ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 287 (2004) 77–84

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Partitions modulo n and circulant matrices

Gérard Maze[a, b, 1]

[a] Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556-5683, USA
[b] Section de Mathématiques, EPFL, 1015 Lausanne, Switzerland

Received 11 March 2002; received in revised form 14 April 2004; accepted 27 April 2004

Abstract

This paper is about a connection between a general problem of partitions in $\mathbb{Z}/n\mathbb{Z}$ and the expression of determinants of certain circulant matrices. The main result of the article is a method for calculating, in certain special cases, explicit formulas for the number of partitions of elements in $\mathbb{Z}/n\mathbb{Z}$ in distinct summands and the number of partitions of elements in $\mathbb{Z}/n\mathbb{Z}$ with less than t repetitions. Explicit formulas for partitions in $\mathbb{Z}/n\mathbb{Z}$ in the general case can be found by explicitly calculating the determinants of certain circulant matrices.

MSC: 05A13; 11P83; 11L03

Keywords: Partitions; Circulant matrices; Ramanujan's sums

1. Introduction

A partition of an integer m is a representation of m as a sum of positive integers. The problem of counting the number of partitions of m is a well-known problem. It has a long history and belongs to the classical problems in number theory, see, e.g., [1,5]. Many questions about partitions are still open [1]. Questions about the unrestricted partition function can be generalized by requiring that the summands belong to a certain subset of $\mathbb{N}$ as in [2,5] or by fixing some constraints on the number of repetitions of the summands (e.g. partitions without repetition, also in [5]).

The goal of this paper is to derive a generalization when m is viewed as an element of $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$. This extended notion of partition must be clarified since unless the number of summands is limited, there will always be an infinite number of representations of a given $m \in \mathbb{Z}/n\mathbb{Z}$ as a sum of elements in $\mathbb{Z}/n\mathbb{Z}$. Indeed, one can add an arbitrary number of summands as long as their sum is equal to zero. The following definition gives the exact type of partitions we will be dealing with in the sequel.

Definition 1. Let n be a positive integer, $m \in \mathbb{Z}/n\mathbb{Z}$ and $\mathscr{C}$ be a nonempty subset of $\{0, 1, 2, 3, \ldots, n-1\}$. A $\mathscr{C}$-partition of m modulo n is an equality of the form

$$x_1 + \cdots + x_k = m \quad \text{in } \mathbb{Z}/n\mathbb{Z},$$

E-mail address: gerard.maze@epfl.ch (G. Maze).

[1] Supported in part by NSF Grant DMS-00-72383.

0012-365X/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.04.015

where

- $k \geqslant 1$,
- $\forall i \in \{1, \ldots, k\}, \;\; x_i \in \{1, \ldots, n-1\}$,
- $\forall x \in \{1, \ldots, n-1\}, |\{i \in \{1, \ldots, k\} \mid x_i = x\}| \in \mathscr{C}$.

Two $\mathscr{C}$-partitions $x_1 + \cdots + x_k = m$ and $y_1 + \cdots + y_l = m$ are the same if and only if $l = k$ and there exists a permutation σ of $\{1, \ldots, k\}$ such that $y_i = x_{\sigma(i)}$, i.e., the order of the summands is unimportant.

Example 2. Let $\mathscr{C} = \{0, 1, 3\}$. Then $1 + 2 + 2 + 2 + 5 = 4 \bmod 8$ is a $\mathscr{C}$-partition of 4 modulo 8. This partition is equal to the $\mathscr{C}$-partition $2 + 1 + 2 + 5 + 2 = 4 \bmod 8$.

We can now pose the following natural problem:

Problem 3. Let n, m and $\mathscr{C}$ be as above. Find the number of $\mathscr{C}$-partitions of m modulo n.

A special case of this problem, when $\mathscr{C} = \{0, 1\}$, asks to enumerate the number of partitions of m without repetition of summands. Such partitions will be called *strict partitions* in the sequel. In this case, Problem 3 asks to enumerate the number of possible expressions

$$x_1 + \cdots + x_k = m \quad \text{in } \mathbb{Z}/n\mathbb{Z},$$

where the x_i are all different and where the order of the summands is irrelevant. This problem can be seen as the modular version of the usual problem of partitions with unequal parts [5, Chapter XIX]. Despite the huge literature on partitions and additive number theory, the author was not able to find any results on problems of this type.

The main result of this paper is a method for calculating the number of $\mathscr{C}$-partitions in $\mathbb{Z}/n\mathbb{Z}$ in terms of the determinant of certain circulant matrices. This method leads to explicit formulas for the number of strict partitions and partitions where less than t repetitions are admitted.

In Section 2, we will deal with properties of circulant matrices and technical results helpful in the computation of some of them. In Section 3, some theory about Ramanujan's sums will be recalled and the inverse of a matrix, with Ramanujan's sums as entries, will be found. We will prove the main result on general $\mathscr{C}$-partitions in Section 4 and give the explicit formulas when $\mathscr{C} = \{0, 1, 2, \ldots, t-1\}$ and for strict partitions in Section 5.

2. Circulant matrices

Let M be a circulant n by n matrix, i.e., a matrix of the form

$$M = \mathrm{Circ}_n[a_0, a_1, \ldots, a_{n-1}] = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}.$$

From the usual theory of such matrices [4], it is known that given a primitive nth root of unity, say ζ_n, one has

$$\det \mathrm{Circ}_n[a_0, a_1, \ldots, a_{n-1}] = \prod_{j=0}^{n-1} p(\zeta_n^j) \quad \text{where } p(x) = \sum_{k=0}^{n-1} a_k x^k. \tag{2.1}$$

A point that will be implicitly used in the sequel is that any primitive nth root of unity can be considered in the product, a direct consequence of Galois theory. A useful result in the computation of such a determinant is the following technical Lemma:

Lemma 4. *Let n, t be positive integers, d a divisor of n and let (t, d) be the greatest common divisor of t and d. The following equality holds*:

$$\prod_{j=0}^{n-1} (1 + (\zeta_d)^j + (\zeta_d)^{2j} + \cdots + (\zeta_d)^{(t-1)j}) = \begin{cases} t^{n/d} & if \;\; (t, d) = 1, \\ 0 & otherwise. \end{cases}$$

Proof. A different expression for the sum when $\zeta_d^j \neq 1$ leads to the following equation:

$$\prod_{j=0}^{n-1}(1+\zeta_d^j+\zeta_d^{2j}+\cdots+\zeta_d^{(t-1)j}) = t^{n/d}\prod_{\substack{j=1\\ d\nmid j}}^{n-1}\frac{1-\zeta_d^{tj}}{1-\zeta_d^j}.$$

If t and d have a non-trivial common divisor then there exists j with $0<j<d$ and $\zeta_d^{tj}=1$. Thus, the product is null. If t and d are relatively prime, the numerator and the denominator of the product on the right-hand side are the same, which gives the result. □

Proposition 5. *Let* $\mathscr{C}\subset\{0,1,2,3,\ldots,n-1\}$ *and* $d\mid n$. *If*

$$a_k = |\{c\in\mathscr{C} \mid cd = k \bmod n\}|$$

then

$$\prod_{j=0}^{n-1}\left(\sum_{c\in\mathscr{C}}\zeta_n^{cdj}\right) = \det \mathrm{Circ}_n[a_0,a_1,\ldots,a_{n-1}].$$

Proof. This follows by applying (2.1) to the equality

$$\sum_{c\in\mathscr{C}}(\zeta_n^j)^{cd} = \sum_{k=0}^{n-1}|\{c\in\mathscr{C}\mid cd = k \bmod n\}|(\zeta_n^j)^k = \sum_{k=0}^{n-1}a_k(\zeta_n^j)^k. \qquad \square$$

3. Ramanujan’s sums

Let $n\geqslant 1$ and k be integers and let U_n be the set of primitive nth roots of unity in $\mathbb{C}$. Consider Ramanujan’s sums $C(k,n)$ (notation of [3], also written $c_n(k)$ in [5]) defined by

$$C(k,n) = \sum_{\substack{(m,n)=1\\ 1\leqslant m\leqslant n}}\zeta_n^{mk} = \sum_{\zeta\in U_n}\zeta^k = \frac{\varphi(n)\cdot\mu(\frac{n}{(k,n)})}{\varphi(\frac{n}{(k,n)})},$$

where φ is Euler’s totient function and μ the Möbius function. The last equality is proved in [5]; using it, one can explicitly compute Ramanujan’s sums if the factorization of n is known. These sums are integers. This section is devoted to proving and recalling some results on these sums.

Lemma 6. *For any* $d\mid n$, *we have*

$$\sum_{\substack{(m,n)=d\\ 1\leqslant m\leqslant n}}\zeta_n^{mk} = \sum_{\zeta\in U_{n/d}}\zeta^k = C(k,n/d). \tag{3.1}$$

The proof is left to the reader. The next lemma is exactly Theorem 2 of [3].

Lemma 7. *For all* $d_1\mid n$, $d_2\mid n$, *Ramanujan’s sums satisfy the following orthogonal relation*:

$$\sum_{d\mid n}C(n/d,d_1)\cdot C(n/d_2,d) = \begin{cases} n & if\ d_1=d_2,\\ 0 & otherwise.\end{cases}$$

Given a positive integer n, let D_n be the set of divisors of n, with $\tau=|D_n|$, written as $D_n=\{d_1=1<d_2<\cdots<d_\tau=n\}$. Note that with this notation, we have $n/d_i = d_{\tau-i}$. For such n and D_n we define the matrix $\mathscr{R}_n$ as follows:

$$\mathscr{R}_n\in Mat_{\tau\times\tau}(\mathbb{Z}) \quad \text{with } (\mathscr{R}_n)_{ij} = C(d_i,d_j).$$

This matrix will naturally appear in the next section. All the information we need from it is in the next proposition.

Proposition 8. *Let $\mathscr{R}'_n \in Mat_{\tau\times\tau}(\mathbb{Z})$ be defined by $(\mathscr{R}'_n)_{ij} = C(n/d_i, n/d_j) = C(d_{\tau-i}, d_{\tau-j})$. Then*

(1) *the matrix $\mathscr{R}_n$ is invertible with $\mathscr{R}_n^{-1} = \frac{1}{n}\mathscr{R}'_n$,*
(2) $\det \mathscr{R}_n = \det \mathscr{R}'_n$,
(3) $\det \mathscr{R}_n = n^{\frac{\tau}{2}}$.

Proof. (1) Using Lemma 7, we have

$$\begin{aligned}(\mathscr{R}_n \cdot \mathscr{R}'_n)_{ij} &= \sum_{k=1}^{\tau} C(d_i, d_k)C(n/d_k, n/d_j)\\ &= \sum_{d|n} C(n/d, d_{\tau-j})C(n/d_{\tau-i}, d)\\ &= \begin{cases} n & \text{if } d_{\tau-j} = d_{\tau-i}, \text{ i.e. if } i = j,\\ 0 & \text{otherwise} \end{cases}.\end{aligned}$$

The same equality with $(\mathscr{R}'_n \cdot \mathscr{R}_n)_{ij}$ is also true, which gives the result.

(2) The equality is obvious since $\mathscr{R}_n$ is obtained from $\mathscr{R}'_n$ by an even number of permutations of rows and columns.

(3) From (1) and (2), we have $n^\tau = \det(nI) = \det(\mathscr{R}_n \cdot \mathscr{R}'_n) = (\det \mathscr{R}_n)^2$. □

4. The number of $\mathscr{C}$-partitions modulo *n*

Let us fix a positive integer n as well as a nonempty subset $\mathscr{C}$ of $\{0, 1, \ldots, n-1\}$. We define $p_n(m, \mathscr{C})$ to be the number of $\mathscr{C}$-partitions of m modulo n:

$$p_n(m, \mathscr{C}) = |\{x_1 + \cdots + x_k = m \text{ is a } \mathscr{C}\text{-partition of } m \bmod n\}|.$$

The multiplicative group of units in $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$, acts naturally by multiplication on $\mathbb{Z}/n\mathbb{Z}$. Interestingly, it also acts on the set of all $\mathscr{C}$-partitions in $\mathbb{Z}/n\mathbb{Z}$. Suppose $x_1 + x_2 + \cdots + x_k = m$ is a $\mathscr{C}$-partition of *m*. Then clearly for any $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $ax_1 + ax_2 + \cdots + ax_k = am$ is a $\mathscr{C}$-partition of *am*, as defined in the introduction. In other words, if S_m is the set of $\mathscr{C}$-partitions of *m*, one has

$$aS_m = \{ax_1 + \cdots + ax_k = am \mid x_1 + \cdots + x_k = m \text{ is a } \mathscr{C}\text{-partition of } m\}$$

and

$$aS_m = S_{am}.$$

This yields the following fact for m and m' in $\mathbb{Z}/n\mathbb{Z}$: if there exists an $a \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $am = m'$, then $p_n(m, \mathscr{C}) = p_n(m', \mathscr{C})$. Thus, the action of $(\mathbb{Z}/n\mathbb{Z})^*$ on $\mathbb{Z}/n\mathbb{Z}$ will be a crucial point in the following. The equivalence relation on $\mathbb{Z}/n\mathbb{Z}$ induced by this action is the point of the next lemma, the proof of which is left to the reader.

Lemma 9. (1) *In $\mathbb{Z}/n\mathbb{Z}$, two elements m and $\widetilde{m}$ are equivalent under the action of $(\mathbb{Z}/n\mathbb{Z})^*$ if and only if $(m, n) = (\widetilde{m}, n)$.*
(2) *For all $m \in \mathbb{Z}/n\mathbb{Z}$, there exists a unique $d|n$ such that d and m are in the same equivalence class.*

Lemma 9 shows that in order to solve Problem 3, it is sufficient to compute $p_n(d, \mathscr{C})$ for all $d|n$ since

$$p_n(m, \mathscr{C}) = p_n(d, \mathscr{C}) \quad \text{with } d = (m, n). \tag{4.1}$$

Here is the main theorem:

Theorem 10. *Let n be a positive integer, m an element of $\mathbb{Z}/n\mathbb{Z}$, $a=(m,n)$, and $\mathscr{C}$ a nonempty subset of* $\{0,1,\dots,n-1\}$. *Given $d|n$, let*

$$a_k = |\{c \in \mathscr{C} \mid cd = k \bmod n\}|$$

and

$$\varepsilon_d = \frac{1}{|\mathscr{C}|}\ \det\ \mathrm{Circ}_n[a_0,\dots,a_{n-1}].$$

Then the number of $\mathscr{C}$-partitions of m in $\mathbb{Z}/n\mathbb{Z}$ is given by

$$\begin{aligned} p_n(m,\mathscr{C}) &= \frac{1}{n}\sum_{d|n} C(a,d)\varepsilon_{n/d} \\ &= \frac{1}{n}\sum_{d|n} \frac{\varphi(d)\mu(\frac{d}{(a,d)})}{\varphi(\frac{d}{(a,d)})}\varepsilon_{n/d}. \end{aligned}$$

Proof. For a fixed $d \mid n$, let a_k be as above. Using Proposition 5, we have

$$\begin{aligned} \det\ \mathrm{Circ}_n[a_0,\dots,a_{n-1}] &= \prod_{j=0}^{n-1}\left(\sum_{c\in\mathscr{C}} \zeta_n^{cdj}\right) \\ &= |\mathscr{C}|\prod_{j=1}^{n-1}\left(\sum_{c\in\mathscr{C}} \zeta_n^{cdj}\right) \\ &= |\mathscr{C}|\left(\sum_{\substack{i_j\in\mathscr{C}\\ j=1,\dots,n-1}} (\zeta_n)^{d(1i_1+2i_2+\cdots+(n-1)i_{n-1})}\right). \end{aligned} \tag{4.2}$$

Let $\mathscr{C}=\{c_1,c_2,\dots,c_r\}$ and let us fix notation: for any finite subset L of $\mathbb{N}$, we define $\|L\| = \sum_{l\in L} l$ (and $\|\emptyset\|=0$). If for each term $(\zeta_n)^{d(1i_1+2i_2+\cdots+(n-1)i_{n-1})}$ of 4.4 we define

$$L_j = \{x \in \{1,2,\dots,n-1\} \mid i_x = c_j\},$$

then the above summation can be written as a sum over all possible disjoint unions in

$$U = \{L=(L_1,\dots,L_r) \mid L_1 \sqcup \cdots \sqcup L_r = \{1,2,\dots,n-1\}\}$$

as

$$\det\ \mathrm{Circ}_n[a_0,\dots,a_{n-1}] = |\mathscr{C}|\left(\sum_{L\in U} (\zeta_n)^{d(c_1\|L_1\|+c_2\|L_2\|+\cdots+c_r\|L_r\|)}\right).$$

For all L in U, let us write $\mu(L) = c_1\|L_1\| + c_2\|L_2\| + \cdots + c_r\|L_r\| \bmod n$. Note that the set $\{L \in U \mid \mu(L) = m\}$ is in bijection with the set of $\mathscr{C}$-partitions of m. Thus

$$\begin{aligned}
\det \operatorname{Circ}_n[a_0,\ldots,a_{n-1}] &= |\mathscr{C}| \left(\sum_{m=0}^{n-1} \left(\sum_{\substack{L\in U \\ \mu(L)=m}} 1 \right) (\zeta_n)^{dm} \right) \\
&= |\mathscr{C}| \left(\sum_{m=0}^{n-1} p_n(m,\mathscr{C})(\zeta_n)^{dm} \right) \\
&= |\mathscr{C}| \left(\sum_{l|n} p_n(l,\mathscr{C}) \underbrace{\left(\sum_{\substack{(m,n)=l, \\ 1\leqslant m\leqslant n}} (\zeta_n)^{dm} \right)}_{\text{c.f. } 3.2} \right) \\
&= |\mathscr{C}| \left(\sum_{l|n} p_n(l,\mathscr{C}) C(d, n/l) \right), \qquad (4.3)
\end{aligned}$$

where Eq. (4.1) has been used in (4.3). In other words, for each divisor d of n, we have the following equation:

$$\sum_{l|n} C(d, n/l) p_n(l,\mathscr{C}) = \frac{1}{|\mathscr{C}|} \det \operatorname{Circ}_n[a_0,\ldots,a_{n-1}] = \varepsilon_d.$$

When d goes through all divisors of n, we obtain the following system of linear equations:

$$\begin{bmatrix} C(d_1,d_1) & C(d_1,d_2) & C(d_1,d_3) & \ldots & C(d_1,d_\tau) \\ C(d_2,d_1) & C(d_2,d_2) & C(d_2,d_3) & \ldots & C(d_2,d_\tau) \\ C(d_3,d_1) & C(d_3,d_2) & C(d_3,d_3) & \ldots & C(d_3,d_\tau) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C(d_\tau,d_1) & C(d_\tau,d_2) & C(d_\tau,d_3) & \ldots & C(d_\tau,d_\tau) \end{bmatrix} \begin{bmatrix} p_n(n/d_1,\mathscr{C}) \\ p_n(n/d_2,\mathscr{C}) \\ p_n(n/d_3,\mathscr{C}) \\ \vdots \\ p_n(n/d_\tau,\mathscr{C}) \end{bmatrix} = \begin{bmatrix} \varepsilon_{d_1} \\ \varepsilon_{d_2} \\ \varepsilon_{d_3} \\ \vdots \\ \varepsilon_{d_\tau} \end{bmatrix}.$$

This system can now easily be solved since the matrix on the left-hand-side is $\mathscr{R}_n$ which possesses the inverse $\frac{1}{n}\mathscr{R}'_n$ by Proposition 8. Thus

$$\begin{bmatrix} p_n(n/d_1,\mathscr{C}) \\ p_n(n/d_2,\mathscr{C}) \\ p_n(n/d_3,\mathscr{C}) \\ \vdots \\ p_n(n/d_\tau,\mathscr{C}) \end{bmatrix} = \frac{1}{n} \begin{bmatrix} C(n/d_1,n/d_1) & C(n/d_1,n/d_2) & \ldots & C(n/d_1,n/d_\tau) \\ C(n/d_2,n/d_1) & C(n/d_2,n/d_2) & \ldots & C(n/d_2,n/d_\tau) \\ C(n/d_3,n/d_1) & C(n/d_3,n/d_2) & \ldots & C(n/d_3,n/d_\tau) \\ \vdots & \vdots & \ddots & \vdots \\ C(n/d_\tau,n/d_1) & C(n/d_\tau,n/d_2) & \ldots & C(n/d_\tau,n/d_\tau) \end{bmatrix} \begin{bmatrix} \varepsilon_{d_1} \\ \varepsilon_{d_2} \\ \varepsilon_{d_3} \\ \vdots \\ \varepsilon_{d_\tau} \end{bmatrix}.$$

Thus, replacing all the n/d_i with d_i, together with Eq. (4.1), we have shown that

$$p_n(m,\mathscr{C}) = p_n(a,\mathscr{C}) = \frac{1}{n} \sum_{d|n} C(a,d)\varepsilon_{n/d}.$$

This ends the proof of the theorem. □

Example 11. Let $n = 15$, $D_{15} = \{1, 3, 5, 15\}$, and $\mathscr{C} = \{0, 1, 2, 5\}$. We get

$$\begin{aligned}
\varepsilon_1 &= \tfrac{1}{4} \det \operatorname{Circ}_{15}[1,1,1,0,0,1,0,0,0,0,0,0,0,0,0] = 341, \\
\varepsilon_3 &= \tfrac{1}{4} \det \operatorname{Circ}_{15}[2,0,0,1,0,0,1,0,0,0,0,0,0,0,0] = 21296, \\
\varepsilon_5 &= \tfrac{1}{4} \det \operatorname{Circ}_{15}[1,0,0,0,0,1,0,0,0,0,2,0,0,0,0] = 256, \\
\varepsilon_{15} &= \tfrac{1}{4} \det \operatorname{Circ}_{15}[4,0,0,0,0,0,0,0,0,0,0,0,0,0,0] = 4^{14} = 268435456
\end{aligned}$$

and

$$\begin{bmatrix} p_{15}(15,\mathscr{C}) \\ p_{15}(5,\mathscr{C}) \\ p_{15}(3,\mathscr{C}) \\ p_{15}(1,\mathscr{C}) \end{bmatrix} = \frac{1}{15}\begin{bmatrix} C(15,15) & C(15,5) & C(15,3) & C(15,1) \\ C(5,15) & C(5,5) & C(5,3) & C(5,1) \\ C(3,15) & C(3,5) & C(3,3) & C(3,1) \\ C(1,15) & C(1,5) & C(1,3) & C(1,1) \end{bmatrix}\begin{bmatrix} \varepsilon_1 \\ \varepsilon_3 \\ \varepsilon_5 \\ \varepsilon_{15} \end{bmatrix}$$

$$= \frac{1}{15}\begin{bmatrix} 8 & 4 & 2 & 1 \\ -4 & 4 & -1 & 1 \\ -2 & -1 & 2 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 341 \\ 21296 \\ 256 \\ 268435456 \end{bmatrix},$$

which gives

$$p_{15}(m,\mathscr{C}) = \begin{cases} 17901592 & \text{if } m = 0, \\ 17901268 & \text{if } m \in \{3,6,9,12\}, \\ 17894266 & \text{if } m \in \{5,10\}, \\ 17894283 & \text{if } m \in \{1,2,4,7,8,11,13,14\}. \end{cases}$$

5. Partitions modulo *n* with less than *t* repetitions

When $\mathscr{C} = \{0,1,2,\ldots,t-1\}$, the $\mathscr{C}$-partitions are partitions where less than t repetitions of summands are allowed. In this section, we give explicit formulas for the number of such partitions and give some examples.

Corollary 12. *Let n be a positive integer, m an element of $\mathbb{Z}/n\mathbb{Z}$, $a = (m,n)$, and $\mathscr{C} = \{0,1,\ldots,t-1\}$. The number of $\mathscr{C}$-partitions of m in $\mathbb{Z}/n\mathbb{Z}$, i.e., the number of partitions of m with less than t repetitions of summands is given by*

$$p_n(m,\{0,1,\ldots,t-1\}) = \frac{1}{n}\sum_{\substack{d|n \\ (d,t)=1}} C(a,d)t^{n/d-1}$$

$$= \frac{1}{n}\sum_{\substack{d|n \\ (d,t)=1}} \frac{\varphi(d)\mu(\frac{d}{(a,d)})}{\varphi(\frac{d}{(a,d)})}t^{n/d-1}.$$

Proof. Theorem 10 and Proposition 5 show that

$$t\varepsilon_d = \prod_{j=0}^{n-1}\left(\sum_{k=0}^{t-1}(\zeta_n)^{kdj}\right) = \prod_{j=0}^{n-1}\left(\sum_{k=0}^{t-1}(\zeta_{n/d})^{kj}\right).$$

Using Lemma 4, we see that

$$\varepsilon_d = \begin{cases} t^{d-1} & \text{if } (t,n/d) = 1, \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

Example 13. Let us consider the case when $n = q$ is prime. We have $D_q = \{1,q\}$ and the above formula becomes

$$p_q(m,\{0,1,\ldots,t-1\}) = \begin{cases} \frac{t^{q-1}-1+q}{q} & \text{if } t < q,\ m = 0, \\ \frac{t^{q-1}-1}{q} & \text{if } t < q,\ m \neq 0, \\ q^{q-2} & \text{if } t = q. \end{cases}$$

Note that for all possible $t \in \{2,\ldots,q-1\}$ the numbers given by the formula are integers because of Fermat's little Theorem.

Corollary 14. *Let n be a positive integer, m an element of $\mathbb{Z}/n\mathbb{Z}$, and $a = (m, n)$. The number of partitions of m in $\mathbb{Z}/n\mathbb{Z}$ in distinct summands is given by*

$$p_n(m, \{0, 1\}) = \frac{1}{n} \sum_{\substack{d|n \\ d:odd}} C(a, d)2^{n/d-1}$$

$$= \frac{1}{n} \sum_{\substack{d|n \\ d:odd}} \frac{\varphi(d)\mu(\frac{d}{(a,d)})}{\varphi(\frac{d}{(a,d)})} 2^{n/d-1}.$$

Example 15. Let $n = 2^t$. In this case $D_n = \{1, \text{even numbers}\}$ and the above formula becomes

$$p_{2^t}(m, \{0, 1\}) = \frac{2^{n-1}}{n} = 2^{2^t-t-1} \quad \forall m \in \mathbb{Z}_{2^t},$$

since there is only one term in the sum.

Acknowledgements

I would like to thank Professor Joachim Rosenthal and the anonymous referees for their helpful comments.

References

[1] S. Ahlgren, K. Ono, Addition and Counting: the Arithmetic of Partitions, Notice of the AMS, vol. 48(9), 2001, pp. 978–984.
[2] G. Andrews, The Theory of Partitions, Addison-Wesley Publishing, Reading, MA, 1976.
[3] E. Cohen, An extension of Ramanujan's sums. II. Additive properties, Duke Mat. J. 22 (1955) 543–550.
[4] P.J. Davis, Circulant Matrices, Pure and Applied Mathematics, Wiley Interscience Publications, New York, 1979.
[5] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, fifth ed., Oxford Science Publication, Oxford, 1979.