PERMANENTS OF CYCLIC MATRICES

Dissertation

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of the Ohio State University

By

Marion Franklin Tinsley, B.S., M.A.

The Ohio State University

1957

Approved by:

Herbert J. Ryan
Adviser
Department of Mathematics
# TABLE OF CONTENTS

1. Introduction ........................................ 1
2. Representation of Cycles .......................... 3
3. Primitive Solutions ................................. 5
4. Some Properties of Primitive Solutions .............. 12
5. Applications .......................................... 24
6. The Main Theorem .................................... 31
1. Introduction. Let \( A = \left[ a_{ij} \right] \) be an \( nxn \) matrix composed of 0's and 1's with row and column sums equal to \( s \). Let \( \Sigma = \left[ \sigma_{ij} \right] \) be a permutation submatrix of \( A \). This means that \( \Sigma \) is a permutation matrix of order \( n \) such that \( \sigma_{k\ell} = 1 \) implies \( a_{k\ell} = 1 \). With \( \Sigma \) we associate a permutation \( \Sigma' \) of the letters 1, 2, \ldots, \( n \),

\[
(1.1) \quad \sigma_{ij} = 1 \text{ if and only if } \Sigma'(i) = j.
\]

Then the permanent of \( A \), written \( P(A) \), equals the absolute value of the determinant of \( A \), written \( |D(A)| \), if and only if every \( \Sigma' \) is even or else every \( \Sigma' \) is odd. The object of this paper is to determine for a certain class of \( A \), conditions for \( P(A) \) to equal \( |D(A)| \).

Now let the 0,1 matrix \( A \) be cyclic and written in the form

\[
A = \begin{bmatrix}
c_1 & c_2 & c_3 & \cdots & c_n \\
c_n & c_1 & c_2 & \cdots & c_{n-1} \\
c_2 & c_3 & \cdots & c_1
\end{bmatrix}.
\]

Then \( A = \prod_1 + \prod_2 + \ldots + \prod_s \), where the \( \prod_i \)'s are permutation matrices of order \( n \) and \( \prod_i' = (1,2,\ldots,n)^{d_i}, \ 0 \leq d_i < n(i = 1,2,\ldots,s) \). The \( d_i \)'s will be called differences and they in turn clearly define the \( nxn \) matrix \( A \). The non cyclic \( A \) also may be written as a sum of \( s \) permutation matrices by a theorem due to König (1). However, our results seem to hinge upon the special character of the \( \prod_i \)'s and the \( d_i \)'s.

If every integer 1, 2, \ldots, \( n-1 \) is congruent mod \( n \) to exactly one of the numbers \( d_j - d_k \) \((1 \leq j,k \leq s)\), then the \( d_i \)'s are said to form
a perfect difference set mod n. Difference sets have been used extensively in the study of cyclic projective planes and designs (2,3), but for the purposes of this paper we are interested only in the unique role played by the perfect difference sets Mod 7.

Without any loss of generality, the cyclic A may be written in the form

\[ A = \mathcal{P}_0 + \mathcal{P}_1 + \ldots + \mathcal{P}_{s-1}, \]

where \( \mathcal{P}_i = (1,2,\ldots, n) d_i, 0 < d_i < n (i=1,2,\ldots,s-1), \) and \( d_0 = 0. \)

Thus \( \mathcal{P}_0 \) is taken as the identity matrix I.

In section 2 the problem of determining if \( P(A) = |D(A)| \) is reduced to a study of the solutions of the linear congruence

\[ d_1 x_1 + d_2 x_2 + \ldots + d_{s-1} x_{s-1} \equiv 0 \pmod{n}. \]

In sections 3 and 4 we study these solutions and derive several results of combinatorial and number theoretic interest. In sections 5 and 6 we prove the main theorem of the paper:

Let \( s = 3 \) and A be of order n and defined by the differences \( 0, d_1, d_2. \) Then \( P(A) = |D(A)| \) if and only if for some positive integer \( e, n = 7e, d_1 = ed_1^1 \) and \( d_2 = ed_2^1 \) where \( 0, d_1^1, d_2^1 \) is a perfect difference set mod 7.

As corollaries, one obtains (1) If \( s \geq 4 \) then \( P(A) > |D(A)| \) and (2) If \( s = 3, P(A) = |D(A)| \) and \( n = 7e, \) then \( P(A) = 24^e. \)
2. Representation of Cycles. From now on we shall consider
only cyclic 0,1 matrices $A$. In the notation of section 1 let
$A = \Pi_0 + \Pi_1 + \ldots + \Pi_r$, where $\Pi_i = (1,2,\ldots,n)^{d_i}, 0 \leq d_i < n(i = 0,1,\ldots,r)$ and $d_0 = 0$. Let $\Sigma$ be a permutation submatrix of
$A$. Since $\Pi_0 = I$, a cycle of $\Sigma$ also corresponds to a permutation
submatrix of $A$. Thus $P(A) = |D(A)|$ if and only if all such cycles
are even.

Now, read mod $n$, a cycle must have the form
$a \rightarrow a + d_1 \rightarrow a + d_1 + d_2 \rightarrow \ldots \rightarrow a + d_1 + d_2 + \ldots + d_j$, where $j \leq n$,
and $d_1 + d_2 + \ldots + d_j \equiv 0 \pmod{n}$. Arrange the $d_i$'s in a circle:

Then no consecutive selection of $t$ of the $d_i$'s, $0 < t < j$, has a sum
divisible by $n$. Otherwise there would be a cycle within a cycle.

Conversely, let $d_{i_1}, d_{i_2}, \ldots, d_{i_j}$ be a sequence of the $d_i$'s
such that $d_{i_1} + d_{i_2} + \ldots + d_{i_j} \equiv 0 \pmod{n}, 0 < j \leq n$, and, when
arranged in a circle, no proper consecutive selection of the $d_{i_k}$'s
has a sum divisible by $n$.

Then for each $b=1,2,\ldots,n$, $b \rightarrow b + d_{i_1} \rightarrow b + d_{i_1} + d_{i_2} \rightarrow \ldots \rightarrow b + d_{i_1} + d_{i_2} + \ldots + d_{i_j}$
is a cycle.

Now for a cycle $a \rightarrow a + d_{i_1} \rightarrow a + d_{i_1} + d_{i_2} \rightarrow \ldots \rightarrow a + d_{i_1} + d_{i_2} + \ldots + d_{i_j}$
let $x_1$ denote the number of times that $d_1$ occurs among $d_{i_1}, d_{i_2}, \ldots, d_{i_j}$.
Then \( j = x_1 + x_2 + \ldots + x_r \) and

\[(2.1) \quad d_1 x_1 + d_2 x_2 + \ldots + d_r x_r \equiv 0 \pmod{n}.
\]

**Definition.** We say that the solution \((x_1, x_2, \ldots, x_r)\) of the congruence (2.1) represents a cycle of the matrix \(A\) defined by the differences \(0, d_1, d_2, \ldots, d_r\).

More precisely, if \((y_1, y_2, \ldots, y_r)\) is a solution of (2.1) and \(0 < y_1 + y_2 + \ldots + y_r \leq n\), then \((y_1, y_2, \ldots, y_r)\) represents a cycle provided there is a sequence \(d_{j_1}, d_{j_2}, \ldots, d_{j_k}\) containing exactly \(y_1 - d_1\)'s, \(y_2 - d_2\)'s, \ldots, \(y_r - d_r\)'s and no proper consecutive selection of the \(d_{j_i}\)'s contains exactly \(z_1\) \(d_1\)'s, \(z_2\) \(d_2\)'s, \ldots, \(z_r\) \(d_r\)'s where \((z_1, z_2, \ldots, z_r)\) is a solution of (2.1).

Note that if \((y_1, y_2, \ldots, y_r)\) represents a cycle then the cycle has length \(y_1 + y_2 + \ldots + y_r\) and hence is even or odd according as \(y_1 + y_2 + \ldots + y_r\) is odd or even. Thus to determine if \(P(A) = |D(A)|\) it suffices to study the solutions of (2.1).

**Example 1.** Let \(A\) be the 8x8 matrix

\[
\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]
\[ A = \pi_0' + \pi_1' + \pi_2' \text{ where } \pi_0' = 1, \quad \pi_1' = (1, 2, 3, 4, 5, 6, 7, 8) \text{ and } \pi_2' = (1, 2, 3, 4, 5, 6, 7, 8)^2. \] Thus \( d_0 = 0, \quad d_1 = 1 \) and \( d_2 = 2. \) The circled 1's constitute a permutation submatrix \( \Sigma^- \) and \( \Sigma'^- = (2)(4)(7)(3, 5, 6, 8, 1). \)

The cycle \( (3, 5, 6, 8, 1) \) has the form
\[ 3 \to 3 + d_2 \to 3 + d_2 + d_1 \to 3 + d_2 + d_1 + d_2 \to 3 + d_2 + d_1 + d_2 + d_1 \to 3 + d_2 + d_1 + d_2 + d_1 + d_2 = 3 \pmod{8}. \]
Thus \( x_1 = 2 \) and \( x_2 = 3. \)

3. **Primitive solutions.** In this section we consider the solutions \((x_1, x_2, \ldots, x_r)\) of the general congruence
\[ (3.1) \quad d_1 x + d_2 y + \ldots + d_r z \equiv 0 \pmod{n}, \]
where the only restrictions are that the \( d_i \)'s be positive integers and the \( x_i \)'s be non-negative integers. In succeeding sections we will assume that \( 0 < d_i < n, \)
\( 0 \leq x_i < n (i = 1, 2, \ldots, r), \) and that the \( d_i \)'s are distinct. For the present however, we need this more general formulation for the proof of Theorem 2.

The following definition is of great notational convenience.

Let \((z_1, z_2, \ldots, z_t)\) and \((z_1', z_2', \ldots, z_t')\) be real vectors. We write \((z_1, z_2, \ldots, z_t) \geq (z_1', z_2', \ldots, z_t')\) provided
\[ z_t \geq z_t' (i = 1, 2, \ldots, t), \text{ and } (z_1, z_2, \ldots, z_t) = (z_1', z_2', \ldots, z_t') \text{ if } z_i = z_i' (i = 1, 2, \ldots, t). \]

Furthermore, we write \((z_1, z_2, \ldots, z_t) > (z_1', z_2', \ldots, z_t')\) provided
$z_1 \geq z_1'(i=1,2,\ldots,t)$ and with equality not holding for at least one $i$.

Now let $(x_1, x_2, \ldots, x_r)$ be a solution of $(3.1)$ such that 

$0 < x_i (i = 1,2,\ldots,r)$.

**Definition.** We say $(x_1, x_2, \ldots, x_r)$ is primitive if for every solution $(y_1, y_2, \ldots, y_r)$ such that $(0,0,\ldots,0) \leq (y_1, y_2, \ldots, y_r) \leq (x_1, x_2, \ldots, x_r)$ either $(y_1, y_2, \ldots, y_r) = (0,0,\ldots,0)$ or $(y_1, y_2, \ldots, y_r) = (x_1, x_2, \ldots, x_r)$. We will now prove two theorems on primitive solutions which have both combinatorial and number theoretic interest.

**Theorem 1.** If $d_1 x_1 + d_2 x_2 + \ldots + d_r x_r \equiv 0 \pmod{n}$ and $(x_1, x_2, \ldots, x_r)$ is primitive, then $x_1 + x_2 + \ldots + x_r \leq n$.

**Proof:** Consider the following $x_1 + x_2 + \ldots + x_r$ terms:

$d_1x_1 + d_2x_2, \ldots, d_1x_1 + d_2x_1 + d_2x_2 + \ldots, d_1x_1 + d_2x_2 + \ldots + d_1x_2 + d_2(2), \ldots,$

$d_1x_1 + d_2x_2 + \ldots + d_r, d_1x_1 + d_2x_2 + \ldots + d_r(2), \ldots,$

$d_1x_1 + d_2x_2 + \ldots + d_r x_r$. If two of the terms are congruent mod $n$ then subtracting implies that $(x_1, x_2, \ldots, x_r)$ is not primitive. Thus all the terms are distinct mod $n$ and $x_1 + x_2 + \ldots + x_r \leq n$.

**Theorem 2.** Let $d_1, d_2, \ldots, d_r$ be positive integers and distinct mod $n$. If $0 < x_i < n (i = 1,2,\ldots,r)$, and $(x_1, x_2, \ldots, x_r)$ is a primitive solution of $(3.1)$ then

$x_1 + x_2 + \ldots + x_r < n.$
Proof: By number theory there is a $t$ such that

$$td_1 \equiv (n, d_1) \pmod{n}$$

and

$$t \equiv (n, d_1) \pmod{n}.$$ Since

$$td_1 \equiv (n, d_1) \pmod{n} \text{ we may suppose initially that } d_1 \text{ divides } n.$$ We assume that $x_1 + x_2 + \ldots + x_r = n$ and shall prove the theorem by contradicting the primitivity of $(x_1, x_2, \ldots, x_r)$. Since

$$(x_1, x_2, \ldots, x_r) \text{ is primitive, } n > d_1 x_1 > 0.$$ Now consider a set of $n - x_1$ terms

$$(3.2) \quad \left\{d_2 y_2^{(i)} + d_3 y_3^{(i)} + \ldots + d_r y_r^{(i)} \right\}, \quad (i = 1, 2, \ldots, n - x_1),$$

such that

$$1 \leq i < n - x_1,$$

$$d_2 y_2^{(i)} + d_3 y_3^{(i)} + \ldots + d_r y_r^{(i)} < (y_2^{(n-x)}, y_3^{(n-x)}, \ldots, y_r^{(n-x)}),$$

and

$$y_2^{(n-x)}, y_3^{(n-x)}, \ldots, y_r^{(n-x)} = x_2, x_3, \ldots, x_r.$$ Such sets exist since $d_2, d_2(2), \ldots, d_2 x_2, d_2 x_2 + d_3, \ldots, d_2 x_2 + d_3 x_3, \ldots, d_2 x_2 + d_3 x_3 + \ldots + d_r x_r$ is an example of one. Because of the primitivity of $(x_1, x_2, \ldots, x_r)$, none of the terms in the set is congruent to 0 mod $n$ and no two terms can be congruent mod $n$. Thus the number of terms in (3.2) congruent mod $n$ to a multiple of $d_1$ is at least

$$\frac{n}{d_1} - 1 - \left\lfloor n - 1 - (n - x_1) \right\rfloor = \frac{n}{d_1} - x_1.$$ Moreover, if a term in (3.2) is congruent mod $n$ to $kd_1$, $1 \leq k < \frac{n}{d_1}$, then
the primitivity implies $k \leq \frac{n}{d_1} - x_1$.

Hence each $kd_1$ ($k = 1, 2, \ldots, \frac{n}{d_1} - x_1$) is congruent mod $n$ to a term in the set. Thus for each $j = 1, 2, \ldots, \frac{n}{d_1} - x_1$, there is in the set a unique term

$$d_2x_2^{(j)} + \ldots + d_rx_r^{(j)} \equiv jd_1 \pmod{n}.$$ 

Finally, for these $\frac{n}{d_1} - x_1$ terms,

$$(3.3) \quad (x_2^{(l)}, \ldots, x_r^{(l)}) < (x_2^{(j)}, \ldots, x_r^{(j)}) < \ldots < (x_2^{(0)} - x_1, \ldots, x_r^{(0)} - x_1) = (x_2, \ldots, x_r).$$

For suppose $(x_2^{(k)}, \ldots, x_r^{(k)}) > (x_2^{(l)}, \ldots, x_r^{(l)})$ for some $k, l \leq \frac{n}{d_1} - x_1$. Then $d_2(x_2^{(k)} - x_2^{(l)}) + \ldots + d_r(x_r^{(k)} - x_r^{(l)}) \equiv kd_1 - (k+1)d_1 \equiv n-d_1 \pmod{n}$ and since $(x_2, \ldots, x_r) > (x_2^{(k)}, \ldots, x_r^{(k)}) - x_2^{(k)}, \ldots, x_r^{(k)})$ this would imply $n-d_1 < n-d_1 x_1$ and $x_1 = 0$. Since this contradicts the primitivity of $(x_1, x_2, \ldots, x_r)$, $(3.3)$ holds.

Now suppose for every $(z_2, z_3, \ldots, z_r)$ such that $(0, 0, \ldots, 0) < (z_2, z_3, \ldots, z_r) \leq (x_2, x_3, \ldots, x_r)$ and

$$d_2z_2 + d_3z_3 + \ldots + d_rz_r \equiv d_1 \pmod{n},$$

that

$$z_2 + z_3 + \ldots + z_r \leq d_1.$$ 

Then since for $1 \leq j < \frac{n}{d_1} - x_1$,

$$d_2(x_2^{(j)} - x_2^{(i)}) + d_3(x_3^{(j)} - x_3^{(i)}) + \ldots + d_r(x_r^{(j)} - x_r^{(i)}) \equiv d_1 \pmod{n},$$

For suppose $(x_2^{(k)}, \ldots, x_r^{(k)}) > (x_2^{(l)}, \ldots, x_r^{(l)})$ for some $k, l \leq \frac{n}{d_1} - x_1$. Then $d_2(x_2^{(k)} - x_2^{(l)}) + \ldots + d_r(x_r^{(k)} - x_r^{(l)}) \equiv kd_1 - (k+1)d_1 \equiv n-d_1 \pmod{n}$ and since $(x_2, \ldots, x_r) > (x_2^{(k)}, \ldots, x_r^{(k)}) - x_2^{(k)}, \ldots, x_r^{(k)})$ this would imply $n-d_1 < n-d_1 x_1$ and $x_1 = 0$. Since this contradicts the primitivity of $(x_1, x_2, \ldots, x_r)$, $(3.3)$ holds.
it follows that

\[(x_2^{(i)} - x_2^{(i)}) + (x_3^{(i)} - x_3^{(j)}) + \ldots + (x_r^{(j)} - x_r^{(j)}) \leq d_1.\]

But then \(\frac{(x_2^{(i)} - x_1^{(i)})}{x_2^{(i)}} + \ldots + x_r^{(i)} =\)

\[\left[ x_2^{(i)} + x_3^{(i)} + \ldots + x_r^{(i)} \right] + \left[ (x_2^{(i)} - x_2^{(i)}) + (x_3^{(i)} - x_3^{(i)}) + \ldots + (x_1^{(i)} - x_1^{(i)}) \right]
+ \left[ (x_2^{(i)} - x_2^{(i)}) + (x_3^{(i)} - x_3^{(i)}) + \ldots + (x_1^{(i)} - x_1^{(i)}) \right] + \ldots
+ \left[ (x_2^{(i)} - x_2^{(i)}) + \ldots + (x_r^{(i)} - x_r^{(i)}) \right] \leq\]

\[\left( \frac{n}{d_1} - x_1 \right) d_1 = n - d_1 x_1.\]

Thus \(n - x_1 = x_2 + x_3 + \ldots + x_r = x_2^{(i)} + x_3^{(i)} + \ldots + x_r^{(i)} \leq\)

\(n - d_1 x_1\) and \(d_1 = 1\). However, by taking the original set (3.2) of \(n - x_1\) terms as \(d_2, d_2(2), \ldots, d_2 x_2, d_2 x_2 + d_2, \ldots, d_2 x_2 + d_3 x_3, \ldots\), \(d_2 x_2 + d_3 x_3 + \ldots + d_r x_r\), we see by (3.3) that \(d_2\) must then also be 1.

But then \(d_1 = d_2 = 1\) contradicts the assumption that the \(d\)'s are different.

We may assume then that there is a \((z_2, z_3, \ldots, z_r)\) such that \((0, 0, \ldots, 0) < (z_2, z_3, \ldots, z_r) \leq (x_2, x_3, \ldots, x_r)\),

\(d_2 z_2 + d_3 z_3 + \ldots + d_r z_r \equiv d_1 \pmod{n}\) and \(z_2 + z_3 + \ldots + z_r > d_1\).

Now \(d_2 z_2 + d_3 z_3 + \ldots + d_r z_r \equiv 0 \pmod{d_1}\).

Not all of the \(z_i\)'s are 0 so that by Theorem 1 there is a

\((y_2, y_3, \ldots, y_r)\) such that \((0, 0, \ldots, 0) < (y_2, y_3, \ldots, y_r) < (z_2, z_3, \ldots, z_r)\)

and \(d_2 y_2 + d_3 y_3 + \ldots + d_r y_r \equiv 0 \pmod{d_1}\).
Now we have $d_2z_2 + d_3z_3 + \ldots + d_rz_r \equiv d_1$ (mod $n$) and by the primitivity of $x_1, x_2, \ldots, x_r$ we may write

$$d_2y_2 + d_3y_3 + \ldots + d_ry_r \equiv ud_1 \pmod{n}$$

for some $u$, $1 < u \leq \frac{n}{d_1} - x_1$.

But now take the original set (3.2) of $n - x_1$ terms as

$$d_2, d_2(2), \ldots, d_2y_2, d_2y_2 + d_3, d_2y_2 + d_3(2), \ldots, d_2y_2 + d_3y_3, \ldots,$$

$$d_2y_2 + d_3y_3 + \ldots + d_ry_r, d_2(y_2 + 1) + d_3y_3 + \ldots + d_ry_r,$$

$$d_2(y_2 + 2) + d_3y_3 + \ldots + d_ry_r, \ldots, d_2z_2 + d_3y_3 + \ldots + d_ry_r,$$

$$d_2z_2 + d_3(y_3 + 1) + d_4y_4 + \ldots + d_ry_r, \ldots, d_2z_2 + d_3z_3 + \ldots + d_ry_r,$$

$$d_2(z_2 + 1) + d_3z_3 + \ldots + d_ry_r, d_2(z_2 + 2) + d_3z_3 + \ldots + d_ry_r, \ldots,$$

$$d_2x_2 + d_3z_3 + \ldots + d_ry_r, \ldots, d_2x_2 + d_3x_3 + \ldots + d_ry_r.$$

The conclusion (3.3) is contradicted for this set so that $(x_1, x_2, \ldots, x_r)$ cannot be primitive.

Suppose the $d_i$'s are distinct positive integers and less than $n$. Theorem 1 then implies that primitive solutions represent cycles. However, a cycle need not be represented by a primitive solution.

**Example 2.** Consider the perfect difference set mod 7, $d_0 = 0, d_1 = 1, d_2 = 3$.

The solutions of $x + 3y \equiv 0 \pmod{7}$ are given in the table.
$(4,1)$ and $(1,2)$ are the primitive ones and so represent cycles. The solution $(2,4)$ will represent a cycle only if two 1's and four 3's can be arranged in a circle so that no consecutive three totals one 1 and two 3's. This is not possible so only $(4,1)$ and $(1,2)$ represent cycles.

Now let $A$ be the 0,1 matrix of order 7 defined by $d_0$, $d_1$, and $d_2$. Then for every permutation submatrix $\Sigma$ of $A$, the permutation $\Sigma'$ is even. Hence $P(A) = D(A)$.

The same conclusion holds for any perfect difference set mod 7, $0, d'_1, d'_2$.

Example 3. Modulo 13, $d_0 = 0, d_1 = 1, d_2 = 3, d_3 = 9$ is a perfect difference set.

The solutions of $x + 3y \equiv 0 \pmod{13}$ are as follows:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>
The first four solutions are primitive.

Two 1's and eight 3's cannot be arranged in a circle so that no consecutive five totals one 1 and four 3's. Thus (2,8) does not represent a cycle.

However, (5,7) does represent a cycle since an acceptable arrangement is

\[
\begin{array}{ccc}
3 & 1 & 3 \\
1 & 3 & 1 \\
3 & 1 & 3 \\
1 & 3 & 1 \\
\end{array}
\]

4. Some properties of primitive solutions. In this section we study the solutions of the congruence \( x + dy \equiv 0 \pmod{n} \), \( 0 < d < n \).

The first theorem, Theorem 3, gives an algorithmic determination of the primitive solutions.

Theorem 3. Let \( n \equiv n_1 \pmod{d} \) and \( d \equiv d_1 \pmod{n_1} \), where \( 0 \leq d_1 < n_1 < d < n \). If the primitive solutions of \( x' + d_1y' \equiv 0 \pmod{n_1} \)
are those solutions for which \( y' = i, j, k, \ldots \), then the primitive solutions of \( x + dy \equiv 0 \pmod{n} \) are those solutions for which

\[
y = 1, 2, \ldots, \left[ \frac{n}{d} \right], \left[ \left\lfloor \frac{1}{d} \right\rfloor + 1 \right] \left[ \frac{n}{d} \right], \left[ \left\lceil \frac{1}{d} \right\rceil + 1 \right] \left[ \frac{n}{d} \right], \ldots.
\]

If \( n \equiv 0 \pmod{d} \), then the primitive solutions of \( x + dy \equiv 0 \pmod{n} \) are those solutions with \( y = 1, 2, \ldots, \frac{n}{d} - 1 \).

**Proof:** Clearly the solutions of \( x + dy \equiv 0 \pmod{n} \) with \( y = 1, 2, \ldots, \left[ \frac{n}{d} \right] - 1 \) are primitive, since as \( y \) increases the corresponding \( x \) decreases. If \( n \) is divisible by \( d \) then these are all the primitive solutions. If \( n \not\equiv 0 \pmod{d} \) then the solution with \( y = \left[ \frac{n}{d} \right] \) is also primitive. If, in addition, \( d_1 = 0 \) then \( n_1 \) is the greatest common divisor of \( n \) and \( d \), and \( \left( n_1, \left[ \frac{n}{d} \right] \right) \) is a primitive solution of \( x + dy \equiv 0 \pmod{n} \). Moreover, if \( (x_0, y_0) \) is another solution and \( y_0 > \left[ \frac{n}{d} \right] \), then \( (x_0, y_0) \) is not primitive since \( x_0 \) must be a multiple of \( n_1 \). Thus in proving the theorem, both \( n_1 \) and \( d_1 \) may be supposed not zero.

Assume now that \( \left[ \frac{n}{d} \right] < v \neq \left[ \frac{jn}{d} \right] \), \( i = 1, 2, \ldots, d-1 \). Let \((x_1, y_1)\) be the solution of \( x + dy \equiv 0 \pmod{n} \) with \( y_1 = v \). Then there is a solution \((x', y')\) where \((0,0) < (x', y') < (x_1, y_1)\) and

\[
y' = \left[ \frac{jn}{d} \right] \quad \text{for some } j, 1 \leq j \leq d-1.
\]

To show this let \( j \) be such that \( \left[ \frac{jn}{d} \right] < v < \left[ \frac{(j+1)n}{d} \right] \). Since \( \left[ \frac{n}{d} \right] \leq \left[ \frac{(j+1)n}{d} \right] - \left[ \frac{jn}{d} \right] \leq \left[ \frac{n}{d} \right] + 1 \), we have \( v = \left[ \frac{jn}{d} \right] + r \), \( r 
eq 0 \).
Then \( x_1 = (j+1)n - \left( \left\lfloor \frac{jn}{d} \right\rfloor + r \right) d \). Now the \( x' \) corresponding to \( y' = \left\lfloor \frac{jn}{d} \right\rfloor \) is \( jn - \left\lfloor \frac{jn}{d} \right\rfloor d \). Thus if we set \( x' = jn - \left\lfloor \frac{jn}{d} \right\rfloor d \) and \( y' = \left\lfloor \frac{jn}{d} \right\rfloor \), then

\[
x_1 - x' = \left\{ (j+1)n - \left( \left\lfloor \frac{jn}{d} \right\rfloor + r \right) d \right\} - \left\{ jn - \left\lfloor \frac{jn}{d} \right\rfloor d \right\} = n - rd > n - \left\lfloor \frac{n}{d} \right\rfloor \geq 0
\]

and \((x', y') < (x_1, y_1)\). As a consequence, to determine the primitive solutions of the congruence \( x + dy \equiv 0 \pmod{n} \) it suffices to consider those solutions with \( y = \left\lfloor \frac{in}{d} \right\rfloor \), \( i = 1, 2, \ldots, d-1 \).

**Lemma 1.** If \( 0 \leq a_i < d < n \) \( (i = 1, 2, \ldots, d-1) \) then

1) \( in \equiv a_i \pmod{d} \) if and only if \( a_i + d \left\lfloor \frac{in}{d} \right\rfloor \equiv 0 \pmod{n} \).

For \( 0 \leq a_i < d < n \) and \( in \equiv a_i \pmod{d} \) \( (i = 1, 2, \ldots, d-1) \),

2) \( x_0 = a_g, y_0 = \left\lfloor \frac{gn}{d} \right\rfloor \) is a primitive solution of \( x + dy \equiv 0 \pmod{n} \) if and only if \( a_1, a_2, \ldots, a_g \) are all \( a_i > 0 \).

**Proof:** 1) **Necessity.** If \( in \equiv a_i \pmod{d} \) then

\[
in = a_i + u_1 d \quad \text{for some } u_1, \quad a_i = \frac{in - a_i}{d} = \left\lfloor \frac{in}{d} \right\rfloor.
\]

Substituting \( \left\lfloor \frac{in}{d} \right\rfloor \) for \( u_1 \), \( a_i + d \left\lfloor \frac{in}{d} \right\rfloor = in \equiv 0 \pmod{n} \).

**Sufficiency.** If \( a_i + d \left\lfloor \frac{in}{d} \right\rfloor \equiv 0 \pmod{n} \) then since

\[
in \geq d \left\lfloor \frac{in}{d} \right\rfloor > (i-1)n, \quad \text{we have } a_i + d \left\lfloor \frac{in}{d} \right\rfloor = in. \quad \text{Thus } in \equiv a_i \pmod{d}.\]
2) **Necessity.** Let \( x_0 = a_g, y_0 = \left\lfloor \frac{kn}{d} \right\rfloor \) be a primitive solution of \( x + dy \equiv 0 \pmod{n} \) and \( x', y' \) another solution. If \( 0 < y' < y_0 \), then we must have \( x' > x_0 \). Thus for \( y' = \left\lfloor \frac{jn}{d} \right\rfloor \) (\( j = 1, 2, \ldots, g-1 \)), \( a_j = x' > x_0 = a_g \).

**Sufficiency.** If \( (x_0, y_0) \) is not primitive then there is a solution \( (x_1, y_1) \) such that \( (0, 0) < (x_1, y_1) < (x_0, y_0) \). If now \( y_1 > \left\lfloor \frac{n}{d} \right\rfloor \), then by the earlier remarks of this section there is a solution \( (x', y') \) such that \( (0, 0) < (x', y') \leq (x_1, y_1) \) and \( y' = \left\lfloor \frac{jn}{d} \right\rfloor \) for some \( j, 1 \leq j \leq d-1 \).

Since \( y' < y_0 \) we have \( j < g \). But also since \( x' \leq x_0 \), we have \( a_j \leq a_g \).

If \( y_1 \leq \left\lfloor \frac{n}{d} \right\rfloor \), then \( a_1 < x_1 \) so \( a_1 < y_0 = a_g \) and \( 1 < g \).

In either case we contradict \( a_1, a_2, \ldots, a_{g-1} > a_g \).

Now consider the following table of values defined for each \( k = 0, 1, 2, \ldots, n_1 - 1 \).

\[
\begin{array}{cc}
\left( \left\lfloor \frac{kd}{n_1} \right\rfloor + 1 \right) n_1 - kd & \left( \left\lfloor \frac{kd}{n_1} \right\rfloor + 1 \right) n_1 - kd \\
\left( \left\lfloor \frac{kd}{n_1} \right\rfloor + 2 \right) n_1 - kd & \left( \left\lfloor \frac{kd}{n_1} \right\rfloor + 2 \right) n_1 - kd \\
& \vdots \\
\left( \left\lfloor \frac{(k+1)d}{n_1} \right\rfloor \right) n_1 - kd & \left( \left\lfloor \frac{(k+1)d}{n_1} \right\rfloor \right) n_1 - kd \\
\end{array}
\]

It follows readily that for the \( a_i \) of Lemma 1, \( a_1 \equiv \text{in} \equiv \text{in}_1 \equiv b_1 \) (mod \( d \)), that \( 0 < b_1 \leq d \) and that \( b_1 \) increases with \( i \). Here \( i \) is
understood as limited to those values in the table. Now

\[(k+1)d \geq \left[\frac{(k+1)d}{n_1}\right] n_1\] implies \[\left[\frac{(k+1)d}{n_1}\right] n_1 - kd \leq d\] where equality holds only if \((k+1)d \equiv 0 \pmod{n_1}\). Thus \(b_i = a_i\) unless

\[i = \left[\frac{(k+1)d}{n_1}\right]\] and \((k+1)d \equiv 0 \pmod{n_1}\). In this case \(a_i = 0\) and \(b_i = d\).

Now let \(\left(a_j, \left[\frac{jin}{d}\right]\right)\) be a primitive solution of the congruence

\[x + dy \equiv 0 \pmod{n}\]. The integer \(j\) must occur as some \(i\) in table \((4.1)\). Since \(b_i\) increases with \(i\), we must have \(j = \left[\frac{kd}{n_1}\right] + 1\), for some \(k, 0 \leq k \leq n_1-1\).

Finally, \(kd \equiv 0 \pmod{n_1}\) implies \(k\) is divisible by \(u = \frac{n_1}{(d,n)}\).

Thus since \(\left(0, \left[\frac{ud}{n_1}\right]\right)\) is a solution, those solutions \(\left(a_i, \left[\frac{jin}{d}\right]\right)\), where \(i = \left[\frac{kd}{n_1}\right] + 1\) and \(kd \equiv 0 \pmod{n_1}\), are not primitive.

Next consider the solutions of \(x' + dy' \equiv 0 \pmod{n_1}\).

For \(k = 1, 2, \ldots, n_1-1\) define \(\alpha'_k \equiv -kd \equiv -kd_1 \pmod{n_1}\) where

\[0 \leq \alpha'_k < n_1\]. Then the nontrivial solutions are \((\alpha'_1, 1), (\alpha'_2, 2), \ldots, (\alpha'_{n_1-1}, n_1-1)\).

**Lemma 2.** Let \(1 \leq k, l < n\) where \(kd\) and \(ld\) are not divisible by \(n_1\). Then if \(e = \frac{kd}{n_1} + 1\) and \(f = \frac{ld}{n_1} + 1\), then

\[a_e - a_f = k - l\].
Proof: $a = b = en_1 - kd$ and $a = b = fn_1 - kd$ while

$$\alpha_k = n_1 - \left\{ kd - \left[ \frac{kd}{n_1} \right] n_1 \right\} \text{ and }$$

$$\alpha_l = n_1 - \left\{ ld - \left[ \frac{ld}{n_1} \right] n_1 \right\} .$$

Thus $a_e - a_f = \left( \left[ \frac{kd}{n_1} \right] - \left[ \frac{ld}{n_1} \right] \right) n_1 + (k-l)d = \alpha_k - \alpha_l$.

Now we may prove the theorem. List the primitive solutions of $x + dy \equiv 0 \pmod{n}$ as $(n-d,1)$, $(n-2d,2)$, ..., $(n_l, \left[ \frac{n}{d} \right]) = (a_1, \left[ \frac{n}{d} \right]), (a_2, \left[ \frac{j_1 n}{d} \right]), (a_2, \left[ \frac{j_2 n}{d} \right]), \ldots, (a_v, \left[ \frac{j_v n}{d} \right])$, where by primitivity $a_1 > a_2 > \ldots > a_v > 0$ and $1 < j_1 < j_2 < \ldots < j_v$.

We have seen that each $j_t$ must have the form $\left[ \frac{kd}{n_1} \right] + 1$ where $kd \not\equiv 0 \pmod{n_1}$. For $1 \leq p \leq v$ define $k_p$ by setting $j_p = \left[ \frac{k_p d}{n_1} \right] + 1$ and consider the following solutions of $x^t + d_1 y^t \equiv 0 \pmod{n_1}$:

$$(\alpha_{k_1}, k_1), (\alpha_{k_2}, k_2), \ldots, (\alpha_{k_v}, k_v).$$

By Lemma 2, $\alpha_k > \alpha_{k_2} > \ldots > \alpha_{k_v}$. We cannot have $\alpha_{k_v} = 0$ for then $k_v d \equiv 0 \pmod{n_1}$.

If for some $u$, $1 \leq u \leq v$, $(\alpha_{k_u}, k_u)$ is not a primitive solution of $x^t + d_1 y^t \equiv 0 \pmod{n_1}$, then there is a solution $(\alpha_r, r)$ such that $(0,0) < (\alpha_r, r) < (\alpha_{k_u}, k_u)$. If $\alpha_r = 0$ then $rd_1 \equiv 0 \pmod{n_1}$ and $k_u > \frac{n_1}{(d_1, n_1)}$. 
But then
\[ j_u \geq \left[ \frac{n_1}{d_1, n_1} \frac{d}{n_1} \right] + 1 = \frac{d}{(d_1, n_1)} + 1 = \frac{d}{(d, n)} + 1 \]
and
\[ \left( 0, \frac{d}{(d, n)} \right) < \left( a_{j_u}, \left[ \frac{j_u n_1}{d} \right] \right), \]
contradicting the primitivity of \( \left( a_{j_u}, \left[ \frac{j_u n_1}{d} \right] \right) \).

If \( \alpha_r > 0 \) then by Lemma 2, if \( f = \left[ \frac{rd}{n_1} \right] + 1 \),
\[ (0, 0) < \left( a_r, \left[ \frac{fn_1}{d} \right] \right) \leq \left( a_{j_u}, \left[ \frac{j_u n_1}{d} \right] \right) \]
again contradicting the primitivity of \( \left( a_{j_u}, \left[ \frac{j_u n_1}{d} \right] \right) \).

Thus for \( 1 \leq p \leq v \), \( (\alpha_k, k) \) is a primitive solution of
\[ x' + d_1 y' \equiv 0 \pmod{n_1}. \]
To complete the proof of the theorem we must show that there are no others.

Suppose \( (\alpha_q, q) \) is a primitive solution of \( x' + d_1 y' \equiv 0 \pmod{n_1} \). Since \( \alpha_1, \alpha_2, \ldots, \alpha_{q-1} > \alpha_q > 0 \), Lemma 2 implies
\[ a \left[ \frac{d}{n_1} \right] + 1, a \left[ \frac{2d}{n_1} \right] + 1, \ldots, a \left[ \frac{(q-1)d}{n_1} \right] + 1, \frac{qd}{n_1} + 1 \]
are \( a \left[ \frac{q}{n_1} \right] + 1 \) and so is \( n_1 - qd \) and so is \( > 0 \).

Also \( a \left[ \frac{qd}{n_1} \right] + 1 = \left( \frac{qd}{n_1} + 1 \right) n_1 = qd \) and so is \( > 0 \).

Now for each \( t, 1 \leq t \leq q \), \( a \left[ \frac{td}{n_1} \right] > 0 \) for otherwise \( td \) would be divisible by \( n_1 \) and \( \alpha_t \) would be 0. Moreover,
\[ a_1 = n_1 \quad \frac{d}{n_1} n_1 + (n_1-d) = a_1 \quad \frac{d}{n_1} + 1. \]

Hence by the discussion of the tables of (4.1) with \( k = 0, 1, \ldots, q-1 \) we may conclude that

\[ a_1, a_2, \ldots, a_q \quad \frac{qd}{n_1} \quad 0. \]

In Lemma 1 set \( g = \frac{qd}{n_1} + 1 \). This means that \( a_q \), \( \frac{qd}{n_1} \) is primitive. Thus \( q \) was one of the \( k \)'s and the theorem is proved.

As a corollary we give a more convenient computational form of the primitive solutions.

**Corollary.** Let \((x,y)\) be a solution of \( x + dy \equiv 0 \pmod{n} \) such that \( y = \frac{id}{n_1} + l + 1 \). Then \( x = n_1d \frac{y}{n_1} + 1 + n_1d \frac{y}{n_1} + 1 \).

**Proof:** Let \( n = q_1d + n_1, 0 \leq n_1 \leq d \). Then \( q_1 = \frac{n}{d} \),

\[ \frac{id}{n_1} + l + 1 \quad n_1d \frac{y}{n_1} + 1 + n_1d \frac{y}{n_1} + 1, \quad \text{and} \]

\[ y = q_1 \frac{id}{n_1} + l + 1 + \frac{n_1}{d} \frac{id}{n_1} + 1. \]

Since \( id \frac{n_1}{n_1} + l + n_1d (i + 1)d \), we have \( y = q_1 \frac{id}{n_1} + l + i \).

Now write \( x = \frac{id}{n_1} + l + 1 + n - yd \). By substituting

\[ \frac{n}{d} \quad \frac{id}{n_1} + l + 1 + i \quad \text{for} \quad y \quad \text{we obtain} \]
\[ x = n \left[ \frac{1}{n} \right] + n - d \left[ \frac{n}{d} \right] \left[ \frac{1}{n} \right] - d \left[ \frac{n}{d} \right] - \text{id}. \] Then substituting \[ \left[ \frac{n}{d} \right] d + n_1 \] for \( n \) and clearing gives \( x = n_1 - (\text{id} - \left[ \frac{n}{d} \right] n_1). \)

In the notation of Theorem 3, let

\[ n > d > n_1 > d_1 > 0. \]

Let \( (x_1, y_1) = \left( n - \left[ \frac{n}{d} \right] d, \left[ \frac{n}{d} \right] \right) = (n_1, \left[ \frac{n}{d} \right]) \) and

\[ (x_2, y_2) = \left( n_1 - d + \left[ \frac{d}{n_1} \right] n_1, \left[ \frac{n}{d} \right] \left( \left[ \frac{d}{n_1} \right] + 1 \right) + 1 \right) = \left( n_1 - d_1, \left[ \frac{n}{d} \right] \left( \left[ \frac{d}{n_1} \right] + 1 \right) + 1 \right). \]

By Theorem 3 and Corollary, \( (x_1, y_1) \) and \( (x_2, y_2) \) are primitive solutions of \( x + dy \equiv 0 \pmod{n} \). Concerning them we shall now prove the following useful theorem:

**Theorem 4.** If \( (x', y') \) is a solution of \( x + dy \equiv 0 \pmod{n} \) and \( (0, 0) < (x', y') < (x_1 + x_2, y_1 + y_2) \), where \( (x_1, y_1) \) and \( (x_2, y_2) \) are the primitive solutions, then either \( (x', y') = (x_1, y_1) \) or \( (x', y') = (x_2, y_2) \). Moreover, \( x_1 + x_2 + y_1 + y_2 \leq n \) if and only if

\[
\left[ \frac{n_1 + 1 - d}{\left[ \frac{n}{d} \right] (n_1 - 1)} \right] \leq \left[ \frac{d}{n_1} \right].
\]

**Proof:** To prove the first part of the theorem we need the following lemma.

**Lemma.** Suppose there exist primitive solutions \( (x_1, y_1) \) and \( (x_2, y_2) \) of \( x + dy \equiv 0 \pmod{n} \) such that \( x_1 + x_2 \leq n, y_1 + y_2 \leq n \) and there is no other primitive solution \( (x', y') \) for which \( (x', y') \)
(x_1 + x_2, y_1 + y_2). Then there is no other solution (x*,y*) such that (0,0) < (x*,y*) < (x_1 + x_2, y_1 + y_2).

Proof of lemma. Let (0,0) < (x*,y*) < (x_1 + x_2, y_1 + y_2) where (x*,y*) is a solution of x + dy \equiv 0 \pmod{n}. Clearly y* \neq 0 since x* must be less than n. If there are solutions (x*,y*) with x* = 0 and (0,0) < (x*,y*) < (x_1 + x_2, y_1 + y_2) then select the one with y* minimal. Then (x_1 + x_2, y_1 + y_2 - y*) is a solution and by primitivity y* > y_1, y_2. This implies y_1 + y_2 - y* < y*, y_1, y_2. But now the choice of y* implies that there must be a primitive solution (x',y') < (x_1 + x_2, y_1 + y_2 - y*). Such a primitive solution cannot be (x_1,y_1) or (x_2,y_2), and this contradicts the hypothesis. Hence we have shown that an arbitrary solution (x*,y*) which satisfies (0,0) < (x*,y*) < (x_1 + x_2, y_1 + y_2) can have neither x* = 0 nor y* = 0.

Thus the solution (x*,y*) must contain a primitive solution. This means for i = 1 or 2, x_1 = x* and y_1 = y*. For this i, (x* - x_i, y* - y_i) is a solution. Either both x* - x_i and y* - y_i are zero or neither is zero. If x* \neq x_i and y* \neq y_i then for j = 1 or 2, x* = x_i \geq x_j and y* - y_i \geq y_j. Again, either both x* - x_i - x_j and y* - y_i - y_j are zero or neither is zero. Continuing, we obtain

x* = c_1 x_1 + c_2 x_2 and y* = c_1 y_1 + c_2 y_2,

where c_1 and c_2 are non-negative integers. If (x_1,y_1) = (x_2,y_2) x* = cx_1, y* = cy_1 where c = c_1 + c_2. In this case c would be 1 or 2
and the lemma follows. If \((x_1,y_1) \neq (x_2,y_2)\) we may let \(x_1 > x_2, y_1 < y_2\). Then \(x_1 > x_2\) and \(x^* \leq x_1 + x_2\) imply \(c_1 \leq 1\) while \(y_1 < y_2\) and \(y^* \leq y_1 + y_2\) imply \(c_2 \leq 1\). This proves the lemma.

We must show that the solutions \((x_1, y_1)\) and \((x_2, y_2)\) of the theorem satisfy the hypothesis of the lemma. One readily verifies that \(x_1 + x_2\) and \(y_1 + y_2\) are less than \(n\). Let \((x^*, y^*)\) be a primitive solution such that \((0, 0) < (x^*, y^*) < (x_1 + x_2, y_1 + y_2)\). To prove the first part of the theorem it suffices to show that \(x^* \leq x_1\) and \(y^* \leq y_2\). Now consider the solution \((x_3, y_3)\) where

\[
y_3 = \left\lfloor \frac{n}{d} \right\rfloor \left(\left\lfloor \frac{2d}{n_1} \right\rfloor + 1 \right) + 2.
\]

By Theorem 3 and its corollary there is no primitive solution \((x', y')\) such that \(y_2 < y' < y_3\). We have

\[
y_3 - y_1 - y_2 = \left\lfloor \frac{n}{d} \right\rfloor \left(\left\lfloor \frac{2d}{n_1} \right\rfloor - \left\lfloor \frac{d}{n_1} \right\rfloor - 1 \right) + 1 \geq \left\lfloor \frac{n}{d} \right\rfloor \left(\left\lfloor \frac{d}{n_1} \right\rfloor - 1 \right) + 1 \geq 1.
\]

From this it follows that \(y^* \leq y_2\).

Now if \(\left\lfloor \frac{n}{d} \right\rfloor = 1\), then \(x^* \leq x_1\). If \(\left\lfloor \frac{n}{d} \right\rfloor > 1\), consider the solution

\((x_0, y_0) = (n - \left\lfloor \frac{n}{d} \right\rfloor d + d, \left\lfloor \frac{n}{d} \right\rfloor - 1)\). This is no primitive solution \((x'', y'')\) such that \(x_0 > x'' > x_1\).

Furthermore

\[
x_0 - x_1 - x_2 = n - \left\lfloor \frac{n}{d} \right\rfloor d + d - (n - \left\lfloor \frac{n}{d} \right\rfloor d - \left\lfloor \frac{d}{n_1} \right\rfloor n_1) = 2d - n_1 - n_1 \left\lfloor \frac{d}{n_1} \right\rfloor > 0.
\]

Hence \(x^* \leq x_1\). Thus \(x^* \leq x_1\) and \(y^* \leq y_2\) so that \((x^*, y^*)\) equals \((x_1, y_1)\) or \((x_2, y_2)\). The first part of the theorem follows from the lemma.
Now \( x_1 + x_2 + y_1 + y_2 \leq n \) if and only if

\[
n_1 + n_1 - d_1 + \left\lfloor \frac{n}{d} \right\rfloor \left( \left\lfloor \frac{d}{n_1} \right\rfloor + 2 \right) + 1 \leq \left\lfloor \frac{n}{d} \right\rfloor d + n_1.
\]

Substituting \( \left\lfloor \frac{d}{n_1} \right\rfloor n_1 + d_1 \) for \( d \), this inequality holds if and only if

\[
1 + n_1 - d_1 - \left\lfloor \frac{n}{d} \right\rfloor d_1 + 2 \left\lfloor \frac{n}{d} \right\rfloor \left( n_1 - 1 \right) \left\lfloor \frac{d}{n_1} \right\rfloor.
\]

Thus \( x_1 + x_2 + y_1 + y_2 \leq n \) if and only if

\[
\frac{n_1 + 1 - d_1}{\left\lfloor \frac{n}{d} \right\rfloor (n_1 - 1)} - \frac{d_1 - 2}{(n_1 - 1)} \leq \left\lfloor \frac{d}{n_1} \right\rfloor.
\]

**Corollary.** Let the hypothesis be as for Theorem 4.

If \( d_1 > 1 \) then \( x_1 + x_2 + y_1 + y_2 \leq n \).

If \( d = 1 \) then \( x_1 + x_2 + y_1 + y_2 \leq n \) if one of the following conditions holds.

1) \( \left\lfloor \frac{d}{n_1} \right\rfloor \geq 3 \).

2) \( \left\lfloor \frac{d}{n_1} \right\rfloor = 2 \) and \( \left\lfloor \frac{n}{d} \right\rfloor \geq 2 \).

3) \( \left\lfloor \frac{d}{n_1} \right\rfloor = 2 \) and \( n_1 \geq 3 \).

**Proof:** Let \( L \) denote \( \frac{n_1 + 1 - d_1}{\left\lfloor \frac{n}{d} \right\rfloor (n_1 - 1)} - \frac{d_1 - 2}{(n_1 - 1)} \).

If \( d_1 > 1 \) then \( L \leq 1 \leq \left\lfloor \frac{d}{n_1} \right\rfloor \). Hence the theorem implies

\( x_1 + x_2 + y_1 + y_2 \leq n \). Now let \( d_1 = 1 \).

Then \( L = \frac{n_1}{\left\lfloor \frac{n}{d} \right\rfloor (n_1 - 1)} + \frac{1}{(n_1 - 1)} \).
If \([d_{n_1}] \geq 3\), then \(L \leq \frac{n_1 + 1}{(n_1 - 1)} \leq 3 \leq \left[ \frac{d_{n_1}}{n_1} \right]\).

If \([d_{n_1}] = 2\) and \(\left[ \frac{n_1}{d} \right] \geq 2\), then \(L \leq \frac{n_1}{2(n_1 - 1)} + \frac{1}{n_1 - 1} \leq 2 = \left[ \frac{d_{n_1}}{n_1} \right]\).

If \([d_{n_1}] = 2\) and \(n_1 \geq 3\), then \(L \leq \frac{3}{2 \left[ \frac{n_1}{d} \right]} + \frac{1}{2} \leq 2 = \left[ \frac{d_{n_1}}{n_1} \right]\).

5. Applications. Let \(A\) be a cyclic 0,1 matrix of order \(n\) defined by differences 0,1 and \(d\). In this section we shall prove that \(P(A) = |D(A)|\) if and only if \(n = 7\) and \(d = 3\) or 5. Thus the difference sets mod 7 are truly exceptional.

As covered in Sections 2 and 3, to show \(P(A) \geq |D(A)|\) it is necessary and sufficient to show the existence of a solution \((x',y')\) of \(x + dy \equiv 0 \pmod{n}\) such that \((x',y')\) represents a cycle and \(x' = y'\) is even. The problem of determining when a solution \((x',y')\), \(0 < x' + y' \leq n\), represents a cycle may be described as follows. Suppose there exists some arrangement of \(x' \alpha 's\) and \(y' \beta 's\) in a circle with the following property. For each solution \((x^*,y^*) < (x',y')\), no selection of \(x^* + y^*\) consecutive \(\alpha 's\) and \(\beta 's\) totals exactly \(x^* \alpha 's\) (or \(y^* \beta 's\)). Then \((x',y')\) represents a cycle. If no such arrangement is possible then \((x',y')\) does not represent a cycle.

For the purposes of this section it is not necessary to solve completely this problem in arrangements. In an important class of \(d\) and \(n\) Theorem 4 yields two primitive solutions \((x_1,y_1)\) and \((x_2,y_2)\) having the property that \(x_1 + x_2 + y_1 + y_2 \leq n\) and
there is no other solution \((x', y')\) such that 
\((0, 0) < (x', y') < (x_1 + x_2, y_1 + y_2)\). Thus if there is an arrange-
ment of \(x_1 + x_2 \alpha's\) and \(y_1 + y_2 \beta's\) in a circle such that no
selection of \(x_1 + y_1\) consecutive \(\alpha's\) and \(\beta's\) totals exactly
\(x_1 \alpha's\) (or \(y_1 \beta's\) then \((x_1 + x_2, y_1 + y_2)\) represents a cycle.
Under these circumstances we have \(P(A) > |D(A)|\). For \((x_1, y_1)\) and
\((x_2, y_2)\) represent cycles, and if \(x_1 + y_1\) and \(x_2 + y_2\) are both odd
then \(x_1 + x_2 + y_1 + y_2\) is even. The proof of Theorem 5 is based
upon this device.

Theorem 5. Let \(A\) be a cyclic \(0,1\) matrix of order \(n\) defined
by the differences \(0,1,d\). Then \(P(A) = |D(A)|\) if and only if \(n = 7\)
and \(d = 3\) or \(5\).

**Proof:** If \(n = 7\) and \(d = 3\) or \(5\) then \(P(A) = |D(A)|\) by
Example 2. We assume \(P(A) = |D(A)|\) and will show \(n = 7\) and \(d = 3\)
or \(5\). If \(n\) or \(d\) is even then \(P(A) > |D(A)|\). For if \(n\) is even the
permutation \((1, 2, \ldots, n)\) is odd. The solution \((x', y') = (n-d, 1)\)
is primitive so if \(n\) is odd and \(d\) is even then \(x' + y' = n-d+1\) is
even. Thus we may assume that both \(n\) and \(d\) are odd.

We may also assume that \(\left\lfloor \frac{n}{d} \right\rfloor = 1\).

For if \(\left\lfloor \frac{n}{d} \right\rfloor \geq 2\) then \(d < \left(\frac{n}{2}\right)\) and \(n-d+1 > \frac{n}{2} + 1\). Thus \(\left\lfloor \frac{n}{n-d+1} \right\rfloor = 1\).

Now if we let \(B\) be the \(n\times n\) matrix defined by the differences
\(0,1, n-d+1\) and \(C\) be the \(n\times n\) matrix defined by the differences
0, d-1, n-1, then \( B = C^T \). Since \( P(A) = P(C) = P(C^T) = P(B) \) while 
D(A) = D(B), it follows that \( P(A) = D(A) \) if and only if 
P(B) = D(B). Thus if \( \left[ \frac{n}{d} \right] \geq 2 \), we may study the matrix B with 
\[ \left[ \frac{n}{n-d+1} \right] = 1. \] Hence we may assume \( \left[ \frac{n}{d} \right] = 1. \) Note that if \( n = 7, d = 3 \) then \( n-d+1 = 5 \).

We may assume further that in the notation of Theorem 3, 
n > d > n_1 > d_1 \geq 1. \) For if \( d_1 = 0 \) then \( n_1 \) is the greatest common 
 divisor of \( n \) and \( d \). Since \( n_1 = n-d \) this would imply \( n_1 \) to be even 
 and hence \( n \) and \( d \) also.

Finally, we may assume \( \left[ \frac{d}{n_1} \right] > 1. \) For if \( \left[ \frac{d}{n_1} \right] = 1, \) consider 
the primitive solution \((x', y') = (n_1-d_1, \left[ \frac{n}{d} \right] (\left[ \frac{d}{n_1} \right] + 1) + 1). \) Since 
d is odd and \( d = n_1+d_1 \), \( x'+y' \equiv n_1+d_1+1 \equiv 0 \) (mod 2).

In the remainder of the proof let \((x_1, y_1) \) and \((x_2, y_2) \) denote 
the primitive solutions \((n_1, 1) \) and \((n_1-d_1, \left[ \frac{d}{n_1} \right] + 2 \) respectively, 
as in Theorem 4. Note that under our present assumptions about \( d \) 
and \( n \), \( x_1 + x_2 + y_1 + y_2 \leq n \) except when \( \left[ \frac{d}{n_1} \right] = n_1 = 2 \) and for this case 
n = 7 and \( d = 5 \).

The proof will be completed by showing that if \( n \) and \( d \) are 
not 7 and 5 respectively, then \((x_1+x_2, y_1+y_2) \) represents a cycle. 
Several cases will be considered.
Case 1a $y_1 + y_2 \equiv 0 \pmod{x_1 + x_2}$.

Consider the following circular arrangement of $x_1 + x_2$ $\alpha$'s and $y_1 + y_2$ $\beta$'s.

If a selection of $t = x_1 + y_1$ consecutive $\alpha$'s and $\beta$'s totals $x_1$ $\alpha$'s then it totals at least $(x_1 - 1) \frac{y_1 + y_2}{x_1 + x_2}$ $\beta$'s. Since $\left\lceil \frac{d}{n_1} \right\rceil \geq 2$,

$$(x_1 - 1) \frac{y_1 + y_2}{x_1 + x_2} = \frac{(n_1 - 1) \left\lceil \frac{d}{n_1} \right\rceil + 3}{2n_1 - d_1} \geq \frac{5(n_1 - 1)}{2n_1 - d_1} > 1 = y_1.$$ 

Thus for this case $P(A) > |D(A)|$. 
Case lb \( y_1 + y_2 \not\equiv 0 \pmod{x_1 + x_2} \) and \( x_1 + x_2 < y_1 + y_2 \).

Consider the following circular arrangement of \( x_1 + x_2 \) \( \alpha \)'s and \( y_1 + y_2 \) \( \beta \)'s.

Since \( y_1 + y_2 - 1 \geq (x_1 + x_2) \left[ \frac{y_1 + y_2}{x_1 + x_2} \right] \), we have

\[
y_1 + y_2 - (x_1 + x_2 - 1) \left[ \frac{y_1 + y_2}{x_1 + x_2} \right] \geq \left[ \frac{y_1 + y_2}{x_1 + x_2} \right].
\]

Thus if \( 1 \leq t \leq x_1 + x_2 - 1 \), a selection of consecutive \( \alpha \)'s and \( \beta \)'s which totals \( t \) \( \alpha \)'s will total at most

\[
y_1 + y_2 - (x_1 + x_2 - t - 1) \left[ \frac{y_1 + y_2}{x_1 + x_2} \right] + t \left[ \frac{y_1 + y_2}{x_1 + x_2} \right] + 1 =
\]

\[
y_1 + y_2 - (x_1 + x_2 - t - 1) \left[ \frac{y_1 + y_2}{x_1 + x_2} \right] \beta \)'s.
\]

Let \( t = x_2 \). It suffices to show that

\[
y_2 > y_1 + y_2 - (x_1 + x_2 - x_2 - 1) \left[ \frac{y_1 + y_2}{x_1 + x_2} \right]
\]

and thus to show \((n_1 - 1) \left[ \frac{d}{n_1} + 3 \right] > 1\).

This will be true if \( n_1 > 2 \).

If \( n_1 = 2 \) then \( d_1 = 1 \) and \((n_1 - 1) \left[ \frac{d}{n_1} + 3 \right] = \left[ \frac{d}{n_1} + 3 \right] \).
This is $>1$ unless $\left\lceil \frac{d}{n_1} \right\rceil = 2$. But then $d_1 = 1, n_1 = 2 = \left\lceil \frac{d}{n_1} \right\rceil$ and $\left\lceil \frac{n}{d} \right\rceil = 1$ together imply $d = 5$ and $n = 7$.

**Case 2** \[x_1 + x_2 \geq y_1 + y_2.\]

Consider the following circular arrangement of $\alpha$'s and $\beta$'s.

We are supposing throughout the proof that $(x_1, y_1) = (n_1, 1)$ and $(x_2, y_2) = (n_1 - d_1, \left\lceil \frac{d}{n_1} \right\rceil + 2)$.

Let $u = y_1 + y_2, v = \left\lceil \frac{x_1 + x_2}{y_1 + y_2} \right\rceil$ and set $t_1 = t_3 = t_5 = \ldots = 0$.

For each $i = 1, 2, \ldots, \left\lfloor \frac{u}{2} \right\rfloor$ we wish to select $t_{2i}$ so that $0 \leq t_{2i} \leq n_1 - 2v - 1$ and $t_2 + t_4 + t_6 + \ldots = x_1 + x_2 - (y_1 + y_2) \left\lceil \frac{x_1 + x_2}{y_1 + y_2} \right\rceil$.

For then any selection of consecutive $\alpha$'s and $\beta$'s which totals $y_1 = 1$ $\alpha$ will total less than $n_1 = x_1$ $\beta$'s.

To show that the $t$'s may be so selected it suffices to prove that $uv + \left\lfloor \frac{u}{2} \right\rfloor (n_1 - 2v - 1) \geq x_1 + x_2$. Thus we must show that
The left side equals

\[(\left\lceil \frac{d}{n_1} \right\rceil + 3) \left\lceil \frac{2n_1 - d_1}{n_1} \right\rceil + \left\lceil \frac{d}{n_1} \right\rceil + 3 \left( n_1 - 2 \right) \left( \left\lfloor \frac{d}{n_1} \right\rfloor + 3 \right) \geq 2n_1 - d_1.\]

and is \(\geq \left\lceil \frac{d}{n_1} \right\rceil + 3\) \((n_1 - 1)\). This is \(\geq 2n_1 - d_1\) unless \(d_1 = 1\) and \(n_1 = 2\). If \(d_1 = 1\) and \(\left\lceil \frac{d}{n_1} \right\rceil = 2\), then (5.1) becomes

\[2n_1 + \left\lfloor \frac{2n_1 - 1}{5} \right\rfloor - 2.\]

However, \(2n_1 + \left\lfloor \frac{2n_1 - 1}{5} \right\rfloor - 2 \leq 2n_1 - 1\) and \(n_1 > 1\) together imply that \(n_1 = 2\) and hence that \(d = 5\), \(n = 7\). Thus (5.1) \(\geq 2n_1 - d_1\) unless \(d = 5\) and \(n = 7\).
6. The Main Theorem. In this section we prove the main theorem, a generalization of Theorem 5. Preparatory to this, however, we need a theorem on arrangements.

Let \( u, v \geq 1 \) and consider a given circular arrangement of \( u \alpha \)'s and \( v \beta \)'s, grouping the \( \alpha \)'s and \( \beta \)'s as follows:

For \( 1 \leq t < u \), define the arrangement functions \( M(t) \) and \( m(t) \) as follows:

\[
\begin{align*}
t + M(t) &= \text{the maximum number of consecutive } \alpha \text{'s and } \beta \text{'s which totals exactly } t \text{ } \alpha \text{'s,} \\
t + m(t) &= \text{the minimum number of consecutive } \alpha \text{'s and } \beta \text{'s which totals exactly } t \text{ } \alpha \text{'s.}
\end{align*}
\]

Then \( M(u) = v, m(1) = 0 \) and for \( 1 < t < u \),

\[
\begin{align*}
M(t) &= \text{maximum } (a_{i-1} + a_i + \ldots + a_{i+t-1}), 0, 1, \ldots, u-1 \text{ and} \\
m(t) &= \text{minimum } (a_i + a_{i+1} + \ldots + a_{i+t-2}), i = 0, 1, \ldots, u-1.
\end{align*}
\]

Here the subscripts are taken mod \( u \). We may now state the following theorem for the given arrangement with functions \( M \) and \( m \).

Theorem 6. (1) For \( 1 \leq t < u \), \( M(t) + m(u-t) = v \).

(2) Some selection of consecutive \( \alpha \)'s and \( \beta \)'s totals exactly
(3) Let \( r \) and \( s \) be positive integers. In the given circular arrangement of \( \alpha 's \) and \( \beta 's \) replace each \( \alpha \) by \( r \alpha 's \) and each \( \beta \) by \( s \beta 's \). If \( M', m' \) denote the arrangement functions after the replacement, then \( m'(rt) = sm(t) \) and \( M'(rt) = sM(t) \).

**Proof:** (1) This follows at once from the definition of \( M \) and \( m \).

(2) The necessity is clear. For \( 1 < t < u \) and \( i = 0, 1, \ldots, u-1 \) let

\[
M_i(t) = a_{i-1} + a_i + \ldots + a_{i+t-1}
\]

\[
m_i(t) = a_i + a_{i+1} + \ldots + a_{i+t-2}.
\]

Then if \( w \) satisfies \( m_i(t) \leq w \leq M_i(t) \), there is a selection of consecutive \( \alpha 's \) and \( \beta 's \) which totals exactly \( t \) \( \alpha 's \) and \( w \beta 's \) and we are finished. Also, \( m_i(t) \leq M_{i+1}(t) \) and \( m_{i+1}(t) \leq M_{i}(t) \) for \( i = 0, 1, \ldots, u-1 \). We may suppose \( w < \max \{m_0(t), m_1(t), \ldots, m_{u-1}(t)\} \).

For if \( w \geq \max \{m_0(t), m_1(t), \ldots, m_{u-1}(t)\} \) then for some \( i \)

\[
m_i(t) \leq w \leq M_i(t) = M, \text{ and we are finished.}
\]

Thus for some \( k, w \leq m_k(t) \) and either \( w \geq m_{k-1}(t) \) or \( w \geq m_{k+1}(t) \). But then \( w \leq m_k(t) \leq M_{k-1}(t) \), \( M_{k+1}(t) \) so (2) follows.

(3) In the given arrangement the \( \alpha 's \) are numbered \( o, 1, 2, \ldots, u-1 \) in a clockwise direction. After the replacement, the \( \alpha 's \) fall into \( u \) groups of \( r \) each. For \( 0 \leq j \leq u-1 \), group \( j \) consists
of the r α's replacing the jth α. Now consider for the new arrangement a selection of consecutive α's and β's which totals rτ α's. Moving in a clockwise direction let the first α's used be from group i. If all of group i is used then the selection will total at most \( s(a_{i-1} + a_i + \ldots + a_{i+t-1}) \) β's and at least \( s(a_i + a_{i+1} + \ldots + a_{i+t-2}) \) β's. If only part of group i is used then only part of group \( i + t - 1 \) is used and the selection will total exactly \( s(a_i + a_{i+1} + \ldots + a_{i+t-2}) \) β's. Thus (3) follows.

**Theorem 7.** Let \( A \) be a cyclic 0,1 matrix of order \( n \) and defined by the differences \( d_0 = o, d_1, d_2 \). Then \( P(A) = |D(A)| \) if and only if \( n = 7e, d_1 = ed_1', d_2 = ed_2' \), where \( o, d_1', d_2' \) is a perfect difference set mod 7.

**Proof:** Let \( c, d \) and \( n, o < c, d < n \), be positive integers. Suppose the greatest common divisor \( (c,d,n) = 1 \). Then \( cx_o + dy_o \equiv 0 \pmod{n} \) if and only if \( c'x_o' + d'y_o' \equiv 0 \pmod{n'} \), where \( c = (c,n)c', d = (d,n)d', x_o = (d,n)x_o', y_o = (c,n)y_o' \), and \( n = (c,n)(d,n)n' \). Suppose \( c' \neq d' \).

Now let \( A \) be the cyclic \( nxn \) matrix defined by the differences \( o, c, d \) and \( B \) be the cyclic \( n'xn' \) matrix defined by \( o, c', d' \). We will now prove the following lemma.

**Lemma 1.** If \((x_o', y_o')\) represents a cycle of \( B \) then \((x_o, y_o)\) represents a cycle of \( A \).
Proof: Let \( s = (c, n) \) and \( r = (d, n) \). \( x_0^i + y_0^i \leq n' \) implies \( x_0^i + y_0^i = rx_0^i + sy_0^i \leq n \). By Theorem 6 there is a circular arrangement of \( x_0^i \alpha 's \) and \( y_0^i \beta 's \) with functions \( M \) and \( m \) such that if \( (o,o) < (x_1^i, y_1^i) < (x_0^i, y_0^i) \) and \( c'x_1^i + d'y_1^i \equiv 0 \pmod{n'} \) then \( M(x_1^i) < y_1^i \) or else \( m(x_1^i) > y_1^i \). In this arrangement replace each \( \alpha \) by \( r \alpha 's \) and each \( \beta \) by \( s \beta 's \) thus obtaining a circular arrangement of \( x_0^i \alpha 's \) and \( y_0^i \beta 's \).

By Theorem 6, this arrangement has functions \( M' \) and \( m' \) where \( M'(rt) = sM(t) \) and \( m'(rt) = sm(t) \). Now let \( (x_1^i, y_1^i) \) be a solution of \( cx + dy \equiv 0 \pmod{n} \) and suppose \( (o,o) < (x_1^i, y_1^i) < (x_0^i, y_0^i) \). Then if we let \( x_1^i \) and \( y_1^i \) satisfy \( x_1^i = rx_1^i \) and \( y_1^i = sy_1^i \), we have \( c'x_1^i + d'y_1^i \equiv 0 \pmod{n'} \) and \( (o,o) < (x_1^i, y_1^i) < (x_0^i, y_0^i) \). Thus either \( M(x_1^i) < y_1^i \) or \( m(x_1^i) > y_1^i \). But then \( M'(x_1^i) = M'(rx_1^i) = sM(x_1^i) < y_1^i \) or \( m'(x_1^i) = m'(rx_1^i) = sm(x_1^i) > y_1^i \) and the lemma follows.

Lemma 2. Let \( A \) be cyclic of order \( n \) and defined by the differences \( d_1, d_2, \ldots, d_s \). For \( e > 1 \) a positive integer, let \( A_e \) be the cyclic matrix of order \( ne \) defined by the differences \( ed_1, ed_2, \ldots, ed_s \). If \( B = A \oplus A \oplus \ldots \oplus A \), the direct sum of \( A \) taken \( e \) times, then \( B \) may be obtained from \( A_e \) by simultaneous permutations of rows and columns.
Proof: Let $A_t$ denote the nxn matrix formed from the intersections of the rows $t$, $e+t$, $2e+t$, ..., $e(n-1)+t$ and columns $t$, $e+t$, $2e+t$, ..., $(n-1)e+t$. Here $t$ is a fixed integer on the interval $1 \leq t \leq e$. We prove $A_t = A$.

Suppose $1 \leq i, j \leq n$. There is a 1 in row $(i-1)e+t$, column $(j-1)e+t$ of $A_t$ if and only if for some $k$, $1 \leq k \leq s$,

$$(j-1)e+t \equiv (i-1)e+t+\epsilon d_k \pmod{en}.$$ 

This congruence holds if and only if $j \equiv i+\epsilon d_k \pmod{n}$. Thus for each $t$, $1 \leq t \leq e$, $A_t = A$. Thus the matrix $A_e$ contains $e$ principal minors $A$, and these minors are disjoint from one another. This means that by simultaneous permutations of rows and columns, we may write $A_e$ in the form $B$.

Lemma 3. Let $r$ and $s$ be positive integers not both 1. There is a circular arrangement of $5r \alpha$'s and $3s \beta$'s such that no consecutive $r + 2s \alpha$'s and $\beta$'s total exactly $r \alpha$'s.

Proof:

Case 1. $5r \leq 3s$.

Consider an arrangement of $x_1 + x_2 = 5r \alpha$'s and $y_1 + y_2 = 3s \beta$'s of the type shown in Case 1b of the proof of Theorem 5. By Theorem 6, $M(r) = 3s - m(4r)$ so $m(4r) \geq s$ if and only if $M(r) < 2s$. Thus it suffices to show that $m(4r) > s$. Now $m(4r) = (4r-1) \left\lceil \frac{2s}{5r} \right\rceil$. If $k = \left\lceil \frac{2s}{5r} \right\rceil$ then $5r(k+1) > 3s \geq 5rk$. Then $m(4r) > s$ if $(4r-1)k \geq \frac{5r(k+1)}{3}$ or if $\frac{3k}{k+1} \geq \frac{5r}{4r-1}$. This will be true unless $k = r = 1$. Then however
m(4r) > s unless s = 3 and for this case an acceptable arrangement is

Case 2. \(5r \geq 3s\).

Again consider an arrangement of the type shown in Case 1b of Theorem 5, using \(x_1 + x_2 = 3s\) \(\alpha\)'s and \(y_1 + y_2 = 5r\) \(\beta\)'s.

\[m(2s) = 5r - M(s)\] so \(m(2s) > r\) if and only if \(M(s) < 4r\). Now

\[m(2s) = (2s-1) \left[ \frac{5r}{3s} \right].\]

If \(k = \frac{5r}{3s}\) then \(3s (k+1) > 5r \geq 3sk\). To show \(m(2s) > r\) it suffices to show \(k(2s-1) \geq \frac{3s(k+1)}{5}\) and thus to show

\[\frac{5k}{k+1} \geq \frac{3s}{2s-1}.\] This holds unless \(k = s = 1\). But then also \(r = 1\).

Theorem 7 will now be proved by using Theorem 5 and Lemmas 1, 2 and 3. The sufficiency follows by Lemma 2 and Example 2 of Section 3. The proof of the necessity is by induction. The theorem is true for \(n = 3\). Let \(B\) be cyclic of order \(N(3 \leq N < n)\) and defined by differences \(o, a, b\) and suppose that \(P(B) = |D(B)|\). The induction hypothesis asserts that for every such \(B, N = 7l, a = a' l, b = b' l\) where \(o, a', b'\) form a perfect difference set mod 7.
We may suppose \((d_1, d_2, n) = 1\).

For if \(t = (d_1, d_2, n) > 1\), we may define a matrix \(A^*\) of order \(\frac{n}{t}\) by the differences \(\frac{d_1}{t}, \frac{d_2}{t}\). By Lemma 2, \(P(A^*) = |D(A^*)|\). The induction hypothesis completes the proof.

We will now show that if \((d_1, d_2, n) = 1\) and \(n \neq 7\) or if \(n = 7\) but \(d_1, d_2\) is not a perfect difference set mod 7, then \(P(A) > |D(A)|\). This will complete the proof. If \((d_1, n) = 1\) the solutions of \(d_1x + d_2y \equiv 0 \pmod{n}\) coincide with the solutions of \(x + d_1^{-1}d_2y \equiv 0 \pmod{n}\). Thus Theorem 5 applies and we obtain \(P(A) > |D(A)|\). If \((d_1, n)\) is even, then \((d_2, n)\) is odd and \(\frac{n}{(d_2, n)} = t\) is even. This yields a cycle of even length \(t\) in \(A\) and hence \(P(A) > |D(A)|\). Hence we may assume \((d_1, d_2, n) = 1\) and both \((d_1, n)\) and \((d_2, n)\) are odd and \(t > 1\).

Let \(d_1 = (d_1, n)d_1', \ d_2 = (d_2, n)d_2', \ \text{and} \ n = (d_1, n)(d_2, n)n'\). We consider the case \(d_1' \neq d_2'\) and dispose of the case \(d_1' = d_2'\) later.

We then have the cyclic \(n'x'n'\) matrix \(B\) of Lemma 1 defined by the differences \(\circ, d_1', d_2'. \ \text{Under these restrictions we consider the two cases} \ P(B) > |D(B)| \ \text{and} \ P(B) = |D(B)|. \ \text{If} \ P(B) > |D(B)|, \ \text{then in Lemma 1, we must have an} \ (x'_0, y'_0) \ \text{that represents a cycle and has} \ x'_0 + y'_0 \ \text{even. But then} \ x'_0 + y'_0 = (d_1, n)x'_0 + (d_1, n)y'_0 \ \text{is also even and hence by Lemma 1,} \ P(A) > |D(A)|. \ \text{If} \ P(B) = |D(B)| \ \text{then the}
induction hypothesis implies that \( n' = 7l, d' = d_1' l, d_2' = d_2'' l \),
where \( 0, d_1', d_2' \) is a perfect difference set mod \( 7 \). Let \((d_1, n) = s\)
and \((d_2, n) = r\). Then \((1, 2)\) and \((4, 1)\) are primitive solutions of
\[ d_1' x + d_2' y \equiv 0 \pmod{n'} \]
and there is no other solution \((x', y')\) such that \((0, 0) < (x', y') < (5*3)\).
Consequently by the remarks preceding Lemma 1, \((r, 2s)\) and \((4r, s)\) are primitive solutions of \(d_1 x + d_2 y \equiv 0 \pmod{n}\)
and there is no other solution \((x', y')\) such that \((0, 0) < (x', y') < (5r, 3s)\).
Since \(5r + 3s \leq n\), Lemma 3 implies \((5r, 3s)\) represents a cycle. Since \(5r + 3s\) is even, \(P(A) > \lvert D(A)\rvert\).

We conclude by disposing of the last of the unsettled cases.

We are now assuming \((d_1, d_2, n) = 1, (d_1, n)\) and \((d_2, n)\) are odd and
\( >1, \) and \(d_1' = d_2' = t\). With these assumptions we prove \(P(A) > \lvert D(A)\rvert\).

Since \((d_1, d_2, n) = 1, d_1 x_0 + d_2 y_0 \equiv 0 \pmod{n}\) if and only if
\[ d_1' x_0' + d_2' y_0' \equiv 0 \pmod{n'} \]
where \(x_0 = (d_2, n) x_0'\) and \(y_0 = (d_1, n) y_0'\).

Let \((d_1, n) = v\) and \((d_2, n) = u\). We may assume that \( u < v\). Now we have
\((t, n') = 1, \) so the solutions of \(d_1' x' + d_2' y' \equiv 0 \pmod{n'}\) are \((0, n'),\)
\((l, n'-l), (2, n'-2), \ldots \). Hence \((u, v(2n'-1))\) is a solution of
\(d_1 x + d_2 y \equiv 0 \pmod{n}\) and contains only the solution \((u, v(n'-1))\),
\((0, vn')\) and \((0, 0)\). We show that there is an arrangement of \(u \alpha's\)
and \(v(2n'-1) \beta's\) with arrangement functions \(M\) and \(m\) such that
\(m(u) > v(n'-1)\) and \(M(0) < vn'.\)

Since \( u + v(2n'-1)\) is even this will show \(P(A) > \lvert D(A)\rvert\).
Consider an arrangement of the type shown in Case 1b of Theorem 5 using \( x_1 + x_2 = u \neq \alpha \)'s and \( y_1 + y_2 = u(2n' - 1) \neq \beta \)'s. We have

\[
m(u) \geq (u-1) \left[ \frac{y_1 + y_2}{x_1 + x_2} \right] = (u-1) \left[ \frac{y(2n' - 1)}{u} \right].
\]

But \( (u-1) \left[ \frac{y(2n' - 1)}{u} \right] > (u-1) \left( \frac{v(2n' - 1)}{u} - 1 \right) > v(n' - 1). \)

Thus \( m(u) > v(n' - 1) \) and also \( M(o) < v n' \). This completes the proof.

**Corollary 1.** Let \( A \) be a cyclic 0,1 matrix of order \( n \) with \( k \) ones in each row and column. *If \( k > 3 \) then \( P(A) > |D(A)| \).*

**Proof:** Since it suffices to prove the corollary for \( k = 4 \), we may let \( A \) be defined by the differences \( o, d_1, d_2, d_3 \) and suppose \( P(A) = |D(A)| \). By the theorem, \( n = 7e, d_o = ed'_o = 0, d_1 = ed'_1, d_2 = ed'_2 \) and \( d_3 = ed'_3 \) where any three in the set \( d' = o, d'_1, d'_2, d'_3 \) form a perfect difference set mod 7. This is readily seen to be impossible.

**Corollary 2.** Let \( A \) be a cyclic 0,1 matrix of order \( n \) with 3 ones in each row and column. *If \( P(A) = |D(A)| \), then \( P(A) = 24 \) where \( n = 7e \).*

**Proof:** By Lemma 2 it suffices to show that \( |D(A)| = 24 \) if \( A \) is of order 7 and defined by a perfect difference set mod 7. The determinant here is readily calculated to be 24.
BIBLIOGRAPHY


I, Marion Franklin Tinsley, was born in Ironton, Ohio, February 3, 1927. I received my secondary education at the public schools of Columbus, Ohio. All of my University training has been at Ohio State University, which granted me the Bachelor of Science degree in 1950 and the Master of Arts degree in 1953. During the past three years, 1955-57, I have been Research Assistant on an Office of Ordnance Research project devoted to a study of projective planes and related subjects. During this time I have served under Professor Erwin Kleinfeld, Marshall Hall, Jr., and Herbert Ryser.