Finite Fields and Their Applications 48 (2017) 10–19

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Power sums over finite commutative unital rings

José María Grau [a], Antonio M. Oller-Marcén [b]

[a] *Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo s/n, 33007 Oviedo, Spain*
[b] *Centro Universitario de la Defensa de Zaragoza, Ctra. Huesca s/n, 50090 Zaragoza, Spain*

A R T I C L E I N F O

Article history:
Received 18 March 2016
Received in revised form 5 July 2017
Accepted 6 July 2017
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
13B99
13A99
13F99

Keywords:
Power sum
Finite commutative unital ring
Polynomial ring over $\mathbb{Z}/n\mathbb{Z}$

A B S T R A C T

In this paper we compute the sum of the k-th powers of all the elements of a finite commutative unital ring, thus generalizing known results for finite fields, the rings of integers modulo n or the ring of Gaussian integers modulo n. As an application, we focus on quotient rings of the form $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$ for a polynomial $f \in \mathbb{Z}[x]$.

1. Introduction

For a finite ring R and $k \geq 1$, we define the power sum

$$S_k(R) := \sum_{r \in R} r^k.$$

E-mail addresses: grau@uniovi.es (J.M. Grau), oller@unizar.es (A.M. Oller-Marcén).

http://dx.doi.org/10.1016/j.ffa.2017.07.003
1071-5797/

Throughout the paper we will deal only with finite commutative unital rings and our main objective will be the computation of $S_k(R)$ in this case.

The problem of computing $S_k(R)$ has been completely solved only for some particular families of finite rings. If R is a finite field $\mathbb{F}_q$, the value of $S_k(\mathbb{F}_q)$ is well-known. If $R = \mathbb{Z}/n\mathbb{Z}$, the study of $S_k(\mathbb{Z}/n\mathbb{Z})$ dates back to 1840 [5] and has been addressed in various works [1,3,4]. More recently, the case $R = \mathbb{Z}/n\mathbb{Z}[i]$ has been solved in [2]. For these cases, we have the following known results.

Proposition 1.

i)

$$S_k(\mathbb{F}_q) = \begin{cases} -1, & \text{if } (q-1) \mid k \,; \\ 0, & \text{otherwise.} \end{cases}$$

ii)

$$S_k(\mathbb{Z}/n\mathbb{Z}) = \begin{cases} -\displaystyle\sum_{p \mid n,\, p-1 \mid k} \frac{n}{p}, & \text{if } k \text{ is even or } k=1 \text{ or } n \not\equiv 0 \pmod 4; \\ 0, & \text{otherwise.} \end{cases}$$

iii)

$$S_k(\mathbb{Z}/n\mathbb{Z}[i]) = \begin{cases} \frac{n}{2}(1+i), & \text{if } k>1 \text{ is odd and } n \equiv 2 \pmod 4; \\ -\displaystyle\sum_{p \in \mathcal{P}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

where

$$\mathcal{P}(k,n) := \{\text{prime } p : p \mid\mid n, p^2-1 \mid k, p \equiv 3 \pmod 4\}$$

and $p \mid\mid n$ means that $p \mid n$, but $p^2 \nmid n$.

Let R be a finite commutative unital ring and assume that $|R| = p_1^{s_1} \cdots p_l^{s_l}$. This implies that $\operatorname{char}(R) = p_1^{t_1} \cdots p_l^{t_l}$ with $1 \leq t_i \leq s_i$ for every i. Define rings $R_i = R/p_i^{t_i} R$ for every $i \in \{1, \dots, l\}$. Then, we have the following decomposition as a direct sum of rings,

$$R \cong R_1 \oplus \cdots \oplus R_l, \tag{1}$$

with $\operatorname{char}(R_i) = p_i^{t_i}$ and $t_i = s_i$ if and only if R_i is isomorphic to $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$.

In addition, for every $1 \leq i \leq l$, the additive group $(R_i, +)$ is a finite abelian p-group so it can be decomposed as a direct sum of cyclic p-groups