A CONGRUENCE IDENTITY ON ORDERED PARTITIONS USING PERMUTATION POLYNOMIALS

Chandan Kumar Vishwakarma
Dept. of Mathematics, Central University of South Bihar, Gaya, Bihar, India
7091chandankvis@gmail.com

Rajesh P. Singh[1]
Dept. of Mathematics, Central University of South Bihar, Gaya, Bihar, India
rpsingh@cub.ac.in

Received: 3/9/23, Revised: 9/5/23, Accepted: 12/29/23, Published: 1/29/24

Abstract

In this paper, we investigate a class of permutation polynomials of the form $h_k^t(x) = \sum_{n=1}^{k} n^t x^n$ over a finite field $\mathbb{F}_p$, where k and t are positive integers, and p is an odd prime. We find certain conditions on k and t for $h_k^t(x)$ to be a permutation polynomial over $\mathbb{F}_p$. We then use this class of permutation polynomials to find a new congruence identity on the parts of ordered partitions of $(p-1), 2(p-1), \ldots, \mu(p-1)$ into s parts, where μ is the largest integer satisfying $\mu(p-1) \leq ks$.

1. Introduction

Let n be a positive integer. A *partition* of n is a finite non-increasing sequence of positive integers $\omega_1, \omega_2, \ldots, \omega_s$ such that $\sum_{t=1}^{s} \omega_t = n$. Each w_i is called a *part* of the partition, and s is called the *length* of the partition. Thus, a partition is an unordered collection of parts, and when the order of the parts is relevant, we call it an *ordered partition* or *composition*. It is easy to see that the number of compositions of n into s parts is $\binom{n-1}{s-1}$, and that the total number of compositions is 2^{n-1}. Compositions with some restrictions on parts are interesting. Restrictions on compositions can happen in many ways, such as restricting how parts of the compositions are arranged or restricting the set from which the parts are taken. In a composition, if the parts are taken from the set S, compositions are called *S-restricted compositions*. We refer interested readers to [1, 2] for a complete survey and the history of compositions.

Throughout the paper, let $\mathbb{N}_k$ denote the set $\{1, \ldots, k\}$, and $[x]$ denote the greatest integer less than or equal to x. We denote the parts of the $\mathbb{N}_k$-restricted compo-

DOI: 10.5281/zenodo.10580967
[1]Corresponding Author

sitions of $j(p-1)$ into s parts by $\omega_1^{(j)}, \omega_2^{(j)}, \ldots, \omega_s^{(j)}$, i.e., $\omega_1^{(j)} + \omega_2^{(j)} + \cdots + \omega_s^{(j)} = j(p-1)$, where j is a positive integer; $\omega_i^{(j)} \in \mathbb{N}_k$ for all $1 \leq i \leq s$, and p is an odd prime. In this paper, we obtain an interesting congruence relation among the parts of $\mathbb{N}_k$-restricted compositions of $j(p-1)$ into s parts for $1 \leq j \leq [ks/(p-1)]$. In particular, we have established the following congruence identity.

Theorem 1. *Assume that p is an odd prime and t is any positive integer. Let k and s be positive integers such that $s \not\equiv 0 \pmod{p}$ and $k \equiv 1 \pmod{p(p-1)}$. The integer k satisfies an additional condition that $(k-1)$ is a multiple of p^2 whenever t is a multiple of $(p-1)$. Let μ be the greatest integer such that $\mu(p-1) \leq ks$, that is, $\mu = \big[ks/(p-1)\big]$. Then the following congruence identity holds:*

$$\sum_{j=1}^{\mu} \sum_{\Upsilon_s(j(p-1))} \Big(\omega_1{}^{(j)} \cdot \omega_2{}^{(j)} \cdots \omega_s{}^{(j)}\Big)^t \equiv 0 \pmod{p},$$

where $\Upsilon_s(j(p-1))$ for each $1 \leq j \leq \mu$ indicates summation over all the s-tuples $(\omega_1^{(j)}, \omega_2^{(j)}, \ldots, \omega_s^{(j)})$ satisfying $\omega_1^{(j)} + \omega_2^{(j)} + \cdots + \omega_s^{(j)} = j(p-1)$, and $\omega_i^{(j)} \in \mathbb{N}_k$ for all $1 \leq i \leq s$.

This work is in continuation of the earlier work by the second author and M. K. Singh [7], in which they obtained some congruence identities on the ordered partition using permutation polynomials. In particular, they proved the congruence identity in Theorem 1 for $t = 1$. It is surprising that the congruence identity in Theorem 1 holds for every positive integer t, and proving this theorem is the main objective of the paper.

This paper is organized as follows. In Section 2, we illustrate some significant preliminary results and lemmas. In Section 3, we propose a new class of permutation polynomials and use it to give the proof of Theorem 1.

2. Preliminaries

Let q be a prime power, and $\mathbb{F}_q$ be a finite field with size q. It is well known that for every function $\phi : \mathbb{F}_q \to \mathbb{F}_q$, there is a unique polynomial $f(x) \in \mathbb{F}_q[x]$ such that $\deg(f(x)) \leq q-1$ and $\phi(a) = f(a)$ for every $a \in \mathbb{F}_q$. The polynomial $f(x) \in \mathbb{F}_q[x]$ representing ϕ can be easily obtained by the Lagrange interpolation formula $f(x) = \sum_{c \in \mathbb{F}_q} \phi(c)(1-(x-c)^{q-1})$. Also note that for any two polynomials $f(x)$ and $g(x)$ over the finite field $\mathbb{F}_q$, we have $f(a) = g(a)$ for each $a \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \pmod{x^q - x}$ (see [4, Chapter 7]).

A polynomial $f(x)$ in $\mathbb{F}_q[x]$ is a *permutation polynomial* of $\mathbb{F}_q$ if its associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$. Finding a new class of permutation polynomials over a finite field is a nontrivial problem

[4, 5, 6]. We refer the interested reader to [4, Chapter 7] for the detailed study of permutation polynomials over finite fields.

This section gives a brief introduction to permutation polynomials over a finite field. We use permutation polynomials over finite fields to prove our result on restricted composition. Since $\mathbb{F}_q$ contains a finite number of elements, we have the following equivalent conditions for a permutation polynomial.

Lemma 1 ([4]). *The polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) *the function $f : c \mapsto f(c)$ is onto,*

(2) *the function $f : c \mapsto f(c)$ is one-to-one,*

(3) *$f(x) = d$ has a solution in $\mathbb{F}_q$ for each $d \in \mathbb{F}_q$,*

(4) *$f(x) = d$ has a unique solution in $\mathbb{F}_q$ for each $d \in \mathbb{F}_q$.*

The following theorem, known as Hermite's Criterion, will be used to prove our result in Section 3.

Theorem 2 ([4, Theorem 7.6]). *A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(1) *$f(x)$ has exactly one root in $\mathbb{F}_q$,*

(2) *for each integer t with $1 \le t \le q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{x^q - x}$ has degree $\le q-2$.*

We need the next result on summation involving binomial coefficients.

Theorem 3 ([3]). *For any two real or complex numbers x and y, and for any two positive integers n and m, we have the following identity:*

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (kx + iy)^m = \begin{cases} (-1)^n y^n n!, & \text{for } n = m, \\ 0, & \text{for each } n > m. \end{cases} \tag{1}$$

We also need the following two lemmas in the sequel.

Lemma 2 ([4, Theorem 7.8]). *The polynomial x^d is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$.*

Lemma 3 ([4, Lemma 7.3]). *Let $a_1, a_2, \ldots, a_q$ be elements of $\mathbb{F}_q$. Then the following two conditions are equivalent:*

(1) *$a_1, a_2, \ldots, a_q$ are distinct,*

(2) $\sum_{i=1}^{q} {a_i}^t = \begin{cases} 0, & \text{for } t = 0, 1, \ldots, q-2, \\ -1, & \text{for } t = q-1. \end{cases}$

3. Results

Let $h_k^t(x) = \sum_{n=1}^{k} n^t x^n$ be a polynomial over finite field $\mathbb{F}_p$, where t and k are positive integers. We start this section with the following lemma in which we find a function $g(x)$, that is equivalent to the polynomial $h_k^t(x)$ such that $g(\alpha) = h_k^t(\alpha)$ for each $\alpha \in \mathbb{F}_p \setminus \{1\}$. This lemma will be used to investigate the permutation properties of the polynomial $h_k^t(x)$.

Lemma 4. *For positive integers t, k, and for $x \neq 1$, a function equivalent to the polynomial $h_k^t(x) = \sum_{n=1}^{k} n^t x^n$ is given by*

$$\frac{\sum_{n=1}^{t}\sum_{i=0}^{n-1}(-1)^i\binom{t+1}{i}(n-i)^t x^n + \sum_{m=1}^{t+1}\sum_{i=m}^{t+1}(-1)^i\binom{t+1}{i}(k+m-i)^t x^{k+m}}{(1-x)^{t+1}}.$$

Proof. We assume that

$$(1-x)^r h_k^t(x) = \sum_{n=1}^{k+r} T_{(n,t)}^{(r)} x^n,$$

where $T_{(n,t)}^{(r)}$ is the coefficient of x^n in the expansion of $(1-x)^r h_k^t(x)$. It is easy to see that $T_{(n,t)}^{(r)}$ satisfies the recurrence relation $T_{(n,t)}^{(r)} = T_{(n,t)}^{(r-1)} - T_{(n-1,t)}^{(r-1)}$. We clearly have $T_{(1,t)}^{(r)} = 1$ for all $r \in \mathbb{N}$ and $T_{(n,t)}^{(r)} = 0$ for all $n > k + r$. We claim that the coefficients $T_{(n,t)}^{(r)}$ can be obtained by the following expressions:

$$T_{(n,t)}^{(r)} = \begin{cases} \sum_{i=0}^{n-1}(-1)^i\binom{r}{i}(n-i)^t, & \text{for } n \leq r, \\ \sum_{i=0}^{r}(-1)^i\binom{r}{i}(n-i)^t, & \text{for } r+1 \leq n \leq k, \\ \sum_{i=m}^{r}(-1)^i\binom{r}{i}(n-i)^t, & \text{for } n = k+m, m = 1, \ldots, r. \end{cases} \tag{2}$$

We prove the claim by induction on r. For $r = 1$, we have

$$\begin{aligned}(1-x)h_k^t(x) &= x + (2^t - 1)x^2 + (3^t - 2^t)x^3 + \cdots + (k^t - (k-1)^t)x^k - k^t x^{k+1} \\ &= x + \sum_{n=2}^{k}\left(n^t - (n-1)^t\right)x^n - k^t x^{k+1}. \end{aligned} \tag{3}$$

Substituting $r = 1$ in Equation (2), we have

$$T^{(1)}_{(n,t)} = \begin{cases} \sum_{i=0}^{n-1} (-1)^i \binom{1}{i} (n-i)^t = 1, & \text{for } n \le 1, \\ \sum_{i=0}^{1} (-1)^i \binom{1}{i} (n-i)^t = n^t - (n-1)^t, & \text{for } 2 \le n \le k, \\ \sum_{i=m}^{1} (-1)^i \binom{1}{i} (n-i)^t = -k^t, & \text{for } n = k+m,\ m = 1. \end{cases} \tag{4}$$

We see from Equations (3) and (4) that the expressions in Equation (2) are satisfied when $r = 1$. We assume that the expressions in Equation (2) are satisfied for r. We next show that this is also true for $r+1$, that is, the coefficients of x^n in the expansion of $(1-x)^{r+1} h_k^t(x)$ are given by the following expressions:

$$T^{(r+1)}_{(n,t)} = \begin{cases} \sum_{i=0}^{n-1} (-1)^i \binom{r+1}{i} (n-i)^t, & \text{for } n \le r+1, \\ \sum_{i=0}^{r+1} (-1)^i \binom{r+1}{i} (n-i)^t, & \text{for } r+2 \le n \le k, \\ \sum_{i=m}^{r+1} (-1)^i \binom{r+1}{i} (n-i)^t, & \text{for } n = k+m, m = 1, \ldots, r+1. \end{cases} \tag{5}$$

Now, using the recurrence relation $T^{(r)}_{(n,t)} - T^{(r)}_{(n-1,t)} = T^{(r+1)}_{(n,t)}$, and using Equation (2) for $n \le r+1$, we get

$$\begin{aligned} T^{(r+1)}_{(n,t)} &= T^{(r)}_{(n,t)} - T^{(r)}_{(n-1,t)} \\ &= \sum_{i=0}^{n-1} (-1)^i \binom{r}{i} (n-i)^t - \sum_{i=0}^{n-2} (-1)^i \binom{r}{i} (n-1-i)^t \\ &= n^t - \sum_{i=1}^{n-1} (-1)^i \binom{r}{i} (n-i)^t - \sum_{i=1}^{n-1} (-1)^{i-1} \binom{r}{i-1} (n-i)^t \\ &= n^t - \sum_{i=1}^{n-1} (-1)^i \left(\binom{r}{i} + \binom{r}{i-1} \right) (n-i)^t \\ &= \sum_{i=0}^{n-1} (-1)^i \binom{r+1}{i} (n-i)^t. \end{aligned} \tag{6}$$

Further, for $r+2 \leq n \leq k$. We have

$$\begin{aligned}
T_{(n,t)}^{(r+1)} &= T_{(n,t)}^{(r)} - T_{(n-1,t)}^{(r)} \\
&= \sum_{i=0}^{r}(-1)^i\binom{r}{i}(n-i)^t - \sum_{i=0}^{r}(-1)^i\binom{r}{i}(n-1-i)^t \\
&= n^t - \sum_{i=1}^{r}(-1)^i\binom{r}{i}(n-i)^t - \sum_{i=1}^{r+1}(-1)^{i-1}\binom{r}{i-1}(n-i)^t \\
&= n^t - \sum_{i=1}^{r}(-1)^i\left(\binom{r}{i}+\binom{r}{i-1}\right)(n-i)^t + (-1)^{r+1}\binom{r}{r}(n-r-1)^t \\
&= \sum_{i=0}^{r+1}(-1)^i\binom{r+1}{i}(n-i)^t. \qquad (7)
\end{aligned}$$

Similarly, for $n = k+m, m = 1, \ldots, r+1$, we can obtain the following identity:

$$T_{(n,t)}^{(r+1)} = \sum_{i=m}^{r+1}(-1)^i\binom{r+1}{i}(n-i)^t. \qquad (8)$$

Thus, we see from Equations (6), (7), and (8) that the expressions in Equation (2) are true for $r+1$. Now, we can obtain the coefficients of x^n in the expansion of $(1-x)^r h_k^t(x)$ using expressions in Equation (2) for any values of $r \in \mathbb{N}$. Hence, for $r = t+1$, we have

$$(1-x)^{t+1}h_k^t(x) = \sum_{n=1}^{k+t+1} T_{(n,t)}^{(t+1)}x^n \qquad (9)$$

and

$$T_{(n,t)}^{(t+1)} = \begin{cases} \sum_{i=0}^{n-1}(-1)^i\binom{t+1}{i}(n-i)^t, & \text{for } n \leq t+1, \\ \sum_{i=0}^{t+1}(-1)^i\binom{t+1}{i}(n-i)^t, & \text{for } t+2 \leq n \leq k, \\ \sum_{i=m}^{t+1}(-1)^i\binom{t+1}{i}(k+m-i)^t, & \text{for } n = k+m, m = 1, \ldots, t+1. \end{cases} \qquad (10)$$

Using Theorem 3, we see that $\sum_{i=0}^{t}(-1)^i\binom{t+1}{i}(t+1-i)^t = \sum_{i=0}^{t+1}(-1)^i\binom{t+1}{i}(t+1-i)^t = 0$, and $\sum_{i=0}^{t+1}(-1)^i\binom{t+1}{i}(n-i)^t = 0$. Therefore, Equation (10) is equivalent to

$$T_{(n,t)}^{(t+1)} = \begin{cases} \sum_{i=0}^{n-1}(-1)^i\binom{t+1}{i}(n-i)^t, & \text{for } n \leq t, \\ 0, & \text{for } t+1 \leq n \leq k, \\ \sum_{i=m}^{t+1}(-1)^i\binom{t+1}{i}(k+m-i)^t, & \text{for } n = k+m, m = 1, \ldots, t+1. \end{cases} \qquad (11)$$

Thus, we have the following required expression:

$$(1-x)^{t+1}h_k^t(x) = \sum_{n=1}^{t}\sum_{i=0}^{n-1}(-1)^i\binom{t+1}{i}(n-i)^t x^n + \sum_{m=1}^{t+1}\sum_{i=m}^{t+1}(-1)^i\binom{t+1}{i}(k+m-i)^t x^{k+m}.$$

This completes the proof. □

The next lemma presents a new class of permutation polynomials having exponents in arithmetic progression. Due to their simple algebraic structure, such permutation polynomials are interesting and have been studied previously in the literature. In 1994 [5], Matthews investigated permutation polynomials of the form $h_k(x) = \sum_{i=0}^{k} x^i$ over $\mathbb{F}_q$ with odd q and proved that $h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $k \equiv 1 \pmod{p(p-1)}$. Later, in 1998 [6], Park and Lee examined permutation properties of polynomials of the type $h_{k,r,s}(x) = x^r \sum_{i=0}^{k} x^{si}$ over $\mathbb{F}_q$. They determined the necessary and sufficient conditions on k and r for the polynomial $h_{k,r,1}(x)$ to be a permutation polynomial over $\mathbb{F}_q$, where $q = p$ or $q = p^2$.

In the following lemma, we find certain conditions on k and t under which the polynomial $\sum_{n=1}^{k} n^t x^n$ is a permutation polynomial of $\mathbb{F}_p$. Later, we give the proof of Theorem 1 by using this class of permutation polynomials.

Lemma 5. *Let $\mathbb{F}_p$ be a finite field with odd characteristic p, and let k and t be positive integers. If $k \equiv 1 \pmod{p(p-1)}$, then the polynomial*

$$h_k^t(x) = \sum_{n=1}^{k} n^t x^n$$

is a permutation polynomial over $\mathbb{F}_p$ if one of the following two conditions holds:

- *$t \neq u(p-1)$ for any $u \in \mathbb{N}$,*
- *if $t = u(p-1)$ for some $u \in \mathbb{N}$, then $p^2 | (k-1)$.*

Proof. In order to prove this, first we show that if $k \equiv l \pmod{p(p-1)}$, then $h_k^t(x) = h_l^t(x)$ for all $x \in \mathbb{F}_p \setminus \{1\}$. To show this, if $x \in \mathbb{F}_p$ and $x \neq 1$, then from Lemma 4, we have

$$(1-x)^{t+1}h_k^t(x) = \sum_{n=1}^{k+t+1} T_{(n,t)}^{(t+1)} x^n \pmod{x^p - x},$$

where

$$T_{(n,t)}^{(t+1)} = \begin{cases} \sum_{i=0}^{n-1} (-1)^i \binom{t+1}{i} (n-i)^t, & \text{for } n \le t, \\ 0, & \text{for } t+1 \le n \le k, \\ \sum_{i=m}^{t+1} (-1)^i \binom{t+1}{i} (n-i)^t, & \text{for } n = k+m, m = 1, \ldots, t+1. \end{cases} \tag{12}$$

Since $k = up(p-1) + l$ for some $u \in \mathbb{Z}^+$, plugging k into the above equation, we have

$$\begin{aligned} (1-x)^{t+1} h_k^t(x) &= \sum_{n=1}^{t} \sum_{i=0}^{n-1} (-1)^i \binom{t+1}{i} (n-i)^t x^n \\ &\quad + \sum_{m=1}^{t+1} \sum_{i=m}^{t+1} (-1)^i \binom{t+1}{i} (up(p-1) + l + m - i)^t x^{up(p-1)+l+m} \\ &\equiv \sum_{n=1}^{t} \sum_{i=0}^{n-1} (-1)^i \binom{t+1}{i} (n-i)^t x^n \\ &\quad + \sum_{m=1}^{t+1} \sum_{i=m}^{t+1} (-1)^i \binom{t+1}{i} (l+m-i)^t x^{l+m} \pmod{x^p - x} \\ &\equiv (1-x)^{t+1} h_l^t(x) \pmod{x^p - x}. \end{aligned}$$

Thus, for $k \equiv l \pmod{p(p-1)}$, we have $h_k^t(\alpha) = h_l^t(\alpha)$ for all $\alpha \in \mathbb{F}_p \setminus \{1\}$. Since $k \equiv 1 \pmod{p(p-1)}$ and $h_1^t(x) = x$, we have $h_k^t(\alpha) = h_1^t(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_p \setminus \{1\}$. Now, for $x = 1$, we have

$$h_k^t(1) = 1 + 2^t + 3^t + \cdots + k^t \pmod{p}.$$

It is given that $k \equiv 1 \pmod{p(p-1)}$, or equivalently, $k = vp(p-1) + 1$ for some $v \in \mathbb{Z}^+$. This implies that

$$\begin{aligned} h_k^t(1) &= 1 + 2^t + 3^t + \cdots + k^t \pmod{p} \\ &= v(p-1)\Big(\sum_{a \in \mathbb{F}_p} a^t \Big) + k^t = v(p-1)\Big(\sum_{a \in \mathbb{F}_p} a^t \Big) + 1 \pmod{p}. \end{aligned}$$

Therefore, using Lemma 3, we get

$$h_k^t(1) = \begin{cases} 1, & \text{for } t = 0, 1, \ldots, p-2, \\ v + 1 = 1, & \text{for } t = p-1. \end{cases}$$

Thus, if $k \equiv 1 \pmod{p(p-1)}$, then $h_k^t(x)$ and $h_1^t(x) = x$ induce the same map on $\mathbb{F}_p$. This proves that $h_k^t(x)$ is a permutation polynomial of $\mathbb{F}_p$. □

Let a be any positive integer such that $\gcd(a+1, p-1) = 1$. Then from Lemma 2 and Lemma 5, we have the following corollary.

Corollary 1. *Let $\mathbb{F}_p$ be a finite field with odd characteristic p, and let k and t be positive integers. Let a be any positive integer such that $\gcd(a+1, p-1) = 1$. If $k \equiv 1 \pmod{p(p-1)}$, then the polynomial*

$$h(x) = \sum_{n=1}^{k} n^t x^{n+a}$$

is a permutation polynomial over $\mathbb{F}_p$ if one of the following two conditions holds:

- *$t \neq u(p-1)$ for any $u \in \mathbb{N}$,*
- *if $t = u(p-1)$ for some $u \in \mathbb{N}$, then $p^2 | (k-1)$.*

Proof. For $k \equiv 1 \pmod{p(p-1)}$, we have seen that $h_k^t(x) \equiv x \pmod{x^p - x}$. Now the proof is direct by noting the fact that

$$h(x) = x^a h_k^t(x) = \sum_{n=1}^{k} n^t x^{n+a} \equiv x^{a+1} \pmod{x^p - x}.$$

□

Proof of Theorem 1. Since $k \equiv 1 \pmod{p(p-1)}$, from Lemma 5, $h_k^t(x)$ is a permutation polynomial over $\mathbb{F}_p$. For $j(p-1) \leq ks$, the coefficient of $x^{j(p-1)}$ in the expansion of $h_k^t(x)^s$ is

$$\sum_{\Upsilon_s(j(p-1))} \left(\omega_1^{(j)} \cdot \omega_2^{(j)} \cdots \omega_s^{(j)}\right)^t,$$

where $\Upsilon_s(j(p-1))$ indicates summation over all s-part compositions of $j(p-1)$, or equivalently, the summation over all s-tuples $(\omega_1^{(j)}, \omega_2^{(j)}, \ldots, \omega_s^{(j)})$ satisfying $\omega_1^{(j)} + \omega_2^{(j)} + \cdots + \omega_s^{(j)} = j(p-1)$. In the reduction of $h_k^t(x)^s \pmod{x^p - x}$, the coefficient of x^{p-1} is the sum of all the coefficients of x^{p-1}, $x^{2(p-1)}, \ldots, x^{\mu(p-1)}$, where μ is the largest integer satisfying $\mu(p-1) \leq ks$. So, the coefficient of x^{p-1} in $h_k^t(x)^s \pmod{x^p - x}$ is given as

$$\sum_{\Upsilon_s(p-1)} \left({\omega_1}^{(1)} \cdot {\omega_2}^{(1)} \cdots {\omega_s}^{(1)}\right)^t + \cdots + \sum_{\Upsilon_s(\mu(p-1))} \left({\omega_1}^{(\mu)} \cdot {\omega_2}^{(\mu)} \cdots {\omega_s}^{(\mu)}\right)^t,$$

or equivalently, the coefficient of x^{p-1} in $h_k^t(x)^s \pmod{x^p - x}$ is

$$\sum_{j=1}^{\mu} \sum_{\Upsilon_s(j(p-1))} \left({\omega_1}^{(j)} \cdot {\omega_2}^{(j)} \cdots {\omega_s}^{(j)}\right)^t.$$

Since $h_k^t(x)$ is a permutation polynomial over $\mathbb{F}_p$, from Theorem 2, we have

$$\sum_{j=1}^{\mu} \sum_{\Upsilon_s(j(p-1))} \left(\omega_1{}^{(j)} \cdot \omega_2{}^{(j)} \cdots \omega_s{}^{(j)}\right)^t \equiv 0 \pmod{p}.$$

This completes the proof. □

Clearly, for $t = 1$ and $k \equiv 1 \pmod{p(p-1)}$, the polynomial $h_k^{(1)}(x) = \sum_{n=1}^{k} nx^n$ is a permutation polynomial over $\mathbb{F}_p$. This gives the following known congruence identity.

Corollary 2 ([7])**.** *Assume that p is an odd prime. Let k and s be positive integers such that $s \not\equiv 0 \pmod{p}$ and $k \equiv 1 \pmod{p(p-1)}$. Let μ be the greatest integer such that $\mu(p-1) \leq ks$. Then the following congruence identity holds:*

$$\sum_{j=1}^{\mu} \sum_{\Upsilon_s(j(p-1))} \omega_1{}^{(j)} \cdot \omega_2{}^{(j)} \cdots \omega_s{}^{(j)} \equiv 0 \pmod{p},$$

where $\Upsilon_s(j(p-1))$ for each $1 \leq j \leq \mu$ indicates summation over all s-part compositions $\omega_1^{(j)} + \omega_2^{(j)} + \cdots + \omega_s^{(j)} = j(p-1)$, and $\omega_i^{(j)} \in \mathbb{N}_k$ for all $1 \leq i \leq s$.

We now demonstrate Theorem 1 by the following example.

Example 1. We take $p = 5$, $t = 3$, $k = 21$, and $s = 2$ so that the conditions of Theorem 1 and Lemma 5 are satisfied. Accordingly, $h_k^{(3)}(x) = x + 2^3x^2 + \cdots + 21^3x^{21}$. The coefficients of $x^{j(p-1)}$ in the expansion of $h_k^{(3)}(x)^2$ for $j = 1, 2, \ldots, 10$ are $3, 3, 0, 4, 0, 3, 1, 0, 3, 3$, respectively. The sum of these coefficients is 20, which is congruent to 0 modulo 5.

It is known that for any two permutation polynomials $f(x)$ and $g(x)$ over a finite field, the composition $f(g(x))$ is also a permutation polynomial. Let a be a positive integer such that $\gcd(a, p-1) = 1$. Since the polynomial $\sum_{n=1}^{k}(an)^t x^{an}$ equals $a^t h_k^t(x^a)$, we have the following result using Lemma 5 and Lemma 2.

Corollary 3. *Let $\mathbb{F}_p$ be a finite field with odd characteristic p, and let k and t be positive integers. Let $a \not\equiv 0 \pmod{p}$ be a positive integer such that $\gcd(a, p-1) = 1$. If $k \equiv 1 \pmod{p(p-1)}$, then the polynomial $h_{k,a}^t(x) = \sum_{n=1}^{k}(an)^t x^{an}$ is a permutation polynomial over $\mathbb{F}_p$ if one of the following two conditions holds:*

- *$t \neq u(p-1)$ for any $u \in \mathbb{N}$,*
- *if $t = u(p-1)$ for some $u \in \mathbb{N}$, then $p^2 | (k-1)$.*

As a consequence of Corollary 3 and Theorem 1, we can obtain the following result.

Corollary 4. *Let p be an odd prime and t be a positive integer. Assume that $\gcd(a, p-1) = 1$ for $a \in \mathbb{Z}^+$. Let k and s be positive integers such that $s \not\equiv 0 \pmod{p}$ and $k \equiv 1 \pmod{p(p-1)}$. We take k such that $p^2 \mid (k-1)$ whenever t is a multiple of $(p-1)$. Let μ be the greatest integer such that $\mu(p-1) \leq ks$. Then the following congruence identity holds:*

$$\sum_{j=1}^{\mu} \sum_{\Upsilon_s(j(p-1))} \left({\omega_1}^{(j)} \cdot {\omega_2}^{(j)} \cdots {\omega_s}^{(j)}\right)^t \equiv 0 \pmod{p},$$

where $\Upsilon_s(j(p-1))$ for each $1 \leq j \leq \mu$ indicates summation over all s-part compositions $\omega_1^{(j)} + \omega_2^{(j)} + \cdots + \omega_s^{(j)} = j(p-1)$, and $\omega_i^{(j)} \in \{an : n = 1, \ldots, k\}$ for all $1 \leq i \leq s$.

Acknowledgements. The authors would like to thank the editors and the anonymous referees for their valuable suggestions. The first author is supported by CSIR, New Delhi, Govt. of India (F. No. 09/1144(0003)/2019-EMR-I).

References

[1] G. E. Andrews, *The Theory of Partitions, Encyclopedia Math. Appl., Series Number 2*, Cambridge University Press, Cambridge, 1998.

[2] S. Heubach and T. Mansour, *Combinatorics of Compositions and Words*, Chapman and Hall/CRC, Boca Raton, Florida, 2009.

[3] H. Katsuura, Summations involving binomial coefficients, *College Math. J.* **40**(4) (2009), 275-278.

[4] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia Math. Appl., 2nd ed.*, Cambridge University Press, Cambridge, 1997.

[5] R. Matthews, Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field, *Proc. Amer. Math. Soc.* **120**(1) (1994), 47-51.

[6] Y. Park and J. Lee, Permutation polynomials with exponents in an arithmetic progression, *Bull. Austral. Math. Soc.* **57**(2) (1998), 243-252.

[7] R. P. Singh and M. K. Singh, Two congruence identities on ordered partitions, *Integers* **18** (2018), #A73.