TWO CONGRUENCE IDENTITIES ON ORDERED PARTITIONS

Rajesh P. Singh
Department of Mathematics, Central University of South Bihar, Patna, Bihar, India
rpsingh@cub.ac.in

Mritunjay Kumar Singh[1]
Department of Mathematics, Central University of South Bihar, Patna, Bihar, India
mritunjay@cub.ac.in

Received: 2/19/18, Accepted: 8/20/18, Published: 8/31/18

Abstract

An ordered partition (composition) of a positive integer n in s parts consists of an ordered sequence of s positive integers whose sum is n. In this paper, we have obtained two congruence identities on the compositions of $p-1$, $2(p-1)$, $3(p-1), \cdots, [ks/p-1](p-1)$ in s parts, with parts from the set $\mathbb{N}_k = \{1, 2, 3, \cdots, k\}$ and $k \equiv 1 \pmod{p(p-1)}$, p a prime number.

1. Introduction

Let n be a positive integer. A partition of n, denoted by $p(n)$, is a finite non-increasing sequence of positive integers $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_s$ such that $\sum_{i=1}^{s} \lambda_i = n$. The summand λ_i are called the parts of the partition and s is the length of the partition. Thus a partition is an unordered collection of parts and if the order of the parts is relevant, instead of partitions we have compositions. It is trivial to observe that the total number of compositions of n in s-parts is $\binom{n-1}{s-1}$ and the total number of compositions in all possible parts is 2^{n-1}. The compositions that have certain restrictions are interesting and have been studied extensively in the literature. The restrictions on composition can occur in several ways. For example, restricting the way in which the parts of the composition are arranged or restricting the set from which the parts are taken. The compositions are called S-restricted compositions if the parts of the composition are taken from the set S. There is a vast literature on results on compositions. For a complete survey and the history of compositions, we refer [1, 2] to the interested readers.

[1]Corresponding Author

Throughout the paper, $\mathbb{N}_k$ denotes the set $\{1, 2, 3, \ldots, k\}$ and $C(n, s, a, b)$ as the number of compositions of n in s parts in which parts λ_i satisfy $a \leq \lambda_i \leq b$, where a and b are positive integers. In this paper, we establish interesting congruence properties about the $\mathbb{N}_k$- restricted compositions of $p-1, 2(p-1), 3(p-1), \cdots, [ks/p-1](p-1)$ in s parts. In other words, the $\mathbb{N}_k$-restricted compositions of $p-1, 2(p-1), 3(p-1), \ldots, r(p-1)$ in s parts, for p prime and r the largest integer satisfying $r(p-1) \leq ks$, where $k \equiv 1 \pmod{p(p-1)}$ and $s \not\equiv 0 \pmod{p}$. For $1 \leq r \leq [ks/p-1]$, we denote the parts of the $\mathbb{N}_k$-restricted compositions of $r(p-1)$ by $\lambda_1^{(r)}, \lambda_2^{(r)}, \ldots, \lambda_s^{(r)}$, i.e., $\lambda_1^{(r)} + \lambda_2^{(r)} + \cdots + \lambda_s^{(r)} = r(p-1)$. We have established the following results.

Theorem 1. *Assume that p is an odd prime. Let k and s be positive integers satisfying $k \equiv 1 \pmod{p(p-1)}$ and $s \not\equiv 0 \pmod{p}$. Then for the largest integer r such that $r(p-1) \leq ks$, the following congruence identity holds*

$$\sum_{r=1}^{[ks/p-1]} \sum_{\Upsilon_s(r(p-1))} \lambda_1^{(r)} \cdot \lambda_2^{(r)} \cdot \ldots \cdot \lambda_s^{(r)} \equiv 0 \pmod{p},$$

where $\Upsilon_s(r(p-1))$ indicates summation over all s-parts compositions $\lambda_1^{(r)} + \lambda_2^{(r)} + \cdots + \lambda_s^{(r)}$ of $r(p-1)$, and $\lambda_i \in \mathbb{N}_k$ for $1 \leq i \leq s$.

Theorem 2. *Assume that p is an odd prime. Let k and s be positive integers with $k \equiv 1 \pmod{p(p-1)}$ and $s \not\equiv 0 \pmod{p}$. Then for the largest integer r such that $r(p-1) \leq ks$, the following identity holds*

$$\sum_{t=1}^{r} C\left(t(p-1), s, 1, k\right) \equiv 0 \pmod{p}.$$

This paper is organized as follows. In Section 2, we introduce some preliminary results and lemmas. In Section 3, we give the proof of the main results. Finally, conclusion is given in section 4.

2. Preliminaries

To prove our results on restricted compositions, we use permutation polynomials over finite fields. In this section, we give a brief introduction about permutation polynomials over finite fields. For the detailed introduction of permutation polynomials over finite fields, we refer to [3, Chapter 7].

Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^e$ a prime power, and $\mathbb{F}_q[x]$ the ring of polynomials over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if the function from $\mathbb{F}_q \to \mathbb{F}_q$ defined by f is a bijection. Since $\mathbb{F}_q$ is finite, we have the following equivalent conditions for a permutation polynomial.

Lemma 1. ([3]) *The polynomial $f \in \mathbb{F}_q[x]$ 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. *$f(x) = a$ has a solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$;*
4. *$f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.*

Finite fields are polynomially complete, that is, every mapping from $\mathbb{F}_q$ into $\mathbb{F}_q$ can be represented by a unique polynomial over $\mathbb{F}_q$. Given any arbitrary function $\phi : \mathbb{F}_q \to \mathbb{F}_q$, the unique polynomial $g \in \mathbb{F}_q[x]$ with $\deg(g) < q$ representing ϕ can be found by the formula $g(x) = \sum_{c \in \mathbb{F}_q} \phi(c)(1 - (x - c)^{q-1})$, see [3, Chapter 7].

Two polynomials represent the same function if and only if they are the same by reduction modulo $x^q - x$, according to the following result.

Lemma 2. ([3]) *For $f, g \in \mathbb{F}_q[x]$ we have $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \pmod{(x^q - x)}$.*

In what follows, we will need the following result that is known as Hermite's criterion.

Theorem 3. ([3]) *A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

1. *f has exactly one root in $\mathbb{F}_q$;*
2. *for each integer t with $1 \leq t \leq q - 2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{(x^q - x)}$ has degree $\leq q - 2$.*

The following lemma is well known and is presented here for the sake of completeness.

Lemma 3. ([3]) *The polynomial x^a is a permutation polynomial of $\mathbb{F}_p$ if and only if $\gcd(a, p - 1) = 1$.*

We also need the following result in the sequel.

Lemma 4. ([4]) *For an odd prime p, the polynomial defined by*

$$f_k(x) = x + x^2 + \cdots + x^k$$

is a permutation polynomial over $\mathbb{F}_p$ if and only if $k \equiv 1 \pmod{p(p-1)}$.

3. Proof of the Main Results

Determining permutation polynomial is a non-trivial problem [3]. Hermite criterion (see, Theorem 3) is interesting theoretically. But in practice it is not easy to check the invertibility of a polynomial using this criterion. In the following lemma, we have a class of permutation polynomial which we use to obtain a new congruence identity on restricted compositions.

Lemma 5. *Let p be an odd prime and $k \equiv 1 \pmod{p(p-1)}$. Then $f_{\mathbb{N}_k}(x) = x + 2x^2 + 3x^3 + \cdots + kx^k$ is a permutation polynomial over $\mathbb{F}_p$.*

Proof. In order to prove the lemma, we first show that $k \equiv l \pmod{p(p-1)}$ implies $f_{\mathbb{N}_k}(\alpha) = f_{\mathbb{N}_l}(\alpha)$ for all α in $\mathbb{F}_p$. To see this, if $x = 1$, then $f_{\mathbb{N}_k}(1) = \frac{k(k+1)}{2} = \frac{l(l+1)}{2} \pmod{p}$. If $x \neq 1$, then $f_{\mathbb{N}_k}(x) = \dfrac{1-x^{k+1}}{(1-x)^2} + \dfrac{kx^{k+1}}{1-x} = \dfrac{1-x^{l+1}}{(1-x)^2} + \dfrac{lx^{l+1}}{1-x} \pmod{(x^p - x)} = f_{\mathbb{N}_l}(x)$. Since $k \equiv 1 \pmod{p(p-1)}$, it follows that $f_{\mathbb{N}_k}(x)$ and $f_{\mathbb{N}_1}(x)$ induce the same map on $\mathbb{F}_p$. The proof is now complete by noting the fact that $f_{\mathbb{N}_1}(x) = x$ is a permutation polynomial of $\mathbb{F}_p$. □

The converse of above lemma is not true in general as the polynomial $x + 2x^2 + 3x^3 \in \mathbb{F}_5[x]$ is a permutation polynomial of $\mathbb{F}_5$.

Proof of Theorem 1. From Lemma 5, we see that $f_{\mathbb{N}_k}(x)$ is a permutation polynomial of $\mathbb{F}_p$. For $r(p-1) \leq ks$, the coefficient of $x^{r(p-1)}$ in the expansion of $f_{\mathbb{N}_k}(x)^s$ is

$$\sum_{\Upsilon_s(r(p-1))} \lambda_1^{(r)} \cdot \lambda_2^{(r)} \cdot \ldots \cdot \lambda_s^{(r)}.$$

In the reduction of $f_{\mathbb{N}_k}(x)^s \pmod{(x^p - x)}$, the coefficient of x^{p-1} is the sum of all the coefficients of the powers of x that are multiples of $p-1$, i.e., the coefficient of x^{p-1} in the reduction of $f_{\mathbb{N}_k}(x)^s \pmod{(x^p - x)}$ is

$$\sum_{\Upsilon_s((p-1))} \lambda_1^{(1)} \cdot \lambda_2^{(1)} \cdot \ldots \cdot \lambda_s^{(1)} + \sum_{\Upsilon_s(2(p-1))} \lambda_1^{(2)} \cdot \lambda_2^{(2)} \cdot \ldots \cdot \lambda_s^{(2)} + \cdots + \sum_{\Upsilon_s(r(p-1))} \lambda_1^{(r)} \cdot \lambda_2^{(r)} \cdot \ldots \cdot \lambda_s^{(r)}.$$

Since r satisfies $r(p-1) \leq ks$, the above summation can be rewritten as

$$\sum_{r=1}^{[ks/p-1]} \sum_{\Upsilon_s(r(p-1))} \lambda_1^{(r)} \cdot \lambda_2^{(r)} \cdot \ldots \cdot \lambda_s^{(r)}.$$

Further, since $f_{\mathbb{N}_k}(x)$ is a permutation polynomial, by Theorem 3 we may conclude that the coefficient of x^{p-1} in the reduction of $f_{\mathbb{N}_k}(x)^s \pmod{(x^p - x)}$ is 0, and hence

$$\sum_{r=1}^{[ks/p-1]} \sum_{\Upsilon_s(r(p-1))} \lambda_1^{(r)} \cdot \lambda_2^{(r)} \cdot \ldots \cdot \lambda_s^{(r)} \equiv 0 \pmod{p}.$$

This completes the proof. □

We now illustrate the above theorem by the following example.

Example 1. To demonstrate, consider the case of $q = 5$, $k = 21$ and $s = 2$, so that the conditions of Theorem 1 and Lemma 5 are satisfied. Accordingly, $f_{\mathbb{N}_k}(x) = x+2x^2+3x^3+\cdots+21x^k$. The coefficients of $x^{r(p-1)}$ for $r = 1, 2, \ldots, 10$ under modulo 5 operations are $0, 4, 1, 0, 0, 1, 0, 1, 0, 3$ respectively. The sum of these coefficients is 10, which is zero modulo 5.

Proof of Theorem 2. Consider the polynomial $f_k(x)^s = \left(x + x^2 + x^3 + \cdots + x^k\right)^s$. Then, in the expansion of $f_k(x)^s$, the coefficient of $x^{r(p-1)}$ is

$$C\left(r(p-1), s, 1, k\right), \qquad \left(r(p-1) \leq ks\right).$$

The coefficient of x^{p-1} in $f_k(x)^s \pmod{(x^p - x)}$ is the sum of all the coefficients of the powers of x that are multiples of $p-1$, i.e., the coefficient of x^{p-1} of $f_k(x)^s \pmod{(x^p - x)}$ is

$$C\left((p-1), s, 1, k\right) + C\left(2(p-1), s, 1, k\right) + \cdots + C\left(r(p-1), s, 1, k\right).$$

Since r satisfies $r(p-1) \leq ks$, the above summation can be rewritten as

$$\sum_{t=1}^{[ks/p-1]} C\left(t(p-1), s, 1, k\right).$$

Further, since $f_k(x)$ is a permutation polynomial, by Theorem 3 we may conclude that the coefficient of x^{p-1} of $f_k(x)^s \pmod{(x^p - x)}$ is 0, and hence

$$\sum_{t=1}^{[ks/p-1]} C\left(t(p-1), s, 1, k\right) \equiv 0 \pmod{p}.$$

This finishes the proof of the theorem. □

Since the composition of two permutation polynomials is again a permutation polynomial, it follows from Lemma 3 and Lemma 4 that $f_{ka}(x) = x^a+x^{2a}+\cdots+x^{ka}$ permutes $\mathbb{F}_p$ if and only if $k \equiv 1 \pmod{p(p-1)}$ and $\gcd(a, p-1) = 1$. We can also deduce the following result easily as a consequence of the above theorem.

Corollary 1. *Assume that p is an odd prime. Let k, s and a be positive integers with $k \equiv 1 \pmod{p(p-1)}, s \not\equiv 0 \pmod{p}$ and $\gcd(a, p-1) = 1$. Then for the largest integer r such that $r(p-1) \leq ks$, the following identity holds*

$$\sum_{t=1}^{[ks/p-1]} C\left(t(p-1), s, a, ka\right) \equiv 0 \pmod{p}.$$

4. Conclusion

In this paper, we have found two congruence identities on ordered partitions using permutation polynomials over finite fields . However, at this stage, the combinatorial interpretation is not clear. To obtain the combinatorial proof needs further investigation. To the best of our knowledge, the presented congruence identities are new and have not been studied before.

Acknowledgment. The authors would like to thank the editor and the anonymous referee for carefully reading the paper and giving valuable comments that improve the quality of the paper.

References

[1] G. E. Andrews, *The Theory of Partitions* No. 2, Cambridge University Press, 1998.

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

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

[4] 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.