INVLUTORY MATRICES, MODULO $m$

by

Dorothy M. Amey

Thesis submitted to the Graduate Faculty of the Virginia Polytechnic Institute in partial fulfillment for the degree of

MASTER OF SCIENCE

in

Mathematics

APPROVED:

Chairman: Dr. James E. Shockley

Dr. Carl E. Hall

Dr. Leon W. Rutland

July 1969

Blacksburg, Virginia
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>iii</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>I. INVOLUTORY MATRICES, ((\text{MOD } p)), (p &gt; 2)</td>
<td>4</td>
</tr>
<tr>
<td>II. INVOLUTORY MATRICES, ((\text{MOD } p^m)), (m &gt; 1)</td>
<td>11</td>
</tr>
<tr>
<td>III. INVOLUTORY MATRICES, ((\text{MOD } 2))</td>
<td>17</td>
</tr>
<tr>
<td>IV. INVOLUTORY MATRICES, ((\text{MOD } 2^m)), (m &gt; 1)</td>
<td>28</td>
</tr>
<tr>
<td>V. INVOLUTORY MATRICES, (\text{GENERAL MODULUS})</td>
<td>48</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>50</td>
</tr>
<tr>
<td>VITA</td>
<td>51</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

The author would like to express her sincere appreciation to [omitted] for his advice and help in the preparation of this paper. She wishes also to thank the members of the graduate faculty and the Department of Mathematics for their continued support and encouragement.

Special thanks are extended to the author's typist and to the members of her committee for their willingness to serve in that capacity.
INTRODUCTION

A square matrix, with components which are elements in the ring of integers modulo m, is involutory (mod m) if the matrix is its own multiplicative inverse. It follows that a square matrix M of order n is involutory (mod m) if and only if M satisfies the matrix congruence $X^2 - I \equiv 0 \pmod{m}$ where I denotes the identity matrix of order n.

The following practical application of involutory matrices leads to a study of the construction of involutory matrices, modulo m. Let $(p_1, p_2, \ldots, p_n)$ and $(c_1, c_2, \ldots, c_n)$ be n-tuples with components from the ring of integers modulo m. An involutory matrix M is used in algebraic cryptography to define a reciprocal correspondence between "plain letters" $(p_1, p_2, \ldots, p_n)$ and "cipher letters" $(c_1, c_2, \ldots, c_n)$. This correspondence is given by

$$PM \equiv C \pmod{m}$$

where P and C represent the row matrices $(p_1, p_2, \ldots, p_n)$ and $(c_1, c_2, \ldots, c_n)$, respectively. Since $P \equiv (PM)M \equiv CM \pmod{m}$, then the same matrix M may be used for the encipherment and decipherment of messages having a fixed numerical association (mod m).

In this paper, characterizations of involutory matrices are proved which allow the construction and enumeration of all involutory matrices (mod m), of a given order n, without duplication. An attempt is made to give simpler and more direct proofs for the main results already established by John H. Hodges [3] and Jack Levine and Robert R. Korfhage [4], [5], [6].

* The numbers in brackets refer to entries in the References.
The notations $I_k$, $J_k$, and $H_k$ are used frequently in the text and have the following meanings: $I_k$ denotes the identity matrix of order $k$; $J_k$ denotes the diagonal matrix $J_k = \text{diag} \left( I_k, I_{n-k} \right)$; and $H_k$ denotes the block-diagonal matrix $H_k = \text{diag} \left( I_{n-2k}, E_1, E_2, \ldots, E_k \right)$ where $E_i = [0, 0]$. The notation $Z_m$ is used to denote the ring of integers, modulo $m$.

The results first established in a paper by Hodges [3] are stated below in three theorems which summarize these results. The proofs of these theorems are not given here; however, equivalent theorems are given with proofs elsewhere in the text.

**Theorem 1:** Let $M$ be an $n \times n$ matrix over a finite field of order $q$. If $q$ is odd, then $M$ is involutory (mod $q$) if and only if $M$ is similar to some matrix $J_k$, where $J_k = \text{diag} \left( I_k, I_{n-k} \right)$, $0 \leq k \leq n$; if $q$ is even, then $M$ is involutory (mod $q$) if and only if $M$ is similar to some matrix $H_k$, where $H_k = \text{diag} \left( I_{n-2k}, E_1, E_2, \ldots, E_k \right)$, $0 \leq 2k \leq n$.

**Theorem 2:** The number of $n \times n$ matrices $M$ over a finite field of order $q$, with $q$ odd, which satisfy the equation $M^2 - I = 0$ is

$$N_o \{x^2 - 1, n\} = g_n \sum_{k=0}^{n} \frac{1}{g_k g_{n-k}} ,$$

where $g_s = \prod_{i=0}^{s-1} (q^s - q^i)$.

**Theorem 3:** The number of $n \times n$ matrices $M$ over a finite field of order $q$, with $q$ even, which satisfy the equation $M^2 - I = 0$ is

$$N_e \{x^2 - 1, n\} = g_n \sum_{0 \leq 2k \leq n} \frac{q^{-k(2n - 3k)}}{g_k g_{n-2k}} ,$$

where $g_s = \prod_{i=0}^{s-1} (q^s - q^i)$. 


The problem of counting all involutory matrices (mod m) without duplication is more easily solved by considering the prime power factorization of the positive integer m. Furthermore, the methods given for constructing involutory matrices (mod \( p^\alpha \)), where p is a prime number, are not identical in all cases. Therefore, each case (mod \( p^\alpha \)) is considered separately for \( p \) odd, \( p = 2 \), \( \alpha = 1 \) and \( \alpha > 1 \).
I. INVOLUTORY MATRICES (MOD p), p > 2.

Let \( p \) be a fixed odd prime number. Assume that all of the considered matrices have integers as elements. We write \( A = B \) provided \( A \equiv B \mod p \).

Let \( \mathbb{Z}_p \) be the ring of integers modulo \( p \). Let \( G = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \), with \( n \) factors. Hence, \( G \) is a vector space of dimension \( n \) with scalars in the field \( \mathbb{Z}_p \). When \( M \) denotes an involutory matrix of order \( n \), consider \( M \) as a linear transformation on \( G \).

The Fixed Space and the Negative Space

Let \( M \) be an involutory matrix. The fixed space \( F \) and the negative space \( F' \) of \( M \) are defined as follows:

\[
F = \{ a \in G \mid aM = a \}
\]

\[
F' = \{ b \in G \mid bM = -b \}
\]

It is easy to see that the sets \( F \) and \( F' \) form subspaces of \( G \).

Theorem 1.1: Let \( M \) be a square matrix of order \( n \). The matrix \( M \) is involutory \( \mod p \) if and only if \( M \) is similar to a matrix

\[
J_k = \operatorname{diag}(I_k, -I_{n-k}), \quad 0 \leq k \leq n.
\]

**Proof:** Let \( M = P^{-1}J_kP \). Since \( M^2 = (P^{-1}J_kP)(P^{-1}J_kP) = I \), then \( M \) is involutory \( \mod p \).

Let \( M \) be involutory \( \mod p \) and write \( M = P^{-1}TP \), where \( T \) is the Jordan canonical form under similarity transformation on \( M \). Then \( T \) is upper triangular with zeros above the first super-diagonal. \( M^2 = I \) implies that \( T^2 = I \), which is true if and only if \( T \) is diagonal. The matrix \( M \) has its minimal equation \( x^2 - 1 = 0 \). Therefore, \( T \), being similar to \( M \), has minimal equation \( x^2 - 1 = 0 \) and hence, eigenvalues \( +1 \) and \( -1 \). We may assume that the \( k \)
plus ones are collected in the first $k$ rows of $T$ and the $n - k$ minus ones are collected in the last $n - k$ rows of $T$. Hence,

$$T = \text{diag}(I_k, - I_{n-k}) = J_k.$$  

Note that the matrix $P$ has integral elements since the elements of $J_k$ are integers (mod $p$), the field property being preserved under similarity transformation.

**Theorem 1.2:** Let $M = P^{-1} J_k P$. If $F$ is the fixed space of $M$ and $F'$ is the negative space of $M$, then $F$ has dimension $k$ and $F'$ has dimension $n - k$. Furthermore, the first $k$ rows of $P$ form a basis for $F$ and the last $n - k$ rows of $P$ form a basis for $F'$.

**Proof:** Let $a \in G$ such that $a$ is left fixed by $M$. Then

$$aM = a(P^{-1} J_k P) = a \text{ so that } (aP^{-1})J_k = aP^{-1}. \text{ Thus, } aP^{-1} \text{ is left fixed by } J_k. \text{ Conversely, if } aP^{-1} \text{ is left fixed by } J_k, \text{ then } a \text{ is left fixed by }$$

$$P^{-1} J_k P = M.$$  

Let $aP^{-1} = w = (w_1, w_2, ..., w_n)$, $w_i \in \mathbb{Z}_p$. Since $w$ is left fixed by $J_k$, then necessarily $w_{k+1} = w_{k+2} = ... = w_n = 0$ and $w = (w_1, w_2, ..., w_k, 0, 0, ... , 0)$.

Since $J_k = \text{diag}(I_k, - I_{n-k})$, then any such vector $w$ is left fixed by $J_k$. Hence, $a$ is left fixed by $M$ if and only if

$$aP^{-1} \in \{ (w_1, w_2, ..., w_k, 0, 0, ..., 0) | w_i \in \mathbb{Z}_p \} = \{ w_1 \varepsilon_1 + w_2 \varepsilon_2 + ... + w_k \varepsilon_k | w_i \varepsilon_i \in \mathbb{Z}_p \}$$

which is the subspace generated by $\varepsilon_1, \varepsilon_2, ..., \varepsilon_k$, where $\varepsilon_i$ is the $n$-tuple with a one in the $i$-th position and zeros elsewhere (unit vectors). The vector $aP^{-1}$ belongs to the subspace generated by $\varepsilon_1, \varepsilon_2, ..., \varepsilon_k$ if and only
if \( a \) belongs to the subspace generated by \( e_1^P, e_2^P, \ldots, e_k^P \). Therefore, \( F \) is the linear span of \( e_1^P, e_2^P, \ldots, e_k^P \). Since these vectors are independent, they form a basis for \( F \). It is clear that \( e_1^P \) is the first row of \( P \), \( e_2^P \) is the second row of \( P \), ..., and \( e_k^P \) is the \( k \)-th row of \( P \). Hence, the first \( k \) rows of \( P \) form a basis for \( F \).

Let \( b \in \mathcal{G} \) such that \( b \) is in the negative space of \( \mathcal{M} \). Then \( b\mathcal{M} = b(P^{-1}J_kP) = -b \) which implies \((bP^{-1})J_k = -(bP^{-1})\). Hence, \( bP^{-1} \) is in the negative space of \( J_k \). Denote \( bP^{-1} \) by \( y = (y_1, y_2, \ldots, y_n) \), \( y_i \in \mathbb{Z}_p \). The vector \( y = (0, \ldots, 0, y_{k+1}, y_{k+2}, \ldots, y_n) \) since necessarily \( y_1 = y_2 = \ldots = y_k = 0 \). Thus, \( b \) is in the negative space of \( \mathcal{M} \) if and only if \( bP^{-1} \in \{b_{k+1}e_{k+1} + b_{k+2}e_{k+2} + \ldots + b_n e_n \mid b_i \in \mathbb{Z}_p \} \) which is the subspace generated by \( e_{k+1}, e_{k+2}, \ldots, e_n \) if and only if \( b \) is in the subspace generated by \( e_{k+1}^P, e_{k+2}^P, \ldots, e_n^P \). By an argument similar to that above \( F' \) is the linear span of \( e_{k+1}^P, e_{k+2}^P, \ldots, e_n^P \). Therefore, the last \( n - k \) rows of \( P \) form a basis for \( F' \).

**Corollary 1.3:** Let \( F \) and \( F' \) be fixed and negative spaces, respectively, of an involutory matrix \( \mathcal{M} \). Then \( \mathcal{G} = F \oplus F' \).

**Proof:** \( \mathcal{G} \) has dimension \( n \), the subspace \( F \) has dimension \( k \), and the subspace \( F' \) has dimension \( n - k \). Suppose \( z \in F \cap F' \), then \( z\mathcal{M} = z \) and \( z\mathcal{M} = -z \). Hence \( z = -z \) and \( p > 2 \) imply \( z = 0 \). Therefore, \( F \cap F' = \{0\} \) and \( \mathcal{G} = F \oplus F' \).

**Corollary 1.4:** Let \( \mathcal{M} \) and \( \mathcal{N} \) be involutory matrices. Then \( \mathcal{M} = \mathcal{N} \) if and only if \( \mathcal{M} \) and \( \mathcal{N} \) have the same fixed space and the same negative space.
Proof: If M = N, then clearly M and N have the same fixed and negative spaces.

Let F and F' denote the fixed and negative spaces, respectively. Since G = F \oplus F', then if a \in G, a can be written a = f + f' where f \in F, f' \in F'. It follows that

\[ aM = (f + f')M = fM + f'M = f - f' \]
\[ aN = (f + f')N = fN + f'N = f - f' \]

Since the linear operators M and N have the same effect on each element of G, then M = N.

**Corollary 1.5:** \( F^{-1}J_k^P = Q^{-1}J_k^Q \) if and only if the first k rows of P span the same space as the first k rows of Q and the last n - k rows of P span the same space as the last n - k rows of Q.

**Proof:** The proof of this corollary follows immediately from Corollary 1.4.

**Theorem 1.6:** The number of distinct involutory matrices of order n similar to \( J_k \) equals the number of distinct ordered pairs of subspaces (F,F') such that \( \dim F = k, \dim F' = n - k \) and \( G = F \oplus F' \).

**Proof:** Let M be an involutory matrix similar to \( J_k \), with \( M = F^{-1}J_k^P \) for some nonsingular matrix P. The first k rows of P span the fixed space F of M and the last n - k rows of P span the negative space F' of M. F and F' have the required dimensions and \( G = F \oplus F' \). By Corollary 1.4, F and F' are uniquely determined.
Suppose $F$ and $F'$ are a pair of subspaces with dimensions $k$ and $n - k$, respectively, such that $G = F \oplus F'$. Let $f_1, f_2, \ldots, f_k$ be a basis for $F$ and $t_1, t_2, \ldots, t_{n-k}$ be a basis for $F'$. Let $P$ be the square matrix with first $k$ rows $f_1, \ldots, f_k$ and last $n - k$ rows $t_1, \ldots, t_{n-k}$. Then $P$ is a nonsingular matrix and $(P^{-1}J_k P)(P^{-1}J_k P) = I$. Thus $M = P^{-1}J_k P$ is an involutory matrix. Furthermore, if $(F, F')$ determine the involutory matrix $Q^{-1}J_k Q$, then $P^{-1}J_k P = Q^{-1}J_k Q$.

**Theorem 1.7:** The number of distinct involutory matrices similar to $J_k$ is given by

$$N_k = \frac{(p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1) \ldots (p^{n-k+1} - 1)}{(p^k - 1)(p^{k-1} - 1) \ldots (p - 1)} \cdot p^{k(n-k)}$$

**Proof:** From Theorem 1.6, we have that the number of distinct involutory matrices similar to $J_k$ equals the number of ordered pairs of subspaces $F$ and $F'$ such that $F$ has dim $k$, $F'$ has dim $n - k$, and $G = F \oplus F'$. Therefore,

$$N_k = (\text{number of ways of choosing a subspace } F \text{ of dim } k) \times (\text{number of ways of choosing a subspace } F' \text{ of dim } n - k, \text{ once } F \text{ has been chosen}).$$

Since the space $G$ has $p^n$ elements, an ordered set of basis elements for a subspace $F$ may be selected from the $p^n - 1$ nonzero elements of $G$. Hence, there are $p^n - 1$ ways of choosing the first basis element for $F$. This element generates a subspace containing $p - 1$ nonzero elements;
therefore, a second basis element for $F$ may be chosen in $p^n - p$ ways.

In this manner, $k$ elements are found to form a basis for $F$ in

$$(p^n - 1)(p^n - p)(p^n - p^2) \ldots (p^n - p^{k-1})$$

ways. Since the space $F$ has order $p^k$, then $k$ generators for $F$ may be found in

$$(p^k - 1)(p^k - p) \ldots (p^k - p^{k-1})$$

ways.

(1) The number of ways of choosing a subspace $F$ of dimension $k$ is

$$\frac{(p^n - 1)(p^n - p) \ldots (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \ldots (p^k - p^{k-1})} = \frac{(p^n - 1)(p^{n-1} - 1) \ldots (p^{n-k+1} - 1)}{(p^k - 1)(p^{k-1} - 1) \ldots (p - 1)}$$

Once the subgroup $F$ has been selected, then the nonzero elements of $F'$ may be chosen from the remaining $p^n - p^k$ elements to form a basis with $n - k$ elements.

(2) The number of ways of choosing the space $F'$, after choosing $F$, is

$$\frac{(p^n - p^k)(p^n - p^{k+1})(p^n - p^{k+2}) \ldots (p^n - p^{n-1})}{(p^{n-k} - 1)(p^{n-k} - p)(p^{n-k} - p^2) \ldots (p^{n-k} - p^{n-k-1})} = p^{k(n-k)}$$

Therefore,

$$N_k = \frac{(p^n - 1)(p^{n-1} - 1) \ldots (p^{n-k+1} - 1)}{(p^k - 1)(p^{k-1} - 1) \ldots (p - 1)} \cdot p^{k(n-k)}$$

The above result is equivalent to Hodges' result,[3;519], since

$$N_k = \frac{(p^n - 1)(p^n - p) \ldots (p^n - p^{k-1})(p^n - p^k) \ldots (p^n - p^{n-1})}{(p^k - 1)(p^k - p) \ldots (p^k - p^{k-1})(p^{n-k} - 1) \ldots (p^{n-k} - p^{n-k-1})}$$

$$= \frac{g_n}{g_k g_{n-k}}, \text{ where } g_s = \prod_{i=0}^{s-1} (p^s - p^i).$$
The next corollary follows immediately from the preceding theorems and therefore, the proof is omitted.

**Corollary 1.8:** The number of involutory matrices (mod p) of order \( n \) is given by

\[
\sum_{k=0}^{n} N_k = \sum_{k=0}^{n} \frac{(p^n - 1)(p^{n-1} - 1) \ldots (p^{n-k+1} - 1)}{(p^k - 1)(p^{k-1} - 1) \ldots (p - 1)} \cdot p^{k(n-k)}
\]
Let $p$ be an odd prime and $m$ be an integer greater than one. Let $A$ and $B$ be square matrices with integral elements. In this chapter, we write $A = B$ whenever it is clear that $A = B \pmod{p^m}$.

Theorem 2.1: If $A$ is a nonsingular matrix $\pmod{p}$, then $A$ has a two-sided inverse $\pmod{p^m}$.

Proof: (The existence of an inverse for $A$ may be proved by an argument similar to that used to prove the existence of an inverse for the matrix $A$ over a field. We use a different approach here.)

It suffices to show that there are matrices $B_1$ and $B_2$ such that $B_1 A \equiv I \pmod{p^m}$ and $A B_2 \equiv I \pmod{p^m}$; for then $B_1 = B_1 (A B_2) = (B_1 A) B_2 = B_2$.

Since the matrix $A$ is nonsingular, $\pmod{p}$, there exists a matrix $B_0$ such that $A B_0 \equiv B_0 A \equiv I - p C$ for some matrix $C$. Observe that

$$A(B_0(I + p C + p^2 C^2 + \ldots + p^{m-1} C^{m-1})) = (I - p C)(I + p C + p^2 C^2 + \ldots + p^{m-1} C^{m-1})$$

$$= I - p C^m$$

$$= I$$

Also, we have $((I + p C + p^2 C^2 + \ldots + p^{m-1} C^{m-1})B_0)A = I$. Therefore $A^{-1} \pmod{p^m}$ is the matrix $B_0 \left(\sum_{k=0}^{m-1} (p C)^k\right)$ where $(p C)^m = I$.

Theorem 2.2: A square matrix $A$ of order $n$ is involutory $\pmod{p^m}$, $p > 2$, if and only if $A$ is similar $\pmod{p^m}$ to a diagonal matrix $J_t$ for some integer $t$, $0 \leq t \leq n.$

II. INVOLUTORY MATRICES ($\pmod{p^m}$), $p > 2$. 

Let $p$ be an odd prime and $m$ be an integer greater than one. Let $A$ and $B$ be square matrices with integral elements. In this chapter, we write $A = B$ whenever it is clear that $A = B \pmod{p^m}$.
Proof: Obviously, if the matrix $A$ is similar to a diagonal matrix $J_t$, then $A^2 \equiv I \pmod{p^m}$.

Let $A$ be an involutory matrix $\pmod{p^m}$. Then $A^2 \equiv I \pmod{p^m}$ and hence, $A^2 \equiv I \pmod{p}$. There exist matrices $P_1, Q_1$ and a unique matrix $J_t$, $0 \leq t \leq n$, such that $P_1Q_1 \equiv Q_1P_1 \equiv I \pmod{p}$ and $Q_1AP_1 \equiv J_t \pmod{p}$.

By induction, we show that there are matrices $P_k, Q_k$ such that $P_kQ_k \equiv I \pmod{p^k}$ and $Q_kAP_k \equiv J_t \pmod{p^k}$ whenever $k$ is a positive integer with $2 \leq k \leq m$.

Assume that there exist matrices $P_{k-1}, Q_{k-1}, N_{k-1}, M_{k-1}$, such that $P_{k-1}Q_{k-1} \equiv I + p^{k-1}N_{k-1} \equiv I \pmod{p^{k-1}}$ and $Q_{k-1}AP_{k-1} \equiv J_t + p^{k-1}M_{k-1} \equiv J_t \pmod{p^{k-1}}$.

Let us suppose that the required matrices $P_k, Q_k$ exist and have the form $P_k = P_{k-1} + p^{k-1}X$ and $Q_k = Q_{k-1} + p^{k-1}Y$, where $X$ and $Y$ are matrices. Then

\[
P_kQ_k = (P_{k-1} + p^{k-1}X)(Q_{k-1} + p^{k-1}Y)
\]
\[
= P_{k-1}Q_{k-1} + p^{k-1}XQ_{k-1} + p^{k-1}P_{k-1}Y + p^{2k-2}XY
\]
\[
= I + p^{k-1}N_{k-1} + p^{k-1}(XQ_{k-1} + p^{k-1}Y) + p^k(p^{k-2})XY
\]

It is easily shown that $P_kQ_k \equiv I \pmod{p^k}$ if and only if

\[
Y \equiv -Q_{k-1}N_{k-1} - Q_{k-1}XQ_{k-1} \pmod{p}.
\]

Therefore, with $X$ chosen arbitrarily and $Y = -(Q_{k-1}N_{k-1} + Q_{k-1}XQ_{k-1})$, we have

\[
P_kQ_k = (P_{k-1} + p^{k-1}X)(Q_{k-1} + p^{k-1}Y)
\]
\[
= I - (p^{k-1})^2N_{k-1} - (p^{k-1})^2N_{k-1}XQ_{k-1} + (p^{k-1})^2XY
\]
\[
\equiv I \pmod{p^k}.
\]
It follows from Theorem 2.1 that \( P_k Q_k \equiv Q_k P_k \equiv I \pmod{p^k} \).

Let the matrices \( P_k', Q_k' \), and \( Y \) be defined as above. We obtain the following congruence:

\[
Q_k A P_k \equiv J_t + p^{k-1} [M_{k-1} - N_{k-1} J_t - Q_{k-1} Y_{k-1} + Q_{k-1} A X] \pmod{p^k}.
\]

The congruence (1) must hold true for arbitrary \( X \); hence, letting \( X = 0 \) we obtain \( Q_k^2 P_k = J_t + p^{k-1} [M_{k-1} - N_{k-1} J_t] \pmod{p^k} \).

Since \( Q_k^2 P_k = P_k Q_k = I \pmod{p^k} \) and \( A^2 = I \pmod{p^k} \), then \((Q_k A P_k)^2 \equiv I \pmod{p^k} \). It follows that we must have

\[
[J_t + p^{k-1} (M_{k-1} - N_{k-1} J_t)]^2 \equiv I \pmod{p^k},
\]

so that \( p^{k-1} [M_{k-1} J_t - N_{k-1} + J_t M_{k-1} - J_t N_{k-1}] \equiv 0 \pmod{p^k} \). Hence, we have the following identity:

\[
M_{k-1} - N_{k-1} J_t \equiv J_t N_{k-1} - J_t M_{k-1} J_t \pmod{p}.
\]

We conclude the proof by choosing the matrix \( X = (r + 1) P_{k-1} [M_{k-1} J_t - N_{k-1}] \), where \( r = \frac{1}{2} (p^k - 1) \). It follows from (1) and (2) that

\[
Q_k^2 A P_k \equiv J_t + p^{k-1} [M_{k-1} - N_{k-1} J_t - (r + 1) Q_{k-1} P_{k-1} (M_{k-1} J_t - N_{k-1}) J_t
\]

\[
+ (r + 1) Q_{k-1} A P_{k-1} (M_{k-1} J_t - N_{k-1})] \]

\[
\equiv J_t + p^{k-1} [M_{k-1} - N_{k-1} J_t - (r + 1)(M_{k-1} - N_{k-1}) J_t] + (r + 1)(J_t M_{k-1} J_t - J_t N_{k-1})] \]

\[
\equiv J_t + p^{k-1} (2r + 1)(M_{k-1} - N_{k-1} J_t)] \]

\[
\equiv J_t \pmod{p^k}.
\]
Thus, we have found matrices $P_k$, $Q_k$ and $J_t$ with the desired properties and the theorem is proved.

Let $G = \mathbb{Z}_m \times \mathbb{Z}_m \times \cdots \times \mathbb{Z}_m$ with $n$ factors. The set $G$ is an additive abelian group of order $p^m$. We may consider $G$ as a module over the ring $\mathbb{Z}_m$ and $M$ as a linear mapping from $G$ onto $G$ whenever $M$ is an involutory matrix $(\text{mod } p^m)$ of order $n$.

From the preceding discussion, we know that the involutory matrices $(\text{mod } p^m)$ are those matrices of the form $M = PJ_kQ$ where $PQ = QP = I$ (mod $p^m$). Let $M$ be such a matrix. Let $F$ denote the set of elements left fixed by $M$ and $F'$ denote the set of elements mapped into their negatives by $M$. It is clear that $F$ and $F'$ are subgroups of $G$ and that $F \cap F' = \{0\}$. We will call $F$ the fixed group of $M$ and $F'$ the negative group of $M$.

Let $M = PJ_kQ$ be involutory. If $f \in F$, then $fM = f(PJ_kQ) = f$. It follows that $(fP)J_k = fP$; thus, $fP$ is left fixed by $J_k$. If $f' \in F'$, then $f'M = f'(PJ_kQ) = -f'$. This implies that $(f'P)J_k = -f'P$ and therefore, $f'P$ is in the negative group of $J_k$. These results are comparable to those used to prove Theorem 1.2. The proof of the following theorem is analogous to that of Theorem 1.2 and is omitted.

**Theorem 2.3:** Let $M = PJ_kQ$ be an involutory matrix $(\text{mod } p^m)$ of order $n$, where $PQ = I$ (mod $p^m$). If $F$ is the fixed group of $M$ and $F'$ is the negative group of $M$, then $F$ is generated by the first $k$ rows of the matrix $Q$ and $F'$ is generated by the last $n - k$ rows of $Q$.

**Theorem 2.4:** Let $F$ and $F'$ denote the fixed and negative groups, respectively, of an involutory matrix $M$ of order $n$. Then $G = F \oplus F'$. 
Proof: F and F' are subgroups of G. Let \( g \in G \). Then
\[
\frac{1}{2}(g + gM) \in F \text{ since } (\frac{1}{2}(g + gM))M = \frac{1}{2}gM + \frac{1}{2}gM^2 = \frac{1}{2}(g + gM).
\]
Similarly
\[
\frac{1}{2}(g - gM) \in F'. \text{ Hence, } g = \frac{1}{2}(g + gM) + \frac{1}{2}(g - gM) \text{ which is an element of } F + F'.
\]
Clearly, \( F \cap F' = \{0\} \). Therefore, \( G = F \oplus F' \).

Theorem 2.5: Let \( M \) and \( N \) be involutory matrices (mod \( p^m \)). \( M = N \) if and only if \( M \) and \( N \) have the same fixed group and the same negative group.

Proof: The proof follows from the fact that \( M \) and \( N \) have the same effect when considered as mappings on \( G \) whenever they have the same fixed and negative groups. (See the proof of Corollary 1.4).

Theorem 2.6: If \( F \) and \( F' \) are arbitrary subgroups (of \( G \)) with orders \( p^m \) and \( p^{m(n-k)} \), respectively, such that \( G = F \oplus F' \), then the ordered pair \((F,F')\) determines a unique involutory matrix \( M \) with \( F \) as its fixed group and \( F' \) as its negative group.

Proof: Let \( \{f_1, \ldots, f_k\} \) and \( \{f_1', \ldots, f_{n-k}'\} \) be sets of independent generators for the groups \( F \) and \( F' \), respectively. The matrix \( P \) having the \( n \)-tuples \( f_1', \ldots, f_k' \) as its first \( k \) rows and the \( n \)-tuples \( f_1, \ldots, f_{n-k} \) as its last \( n - k \) rows is a nonsingular matrix (mod \( p \)). Let \( M = QJ_kP \) where \( Q \) is the inverse of \( P \) (mod \( p^m \)). The matrix \( M \) is involutory (mod \( p^m \)) and has fixed group \( F \) and negative group \( F' \).

Suppose \( F \) and \( F' \) determine an involutory matrix \( N \). Then \( M \) and \( N \) have the same fixed and negative groups. Therefore, the matrix \( M \) is unique by Theorem 2.5.
Corollary 2.7: The number of involutory matrices of order \(n\) similar to \(J_k \pmod{p^m}\) equals the number of distinct ordered pairs of subgroups \(F\) and \(F'\) or orders \(p^{mk}\) and \(p^{m(n-k)}\), respectively, such that \(G = F \oplus F'\).

Proof: The proof is analogous to the proof of Theorem 1.6.

Corollary 2.8: The number of distinct involutory matrices \((\pmod{p^m})\) of order \(n\) equals \(\sum_{k=0}^{n} N_k\), where

\[
N_k = \frac{(p^{mk} - 1)(p^{m(n-1)} - 1) \ldots (p^{m(n-k+1)} - 1)}{(p^{mk} - 1)(p^{m(k-1)} - 1) \ldots (p^{m} - 1)} \cdot p^{mk(n-k)}
\]

Proof: The proof of this theorem is analogous to the proof of Theorem 1.7.
III. INVOLUTORY MATRICES (MOD 2).

In this chapter, we consider all scalars to be in the field \( \mathbb{Z}_2 \).
For a given positive integer \( n \), the \( n \)-tuples will be elements of the vector space \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 \), with \( n \) factors. We write \( A = B \) whenever it is clear that \( A \equiv B \) (mod 2).

Some of the characterizations of involutory matrices (mod 2) are similar to those found in the case (mod \( p \)), where \( p \) is an odd prime.
Again we consider involutory matrices as linear transformations on \( G \).
The following theorem has its parallel in the discussion, modulo \( p \).

Theorem 3.1: Let \( M \) be a square matrix of order \( n \). The matrix \( M \) is involutory (mod 2) if and only if \( M \) is similar to a diagonal matrix
\[
H_t = \text{diag}(I_{n-2t}, E_1, E_2, \ldots, E_t),
\]
where \( 0 \leq 2t \leq n \).

Proof: Let \( M \) be involutory (mod 2). Write \( M = P^{-1}JP \), where \( J \) is the Jordan canonical form of \( M \). Then \( J \) is a block-diagonal matrix of the form
\[
J = \begin{bmatrix}
J_{\lambda_1} & 0 & 0 & \ldots & 0 & 0 \\
0 & J_{\lambda_2} & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 0 & J_{\lambda_s}
\end{bmatrix},
\]
where \( J_{\lambda_i} = \begin{bmatrix}
\lambda_i & 1 & 0 & \ldots & 0 & 0 \\
0 & \lambda_i & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & \lambda_i & 1 \\
0 & 0 & 0 & \ldots & 0 & \lambda_i
\end{bmatrix} \]
for each \( i = 1, \ldots, s \) and \( s \leq n \). Squaring the matrix \( J \), we obtain the block-diagonal matrix \( J^2 \) partitioned by \( (J_{\lambda_i})^2 \), for \( 1 \leq i \leq s \). For each \( i \),
\((J_{\lambda_1})^2\) is the matrix
\[
\begin{pmatrix}
\lambda_1^2 & 2\lambda_1 & 1 & 0 & \ldots & 0 & 0 \\
0 & \lambda_1^2 & 2\lambda_1 & 1 & \ldots & 0 & 0 \\
& \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & 0 & \ldots & \lambda_1^2 & 2\lambda_1 \\
0 & 0 & 0 & 0 & \ldots & 0 & \lambda_1^2
\end{pmatrix}
\equiv
\begin{pmatrix}
1 & 0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & 1 & \ldots & 0 & 0 \\
& \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & 0 & \ldots & 1 & 0 \\
0 & 0 & 0 & 0 & \ldots & 0 & 1
\end{pmatrix} \pmod{2}.
\]

However, \(M^2 = (P^{-1}JP)(P^{-1}JP) = I\) implies that \(J^2 = I\). Therefore, \((J_{\lambda_1})^2\)
must be a matrix of the form \(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\) or \(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\). Hence, \(J_{\lambda_1}\) is a matrix of the
form \(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\) or the matrix of order one with element 1.

Since \(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\), then the matrix \(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\) is similar to
the matrix \(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\). Thus, there is a matrix \(Q\) such that \(M = Q^{-1}H_tQ\),
where \(t\) is the number of matrices \(J_{\lambda}\) of the form \(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\) and
\[
H_t = \text{diag}(I_{n-2t}, E_t, \ldots, E_t).
\]

Therefore, \(M\) is similar to \(H_t = \text{diag}(I_{n-2t}, E_t, \ldots, E_t)\) for unique integer \(t, 0 \leq 2t \leq n\).

Obviously, if \(M \equiv Q^{-1}H_tQ \pmod{2}\) for some matrix \(H_t = \text{diag}(I_{n-2t}, E_t, \ldots, E_t)\),
then \(M^2 \equiv I \pmod{2}\) and \(M\) is involutory.

**Theorem 3.2:** If \(M\) is an involutory matrix \(\pmod{2}\) of order \(n\), then
\(M\) leaves fixed \(2^k\) elements, where \(k \geq \left\lceil \frac{n+1}{2} \right\rceil\).
Proof: Let \( M \) be involutory (mod 2). Then \( M \) is similar to a diagonal matrix \( H_t \), where \( 0 \leq 2t \leq n \). Hence, \( M = Q^{-1} H_t Q \) for some non-singular matrix \( Q \). Let \( a \in G \) and denote \( aQ^{-1} \) by \( w = (w_1, w_2, \ldots, w_n) \). Observe that \( aM = a \) if and only if \( wH_t = w \).

Let \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \) denote unit vectors in \( G \). It is easy to see that \( H_t \) leaves fixed the vectors \( w_1 \varepsilon_1, w_2 \varepsilon_2, \ldots, w_{n-2t} \varepsilon_{n-2t} \) and the vectors of the form \( (w_1 w_2, \ldots, w_s, 0, \ldots, 0) \), where \( 2 \leq s \leq n - 2t \). Observe also that the vectors

\[
\begin{align*}
\varepsilon_{n-2t+1} e_{n-2t+1} + w_{n-2t+2} \varepsilon_{n-2t+2} + w_{n-2t+3} \varepsilon_{n-2t+3} + w_{n-2t+4} \varepsilon_{n-2t+4}, \\
\varepsilon_{n-1} e_{n-1} + w_n e_n
\end{align*}
\]

and \( w_{n-2t+1} \varepsilon_{n-2t+1} + w_{n-2t+2} \varepsilon_{n-2t+2} + w_{n-2t+3} \varepsilon_{n-2t+3} + w_{n-2t+4} \varepsilon_{n-2t+4} \ldots \) leave fixed by \( H_t \).

The least number of fixed elements for a matrix \( H_t \) result when \( n \) is even and \( t = \frac{n}{2} \); for then all of the fixed elements are sums of pairs. In this event we would have \( 2^k \) fixed elements with \( k = \frac{n}{2} \). If \( n \) is odd, then \( k \geq \frac{n+1}{2} \).

Hence, there are at least \( 2^{\left\lfloor \frac{n+1}{2} \right\rfloor} \) fixed elements corresponding to an involutory matrix (mod 2).

Remark 3.3: The set of fixed elements of an involutory matrix \( M \) is a subspace of \( G \).

It was noted at the beginning of this chapter that the group \( G = Z_2 \times Z_2 \times \ldots \times Z_2 \), with \( n \) factors, is a vector space over the field \( Z_2 \). Because of the way in which scalar multiplication is defined, it follows that any subgroup of \( G \) is also a subspace over \( Z_2 \). However, we now consider properties which are usually associated with groups.

We define an involutionary mapping of \( G \) to be an automorphism \( \mu \) such
that $\mu^2 = i$, where $i$ is the identity mapping of $G$. It is obvious that if $\mu$ is an endomorphism of $G$ such that $\mu^2 = i$, then $\mu$ is involutory.

There is an obvious one-to-one correspondence between involutory matrices $M$ and involutory mappings $\mu$. It follows that each involutory mapping $\mu$ has a corresponding fixed subgroup.

Let $\mu$ be an involutory mapping of $G$ and let $\theta$ be defined by $\theta = \mu - i$. Then $x\theta = x\mu - x$ for each $x \in G$. It is clear that $\theta$ is an endomorphism of $G$. (Observe that we write mappings on the right rather than on the left.)

**Theorem 3.4:** Let $\mu$ be an involutory mapping of $G$ with fixed group $F$. There exist a unique subgroup $F'$ of $F$ and a unique isomorphism $\phi : G/F \to F'$ such that $x\mu = x + (x + F)\phi$.

**Proof:** Let $\theta = \mu - i$, where $i$ is the identity mapping of $G$. Then for each $x \in G$, $x\theta = x\mu - x$. If $x \in F$, then $x\theta = x\mu - x = x - x = 0$.

Hence, $x$ is an element of the kernel of $\theta$ for all $x \in F$ and thus, $F \subseteq \ker \theta$. If $y \in \ker \theta$, then $y\theta = y\mu - y = 0$. This implies that $y\mu = y$ and thus, $y \in F$. Therefore, $\ker \theta \subseteq F$ which implies that $F = \ker \theta$.

Let $F'$ be the range of $\theta$. Since $F'$ is the homomorphic image of $G$ with kernel $F$, then $G/F$ is isomorphic to $F'$.

Since $(x\theta)\mu = (x\mu - x)\mu = x\mu^2 - x\mu = x - x\mu$

\[= x\mu - x\]

\[= x\theta\]

then $(x\theta)\theta = (x\theta)\mu - x\theta = x\theta - x\theta = 0$. Thus, $x\theta \in F$ for each $x$ which implies $F' \subseteq F$. 

Let φ be the canonical isomorphism from G/F onto F' induced by θ; that is, let \((C_x)φ = xθ\), where \(C_x\) is the coset in G/F containing \(x\).

Therefore, \(xμ = x + xθ\)

\[= x + (C_x)φ.\]

This last equation shows that the subgroup F' and the isomorphism φ are uniquely determined by μ.

The subgroup F' will be called the secondary group of μ.

We have shown that if μ is an involutory mapping of G, then there exist a fixed subgroup F of order \(2^k\), \(k \geq \left[\frac{n+1}{2}\right]\), and a subgroup \(F' \subseteq F\) such that G/F is isomorphic to F'. We now show that if such subgroups F and F' are given with an isomorphism φ mapping G/F onto F', then there exists a unique corresponding involutory mapping μ of G.

**Theorem 3.5:** Let F be a subgroup of G of order \(2^k\), \(k \geq \left[\frac{n+1}{2}\right]\). Let F' be a subgroup of F of order \(2^{n-k}\). Let φ be an isomorphism from G/F onto F' and define μ on G by \(xμ = x + (C_x)φ\). Then μ is involutory.

**Proof:** Suppose \(x \in F\). Since φ is an isomorphism and F is the zero element of G/F, then

\[(1) \quad xμ = x + (C_x)φ = x + (F)φ = x + 0.\]

Hence, \(xμ = x\). Conversely, if \(xμ = x\), then \(x \in F\). It follows that F is the fixed group of the mapping μ.

It is easy to show that μ is a homomorphism of G; for if \(x_1, x_2 \in G\), then

\[(x_1 + x_2)μ = (x_1 + x_2) + (C_{x_1 + x_2})φ\]

\[= (x_1 + x_2) + (C_{x_1} + C_{x_2})φ\]

\[= x_1 + (C_{x_1})φ + x_2 + (C_{x_2})φ\]

\[= x_1μ + x_2μ.\]
We now show that $\mu^2 = i$. Let $x \in G$. By the definition of the mapping $\mu$,

$$x\mu^2 = (x + (C_x)\varphi)\mu = x\mu + ((C_x)\varphi)\mu$$

We have that $(C_x)\varphi \in F' \subseteq F$ and thus, by (1), $((C_x)\mu = (C_x)\varphi$. Therefore,

$$x\mu^2 = x\mu + (C_x)\varphi$$

$$= x + (C_x)\varphi + (C_x)\varphi$$

$$= x$$

Therefore, $\mu^2 = i$, the identity mapping of $G$ and thus $\mu$ is involutory.

It is trivial to show that $\mu$ preserves scalar multiplication in the space $G$, since the scalars are 0 and 1 in this case. Thus, we may interpret Theorems 3.4 and 3.5 in terms of linear transformations on $G$ considered as a vector space.

**Corollary 3.6:** Let $F$ and $F'$ be subspaces of $G$, with $F' \subseteq F$, $\dim F = k$, $\dim F' = n - k$, where $k \geq \lfloor \frac{n+1}{2} \rfloor$. The number of involutory mappings $\mu$ with fixed space $F$ and secondary space $F'$ is given by

$$g_{n-k} = (2^{n-k} - 1)(2^{n-k} - 2) \cdots (2^{n-k} - 2^{n-k-1})$$

**Proof:** It follows from Theorem 3.5 that the number of involutory mappings $\mu$, with fixed space $F$ and secondary space $F'$, is equal to the number of isomorphisms from $G/F$ onto $F'$.

Let $v_1, v_2, \ldots, v_{n-k}$ be a basis for $G/F$. If $\varphi$ is a mapping from $\{v_1, v_2, \ldots, v_{n-k}\}$ into $F'$ such that $\{(v_1)\varphi, (v_2)\varphi, \ldots, (v_{n-k})\varphi\}$ is a
linearly independent set in $F'$, then $\varphi$ defines an isomorphism from $G/F$ onto $F'$. Such an ordered set $\{(v_1)\varphi, (v_2)\varphi, \ldots, (v_{n-k})\varphi\}$ may be chosen in $g_{n-k} = (2^{n-k} - 1)(2^{n-k} - 2) \ldots (2^{n-k} - 2^{n-k-1})$ ways.

**Theorem 3.7:** The number of involutory matrices (mod 2) of order $n$ is given by

$$g_n = \frac{\sum_{k=\left[\frac{n+1}{2}\right]}^{n} \frac{2^{k(k-n)} n-k-1}{\prod_{i=0}^{k} 2^i}}{g_k g_{n-k}},$$

where $g_s = \frac{s-1}{1} (2^s - 2^i)$.

**Proof:** For each $k$, $k \geq \left[\frac{n+1}{2}\right]$, the number of involutory matrices with fixed space of dimension $k$ and secondary space of dimension $n-k$ equals the product of the number of ways of choosing a subspace $F$ of $G$ of dimension $k$, multiplied by the number of ways of choosing a subspace $F'$ of $F$ of dimension $n-k$, multiplied by the number of possible isomorphisms between $G/F$ and $F'$.

Let $N_k$ denote the number of subspaces $F$ of $G$ of dimension $k$. It is easily shown by a proof similar to the proof of Theorem 1.7 that

$$N_k = \frac{k^{-1}}{\prod_{i=0}^{n} 2^i} (2^k - 2^i).$$

By a direct calculation, we find that

$$g_{n-k} = \frac{n-k-1}{\prod_{i=0}^{k} 2^i} (2^{n-k} - 2^i) = 2^{k(k-n)} \frac{n-k-1}{\prod_{i=0}^{k} 2^i} (2^n - 2^i),$$

and hence, we may write

$$N_k = 2^{k(k-n)} \frac{g_n}{g_k g_{n-k}},$$

where $g_s = \frac{s-1}{1} (2^s - 2^i)$. 

For fixed subspace $F$ of dimension $k$, $k \geq \lceil \frac{n+1}{2} \rceil$, let $M_k$ denote the number of subspaces of $F$ of dimension $n-k$. It follows that

$$M_k = \frac{n-k-1}{\sum_{i=0}^{n-k-1} (2^k - 2^i)}$$

However, $M_k g_{n-k} = \frac{n-k-1}{\sum_{i=0}^{n-k-1} (2^k - 2^i)}$. Therefore, by Theorem 3.6, the number of involutory matrices of order $n$ is equal to

$$g_n \sum_{k=\lceil \frac{n+1}{2} \rceil}^{\frac{n}{2}} M_k g_{n-k} = g_n \sum_{k=\lceil \frac{n+1}{2} \rceil}^{\frac{n}{2}} \frac{2^{k(n-k-1)} - 2^k}{\sum_{i=0}^{n-k-1} (2^k - 2^i)}$$

Remark 3.8: Our discussion in this chapter, along with Theorems 3.2 and 3.7, imply that the set of matrices similar to the diagonal matrix $H_t$ is in one-to-one correspondence with the set of involutory mappings with $2^{n-t}$ fixed elements.

The Construction of Involutory Matrices, (mod 2).

A method for the construction of involutory matrices (mod 2) without duplication was outlined in Theorem 3.5. We now give examples of such a construction by the use of the previous results.

Let $n = 5$ and let $F$ be the subspace generated by the vectors $(1,1,0,0,0)$, $(0,1,1,0,0)$ and $(0,1,0,0,1)$. Thus, the cosets in $G/F$ are...
given by $C_0$, $C_1$, $C_2$, and $C_3$, where

$$C_0 = F = \{(0,0,0,0,0), (1,1,0,0,0), (0,1,1,0,0), (0,1,0,0,1), (1,0,1,0,0), (1,0,0,0,1), (0,0,1,0,1), (1,1,1,0,1)\},$$

$$C_1 = \{(1,1,1,0,0) + F\} = \{(1,1,1,0,0), (0,0,1,0,0), (1,0,0,0,0), (1,0,1,0,1), (0,1,0,0,0), (0,1,1,0,1), (1,1,0,0,1), (0,0,0,0,1)\},$$

$$C_2 = \{(0,0,0,1,0) + F\} = \{(0,0,0,1,0), (1,1,0,1,0), (0,1,1,1,0), (0,1,0,1,1), (1,0,1,1,0), (1,0,0,1,1), (0,0,1,1,1), (1,1,1,1,1)\},$$

$$C_3 = \{(1,1,1,1,0) + F\} = \{(1,1,1,1,0), (0,0,1,1,0), (1,0,0,1,0), (1,0,1,1,1), (0,1,1,1,1), (1,1,0,1,1), (0,0,0,1,1)\}.$$

Let $F'$ be the subspace of $F$ generated by vectors $(1,1,0,0,0)$ and $(0,1,0,0,1)$. Then $F' = \{(0,0,0,0,0), (1,1,0,0,0), (0,1,0,0,1), (1,0,0,0,1)\}$.

Let $\varphi_1 : G/F \to F'$ be defined by $(F)\varphi_1 = (0,0,0,0,0)$, $(C_1)\varphi_1 = (1,1,0,0,0)$, $(C_2)\varphi_1 = (0,1,0,0,1)$, and $(C_3)\varphi_1 = (1,0,0,0,1)$. We define $\mu_1 : G \to G$ by
We observe that $\mu_1$ has the following effect upon the unit vectors $e_1, e_2, \ldots, e_5$:

\[
\begin{align*}
\varepsilon_1\mu_1 &= \varepsilon_1 + (C_1)v_1 = (1, 0, 0, 0, 0) + (1, 1, 0, 0, 0) = (0, 1, 0, 0, 0) = \varepsilon_2 \\
\varepsilon_2\mu_1 &= \varepsilon_2 + (C_1)v_1 = (0, 1, 0, 0, 0) + (1, 1, 0, 0, 0) = (1, 0, 0, 0, 0) = \varepsilon_1 \\
\varepsilon_3\mu_1 &= \varepsilon_3 + (C_1)v_1 = (0, 0, 1, 0, 0) + (1, 1, 0, 0, 0) = (1, 1, 1, 0, 0) \\
\varepsilon_4\mu_1 &= \varepsilon_4 + (C_2)v_1 = (0, 0, 0, 1, 0) + (0, 1, 0, 0, 1) = (0, 1, 0, 1, 1) \\
\varepsilon_5\mu_1 &= \varepsilon_5 + (C_1)v_1 = (0, 0, 0, 1, 0) + (1, 1, 0, 0, 0) = (1, 1, 0, 0, 1)
\end{align*}
\]

It follows that the matrix

\[
M_1 = \begin{bmatrix}
\varepsilon_1\mu_1 \\
\varepsilon_2\mu_1 \\
\varepsilon_3\mu_1 \\
\varepsilon_4\mu_1 \\
\varepsilon_5\mu_1
\end{bmatrix} = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1
\end{bmatrix}
\]

is involutory (mod 2).

We have seen that the involutory mapping $\mu_1$ is determined by the isomorphism $\varphi_1$. We now construct another involutory matrix $M_2$ with the same fixed and secondary spaces, but with a different associated mapping $\mu_2$.

Let $\varphi_2 : G/F \to F'$ be defined by $(F)\varphi_2 = (0, 0, 0, 0, 0), (C_1)\varphi_2 = (1, 0, 0, 0, 1), (C_2)\varphi_2 = (0, 1, 0, 0, 1) \text{ and } (C_3)\varphi_2 = (1, 1, 0, 0, 0)$. We define $\mu_2 : G \to G$ by $\chi\mu_2 = x + (C_x)\varphi_2$. Therefore,

\[
\begin{align*}
\varepsilon_1\mu_2 &= \varepsilon_1 + (C_1)\varphi_2 = (0, 0, 0, 0, 1) = \varepsilon_5 \\
\varepsilon_2\mu_2 &= \varepsilon_2 + (C_1)\varphi_2 = (1, 1, 0, 0, 1)
\end{align*}
\]
\[ \epsilon_3 \mu_2 = \epsilon_3 + (C_1) \varphi_2 = (1,0,1,0,1) \]
\[ \epsilon_4 \mu_2 = \epsilon_4 + (C_2) \varphi_2 = (0,1,0,1,1) \]
\[ \epsilon_5 \mu_2 = \epsilon_5 + (C_1) \varphi_2 = (1,0,0,0,0) = \epsilon_1 \]

The matrix

\[
M_2 = \begin{bmatrix}
\epsilon_1 \mu_2 \\
\epsilon_2 \mu_2 \\
\epsilon_3 \mu_2 \\
\epsilon_4 \mu_2 \\
\epsilon_5 \mu_2 \\
\end{bmatrix} = \begin{bmatrix}
0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

is involutory (mod 2).

The number of involutory mappings \( \mu \), and hence the number of involutory matrices, with fixed space \( F \) and secondary space \( F' \) is given by \((2^2 - 1)(2^2 - 2) = 6\).
IV. INVOLUTORY MATRICES, $(\text{mod } 2^m)$, $m > 1$.

In this chapter, we consider matrices whose rows and columns are elements of the group $G = \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} \times \ldots \times \mathbb{Z}_{2^n}$, with $n$ factors, where all components are from the subring of integers $\mathbb{Z}_{2^n}$, $m > 1$. We find the number of involutory matrices $(\text{mod } 2^m)$ of order $n$ and a method for the construction of these matrices. For elements $A$ and $B$ of $G$ or for matrices $A$ and $B$, we write $A = B$ whenever it is clear that $A = B (\text{mod } 2^m)$.

Let $x \in G$. The order of $x$ is defined to be the smallest positive integer $k$ such that $kx = (0,0,\ldots,0) = 0$. This implies that there is a smallest positive integer $c$ such that $2^c x = (0,0,\ldots,0) = 0$.

**Definition 4.1:** Let $x \in G$. The logarithmic order of $x$ is the smallest positive integer $c$ such that $2^c x = 0$. (The term logarithmic order will be frequently referred to as log order.)

Since $G$ is an abelian group of prime-power order, then any subgroup $F$ of $G$ is also abelian and of prime-power order. Hence, a subgroup $F$ of $G$ may be written as the direct sum of cyclic subgroups.

**Definition 4.2:** Let $F = C_1 \oplus C_2 \oplus \ldots \oplus C_s$, $s \leq n$, be a subgroup of $G$, where $C_1, C_2, \ldots, C_s$ are cyclic subgroups of $F$. The subgroup $F$ is said to be of type $[1^\alpha, 2^\beta, \ldots, m^\gamma]$ if $F$ contains a set of $\alpha + \beta + \ldots + \gamma = s$ independent generators, with $\alpha$ generators of logarithmic order 1, $\beta$ generators of logarithmic order 2, $\ldots$, $\gamma$ generators of logarithmic order $m$.
If $F$ is a subgroup of $G$ and $F = C_1 \oplus C_2 \oplus \ldots \oplus C_s = C'_1 \oplus C'_2 \oplus \ldots \oplus C'_h$ are two decompositions of $F$ as the direct sums of cyclic subgroups, then it follows from the Basis Theorem for Abelian Groups that $s = h$ and that the finite orders of these cyclic subgroups are invariants of $F$. Thus, the type of a subgroup $F$ characterizes the subgroup up to isomorphism. The group $G$ is of type $[m^n]$. Hence $G$ is generated by a set of $n$-independent elements all having logarithmic order $m$. One such set of generators is the set of "unit" elements in $G$ given by the set $\{s_i = (a_{11}, \ldots, a_{ij}, \ldots, a_{in}) | i=1, \ldots, n; a_{ij}=0, i \neq j, a_{ii}=1\}$.

The Fixed Group of an Involutory Matrix, (mod $2^m$)

Let $M$ be an involutory matrix (mod $2^m$). It is easy to see that $M$ has an associated set $F$ of elements left fixed by $M$ and that the set $F$ forms a subgroup of $G$. The fixed group $F$ has the following property: if $x \in G$, then $x + xM$ is an element of $F$. We consider an involutory mapping $\mu$ with fixed group $F$ to be determined by an involutory matrix with fixed group $F$. The following theorem gives an important characterization of the fixed group.

Theorem 4.3: If $m = 2$, then the fixed group $F$ of an involutory mapping $\mu$ must be of the type $[1^\alpha, 2^\beta]$, $(\alpha + \beta \leq n)$; if $m \geq 3$, then the fixed group $F$ must be of the type $[1^\alpha, (m-1)^\beta, m^\gamma]$, $(\alpha + \beta + \gamma \leq n)$.

Proof: The statement of the theorem is obvious in the cases $m = 2$ and $m = 3$. Therefore, we assume that $m \geq 4$.

Suppose that $F$ contains at least one generator of logarithmic
order \( m_0 \), with \( 1 < m_0 < m - 1 \). We will use this generator to obtain a contradiction. Let the generators of \( F \) be elements \( f_0, f_1, \ldots, f_h \) and let \( f_s \) be of log order \( m_s \) for \( s = 0, 1, \ldots, h \). Suppose that

\[
\begin{align*}
&f_1, f_2, \ldots, f_1 \text{ are of log order } m, \\
&f_{i+1}, f_{i+2}, \ldots, f_{i+j} \text{ are of log order } m - 1, \\
&f_0, f_{i+j+1}, \ldots, f_h \text{ are of log order } < m - 1.
\end{align*}
\]

For \( s = 0, 1, \ldots, h \), we may write \( f_s = 2^{m-s}g_s \), where \( g_s \) is an element of log order \( m \). Since \((f_0)^\mu = f_0\), then

\[
2^{m-m_0}(g_0)^\mu \equiv 2^{m-m_0}g_0 \pmod{2^m}.
\]

It follows from the cancellation law for congruences that

\[
(g_0)^\mu \equiv g_0 \pmod{2^{m_0}}.
\]

Therefore, \((g_0)^\mu = g_0 + 2^{m_0}x \) for some \( x \in G \). We also have that \( g_0 + (g_0)^\mu = f \) for some \( f \in F \). Thus,

\[
(1) \quad f = 2g_0 + 2^{m_0}x.
\]

Because \( F \) has generators \( f_0, f_1, \ldots, f_h \) of log orders \( m_0, m_1, \ldots, m_h \), respectively, we may express \( f \) in the following manner:

\[
(2) \quad f = c_0 g_0 + \sum_{s=1}^{i} c_s g_s + \sum_{s=1}^{j} d_s f_{i+s} + \sum_{s=1}^{h-i-j} e_s f_{i+j+s}
\]

\[
= c_0 2^{m-m_0}g_0 + \sum_{s=1}^{i} c_s g_s + \sum_{s=1}^{j} 2d_s g_{i+s} + \sum_{s=1}^{h-i-j} 2^{m-m_{i+j+s}} e_s g_{i+j+s}
\]

where \( c_0, c_s, d_s, e_s \) are elements in \( Z_{2^m} \), for each \( s \). It follows from
(1), (2) and the fact that each $g_s$ has log order $m$ that $c_s = 2c'_s$

where $c'_s \in \mathbb{Z}_{2^m}$. Therefore, we may write $f = 2f$ where

$$
\bar{f} = g_0 + 2^{m_0-1} x = c_0 2^{m-m_0-1} + \sum_{s=1}^{i} c'_sg_s + \sum_{s=1}^{i} d_s g_{i+s} + \sum_{s=1}^{h-i-j} e_s 2^{m_1-m_i+j+s} \pmod{2^{m-1}}
$$

Thus, it is trivial to show that

(3) $\bar{f} = g_0 \equiv \sum_{s=1}^{i} c'_sg_s + \sum_{s=1}^{i} d_s g_{i+s} \pmod{2}$

From (3) we obtain

(4) $2^{m-1} g_0 = 2^{m_0-1} f_0 = \sum_{s=1}^{i} c'_sf_s + \sum_{s=1}^{i} d_s g_{i+s} \pmod{2}$

Since $f_0$ has order $m_0$, then $2^{m_0-1} f_0 \neq 0$. Hence (4) is a contradiction to the fact that the elements $f_0, f_1, \ldots, f_{i+j}$ are independent generators.

**Theorem 4.4**: If $P$ is a nonsingular matrix (mod 2), then $P$ has a two-sided inverse (mod $2^m$).

**Proof**: The proof of this theorem is analogous to the proof of Theorem 2.1.

**Theorem 4.5**: Let $M$ and $N$ be similar involutory matrices (mod $2^m$), $N = P^{-1}MP$. If $F_M$ and $F_N$ are the fixed groups of $M$ and $N$, respectively, then $F_N = F_MP$.

**Proof**: It is clearly seen that the set

$$
F_N = \{ x \mid x(P^{-1}MP) = x \} = \{ x \mid (xP^{-1})M = xP^{-1} \} = \{ yP \mid yM = y \} = F_MP.
$$
Remark 4.6: The existence of the isomorphism between $F_M$ and $F_N$ given by $F_N = F_M P$ implies that the subgroups $F_M$ and $F_N$ are of the same type.

Theorem 4.7: Let $F_1$ and $F_2$ be subgroups of type $[1^\alpha, (m-1)^\beta, m^\gamma]$. There exists a nonsingular matrix $P$ such that $F_2 = F_1 P$.

Proof: Let $F_1$ be defined by the generators

$$f_{11}, f_{12}, \ldots, f_{1\gamma}; g_{11}, g_{12}, \ldots, g_{1\beta}; h_{11}, h_{12}, \ldots, h_{1\alpha}$$

and $F_2$ be defined by the generators

$$f_{21}, f_{22}, \ldots, f_{2\gamma}; g_{21}, g_{22}, \ldots, g_{2\beta}; h_{21}, h_{22}, \ldots, h_{2\alpha}$$

where the $f, g,$ and $h$ elements have logarithmic orders $m, m-1,$ and $1,$ respectively. We define two sets of $\alpha + \beta + \gamma$ independent elements, all of logarithmic order $m$, by

$$S_i = \{f_{i1}, \ldots, f_{i\gamma}; g_{i1}, \ldots, g_{i\beta}; h_{i1}, \ldots, h_{i\alpha}\},$$

$i = 1, 2$ and $g_{ij} = 2g_{ij}'$, $h_{ik} = 2^{m-1}h_{ik}'$ for $j = 1, \ldots, \beta$ and $k = 1, \ldots, \alpha$.

There exist elements $e_{i1}, \ldots, e_{i\delta}$, where $\delta = n - (\alpha + \beta + \gamma)$, all having logarithmic order $m$ such that each set

$$\overline{S}_i = \{f_{i1}, \ldots, f_{i\gamma}; g_{i1}, \ldots, g_{i\beta}; h_{i1}, \ldots, h_{i\alpha}; e_{i1}, \ldots, e_{i\delta}\},$$

$i = 1, 2$, is a basis for the group $G$. The proof of this fact is analogous to the proof that a linearly independent subset of a vector space can be extended to a basis for the space. For convenience, we relabel the elements of $\overline{S}_1$ and $\overline{S}_2$ by letting $\overline{S}_1 = \{v_1, v_2, \ldots, v_n\}$ and $\overline{S}_2 = \{w_1, w_2, \ldots, w_n\}$.
The elements of these sets can be expressed in terms of the unit elements \( e_1, \ldots, e_n \) by

\[
\begin{align*}
  v_i &= \sum_{j=1}^{n} v_{ij} e_j, \\
  w_i &= \sum_{j=1}^{n} w_{ij} e_j
\end{align*}
\]

for \( i = 1, \ldots, n \), \( v_{ij}, w_{ij} \in \mathbb{Z}_2 \).

Let \( P \) be the matrix defined by \( P = v^{-1} W \), where \( v = (v_{ij}) \) and \( W = (w_{ij}) \) are matrices defined by (5). Since \( v_i P = v_i (v^{-1} W) \)

\[
= e_i W
= w_i
\]

for each \( i = 1, \ldots, n \), then \( w_i = v_i P \) for each \( i \). It follows that \( F_2 = F_1 P \).

**Corollary 4.8:** Let \( F_1 \) and \( F_2 \) be subgroups of type \([1^\alpha, (m-1)^\beta, m^\gamma]\) where \( F_1 \) is the fixed group of an involutory matrix \( M \). There exists an involutory matrix \( N \) similar to \( M \) with \( F_2 \) as its fixed group.

**Proof:** By Theorem 4.7, there exists a matrix \( P \), nonsingular, such that \( F_2 = F_1 P \). Define the matrix \( N \) by \( N = P^{-1} M P \). The corollary follows immediately from Theorem 4.5 and the fact that \( N^2 = (P^{-1} M P)(P^{-1} M P) \equiv I \pmod{2^m} \).

**Corollary 4.9:** Let \( F_1 \) and \( F_2 \) be subgroups of \( G \) of the same type \([1^\alpha, (m-1)^\beta, m^\gamma]\) and let the complete set of involutory matrices of order \( n \) admitting \( F_1 \) as the fixed group be \( M_1, M_2, \ldots, M_k \). Then the complete set of involutory matrices of order \( n \) admitting \( F_2 \) as the fixed group is \( N_1, N_2, \ldots, N_k \), where \( N_i = P^{-1} M_1 P \) and \( F_2 = F_1 P \) for some matrix \( P \) and \( i = 1, \ldots, k \).
Proof: Let the complete set of involutory matrices admitting $F_1$ as the fixed group be the set $\Omega = \{M_1, M_2, \ldots, M_k\}$ and the complete set of involutory matrices admitting $F_2$ as the fixed group be $\mathfrak{H} = \{N_1, N_2, \ldots, N_t\}$. Since $N'_i = P^{-1} M_1 P \in \mathfrak{H}$ for each $i = 1, \ldots, k$ and $M'_i = PN_1 P^{-1} \in \Omega$ for each $i = 1, \ldots, t$ where $P$ is a nonsingular matrix such that $F_2 = F_1 P$, then $t = k$.

The Matrix Form and the Enumeration of Involutory Matrices, $(\text{mod } 2^m)$.

We will use the following procedure to enumerate all involutory matrices $(\text{mod } 2^m)$ of order $n$:

1.) Find a matrix form for all involutory matrices with a fixed group of the type $[1^\alpha, (m-1)^\beta, m^\gamma]$ and thereby find the number of involutory matrices admitting a common fixed group of type $[1^\alpha, (m-1)^\beta, m^\gamma]$;

2.) Find the number of subgroups of $G$ of the type $[1^\alpha, (m-1)^\beta, m^\gamma]$, given the integers $\alpha$, $\beta$ and $\gamma$.

Not all of the mappings defined in Chapter Three for the case modulo 2 are applicable to the case modulo $2^m$, $m > 1$, since in the first case we were able to work with a subgroup $F'$ contained in the fixed group $F$ and isomorphic to $G/F$. We now introduce coset properties which are important when we consider involutory mappings $(\text{mod } 2^m)$.

Remark 4.10: Let $\mu$ be an involutory mapping of $G$ with fixed group $F$. If $C = x + F$ is a coset in $G/F$, then $C \mu = x \mu + F$.

Theorem 4.11: Let $\mu$ be an involutory mapping of $G$ with fixed group $F$. Let $C = x + F$ be a coset in $G/F$. Then $C \mu = C$ if and only if
2x ∈ F.

**Proof:** Let \( C = x + F \). We have \( C\mu = x\mu + F \). Thus, \( C\mu = C \) if and only if \( x\mu = x + f_1 \) for some \( f_1 \in F \). Recall that \( x + x\mu \in F \) and therefore, \( x + x\mu = f_2 \) for some \( f_2 \in F \). Hence,

\[
2x = (x + x\mu) + (x - x\mu) = f_2 - f_1
\]

which implies that \( 2x \in F \).

Suppose that \( 2x = f_3 \in F \). Then

\[
x\mu = f_2 - x = f_2 - (f_3 - x) = x + (f_2 - f_3) \in x + F = C
\]

Thus, \( C\mu = x + F = C \).

It follows from the previous theorem that if \( \mu \) is an involutory mapping of \( G \), then we may consider all elements of \( G \) to be divided into the following two sets:

1.) elements \( x \) such that if \( y \in C = x + F \), then \( y\mu = C\mu = x\mu + F \) and \( C\mu \neq C \) and

2.) elements \( x \) such that if \( y \in C = x + F \), then \( y\mu \in C\mu = C \).

**Theorem 4.12:** Let \( \mu \) be an involutory mapping on \( G \) with fixed group \( F \). Let \( x \in G \) such that \( x \not\in F \), \( 2x \not\in F \), \( 2^2x \not\in F \), \( \ldots \), \( 2^{n-1}x \not\in F \), with \( 2^hx \in F \), \( h > 1 \). Let the cosets \( C_0, C_1, \ldots, C_{h-2}; C_0', C_1', \ldots, C_{h-2}' \) be defined by \( C_i = 2^ix + F \) and \( C_i' = (C_i)\mu = -2^ix + F \), \( i = 0, 1, \ldots, h - 2 \). Then no two of these cosets contain a common element.

**Proof:** Suppose that \( C_i \cap C_i' \neq \emptyset \) for some \( i = 0, 1, \ldots, h - 2 \) and thus, \( 2^ix + f_1 = -2^ix + f_2 \) for \( 2^ix + f_1 \in C_i \) and \( -2^ix + f_2 \in C_i' \). This
implies that \(2^{i+1}x = f_2 - f_1 = f_3\) and hence \(2^{i+1}x \in F\) for \(i + 1 < h\) which is a contradiction. Therefore \(C_i \cap C_i' = \emptyset\).

Let \(i > j\) and suppose that \(C_i \cap C_j \neq \emptyset\). Suppose that \(2^i x + f_1 = 2^j x + f_2\). Then \(2^{i} (2^i - 1) x = f_3 \in F\). Since \(2^{i} - 1\) is relatively prime to \(2^m\), there exists an integer \(b\) such that 
\((2^i - 1)b \equiv 1 \pmod{2^m}\) and thus, \(2^j x = bf_3 \in F\). Since \(j < h\), the last equality \((\mod 2^m)\) is a contradiction. Therefore, \(C_i \cap C_j = \emptyset\).

By arguments similar to those stated above, we find that \(C_i' \cap C_i' = \emptyset\) and \(C_i \cap C_j' = \emptyset\) for \(i = 0, 1, \ldots, h - 2\), \(j = 0, 1, \ldots, h - 2\), \(i \neq j\).

**The Matrix Form:** The number of involutory matrices admitting a common fixed group \(F\) of type \([1^\alpha, (m-1)^{\beta}, m^\gamma]\) may be calculated by first finding the number of involutory matrices admitting a common fixed group \(F_0\) of the same type having all generating elements of the form \(a_i \varepsilon_i\), where \(\varepsilon_i\) are unit elements in \(G\) and \(a_i \in \mathbb{Z}_{2^m}\), \(i = 1, \ldots, \sigma\), \(\sigma = \alpha + \beta + \gamma\).

**Theorem 4.14:** Let \(F_0\) be a subgroup of \(G\) of type \([1^\alpha, (m-1)^{\beta}, m^\gamma]\) which has generating elements of the form \(a_i \varepsilon_i\), \(i = 1, \ldots, \alpha + \beta + \gamma\). If \(F_0\) is the fixed group of an involutory mapping \(\mu\) of \(G\), then the involutory matrix \(M\) of the transformation \(\mu\) is given by

\[
M = \begin{bmatrix}
I_{\gamma} & 0 & 0 & 0 \\
0 & I_{\beta} + tB & tA & 0 \\
2C' & 2B' & -I_{\alpha} + tA' & 0 \\
C'' & 2B'' & tA'' & -I_{\delta}
\end{bmatrix}
\]

for matrices \(A, B, C, A', \ldots, C''\) and \(t = 2^{m-1}\).
Proof: Let $F_0$ be the subgroup of $G$ generated by the following elements:

$$
\begin{align*}
  f_i &= \varepsilon_i, & i &= 1, \ldots, \gamma \\
  g_j &= 2\varepsilon_{\gamma+j}, & j &= 1, \ldots, \beta \\
  h_k &= 2^{m-1}\varepsilon_{\gamma+\beta+k}, & k &= 1, \ldots, \alpha.
\end{align*}
$$

Then $F_0$ is of type $[1^\alpha, (m-1)^\beta, \gamma]$ and $\varepsilon_{\gamma+j} \notin F_0$, $2^s\varepsilon_{\gamma+\beta+k} \notin F_0$ for $j=1, \ldots, \beta$, $s < m-1$ and $k=1, \ldots, \alpha$. Also any element $f \in F_0$ may be expressed in the following manner:

$$
\begin{align*}
  (\star) \quad f &= \sum_{i=1}^{\gamma} c_i f_i + \sum_{j=1}^{\beta} b_j g_j + \sum_{k=1}^{\alpha} a_k h_k,
\end{align*}
$$

where $c_i, b_j, a_k$ are elements in $\mathbb{Z}_{2^m}$ for each $i, j$ and $k$.

Since $f_1, \ldots, f_\gamma \in F_0$, then

$$
(6) \quad (\varepsilon_i)\mu = \varepsilon_i, \quad i = 1, \ldots, \gamma.
$$

It follows from the fact that $\varepsilon_{\gamma+j} + (\varepsilon_{\gamma+j})\mu = \theta_j$ for some $\theta_j \in F_0$, $j=1, \ldots, \beta$, and the fact that $2\varepsilon_{\gamma+j} = g_j \in F_0$, but $\varepsilon_{\gamma+j} \notin F_0$ that we must have

$$
(7) \quad (\varepsilon_{\gamma+j})\mu = \varepsilon_{\gamma+j} + \eta_j, \quad j = 1, \ldots, \beta
$$

for some $\eta_j \in F_0$, such that $2\eta_j = 0$, $\eta_j \neq 0$. Also, $2\varepsilon_{\gamma+\beta+k} \notin F_0$ implies

$$
(8) \quad (\varepsilon_{\gamma+\beta+k})\mu = -\varepsilon_{\gamma+\beta+k} + \psi_k, \quad k = 1, \ldots, \alpha
$$

where $\psi_k \in F_0$ and $2^{m-1}\psi_k = 0$. Next, let $\delta = n - (\alpha + \beta + \gamma)$ and let

$$
(9) \quad (\varepsilon_{\gamma+\beta+\alpha+\rho})\mu = -\varepsilon_{\gamma+\beta+\alpha+\rho} + \varphi_{\rho}, \quad \rho = 1, \ldots, \delta
$$
where \(2e^\gamma + \beta + \alpha + \rho \notin F_o\) and \(\varphi \rho \in F_o\). Let \(t = 2^{m-1}\). Since \(\eta_j, \psi_k, \varphi_p\) are elements in \(F_o\) \((j = 1, \ldots, \beta; k = 1, \ldots, \alpha; \rho = 1, \ldots, \delta)\), then we may express \(\eta_j, \psi_k, \varphi_p\) in component form, in accord with the representation (*) as shown below:

\[
\begin{align*}
\eta_j &= (tc_{j1}, \ldots, tc_{j\beta}; tb_{j1}, \ldots, tb_{j\beta}; ta_{j1}, \ldots, ta_{j\alpha}; 0, \ldots, 0) \\
(10) \psi_k &= (2c'_{k1}, \ldots, 2c'_{k\beta}; 2b'_{k1}, \ldots, 2b'_{k\beta}; ta'_{k1}, \ldots, ta'_{k\alpha}; 0, \ldots, 0) \\
\varphi_p &= (c''_{p1}, \ldots, c''_{p\beta}; 2b''_{p1}, \ldots, 2b''_{p\beta}; ta''_{p1}, \ldots, ta''_{p\alpha}; 0, \ldots, 0)
\end{align*}
\]

The elements \(c_{ji}, c'_{ki}, c''_{pi}, \ldots, a''_{\rho k}\) are in \(Z_{2m}\). (Recall that if \(x \in G\) and \(2^sx = 0, s \leq m,\) then we may write \(x = 2^{m-s}y\) for some \(y \in G, y\) having log order \(m\).) We have \(2^{m-1}\eta_j = 0\) and \(2^{m-1}\psi_k = 0\) as required and we may easily find the elements \(e_i\mu, i = 1, \ldots, n,\) from the identities (6), ..., (10).

Let the matrices \(A, B, C; A', B', C'; A'', B'', C''\) be defined as follows:

\[
\begin{align*}
A &= (a_{jk}), \quad B = (b_{jj}), \quad C = (c_{ji}) \\
A' &= (a'_{kk}), \quad B' = (b'_{kj}), \quad C' = (c'_{ki}) \\
A'' &= (a''_{pk}), \quad B'' = (b''_{pj}), \quad C'' = (c''_{pi})
\end{align*}
\]

where \(i = 1, \ldots, \gamma; j, j' = 1, \ldots, \beta; k, k' = 1, \ldots, \alpha; \rho = 1, \ldots, \delta\). The matrix \(M\) of the transformation \(\mu\) is given by

\[
M = \begin{bmatrix}
I_{\gamma} & 0 & 0 & 0 \\
tC & I_{\beta} + tB & tA & 0 \\
2C' & 2B' & -I_{\alpha} + tA' & 0 \\
c'' & 2B'' & tA'' & -I_{\delta}
\end{bmatrix}
\]
(Recall that the i-th row of M is \( e_i \mu, i = 1, \ldots, n \).) It is easily shown by multiplication that \( M^2 \equiv I \pmod{2^m} \).

**Remark 4.15:** If \( L \) is an \( n \times n \)-matrix which has the same partitioned form as the matrix \( M \) with respect to some matrices \( A, B, C, A', \ldots, C'' \), then \( L \) will be involutory (\( \pmod{2^m} \)) and the fixed group of \( L \) will have \( F_o \) as a subgroup. This fact is easily verified and hence, the proof is omitted.

**Theorem 4.16:** Let \( L \) be an \( n \times n \)-matrix such that

\[
L = \begin{bmatrix}
I_\gamma & 0 & 0 & 0 \\
tR & I_p + tQ & tP & 0 \\
2R' & 2Q' & -I_\alpha + tP' & 0 \\
R'' & 2Q'' & tP'' & -I_\delta
\end{bmatrix}
\]

where \( t = 2^{m-1} \) and \( P, Q, R, P', \ldots, R'' \) are matrices (\( \pmod{2^m} \)). Then \( F_o \) is the fixed group of \( L \) if and only if

1.) \( \delta \leq \gamma \), and

2.) the matrix

\[
L' = \begin{bmatrix}
R & Q & P \\
R' & Q' & -I_\alpha \\
R'' & 0 & 0
\end{bmatrix}
\]

has rank \( \alpha + \beta + \delta \).

**Proof:** First, we give conditions which any element \( x \in G \) must satisfy in order that \( x \in F_L \), the fixed group of \( L \). Let \( x \in F_L \) and write \( x \) in component form as shown below:

\[
x = (u_1, u_2, \ldots, u_\gamma, v_1, v_2, \ldots, v_\beta, y_1, y_2, \ldots, y_\alpha, z_1, z_2, \ldots, z_\delta)
\]

\[
= (u, v, y, z).
\]
Since $xL = x$ if and only if $x(L - 1) = (0, 0, \ldots, 0) = 0$, then $x$ must satisfy the following set of congruences:

\begin{align*}
tvR + 2yR' + zR'' &\equiv 0 \\
tvQ + 2yQ' + 2zQ'' &\equiv 0 \\
-2y + tvP + tyP' + tzP'' &\equiv 0 \\
-2z &\equiv 0
\end{align*}

If follows that $2z \equiv 0 \pmod{2^m}$ and $4y \equiv 0 \pmod{2^m}$. Thus, it is trivial that $tz \equiv 0 \pmod{2^m}$; and if $m \geq 3$, then $ty \equiv 0 \pmod{2^m}$. We assume temporarily that $m \geq 3$ and reduce the set of congruences to the following set:

\begin{align*}
tvR + 2yR' + zR'' &\equiv 0 \\
tvQ + 2yQ' &\equiv 0 \\
tvP - 2y &\equiv 0 \\
-2z &\equiv 0
\end{align*}

Since $z \equiv 0 \pmod{2^{m-1}}$ and $2y \equiv 0 \pmod{2^{m-1}}$, we may set $z = tz'$ and $2y = ty'$ and obtain the reduced set of congruences

\begin{align*}
vR + y'R' + z'R'' &\equiv 0 \\
vQ + y'Q' &\equiv 0 \\
vP - y' &\equiv 0
\end{align*}

The first congruence in (11) represents a congruence between $1 \times \gamma$-matrices, the second represents a congruence between $1 \times \beta$-matrices and the third represents a congruence between $1 \times \alpha$-matrices. Since each component of the row-matrices must be congruent to zero, \pmod{2}, then we may express the system of congruences (11) as a system of component-congruences in the
following manner. (The subscripted matrices denote columns of the indicated matrices):

\[ vR_1 + y'R_1 + z'R_1'' = 0 \]
\[ vR_2 + y'R_2 + z'R_2'' = 0 \]
\[ \cdots \]
\[ vR_\gamma + y'R_\gamma + z'R_\gamma'' = 0 \]
\[ vQ_1 + y'Q_1 = 0 \]
\[ vQ_2 + y'Q_2 = 0 \]
\[ \cdots \]
\[ vQ_\beta + y'Q_\beta = 0 \]
\[ vP_1 + y'e_1 = 0 \]
\[ vP_2 + y'e_2 = 0 \]
\[ \cdots \]
\[ vP_\alpha + y'e_\alpha = 0 \]

(12)

There are \( \alpha + \beta + \gamma \) congruences in \( \alpha + \beta + \delta \) unknowns given in (12).

In the case \( m = 2 \), we may assume that \( \alpha = 0 \) and hence \( F_0 \) has type \([1^\beta, 2^\gamma]\). Therefore, the system (12) is reduced to \( \beta + \gamma \) congruences in \( \beta + \delta \) unknowns.

Suppose \( F_L = F_0 \) and let \( x = (u,v,y,z) \). Recalling the way in which the generators of \( F_0 \) are defined and the fact that \( x \) may be written as

\[ x = \sum_{i=1}^{\gamma} a_i e_i^{\gamma} + \sum_{j=1}^{\beta} b_j e_j^{\gamma} + \sum_{k=1}^{\alpha} c_k e_\gamma^{\gamma} + \sum_{\rho=1}^{\delta} d_\rho e_\gamma^{\gamma} + \alpha + \beta + k \]

we find that if \( x \in F_0 \), then \( tv \equiv 0 \pmod{2^m} \), \( 2y \equiv 0 \pmod{2^m} \), and \( z \equiv 0 \pmod{2^m} \). It follows that \( v \equiv 0 \pmod{2} \), \( y' \equiv 0 \pmod{2} \), and
z' \equiv 0 \pmod{2}. Therefore, the only solution to the system of congruences (12) is the trivial solution. Hence, the rank of the matrix \( L' \) is \( \alpha + \beta + \delta \) and thus, \( \delta \leq \gamma \).

In the case \( m = 2 \), it follows that \( L' \) must have rank \( \beta + \delta \) and therefore, \( \delta \leq \gamma \).

Suppose the matrix \( L' \) has rank \( \alpha + \beta + \delta \). Then the only solution to (12) is the trivial solution \( v \equiv 0 \pmod{2}, y' \equiv 0 \pmod{2}, z' \equiv 0 \pmod{2} \).

If \( x = (u,v,y,z) \) is an element in \( F \) it follows that \( x \in F_0 \).

Therefore, we have shown that if \( x \) is left fixed by the matrix \( L \), then \( x \in F_0 \) if and only if the matrix \( L' \) has rank \( \alpha + \beta + \delta \) and \( \delta \leq \gamma \).

**Corollary 4.17:** Let \( F_0 \) be a subgroup of \( G \) of type \([1^\alpha, (m - 1)^\beta, m^\gamma]\) which has generating elements of the form \( a_i \epsilon_i, a_i \in \mathbb{Z}_2^m, i = 1, \ldots, \alpha + \beta + \gamma \). Then \( F_0 \) is the fixed group of an involutory matrix \((\bmod 2^m)\) if and only if \( \alpha + \beta + 2\gamma \geq n \geq \alpha + \beta + \gamma \).

**Proof:** According to Theorem 4.16, if \( F_0 \) is the fixed group of an involutory matrix, then \( \delta = n - (\alpha + \beta + \gamma) \leq \gamma \) and hence, \( \alpha + \beta + 2\gamma \geq n \).

If \( \alpha + \beta + 2\gamma \geq n \geq \alpha + \beta + \gamma \), let \( M \) be the matrix

\[
M = \begin{bmatrix}
I_\gamma & 0 & 0 & 0 \\
0 & (1-t)I_\beta & 0 & 0 \\
0 & 0 & -I_\alpha & 0 \\
-I_\delta & 0 & 0 & -I_\delta
\end{bmatrix}
\]

where \( \delta = n - (\alpha + \beta + \gamma) \) and \( t = 2^{m-1} \). Then \( M \) is involutory \((\bmod 2^m)\) and
the associated matrix

\[
M' = \begin{bmatrix}
-\mathbf{I}_\beta & 0 \\
0 & -\mathbf{I}_\alpha \\
-\mathbf{I}_\delta & 0 & 0
\end{bmatrix}
\]

has rank $\alpha + \beta + \delta$. Applying Theorem 4.16, we find that $\mathbf{F}$ is the fixed group of $\mathbf{M}$.

The Enumeration of the Involutory Matrices: It is now easy to calculate the number of involutory matrices admitting a common fixed group of type $[1^\alpha, (m-1)^\beta, m^\gamma]$ by using the "canonical" form of the matrix $\mathbf{L}$ given in the statement of Theorem 4.16.

**Theorem 4.18:** The number of involutory matrices (mod $2^m$) of order $n$ with fixed group $\mathbf{F}$ of type $[1^\alpha, (m-1)^\beta, m^\gamma]$, and $\mathbf{F}$ being defined by generators $a_{i\epsilon}$, $i=1,\ldots, \sigma = \alpha + \beta + \gamma$, is

\[
2^K \prod_{i=0}^{\delta-1} (2^\gamma - 2^i) \prod_{i=0}^{\beta-1} (2^\sigma - 2^{\alpha + \delta + i}),
\]

where $\delta = n - \sigma$ and $K = (\sigma + \delta)[(m-1)(\beta + \gamma) + \alpha]$.

**Proof:** The number of involutory matrices admitting $\mathbf{F}$ as the fixed group is the product of the number of ways of selecting a matrix $\mathbf{L}'$ of rank $n - \gamma$ and the number of ways of selecting the matrix $\mathbf{L}$, once $\mathbf{L}'$ has been selected. Let $T_{\mathbf{L}'}$ denote the first factor of this product and $T_{\mathbf{L}}$ denote the second.

$T_{\mathbf{L}'}$ equals the number of ways of choosing linearly independent rows
in the matrix

\[
\begin{bmatrix}
R & Q & P \\
R' & Q' & -I_\alpha \\
R'' & 0 & 0
\end{bmatrix}, \quad (\text{mod } 2).
\]

We may choose the row-block \((R'',0,0)\) of \(\delta\) rows in \((2^\gamma - 1)(2^\gamma - 2)\ldots(2^\gamma - 2^{\delta-1})\) ways. Since \(R'\) and \(Q'\) may be chosen arbitrarily, then the row-block \((R',Q',-I_\alpha)\) of \(\alpha\) rows and \(\alpha + \beta + \gamma\) columns may be selected in \((2^{\gamma+\beta})^\alpha\) ways. It follows that the \(\beta\) rows of \((R,Q,P)\) may be found in

\[
(2^\sigma - 2^{\alpha+\delta})(2^\sigma - 2^{\alpha+\delta+1})\ldots(2^\sigma - 2^{\alpha+\delta+\beta-1})
\]

ways. Therefore, the matrix \(L'\) may be chosen in \(T_{L'}\) ways where

\[
T_{L'} = (2^{\gamma+\beta})^\alpha \prod_{i=0}^{\delta-1} (2^\gamma - 2^i) \prod_{i=0}^{\beta-1} (2^\sigma - 2^{\alpha+\delta+i}).
\]

Once the matrix \(L'\) has been chosen, block-matrices \(tP,tQ,tR,2R',2Q',tP',tR',tQ',tR'',tQ'',tP''\) are selected for the matrix \(L\) such that

1.) All choices for \(P,Q,R,P',P''\) are found modulo 2,
2.) All choices for \(R',Q',Q''\) are found modulo \(2^{m-1}\),
3.) \(\bar{R}' = R'\) (mod 2)
\(\bar{Q}' = Q'\) (mod 2)
\(\bar{R}'' = R''\) (mod 2).

With the conditions stated above, we may choose the matrices given in the first column below in the number of ways given in the same row of
the second column:

<table>
<thead>
<tr>
<th>Matrices</th>
<th>Number of Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>tP</td>
<td>1</td>
</tr>
<tr>
<td>tQ</td>
<td>1</td>
</tr>
<tr>
<td>tR</td>
<td>1</td>
</tr>
<tr>
<td>2R'</td>
<td>((2^{m-2}) \alpha \gamma)</td>
</tr>
<tr>
<td>2Q'</td>
<td>((2^{m-2}) \alpha \beta)</td>
</tr>
<tr>
<td>2P'</td>
<td>(2^\alpha^2)</td>
</tr>
<tr>
<td>R''</td>
<td>((2^{m-1}) \delta \gamma)</td>
</tr>
<tr>
<td>2Q''</td>
<td>((2^{m-1}) \delta \beta)</td>
</tr>
<tr>
<td>tP''</td>
<td>(2^{\delta \alpha})</td>
</tr>
</tbody>
</table>

It follows that \(T_L\) equals the product of the numbers in the second column above. Therefore,

\[
T_L = 2^{(m-1)(\alpha + \delta)(\beta + \gamma) - \alpha(\beta + \gamma) - \alpha(\alpha + \delta)}
\]

Hence, the number of involutory matrices (mod \(2^m\)) admitting \(F_0\) as the fixed group is given by

\[
T_L' T_L = 2^{(\alpha + \delta)[(m-1)(\beta + \gamma) + \alpha] \prod_{i=0}^{\delta-1} (2^\gamma - 2^i) \prod_{i=0}^{\beta-1} (2^\sigma - 2^{\alpha + \delta + i})}.
\]

**Corollary 4.19:** Let \(F\) be a subgroup of \(G\) of the type \([1^\alpha,(m-1)^\beta,m^\gamma]\) with \(\alpha + \beta + 2\gamma \geq n\). There are exactly

\[
2^K \prod_{i=0}^{\delta-1} (2^\gamma - 2^i) \prod_{i=0}^{\beta-1} (2^\sigma - 2^{\alpha + \delta + i})
\]

involutory matrices (mod \(2^m\)) of order \(n\) with fixed group \(F\), where

\[
K = (\alpha + \delta)[(m-1)(\beta + \gamma) + \alpha], \quad \delta = n - \sigma = n - (\alpha + \beta + \gamma).
\]

**Proof:** Corresponding to every subgroup \(F\) of type \([1^\alpha,(m-1)^\beta,m^\gamma]\), there exists an involutory matrix \(N = P^{-1}MP\) where \(F = F_0 P\) and the fixed
group of M is $F_0$. The corollary now follows immediately from Corollary 4.8.

We will use the Delsarte form of the Yeh-Delsarte formula ([2],[9]) to find the number of subgroups of G of the type $[1^{\alpha_1}, (m-1)^{\beta}, m^\gamma]$. We adhere to the simplification of the formula and to the terminology as given by Levine and Korfhage [6].

**Definition 4.20:** Let F be a subgroup of G of type $[1^{\alpha_1}, 2^{\alpha_2}, \ldots, m^{\alpha_m}]$, $\alpha_i \geq 0$ and let $s_i = \sum_{j=1}^{m} \alpha_j$ for $i = 1, \ldots, m$. The signature of F is given by $(s_1, s_2, \ldots, s_m)$.

Denoting the signature of G by $(k_1, k_2, \ldots, k_m)$, the Yeh-Delsarte formula for the number of subgroups F of type $[1^{\alpha_1}, 2^{\alpha_2}, \ldots, m^{\alpha_m}]$ may be written as follows:

$$N_{G,F} = 2^H \left[ \begin{array}{c} k_1 - s_2 \\ s_1 - s_2 \end{array} \right] \left[ \begin{array}{c} k_2 - s_3 \\ s_2 - s_3 \end{array} \right] \cdots \left[ \begin{array}{c} k_{m-2} - s_{m-1} \\ s_{m-2} - s_{m-1} \end{array} \right] \left[ \begin{array}{c} k_{m-1} - s_m \\ s_{m-1} - s_m \end{array} \right] \left[ \begin{array}{c} k_m \\ s_m \end{array} \right]$$

where $H = (k_1 s_2 + k_2 s_3 + \ldots + k_{m-1} s_m) - (k_1 k_2 + k_2 k_3 + \ldots + k_{m-1} k_m)$ and

$$\left[ \begin{array}{c} q \\ b \end{array} \right] = \frac{\prod_{i=0}^{b-1} (2^{n-i} - 1)}{\prod_{i=0}^{b-1} (2^{b-i} - 1)} \cdot \left[ \begin{array}{c} q \\ 0 \end{array} \right] = 1.$$

Since our group G is of type $[n^n]$, G has signature $(n, n, \ldots, n)$. A subgroup F of type $[1^{\alpha}, (m-1)^{\beta}, m^\gamma]$ has signature $(\alpha + \beta + \gamma, \beta + \gamma, \beta + \gamma, \ldots, \beta + \gamma, \gamma)$. Therefore, the number of subgroups F of G of type $[1^{\alpha}, (m-1)^{\beta}, m^\gamma]$ is

$$N_{G,F} = 2^H \left[ \begin{array}{c} n - \beta - \gamma \\ \alpha \end{array} \right] \left[ \begin{array}{c} n - \beta - \gamma \\ 0 \end{array} \right] \cdots \left[ \begin{array}{c} n - \beta - \gamma \\ 0 \end{array} \right] \left[ \begin{array}{c} n - \gamma \\ \beta \end{array} \right] \left[ \begin{array}{c} n \\ \gamma \end{array} \right]$$

$$= 2^H \left[ \begin{array}{c} n - \beta - \gamma \\ \alpha \end{array} \right] \left[ \begin{array}{c} n - \gamma \\ \beta \end{array} \right] \left[ \begin{array}{c} n \end{array} \right].$$
where
\[ H = \left( n - (\alpha + \beta + \gamma) \right) (\beta + \gamma) + \left( n - (\beta + \gamma) \right) (\beta + \gamma) + \ldots + \left( n - (\beta + \gamma) \right) (\beta + \gamma) + \left( n - (\beta + \gamma) \right) \gamma \]
\[ = (n - \alpha - \beta - \gamma) (\beta + \gamma) + (n - \beta - \gamma) (\beta + \gamma) (m - 3) + (n - \beta - \gamma) \gamma. \]
\[ = \delta (\beta + \gamma) + (\alpha + \delta) (\beta + \gamma) (m - 3) + (\alpha + \delta) \gamma \]

**Theorem 4.21:** The number of distinct involutory matrices (mod 2^m) of order \( n \) is

\[ \sum_{\alpha, \beta, \gamma} T_{L, L, N, G, F} = \sum_{\alpha, \beta, \gamma} 2^W \prod_{i=0}^{\delta-1} (2^\gamma - 2^{i+1}) \prod_{i=0}^{\beta-1} (2^\sigma - 2^{\alpha + \delta + 1}) \left[ \begin{array}{c} n - \beta - \gamma \\ \alpha \end{array} \right] \left[ \begin{array}{c} n - \gamma \\ \beta \end{array} \right] \left[ \begin{array}{c} n \\ \gamma \end{array} \right] \]

where the sums are over all \( \alpha, \beta, \gamma \) such that \( \alpha + \beta + 2\gamma \geq n \geq \alpha + \beta + \gamma \) and

\[ W = K + H = (\alpha + \delta) \left[ (2m - 4)(\beta + \gamma) + \alpha + \gamma \right] + \delta (\beta + \gamma). \]

**Proof:** The number of involutory matrices with fixed group \( F \) of type \( [1^\alpha, (m - 1)^\beta, m^\gamma] \) is given by the product \( T_{L, L, N, G, F} \) whenever \( \alpha, \beta \) and \( \gamma \) are known. The numerical value of this product is obtained by direct calculation using the previous results.

Each involutory matrix (mod 2^m) has an associated fixed group of type \( [1^\alpha, (m - 1)^\beta, m^\gamma] \) for non-negative integers \( \alpha, \beta, \gamma \). Hence, the complete set of involutory matrices (mod 2^m) of order \( n \) is the sum of all matrices having a fixed group of type \( [1^\alpha, (m - 1)^\beta, m^\gamma] \) such that \( \alpha + \beta + 2\gamma \geq n \geq \alpha + \beta + \gamma \). (Recall Theorem 4.16).
V. INVOLUTORY MATRICES, GENERAL MODULUS

We now present the construction and enumeration of involutory matrices, or order n, modulo m where m is any positive integer. Throughout this chapter, we assume the methods for the construction and the enumeration of involutory matrices developed in the four preceding chapters.

Theorem 5.1: Let \( m_1, m_2, \ldots, m_s \) be pairwise relatively prime positive integers and let \( m = m_1 \cdot m_2 \cdot \ldots \cdot m_s \). A matrix \( M \) is involutory (mod \( m \)) if and only if there exist matrices \( M_1, M_2, \ldots, M_s \) such that

1. \( M \equiv M_1 \pmod{m_1} \)
2. \( M_i^2 \equiv I \pmod{m_1} \), \( i = 1, \ldots, s \).

Furthermore, if matrices \( M_1, M_2, \ldots, M_s \) are given with the stated properties, then these matrices uniquely determine the matrix \( M \) (mod \( m \)).

Proof: Let \( M \) be involutory (mod \( m \)). Since \( M^2 = I \pmod{m} \), then \( M^2 = I \pmod{m_i} \), \( i = 1, \ldots, s \). Hence, there exist matrices \( M_1, M_2, \ldots, M_s \) such that \( M \equiv M_1 \pmod{m_1} \) and \( M_i^2 \equiv I \pmod{m_1} \) for each \( i = 1, \ldots, s \).

Let \( M_1, M_2, \ldots, M_s \) be matrices such that

\[
M_1^2 \equiv I \pmod{m_1}.
\]

We denote the element in the \( i \)-th row and \( j \)-th column (\( i = 1, \ldots, n; j = 1, \ldots, n \)) of the matrices \( M_k \) by \( m_{ij}^{(k)} \), \( k = 1, \ldots, s \), and define \( m_{ij} \) to be a solution of the system of congruences

\[
\begin{align*}
    x \equiv m_{ij}^{(1)} & \pmod{m_1} \\
    x \equiv m_{ij}^{(2)} & \pmod{m_2} \\
    & \ldots \ldots \ldots \ldots \\
    x \equiv m_{ij}^{(s)} & \pmod{m_s}.
\end{align*}
\]
Let $M$ be the matrix $M = (m_{ij})$. It is easy to see that $M$ satisfies condition 1.) and hence, $M^2 \equiv I \pmod{m_k}$, $k = 1, \ldots, s$. Since $m$ is the least common multiple of $m_1, \ldots, m_s$, then $M^2 \equiv I \pmod{m}$. Furthermore, any other solution to the set of congruences represented by (2) will determine an involutory matrix $N$ such that $N \equiv M \pmod{m}$. Therefore, all solutions are congruent to the solution obtained.

**Corollary 5.2:** Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ be the prime power factorization of a positive integer $m$. The number of distinct involutory matrices (mod $m$) of order $n$ is given by

$$T_{n,m} = \prod_{k=1}^{s} T_{n,p_k^{\alpha_k}}$$

where $T_{n,p_k^{\alpha_k}}$ denotes the number of involutory matrices (mod $p_k^{\alpha_k}$) of order $n$, $k = 1, \ldots, s$.

**Proof:** The number of choices for distinct matrices $M_1, M_2, \ldots, M_s$ which satisfy (1) will give the total number of involutory matrices $M$, (mod $m$), such that $M \equiv M_1 \pmod{m_1}$. It follows that

$$T_{n,m} = \prod_{k=1}^{s} T_{n,p_k^{\alpha_k}}$$

**Remark 5.3:** An involutory matrix (mod $m$), $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ may be constructed by the use of the general solution to congruences (2) where matrices $M_1, \ldots, M_s$ are chosen arbitrarily to satisfy (1). Thus, some or all of the methods previously developed for the construction of involutory matrices (mod $p_k^{\alpha_k}$), $k = 1, \ldots, s$, may be applied.
REFERENCES


8. Irma Reiner, The Matrix Congruence $X^2 \equiv I \pmod{p^m}$, American Mathematical Monthly, 67(1960), 773-775.

The vita has been removed from the scanned document.
IN VolUToRy MaTRICEs, MODUlo m

by

Dorothy M. Amey

Abstract

Given the prime power factorization of a positive integer m, a method for calculating the number of all distinct n x n - involutory matrices (mod m) is derived. This is done by first developing a method for the construction and enumeration of involutory matrices (mod p^α), without duplication, for each prime power modulus p^α. Using these results, formulas for the number of distinct involutory matrices (mod p^α) of order n are given where p is an odd prime, p = 2, α = 1 and α > 1.

The concept of a fixed group associated with an involutory matrix (mod p^α) is used to characterize such matrices. Involutory matrices (mod p) of order n are considered as linear transformations on a vector space of n-tuples to provide uncomplicated proofs for the basic results concerning involutory matrices over a finite field.