ON POWER SUMS OF MATRICES OVER A FINITE COMMUTATIVE RING

P. FORTUNY, J.M. GRAU, A.M. OLLER-MARCÉN, AND I.F. RÚA

Abstract. In this paper we deal with the problem of computing the sum of the $k$-th powers of all the elements of the matrix ring $M_d(R)$ with $d > 1$ and $R$ a finite commutative ring. We completely solve the problem in the case $R = \mathbb{Z}/n\mathbb{Z}$ and give some results that compute the value of this sum if $R$ is an arbitrary finite commutative ring $R$ for many values of $k$ and $d$. Finally, based on computational evidence and using some technical results proved in the paper we conjecture that the sum of the $k$-th powers of all the elements of the matrix ring $M_d(R)$ is always 0 unless $d = 2$, $\text{card}(R) \equiv 2 \pmod{4}$, $1 < k \equiv -1, 0, 1 \pmod{6}$ and the only element $e \in R \setminus \{0\}$ such that $2e = 0$ is idempotent, in which case the sum is $\text{diag}(e, e)$.

1. Introduction

For a ring $R$ we denote by $M_d(R)$ the ring of $d \times d$ matrices over $R$. Now, given an integer $k \geq 1$ we define the sum

$$S^d_k(R) := \sum_{M \in M_d(R)} M^k.$$ 

This paper deals with the computation of $S^d_k(R)$ in the case when $R$ is finite and commutative.

When $d = 1$, the problem of computing $S^1_k(R)$ is completely solved only for some particular families of finite commutative rings. If $R$ is a finite field $\mathbb{F}_q$, the value of $S^1_k(\mathbb{F}_q)$ is well-known. If $R = \mathbb{Z}/n\mathbb{Z}$ the study of $S^1_k(\mathbb{Z}/n\mathbb{Z})$ dates back to 1840 \cite{9} and has been completed in various works \cite{2, 5, 7}. Finally, the case $R = \mathbb{Z}/n\mathbb{Z}[i]$ has been recently solved in \cite{3}. For those rings, we have the following result.

Theorem 1. Let $k \geq 1$ be an integer.

i) Finite fields:

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

ii) Integers modulo $n$:

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

iii) Gaussian integers modulo $n$:

$$S_k^1(\mathbb{Z}/n\mathbb{Z}[i]) = \begin{cases} \frac{4}{9}(1+i), & \text{if } k > 1 \text{ is odd and } n \equiv 2 \pmod{4}; \\ -\sum_{p \in \mathcal{P}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

where

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

and $p \mid n$ means that $p \mid n$, but $p^2 \not\mid n$.

On the other hand, if $d > 1$ the problem has been only solved when $R$ is a finite field \[1\]. In particular, the following result holds.

**Theorem 2.** Let $k, d \geq 1$ be integers. Then $S^d_k(\mathbb{F}_q) = 0$ unless $q = 2 = d$ and $1 < k \equiv -1, 0, 1 \pmod{6}$ in which case $S^d_k(\mathbb{F}_q) = I_2$.

In this paper we deal with the computation of $S^d_k(R)$ with $d > 1$ and $R$ a finite commutative ring. In particular Section 2 is devoted to completely determine the value of $S^d_k(R)$ in the case $R = \mathbb{Z}/n\mathbb{Z}$ (that we usually write as $\mathbb{Z}_n$). In Section 3 we give some technical results regarding sums of non-commutative monomials over $\mathbb{Z}/n\mathbb{Z}$ which will be used in Section 4 to compute $S^d_k(R)$ for an arbitrary finite commutative ring $R$ in many cases. Finally, we close the paper in Section 5 with the following conjecture based on strong computational evidence

**Conjecture 1.** Let $d > 1$ and let $R$ be a finite commutative ring. Then $S^d_k(R) = 0$ unless the following conditions hold:

1. $d = 2$,
2. $\text{card}(R) \equiv 2 \pmod{4}$ and $1 < k \equiv -1, 0, 1 \pmod{6}$,
3. The unique element $e \in R \setminus \{0\}$ such that $2e = 0$ is idempotent.

Moreover, in this case

$$S^d_k(R) = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}.$$  

2. Power sums of matrices over $\mathbb{Z}_n$

In what follows we will consider integers $n, d > 1$. For the sake of simplicity, $M^d_n$ will denote the set of integer matrices with entries in the range $\{0, \ldots, n-1\}$. Furthermore, for an integer $k \geq 1$, let $S^d_k(n) = \sum_{M \in M^d_n} M^k$. Our main goal in this section will be to compute the value of $S^d_k(n)$ modulo $n$. This is exactly the sum $S^d_k(\mathbb{Z}/n\mathbb{Z})$.

We start with the prime case. If $n = p$ is a prime, we have the following result \[1\] Corollary 3.2

**Proposition 1.** Let $p$ be a prime. Then, $S^d_k(p) \equiv 0 \pmod{p}$ unless $d = p = 2$.

Thus, the case $n = 2$ must be studied separately. In fact, we have

**Proposition 2.**

$$S^2_k(2) \equiv \begin{cases} 02 \pmod{2}, & \text{if } k = 1 \text{ or } k \equiv 2, 3, 4 \pmod{6}; \\ I_2 \pmod{2}, & \text{if } 1 < k \equiv 0, 1, 5 \pmod{6}. \end{cases}$$
Proof. For every $M \in M^2_n$ it holds that $M^2 \equiv M^8 \pmod 2$. As a consequence $S_k^2(2) \equiv S_k^2(2) + 6 \pmod 2$ for every $k > 1$. Thus, the result follows just computing $S_k^2(2)$ for $1 \leq k \leq 7$. \qed

Now, we turn to the prime power case. The following lemma is straightforward.

**Lemma 1.** Let $p$ be a prime. Then, any element $M \in M^d_{p^{s+1}}$ can be uniquely written in the form $A + p^sB$, where $A \in M^d_p, B \in M^d_p$.

Using this lemma we can prove the following useful result.

**Proposition 3.** Let $p$ be a prime. Then, $S_k^d(p^{s+1}) \equiv p^dS_k^d(p^s) \pmod {p^{s+1}}$.

**Proof.** By the previous lemma we have

$$S_k^d(p^{s+1}) = \sum_{M \in M^d_{p^{s+1}}} M^k = \sum_{A \in M^d_p} \sum_{B \in M^d_p} (A + p^sB)^k.$$

Using the non-commutative version of the binomial theorem we have that

$$(A + p^sB)^k \equiv A^k + p^s \sum_{t=1}^k A^{k-t} B A^{t-1}) \pmod {p^{s+1}}.$$

Thus, combining this with (1) we obtain

$$S_k^d(p^{s+1}) \equiv \sum_{B \in M^d_p} \left( \sum_{A \in M^d_p} A^k \right) + \sum_{t=1}^k \sum_{A \in M^d_p} A^{k-t} \left( p^s \sum_{B \in M^d_p} B \right) A^{t-1}$$

$$\equiv p^dS_k^d(p^s) + \sum_{t=1}^k \sum_{A \in M^d_p} A^{k-t} (p^sS_k^d(p)) A^{t-1}$$

$$\equiv p^dS_k^d(p^s) \pmod {p^{s+1}}$$

because $S_k^d(p) \equiv 0 \pmod p$ by Propositions 1 and 2 (depending on whether $p$ is odd or not). \qed

**Remark.** Note that Proposition 3 implies that if $S_k^d(p^s) \equiv 0 \pmod {p^s}$, then also $S_k^d(p^{s+1}) \equiv 0 \pmod {p^{s+1}}$.

As a consequence we get the following result which extends Proposition 1.

**Corollary 1.** $S_k^d(p^s) \equiv 0 \pmod {p^s}$ unless $d = p = 2$ and $s = 1$.

**Proof.** If $p = d = 2$, then Proposition 3 implies that $S_k^2(4) \equiv 2^4S_k^2(2) \equiv 0 \pmod 4$, so the previous remark leads to $S_k^2(2^s) \equiv 0 \pmod {2^s}$, for every $s > 1$. On the other hand, if $d$ or $p$ is odd, then we know by Proposition 1 that $S_k^d(p) \equiv 0 \pmod p$. Again, the remark gives us $S_k^d(p^s) \equiv 0$, by induction for all $s \geq 1$. \qed

In order to study the general case the following lemma will be useful. It is an analogue of [3, Lemma 3 i)]

**Lemma 2.** If $m | n$, then $S_k^d(n) \equiv \left( \frac{n}{m} \right) d^2 S_k^d(m) \pmod m$. 

Proof. Given a matrix $M \in M_n^d$, let $M = (m_{i,j})$ with $1 \leq i, j \leq d$. Then,

$$S^d_k(n) = \sum_{M \in M_n^d} M^k = \sum_{0 \leq m_{i,j} \leq n-1} \left( m_{i,j} \right)^k \equiv \left( \frac{n}{m} \right)^d \sum_{0 \leq m_{i,j} \leq m-1} \left( m_{i,j} \right)^k = S^d_k(m) \pmod{m}$$

\[\square\]

Now, we can prove the main result of this section.

**Theorem 3.** The following congruence modulo $n$ holds:

$$S^d_k(n) \equiv \begin{cases} \frac{n}{2} \cdot I_2, & \text{if } d = 2, \ n \equiv 2 \pmod{4} \ \text{and} \ \ 1 < k \equiv 0, 1, 5 \pmod{6}; \\ 0, & \text{otherwise.} \end{cases}$$

**Proof.** Let $n = 2^s p_1^{r_1} \cdots p_t^{r_t}$ be the prime power decomposition of $n$. If $1 \leq i \leq t$, we have by Lemma 2 and Corollary 1 that

$$S^d_k(n) \equiv \left( \frac{n}{p_i^{r_i}} \right)^d S^d_k(p_i^{r_i}) \equiv 0 \pmod{p_i^{r_i}}.$$ 

On the other hand, using again Lemma 2 we have that

$$S^d_k(n) \equiv \left( \frac{n}{2^s} \right)^d S^d_k(2^s) \pmod{2^s}.$$ 

Hence, Corollary 1 implies that $S^d_k(n) \equiv 0 \pmod{2^s}$ unless $d = p = 2$ and $s = 1$.

To conclude, it is enough to apply Proposition 2 together with the Chinese Remainder Theorem. \[\square\]

The following corollary easily follows from Theorem 3 and it confirms the conjecture stated in the sequence A017593 from the OEIS.

**Corollary 2.** $S^2_k(n) \not\equiv 0 \pmod{n}$ if and only if $n \equiv 6 \pmod{12}$.

As a further application of Theorem 3 application we are going to compute the sum of the powers of the Hamilton quaternions over $\mathbb{Z}/n\mathbb{Z}$.

**Proposition 4.** For every $n \in \mathbb{N}$ and $l > 0$, it holds that

$$\sum_{z \in \mathbb{Z}_n[i,j,k]} z^l = 0.$$ 

**Proof.** Since for all $z \in \mathbb{Z}_2[i,j,k]$ we have that $z^2 \in \mathbb{Z}_2$, we deduce that $z^4 = z^2$, and so it can be straightforwardly checked that

$$\sum_{z \in \mathbb{Z}_2[i,j,k]} z^l = 0.$$ 

Now, if $s > 1$, observing that

$$\mathbb{Z}_{2^s}[i,j,k] \cong \left\{ \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} : a, b, c, d \in \mathbb{Z}_2 \right\}$$
Lemma 4. Let \( r > 1 \) from Section 2. Thus, in what follows we assume we can adapt Lemma 1, Proposition 3 and Corollary 1 to inductively obtain that
\[
\sum_{z \in \mathbb{Z}_2^* \cdot [i,j,k]} z^l = 0.
\]

Finally, if \( n = 2^s m \) with \( m \) odd we know [3] Theorem 4 that
\[
\mathbb{Z}_n[i,j,k] \cong \mathbb{Z}_2^* \cdot [i,j,k] \times \mathbb{Z}_m[i,j,k] \cong \mathbb{Z}_2^* \cdot [i,j,k] \times M_2(\mathbb{Z}_m)
\]
and the result follows from Theorem 3. \( \square \)

3. Sums of non-commutative monomials over \( \mathbb{Z}_n \)

We will now consider a more general setting. Let \( r \geq 1 \) be an integer and consider \( w(x_1, \ldots, x_r) \) a monomial in the non-commuting variables \( \{x_1, \ldots, x_r\} \) of total degree \( k \). In this situation, we define the sum
\[
S^d_w(n) := \sum_{A_1, \ldots, A_r \in M_d^2} w(A_1, \ldots, A_r).
\]
Note that if \( r = 1 \), then \( w(x_1) = x_1^k \) and \( S^d_w(n) = S^d_k(n) \) so we recover the situation from Section 2. Thus, in what follows we assume \( r > 1 \).

We want to study the value of \( S^d_w(n) \) modulo \( n \). To do so we first introduce two technical lemmas that extend [1] Lemma 2.3.

Lemma 3. Let \( \tau \geq 1 \) be an integer and let \( \beta_i > 0 \) for every \( 1 \leq i \leq \tau \). If \( p \) is an odd prime,
\[
\sum_{x_1, \ldots, x_\tau} x_1^{\beta_1} \cdots x_\tau^{\beta_\tau} \equiv \begin{cases} (-p^{s-1})^{\tau}, & \text{if } p - 1 \mid \beta_i \text{ for every } i; \\ 0, & \text{otherwise.} \end{cases} \quad (\text{mod } p^s)
\]
where the sum is extended over \( x_1, \ldots, x_\tau \) in the range \( \{0, \ldots, p^s - 1\} \). Also, if some \( \beta_i = 0 \), then
\[
\sum_{x_1, \ldots, x_\tau} x_1^{\beta_1} \cdots x_\tau^{\beta_\tau} \equiv 0 \pmod{p^s}.
\]

Proof. It is enough to apply [3] Lemma 3 ii) which states that
\[
\sum_{x_i = 0}^{p^s - 1} x_i^{\beta_i} \equiv \begin{cases} -p^{s-1}, & \text{if } p - 1 \mid \beta_i; \\ 0, & \text{otherwise.} \end{cases} \quad (\text{mod } p^s)
\]
for every \( 1 \leq i \leq \tau \). Observe that, if \( \beta_i = 0 \), then:
\[
\sum_{x_1, \ldots, x_\tau} x_1^{\beta_1} \cdots x_\tau^{\beta_\tau} = \sum_{x_i, x_j \neq i} x_1^{\beta_1} \cdots x_{i-1}^{\beta_{i-1}} x_{i+1}^{\beta_{i+1}} \cdots x_\tau^{\beta_\tau} \equiv 0 \pmod{p^s}
\]
\( \square \)

Remark. Observe that in the previous situation, if \( \tau \geq 2 \) and \( s > 1 \), it easily follows that
\[
\sum_{x_1, \ldots, x_\tau} x_1^{\beta_1} \cdots x_\tau^{\beta_\tau} \equiv 0 \pmod{p^s}
\]
regardless the values of \( \beta_i \geq 0 \).

Lemma 4. Let \( \tau \geq 1 \) be an integer and let \( \beta_i > 0 \) for every \( 1 \leq i \leq \tau \). Then,
\[
\sum_{x_1, \ldots, x_\tau} x_1^{\beta_1} \cdots x_\tau^{\beta_\tau} \equiv \begin{cases} 1, & \text{if } s = 1; \\ 0, & \text{if } s > 1 \text{ and } \beta_i > 1 \text{ and odd for some } i; \\ (-1)^A(2^{s-1})^B, & \text{if } s > 1 \text{ and } \beta_i = 1 \text{ or even for every } i, \end{cases} \quad (\text{mod } 2^s)
\]
where the sum is extended over $x_1, \ldots, x_\tau$ in the range $\{0, \ldots, 2^s-1\}$. $A = \text{card}\{\beta_i : \beta_i = 1\}$ and $B = \text{card}\{\beta_i : \beta_i \text{ is even}\}$. Also, if some $\beta_i = 0$, then $\sum_{x_1, \ldots, x_\tau} x_1^{\beta_1} \cdots x_\tau^{\beta_\tau} \equiv 0 \pmod{2^s}$.

Proof. It is enough to apply [6, Lemma 3 iii)] which states that

$$\sum_{x_i=0}^{2^s-1} x_i^{\beta_i} \equiv \begin{cases} 2^s-1, & \text{if } s = 1 \text{ or } s > 1 \text{ and } \beta_1 > 1 \text{ is even;} \\ -1, & \text{if } s > 1 \text{ and } \beta_i = 1; \\ 0, & \text{if } s > 1 \text{ and } \beta_1 > 1 \text{ is odd} \end{cases} \pmod{p^s}$$

for every $1 \leq i \leq \tau$. The proof of the case when some $\beta_i = 0$ is identical to that of the previous lemma. □

As a consequence, we get the following results.

**Proposition 5.** Let $p$ be an odd prime and let $s > 1$ be an integer. Then,

$$S^d_w(p^s) \equiv 0 \pmod{2^s}.$$

Proof. Let $A_l = (a_{l,j})_{1 \leq i,j \leq d}$ for every $1 \leq l \leq r$. Note that each entry in the matrix $S^d_w(p^s)$ is a homogeneous polynomial in the variables $a_{l,j}$. Observe also that these variables are summation indexes in the range $\{0, \ldots, p^s-1\}$. Hence, the number of variables is $rd^2 > 2$ and, since $s > 1$, the Remark 3 can be applied to the sum of its monomials, and the result follows. □

**Proposition 6.** Let $s > 1$ be an integer. Assume that one of the following conditions holds:

i) $k \leq rd^2$,

ii) $k > rd^2$ and $k + rd^2$ is even.

Then, $S^d_w(2^s) \equiv 0 \pmod{2^s}$.

Proof. Just like in the previous proposition each entry in the matrix $S^d_w(2^s)$ is a homogeneous polynomial in the $rd^2$ variables $a_{l,j}$. Hence, it is a sum of elements of the form

$$\sum_{a_{l,j} \in \mathbb{Z}_{2^s}} \prod_{l,j} (a_{l,j})^{\beta_{l,j,l}}.$$

Observe that $\sum_{i,j,l} \beta_{i,j,l} = k$ so, if $k < rd^2$ it follows that some $\beta_{i,j,l} = 0$, and so each monomial sum is $0 \pmod{2^s}$ (because of Lemma 3). Therefore, each entry in the matrix $S^d_w(p)$ is $0 \pmod{2^s}$ in this case, as claimed.

Now, assume that $k \geq rd^2$ and $k + rd^2$ is even (in particular if $k = rd^2$). Due to Lemma 4 an element

$$\sum_{a_{l,j} \in \mathbb{Z}_{2^s}} \prod_{l,j} (a_{l,j})^{\beta_{l,j,l}}$$

is $0 \pmod{2^s}$ unless in one of its monomials the set of $rd^2$ exponents $\beta_{i,j,l}$ is formed by exactly $rd^2 - 1$ ones and 1 even value. But in this case $k = (rd^2 - 1) + 2\alpha$ so $k + rd^2$ is odd, a contradiction. Consequently, each entry in the matrix $S^d_w(p)$ is also $0 \pmod{2^s}$ in this case and the result follows. □

As Remark 3 and Lemma 4 point out, the case $s = 1$ must be considered separately. In this case, we have the following result.

**Proposition 7.** Let $p$ be a prime. Assume that one of the following conditions holds:
i) \( k < rd^2(p - 1) \),

ii) \( k \) is not a multiple of \( p - 1 \).

Then, \( S^d_w(p) \equiv 0 \pmod{p} \).

**Proof.** If \( p = 2 \) condition ii) cannot hold and if condition i) holds, we can apply the same argument of the proof of the first part of Proposition 6 to get the result.

Now, if \( p \) is odd, again each entry in the matrix \( S^d_w(p) \) is a homogeneous polynomial in the \( rd^2 \) variables \( a_{i,j}^l \). Hence, it is a sum of elements of the form

\[
\sum_{a_{i,j}^l \in \mathbb{Z}_p} \prod_{i,j} (a_{i,j}^l)^{\beta_{i,j,l}}.
\]

We have that \( \sum_{i,j} \beta_{i,j,l} = k \) so, if \( k < rd^2(p - 1) \) or if it is not a multiple of \( p - 1 \) it follows that some \( \beta_{i,j,l} \) is either 0 or not a multiple of \( p - 1 \). In either case the corresponding element is 0 \pmod{p} due to Lemma 3 and, consequently, each entry in the matrix \( S^d_w(p) \) is also 0 \pmod{p} as claimed. \( \square \)

Observe that in the previous results we have considered sums of the form

\[
S^d_w(p) = \sum_{A_1, \ldots, A_r \in M^d_{d^{s_1}}} w(A_1, \ldots, A_r),
\]

where all the matrices \( A_i \) belong to the same matrix ring \( M^d_{d^{s_i}} \). The following proposition will be useful in the next section and deals with the case when the matrices \( A_i \) belong to different matrix rings. First, we introduce some notation.

Given a prime \( p \), let

\[
S^d_w(p^{s_1}, \ldots, p^{s_r}) := \sum_{A_i \in M^d_{d^{s_i}}} w(A_1, \ldots, A_r).
\]

If \( s_1 = \cdots = s_r = s \), then \( S^d_w(p^{s_1}, \ldots, p^{s_r}) = S^d_w(p^s) \) and we are in the previous situation.

**Proposition 8.** With the previous notation, if \( s_1 > 1 \), then

\[
S^d_w(p^{s_1+1}, p^{s_2}, \ldots, p^{s_r}) \equiv p^{d^2} S^d_w(p^{s_1}, p^{s_2}, \ldots, p^{s_r}) \pmod{p^{s_1+1}}.
\]
Proof. Since $s_1 > 1$ we have that $2s_1 > s_1 + 1$ so, due to Lemma 1

\[ S_w^d(p^{s_1 + 1}, p^{s_2}, \ldots, p^{s_t}) = \sum_{A_i \in M_{p^{s_1 + 1}}^d} w(A_1, \ldots, A_t) = \sum_{B \in M_{p^{s_1 + 1}}^d, C \in M_p^d} w(B + p^{s_1} C, A_2, \ldots, A_r) \equiv \sum_{B \in M_{p^{s_1 + 1}}^d, C \in M_p^d} w(B, A_2, \ldots, A_r) + p^{s_1} \sum_l w_l(B, C, A_2, \ldots, A_r) \]

\[ = p^d S_w^d(p^{s_1}, \ldots, p^{s_t}) + p^{s_1} \sum_l w_l(B, C, A_2, \ldots, A_r) \]

\[ \equiv \left( w(B, A_2, \ldots, A_r) + p^{s_1} \sum_l w_l(B, C, A_2, \ldots, A_r) \right) \]

\[ \equiv \left( w(B, A_2, \ldots, A_r) + p^{s_1} \sum_l w_l(B, C, A_2, \ldots, A_r) \right) \equiv 0 \pmod{p} \]

because $S_w^d(p) \equiv 0 \pmod{p}$ and the result follows. \hfill \Box

The following corollary is now straightforward.

Corollary 3. Assume that $S_w^d(p) \equiv 0 \pmod{p}$. Let us consider $s_1 \geq s_2 \geq \cdots \geq s_r = s$. Then,

\[ S_w^d(p^{s_1}, \ldots, p^{s_r}) \equiv 0 \pmod{p^{s_1}}. \]

Proof. Just apply the previous proposition repeatedly. \hfill \Box

4. Power sums of matrices over a finite commutative ring

In this section we will use the results from Section 3 to compute $S_w^d(R)$ for an arbitrary finite commutative ring $R$ in many cases.

First of all, note that if char$(R) = n = p_1^{s_1} \cdots p_r^{s_r}$, then $R \cong R_1 \times \cdots \times R_t$, where char$(R_i) = p_i^{s_i}$ and each $R_i$ is a subring of characteristic $p_i^{s_i}$ and, in particular, a $\mathbb{Z}/p_i^{s_i} \mathbb{Z}$-module. This allows us to restrict ourselves to the case when char$(R)$ is a prime power.

The simplest case arises when $R$ is a free $\mathbb{Z}/p \mathbb{Z}$-module for an odd prime $p$.

Proposition 9. Let $p$ be an odd prime and let $R$ be a finite commutative ring of characteristic $p^r$, such that $R$ is a free $\mathbb{Z}/p \mathbb{Z}$-module of rank $r$. Then,

i) If $s > 1$, $S_w^d(R) = 0$ for every $k \geq 1$ and $d \geq 2$. 

\[ \]
If \( s = 1 \), \( S_k^d(R) = 0 \) for every \( d \geq 2 \) and \( k \) such that either \( k < rd^2(p - 1) \) or \( k \) is not a multiple of \( p - 1 \).

**Proof.** Note that under the previous assumptions and using Proposition\( \ref{prop:9} \) or Proposition\( \ref{prop:10} \) (depending on whether \( s > 1 \) or \( s = 1 \)), it follows that

\[
\sum_{A_1, \ldots, A_r \in \mathbb{M}_{p^r}^d} (x_1 A_1 + \cdots + x_r A_r)^k \equiv 0 \pmod{p^s}
\]

because each entry of such a matrix is a polynomial in \( x_1, \ldots, x_r \) whose coefficients are 0 modulo \( p^s \).

Consequently, for every \( g_1, \ldots, g_r \in R \) we have that

\[
\sum_{A_1, \ldots, A_r \in \mathbb{M}_{p^r}^d} (g_1 A_1 + \cdots + g_r A_r)^k = 0.
\]

Now, since \( R \) is free of rank \( r \) we can take a basis \( g_1, \ldots, g_r \) of \( R \) so that \( \mathbb{M}_{p^r}^d = \{g_1 A_1 + \cdots + g_r A_r | A_i \in \mathbb{M}_{p^r}^d\} \). Therefore

\[
S_k^d(R) = \sum_{A_1, \ldots, A_r \in \mathbb{M}_{p^r}^d} (g_1 A_1 + \cdots + g_r A_r)^k.
\]

This concludes the proof. \( \square \)

If \( p = 2 \), we have the following version of Proposition\( \ref{prop:9} \).

**Proposition 10.** Let \( R \) be a finite commutative ring of characteristic \( 2^s \), such that \( R \) is a free \( \mathbb{Z}_{2^s} \)-module of rank \( r \). Then,

i) If \( s > 1 \), \( S_k^d(R) = 0 \) for every \( d \geq 2 \) and \( k \) such that \( k \leq rd^2 \) or \( k > rd^2 \) with \( k + rd^2 \) even.

ii) If \( s = 1 \), \( S_k^d(R) = 0 \) for every \( d \geq 2 \) and \( k \) such that either \( k < rd^2 \).

**Proof.** The proof is similar to that of Proposition\( \ref{prop:9} \) using Proposition\( \ref{prop:10} \) or Proposition\( \ref{prop:11} \) depending on whether \( s > 1 \) or \( s = 1 \). \( \square \)

**Remark.** Note that if \( R \) is a finite commutative ring of characteristic \( p^s \) and \( s = 1 \), then \( R \) is necessarily free. Consequently, to study the non-free case we may assume that \( s > 1 \).

Assume that elements \( g_1, \ldots, g_r \) form a minimal set of generators of a non-free \( \mathbb{Z}_{p^s} \)-module \( R \). Since \( R \) is non-free and \( \text{char}(R) = p^s \), it follows that \( r > 1 \) and also \( s > 1 \). For every \( i \in \{1, \ldots, r\} \) let \( 1 \leq s_i \leq s \) be minimal such that \( p^{s_i} g_i = 0 \). Note that it must be \( s_i = s \) for some \( i \) and \( s_j < s \) for some \( j \). There is no loss of generality in assuming that \( s = s_1 \geq \cdots \geq s_r \) and at least one of the inequalities is strict. Note that \( p^{s_1}, \ldots, p^{s_r} \) are the invariant factors of the \( \mathbb{Z} \)-module \( R \). With this notation we have the following result extending Proposition\( \ref{prop:9} \).

**Proposition 11.** Let \( p \) be an odd prime and let \( R \) be a finite commutative ring of characteristic \( p^s \), such that \( R \) is a non-free \( \mathbb{Z}_{p^s} \)-module. Then,

i) If \( s_r > 1 \), \( S_k^d(R) = 0 \) for every \( k \geq 1 \) and \( d \geq 2 \).

ii) If \( s_r = 1 \), \( S_k^d(R) = 0 \) for every \( d \geq 2 \) and \( k \) such that either \( k < rd^2(p - 1) \) or \( k \) is not a multiple of \( p - 1 \).
Proof. First of all, observe that
\[ S^d_k(R) = \sum_{A_i \in \mathbb{M}^d_{p^s_i}} (g_1 A_1 + \cdots + g_r A_r)^k. \]
In both situations i) and ii) it follows that \( S^d_w(p^{s_r}) \equiv 0 \pmod{p^{s_r}} \). Moreover, we are in the conditions of Corollary 3, so it follows that \( S^d_w(p^s, p^{s^2}, \ldots, p^{s_r}) \equiv 0 \pmod{p^s} \). Consequently all the coefficients of the above sum are 0 modulo \( p^s \) and the result follows. \( \square \)

The corresponding result for \( p = 2 \) is as follows.

**Proposition 12.** Let \( R \) be a finite commutative ring of characteristic \( 2^s \), such that \( R \) is a non-free \( \mathbb{Z}_{2^s} \)-module. Then,

i) If \( s_r > 1 \), \( S^d_k(R) = 0 \) for every \( d \geq 2 \) and \( k \) such that \( k \leq rd^2 \) or \( k > rd^2 \) with \( k + rd^2 \) even.

ii) If \( s_r = 1 \), \( S^d_k(R) = 0 \) for every \( d \geq 2 \) and \( k \) such that either \( k < rd^2 \).

**Proof.** It is identical to the proof of Proposition 11. \( \square \)

5. Conjectures and further work

Given a finite commutative ring \( R \) of characteristic \( n \), we have seen in the last section that \( S^d_k(R) = 0 \) for many values of \( k, d \) and \( n \). In this section we present two conjectures based on strong computational evidence which, being true, would let us to give a general result about \( S^d_k(R) \).

With the notation from the previous section, given an \( r \)-tuple of integers \( \kappa = (k_1, \ldots, k_r) \), we consider the set of monomials in the non-commuting variables \( \{x_1, \ldots, x_r\} \)
\[ \Omega_\kappa := \{w : \deg_{x_i}(w) = k_i, \text{ for every } i\}. \]
The following conjectures are based on computational evidence.

**Conjecture 2.** With the previous notation, let \( s_1 \geq s_2 \geq \cdots \geq s_r \). Then
\[ S^d_w(p^{s_1}, p^{s_2}, \ldots, p^{s_r}) \equiv 0 \pmod{p^{s_1}}, \]
unless \( d = p = 2 \) and \( s_i = 1 \) for all \( i \).

**Conjecture 3.** If \( p = 2 = d \) and \( r > 1 \) then for every \( \kappa \in \mathbb{N}^r \)
\[ \sum_{w \in \Omega_\kappa} \sum_{A_i \in \mathbb{M}^d_2} w(A_1, \ldots, A_r) \equiv 0 \pmod{2}. \]

The next lemma extends Lemma 2 in some sense. Its proof is straightforward.

**Lemma 5.** Let \( R_1 \) and \( R_2 \) be finite commutative rings, and let \( R = R_1 \times R_2 \) be its direct product. Then
\[ S^d_k(R) = (\text{card}(R_2)^d \cdot S^d_k(R_1), \text{card}(R_1)^d \cdot S^d_k(R_2)) \in \mathbb{M}_d(R_1) \times \mathbb{M}_d(R_2) \]

Now, the following proposition would follow from Conjectures 2 and 3.

**Proposition 13.** Let \( R \) be a finite commutative ring of characteristic \( p^s \) for some prime \( p \). Then \( S^d_k(R) = 0 \) unless \( d = 2 \), \( R = \mathbb{Z}/2\mathbb{Z} \) and \( 1 < k \equiv -1, 0, 1 \pmod{6} \). Moreover, in this case \( S^d_k(R) = I_2 \).
**Theorem 4.** Let \( d > 1 \) and let \( R \) be a finite commutative ring. Then \( S_k^d(R) = 0 \) unless the following conditions hold:

1. \( d = 2 \),
2. \( \text{card}(R) \equiv 2 \pmod{4} \) and \( 1 < k \equiv -1, 0, 1 \pmod{6} \),
3. The unique element \( e \in R \setminus \{0\} \) such that \( 2e = 0 \) is idempotent.

Moreover, in this case

\[
S_k^d(R) = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}.
\]

**Proof.** First, observe that if \( \text{card}(R) \equiv 2 \pmod{4} \), then \( R \) has \( 2m \) elements, where \( m \) is odd. Therefore, the 2–primary component of the additive group \( R \) has only two elements, and so there is a unique element \( e \in R \) of additive order 2.

Now, if \( R \) is of characteristic \( p^s \) for some prime, the result follows from the above proposition. Hence, we assume that \( R \) has composite characteristic. Let \( R = R_1 \times R_2 \) with \( R_1 \) the zero ring or \( \text{char}(R_1) = 2^s \) and \( \text{char}(R_2) \) odd. Due to Lemma 5 and Proposition 13 it follows that \( S_k^d(R) = (\text{card}(R_2))^{d^2} : S_k^d(R_1), 0) \).

Now, \( S_k^d(R_1) = 0 \) unless \( d = 2 = p, R_1 = \mathbb{Z}/2\mathbb{Z} \) and \( 1 < k \equiv -1, 0, 1 \pmod{6} \) in which case

\[
S_k^d(R_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix},
\]

where \( e = (1, 0) \in R_1 \times R_2 \) is the only idempotent of \( R \) such that \( 2e = 0 \). \( \square \)

**Remark.** Note that if, in addition, \( R \) is unital then the element \( e \) from the previous theorem is just \( e = \frac{\text{card}(R)}{2} \cdot 1_R \). Also note that if \( S_k^d(R) \neq 0 \), then \( R \cong \mathbb{Z}/2\mathbb{Z} \times R_2 \) with \( \text{card}(R_2) \) odd or \( R_2 = \{0\} \).

We close the paper with a final conjecture.

**Conjecture 4.** Theorem 4 remains true if \( R \) is non-commutative.
References

[1] J.V. Brawley, L. Carlitz, J. Levine. Power sums of matrices over a finite field. *Duke Math. J.*, 41:9–24, 1974.
[2] L. Carlitz. The Staudt-Clausen theorem. *Math. Mag.*, 34:131–146, 1960-1961.
[3] P. Fortuny, J.M. Grau, A. M. Oller-Marcén. A von Staudt-type result for $\sum_{x \in \mathbb{Z}_n} x^k$. *Monatsh. Math.* DOI: 10.1007/s00605-015-0736-5, 2015.
[4] J.M. Grau, C. Miguel, A.M. Oller-Marcén. On the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$. *Adv. Appl. Clifford Algebr.*, DOI: 10.1007/s00006-015-0544-y, 2015.
[5] J.M. Grau, P. Moree, A.M. Oller-Marcén. Solutions of the congruence $\sum_{k=1}^{n} k^{f(n)} \equiv 0 \pmod{n}$. *Math. Nachr.*, to appear.
[6] J.M. Grau, A.M. Oller-Marcén, J. Sondow. On the congruence $1^m + 2^m + \cdots + m^m \equiv n \pmod{m}$ with $n \mid m$. *Monatsh. Math.*, DOI 10.1007/s00605-014-0660-0, 2014.
[7] P. Moree. On a theorem of Carlitz-von Staudt. *C. R. Math. Rep. Acad. Sci. Canada*, 16(4):166–170, 1994.
[8] N.J.A. Sloane. The On-Line Encyclopedia of Integer Sequences. https://oeis.org.
[9] K.G.C. von Staudt. Beweis eines Lehrsatzes die Bernoullischen Zahlen betreffend. *J. Reine Angew. Math.*, 21:372–374, 1840.

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain
E-mail address: fortunypedro@uniovi.es

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain
E-mail address: grau@uniovi.es

Centro Universitario de la Defensa de Zaragoza, Ctra. Huesca s/n, 50090 Zaragoza, Spain
E-mail address: oller@unizar.es

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain
E-mail address: rua@uniovi.es