sciendo

uniform distribution theory

DOI: 10.2478/udt-2019–0008
Unif. Distrib. Theory **14** (2019), no.1, 123–140

# CYCLOTOMIC EXPRESSIONS FOR REPRESENTATION FUNCTIONS

Charles Helou

Pennsylvania State University, Media, PA, USA

ABSTRACT. Given a subset $A$ of the natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ (resp. of the ring $\mathbb{Z}/N\mathbb{Z}$ of residue classes modulo a positive integer $N$), we introduce certain sums of roots of unity associated with $A$. We study some of their properties, and we use them to obtain new expressions for the classical functions that characterize $A$, i.e. of the representation function, the counting function and the characteristic function of $A$. We also give an example of computations of the representation function using such expressions.

*Communicated by Werner Georg Nowak*

## 1. Introduction

Let $A$ denote a subset of the semi-group $\mathbb{N} = \{0, 1, 2, \ldots\}$ of natural numbers (resp. of the quotient ring $\mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \ldots, N-1\}$, whose elements are identified to their minimal non-negative residues modulo $N$, where $N$ is a positive integer). For every $n \in \mathbb{N}$, let $A_n = A \cap [0, n]$ be the set of all elements $a \leq n$ in $A$. The counting function of $A$ is $A(n) = |A_n|$, the number of elements in $A_n$, while the representation function of $A$ is defined by

$$r_A(n) = |\{(a, b) \in A \times A : a + b = n\}|,$$

and the characteristic function of $A$ is given by $\chi_A(n) = 1$ if $n \in A$, and $\chi_A(n) = 0$ if $n \notin A$. All three functions characterize $A$, with the most important one being $r_A(n)$. Representation functions have been studied extensively [2, 3, 4, 9, 12, 15,



2010 Mathematics Subject Classification: 11B34, 11B75, 11L03, 11R18.
Keywords: Representation function, exponential sums, cyclotomic fields.

16, 17, 18, 19, 20], and many conjectures and open problems about them remain the subject of intensive research [5, 6, 7, 8, 10, 20, 21, 22, 23].

Let $m$ be a positive integer, and $\zeta_m = e^{\frac{2\pi i}{m}}$ be the standard primitive $m$th root of unity in the field $\mathbb{C}$ of complex numbers. We introduce the exponential sums

$$S_k(A, m, n) = \sum_{a \in A_n} \zeta_m^{ka}, \tag{1.1}$$

where $k \in \mathbb{Z}$ is a rational integer, and $n \in \mathbb{N}$ is a natural number. We study some of their properties, and we establish, in their terms, expressions for the three characterizing functions

$$r_A(n), \ A(n) \quad \text{and} \quad \chi_A(n) \ \ of \ \ A.$$

We thus prove that if $m > n$ (resp. $m = N$), then

$$r_A(n) = \frac{1}{m} \sum_{k=0}^{m-1} \zeta_m^{-kn} S_k(A, m, n)^2. \tag{1.2}$$

Moreover, for $A \subset \mathbb{N}$ and for $m > n$, we also have

$$A(n) = \frac{1}{m} \sum_{k=0}^{m-1} |S_k(A, m, n)|^2. \tag{1.3}$$

On the other hand, for any integer $n > 0$,

$$r_A(n) = \frac{1}{n} \sum_{k=0}^{n-1} S_k(A, n, n)^2 - \chi_A(0) - \chi_A(n), \tag{1.4}$$

$$A(n) = \frac{1}{n} \sum_{k=0}^{n-1} |S_k(A, n, n)|^2 - 2\chi_A(0)\chi_A(n), \tag{1.5}$$

and

$$\chi_A(n) = \frac{1}{n} \sum_{k=0}^{n-1} S_k(A, n, n) - \chi_A(0). \tag{1.6}$$

Two further expressions for the representation function are given by

$$r_A(n) = \frac{1}{m} \sum_{d|m} Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}} \left( \zeta_d^{-n} S_1(A, d, n)^2 \right), \tag{1.7}$$

where $m > n$ (resp. $m = N$), and $Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}$ is the trace form in the field extension $\mathbb{Q}(\zeta_d)|\mathbb{Q}$, with $d$ ranging over the set of positive integers dividing $m$ (resp. $N$),

and

$$r_A(n) = \frac{1}{m} \sum_{(a,b)\in A_n\times A_n} \sum_{d\mid m} \mu\left(\frac{d}{(d,a+b-n)}\right) \frac{\varphi(d)}{\varphi\left(\frac{d}{(d,a+b-n)}\right)}, \tag{1.8}$$

where $m > n$ (resp. $m = N$), $\mu$ is the Möbius function, and $\varphi$ is the Euler totient function.

We also give an example of computations with those expressions.

## 2. Orthogonality Relations

The following results concerning character sums are well-known (e.g., [1], Chapter 6).

**Lemma 2.1.** *For any integers $m > 0$ and $x \in \mathbb{Z}$, we have*

$$\sum_{k=0}^{m-1} \zeta_m^{kx} = \begin{cases} m & \text{if } m \mid x, \\ 0 & \text{if } m \nmid x. \end{cases} \tag{2.1}$$

In particular,

**Corollary 2.2.** *For $a, b, n \in \mathbb{N}$, we have*

$$\sum_{k=0}^{m-1} \zeta_m^{k(a+b-n)} = \begin{cases} m & \text{if } a+b \equiv n \pmod m, \\ 0 & \text{if } a+b \not\equiv n \pmod m. \end{cases} \tag{2.2}$$

**Corollary 2.3.** *If $|a+b-n| < m$, and in particular if $a, b \le n < m$, then*

$$\sum_{k=0}^{m-1} \zeta_m^{k(a+b-n)} = \begin{cases} m & \text{if } a+b = n, \\ 0 & \text{if } a+b \ne n. \end{cases} \tag{2.3}$$

*If $|a+b-n| \le m$, then*

$$\sum_{k=0}^{m-1} \zeta_m^{k(a+b-n)} = \begin{cases} m & \text{if } a+b = n, \quad \text{or} \quad a+b = n \pm m, \\ 0, & \text{otherwise.} \end{cases} \tag{2.4}$$

**Corollary 2.4.** *For $a, b, n \in \mathbb{N}$ such that $n > 0$ and $a, b \le n$, we have*

$$\sum_{k=0}^{n-1} \zeta_n^{k(a+b-n)} = \begin{cases} n & \text{if } a+b = n, \text{ or } a = b = 0, \quad \text{or} \quad a = b = n, \\ 0, & \text{otherwise.} \end{cases} \tag{2.5}$$

## 3. Exponential Sums

Let $A \subset \mathbb{N}$ (resp. $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$, where $N$ is a positive integer). For any integers $k \in \mathbb{Z}$, $m, n \in \mathbb{N}$, with $m > 0$, let

$$S_k(A, m, n) = \sum_{a \in A_n} \zeta_m^{ka}. \tag{3.1}$$

**Remark 3.1.** If $m \mid k$, then

$$S_k(A, m, n) = S_0(A, m, n) = \sum_{a \in A_n} 1 = A(n).$$

**Lemma 3.2.** *For any integers $k, k' \in \mathbb{Z}$, $m, n \in \mathbb{N}$, with $m > 0$,*

– *If* $k' \equiv k \pmod m$, *then* $S_{k'}(A, m, n) = S_k(A, m, n)$. (3.2)

– *If* $k' \equiv -k \pmod m$, *then* $S_{k'}(A, m, n) = \overline{S_k(A, m, n)}$, (3.3)

*where $\overline{z}$ is the complex conjugate of $z$ in $\mathbb{C}$.*

Proof. Indeed, in the first case

$$\zeta_m^{k'a} = \zeta_m^{ka},$$

and in the second case,

$$\zeta_m^{k'a} = \zeta_m^{-ka} = \overline{\zeta_m^{ka}},$$

for any $a \in A_n$. The results follow by summation over $a$. □

**Lemma 3.3.** *Let $A' = \mathbb{N} \setminus A$ (resp. $A' = (\mathbb{Z}/N\mathbb{Z}) \setminus A$) be the complement set of $A$ in $\mathbb{N}$ (resp. in $\mathbb{Z}/N\mathbb{Z}$). Then, for any $k \in \mathbb{Z}$ and any $m, n \in \mathbb{N}$, with $m > 0$, we have*

$$S_k(A', m, n) = \begin{cases} \dfrac{1 - \zeta_m^{kM}}{1 - \zeta_m^k} - S_k(A, m, n) & \text{if } m \nmid k, \\ M - A(n) & \text{if } m \mid k, \end{cases} \tag{3.4}$$

*where $M = n + 1$ (resp. $M = N$).*

Proof.

$$\begin{aligned} S_k(A', m, n) &= \sum_{a \in A'_n} \zeta_m^{ka} \\ &= \sum_{a=0}^{M-1} \zeta_m^{ka} - \sum_{a \in A_n} \zeta_m^{ka} = \sum_{a=0}^{M-1} \zeta_m^{ka} - S_k(A, m, n). \end{aligned}$$

If $m \nmid k$, then $\sum_{a=0}^{M-1} \zeta_m^{ka} = \frac{1-\zeta_m^{kM}}{1-\zeta_m^k}$. If $m \mid k$, then $\sum_{a=0}^{M-1} \zeta_m^{ka} = \sum_{a=0}^{M-1} 1 = M$ and $S_k(A, m, n) = A(n)$, by Remark 3.1. The result follows. □

**Lemma 3.4.** *For any two subsets $A, B$ of $\mathbb{N}$ (resp. of $\mathbb{Z}/N\mathbb{Z}$), any $k \in \mathbb{Z}$ and any $m, n \in \mathbb{N}$, with $m > 0$, we have*

$$S_k(A \cup B, m, n) = S_k(A, m, n) + S_k(B, m, n) - S_k(A \cap B, m, n). \tag{3.5}$$

P r o o f. Since $A \cup B$ is the union of the three pairwise disjoint sets

$$A^- = A \setminus (A \cap B),\ B^- = B \setminus (A \cap B) \quad \text{and} \quad (A \cap B),$$

and since

$$A = A^- \cup (A \cap B) \quad \text{and} \quad B = B^- \cup (A \cap B),$$

the result follows by simple summations. □

## 4. Relations with the Characterizing Functions

**Lemma 4.1.** *Let $A \subset \mathbb{N}$ (resp. $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$). For any $k \in \mathbb{Z}$ and $m, n \in \mathbb{N}$, with $m > 0$ (resp. $m = N$), we have*

$$S_k(A, m, n)^2 = \sum_c r_{A_n}(c) \zeta_m^{kc}, \tag{4.1}$$

*where $0 \le c \le 2n$ (resp. $c \in \mathbb{Z}/N\mathbb{Z}$).*

P r o o f.

$$\begin{aligned} S_k(A, m, n)^2 &= \sum_{a,b \in A_n} \zeta_m^{k(a+b)} \\ &= \sum_c \left( \sum_{\substack{(a,b) \in A_n \times A_n: \\ a+b=c}} 1 \right) \zeta_m^{kc} = \sum_c r_{A_n}(c) \zeta_m^{kc}, \end{aligned}$$

where $0 \le c \le 2n$, since $r_{A_n}(c) = 0$ if $c > 2n$ (resp. $c \in \mathbb{Z}/N\mathbb{Z}$, since $m = N$). □

**Proposition 4.2.** *Let $A \subset \mathbb{N}$ (resp. $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$). For any $m, n \in \mathbb{N}$, with $m > n$ (resp. $m = N$ and $n \bmod N$ denoting the residue class of $n$ in $\mathbb{Z}/N\mathbb{Z}$), we have*

$$r_A(n) = \frac{1}{m} \sum_{k=0}^{m-1} \zeta_m^{-kn} S_k(A, m, n)^2 \tag{4.2}$$

*respectively,*

$$r_{A_n}(n \bmod N) = \frac{1}{N} \sum_{k=0}^{N-1} \zeta_N^{-kn} S_k(A, N, n)^2. \tag{4.3}$$

P r o o f. By Lemma 4.1, with $m > n$ (resp. $m = N$),

$$\sum_{k=0}^{m-1} \zeta_m^{-kn} S_k(A,m,n)^2 = \sum_{k=0}^{m-1} \zeta_m^{-kn} \sum_c r_{A_n}(c)\zeta_m^{kc}$$
$$= \sum_c r_{A_n}(c) \sum_{k=0}^{m-1} \zeta_m^{k(c-n)},$$

where $0 \le c \le 2n$ (resp. $c \in \mathbb{Z}/N\mathbb{Z}$). By Lemma 2.1,

$$\sum_{k=0}^{m-1} \zeta_m^{k(c-n)} = \begin{cases} m, & \text{if } c \equiv n \pmod m, \\ 0, & \text{if } c \not\equiv n \pmod m. \end{cases}$$

Therefore,

$$\sum_{k=0}^{m-1} \zeta_m^{-kn} S_k(A,m,n)^2 = \sum_{c \equiv n \pmod m} r_{A_n}(c) m.$$

Moreover, $c \equiv n \pmod m$ with $0 \le c \le 2n$ and $m > n$ (resp. with $c \in \mathbb{Z}/N\mathbb{Z} \simeq \{0,1,\dots,N-1\}$ and $m = N$) if and only if $c = n$. So the last sum above is reduced to just one term, namely, $r_{A_n}(n)m$. Thus

$$\sum_{k=0}^{m-1} \zeta_m^{-kn} S_k(A,m,n)^2 = m r_{A_n}(n).$$

Moreover, in the case where $A \subset \mathbb{N}$, we clearly have $r_{A_n}(n) = r_A(n)$. Hence the result. □

**Remark 4.3.** The formula in Proposition 4.2 is quite similar to the finite Fourier inversion formula as given in ([1], Theorem 8.4).

**Lemma 4.4.** *For $A \subset \mathbb{N}$ (resp. $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0,1,\dots,N-1\}$), and $m,n \in \mathbb{N}$, with $m > 0$ (resp. $m = N$), we have*

$$\sum_{k=0}^{m-1} S_k(A,m,n)^2 = m \sum_{0 \le q \le \frac{2n}{m}} r_{A_n}(qm), \tag{4.4}$$

*respectively,*

$$\sum_{k=0}^{N-1} S_k(A,N,n)^2 = N r_{A_n}(0). \tag{4.5}$$

P r o o f. By Lemma 4.1 and Lemma 2.1,

$$\sum_{k=0}^{m-1} S_k(A,m,n)^2 = \sum_{k=0}^{m-1}\sum_{c} r_{A_n}(c)\zeta_m^{kc}$$
$$= \sum_{c} r_{A_n}(c)\sum_{k=0}^{m-1}\zeta_m^{kc} = \sum_{c:m|c} r_{A_n}(c)m,$$

where $0 \le c \le 2n$ (resp. $c \in \mathbb{Z}/N\mathbb{Z}$), so that

$$\sum_{c:m|c} r_{A_n}(c)m = m\sum_{0\le q\le \frac{2n}{m}} r_{A_n}(qm) \quad (\text{resp. } = Nr_{A_n}(0).) \qquad \square$$

**Corollary 4.5.** *For $A \subset \mathbb{N}$, and for any positive integer $n$,*

$$\chi_A(n) = \frac{1}{2n}\sum_{k=0}^{2n-1} S_k(A,2n,n)^2 - \chi_A(0). \tag{4.6}$$

P r o o f. By Lemma 4.4 with $m = 2n$,

$$\sum_{k=0}^{2n-1} S_k(A,2n,n)^2 = 2n\big(r_{A_n}(0) + r_{A_n}(2n)\big).$$

And, clearly, $r_{A_n}(0) = r_A(0) = \chi_A(0)$. Moreover, the only possible representation of $2n$ as a sum of two elements of $A_n$ is $2n = n + n$, provided $n \in A$. So $r_{A_n}(2n) = 1$ if $n \in A$ and $r_{A_n}(2n) = 0$ if $n \notin A$, i.e., $r_{A_n}(2n) = \chi_A(n)$. Thus

$$\sum_{k=0}^{2n-1} S_k(A,2n,n)^2 = 2n\big(\chi_A(0) + \chi_A(n)\big),$$

and the result follows. $\square$

**Remark 4.6.** Another expression for $\chi_A(n)$, in the case where $A \subset \mathbb{N}$ and $n > 0$, can be obtained directly, by similarly establishing that

$$\sum_{k=0}^{n-1} S_k(A,n,n) = \sum_{a\in A_n}\sum_{k=0}^{n-1}\zeta_n^{ak} = \sum_{a\in A_n : n|a} n = n\big(\chi_A(0) + \chi_A(n)\big),$$

which gives

$$\chi_A(n) = \frac{1}{n}\sum_{k=0}^{n-1} S_k(A,n,n) - \chi_A(0). \tag{4.7}$$

**Proposition 4.7.** *Let $A$ be a subset of $\mathbb{N}$. For any positive integer $n$, we have*

$$r_A(n) = \frac{1}{n}\sum_{k=0}^{n-1} S_k(A,n,n)^2 - \chi_A(0) - \chi_A(n) \tag{4.8}$$

$$= \frac{1}{n}\sum_{k=0}^{n-1} S_k(A,n,n)^2 - \frac{1}{2n}\sum_{k=0}^{2n-1} S_k(A,2n,n)^2. \tag{4.9}$$

P r o o f. By Lemma 4.4 with $m = n$,

$$\sum_{k=0}^{n-1} S_k(A,n,n)^2 = n\sum_{0\le q\le 2} r_{A_n}(qn) = n\big(r_{A_n}(0) + r_{A_n}(n) + r_{A_n}(2n)\big).$$

As it is indicated in the previous proof,

$$r_{A_n}(0) = r_A(0) = \chi_A(0), \quad \text{and} \quad r_{A_n}(2n) = \chi_A(n).$$

Moreover, $r_{A_n}(n) = r_A(n)$, since if $n = a + b$ with $a, b \in A$, then $a, b \le n$, i.e., $a, b \in A_n$. Thus

$$\sum_{k=0}^{n-1} S_k(A,n,n)^2 = n\big(\chi_A(0) + r_A(n) + \chi_A(n)\big).$$

This gives the first equality. The second equality follows from the first one and from Corollary 4.5. □

**Proposition 4.8.** *Let $A \subset \mathbb{N}$ and $m, n \in \mathbb{N}$ such that $m > n$, then*

$$A(n) = \frac{1}{m}\sum_{k=0}^{m-1} |S_k(A,m,n)|^2. \tag{4.10}$$

P r o o f.

$$\begin{aligned}
\sum_{k=0}^{m-1} |S_k(A,m,n)|^2 &= \sum_{k=0}^{m-1} S_k(A,m,n)\overline{S_k(A,m,n)} \\
&= \sum_{k=0}^{m-1} \left(\sum_{a\in A_n} \zeta_m^{ka}\right)\left(\sum_{b\in A_n} \zeta_m^{-kb}\right) \\
&= \sum_{k=0}^{m-1} \sum_{a,b\in A_n} \zeta_m^{k(a-b)} = \sum_{a,b\in A_n} \sum_{k=0}^{m-1} \zeta_m^{k(a-b)} \\
&= \sum_{a,b\in A_n : a\equiv b \pmod m} m = m\cdot|A_n| = m\cdot A(n),
\end{aligned}$$

where in the last line of equalities, we used Lemma 2.1, and the fact that $m > n$, so that, for $a, b \in A_n$, $a \equiv b \pmod m$ if and only if $a = b$. □

**Remark 4.9.** If, in the preceding Proposition, we take $m = n > 0$ (instead of $m > n$), then, for $a, b \in A_n$, $a \equiv b \pmod n$ if and only if $a = b$ or $(a, b) = (0, n)$ or $(a, b) = (n, 0)$, provided 0 and $n$ lie in $A$. Therefore, in this case,

$$\sum_{k=0}^{n-1} |S_k(A, n, n)|^2 = n\big(A(n) + 2\chi_A(0)\chi_A(n)\big).$$

Thus

$$A(n) = \frac{1}{n}\sum_{k=0}^{n-1} |S_k(A, n, n)|^2 - 2\chi_A(0)\chi_A(n). \tag{4.11}$$

**Lemma 4.10.** *Let $A \subset \mathbb{N}$ (resp. $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$), and $m, n \in \mathbb{N}$, with $m > 0$ (resp. $m = N$). For any integer $r \in \mathbb{Z}$, we have*

$$\sum_{k=0}^{m-1} \zeta_m^{-kr} S_k(A, m, n) = m \sum_{-\frac{r}{m} \le j \le \frac{n-r}{m}} \chi_A(jm + r), \tag{4.12}$$

*respectively,*

$$\sum_{k=0}^{N-1} \zeta_m^{-kr} S_k(A, N, n) = N \cdot \chi_{A_n}(r \bmod N). \tag{4.13}$$

P r o o f. In the case where $A \subset \mathbb{N}$, by Lemma 2.1

$$\begin{aligned}\sum_{k=0}^{m-1} \zeta_m^{-kr} S_k(A, m, n) &= \sum_{k=0}^{m-1} \zeta_m^{-kr} \sum_{a \in A_n} \zeta_m^{ka} \\ &= \sum_{a \in A_n} \sum_{k=0}^{m-1} \zeta_m^{k(a-r)} \\ &= m \cdot |\{a \in A_n : a \equiv r \pmod m\}|.\end{aligned}$$

Moreover, $a \equiv r \pmod m$ if and only if $a = jm + r$ for some $j \in \mathbb{Z}$, and $a = jm + r \in A_n$ if and only if $\chi_A(jm + r) = 1$ and $0 \le jm + r \le n$, i.e., $-\frac{r}{m} \le j \le \frac{n-r}{m}$. Hence

$$|\{a \in A_n : a \equiv r \pmod m\}| = \sum_{-\frac{r}{m} \le j \le \frac{n-r}{m}} \chi_A(jm + r),$$

which implies the first formula.

Similarly, in the case where $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$ and $m = N$,

$$\begin{aligned}\sum_{k=0}^{N-1} \zeta_N^{-kr} S_k(A, N, n) &= \sum_{k=0}^{N-1} \zeta_N^{-kr} \sum_{a \in A_n} \zeta_N^{ka} \\ &= \sum_{a \in A_n} \sum_{k=0}^{N-1} \zeta_N^{k(a-r)} \\ &= N \cdot |\{a \in A_n : a \equiv r \pmod N\}|.\end{aligned}$$

Moreover, $|\{a \in A_n : a \equiv r \pmod N\}|$ is equal to 1 if the congruence class of $r$ mod $N$ lies in $A_n$, and to 0 otherwise, i.e.,

$$|\{a \in A_n : a \equiv r \pmod N\}| = \chi_{A_n}(r \bmod N).$$

Hence the second formula. □

**Corollary 4.11.** *Let $A \subset \mathbb{N}$ (resp. $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$), and $m, n \in \mathbb{N}$, with $m > 0$ (resp. $m = N$), we have*

$$\sum_{k=0}^{m-1} S_k(A, m, n) = m \sum_{0 \le j \le \frac{n}{m}} \chi_A(jm). \tag{4.14}$$

*respectively,*

$$\sum_{k=0}^{N-1} S_k(A, N, n) = N \cdot \chi_A(0). \tag{4.15}$$

Proof. This is the special case $r = 0$ of the previous Lemma, taking into account that $\chi_{A_n}(0) = \chi_A(0)$. □

## 5. Cyclotomic Expressions

We still denote by $A$ a subset of $\mathbb{N}$ (resp. of $\mathbb{Z}/N\mathbb{Z} \simeq \{0, 1, \dots, N-1\}$), by $m$ a positive integer, while $n \in \mathbb{N}$ and $k \in \mathbb{Z}$.

From the definition of $\zeta_m = e^{\frac{2\pi i}{m}}$, it easily follows that if $d$ is a positive integer dividing $m$, then

$$\zeta_m^d = \zeta_{\frac{m}{d}}. \tag{5.1}$$

If $d = \gcd(k, m)$, and $m = dm_1$, $k = dk_1$, where $k_1 \in \mathbb{Z}$, and the integers $d, m_1 > 0$ with $\gcd(k_1, m_1) = 1$, then

$$S_k(A, m, n) = S_{k_1}(A, m_1, n). \tag{5.2}$$

Indeed,

$$S_k(A,m,n) = \sum_{a\in A_n} \zeta_m^{ka} = \sum_{a\in A_n} \zeta_m^{dk_1 a}$$

$$= \sum_{a\in A_n} \zeta_{m_1}^{k_1 a} = S_{k_1}(A,m_1,n).$$

Thus, considering the sums $S_k(A,m,n)$, we may assume that $\gcd(k,m)=1$.

The sums

$$S_k(A,m,n) = \sum_{a\in A_n} \zeta_m^{ka}$$

are cyclotomic integers, i.e., they lie in the ring of integers $\mathbb{Z}[\zeta_m]$ of the cyclotomic field $\mathbb{Q}(\zeta_m)$.

The field extension $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ is an abelian extension of degree $\varphi(m)$, where $\varphi$ is Euler's totient function. The Galois group $G_m$ of $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ is isomorphic to the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$ of invertible elements of the ring $\mathbb{Z}/m\mathbb{Z}$ of residue classes of integers modulo $m$. The elements of $G_m$ are the $\mathbb{Q}$-automorphisms $\sigma_{m,k}$ of $\mathbb{Q}(\zeta_m)$ defined by

$$\sigma_{m,k}(\zeta_m) = \zeta_m^k, \quad \text{for } \dot{k} \in (\mathbb{Z}/m\mathbb{Z})^*,$$

where $\dot{k} = k + m\mathbb{Z}$ is the congruence class of $k$ modulo $m$, i.e., for $k$ ranging through a reduced residue sytem of integers modulo $m$. Moreover, the irreducible polynomial of $\zeta_m$ over $\mathbb{Q}$ is the $m$th cyclotomic polynomial

$$\Phi_m(X) = \prod_{\substack{1\le k\le m:\\ \gcd(k,m)=1}} (X - \zeta_m^k),$$

of degree $\varphi(m)$, and having integer coefficients ([14]).

**Lemma 5.1.** *For any integers $h,k\in\mathbb{Z}$ and $m,n\in\mathbb{N}$, with $m>0$, such that $\gcd(k,m)=1$, we have*

$$\sigma_{m,k}\big(S_h(A,m,n)\big) = S_{kh}(A,m,n). \tag{5.3}$$

P r o o f. Indeed,

$$\sigma_{m,k}(S_h(A,m,n)) = \sigma_{m,k}\left(\sum_{a\in A_n}\zeta_m^{ha}\right) = \sum_{a\in A_n}\zeta_m^{kha} = S_{kh}(A,m,n).$$

□

**Corollary 5.2.** *In particular, for any natural numbers $m,n\in\mathbb{N}$, with $m>0$, and any integer $k\in\mathbb{Z}$ such that $\gcd(k,m)=1$, we have*

$$S_k(A,m,n) = \sigma_{m,k}\big(S_1(A,m,n)\big). \tag{5.4}$$

**Remark 5.3.** It follows from (5.2) and (5.4), setting $(k,m)=\gcd(k,m)$, that

$$S_k(A,m,n)=S_{\frac{k}{(k,m)}}\Big(A,\frac{m}{(k,m)},n\Big)=\sigma_{\frac{m}{(k,m)},\frac{k}{(k,m)}}\bigg(S_1\Big(A,\frac{m}{(k,m)},n\Big)\bigg). \quad (5.5)$$

Thus, in order to determine all the sums $S_k(A,m,n)$, it is enough just to determine the sums

$$S_1(A,m,n)=\sum_{a\in A_n}\zeta_m^a.$$

**Proposition 5.4.** *Let $A$ be a subset of $\mathbb{N}$ (resp. of $\mathbb{Z}/N\mathbb{Z}\simeq\{0,1,\dots,N-1\}$), and let $m,n\in\mathbb{N}$ such that $m>n$ (resp. let $m=N$ and $n \bmod N$ be the residue class of $n$ in $\mathbb{Z}/N\mathbb{Z}$), then*

$$r_A(n)=\frac{1}{m}\sum_{d|m}Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}\left(\zeta_d^{-n}S_1(A,d,n)^2\right), \quad (5.6)$$

*respectively,*

$$r_A(n \bmod N)=\frac{1}{N}\sum_{d|N}Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}\left(\zeta_d^{-n}S_1(A,d,n)^2\right), \quad (5.7)$$

*where $Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}$ is the trace form in the field extension $\mathbb{Q}(\zeta_d)|\mathbb{Q}$, and $d$ ranges over the set of positive integers dividing $m$ (resp. $N$).*

P r o o f. Using Proposition 4.2, Remark 3.1, (5.1) and Corollary 5.2 successively, we get

$$\begin{aligned}
r_A(n)&=\frac{1}{m}\sum_{k=0}^{m-1}\zeta_m^{-kn}S_k(A,m,n)^2\\
&=\frac{1}{m}\sum_{k=1}^{m}\zeta_m^{-kn}S_k(A,m,n)^2\\
&=\frac{1}{m}\sum_{e|m}\sum_{\substack{1\le k\le m:\\ \gcd(k,m)=e}}\zeta_m^{-kn}S_k(A,m,n)^2\\
&=\frac{1}{m}\sum_{e|m}\sum_{\substack{1\le k\le m:\\ \gcd(k,m)=e}}\zeta_{\frac{m}{e}}^{-\frac{k}{e}n}S_{\frac{k}{e}}\left(A,\frac{m}{e},n\right)^2\\
&=\frac{1}{m}\sum_{e|m}\sum_{\substack{1\le k\le m:\\ \gcd(k,m)=e}}\sigma_{\frac{m}{e},\frac{k}{e}}\left(\zeta_{\frac{m}{e}}^{-n}S_1\left(A,\frac{m}{e},n\right)^2\right).
\end{aligned}$$

Setting $d = \frac{m}{e}$ and $h = \frac{k}{e}$, noting that $\gcd(d,h) = 1$, and substituting into the latter sum, we obtain

$$\begin{aligned} r_A(n) &= \frac{1}{m} \sum_{d|m} \sum_{\substack{1\le h\le d:\\ \gcd(d,h)=1}} \sigma_{d,h}\left(\zeta_d^{-n} S_1(A,d,n)^2\right) \\ &= \frac{1}{m} \sum_{d|m} Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}\left(\zeta_d^{-n} S_1(A,d,n)^2\right), \end{aligned}$$

since, for each $d \mid m$,

$$\sum_{\substack{1\le h\le d:\\ \gcd(d,h)=1}} \sigma_{d,h}\left(\zeta_d^{-n} S_1(A,d,n)^2\right)$$

is the sum of all the conjugates in $\mathbb{Q}(\zeta_d)|\mathbb{Q}$ of $\zeta_d^{-n} S_1(A,d,n)^2$, which is, by definition, the trace in $\mathbb{Q}(\zeta_d)|\mathbb{Q}$ of $\zeta_d^{-n} S_1(A,d,n)^2$.

The same proof works in the case where $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0,1,\dots,N-1\}$ and $m = N$, just replacing $r_A(n)$ by $r_A(n \bmod N)$ and $m$ by $N$. □

**Lemma 5.5.** *For any positive integer $n$ and any integer $h \in \mathbb{Z}$, if $d = \gcd(h,n)$, then*

$$Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_n^h) = \mu\left(\frac{n}{d}\right) \frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)} = \mu\left(\frac{n}{(h,n)}\right) \frac{\varphi(n)}{\varphi\left(\frac{n}{(h,n)}\right)}, \tag{5.8}$$

*where $\mu$ is the Möbius function defined by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ has a prime square factor,} \\ (-1)^s & \text{if } n \text{ is the product of } s \text{ distinct primes.} \end{cases} \tag{5.9}$$

*In particular, if $h$ and $n$ are relatively prime, then $Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_n^h) = \mu(n)$.*

Proof. This results from ([11], p. 427, IV), in the special case of the trivial character. □

**Proposition 5.6.** *Let $A$ be a subset of $\mathbb{N}$ (resp. of $\mathbb{Z}/N\mathbb{Z} \simeq \{0,1,\dots,N-1\}$), and let $m, n \in \mathbb{N}$ such that $m > n$ (resp. let $m = N$ and $n \bmod N$ be the residue class of $n$ in $\mathbb{Z}/N\mathbb{Z}$), then*

$$r_A(n) = \frac{1}{m} \sum_{(a,b)\in A_n\times A_n} \sum_{d|m} \mu\left(\frac{d}{(d,a+b-n)}\right) \frac{\varphi(d)}{\varphi\left(\frac{d}{(d,a+b-n)}\right)}. \tag{5.10}$$

*respectively,*

$$r_A(n \bmod N) = \frac{1}{N} \sum_{(a,b)\in A_n\times A_n} \sum_{d|N} \mu\left(\frac{d}{(d,a+b-n)}\right) \frac{\varphi(d)}{\varphi\left(\frac{d}{(d,a+b-n)}\right)}. \tag{5.11}$$

P r o o f. By Proposition 5.4,

$$r_A(n) = \frac{1}{m} \sum_{d|m} Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}\left(\zeta_d^{-n} S_1(A,d,n)^2\right).$$

Moreover,

$$\begin{aligned}\zeta_d^{-n} S_1(A,d,n)^2 &= \zeta_d^{-n}\left(\sum_{a\in A_n} \zeta_d^a\right)^2 \\ &= \sum_{(a,b)\in A_n\times A_n} \zeta_d^{a+b-n},\end{aligned}$$

and by Corollary 5.5,

$$Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}\left(\zeta_d^{a+b-n}\right) = \mu\left(\frac{d}{(d,a+b-n)}\right) \frac{\varphi(d)}{\varphi\left(\frac{d}{(d,a+b-n)}\right)}.$$

Hence

$$\begin{aligned}r_A(n) &= \frac{1}{m} \sum_{d|m} \sum_{(a,b)\in A_n\times A_n} Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}\left(\zeta_d^{a+b-n}\right) \\ &= \frac{1}{m} \sum_{(a,b)\in A_n\times A_n} \sum_{d|m} \mu\left(\frac{d}{(d,a+b-n)}\right) \frac{\varphi(d)}{\varphi\left(\frac{d}{(d,a+b-n)}\right)}.\end{aligned}$$

The same proof works in the case where $A \subset \mathbb{Z}/N\mathbb{Z} \simeq \{0,1,\dots,N-1\}$ and $m = N$, just replacing $r_A(n)$ by $r_A(n \bmod N)$ and $m$ by $N$. □

## 6. Example

Let $p$ be an odd prime number. In $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \simeq \{0,1,\dots,p-1\}$, let

$$A = \{x^2 : x \in \mathbb{F}_p\}.$$

Fix

$$n \in \mathbb{F}_p \simeq \{0,1,\dots,p-1\}.$$

By Proposition 5.6

$$\begin{aligned}
r_A(n) &= \frac{1}{p}\sum_{a,b\in A_n}\sum_{d\mid p}\mu\left(\frac{d}{(d,a+b-n)}\right)\frac{\varphi(d)}{\varphi\left(\frac{d}{(d,a+b-n)}\right)}\\
&= \frac{1}{p}\sum_{a,b\in A_n}\mu\left(\frac{1}{(1,a+b-n)}\right)\frac{\varphi(1)}{\varphi\left(\frac{1}{(1,a+b-n)}\right)}\\
&+ \frac{1}{p}\sum_{a,b\in A_n}\mu\left(\frac{p}{(p,a+b-n)}\right)\frac{\varphi(p)}{\varphi\left(\frac{p}{(p,a+b-n)}\right)}\\
&= \frac{1}{p}\sum_{a,b\in A_n}1+\frac{1}{p}\sum_{\substack{a,b\in A_n:\\ a+b=n}}\mu(1)\frac{\varphi(p)}{\varphi(1)}+\frac{1}{p}\sum_{\substack{a,b\in A_n:\\ a+b\neq n}}\mu(p)\frac{\varphi(p)}{\varphi(p)}\\
&= \frac{1}{p}A(n)^2+\frac{p-1}{p}\sum_{\substack{a,b\in A_n:\\ a+b=n}}1-\frac{1}{p}\sum_{\substack{a,b\in A_n:\\ a+b\neq n}}1\\
&= \frac{1}{p}\left(A(n)^2+(p-1)|R_n(A)|-|A_n\times A_n\setminus R_n(A)|\right)\\
&= |R_n(A)|, \qquad (6.1)
\end{aligned}$$

where

$$\begin{aligned}
R_n(A) &= \{(a,b)\in A_n\times A_n : a+b=n\}\\
&= \{0\le a\le n : a\in A \text{ and } n-a\in A\}\\
&= \Big\{0\le a\le n : \Big(\frac{a}{p}\Big)=\Big(\frac{n-a}{p}\Big)=1,\\
&\qquad \text{or } a=0, n\in A, \quad \text{or } a=n\in A\cup\{0\}\Big\}, \qquad (6.2)
\end{aligned}$$

with $\left(\frac{\cdot}{p}\right)$ denoting the Legendre symbol.

Moreover, for any $0\le a\le n$,

$$\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{n-a}{p}\right)\right)=\begin{cases}4 & \text{if } a, n-a\in A, a\neq 0, n,\\ 2 & \text{if } (a=0\neq n\in A), \text{ or } (0\neq a=n\in A),\\ 1 & \text{if } a=n=0,\\ 0 & \text{if } a\notin A, \text{ or } (n-a)\notin A,\end{cases} \qquad (6.3)$$

and

$$1+\left(\frac{n}{p}\right)=\begin{cases}2 & \text{if } n\in A, n\neq 0,\\ 1 & \text{if } n=0,\\ 0 & \text{if } n\notin A.\end{cases} \tag{6.4}$$

It follows that

$$\begin{aligned} r_A(n) &= \frac{1}{4}\sum_{a\in\mathbb{F}_p: a\neq 0,n}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{n-a}{p}\right)\right)+1+\left(\frac{n}{p}\right)\\ &= \frac{1}{4}\left(\sum_{a\in\mathbb{F}_p}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{n-a}{p}\right)\right)+\delta_{n,0}\right)+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right)\\ &= \frac{1}{4}\sum_{a=0}^{p-1}\left(1+\left(\frac{a}{p}\right)+\left(\frac{n-a}{p}\right)+\left(\frac{a(n-a)}{p}\right)\right)+\frac{\delta_{n,0}}{4}+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right)\\ &= \frac{1}{4}\left(p+\delta_{n,0}+\sum_{a=0}^{p-1}\left(\frac{a(n-a)}{p}\right)\right)+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right), \end{aligned} \tag{6.5}$$

where $\delta_{n,0}$ is equal to 1 if $n=0$, and to 0 otherwise. It is added to the second line of the above equalities to compensate for the fact that, just in the case $n=0$, without it, the second line would be equal to $r_A(0)-\frac{1}{4}$, due to the third case in the equality 6.3. We also tacitly used the fact that

$$\sum_{a=0}^{p-1}\left(\frac{a}{p}\right)=\sum_{a=0}^{p-1}\left(\frac{n-a}{p}\right)=0,$$

since the number of non-zero quadratic residues is equal to that of non-residues.

Now, by ([13], Theorem 8.2, p. 174), if $n\neq 0$, then

$$\sum_{a=0}^{p-1}\left(\frac{a(n-a)}{p}\right)=\left(\frac{-1}{p}\right)\sum_{a=0}^{p-1}\left(\frac{a^2-na}{p}\right)=\left(\frac{-1}{p}\right)(-1)=(-1)^{\frac{p+1}{2}}. \tag{6.6}$$

While if $n=0$, then, trivially,

$$\sum_{a=0}^{p-1}\left(\frac{a(n-a)}{p}\right)=\left(\frac{-1}{p}\right)\sum_{a=1}^{p-1}\left(\frac{a^2}{p}\right)=(-1)^{\frac{p-1}{2}}(p-1). \tag{6.7}$$

It follows from 6.6 and 6.7 that

$$\sum_{a=0}^{p-1}\left(\frac{a(n-a)}{p}\right) = (-1)^{\frac{p-1}{2}}(\delta_{n,0}p-1). \tag{6.8}$$

Substituting 6.8 into 6.5 gives

$$\begin{aligned} r_A(n) &= \frac{1}{4}\left(p+\delta_{n,0}+\sum_{a=0}^{p-1}\left(\frac{a(n-a)}{p}\right)\right)+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right) \\ &= \frac{1}{4}\left(p+\delta_{n,0}+(-1)^{\frac{p-1}{2}}(\delta_{n,0}p-1)\right)+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right) \\ &= \frac{1}{4}\left(p+(-1)^{\frac{p+1}{2}}+\delta_{n,0}\left((-1)^{\frac{p-1}{2}}p+1\right)\right)+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right), \end{aligned} \tag{6.9}$$

i.e.,

$$r_A(n) = \begin{cases} \frac{1}{4}\left(p+(-1)^{\frac{p+1}{2}}\right)+\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right), & \text{if } n\neq 0, \\ 1+\frac{1}{4}\left(1+(-1)^{\frac{p-1}{2}}\right)(p-1), & \text{if } n=0. \end{cases} \tag{6.10}$$

**Acknowledgement.** I would like to thank the referee, whose suggestions helped simplify some proofs.

## REFERENCES

[1] APOSTOL, T. M.: *Introduction to Analytic Number Theory*. Springer-Verlag, New York-Heidelberg 1976.

[2] CILLERUELO, J.—NATHANSON, M. B.: *Dense sets of integers with prescribed representation functions*, European J. Combin. **34** (2013), no. 8, 1297–1306.

[3] DUBICKAS, A.: *A basis of finite and infinite sets with small representation function*, Electron. J. Combin. **19** (2012), no. 1, Paper 6, 16 pp.

[4] ———— *On the supremum of the representation function of a sumset*, Quaest. Math. **37** (2014), no. 1, 1–8.

[5] ERDŐS, P.—TURÁN, P.: *On a problem of Sidon in additive number theory*, J. London Math. Soc. **16** (1941), 212–215.

[6] GREKOS, G.—HADDAD, L.—HELOU, C.—PIHKO, J.: *On the Erdős-Turán conjecture*, J. Number Theory **102** (2003), 339–352.

[7] ——— *The class of Erdős-Turán sets*, Acta Arithmetica, **117** (2005), 81–105.

[8] ——— *Representation functions, Sidon sets and bases*, Acta Arithmetica **130** (2007), no. 2, 149–156.

[9] ——— *Supremum of representation functions*, Integers **11** (2011), A30, 14 pp.

[10] ——— *On the General Erdős-Turán conjecture*, International Journal of Combinatorics, **2014** (2014), Article ID 826141, 11 pp.

[11] HASSE, H.: *Vorlesungen über Zahlentheorie*. Springer-Verlag, Berlin, 1950.

[12] HELOU, C.: *Characteristic, counting, and representation functions characterized*, Combinatorial and additive number theory. II, 139–155, Springer Proc. Math. Stat., 220, 2017.

[13] HUA, L. K.: *Introduction to Number Theory*. Springer-Verlag, New York, 1982.

[14] IRELAND, K.—ROSEN, M.: *A Classical Introduction to Modern Number Theory*. Springer, New York, 1990.

[15] KISS, S.—SÁNDOR, C.: *On the maximum values of the additive representation functions*, Int. J. Number Theory, **12** (2016), 1055–1075.

[16] ——— *Partitions of the set of nonnegative integers with the same representation functions*, Discrete Math., **340** (2017), 1154–1161.

[17] LEE, J.: *Infinitely often dense bases for the integers with a prescribed representation function*, Integers **10** (2010), A24, 299–307.

[18] LEV, V. F.: *Reconstructing integer sets from their representation functions*, Electron. J. Combin. **11** (2004), no. 1, Research Paper 78, 6 pp.

[19] NATHANSON, M. B.: *Representation functions of sequences in additive number theory*, Proc. Amer. Math. Soc. **72** (1978), 16–20.

[20] ——— *Representation functions of additive bases for abelian semigroups*, Int. J. Math. Math. Sci. 2004, no. 29-32, 1589–1597.

[21] ——— *Every function is the representation function of an additive basis for the integers*, Port. Math. (N.S.) **62** (2005), no. 1, 55–72.

[22] ——— *Inverse problems for representation functions in additive number theory*, Surveys in number theory, Dev. Math., Vol. 17, 2008 pp. 89–117.

[23] SÁNDOR, C.: *A note on a conjecture of Erdős and Turán*, Integers **8** (2008), A30, 4 pp.

Received August 20, 2018
Accepted November 5, 2018

**Charles Helou**
*Pennsylvania State University*
*Brandywine Campus*
*25 Yearsley Mill Road*
*Media, Pensylvania*
*PA 19063*
*USA*
*E-mail*: cxh22@psu.edu