum_{k=0}^{2^{a-2}} \binom{2^{a-2}}{k}(-2)^k(x^2-x)^{2^{a-1}-k} \pmod{2^a}.$$

We claim that

$$2^a \mid 2^k\binom{2^{a-2}}{k}$$

for every $3 \leqslant k \leqslant 2^a$. Let t be the non-negative integer such that $2^t \| k$. By Proposition 1,

$$2^{a-2-t} \| \binom{2^{a-2}}{k}.$$

Hence, in order to prove our claim, it suffices to prove that $a \leqslant k + a - 2 - t$, that is, $t + 2 \leqslant k$. Indeed, if $0 \leqslant t \leqslant 1$, then $t + 2 \leqslant 3 \leqslant k$, and if $t \geqslant 2$, then $t + 2 \leqslant 2^t \leqslant k$, as required. Since $a \geqslant 3$, it follows that

$$\begin{aligned} f(x) &\equiv (x^2-x)^{2^{a-1}} - 2\binom{2^{a-2}}{1}(x^2-x)^{2^{a-1}-1} + 4\binom{2^{a-2}}{2}(x^2-x)^{2^{a-1}-2} \\ &= (x^2-x)^{2^{a-1}} - 2^{a-1}(x^2-x)^{2^{a-1}-1} + 2^{a-1}(2^{a-2}-1)(x^2-x)^{2^{a-1}-2} \\ &\equiv (x^2-x)^{2^{a-1}} + 2^{a-1}(x^2-x)^{2^{a-1}-1} + 2^{a-1}(x^2-x)^{2^{a-1}-2} \\ &= (x^2-x)^{2^{a-1}} + 2^{a-1}\big(\underbrace{(x^2-x)^{2^{a-1}-1} + (x^2-x)^{2^{a-1}-2}}_{g(x)}\big) \pmod{2^a}. \end{aligned}$$

We shall prove that

$$g(x) \equiv x^{2^a-2} + \sum_{j=1}^{2^{a-2}} x^{2^a-(2j+1)} + x^{2^{a-1}-2} \pmod 2$$

for every $a \geqslant 3$. Set $A = 2^{a-1}$. Note that $A \geqslant 4$ and

$$\begin{aligned} g(x) &= \sum_{i=0}^{A-1}(-1)^i\binom{A-1}{i}x^{2A-2-i} + \sum_{j=0}^{A-2}(-1)^j\binom{A-2}{j}x^{2A-4-j} \\ &= x^{2A-2} - (A-1)x^{2A-3} + \sum_{i=2}^{A-1}(-1)^i\binom{A-1}{i}x^{2A-2-i} \\ &\quad + \sum_{j=0}^{A-3}(-1)^j\binom{A-2}{j}x^{2A-4-j} + x^{A-2} \\ &= x^{2A-2} - (A-1)x^{2A-3} + \sum_{j=0}^{A-3}(-1)^j\left(\binom{A-1}{j+2} + \binom{A-2}{j}\right)x^{2A-4-j} + x^{A-2} \\ &\equiv x^{2A-2} + x^{2A-3} + \sum_{j=0}^{A-3}\left(\binom{A-1}{j+2} + \binom{A-2}{j}\right)x^{2A-4-j} + x^{A-2} \pmod 2. \end{aligned}$$

We shall prove now that

$$\binom{A-1}{j+2} + \binom{A-2}{j} \equiv \begin{cases} 0, & \text{if } j \text{ is even} \\ 1, & \text{if } j \text{ is odd} \end{cases} \pmod 2,$$

for every $0 \leqslant j \leqslant A-3$. To do so, we shall use Lucas's theorem [2], which claims, in particular for the prime $p = 2$, that if m, n are non-negative integers and if

$$m = m_k 2^k + \ldots + m_2 2^2 + m_1 2 + m_0$$
$$n = n_k 2^k + \ldots + n_2 2^2 + n_1 2 + n_0$$

are the base-2 expansions of m and n, respectively, then the following congruence relation holds:

$$\binom{m}{n} \equiv \binom{m_k}{n_k} \cdots \binom{m_2}{n_2}\binom{m_1}{n_1}\binom{m_0}{n_0} \pmod 2,$$

where we use the convention that $\binom{m}{n} = 0$ whenever $m < n$. In our case, the base-2 expansions of $A-1$ and of $A-2$ are

$$A - 1 = 2^{a-1} - 1 = 2^{a-2} + \ldots + 2^2 + 2 + 1$$

and

$$A - 2 = 2^{a-1} - 2 = 2^{a-2} + \ldots + 2^2 + 2.$$

If

$$j + 2 = m_{a-2} 2^{a-2} + \ldots + m_2 2^2 + m_1 2 + m_0$$

and

$$j = n_{a-2} 2^{a-2} + \ldots + n_2 2^2 + n_1 2 + n_0$$

are the base-2 expansions of j and $j+2$, then

$$\binom{A-1}{j+2} \equiv \binom{1}{m_{a-2}} \cdots \binom{1}{m_2}\binom{1}{m_1}\binom{1}{m_0} \pmod 2$$

and

$$\binom{A-2}{j} \equiv \binom{1}{n_{a-2}} \cdots \binom{1}{n_2}\binom{1}{n_1}\binom{0}{n_0} \pmod 2.$$

Since each of $m_0, m_1, \ldots, m_{a-2}$ and $n_0, n_1, \ldots, n_{a-2}$ is either 0 or 1, it follows that $\binom{A-1}{j+2} \equiv 1 \pmod 2$. If j is odd, then $n_0 = 1$, so $\binom{A-2}{j} \equiv 0 \pmod 2$, and if j is even, then $n_0 = 0$, so $\binom{A-2}{j} \equiv 1 \pmod 2$. Therefore,

$$\binom{A-1}{j+2} + \binom{A-2}{j} \equiv \begin{cases} 0, & \text{if } j \text{ is even} \\ 1, & \text{if } j \text{ is odd} \end{cases} \pmod 2,$$

as required. Hence

$$\begin{aligned} g(x) &\equiv x^{2A-2} + x^{2A-3} + \sum_{\substack{0\leqslant j\leqslant A-3\\ j \text{ is odd}}} x^{2A-4-j} + x^{A-2} \\ &= x^{2A-2} + x^{2A-3} + x^{2A-5} + x^{2A-7} + \cdots + x^{2A-(A+1)} + x^{A-2} \\ &= x^{2A-2} + \sum_{j=1}^{A/2} x^{2A-(1+2j)} + x^{A-2} \\ &= x^{2^a-2} + \sum_{j=1}^{2^{a-2}} x^{2^a-(2j+1)} + x^{2^{a-1}-2} \pmod 2, \end{aligned}$$

as claimed. Therefore,

$$\begin{aligned} f(x) &\equiv (x^2-x)^{2^{a-1}} + 2^{a-1}\left(x^{2^a-2} + \sum_{j=1}^{2^{a-2}} x^{2^a-(2j+1)} + x^{2^{a-1}-2}\right) \\ &\equiv \sum_{i=0}^{2^{a-1}} (-1)^i \binom{2^{a-1}}{i} x^{2^a-i} \\ &\quad + 2^{a-1}\left(x^{2^a-2} + \sum_{j=1}^{2^{a-2}} x^{2^a-(2j+1)} + x^{2^a-(2^{a-1}+2)}\right) \pmod{2^a}. \end{aligned}$$

Now, given $0 \leqslant k \leqslant 2^a$, let c_k be the coefficient of the term x^{2^a-k} in $f(x)$. By the above expression we deduce that

$$c_k \equiv \begin{cases} 1, & \text{if } k=0 \\ -\binom{2^{a-1}}{1}, & \text{if } k=1 \\ \binom{2^{a-1}}{2} + 2^{a-1}, & \text{if } k=2 \\ 2^{a-1} - \binom{2^{a-1}}{k}, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is odd} \\ \binom{2^{a-1}}{k}, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is even} \\ 2^{a-1}, & \text{if } 2^{a-1}<k\leqslant 2^{a-1}+2 \\ 0, & \text{if } 2^{a-1}+2<k\leqslant 2^a \end{cases} \pmod{2^a}.$$

Note that

$$-\binom{2^{a-1}}{1} = -2^{a-1} \equiv 2^{a-1} \pmod{2^a}$$

and

$$\binom{2^{a-1}}{2} + 2^{a-1} = 2^{a-2}(2^{a-1}-1) + 2^{a-1} = 2^{2a-3} + 2^{a-2} \equiv 2^{a-2} \pmod{2^a}.$$

In addition, if k is odd, then by Proposition 1 it follows that $\binom{2^{a-1}}{k} = 2^{a-1}b$, where $2 \nmid b$. Thus

$$2^{a-1} - \binom{2^{a-1}}{k} = 2^{a-1}(1-b) \equiv 2^a \cdot \frac{1-b}{2} \equiv 0 \pmod{2^a}.$$

Therefore,

$$c_k \equiv \begin{cases} 1, & \text{if } k=0 \\ 2^{a-1}, & \text{if } k=1 \\ 2^{a-2}, & \text{if } k=2 \\ 0, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is odd} \\ \binom{2^{a-1}}{k}, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is even} \\ 2^{a-1}, & \text{if } 2^{a-1}<k\leqslant 2^{a-1}+2 \\ 0, & \text{if } 2^{a-1}+2<k\leqslant 2^a \end{cases} \pmod{2^a}.$$

Since

$$f(x)=\sum_{k=0}^{2^a}(-1)^k e_k(0,1,2,\ldots,2^a-1)x^{2^a-k},$$

it follows that $(-1)^k e_k(0,1,2,\ldots,2^a-1)\equiv c_k \pmod{2^a}$, that is, $e_k(0,1,2,\ldots,2^a-1)\equiv(-1)^k c_k \pmod{2^a}$. By noting that $-2^{a-1}\equiv 2^{a-1} \pmod{2^a}$, we deduce that

$$e_k(0,1,2,\ldots,2^a-1) \equiv \begin{cases} 1, & \text{if } k=0 \\ 2^{a-1}, & \text{if } k=1 \\ 2^{a-2}, & \text{if } k=2 \\ 0, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is odd} \\ \binom{2^{a-1}}{k}, & \text{if } 2<k\leqslant 2^{a-1} \text{ and } k \text{ is even} \\ 2^{a-1}, & \text{if } 2^{a-1}<k\leqslant 2^{a-1}+2 \\ 0, & \text{if } 2^{a-1}+2<k\leqslant 2^a \end{cases} \pmod{2^a},$$

as required. □

4. Our main results

In this section, we shall prove the four main theorems of this paper. All four proofs are based on the following observation: The fraction $s=\frac{1}{a_1}+\ldots+\frac{1}{a_k}$ can be written as N/D, where $N=e_{k-1}(a_1,\ldots,a_k)$, $D=a_1\cdots a_k$, and e_{k-1} denotes the $(k-1)$th elementary symmetric function. Now, if $p\nmid D$ and $p^e\|N$, then p^e is also the maximal prime power which divides the numerator of the fraction s, when written in reduced form. Therefore, it suffices to determine the maximal power e for which $p^e\|N$. This goal will be accomplished by using the results proven in Section 3 according to different cases. We begin with the case where p is an odd prime number.

Theorem 2. *If p is an odd prime number and a,b,m are positive integers such that $p\nmid m$, then the maximal prime power p^e which divides the numerator of the fraction*

$$\frac{1}{m}+\frac{1}{m+p^b}+\frac{1}{m+2p^b}+\ldots+\frac{1}{m+(p^a-1)p^b},$$

when written in reduced form, is p^a.

Proof. Suppose that

$$\frac{1}{m}+\frac{1}{m+p^b}+\frac{1}{m+2p^b}+\ldots+\frac{1}{m+(p^a-1)p^b}=\frac{n}{d},$$

where $\gcd(n,d)=1$. We claim that $p^a\|n$. Set

$$\begin{aligned}N&=e_{p^a-1}(m,m+p^b,m+2p^b,\cdots,m+(p^a-1)p^b)\\ D&=m(m+p^b)(m+2p^b)\cdots(m+(p^a-1)p^b),\end{aligned}$$

where e_{p^a-1} denotes the (p^a-1)th elementary symmetric function. Note that $n/d=N/D$, but the fraction N/D is not necessary in its reduced form. Nevertheless, since $\gcd(m,p)=1$ and $b\geqslant 1$, it follows that $p\nmid D$, so $p^a\|n$ if and only if $p^a\|N$. Hence, it suffices to prove that $p^a\|N$. To do so, consider the polynomial

$$\begin{aligned}f(x)&=(x-m)(x-(m+p^b))(x-(m+2p^b))\cdots(x-(m+(p^a-1)p^b))\\ &=(x-m)(x-m-p^b)(x-m-2p^b)\cdots(x-m-(p^a-1)p^b)\\ &=\sum_{k=0}^{p^a}(-1)^k e_k(0,p^b,2p^b,\ldots,(p^a-1)p^b)(x-m)^{p^a-k}\\ &=\sum_{k=0}^{p^a}(-1)^k p^{bk}e_k(0,1,2,\ldots,p^a-1)(x-m)^{p^a-k}.\end{aligned}$$

We claim that $p^{bk}e_k(0,1,2,\ldots,p^a-1)\equiv 0\pmod{p^{a+1}}$ for every $1\leqslant k\leqslant p^a$.

If $k=1$, then indeed

$$p^be_1(0,1,2,\ldots,p^a-1)=p^b\cdot\frac{(p^a-1)p^a}{2}=\frac{p^a-1}{2}\cdot p^{a+b}\equiv 0\pmod{p^{a+1}},$$

as required.

Next, suppose that $k\geqslant 2$. If either $p^a-p^{a-1}<k\leqslant p^a$ or $p-1\nmid k$, then by Proposition 2 $e_k(0,1,2,\ldots,p^a-1)\equiv 0\pmod{p^a}$, so $p^{bk}e_k(0,1,2,\ldots,p^a-1)\equiv 0\pmod{p^{a+1}}$, as required.

It remains only to deal with k such that $2\leqslant k\leqslant p^a-p^{a-1}$ and $p-1\mid k$. Let t be the non-negative integer such that $p^t\|k$. Then $p^t\|\frac{k}{p-1}$ and by Proposition 1,

$$p^{a-1-t}\mid\binom{p^{a-1}}{\frac{k}{p-1}}.$$

Since by Proposition 2

$$e_k(0,1,2,\ldots,p^a-1)\equiv(-1)^k(-1)^{k/(p-1)}\binom{p^{a-1}}{\frac{k}{p-1}}\pmod{p^a},$$

it follows that

$$p^{bk}e_k(0,1,2,\ldots,p^a-1)\equiv 0\pmod{p^{bk+a-1-t}}.$$

Thus, in order to prove our claim it suffices to prove that $bk + a - 1 - t \geqslant a + 1$, that is, $bk \geqslant t + 2$. Indeed, if $t = 0$, then $bk \geqslant 2 = t + 2$ since $k \geqslant 2$, and if $t \geqslant 1$, then $bk \geqslant bp^t \geqslant 3^t \geqslant t + 2$, so our claim is proved.

It follows by the above discussion that

$$f(x) \equiv (x - m)^{p^a} \pmod{p^{a+1}}.$$

On the one hand, the coefficient of x in $f(x)$ is

$$N = e_{p^a-1}(m, m + p^b, m + 2p^b, \cdots m + (p^a - 1)p^b).$$

Now, the coefficient of x in $(x-m)^{p^a}$ is $p^a(-1)^{p^a-1}m^{p^a-1}$. Therefore, $N \equiv p^a(-1)^{p^a-1} \cdot m^{p^a-1} \pmod{p^{a+1}}$. Since $p \nmid m$, it follows that $p^a \| N$, as required. □

The next three theorems handle the case where $p = 2$. The first theorem deals with the case when $b \geqslant 2$, while the second and the third theorem treat the case when $b = 1$.

Theorem 3. *If a, b, m are positive integers such that $2 \nmid m$ and $b \geqslant 2$, then the maximal prime power 2^e which divides the numerator of the fraction*

$$\frac{1}{m} + \frac{1}{m + 2^b} + \frac{1}{m + 2 \cdot 2^b} + \frac{1}{m + 3 \cdot 2^b} + \ldots + \frac{1}{m + (2^a - 1)2^b},$$

when written in reduced form, is 2^a.

Proof. Set

$$N = e_{2^a-1}(m, m + 2^b, m + 2 \cdot 2^b, \cdots, m + (2^a - 1)2^b),$$

where e_{2^a-1} denotes the $(2^a - 1)$th elementary symmetric function. As in the proof of Theorem 2, it suffices to prove that $2^a \| N$. To do so, consider the polynomial

$$\begin{aligned} f(x) &= (x - m)(x - (m + 2^b))(x - (m + 2 \cdot 2^b)) \cdots (x - (m + (2^a - 1)2^b)) \\ &= (x - m)(x - m - 2^b)(x - m - 2 \cdot 2^b) \cdots (x - m - (2^a - 1)2^b) \\ &= \sum_{k=0}^{2^a} (-1)^k e_k(0, 2^b, 2 \cdot 2^b, \ldots, (2^a - 1)2^b)(x - m)^{2^a-k} \\ &= \sum_{k=0}^{2^a} (-1)^k 2^{bk} e_k(0, 1, 2, \ldots, 2^a - 1)(x - m)^{2^a-k}. \end{aligned}$$

We claim that if $b \geqslant 2$, then $2^{bk}e_k(0, 1, 2, \ldots, 2^a - 1) \equiv 0 \pmod{2^{a+1}}$ for every $1 \leqslant k \leqslant 2^a$. For simplicity, let us denote $e_k(0, 1, 2, \ldots, 2^a - 1)$ by e_k. If $k = 1$, then $2^b e_1 \equiv 0 \pmod{2^{b+a-1}}$ by Proposition 3, and since $b \geqslant 2$, it follows that $a + 1 \leqslant b + a - 1$, so $2^b e_1 \equiv 0 \pmod{2^{a+1}}$, as claimed. If $k = 2$, then $2^{2b}e_2 \equiv 0 \pmod{2^{2b+a-2}}$ by Proposition 3, and since $b \geqslant 2$, it follows that $a + 1 \leqslant 2b + a - 2$, so $2^{2b}e_2 \equiv 0 \pmod{2^{a+1}}$, as claimed. Next, suppose that $2 < k \leqslant 2^{a-1}$. If $2 \nmid k$, then $2^{bk}e_k \equiv 0 \pmod{2^{bk+a}}$ by Proposition 3, and since $a + 1 < bk + a$, it follows that

$2^{kb}e_k \equiv 0 \pmod{2^{a+1}}$, as claimed. If $2 \mid k$, let t be the positive integer such that $2^t \| k$. By propositions 1 and 3, we deduce that $2^{kb}e_k \equiv 0 \pmod{2^{bk+a-1-t}}$. Since $t \geqslant 1$ and $b \geqslant 2$, it follows that $2 + t < 2 \cdot 2^t \leqslant bk$, that is, $a + 1 < bk + a - 1 - t$, so $2^{bk}e_k \equiv 0 \pmod{2^{a+1}}$, as claimed. If $2^{a-1} < k \leqslant 2^{a-1} + 2$, then $2^{bk}e_k \equiv 0 \pmod{2^{bk+a-1}}$ by Proposition 3, and since $a + 1 \leqslant bk + a - 1$, it follows that $2^{bk}e_k \equiv 0 \pmod{2^{a+1}}$, as claimed. Finally, if $2^{a-1} + 2 < k \leqslant 2^a$, then $2^{bk}e_k \equiv 0 \pmod{2^{bk+a}}$ by Proposition 3, so $2^{bk}e_k \equiv 0 \pmod{2^{a+1}}$, as claimed.

To conclude, we proved that if $b \geqslant 2$, then $2^{bk}e_k \equiv 0 \pmod{2^{a+1}}$ for every $1 \leqslant k \leqslant 2^a$. Consequently, $f(x) \equiv (x - m)^{2^a} \pmod{2^{a+1}}$. As in the proof of Theorem 2, it follows that $N \equiv 2^a(-1)^{2^a-1}m^{2^a-1} \equiv 2^a m^{2^a-1} \pmod{2^{a+1}}$, and since $2 \nmid m$, we deduce that $2^a \| N$, as required. □

For the prime $p = 2$, we are left with the case $b = 1$. This case will be handled according to two sub-cases: $m = 1$ and $m > 1$.

Theorem 4. *If a is a positive integer, then the maximal prime power 2^e which divides the numerator of the fraction*

$$1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots + \frac{1}{1 + 2(2^a - 1)},$$

when written in reduced form, is 2^{2a}.

Proof. Note that

$$\begin{aligned} 1+&\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{1 + 2(2^a - 1)} \\ &= \sum_{\substack{1 \leqslant s < 2^{a+1} \\ s \text{ is odd}}} \frac{1}{s} = \sum_{\substack{1 \leqslant s < 2^a \\ s \text{ is odd}}} \left(\frac{1}{s} + \frac{1}{2^{a+1} - s}\right) = 2^{a+1} \sum_{\substack{1 \leqslant s < 2^a \\ s \text{ is odd}}} \frac{1}{s(2^{a+1} - s)}. \end{aligned}$$

Hence, in order to prove the claim it suffices to prove that the numerator of the fraction

$$\sum_{\substack{1 \leqslant s < 2^a \\ s \text{ is odd}}} \frac{1}{s(2^{a+1} - s)},$$

when written in reduced form, is divisible by 2^{a-1} but not by 2^a. For simplicity, for every $0 \leqslant k \leqslant 2^{a-1}$, let us denote the following kth elementary symmetric expression:

$$e_k(1(2^{a+1} - 1), 3(2^{a+1} - 3), \ldots, (2^a - 1)(2^a + 1)),$$

by e_k. As in the proof of Theorem 2, it suffices to prove that $2^{a-1} \| e_{2^{a-1}-1}$. To do so, consider the polynomial

$$f(x) = \prod_{\substack{1 \leqslant s < 2^{a+1} \\ s \text{ is odd}}} (x - s).$$

On the one hand, by Bauer's Theorem [3, p. 127],

$$f(x) \equiv (x^2 - 1)^{2^{a-1}} = \sum_{k=0}^{2^{a-1}} \binom{2^{a-1}}{k} (-1)^k x^{2^a - 2k} \pmod{2^{a+1}}.$$

On the other hand,

$$f(x) = \prod_{\substack{1\leqslant s<2^{a+1}\\ s \text{ is odd}}} (x-s) = \prod_{\substack{1\leqslant s<2^{a}\\ s \text{ is odd}}} (x-s)(x-(2^{a+1}-s))$$

$$\equiv \prod_{\substack{1\leqslant s<2^{a}\\ s \text{ is odd}}} (x^2+s(2^{a+1}-s)) = \sum_{k=0}^{2^{a-1}} e_k x^{2^a-2k} \pmod{2^{a+1}}.$$

By comparing the coefficient of x^{2^a-2k} we obtain that

$$e_k \equiv \binom{2^{a-1}}{k}(-1)^k \pmod{2^{a+1}},$$

for every $0 \leqslant k \leqslant 2^{a-1}$. In particular, $2^{a-1} \| e_{2^{a-1}-1}$, as required. □

Theorem 5. *Suppose that a is a positive integer and $m > 1$ is an odd integer. In addition, let c be the positive integer such that $2^c \| m-1$. Then the maximal prime power 2^e which divides the numerator of the fraction*

$$\frac{1}{m} + \frac{1}{m+2} + \frac{1}{m+4} + \frac{1}{m+6} + \ldots + \frac{1}{m+2(2^a-1)},$$

when written in reduced form, is either $2^{a+\min\{a,c\}}$ if $a \neq c$, or at least 2^{2a+1} if $a = c$.

Proof. Consider the polynomial

$$f(x) = (x-m)(x-(m+2))(x-(m+4))\cdots(x-(m+2(2^a-1))),$$

and let u be the odd positive integer such that $m = 1 + 2^c u$. As in the proof of Theorem 2,

$$f(x) = \sum_{k=0}^{2^a} (-1)^k 2^k e_k (x-m)^{2^a-k},$$

where we denote $e_k = e_k(0,1,2,\ldots,2^a-1)$ for simplicity. Note that in order to prove our claim, it suffices to find the maximal power of 2 which divides the coefficient of x in $f(x)$. Since

$$f(x) = \sum_{k=0}^{2^a} \left((-1)^k 2^k e_k \sum_{j=0}^{2^a-k} \binom{2^a-k}{j} x^j (-m)^{2^a-k-j} \right)$$

$$= \sum_{k=0}^{2^a} \sum_{j=0}^{2^a-k} (-1)^{2^a-j} m^{2^a-k-j} 2^k e_k \binom{2^a-k}{j} x^j,$$

it follows that the coefficient A of x in $f(x)$ is

$$\begin{aligned} A &= \sum_{k=0}^{2^a} (-1)^{2^a-1} m^{2^a-k-1} 2^k e_k \binom{2^a-k}{1} = -\sum_{k=0}^{2^a} (1+2^c u)^{2^a-k-1} 2^k e_k (2^a-k) \\ &= -\sum_{k=0}^{2^a} \sum_{i=0}^{2^a-k-1} \binom{2^a-k-1}{i} (2^c u)^i 2^k e_k (2^a-k) \\ &= -\underbrace{\sum_{k=0}^{2^a} 2^k e_k (2^a-k)}_{B} - \sum_{k=0}^{2^a} \sum_{i=1}^{2^a-k-1} \underbrace{\binom{2^a-k-1}{i} 2^{ci+k} u^i e_k (2^a-k)}_{C_{ki}} . \end{aligned}$$

First, we shall prove that $C_{ki} \equiv 0 \pmod{2^{a+c+1}}$ for all $0 \leqslant k \leqslant 2^a$ and $1 \leqslant i \leqslant 2^a - k - 1$, except when $(k, i) = (0, 1)$. Let t be the non-negative integer such that $2^t \| k$.

If either $3 \leqslant k \leqslant 2^{a-1}$ is odd or $2^{a-1} < k \leqslant 2^a$, then by Proposition 3, $e_k \equiv 0 \pmod{2^{a-1}}$, so $2^{ci+k} e_k \equiv 0 \pmod{2^{ci+k+a-1}}$, and since $ci + k + a - 1 > a + c + 1$, it follows that $C_{ki} \equiv 0 \pmod{2^{a+c+1}}$, as claimed. If $3 \leqslant k \leqslant 2^{a-1}$ is even, then by Proposition 3, $e_k \equiv \binom{2^{a-1}}{k} \pmod{2^a}$, so $e_k \equiv 0 \pmod{2^{a-1-t}}$ by Proposition 1. In addition, since $2^a - k \equiv 0 \pmod{2^t}$, it follows that $e_k(2^a - k) \equiv 0 \pmod{2^{a-1}}$, so $2^{ci+k} e_k (2^a - k) \equiv 0 \pmod{2^{ci+k+a-1}}$. Since $ci + k + a - 1 > a + c + 1$, it follows that $C_{ki} \equiv 0 \pmod{2^{a+c+1}}$, as claimed.

Next, if $k = 0$, then $C_{0i} = \binom{2^a-1}{i} 2^{ci} u^i 2^a$. Now, for $i \geqslant 2$, we get that $ic + a \geqslant c + a + 1$, so $C_{0i} \equiv 0 \pmod{2^{a+c+1}}$. If $k = 1$, then $C_{1i} = \binom{2^a-2}{i} 2^{ci+1} e_1 u^i (2^a - 1)$. Suppose that $i \geqslant 2$. Since $e_1 \equiv 0 \pmod{2^{a-1}}$ by Proposition 3, and since $(ci + 1) + (a - 1) \geqslant c + a + 1$, it follows that $C_{1i} \equiv 0 \pmod{2^{a+c+1}}$. If $i = 1$, then $C_{11} = (2^a - 2) 2^{c+1} e_1 u (2^a - 1)$, so $C_{11} \equiv 0 \pmod{2^{a+c+1}}$ since $2 \mid 2^a - 2$.

If $k = 2$, then $C_{2i} = \binom{2^a-3}{i} 2^{ci+2} e_2 u^i (2^a - 2)$. By Proposition 3, $e_2 \equiv 0 \pmod{2^{a-2}}$. In addition, since $2 \mid 2^a - 2$ and $(ci + 2) + (a - 2) + 1 \geqslant c + a + 1$, it follows that $C_{2i} \equiv 0 \pmod{2^{a+c+1}}$, as required. To conclude, it follows that

$$A \equiv -B - C_{01} = -B - (2^a - 1) 2^{a+c} u \pmod{2^{a+c+1}}.$$

Next, note that once we prove that $2^{2a} \| B$, then in the case $a > c$, we obtain that $2a \geqslant a + c + 1$, so $A \equiv -(2^a - 1) 2^{a+c} u \pmod{2^{a+c+1}}$, which implies that $2^{a+c} \| A$, as required. In the case $a < c$, we obtain that $2a + 1 < a + c + 1$, so $A \equiv -B \pmod{2^{2a+1}}$, which implies that $2^{2a} \| A$, as required. Finally, in the case $a = c$, we obtain

$$A \equiv -2^{2a} \left(\frac{B}{2^{2a}} + (2^a - 1) u \right) \pmod{2^{2a+1}},$$

and since $\frac{B}{2^{2a}} + (2^a - 1) u$ is a sum of two odd numbers, it follows that $2^{2a+1} \mid A$, as required.

So, it suffices to prove that $2^{2a} \| B$. To do so, consider the polynomial

$$\begin{aligned} f(x) &= \prod_{k=0}^{2^a-1}(x-(1+2k)) = \prod_{k=0}^{2^a-1}((x-1)+2k) \\ &= \sum_{k=0}^{2^a}(-1)^k e_k(0,2,4,6,\ldots,2(2^a-1))(x-1)^{2^a-k} \\ &= \sum_{k=0}^{2^a}\sum_{i=0}^{2^a-k}(-1)^{k+i}2^k e_k(0,1,2,3,\ldots,2^a-1)\binom{2^a-k}{i}x^{2^a-k-i} \end{aligned}$$

On the one hand, by recalling that $e_k = e_k(0,1,2,3,\ldots,2^a-1)$, we deduce that the coefficient of x in $f(x)$ is

$$\sum_{k=0}^{2^a}(-1)^{2^a-1}2^k e_k\binom{2^a-k}{2^a-k-1} = -\sum_{k=0}^{2^a}2^k e_k(2^a-k) = -B$$

On the other hand, by Theorem 4, it follows that $2^{2a}\|B$, as required. □

We stress that if $a = c$ in Theorem 5, then the numerator of the corresponding fraction may be divisible by larger power of 2 than 2^{2a+1}. As an illustrative example, for $a = 2$ and $m = 1021$, we obtain that

$$\frac{1}{1021}+\frac{1}{1023}+\frac{1}{1025}+\frac{1}{1027}=\frac{4294946816}{1099501142025}.$$

Since here $2^2\|m-1$, it follows that $a = c$, so by Theorem 5, we deduce that the numerator 4294946816 is divisible by 2^5, although it is actually divisible by 2^{12}.

References

[1] L. Carlitz, *A note on Wolstenholme's theorem*, Amer. Math. Monthly **61**(1954), 174—176.

[2] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54**(1947), 589–592.

[3] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, 6th edition, Clarendon Press, Oxford, 2008.

[4] W. J. Leveq, *Topics in Number Theory*, Vol I, Dover Publications, New York, 2002.

[5] R. Meštrović, *Wolstenholme's theorem: its generalizations and extensions in the last hundred and fifty years (1862–2012)*, arXiv:1111.3057v2 [math.NT].

[6] H. S. Vandiver, *The generalized Lagrange Indeterminate Congruence for a composite ideal modulus*, Ann. Math., **18**(1917), 115–119.