JOURNAL OF RESEARCH of the National Bureau of Standards — Mathematical Sciences Vol. 74B, No. 1, January–March 1970

An Enumeration Problem for a Congruence Equation*

Richard A. Brualdi and Morris Newman**

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(September 9, 1969)

It is shown that the number of n-tuples $(x_0, x_1, \ldots, x_{n-1})$ of nonnegative integers such that

$$\sum_{i=0}^{n-1} x_i = n,$$

$$\sum_{i=0}^{n-1} ix_i \equiv 0 \bmod n,$$

is given by

$$\frac{1}{n}\sum_{d|n}\binom{2d-1}{d}\varphi\left(\frac{n}{d}\right).$$

Key words: Circulants; congruences; permanents.

1. Introduction

In 1952 M. Hall, Jr. proved the following theorem [1] (see footnote 1): If G is a finite abelian group of order n with elements $a_1, a_2, \ldots, a_n$, and $c_1, c_2, \ldots, c_n$ are n (not necessarily distinct) elements of G, then there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that the differences $a_{\sigma(1)}-a_1, a_{\sigma(2)}-a_2, \ldots, a_{\sigma(n)}-a_n$ are $c_1, c_2, \ldots, c_n$ in some order, if and only if

$$\sum_{i=1}^{n} c_i = 0. \tag{1}$$

The necessity of (1) is trivial, and Hall gives an elegant proof that condition (1) implies the existence of such a permutation σ. If G is the cyclic group of order n, then Hall's theorem may be rephrased in terms of congruences as follows: Let $x_0, x_1, \ldots, x_{n-1}$ be n nonnegative integers with

$$\sum_{i=0}^{n-1} x_i = n.$$

Then there is a permutation σ of $\{1, 2, \ldots, n\}$ such that

$$\sigma(i) - i \equiv k \qquad (\text{mod } n)$$

has exactly x_k solutions in i, $1 \leq i \leq n$, for each $k = 0, 1 \ldots, n-1$ if and only if

$$0x_0 + 1x_1 + \ldots + (n-1)x_{n-1} \equiv 0 \ (\text{mod } n). \tag{2}$$

*Partially supported by N.S.F. Grant No. GP-7073.

**Present address: Department of Mathematics, University of Wisconsin, Madison, Wis. 53706.

[1] M. Hall, Jr., A Combinatorial Problem on Abelian Groups, Proc. A. M. S. 584 – 587 (1952).

The purpose of this note is to count the number of solutions of (2) in nonnegative integers x_i with $\sum_{i=0}^{n-1} x_i=n$. An application to the permanent of a circulant is given.

2. Main Result

The motivation having been given, we may now state and prove our main result.

THEOREM: *Let* n *be a positive integer. Let* F(n) *be the number of n-tuples* $(x_0, x_1, \ldots, x_{n-1})$ *satisfying:*

$$x_i \geqslant 0, (i=0, 1, \ldots, n-1),$$

$$\sum_{i=0}^{n-1} x_i = n,$$

$$\sum_{i=0}^{n-1} i x_i \equiv 0 \pmod{n}.$$

Then

$$F(n)=\frac{1}{n}\sum_{d|n}\binom{2d-1}{d}\varphi\left(\frac{n}{d}\right),$$

where the summation extends over all positive integers d *dividing* n, *and where* φ *is Euler's function.*

PROOF: The proof uses generating functions. Define

$$f_n(w, z)=[(1-z)(1-wz)\ \ldots\ (1-w^{n-1}z)]^{-1}.$$

Then

$$f_n(w, z)=\left(\sum_{k=0}^{\infty} z^k\right)\left(\sum_{k=0}^{\infty} w^k z^k\right)\ \ldots\ \left(\sum_{k=0}^{\infty} w^{k(n-1)}z^k\right),$$

and it is clear that $F(n)$ is the sum of the coefficients of $z^n w^{nt}$, $0 \leqslant t \leqslant n-1$, in $f_n(w, z)$. Write

$$f_n(w, z)=\sum_{k=0}^{\infty} B_k z^k \qquad (B_k=B_k(n, w)).$$

Then because

$$f_{n+1}(w, z)=\frac{f_n(w, z)}{1-w^n z},$$

and

$$f_n(w, wz)=[(1-wz)(1-w^2z)\ \ldots\ (1-w^n z)]^{-1},$$

we obtain

$$f_n(w, wz)=(1-z)f_{n+1}(w, z)=\frac{1-z}{1-w^n z}f_n(w, z).$$

Thus

$$\sum_{k=0}^{\infty} B_k w^k z^k=\frac{1-z}{1-w^n z}\sum_{k=0}^{\infty} B_k z^k,$$

so that

$$\sum_{k=0}^{\infty} B_k w^k z^k-\sum_{k=0}^{\infty} B_k w^{n+k} z^{k+1}=\sum_{k=0}^{\infty} B_k z^k-\sum_{k=0}^{\infty} B_k z^{k+1}.$$

Hence for $k \geqslant 1$,

$$B_k w^k - B_{k-1} w^{n+k-1}=B_k-B_{k-1},$$

or

$$B_k=\frac{1-w^{n+k-1}}{1-w^k}B_{k-1} \qquad (k \geqslant 1).$$

Thus since $B_0=1$,

$$B_k=\prod_{r=1}^{k}\frac{1-w^{n+r-1}}{1-w^r} \qquad (k\geq 0),$$

an empty product being 1. Therefore

$$f_n(w,z)=\sum_{k=0}^{\infty}\left\{\prod_{r=1}^{k}\frac{1-w^{n+r-1}}{1-w^r}\right\}z^k,$$

and $F(n)$ is the sum of the coefficients of w^{nt}, $0\leq t\leq n-1$, in

$$g_n(w)=\prod_{r=1}^{n}\frac{1-w^{n+r-1}}{1-w^r}=\prod_{r=1}^{n-1}\frac{1-w^{n+r}}{1-w^r}.$$

Now, $g_n(w)$ is a polynomial in w of degree $\sum_{r=1}^{n-1}\{n+r-r\}=n(n-1)$, and has nonnegative coefficients (since $f_n(w,z)$ has nonnegative coefficients). Since

$$\sum_{\zeta:\zeta^n=1}\zeta^k=\begin{cases} n, \text{ if } n \text{ divides } k\\ 0, \text{ otherwise}\end{cases}$$

we have

$$nF(n)=\sum_{\zeta:\zeta^n=1}g_n(\zeta),$$

the summations extending over all nth roots of unity.

Suppose now that ζ is a primitive dth root of unity, where $d|n$. Since

$$\lim_{w\to\zeta}\frac{1-w^{n+r}}{1-w^r}=\begin{cases}\dfrac{n+r}{r}, \text{ if } d \text{ divides } r\\ 1, \text{ otherwise}\end{cases}$$

we have that

$$g_n(\zeta)=\prod_{\substack{1\leq r\leq n-1\\ r\equiv 0 \bmod d}}\frac{n+r}{r}=\prod_{s=1}^{\frac{n}{d}-1}\frac{n+sd}{sd}=\binom{2\frac{n}{d}-1}{\frac{n}{d}}.$$

Therefore, since there are $\varphi(d)$ nth roots of unity which are primitive dth roots of unity,

$$F(n)=\frac{1}{n}\sum_{d|n}\binom{2\frac{n}{d}-1}{\frac{n}{d}}\varphi(d)$$

$$=\frac{1}{n}\sum_{d|n}\binom{2d-1}{d}\varphi\left(\frac{n}{d}\right).$$

This proves the theorem.

3. An Application

Let $A=[a_{ij}]$ be an $n\times n$ matrix. If σ is a permutation of $\{1, 2, \ldots, n\}$ then

$$a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$

is called a *diagonal product* of A. The *permanent* of A, denoted by per (A), is the sum of the diagonal products of A. Thus

$$\text{per}\ (A)=\sum_{\sigma} a_{1\sigma(1)}a_{2\sigma(2)}\ .\ .\ .\ a_{n\sigma(n)},$$

the summation extending over all permutations of $\{1, 2, \ldots, n\}$. Suppose A is the n by n circulant

$$\begin{bmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \cdot & \cdot & & \cdot \\ a_1 & a_2 & \ldots & a_0 \end{bmatrix}.$$

Then the diagonal product $a_{1\sigma(1)}a_{2\sigma(2)}\ .\ .\ .\ a_{n\sigma(n)}$ equals $a_0^{x_0}a_1^{x_1}\ .\ .\ .\ a_{n-1}^{x_{n-1}}$ where x_k is the number of integers i, $1 \leq i \leq n$, such that $\sigma(i)-i\equiv k \pmod{n}$.

By Hall's theorem, if $x_0, x_1, \ldots, x_{n-1}$ are integers satisfying the hypothesis of the theorem, then $a_0^{x_0}a_1^{x_1}\ .\ .\ .\ a_{n-1}^{x_{n-1}}$ is a diagonal product of the circulant A. Thus we have the following corollary.

COROLLARY: *The number of formally distinct diagonal products of an* n *by* n *circulant is given by*

$$\frac{1}{\mathrm{n}}\sum_{\mathrm{d}|\mathrm{n}}\binom{2\mathrm{d}-1}{\mathrm{d}}\varphi\left(\frac{\mathrm{n}}{\mathrm{d}}\right).$$

Some other results on the permanent of a circulant are given by the authors in the reference below.[2]

(Paper 74B1–315)

---

[2] R. A. Brualdi and M. Newman, Some Theorems on the Permanent, J. Res. Nat. Bur. Stand. (U.S.), 69B (Math. Sci.) No. 3, 159–163 (July–Oct. 1965).