PERMUTATION POLYNOMIALS OF THE FORM $\sum_{n=1}^{k} h(n)X^n$

Zhiguo Ding
Department of Mathematics, University of Michigan, Ann Arbor, Michigan
dingz@umich.edu

Michael E. Zieve
Department of Mathematics, University of Michigan, Ann Arbor, Michigan
zieve@umich.edu

Received: 6/10/24, Accepted: 9/25/24, Published: 10/9/24

Abstract
Vishwakarma and Singh showed that $\sum_{n=1}^{k} n^t X^n$ permutes $\mathbb{F}_p$ for certain choices of k and t. We give a simpler proof of a more general result.

1. Introduction

Vishwakarma and Singh proved the following result.

Theorem 1 ([1]). *If p is an odd prime, and k and t are positive integers such that $k \equiv 1 \pmod{p(p-1)}$ and either $k \equiv 1 \pmod{p^2}$ or $(p-1) \nmid t$, then $\sum_{n=1}^{k} n^t X^n$ permutes $\mathbb{F}_p$.*

This is [1, Lemma 5], whose proof comprises the bulk of the paper [1], and from which the main result of [1] follows at once via known methods. In this paper we give a much shorter and simpler proof of the following more general result.

Theorem 2. *Let $q = p^\ell$ where p is prime and ℓ is a positive integer, and let k be a positive integer such that $k \equiv 1 \pmod{p(q-1)}$. Pick any $h(X) \in \mathbb{F}_q[X]$, and write $f(X) := \sum_{n=1}^{k} h(n)X^n$ and $h(X) = \sum_{i=0}^{m} b_i X^i$ with $b_i \in \mathbb{F}_q$. If $q > 2$ then $f(X)$ acts as the identity map on $\mathbb{F}_q$ if and only if $h(1) = 1$ and at least one of the following holds:*

1. $k \equiv 1 \pmod{p^2}$; *or*
2. $\sum_{j=1}^{\lfloor m/(p-1) \rfloor} b_{j(p-1)} = 0$.

Remark 1. For completeness, we note that if $q = 2$ then the polynomial $f(X)$ in Theorem 2 acts as the identity map on $\mathbb{F}_q$ if and only if the integer $M := (k+1)/2$ satisfies $h(M) = 1$.

DOI: 10.5281/zenodo.13909182

There are four main differences between Theorem 2 and Theorem 1. Most importantly, the coefficient of X^n in the polynomial $f(X)$ in Theorem 2 is $h(n)$, which is much more general than the coefficient n^t in Theorem 1. Next, Theorem 2 gives necessary and sufficient conditions rather than merely sufficient conditions. Theorem 2 applies to arbitrary finite fields $\mathbb{F}_q$ with $q > 2$, while Theorem 1 restricts to the case that q is odd and prime. Finally, Theorem 2 shows that $f(X)$ acts as the identity map on $\mathbb{F}_q$, while [1, Lemma 5] only asserts that $f(X)$ is some permutation of $\mathbb{F}_q$; however, the stronger assertion is shown in the proof of [1, Lemma 5].

2. Proof

In this section we prove Theorem 2. We use the following classical lemma.

Lemma 1. *For any prime p and any positive integer t, the value $S_t := \sum_{a\in\mathbb{F}_p} a^t$ equals -1 if $(p-1) \mid t$, and equals 0 otherwise.*

Remark 2. Lemma 1 has been known for hundreds of years. It is immediate when $(p-1) \mid t$. One proof for the nontrivial case $(p-1) \nmid t$ is that S_t is unchanged upon multiplication by b^t for any $b \in \mathbb{F}_p^*$, which forces S_t to be 0 since there exists b with $b^t \neq 1$. Another proof is by applying Newton's identities to $\prod_{a\in\mathbb{F}_p}(X-a) = X^p - X$.

Proof of Theorem 2. Write $k = 1 + Np(q-1)$ where N is a nonnegative integer, and assume $q > 2$. Then $k = q + (Np-1)(q-1)$, so that

$$f(X) = h(1)X + \sum_{n=2}^{k} h(n)X^n = h(1)X + \sum_{r=2}^{q} \sum_{s=0}^{Np-1} h\bigl(r + s(q-1)\bigr)X^{r+s(q-1)}.$$

Since $c^{r+s(q-1)} = c^r$ for any $c \in \mathbb{F}_q$ and any integers $r > 0$ and $s \geq 0$, it follows that if $c \in \mathbb{F}_q$ then

$$f(c) = h(1)\cdot c + \sum_{r=2}^{q} \sum_{s=0}^{Np-1} h\bigl(r + s(q-1)\bigr)\cdot c^r.$$

As s varies over the integers $0, 1, \ldots, Np-1$, exactly N of the values $r + s(q-1)$ lie in any prescribed congruence class mod p. Thus if $c \in \mathbb{F}_q$ then, writing $H := \sum_{a\in\mathbb{F}_p} h(a)$, we have

$$f(c) = h(1)\cdot c + NH\sum_{r=2}^{q} c^r = h(1)\cdot c + NH\sum_{r=1}^{q-1} c^r.$$

It follows that $f(X)$ acts as the identity on $\mathbb{F}_q$ if and only if the polynomial

$$\bigl(h(1)-1\bigr)X + NH\sum_{r=1}^{q-1} X^r$$

vanishes on $\mathbb{F}_q$. Since this polynomial has degree less than q, it vanishes on $\mathbb{F}_q$ if and only if it is the zero polynomial; since $q > 2$, this occurs if and only if $NH = 0$ and $h(1) = 1$. Next, $NH = 0$ if and only if either $p \mid N$ or $H = 0$. Plainly $p \mid N$ if and only if $k \equiv 1 \pmod{p^2}$. Finally, by Lemma 1 we have

$$H = pb_0 + \sum_{a \in \mathbb{F}_p} \sum_{i=1}^{m} b_i a^i = \sum_{i=1}^{m} b_i \sum_{a \in \mathbb{F}_p} a^i = -\sum_{j=1}^{\lfloor m/(p-1) \rfloor} b_{j(p-1)},$$

so that $H = 0$ if and only if Item 2 in Theorem 2 holds. □

Acknowledgement. The first author was supported in part by the Natural Science Foundation of Hunan Province of China (No. 2020JJ4164).

References

[1] C. K. Vishwakarma and R. P. Singh, A congruence identity on ordered partitions using permutation polynomials, *Integers* **24** (2024), #A12.