Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(9): 24546–24554.
DOI: 10.3934/math.20241195
Received: 27 May 2024
Revised: 28 July 2024
Accepted: 12 August 2024
Published: 21 August 2024

Research article

Counting sums of exceptional units in $\mathbb{Z}_n$

Junyong Zhao[*]

School of Mathematics and Physics, Nanyang Institute of Technology, Nanyang 473004, China

* **Correspondence:** Email: jyzhao_math@163.com.

Abstract: Let R be a commutative ring with the identity 1_R, and let R^* be the multiplicative group of units in R. An element $a \in R^*$ is called an exceptional unit if there exists a $b \in R^*$ such that $a + b = 1_R$. We set R^{**} to be the set of all exceptional units in R. In this paper, we consider the residue-class ring $\mathbb{Z}_n$. For any positive integers n, s, and $c \in \mathbb{Z}_n$, let $\mathcal{N}_s(n, c) := \sharp\{(x_1, ..., x_s) \in (\mathbb{Z}_n^{**})^s : x_1 + ... + x_s \equiv c \pmod{n}\}$. In 2016, Sander (J.Number Theory 159 (2016)) got a formula for $\mathcal{N}_2(n, c)$. Later on, Yang and Zhao (Monatsh. Math. 182 (2017)) extended Sander's theorem to finite terms by using exponential sum theory. In this paper, using matrix theory, we present an explicit formula for $\mathcal{N}_s(n, c)$. This extends and improves earlier results.

Keywords: exceptional unit; circulant matrix; residue class rings; linear congruence; exponential sums
Mathematics Subject Classification: 11B13, 11D45, 15A18

1. Introduction

Let R be a commutative ring with the identity 1_R, and let R^* be the multiplicative group consisting of all the units in R. An element $a \in R^*$ is said to be an *exceptional unit* if $1_R - a \in R^*$, i.e., if $a - 1_R \in R^*$, or, in other words, if there exists a $b \in R^*$ satisfying $a + b = 1_R$. In 1969, exceptional units were first introduced by Nagell [7] to study certain cubic diophantine equations. From then on, many types of diophantine equations have been studied by means of exceptional units, for example, Thue equations [15], Thue-Mahler equations [16] , and discriminant form equations [12].

Exceptional units also became a useful tool in number theory. For example, in 1977, Lenstra [5] introduced a new method to find Euclidean number fields by using exceptional units. Later on, many new Euclidean number fields were found with this method (see [4, 6]). Furthermore, exceptional units also have connections with cyclic resultants [13, 14] and Lehmer's conjecture related to Mahler's measure [10, 11].

Let $\mathbb{Z}$, $\mathbb{Z}^+$, and $\mathbb{P}$ be the sets of integers, positive integers, and primes, respectively. For $n \in \mathbb{Z}^+$, let

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the ring of residue classes modulo n. By definition, one has $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$. In this note, we set $\mathbb{Z}_n^{**}$ to be the set of all exceptional units in $\mathbb{Z}_n$, i.e., $\mathbb{Z}_n^{**} := \{a \in \mathbb{Z}_n : \gcd(a, n) = \gcd(a-1, n) = 1\}$. Given $p \in \mathbb{P}$, we denote by $v_p(n)$ the p-adic valuation of n, i.e., $v_p(n)$ is the unique nonnegative integer r satisfying $p^r | n$ and $p^{r+1} \nmid n$. Moreover, we let ξ_n stand for the primitive n-th root of unity, i.e., $\xi_n := e^{2\pi i/n}$.

In 2010, Harrington and Jones [3] obtained the following identity:

$$\sharp\mathbb{Z}_n^{**} = n \prod_{p|n, p\in\mathbb{P}} (1 - \frac{2}{p}).$$

This result can also be deduced immediately from the theorems of Deaconescu [2] or Sander [8]. By the definition of an exceptional unit, we can see that

$$\sharp\mathbb{Z}_n^{**} = \sharp\Big\{(u, v) \in (\mathbb{Z}_n^*)^2 : u + v \equiv 1 \pmod{n}\Big\}.$$

For $c \in \mathbb{Z}_n$, in 2009, it was proved by Sander [8] that

$$\sharp\Big\{(u, v) \in (\mathbb{Z}_n^*)^2 : u + v \equiv c \pmod{n}\Big\} = n \prod_{\substack{p\in\mathbb{P} \\ p|n, p|c}} (1 - \frac{1}{p}) \prod_{\substack{p\in\mathbb{P} \\ p|n, p\nmid c}} (1 - \frac{2}{p}).$$

In this paper, we shall describe the elements in $\mathbb{Z}_n$, which could be written as the sum of one or more expected units. In addition, for these elements, we will derive the number of representations as such a sum. More specifically, for $n, s \in \mathbb{Z}^+$, and $c \in \mathbb{Z}_n$, we set

$$\mathcal{N}_s(n, c) := \sharp\Big\{(x_1, ..., x_s) \in (\mathbb{Z}_n^{**})^s : x_1 + ... + x_s \equiv c \pmod{n}\Big\}.$$

In 2016, Sander [9] presented an explicit formula for $\mathcal{N}_2(n, c)$. Now, we state Sander's theorem as follows:

Theorem 1.1. (**Sander** *[8]) Given $n, k \in \mathbb{Z}^+$ and $c \in \mathbb{Z}_n$. The number $\mathcal{N}_2(n, c)$ satisfies the following relations:*

$$\mathcal{N}_2(2^k, c) = 0, \quad \mathcal{N}_2(3^k, c) = \begin{cases} 3^{k-1} & \text{if } c \equiv 1 \pmod{3}, \\ 0 & \text{otherwise}, \end{cases}$$

while for all primes $p \geqslant 5$,

$$\mathcal{N}_2(p^k, c) = \begin{cases} p^{k-1}(p-2) & \text{if } c \equiv 1 \pmod{p}, \\ p^{k-1}(p-3) & \text{if } c \equiv 0 \pmod{p} \text{ or } c \equiv 2 \pmod{p}, \\ p^{k-1}(p-4) & \text{otherwise}. \end{cases}$$

Let $\omega(n) := \sum_{p|n, p\in\mathbb{P}} 1$ be the number of distinct prime divisors of n. In 2017, Yang and Zhao [17] extended Sander's theorem to finite terms by means of exponential sums, as below.

Theorem 1.2. (**Yang and Zhao** *[17]) For $n, s \in \mathbb{Z}_{\geqslant 2}^+$ and $c \in \mathbb{Z}_n$, we have*

$$\mathcal{N}_s(n, c) = (-1)^{s\omega(n)} \prod_{p|n, p\in\mathbb{P}} p^{v_p(n)(s-1)-s} \Bigg(p \sum_{\substack{j=0 \\ j\equiv c \pmod{p}}}^{s} \binom{s}{j} + (2-p)^s - 2^s\Bigg).$$

In this paper, by using matrix theory, we give the following two results:

Theorem 1.3. *Let $p \in \mathbb{P}$, $s \in \mathbb{Z}^+$, and let $\xi_j := e^{2\pi i/j}$. Then*

$$\begin{pmatrix} \mathcal{N}_s(p,0) \\ \mathcal{N}_s(p,1) \\ \vdots \\ \mathcal{N}_s(p,p-1) \end{pmatrix} = \frac{1}{p} \begin{pmatrix} (p-2)^s + \sum\limits_{j=1}^{p-1}(-1-\xi_j^{-1})^s \\ (p-2)^s + \sum\limits_{j=1}^{p-1}\xi_j(-1-\xi_j^{-1})^s \\ \vdots \\ (p-2)^s + \sum\limits_{j=1}^{p-1}\xi_j^{(p-1)}(-1-\xi_j^{-1})^s \end{pmatrix}.$$

The second main result of this paper is the following corollary:

Corollary 1.1. *Let $n, s \in \mathbb{Z}^+_{\geqslant 2}$ and $c \in \mathbb{Z}_n$. We have*

$$\mathcal{N}_s(n,c) = \prod_{p|n, p\in\mathbb{P}} p^{(v_p(n)-1)(s-1)}\mathcal{N}_s(p,c),$$

where $\mathcal{N}_s(p,c)$ is determined by Theorem 1.3.

This paper is organized as follows: Section 2 provides several lemmas that are needed in the proof of Theorem 1.3 and Corollary 1.1. Then we give the proofs of Theorem 1.3 and Corollary 1.1 in Section 3.

2. Preliminary lemmas

In this section, we supply several lemmas that will be needed in the proof of Theorem 1.3 and Corollary 1.1. We begin with the following result, which can be proved by using the Chinese remainder theorem:

Lemma 2.1. *[1] Let $k, s \in \mathbb{Z}^+$, $f(x_1, ..., x_s) \in \mathbb{Z}[x_1, ..., x_s]$, and let $m_1, ..., m_k$ be pairwise relatively prime positive integers. For any integer j with $1 \leq j \leq k$, let N_j be the number of zeros of $f(x_1, ..., x_s) \equiv 0 \pmod{m_j}$, and let N denote the number of zeros of $f(x_1, ..., x_s) \equiv 0 \pmod{\prod_{j=1}^k m_j}$. Then $N = \prod_{j=1}^k N_j$.*

Lemma 2.2. *Let $k \in \mathbb{Z}^+, p \in \mathbb{P}$. For any integer c, we have $\mathcal{N}_s(p^{k+1}, c) = p^{s-1}\mathcal{N}_s(p^k, c)$.*

Proof. Let $(b_1, \cdots, b_s)$ be a solution of $x_1 + \cdots + x_s \equiv c \pmod{p^k}$, with b_j $(1 \leq j \leq s)$ being exceptional units. One has $\gcd(b_j, p) = 1$. Let $b_1 + \cdots + b_s - c = ap^k$ for some $a \in \mathbb{Z}$. For $k_1, \cdots, k_s \in \mathbb{Z}_{p^k}$, the congruence

$$(b_1 + k_1 p^k) + \cdots + (b_s + k_s p^k) \equiv c \pmod{p^{k+1}}$$

holds if and only if

$$a + k_1 + \cdots + k_s \equiv 0 \pmod{p}. \tag{2.1}$$

Clearly, the number of solutions to (2.1) is p^{s-1}.

Thus, one get $\mathcal{N}_s(p^{k+1}, c) = p^{s-1}\mathcal{N}_s(p^k, c)$. □

In this paper, we view vector v as a column vector and v^T as the transpose of v. For $a \in \mathbb{Z}$, we let $< a >_m$ denote the unique integer r such that $r \equiv a \pmod{m}$ with $0 \leqslant r \leqslant m-1$.

Definition 2.1. Let $v = (a_0, \cdots, a_{m-1})^T$ be a complex vector. The circulant matrix A_v associated with v is a $m \times m$ complex matrix having the form

$$A_v = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & \cdots & a_{m-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

In other words, if we let $A_v = (A_{i,j})$, then $A_{i,j} = a_{<j-i>_m}$.

Lemma 2.3. *Let A_v be a circulant matrix associated to the vector $v = (a_0, \cdots, a_{m-1})^T$,and let $f(x) = \sum_{i=0}^{m-1} a_i x^i$. Then, for each $j = 0, 1, \cdots, m-1$, $f(\xi_m^j)$ is an eigenvalue of A_v and $v_j = (1, \xi_m^j, \xi_m^{2j}, \cdots, \xi_m^{j(m-1)})^T$ is an eigenvector corresponding to $f(\xi_m^j)$.*

Proof. Let ω be any m-th root of unity. Set

$$\alpha = \begin{pmatrix} 1 \\ \omega \\ \vdots \\ \omega^{m-1} \end{pmatrix}.$$

Consider

$$A_v\alpha = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & \cdots & a_{m-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \vdots \\ \omega^{m-1} \end{pmatrix} := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Clearly,

$$b_1 = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{m-2}\omega^{m-2} + a_{m-1}\omega^{m-1} = f(\omega).$$

For any $k \geq 2$, one has

$$\begin{aligned} b_k =& a_{m-k+1} + a_{m-k+2}\omega + \cdots + a_{m-1}\omega^{k-2} + a_0\omega^{k-1} + a_1\omega^{k-2} + \cdots + a_{m-k}\omega^{m-1} \\ =& (a_{m-k+1}\omega^{m-k+1} + a_{m-k+2}\omega^{m-k+2} + \cdots + a_{m-k}\omega^{m-k})\omega^{k-1} \\ =& f(\omega)\omega^{k-1}. \end{aligned}$$

Therefore, we obtain that

$$A_v\alpha = \begin{pmatrix} f(\omega) \\ f(\omega)\omega \\ \vdots \\ f(\omega)\omega^{m-1} \end{pmatrix} = f(\omega)\alpha.$$

In particular, take $\omega = \xi_m^j$, where j runs from 0 to $m-1$. It then follows that $f(\xi_m^j)$ is an eigenvalue and

$$\begin{pmatrix} 1 \\ \xi_m^j \\ \vdots \\ \xi_m^{j(m-1)} \end{pmatrix}$$

is an eigenvector corresponding to $f(\xi_m^j)$ for each $j = 0, 1, \cdots, m-1$.

This completes the proof of Lemma 2.3. □

Lemma 2.4. *Let k be a nonnegative integer and m be a positive integer. Then*

$$\sum_{j=0}^{m-1} \xi_m^{kj} = \begin{cases} m, & \text{if } m \mid k, \\ 0, & \text{if } m \nmid k. \end{cases}$$

Proof. First, if $m \mid k$, then $\xi_m^{kj} = 1$ for any integer j. So

$$\sum_{j=0}^{m-1} \xi_m^{kj} = \sum_{j=0}^{m-1} 1 = m.$$

Next, we let $m \nmid k$. Then $k = qm + r$ for $0 < r < m$. Then one has

$$\xi_m^k = \xi_m^{qm+r} = (\xi_m^m)^q \xi_m^r = \xi_m^r \neq 1.$$

It follows that

$$\sum_{j=0}^{m-1} \xi_m^{kj} = \sum_{j=0}^{m-1} \xi_m^{rj} = \frac{\xi_m^{mr} - 1}{\xi_m^r - 1} = \frac{1-1}{\xi_m^r - 1} = 0.$$

The proof of Lemma 2.4 is complete. □

We also need the following result, which can be found in any standard linear algebra textbook.

Lemma 2.5. *Let A be a $m \times m$ matrix. Let $\lambda_1, \lambda_2, \cdots, \lambda_m$ be all the eigenvalues of A, and α_j be an eigenvector corresponding to λ_j for every $1 \leqslant j \leqslant m$. If $\alpha_1, \alpha_2, \cdots, \alpha_m$ are linearly independent, then $Q^{-1}AQ = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_m)$ with $Q = (\alpha_1, \alpha_2, \cdots, \alpha_m)$.*

Lemma 2.6. *Let V be a Vandermonde matrix of the form*

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_m & \xi_m^2 & \cdots & \xi_m^{m-1} \\ 1 & \xi_m^2 & \xi_m^4 & \cdots & \xi_m^{2(m-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi_m^{m-1} & \xi_m^{2(m-1)} & \cdots & \xi_m^{(m-1)(m-1)} \end{pmatrix}.$$

Then V is invertible, and

$$V^{-1} = \frac{1}{m} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_m^{m-1} & \xi_m^{2(m-1)} & \cdots & \xi_m^{(m-1)(m-1)} \\ 1 & \xi_m^{m-2} & \xi_m^{2(m-2)} & \cdots & \xi_m^{(m-2)(m-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi_m & \xi_m^2 & \cdots & \xi_m^{m-1} \end{pmatrix}.$$

Proof. The proof follows from a direct calculation. □

3. Proof of Theorem 1.3 and Corollary 1.1

Proof of Theorem 1.3. Let $(x_1, ..., x_s) \in (\mathbb{Z}_n^{**})^s$. It then follows that $x_s \neq 0$ and $x_s \neq 1$. Since

$$\mathcal{N}_s(n, c) := \sharp\Big\{(x_1, ..., x_s) \in (\mathbb{Z}_n^{**})^s : x_1 + ... + x_s \equiv c \pmod{n}\Big\},$$

it is easy to see that for any integer i with $0 \leq k \leq p-1$, one has

$$\mathcal{N}_s(p, k) = \sum_{\substack{j=0 \\ j\neq k, <k-1>_p}}^{p-1} \mathcal{N}_{s-1}(p, j).$$

That is,

$$\begin{pmatrix} \mathcal{N}_s(p,0) \\ \mathcal{N}_s(p,1) \\ \vdots \\ \mathcal{N}_s(p,p-1) \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} \mathcal{N}_{s-1}(p,0) \\ \mathcal{N}_{s-1}(p,1) \\ \vdots \\ \mathcal{N}_{s-1}(p,p-1) \end{pmatrix}$$

$$:= A_v \begin{pmatrix} \mathcal{N}_{s-1}(p,0) \\ \mathcal{N}_{s-1}(p,1) \\ \vdots \\ \mathcal{N}_{s-1}(p,p-1) \end{pmatrix}.$$

It is clear that A_v is a circulant matrix associated with the vector $v = (0, 1, \cdots, 1, 0)^T$. For simplicity, we set $\xi := \xi_p$ in the following. Then $\xi_1 := \xi$, $\xi_2 = \xi^2, \cdots, \xi_{p-1} = \xi^{p-1}$ are all the primitive p-th roots of unity. Let $f(x) = x + x^2 + \cdots + x^{p-2}$. By Lemma 2.3, for each $j = 0, 1, \cdots, p-1$, $f(\xi^j)$ is an eigenvalue of A_v and $v_j = (1, \xi_1^j, \xi_2^j, \cdots, \xi_{p-1}^j)^T$ is an eigenvector corresponding to the eigenvalue $f(\xi^j)$.

Let

$$B = (v_0, v_1, \cdots, v_{p-1}) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_1 & \xi_1^2 & \cdots & \xi_1^{p-1} \\ 1 & \xi_2 & \xi_2^2 & \cdots & \xi_2^{p-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi_{p-1} & \xi_{p-1}^2 & \cdots & \xi_{p-1}^{p-1} \end{pmatrix}.$$

Since $\det(B) = \prod_{0\leqslant i<j\leqslant p-1} (\xi_j - \xi_i) \neq 0$, one has $v_0, v_1, \cdots, v_{p-1}$ are linearly independent. By Lemmas 2.5 and 2.6, we have

$$B^{-1} = \frac{1}{p} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_1^{p-1} & \xi_2^{p-1} & \cdots & \xi_{p-1}^{p-1} \\ 1 & \xi_1^{p-2} & \xi_2^{p-2} & \cdots & \xi_{p-1}^{p-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi_1 & \xi_2 & \cdots & \xi_{p-1} \end{pmatrix}$$

and

$$A_v = B\,\mathrm{diag}(f(\xi^0), f(\xi^1), \cdots, f(\xi^{p-1}))\,B^{-1}.$$

Notice that $\mathcal{N}_1(p,0) = \mathcal{N}_1(p,1) = 0$, $\mathcal{N}_1(p,j) = 1$ for $2 \leqslant j \leqslant p-1$, and for $1 \leqslant j \leqslant p-1$,

$$f(\xi^j) = -1 - \xi^{-j}$$

by Lemma 2.4. Therefore, one has

$$\begin{pmatrix} \mathcal{N}_s(p,0) \\ \mathcal{N}_s(p,1) \\ \vdots \\ \mathcal{N}_s(p,p-1) \end{pmatrix} = B\,\mathrm{diag}\Big(f(\xi^0), f(\xi^1), \cdots, f(\xi^{p-1})\Big)\,B^{-1} \begin{pmatrix} \mathcal{N}_{s-1}(p,0) \\ \mathcal{N}_{s-1}(p,1) \\ \vdots \\ \mathcal{N}_{s-1}(p,p-1) \end{pmatrix}$$

$$= B\,\mathrm{diag}\Big(f^{s-1}(\xi^0), f^{s-1}(\xi^1), \cdots, f^{s-1}(\xi^{p-1})\Big)\,B^{-1} \begin{pmatrix} \mathcal{N}_1(p,0) \\ \mathcal{N}_1(p,1) \\ \vdots \\ \mathcal{N}_1(p,p-1) \end{pmatrix}$$

$$= B\,\mathrm{diag}\Big((p-2)^{s-1}, (-1-\xi^{-1})^{s-1}, \cdots, (-1-\xi^{-p+1})^{s-1}\Big)\,B^{-1} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$= B\,\mathrm{diag}\Big((p-2)^{s-1}, (-1-\xi_1^{-1})^{s-1}, \cdots, (-1-\xi_{p-1}^{-1})^{s-1}\Big)\,B^{-1} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} (p-2)^{s-1} & (-1-\xi_1^{-1})^{s-1} & \cdots & (-1-\xi_{p-1}^{-1})^{s-1} \\ (p-2)^{s-1} & \xi_1(-1-\xi_1^{-1})^{s-1} & \cdots & \xi_{p-1}(-1-\xi_{p-1}^{-1})^{s-1} \\ \vdots & \vdots & & \vdots \\ (p-2)^{s-1} & \xi_1^{p-1}(-1-\xi_1^{-1})^{s-1} & \cdots & \xi_{p-1}^{p-1}(-1-\xi_{p-1}^{-1})^{s-1} \end{pmatrix} B^{-1} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$= \frac{1}{p} \begin{pmatrix} (p-2)^{s-1} & (-1-\xi_1^{-1})^{s-1} & \cdots & (-1-\xi_{p-1}^{-1})^{s-1} \\ (p-2)^{s-1} & \xi_1(-1-\xi_1^{-1})^{s-1} & \cdots & \xi_{p-1}(-1-\xi_{p-1}^{-1})^{s-1} \\ \vdots & \vdots & & \vdots \\ (p-2)^{s-1} & \xi_1^{p-1}(-1-\xi_1^{-1})^{s-1} & \cdots & \xi_{p-1}^{p-1}(-1-\xi_{p-1}^{-1})^{s-1} \end{pmatrix} \begin{pmatrix} p-2 \\ -1-\xi_1^{p-1} \\ \vdots \\ -1-\xi_1 \end{pmatrix}$$

$$= \frac{1}{p} \begin{pmatrix} (p-2)^{s-1} & (-1-\xi_1^{-1})^{s-1} & \cdots & (-1-\xi_{p-1}^{-1})^{s-1} \\ (p-2)^{s-1} & \xi_1(-1-\xi_1^{-1})^{s-1} & \cdots & \xi_{p-1}(-1-\xi_{p-1}^{-1})^{s-1} \\ \vdots & \vdots & & \vdots \\ (p-2)^{s-1} & \xi_1^{p-1}(-1-\xi_1^{-1})^{s-1} & \cdots & \xi_{p-1}^{p-1}(-1-\xi_{p-1}^{-1})^{s-1} \end{pmatrix} \begin{pmatrix} p-2 \\ -1-\xi_1^{-1} \\ \vdots \\ -1-\xi_{p-1}^{-1} \end{pmatrix}$$

$$= \frac{1}{p}\begin{pmatrix} (p-2)^s + \sum\limits_{j=1}^{p-1}(-1-\xi_j^{-1})^s \\ (p-2)^s + \sum\limits_{j=1}^{p-1}\xi_j(-1-\xi_j^{-1})^s \\ \vdots \\ (p-2)^s + \sum\limits_{j=1}^{p-1}\xi_j^{(p-1)}(-1-\xi_j^{-1})^s \end{pmatrix}.$$

This completes the proof of Theorem 1.3.

Proof of Corollary 1.1. Let $n = \prod\limits_{p|n} p^{v_p(n)}$ be the canonical decomposition of n. By Lemmas 2.1 and 2.2, we get

$$\mathcal{N}_s(n,c) = \prod_{p|n}\mathcal{N}_s(p^{v_p(n)},c) = \prod_{p|n} p^{(v_p(n)-1)(s-1)}\mathcal{N}_s(p,c).$$

This finishes the proof of Corollary 1.1.

4. Conclusions

In the current study, by means of matrix theory, we present an explicit expression for $\sharp\Big\{(x_1,...,x_s)\in(\mathbb{Z}_n^{**})^s : x_1^k+...+x_s^k \equiv c \pmod n\Big\}$ with $k=1$. Naturally, one will ask for the formula for $\sharp\Big\{(x_1,...,x_s)\in(\mathbb{Z}_n^{**})^s : x_1^k+...+x_s^k \equiv c \pmod n\Big\}$ with $k>1$. Moreover, exceptional units are interesting and deserve further research.

Use of AI tools declaration

The author declares he has not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The author woulds like to thank the anonymous referees for their careful reading of the manuscript and helpful suggestions that improve the presentation of the paper.

Conflict of interest

The author declares that he have no conflict of interest.

References

1. T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976.
2. M. Deaconescu, Adding units mod *n*, *Elem. Math.*, **55** (2000), 123–127. https://doi.org/10.1007/s000170050078

3. J. Harrington, L. Jones, On the iteration of a function related to Euler's φ-function, *Integers*, **10** (2010), 497–515.

4. J. Houriet, Exceptional units and Euclidean number fields, *Arch. Math.*, **88** (2007), 425–433. https://doi.org/10.1007/s00013-006-1019-0

5. H. W. Lenstra, Euclidean number fields of large degree, *Invent. Math.*, **38**, (1976/1977), 237–254. https://doi.org/10.1007/BF01403131

6. A. Leutbecher, G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, In: H.P. Schlickewei, E. Wirsing (eds.), Number Theory, Springer, 1989, 150–178. https://doi.org/10.1007/BFb0086541

7. T. Nagell, Sur un type particulier d'unites algebriques, *Ark. Mat.*, **8** (1969), 163–184. https://doi.org/10.1007/BF02589556

8. 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

9. J. W. Sander, Sums of exceptional units in residue class rings, *J. Number Theory*, **159** (2016), 1–6. https://doi.org/10.1016/j.jnt.2015.07.018

10. J. H. Silverman, Exceptional units and numbers of small Mahler measure, *Exp. Math.*, **4** (1995), 69–83. https://doi.org/10.1080/10586458.1995.10504309

11. J. H. Silverman, Small Salem numbers, exceptional units, and Lehmer's conjecture, *Rocky Mt. J. Math.*, **26** (1996), 1099–1114.

12. N. P. Smart, Solving discriminant form equations via unit equations, *J. Symbolic Comput.*, **21** (1996), 367–374. https://doi.org/10.1006/jsco.1996.0018

13. C. L. Stewart, Exceptional units and cyclic resultants, *Acta Arith.*, **155** (2012), 407–418. https://doi.org/10.4064/aa155-4-5

14. C. L. Stewart, Exceptional units and cyclic resultants, *Contemp. Math.*, **587** (2013), 191–200.

15. N. Tzanakis, B. M. M. deWeger, On the practical solution of the Thue equation, *J. Number Theory*, **31** (1989), 99–132. https://doi.org/10.1016/0022-314X(89)90014-0

16. N. Tzanakis, B. M. M. deWeger, How to explicitly solve a Thue-Mahler equation, *Compos. Math.*, **84** (1992), 223–288.

17. Q. H. Yang, Q. Q. Zhao, On the sumsets of exceptional units in $\mathbb{Z}_n$, *Monatsh. Math.*, **182** (2017), 489–493. https://doi.org/10.1007/s00605-015-0872-y