Electronic Research Archive

https://www.aimspress.com/journal/era

ERA, 33(3): 1323–1332.
DOI: 10.3934/era.2025059
Received: 23 December 2024
Revised: 24 February 2025
Accepted: 25 February 2025
Published: 05 March 2025

Research article

On the sumsets of units in a ring of matrices over $\mathbb{Z}/m\mathbb{Z}$

Yifan Luo*, **Kaisheng Lei and Qingzhong Ji**

Department of Mathematics, Nanjing University, Nanjing 210000, China

* **Correspondence:** Email: 602022210010@smail.nju.edu.cn.

Abstract: Let $M_{n,m} := Mat_n(\mathbb{Z}/m\mathbb{Z})$ be the ring of matrices of $n \times n$ over $\mathbb{Z}/m\mathbb{Z}$ and $G_{n,m} := Gl_n(\mathbb{Z}/m\mathbb{Z})$ be the multiplicative group of units of $M_{n,m}$ with $n \geqslant 2, m \geqslant 2$. In this paper, we obtain an exact formula for the number of representations of any element of $M_{2,m}$ as the sum of k units in $M_{2,m}$. Furthermore, by using the technique of Fourier transformation, we also give a formula for the case $n \geq 3$ and $m = p$ is a prime.

Keywords: rings of matrices; finite fields; sums of units; Fourier transformation

1. Introduction

Let R be a finite ring with $1 \in R$, and let R^* denote the multiplicative group of units in R. Let k be an integer with $k \geq 2$, and let $\sharp S$ denote the cardinality of any finite set S. For any $c \in R$, we define

$$S_k(R, c) := \left\{ (x_1, x_2, \ldots, x_k) \in (R^*)^k \;\middle|\; \sum_{i=1}^{k} x_i = c \right\},$$

and

$$N_k(R, c) := \sharp S_k(R, c).$$

For a positive integer n, let $\mathbb{Z}/n\mathbb{Z}$ be the ring of residue classes modulo n. In 2000, Deaconescu [1] obtained a formula for $N_2(\mathbb{Z}/n\mathbb{Z}, c)$. In 2009, Sander [2] gave a generalization of the above result. In fact, for any integer c, he determined the number of representations of c as a sum of two units (two nonunits, a unit, and a nonunit, respectively) in $\mathbb{Z}/n\mathbb{Z}$.

For a positive integer n with divisors $k_1, k_2, ..., k_t (t \geqslant 2)$ and $c \in \mathbb{Z}$, let

$$S_{n;k_1,k_2,\ldots,k_t}(c) := \left\{ (x_1, x_2, \ldots, x_t) \;\middle|\; \begin{array}{l} 1 \leq x_i \leq n/k_i, (x_i, n/k_i) = 1,\ i = 1, 2, \ldots, t, \\ \sum_{i=1}^{t} k_i x_i \equiv c \pmod{n} \end{array} \right\}.$$

We define $N_{n;k_1,k_2,\ldots,k_t}(c) := \sharp S_{n;k_1,k_2,\ldots,k_t}(c)$.

In 2013, Sander and Sander [3] gave a formula for $N_{n;k_1,k_2}(c)$. In 2014, Sun and Yang [4] obtained a formula for $N_{n;k_1,k_2,\ldots,k_t}(c)$. In 2015, Yang and Tang [5] extended Sander's results to the quadratic case. In 2017, Ji and Zhang [6] extended Sander's results to the residue ring of a Dedekind ring.

In this paper, we shall extend the above results to the ring of matrices over $\mathbb{Z}/m\mathbb{Z}$. Let $M_{n,m} := Mat_n(\mathbb{Z}/m\mathbb{Z})$, $G_{n,m} := Gl_n(\mathbb{Z}/m\mathbb{Z}) = M_{n,m}^*$. For any matrix $A \in M_{n,m}$, we define

$$S_{n,m,k}(A) := \left\{(x_1, x_2, \ldots, x_k) \in G_{n,m}^k \,\middle|\, \sum_{i=1}^{k} x_i = A\right\},$$

and

$$N_{n,m,k}(A) := \sharp S_{n,m,k}(A).$$

We also define

$$M_{n,m,r} = \left\{A \in M_{n,m} \,\middle|\, \mathrm{rank}(A) = r\right\}, \quad r = 0, 1, \ldots, n.$$

Clearly, $M_{n,m,0} = \{O\}$, $M_{n,p,n} = G_{n,p}$ where p is a prime.

By Lemmas 2.1 and 2.2, it is sufficient to compute $N_{n,p,k}(A)$, where p is a prime . Let $A = (g_{ij})_{n\times n} \in M_{n,p}$ and $l \in \{1, 2, \ldots, n\}$. Define

$$t_l(A) := \sum_{i=1}^{l} g_{ii},$$

$$c_{n,p,r}(l) := \frac{\sharp\left\{A \in M_{n,p,r} \middle| t_l(A) = 0\right\} - \sharp\left\{A \in M_{n,p,r} \middle| t_l(A) = 1\right\}}{\sharp M_{n,p,r}}.$$

In this paper, our main results are the followings:

Theorem 1.1. *Let p be a prime. For any $B, C \in M_{2,p}$ with $rank(B) = 1$, $rank(C) = 2$, set*

$$\alpha_k := N_{2,p,k}(O),\ \beta_k := N_{2,p,k}(B),\ \gamma_k := N_{2,p,k}(C), \quad k \geq 2.$$

Let

$$T = \begin{bmatrix} p & 0 & 0 \\ 0 & (p-1)^2p(p+1) & 0 \\ 0 & 0 & -p(p-1) \end{bmatrix},\ S = \begin{bmatrix} (p-1)^2(p+1) & 1 & (p+1)^2(p-1) \\ 1-p & 1 & p^2-p-1 \\ 1 & 1 & -p-1 \end{bmatrix}.$$

Then we have

$$\alpha_2 = (p-1)^2p(p+1),\ \beta_2 = (p^2-p-1)(p-1)p,\ \gamma_2 = p^4 - 2p^3 - p^2 + 3p,$$

and

$$(\alpha_k, \beta_k, \gamma_k)^t = S T^{k-2} S^{-1} (\alpha_2, \beta_2, \gamma_2)^t, \quad k \geq 2.$$

Theorem 1.2. *Let p be a prime. For any $A \in M_{n,p}$ with $rank(A) = r$, we have*

$$N_{n,p,k}(A) = \frac{(\sharp G_{n,p})^k}{\sharp M_{n,p}} \sum_{l=0}^{n} \sharp M_{n,p,l} \cdot c_{n,p,n}(l)^k c_{n,p,l}(r).$$

This paper is organized as follows: In Section 2, we shall prove some lemmas that will be used in the proofs of our main results. In Sections 3 and 4, we shall give the proofs of Theorems 1.1 and 1.2, respectively.

2. Preliminaries

Lemma 2.1. *Let $m \in \mathbb{N}^*$ and $m \geq 2$ with $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where $p_1, p_2, \ldots, p_t$ are different primes, $e_j \geq 1$, $j = 1, 2, \ldots, t$. For any $A \in M_{n,m}$, let $A_j \in M_{n,p_j^{e_j}}$ be the reduction of A module $p_j^{e_j}$, $j = 1, 2, ..., t$. Then we have*

$$N_{n,m,k}(A) = \prod_{j=1}^{t} N_{n,p_j^{e_j},k}(A_j).$$

Proof. Let $(B_1, B_2, \ldots, B_k) \in S_{n,m,k}(A)$. Then $B_{ij} \in G_{n,p_j^{e_j}}$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, t$, where B_{ij} is the reduction of B_i module $p_j^{e_j}$. It is clear that $(B_{1j}, B_{2j}, \ldots, B_{kj}) \in S_{n,p_j^{e_j},k}(A_j)$, $j = 1, 2, \ldots, t$. Conversely, let $(B_{1j}, B_{2j}, \ldots, B_{kj}) \in S_{n,p_j^{e_j},k}(A_j)$, $j = 1, 2, \ldots, t$. By the Chinese remainder theorem, the reduction induces two isomorphisms:

$$M_{n,m} \cong \bigoplus_{j=1}^{t} M_{n,p_j^{e_j}}, \quad G_{n,m} \cong \bigoplus_{j=1}^{t} G_{n,p_i^{j_i}},$$

So there is a unique $B_i \in G_{n,m}$ such that B_{ij} are the reduction of B_i module $p_j^{e_j}$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, t$. We have

$$\sum_{i=1}^{k} B_k = A,$$

i.e., $(B_1, B_2, \ldots, B_k) \in S_{n,m,k}(A)$. □

For any prime p and $e \geq 2$, the next lemma shows the relation between $N_{n,p^e,k}(A)$ and $N_{n,p,k}(A)$.

Lemma 2.2. *Let p be a prime and $e \geq 2$. For any $A \in G_{n,p^e}$, let $\widetilde{A} \in M_{n,p}$ be the reduction of A module p. Then we have*

$$N_{n,p^e,k}(A) = p^{(e-1)\cdot n^2 \cdot (k-1)} N_{n,p,k}(\widetilde{A}).$$

Proof. Let $(B_1, B_2, \ldots, B_k) \in S_{n,p^e,k}(A)$. Then $\widetilde{B_i} \in G_{n,p}$, where $\widetilde{B_i}$ are the reduction of B_i module p, $i = 1, 2, \ldots, k$. It is clear that $(\widetilde{B}_1, \widetilde{B}_2, \ldots, \widetilde{B}_k) \in S_{n,p,k}(\widetilde{A})$. Conversely, let $\widetilde{B} = (b_{st})_{n\times n} \in G_{n,p}$ with $b_{st} \in \{0, 1, \ldots, p-1\}$, then B is a lift of $\widetilde{B}$ in G_{n,p^e} if and only if B is of the form as

$$(k_{st}p + b_{st})_{n\times n}, \quad 0 \leq k_{st} \leq p^{e-1} - 1, \ s, t = 1, 2, \ldots, n.$$

So the number of lifts of $\widetilde{B}$ in G_{n,p^e} is $p^{(e-1)\cdot n^2}$. So if we choose

$$(\widetilde{B}_1, \widetilde{B}_2, \ldots, \widetilde{B}_k) \in S_{n,p,k}(\widetilde{A}),$$

fix an lift $(B_1, B_2, \ldots, B_{k-1})$ of $(\widetilde{B}_1, \widetilde{B}_2, \ldots, \widetilde{B}_{k-1})$, there is only one lift B_k of $\widetilde{B}_k$ such that

$$\sum_{i=1}^{k} B_i = A.$$

So we have

$$N_{n,p^e,k}(A) = p^{(e-1)\cdot n^2\cdot(k-1)} N_{n,p,k}(\widetilde{A}).$$

□

Next, we start to consider the case $m = p$, where p is a prime .

Lemma 2.3. *Let $A, B \in M_{n,p}$ with rank(A) = rank(B). Then we have*

$$N_{n,p,k}(A) = N_{n,p,k}(B).$$

Proof. By assumption, there exist $C, D \in G_{n,p}$ such that $CAD = B$. It is obvious that the map

$$S_{n,p,k}(A) \to S_{n,p,k}(B),\ (x_1, x_2, \ldots, x_k) \mapsto (Cx_1D, Cx_2D, \ldots, Cx_kD)$$

is bijective. Hence $N_{n,p,k}(A) = N_{n,p,k}(B)$. □

It is well known that we have the following results.

Lemma 2.4. [7] *For any $1 \le r < n$, we have*

$$\sharp G_{n,p} = \prod_{i=0}^{n-1}(p^n - p^i),\ \sharp M_{n,p,r} = \prod_{i=0}^{r-1} \frac{(p^n - p^i)^2}{p^r - p^i}.$$

Next we consider the case $n = 2, k = 2$.

Theorem 2.5. *Let p be a prime and $A \in M_{2,p}$. Then we have*

$$N_{2,p,2}(A) = \begin{cases} (p-1)^2 p(p+1), & \text{if } rank(A) = 0, \\ (p^2 - p - 1)(p-1)p, & \text{if } rank(A) = 1, \\ p^4 - 2p^3 - p^2 + 3p, & \text{if } rank(A) = 2. \end{cases}$$

Proof. **Case 1.** rank$(A) = 0$, i.e., $A = O$. For any $x_1 \in G_{2,p}$, $O - x_1 = -x_1 \in G_{2,p}$. Hence we have

$$N_{2,p,2}(A) = \sharp G_{2,p} = (p-1)^2 p(p+1).$$

Case 2. rank$(A) = 1$. By Lemma 2.3, it is sufficient to compute $N_{2,p,2}(A)$, where $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. To compute $N_{2,p,2}(A)$, we only need to compute the number of $x_1 \in G_{2,p}$ such that $A - x_1$ is not in $G_{2,p}$, i.e., rank$(A - x_1) = 1$. Assume

$$x_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad a, b, c, d \in \mathbb{Z}/p\mathbb{Z}.$$

then

$$A - x_1 = \begin{bmatrix} 1-a & -b \\ -c & -d \end{bmatrix}.$$

For $x_1 \in G_{2,p}$, we have $(-c, -d) \neq (0, 0)$. Then there exists $k \in \mathbb{Z}/p\mathbb{Z}$ such that

$$A - x_1 = \begin{bmatrix} -kc & -kd \\ -c & -d \end{bmatrix}, x_1 = \begin{bmatrix} kc+1 & kd \\ c & d \end{bmatrix}.$$

We have

$$\det(x_1) = (kc + 1)d - kcd = d \neq 0.$$

For x_1 to be uniquely determined by k, c, d, then the number of such x_1 is $p^2(p-1)$. So

$$N_{2,p,2}(A) = \sharp G_{2,p} - p^2(p-1) = (p^2 - p - 1)(p-1)p.$$

Case 3. rank$(A) = 2$. We know that

$$\begin{aligned}\sharp M_{2,p,1} =& \sharp M_{2,p} - \sharp M_{2,p,0} - \sharp M_{2,p,2} \\ =& p^4 - 1 - (p-1)^2 p(p+1) \\ =& (p+1)^2(p-1).\end{aligned}$$

Choose $B \in M_{2,p,0}$, $C \in M_{2,p,1}$, then we have

$$\begin{aligned}\sharp G_{2,p}^2 =& \sum_{x \in M_{2,p}} N_{2,p,2}(x) \\ =& \sharp M_{2,p,0} \cdot N_{2,p,2}(B) + \sharp M_{2,p,1} \cdot N_{2,p,2}(C) + \sharp M_{2,p,2} \cdot N_{2,p,2}(A) \\ =& (p-1)^2 p(p+1) + (p+1)^2(p-1) \cdot (p^2 - p - 1)(p-1)p \\ & + (p-1)^2 p(p+1) \cdot N_{2,p,2}(A).\end{aligned}$$

So we have

$$\begin{aligned}N_{2,p,2}(A) =& \frac{(p-1)^4 p^2 (p+1)^2 - (p-1)^2 p(p+1) - (p-1)^2 (p+1) \cdot (p^2 - p - 1)(p-1)p}{(p-1)^2 p(p+1)} \\ =& \frac{(p-1)^2 p(p+1) \cdot \left((p-1)^2 p(p+1) - 1 - \left(p^2 - p - 1\right)(p+1)\right)}{(p-1)^2 p(p+1)} \\ =& p^4 - 2p^3 - p^2 + 3p.\end{aligned}$$

□

Next, we introduce the Fourier Transformation. Let H be a finite abelian group, and let $\widehat{H} =: \mathrm{Hom}_H(H, \mathbb{C}^*)$ be the character group of H. Clearly, $H \cong \widehat{H}$. For any function $f : H \to \mathbb{C}$, the function

$$\widehat{f} : \widehat{H} \to \mathbb{C},\ \chi \mapsto \sum_{x \in H} f(x)\overline{\chi(x)}, \quad \forall \chi \in \widehat{H}$$

is called the Fourier Transformation of f. The transformation can be inverted. We have

Lemma 2.6. [8] *Let $\widehat{f}$ be the Fourier Transformation of $f : H \to \mathbb{C}$. Then we have*

$$f = \sum_{\chi \in \widehat{H}} \frac{1}{\sharp H} \widehat{f}(\overline{\chi})\chi.$$

3. Proof of Theorem 1.1

Consider the equation

$$x_1 + x_2 + \cdots + x_{k+1} = A, \quad x_1, x_2, \ldots, x_{k+1} \in G_{2,p},\ A \in M_{2,p}.$$

Case 1. $\mathrm{rank}(A) = 0$, i.e., $A = O$. Fix an x_{k+1}, then $O - x_{k+1} = -x_{k+1} \in G_{2,p}$. So the number α_{k+1} of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = -x_{k+1}, \quad x_1, x_2, \ldots, x_{k+1} \in G_{2,p},$$

is $\sharp G_{2,p} \cdot \gamma_k = (p-1)^2 p(p+1)\gamma_k$.

Case 2. $\mathrm{rank}(A) = 1$. By Theorem 2.5, the number of x_{k+1} such that $A - x_{k+1} \in M_{2,p,2}$ is β_2, the number of x_{k+1} such that $A - x_{k+1} \in M_{2,p,1}$ is $\sharp G_{2,p} - \beta_2$. So we have

$$\begin{aligned}\beta_{k+1} &= (\sharp G_{2,p} - \beta_2)\beta_k + \beta_2\gamma_k \\ &= p^2(p-1)\beta_k + (p^2 - p - 1)(p-1)p\gamma_k\end{aligned}$$

Case 3. $\mathrm{rank}(A) = 2$. Use the same way as Case 2; we have

$$\begin{aligned}\gamma_{k+1} =& \alpha_k + \left(\sharp G_{2,p} - \gamma_2 - 1\right)\beta_k + \gamma_2\gamma_k \\ =& \alpha_k + (p^3 - 2p - 1)\beta_k + (p^4 - 2p^3 - p^2 + 3p)\gamma_k.\end{aligned}$$

Let

$$P = \begin{bmatrix} 0 & 0 & (p-1)^2 p(p+1) \\ 0 & p^2(p-1) & (p^2 - p - 1)(p-1)p \\ 1 & p^3 - 2p - 1 & p^4 - 2p^3 - p^2 + 3p \end{bmatrix}.$$

Then $(\alpha_k, \beta_k, \gamma_k)^t = P(\alpha_{k-1}, \beta_{k-1}, \gamma_{k-1})^t = \cdots = P^{k-2}(\alpha_2, \beta_2, \gamma_2)^t$. The characteristic polynomial of P is

$$\begin{aligned}\det(\lambda E - P) =& \det\begin{bmatrix} \lambda & 0 & -(p-1)^2 p(p+1) \\ 0 & \lambda - p^2(p-1) & -(p^2 - p - 1)(p-1)p \\ -1 & -(p^3 - 2p - 1) & \lambda - (p^4 - 2p^3 - p^2 + 3p) \end{bmatrix} \\ =& \lambda\left(\lambda - p^2(p-1)\right)\left(\lambda - p\left(p^3 - 2p^2 - p + 3\right)\right) \\ & - (p-1)^2 p(p+1)\left(\lambda - p^2(p-1)\right) \\ & - (p^2 - p - 1)(p-1)p(p^2 - p - 1)(p+1)\lambda \\ =& (\lambda - p)\left(\lambda - (p-1)^2 p(p+1)\right)(\lambda + p(p-1)).\end{aligned}$$

Hence, P is similar to

$$T := \begin{bmatrix} p & 0 & 0 \\ 0 & (p-1)^2 p(p+1) & 0 \\ 0 & 0 & -p(p-1) \end{bmatrix}.$$

The eigenvectors of $p, (p-1)^2 p(p+1), -p(p-1)$ are respectively

$$e_1 = \begin{bmatrix} (p-1)^2(p+1) \\ 1-p \\ 1 \end{bmatrix},\ e_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},\ e_3 = \begin{bmatrix} (p+1)^2(p-1) \\ p^2 - p - 1 \\ -p-1 \end{bmatrix}.$$

Define $S := (e_1, e_2, e_3)$. Then we have $P = STS^{-1}$. □

4. Proof of Theorem 1.2

For convenience, let $M := M_{n,p}$, $G := G_{n,p}$, $M_r := M_{n,p,r}$. Let S be a finite set. For any map $f : S \to M$ and $x \in M$, we define

$$P_f(x) := \frac{\sharp f^{-1}(x)}{\sharp S},$$

where $f^{-1}(x)$ is the set of all the inverse images of x. Let $\widehat{M} =: \mathrm{Hom}_M(M, \mathbb{C}^*)$ be the additive character group of M. Then we have

$$\widehat{P_f}(\chi) = \sum_{x \in M} P_f(x)\overline{\chi(x)} = \frac{1}{\sharp S} \sum_{s \in S} \overline{\chi(f(s))},\ \chi \in \widehat{M}.$$

By Lemma 2.6, we have

$$P_f(x) = \frac{1}{\sharp \widehat{M}} \sum_{\chi \in \widehat{M}} \widehat{P_f}(\overline{\chi})\chi(x).$$

Let $\phi : G \to M$ be the inclusion map and

$$\begin{aligned} \varphi : G^k &\to M, \\ (x_1, x_2, \ldots, x_k) &\mapsto x_1 + x_2 + \cdots + x_k. \end{aligned}$$

Clearly,

$$N_{n,p,k}(A) = (\sharp G)^k \cdot P_\varphi(A), \quad \forall\ A \in M. \tag{4.1}$$

For all $\chi \in \widehat{M}$, we have

$$\begin{aligned} \widehat{P_\varphi}(\chi) =& \frac{1}{(\sharp G)^k} \sum_{(x_1,x_2,\ldots,x_k) \in G^k} \overline{\chi(x_1 + x_2 + \cdots + x_k)} \\ =& \frac{1}{(\sharp G)^k} \sum_{(x_1,x_2,\ldots,x_k) \in G^k} \overline{\chi(x_1)} \cdot \overline{\chi(x_2)} \cdots \overline{\chi(x_k)} \\ =& \left(\frac{1}{(\sharp G)} \sum_{x_1 \in G} \overline{\chi(x_1)} \right)^k \\ =& \widehat{P_\phi}(\chi)^k. \end{aligned}$$

Next, we consider $\widehat{P_\phi}(\chi)$. Let ψ be a nontrivial additive character of $\mathbb{Z}/p\mathbb{Z}$. Then the map

$$\begin{aligned} \langle \_, \_ \rangle : & M \times M \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^*, \\ & (x_1, x_2) \mapsto tr(x_1 x_2) \mapsto \psi(tr(x_1 x_2)) \end{aligned}$$

is a non-degenerated symmetric bilinear map. Hence $\langle \_, \_ \rangle$ induces a group isomorphism:

$$\begin{aligned} \rho : M &\to \widehat{M}, \\ y &\mapsto \chi_y := \langle \_, y \rangle. \end{aligned}$$

So we have

$$\widehat{P}_{\phi}(\overline{\chi_y}) = \frac{1}{\sharp G}\sum_{x\in G}\overline{\chi_y(\overline{x})} = \frac{1}{\sharp G}\sum_{x\in G}\chi_y(x) = \frac{1}{\sharp G}\sum_{x\in G}\langle x, y\rangle .$$

If $\mathrm{rank}(x) = \mathrm{rank}(y)$, i.e., there exits $g_1, g_2 \in G$ such that $x = g_1 y g_2$. By the properties of the trace function, we have

$$\sum_{z\in M_r}\langle z, x\rangle = \sum_{z\in M_r}\langle z, g_1 y g_2\rangle = \sum_{z\in M_r}\langle g_2 z g_1, y\rangle = \sum_{z\in M_r}\langle z, y\rangle . \tag{4.2}$$

Specially, we have

$$\widehat{P}_{\phi}(\overline{\chi_x}) = \widehat{P}_{\phi}(\overline{\chi_y}).$$

Let $l \in \{1, 2, \dots, n\}$. Set $y_l := \begin{bmatrix} I_l & O \\ O & O \end{bmatrix} \in M$ and $\chi_l := \chi_{y_l}$, where I_l is the identity matrix of order l. Then

$$\chi_l(x) = \psi(t_l(x)), \quad for\ all\ x \in M.$$

For any $a \in (\mathbb{Z}/p\mathbb{Z})^*$, it is obvious that

$$\sharp\left\{x \in M_r \,\middle|\, t_l(x) = a\right\} = \sharp\left\{x \in M_r \,\middle|\, t_l(x) = 1\right\}.$$

Note that $\sum_{a\in\mathbb{Z}/p\mathbb{Z}}\psi(a) = 0$, hence we have

$$\begin{aligned}
\frac{1}{\sharp M_r}\sum_{x\in M_r}\langle x, y_l\rangle =& \frac{1}{\sharp M_r}\sum_{x\in M_r}\psi(t_l(x)) \\
=& \frac{1}{\sharp M_r}\sum_{a\in\mathbb{Z}/p\mathbb{Z}}\psi(a)\sum_{x\in M_r,\, t_l(x)=a} 1 \\
=& \frac{1}{\sharp M_r}\sum_{x\in M_r,\, t_l(x)=0} 1 + \frac{1}{\sharp M_r}\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*}\psi(a)\sum_{x\in M_r,\, t_l(x)=a} 1 \\
=& \frac{1}{\sharp M_r}\sum_{x\in M_r,\, t_l(x)=0} 1 - \frac{1}{\sharp M_r}\sum_{x\in M_r,\, t_l(x)=1} 1 \\
=& c_{n,p,r}(l).
\end{aligned}$$

Especially,

$$\widehat{P}_{\phi}(\overline{\chi_l}) = \frac{1}{\sharp G}\sum_{x\in G}\langle x, y_l\rangle = c_{n,p,n}(l). \tag{4.3}$$

As $\mathrm{rank}(A) = r$, by Eqs (4.2) and (4.3), we have

$$\begin{aligned}
P_{\varphi}(A) =& \frac{1}{\sharp M}\sum_{\chi\in\widehat{M}}\widehat{P}_{\varphi}(\overline{\chi})\chi(A) \\
=& \frac{1}{\sharp M}\sum_{l=0}^{n}\sum_{y\in M_l}\widehat{P}_{\phi}(\overline{\chi_l})^k\langle A, y\rangle \\
=& \frac{1}{\sharp M}\sum_{l=0}^{n} c_{n,p,n}(l)^k\sum_{y\in M_l}\langle A, y\rangle
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\sharp M} \sum_{l=0}^{n} c_{n,p,n}(l)^k \sum_{y \in M_l} \langle y, A \rangle \\
&= \frac{1}{\sharp M} \sum_{l=0}^{n} c_{n,p,n}(l)^k \sum_{y \in M_l} \langle y, y_r \rangle \\
&= \frac{1}{\sharp M} \sum_{l=0}^{n} c_{n,p,n}(l)^k \cdot \sharp M_l \cdot c_{n,p,l}(r).
\end{aligned}
$$

Then by Eq (4.1), we have

$$
N_{n,p,k}(A) = \frac{(\sharp G)^k}{\sharp M} \sum_{l=0}^{n} \sharp M_l \cdot c_{n,p,n}(l)^k c_{n,p,l}(r).
$$

□

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The article is supported by NSFC (Nos. 12071209, 12231009). We would like to thank the referees for reading the manuscript carefully and providing valuable comments and suggestions.

Conflict of interest

The authors declare no conflicts of interest.

References

1. M. Deaconescu, Adding units mod n, *Elem. Math.*, **55** (2000), 123–127. https://doi.org/10.1007/s000170050078
2. J. W. Sander, On the addition of units and nonunits (mod m), *J. Number Theory*, **129** (2009), 2260–2266. https://doi.org/10.1016/j.jnt.2009.04.010
3. J. W. Sander, T. Sander, Adding generators in cyclic groups, *J. Number Theory*, **133** (2013), 705–718. https://doi.org/10.1016/j.jnt.2012.08.021
4. C. F. Sun, Q. H. Yang, On the sumset of atoms in cyclic groups, *Int. J. Number Theory*, **10** (2014), 1355–1363. https://doi.org/10.1142/S1793042114500328
5. Q. H. Yang, M. Tang, On the addition of squares of units and nonunits modulo n, *J. Number Theory* **155** (2015), 1–12. https://doi.org/10.1016/j.jnt.2015.02.019
6. X. Zhang, C. G. Ji, Sums of generators of ideals in residue class ring, *J. Number Theory*, **174** (2017), 14–25. https://doi.org/10.1016/j.jnt.2016.10.018

7. G. Landsberg, Ueber eine anzahlbestimmung und eine damit zusammenhängende reihe, *J. Reine Angew. Math.*, **1893** (1893), 87–88. https://doi.org/10.1515/crll.1893.111.87
8. P. Feinsilver, R. Schott, *Algebraic Structures and Operator Calculus: Volume II: Special Functions and Computer Science*, Springer, Dordrecht, 1994. https://doi.org/10.1007/978-0-585-28003-5

AIMS Press

© 2025 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)