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*

ARTICLE INFO

Article history:
Received 18 March 2016
Received in revised form 5 July 2017
Accepted 6 July 2017
Available online 26 July 2017
Communicated by Dieter Jungnickel

MSC:
13B99
13A99
13F99

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

ABSTRACT

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

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

and $p \,||\, n$ *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 $i \in \{1, \ldots, l\}$. 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

$$R_i \cong R_{i,1} \oplus \cdots \oplus R_{i,m_i}, \tag{2}$$

with $R_{i,j} \cong \mathbb{Z}/p_i^{u_{i,j}}\mathbb{Z}$ and $1 \leq u_{i,j} \leq t_i$.

Given $k \geq 1$, define the sets

$$\mathcal{P}_k(R) := \{p_i : R_i \text{ is a field and } p_i^{s_i} - 1 \mid k\},$$
$$\overline{\mathcal{P}}_k(R) := \{p_i : R_i \text{ is isomorphic to } \mathbb{Z}/p_i^{s_i}\mathbb{Z} \text{ with } s_i > 1 \text{ and } p_i - 1 \mid k\}.$$

Remark 1. Note that, due to Proposition 1, these sets consist of primes p_i such that their corresponding ring R_i in decomposition (1) satisfies that $S_k(R_i) \neq 0$. Proposition 2 below will imply that these are the only primes with this property.

In this paper, we completely solve the problem of computing $S_k(R)$ for any finite commutative unital ring. In particular, we will prove the following result.

Theorem 1. *Let R be a finite commutative unital ring with $|R| = p_1^{s_1} \cdots p_l^{s_l}$ and let $k \geq 1$ be an integer. Then, with the previous notation*

i) *If k is even, then*

$$S_k(R) = -\left(\sum_{p_i \in \mathcal{P}_k} \frac{|R|}{p_i^{s_i}} + \sum_{p_i \in \overline{\mathcal{P}}_k} \frac{|R|}{p_i}\right).$$

ii) *If $k > 1$ is odd and $2 \in \mathcal{P}_k$, then $S_k(R) = -|R|/2^{\nu_2(|R|)}$.*
iii) *If $k > 1$ is odd and $2 \in \overline{\mathcal{P}}_k$, then $S_k(R) = -|R|/2$.*
iv) *If $k > 1$ is odd and $R_i \cong \mathbb{F}_2[x]/(x^2)$ for some i, then $S_k(R) = u$, where u is the only non-zero nilpotent element of R such that $2u = 0$.*
v) *If $k = 1$ and $R_i \cong \mathbb{F}_2$ for some i, then $S_k(R) = -|R|/2$.*
vi) *In any other case, $S_k(R) = 0$.*

The paper is organized as follows. In Section 2 we provide all the results needed in order to prove Theorem 1. The proof of this theorem is the sole purpose of Section 3. Finally, as an application, we compute the power sums over $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$ in Section 4.

2. Preparatory results

We begin this section with the following straightforward result.

Lemma 1. *Let R_1 and R_2 be finite commutative unital rings and let $R = R_1 \oplus R_2$ be its direct sum. Then,*

$$S_k(R) = (|R_2|S_k(R_1), |R_1|S_k(R_2)).$$

Lemma 1, together with decomposition (1) above implies that, in order to get a general result, we can restrict ourselves to the prime-power characteristic case. Hence, throughout this section R will be a finite commutative unital ring with $\mathrm{char}(R) = p^t$.

In such case, due to decomposition (2), the additive group $(R, +)$ is the direct sum of cyclic p-groups. If $(R, +)$ is itself a cyclic p-group, then it must be $R \cong \mathbb{Z}/p^t\mathbb{Z}$ and Proposition 1 ii) applies to obtain that $S_k(R) = -p^{t-1}$ if $p - 1 \mid k$ and $S_k(R) = 0$ otherwise. Consequently, we will just focus on the non-cyclic case.

First of all, we will prove that if $t > 1$; i.e., if the characteristic is a prime-power but not a prime then $S_k(R) = 0$.

Proposition 2. *Let R be a finite commutative unital ring such that $char(R) = p^t$ with $t > 1$. If $(R, +)$ is not a cyclic p-group, then $S_k(R) = 0$ for every $k \geq 1$.*

Proof. Due to decomposition (2) we have that $R \cong R_1 \oplus \cdots \oplus R_m$ with $m \geq 2$, where $R_i \cong \mathbb{Z}/p^{t_i}\mathbb{Z}$ with $1 \leq t_i \leq t$.

Hence, if we denote by x_i a generator of R_i, then every element of R can be uniquely written in the form $a_1x_1 + \cdots + a_mx_m$ with $a_i \in \{0, \ldots, p^{t_i} - 1\}$ for each $i \in \{1, \ldots, m\}$. Thus,

$$S_k(R) = \sum_{a_i=0}^{p^{t_i}-1} (a_1x_1 + \cdots + a_mx_m)^k = \sum_{s=0}^{k} \sum_{a_i=0}^{p^{t_i}-1} \binom{k}{s} (a_1x_1)^s (a_2x_2 + \cdots + a_mx_m)^{k-s}.$$

The proof is by induction on $m \geq 2$.

First of all, assume that $m = 2$. In this case,

$$S_k(R) = \sum_{s=0}^{k} \binom{k}{s} \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_1x_1)^s (a_2x_2)^{k-s}$$

with either $t_1 \geq 2$ or $t_2 \geq 2$, for if $t_1, t_2 < 2$ then $t = 1$ which is not possible.

For every $s \in \{0, \ldots, k\}$, denote by $A(s) := \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_1x_1)^s (a_2x_2)^{k-s}$. Since $p^{t_i}x_i = 0$ we have that

$$A(0) = \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^k = p^{t_2} \sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^k = 0,$$

$$A(k) = \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_1x_1)^k = p^{t_1} \sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^k = 0.$$

On the other hand, if $0 < s < k$, then

$$A(s) = \sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^s \sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^{k-s}$$

and due to Proposition 1 ii) we have that $\sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^s$ is either 0 or $-p^{t_1-1}x_1^s$ and also that $\sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^{k-s}$ is either 0 or $-p^{t_2-1}x_2^{k-s}$. Consequently, it follows that either $A(s) = 0$ or $A(s) = p^{t_1+t_2-2}x_1^s x_2^{k-s}$ but in this latter case, since either $t_1 \geq 2$ or $t_2 \geq 2$, it also follows that $A(s) = 0$ as claimed.

Assume that the result is true for $2 \leq j < m$. We have

$$S_k(R) = \sum_{s=0}^{k} \binom{k}{s} \sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^s \sum_{\substack{a_i=0 \\ i\neq 1}}^{p^{t_i}-1} (a_2x_2 + \cdots + a_mx_m)^{k-s}$$

and for every $0 \leq s \leq k$ at least one of the terms appearing in the last expression is 0 by the induction hypothesis. □

The following series of technical lemmata will be useful when we consider the case $t = 1$ in the sequel. In what follows $\mathbb{F}_q$ will denote the field with q elements.

Lemma 2. *Let R be a finite commutative unital $\mathbb{F}_q$-algebra with $q > 2$ such that there exists $x \in R - \{0\}$ with $x^2 = 0$. Then, $S_k(R) = 0$ for every $k \geq 1$.*

Proof. Given $x \in R - \{0\}$ with $x^2 = 0$ we can decompose R as the direct sum of vector subspaces $R = \langle x \rangle \oplus \overline{R}$ for some $\overline{R} \leq R$. Thus,

$$S_k(R) = \sum_{a\in\mathbb{F}_q} \sum_{t\in\overline{R}} (ax+t)^k = \sum_{a\in\mathbb{F}_q} \sum_{t\in\overline{R}} (t^k + kt^{k-1}ax) =$$

$$= q\sum_{t\in\overline{R}} t^k + \sum_{a\in\mathbb{F}_q} a \sum_{t\in\overline{R}} kt^{k-1}x = \sum_{t\in\overline{R}} kt^{k-1}x \sum_{a\in\mathbb{F}_q} a = 0,$$

because, if $q > 2$, we have $\sum_{a\in\mathbb{F}_q} a = 0$ by Proposition 1 i). □

Lemma 3. *Let R be a finite commutative unital $\mathbb{F}_q$-algebra such that there exists a linearly independent set $\{x, y\}$ with $xy = 0$. Then, $S_k(R) = 0$ for every $k \geq 1$.*

Proof. Given a linearly independent set $\{x, y\}$ with $xy = 0$ we can decompose R as the direct sum of vector subspaces $R = \langle x \rangle \oplus \langle y \rangle \oplus \overline{R}$. Thus,

$$\begin{aligned} S_k(R) &= \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\sum_{t\in\overline{R}}(ax+by+t)^k = \\ &= \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\sum_{t\in\overline{R}}\left(t^k+\sum_{s=1}^{k}\binom{k}{s}(a^sx^s+b^sy^s)t^{k-s}\right) = \\ &= q^2\sum_{t\in\overline{R}}t^k + q\sum_{a\in\mathbb{F}_q}\sum_{t\in\overline{R}}\sum_{s=1}^{k}\binom{k}{s}a^sx^st^{k-s} + q\sum_{b\in\mathbb{F}_q}\sum_{t\in\overline{R}}\sum_{s=1}^{k}\binom{k}{s}b^sy^st^{k-s} = 0 \end{aligned}$$

as claimed. □

Lemma 4. *Let $R\cong\mathbb{F}_2[x]/(x^2)$ and let $e=x+(x^2)$ be the only non-zero nilpotent element of R. Then, $S_k(R)=e$ if $k>1$ is odd and $S_k(R)=0$ otherwise.*

Proof. In this situation, $R=\{0,1,e,1+e\}$ and since $\mathrm{char}(R)=2$, we have that

$$S_k(R)=0^k+1^k+e^k+(1+e)^k=ke$$

and the result follows. □

Finally, the main tool to prove Theorem 1 is the following result.

Lemma 5. *Let R be a finite commutative unital ring of prime-power characteristic.*

i) *If $R\cong\mathbb{F}_{p^r}$ and $p^r-1\mid k$, then $S_k(R)=-1$.*
ii) *If $R\cong\mathbb{Z}/p^r\mathbb{Z}$ and $p-1\mid k$, then $S_k(R)=-p^{r-1}$.*
iii) *If $R\cong\mathbb{F}_2[x]/(x^2)$ and $k>1$ is odd, then $S_k(R)=e$ where e is the only non-zero nilpotent element in R.*
iv) *In any other case, $S_k(R)=0$.*

Proof. To prove i) and ii) it is enough to apply Proposition 1 (Parts i) and ii), respectively). On the other hand, iii) follows from Lemma 4.

To prove iv), assume that $S_k(R)\neq 0$. Proposition 2 implies that if $(R,+)$ is not a cyclic p-group, it must have prime characteristic. If it is cyclic, then Proposition 1 i) or ii) applies (depending on whether R is a field or not) and condition i) or ii) would hold, respectively. If R is not cyclic and has prime characteristic, then it can be a field or not. If it is a field we apply again Proposition 1 i). If it is not a field, then Lemma 3 implies that R cannot contain two linearly independent zero-divisors so, not being a field, it must contain a non-zero nilpotent element of index 2. But in this case, Lemma 2 implies that $\mathrm{char}(R)=2$. Since all the previous restrictions lead to $R\cong\mathbb{F}_2[x]/(x^2)$, Lemma 4 applies and the result follows. □

3. Proof of Theorem 1

After all the previous work we can proceed to proof Theorem 1. First of all, observe that we can apply Lemma 1 to decomposition (1) to obtain that

$$S_k(R) = \left(\frac{|R|}{p_1^{s_1}} S_k(R_1), \ldots, \frac{|R|}{p_l^{s_l}} S_k(R_l) \right).$$

Now,

i) If k is even, Lemma 5 implies that $S_k(R_i) = 0$ unless R_i is a field with $|R_i| - 1 \mid k$ or $R_i \cong \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ with $p_i - 1 \mid k$ (recall that in the latter case $\mathrm{char}(R_i) = |R_i|$). Due to Proposition 1 i) and ii), in the first case $S_k(R_i) = -1$ while in the second case $S_k(R_i) = -p_i^{s_i - 1}$. The result follows.
ii) If $k > 1$ is odd and $2 \in \mathcal{P}_k$, we can assume without loss of generality that $p_1 = 2$. Then, Lemma 5 implies that $S_k(R_i) = 0$ for every $i \geq 2$ and the result follows from Proposition 1 i).
iii) It is enough to reason like in ii) but using Proposition 1 ii).
iv) Again the same idea as in ii) and iii) is used, but the claim follows from Lemma 4.
v) The same as in ii), iii) and iv). Note that in this case $2 \in \mathcal{P}_k$ and we can apply either Proposition 1 i) or ii).
vi) Lemma 5 states that the only cases in which $S_k(R_i) \neq 0$ for some i are precisely the previous ones.

4. Application. Power sums over $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$

As an application of the previous results, we are interested in computing the power sum $S_k((\mathbb{Z}/n\mathbb{Z})[x]/(f(x)))$, where $f(x)$ is a monic polynomial. When $\deg f = 1$, the result is straightforward because $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x)) \cong \mathbb{Z}/n\mathbb{Z}$ and Proposition 1 ii) applies.

Now, let us focus on the quadratic case. Before we proceed, let us introduce some notation. Given any positive integer n and integers b, c we define

$$R_n^{b,c} := (\mathbb{Z}/n\mathbb{Z})[x]/(x^2 + bx + c),$$

and let us denote $e = x + (x^2 + bx + c)$ the residue class of x.

As usual, to compute the value of $S_k(R_n^{b,c})$ we will first focus on the case when n is a prime power.

Proposition 3. *Let $k \geq 1$ be and integer.*

i) *If s is a positive integer,*

$$S_k(R_{2^s}^{b,c}) = \begin{cases} 1, & \text{if } s = 1,\ b \text{ and } c \text{ are odd and } 3 \mid k; \\ 1 + e, & \text{if } s = 1,\ b \text{ is even, } c \text{ is odd and } k > 1 \text{ is odd;} \\ e, & \text{if } s = 1,\ b \text{ and } c \text{ are even and } k > 1 \text{ is odd;} \\ 0, & \text{otherwise.} \end{cases}$$

ii) *If p is an odd prime and s is a positive integer,*

$$S_k(R_{p^s}^{b,c}) = \begin{cases} -1, & \text{if } s = 1,\ p^2 - 1 \mid k \text{ and } b^2 - 4c \text{ is not a square mod. } p; \\ 0, & \text{otherwise.} \end{cases}$$

Proof.

i) First of all, if $s > 1$ then $\mathrm{char}(R_{2^s}^{b,c}) \geq 4$ and we can apply Proposition 2 to obtain that $S_k(R_{2^s}^{b,c}) = 0$ for every k in this case.
If $s = 1$ and both b and c are even, then $R_{2^s}^{b,c} = \mathbb{F}_2[x]/(x^2)$ and by Lemma 4 it follows that $S_k(R_{2^s}^{b,c}) = e$ if $k > 1$ is odd and $S_k(R_{2^s}^{b,c}) = 0$ otherwise.
If $s = 1$, b is even and c is odd, then $R_{2^s}^{b,c} = \mathbb{F}_2[x]/(x^2+1)$ and by Lemma 4 it follows that $S_k(R_{2^s}^{b,c}) = 1 + e$ if $k > 1$ is odd (note that $1 + e$ is the only non-zero nilpotent element) and $S_k(R_{2^s}^{b,c}) = 0$ otherwise.
If $s = 1$, b is odd and c is even, then $R_{2^s}^{b,c} = \mathbb{F}_2[x]/(x^2+x)$. Since $0 = x^2+x = x(x+1)$, we can apply Lemma 3 with the linearly independent set $\{e, e+1\}$ to obtain that $S_k(R_{2^s}^{b,c}) = 0$ for every k in this case.
Finally, if both b and c are odd, then $R_{2^s}^{b,c} = \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$ because x^2+x+1 is irreducible. Hence, we apply Proposition 1 i) to obtain that $S_k(R_{2^s}^{b,c}) = -1 = 1$ if $3 \mid k$ and $S_k(R_{2^s}^{b,c}) = 0$ otherwise.

ii) First of all, if $s > 1$ then $\mathrm{char}(R_{p^s}^{b,c}) \geq p^2$ and we can apply Proposition 2 to obtain that $S_k(R_{p^s}^{b,c}) = 0$ for every k in this case.
If $s = 1$, observe that $x^2 + bx + c$ is reducible if and only if $b^2 - 4c$ is a quadratic residue modulo p. Now, if x^2+bx+c is reducible we can apply Lemma 2 or Lemma 3 to obtain that $S_k(R_{p^s}^{b,c}) = 0$ for every k. Finally, if $x^2 + bx + c$ is irreducible then $R_{p^s}^{b,c} \cong \mathbb{F}_{p^2}$ and Proposition 1 i) ends the proof. □

As a consequence of this proposition, we can prove the following general result in the quadratic case.

Corollary 1. *Let n be any positive integer. Given integers $k \geq 1$, b and c we define the following set:*

$$\mathcal{P}^{b,c}(k,n) := \{\text{prime } p : p \mid\mid n,\ p^2 - 1 \mid k,\ b^2 - 4c \text{ is not a quadratic residue modulo } p\}.$$

Then:

$$S_k(R_n^{b,c}) = \begin{cases} \frac{n}{2}, & \text{if } b \text{ and } c \text{ are odd, } 3 \mid k \text{ and } 2 \mid\mid n; \\ \frac{n}{2}(1+e), & \text{if } b \text{ is even, } c \text{ is odd, } k > 1 \text{ is odd, and } 2 \mid\mid n; \\ \frac{n}{2}e, & \text{if } b \text{ and } c \text{ are even, } k > 1 \text{ is odd and } 2 \mid\mid n; \\ -\displaystyle\sum_{p \in \mathcal{P}^{b,c}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

Proof. Observe that for n_1 and n_2 coprime we have $R^{b,c}_{n_1 n_2} \cong R^{b,c}_{n_1} \oplus R^{b,c}_{n_2}$. Thus, it suffices to apply Proposition 3. □

As a particular case, we obtain the power sum over the rings $(\mathbb{Z}/n\mathbb{Z})[\sqrt{D}]$ for a square-free integer D.

Corollary 2. *Let $k, n \geq 1$ be integers and let D be a square-free integer. Consider the set*

$$\mathcal{P}(k,n) := \{\text{prime } p : p \mid\mid n,\ p^2 - 1 \mid k,\ D \text{ is not a quadratic residue modulo } p\}$$

and let $e = x + (x^2 - D)$ be the residue class of x. Then,

$$S_k((\mathbb{Z}/n\mathbb{Z})[\sqrt{D}]) = \begin{cases} \frac{n}{2}(1+e), & \text{if } k > 1 \text{ is odd and } 2 \mid\mid n; \\ -\sum\limits_{p \in \mathcal{P}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

Proof. Just take $f(x) = x^2 - D$ and apply Corollary 1. □

Remark 2. If we consider the case $D = -1$, the previous corollary immediately gives Proposition 1 iii), which was proved in [2] using different, more direct, techniques.

Finally, we consider the case when the degree of the polynomial is greater than 2. The involved ideas are quite similar to those previously used. We introduce the following notation:

$$R^f_n := (\mathbb{Z}/n\mathbb{Z})[x]/(f(x)).$$

Corollary 3. *Let $f(x)$ be monic polynomial with integer coefficients such that $\deg f > 2$ and let $k, n \geq 1$ be integers. Consider the set*

$$\mathcal{P}^f(k,n) := \{\text{prime } p : p \mid\mid n,\ p^{\deg f} - 1 \mid k,\ f(x) \text{ is irreducible modulo } p\}.$$

Then,

$$S_k(R^f_n) \equiv -\sum_{p \in \mathcal{P}^f(k,n)} \frac{n^{\deg f}}{p^{\deg f}}.$$

Proof. Let $n = p_1^{s_1} \cdots p_l^{s_l}$. Then, as usual

$$R^f_n \cong R^f_{p_1^{s_1}} \oplus \cdots \oplus R^f_{p_l^{s_l}}$$

and we can apply Lemma 1.

Note that $S_k(R^f_{p_i^{s_i}}) = -1$ if $p_i \in \mathcal{P}^f(n,k)$ and $S_k(R^f_{p_i^{s_i}}) = 0$ otherwise. Since $|R^f_n| = n^{\deg f}$, the result follows. □

Acknowledgments

We want to thank the anonymous referee for his useful comments that helped to significantly improve the structure of the paper.

References

[1] L. Carlitz, The Staudt–Clausen theorem, Math. Mag. 34 (1960–1961) 131–146.
[2] P. Fortuny, J.M. Grau, A.M. Oller-Marcén, A von Staudt-type result for $\sum_{z\in\mathbb{Z}_n[i]} z^k$, Monatshefte Math. 178 (3) (2015) 345–359.
[3] J.M. Grau, P. Moree, A.M. Oller-Marcén, Solutions of the congruence $1 + 2^{f(n)} + \cdots + n^{f(n)} \equiv 0 \pmod{n}$, Math. Nachr. 289 (7) (2016) 820–830.
[4] P. Moree, On a theorem of Carlitz–von Staudt, C. R. Math. Acad. Sci. Canada 16 (4) (1994) 166–170.
[5] K.G.C. von Staudt, Beweis eines Lehrsatzes die Bernoullischen Zahlen betreffend, J. Reine Angew. Math. 21 (1840) 372–374.