THE PERMANENT OF A CERTAIN MATRIX

BY

PETER J. HORN

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ARTS

in the Department
of
Mathematics

We accept this thesis as conforming to the standard required from candidates for the degree of MASTER OF ARTS.

THE UNIVERSITY OF BRITISH COLUMBIA

April, 1966
In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the Head of my Department or by his representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Mathematics

The University of British Columbia
Vancouver 8, Canada

Date 06 May 66
ABSTRACT

The purpose of this thesis is to attempt to evaluate the permanent function of a \( n \times n \) complex matrix with entries \( a_{ij} = \theta^{ij} \), \( \theta \) being a primitive \( n \)th root of unity.

If this matrix is denoted by \( A_n \) then its permanent function is given by

\[
\text{per } A_n = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\sigma \in S_n} \theta^{\sigma(1)}. 
\]

In this thesis the following results are proved. Per \( A_n \) is always an integer; with per \( A_n \equiv 0 \mod n \).

If \( n \) is even per \( A_n = 0 \).

For \( n \) odd however, the problem is in general not resolved. It is shown that if \( n = p^2 \) with \( p \) a prime, that per \( A_n \equiv 0 \mod p^4 \) and that for any prime \( n \), per \( A_n \) can be narrowed down to be one of a restricted class of numbers.
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th></th>
<th>Introduction</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>Preliminary Theorems</td>
<td>10</td>
</tr>
<tr>
<td>III</td>
<td>Some General Results on Per $A_n$</td>
<td>18</td>
</tr>
<tr>
<td>IV</td>
<td>Per $A_n$ if n is a Prime</td>
<td>21</td>
</tr>
<tr>
<td>V</td>
<td>The Case of $n=p^2$, Where p is a Prime</td>
<td>33</td>
</tr>
<tr>
<td>VI</td>
<td>Computer Results</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Bibliography</td>
<td>44</td>
</tr>
</tbody>
</table>
ACKNOWLEDGMENTS

I wish to express my sincere thanks to Dr. B.N. Moyls for all the help he has given me in the preparation of this thesis, and to whom many of the theorems and proofs are due.

I am also indebted to Dr. W. McWorter for his helpful suggestions and encouragement, and to Ted Powell for programming assistance.
I INTRODUCTION

The purpose of this thesis is to attempt to evaluate the permanent function of an $n \times n$ complex matrix with entries $a_{ij} = e^{ij}$, $\theta$ being a primitive $n^{th}$ root of unity.

(a) Permanents.

For a matrix $A$ of order $n$ with entries in some field, the permanent function of $A$ is defined by

$$\text{per } A = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)},$$

where $S_n$ is the symmetric group of order $n$. This scalar function of the matrix $A$ appears frequently in combinatorial problems concerning enumerations [1], and has the following formal properties. The $\text{per}(A)$ remains invariant under arbitrary permutations of the rows and columns of $A$ and is also invariant under transposition; i.e., $\text{per}(A) = \text{per}(A^T)$. If $\alpha$ is a scalar from the underlying field of $A$, then the multiplication of a row or column of $A$ by $\alpha$ replaces $\text{per}(A)$ by $\alpha \cdot \text{per}(A)$.

The similarity of the above definition to that of a determinant function of a matrix suggests the possibility of a computational procedure for $\text{per}(A)$ analogous to the well known theory for $\text{det}(A)$. Certain determinantal laws such as
the "Laplace Expansion Theorem", and the "Binet-Cauchy Theorem" for example have analogies for the permanent function, but the most useful property, that determinants are invariant under addition of a multiple of a row (or a column) to another row (or column), has no counterpart. This alone unfortunately invalidated the analogy for the permanent of the basic multiplicative relation, \( \det(AB) = (\det A)(\det B) \) as well as the fact that \( \det(A) \) can be expressed in terms of the characteristic roots \( \lambda_i \) of \( A \) (namely \( \det(A) = \prod \lambda_i \)).

It is these properties that are not possessed by the permanent function that allow the determinants of most matrices to be easily evaluated, and the lack of them greatly inhibits the computation of \( \text{per}(A) \) and, in fact, make it an extremely difficult problem. Many matrices have easily evaluated determinants and undetermined permanents.

Efforts to relate permanents to other more tractable matrix scalar functions, to overcome this inherit computational difficulty, have not been overly successful. In fact, it has been shown for determinants, that no uniform affixing of \( \pm \) signs to the elements of a matrix can convert the permanent into the determinant \([2]\) as well as that there is no linear operation on matrices \( T : A \rightarrow T(A) \) such that \( \text{per} T(A) = \det(A) \) for all \( A \) \([3]\). In fact, it is even a difficult problem to establish if \( \text{per}(A) \geq \det(A) \) or vice versa, for special classes of matrices.
Much work has been done recently [4] to establish bounds and inequality relations for the permanent function by presenting the permanent as an inner product in the symmetric class of completely symmetric tensors (and using the Cauchy-Schwarz inequality). The best result that can be offered at the present time regarding the permanent of a product is the following inequality obtained from this approach.

$$|\text{per}(AB)|^2 \leq (\text{per}(AA^*)) (\text{per}(B^*B))$$

where $A^* = A^T$, the transposed conjugate of A. (For unitary matrix U this inequality trivially gives the result $|\text{per } U| \leq 1$). The useful inequality $|\text{per } A| \leq \left(\frac{\sum w_i}{n}\right)^{\frac{3}{2}}$ where $w_i$ (for all $i = 1, 2, \ldots, n$) are the characteristic roots of $A^*A$, and the Binet-Cauchy relation mentioned earlier, are examples of results obtained by this technique.

To evaluate $\text{per}(A)$ directly is a formidable task if $n$ is large, even for a high speed computer, since this computation involves $n!$ permutations. (On an IBM 7040 this would take almost a day if $n = 11$ and 5 months if $n = 13$.) Various methods have been developed to avoid this evaluation of $n!$ permutations in the computation of $\text{per}(A)$: The best known is the following formula due to RYSER [5].

Let $B$ be a $n$-square matrix and let $B_r$ denote a matrix obtained from $B$ by replacing some $r$ columns of $B$ by zeros. Let $S(X)$ be the product of the row sums of the matrix $X$. 

Then
\[ \text{per } (B) = S(B) - \sum S(B_1) + \sum S(B_2) - \ldots - (-1)^{n-1} \sum S(B_{n-1}), \]
where \( S(B_r) \) denotes the sum over all \( \binom{n}{r} \) replacements of \( r \) of the columns by columns of zeros.

(b) The Matrix \( A_n \).

\( A_n \) is defined to be the \( n \)-square matrix over the complex field with general \( ij^{th} \) entry \( \theta^{ij} \), where \( \theta \) is a \( n^{th} \) primitive root of unity:

\[
\begin{bmatrix}
\theta^1 & \theta^2 & \theta^3 & \ldots & \theta^{n-1} & 1 \\
\theta^2 & \theta^4 & \theta^6 & \ldots & \theta^{n-2} & 1 \\
\theta^3 & \theta^6 & \theta^9 & \ldots & \theta^{n-3} & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\theta^{n-2} & \theta^{n-4} & \theta^{n-6} & \ldots & \theta^2 & 1 \\
\theta^{n-1} & \theta^{n-2} & \theta^{n-3} & \ldots & \theta^1 & 1 \\
1 & 1 & 1 & \ldots & 1 & 1
\end{bmatrix}
\]

i.e. \( A_n = \)

It is readily seen that \( A_n \) is independent of the choice of a primitive \( n^{th} \) root of unity.

This matrix, which is met frequently in problems concerning extreme values of hermitian forms, also occurs very naturally in the study of circulants, which are matrices of the type:
All circulant matrices of order $n$ have in common the set of orthonormal eigenvectors $\{1/\sqrt{n} \, U_k : k = 1, 2, \ldots, n\}$ where

$$U_k = \begin{bmatrix}
\theta^{1k} \\
\theta^{2k} \\
\vdots \\
\theta^{nk}
\end{bmatrix}, \quad \text{for } \theta \text{ a primitive } n^{th} \text{ root of unity.}
$$

The eigenvalues of a circulant are $\lambda_k = \sum_{j=1}^{n} c_j \theta^{k(j-1)}$, $k=1, \ldots, n$. Let $U = (U_1, U_2, \ldots, U_n)/\sqrt{n}$. Then the matrix $U$ is the unitary matrix which transforms all circulant matrices to the diagonal matrix of their eigenvalues [6],

$$U^*C \, U = \begin{bmatrix}
\lambda_1 & \cdots & 0 \\
0 & \lambda_2 & \cdots \\
0 & \cdots & \cdots \\
0 & \cdots & \cdots & \lambda_n
\end{bmatrix}, \quad \text{where } C \text{ is a circulant.}
$$

(Note that $U$ is just the matrix $A_n/\sqrt{n}$.)
By the basic multiplicative law for determinants and since the determinant of a unitary matrix has absolute value 1,

\[ \det C = \prod_{k=1}^{n} \lambda_k; \]

i.e., \( \det C = \prod_{j=1}^{n} (\sum_{j=1}^{n} \epsilon^k (j-1)) \), and the determinant of a circulant is thus easily obtained. To determine the permanent function for circulants on the other hand, poses a very difficult problem which is still unresolved.

In attempting to resolve this problem by applying the "Binet-Cauchy Theorem" we obtain

\[
\text{per } C = \sum_{\omega} 1/\mu(\omega) \text{ per } U^* [1,2,\ldots,n|\omega] \text{ per } U [w|1,2,\ldots,n] \prod \lambda_{w_t}
\]

\[
= \sum_{\omega} 1/\mu(\omega) \lambda_{w} \text{ per } U [1,2,\ldots,n|\omega]^2,
\]

where \( \omega = \{w_1,w_2,\ldots,w_n\} \), \( 1 \leq w_1, \ldots, \leq w_n \leq n; \)

\( \lambda_w = \lambda_{w_1} \lambda_{w_2} \ldots \lambda_{w_n} \); and \( \mu(\omega) \) is the product of the multiplicities of the distinct integers appearing in the sequence \( \omega \). This leads to the study of per \( (U) \) or since \( U = A_n/\sqrt{n} \) to the study of per \( A_n \).

This matrix \( A_n \) is indeed interesting in its own right.

\( A_n \) is normal (i.e., \( A_n A_n^* = A_n^* A_n \)).

\( A_n/\sqrt{n} \) is unitary (i.e., \( A_n^{-1}/\sqrt{n} = A_n^*/\sqrt{n} \)).

\( A_n \) can also be put in equivalent forms by elementary row and column operations such that the permanent remains invariant.
In one equivalent form it is a Vandermonde matrix.

\[ B = \begin{pmatrix} 1 & r_1 & r_1^2 & \cdots & r_1^{n-1} \\ 1 & r_2 & r_2^2 & \cdots & r_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & r_{n-1} & r_{n-1}^2 & \cdots & r_{n-1}^{n-1} \end{pmatrix} \]

Since \( \text{per} A_n = \text{per}(\theta^{ij}) \) by definition,

\[ = (\theta^1, \theta^2, \ldots, \theta^n)^n \text{per}(\theta^{ij}), \]

by taking \( \theta^i \) out of \( i \)th row of \( A_n \),

\[ = \theta^n(n+1)/2 \text{ per}(\theta^{ij}). \]

\[ \text{per} A_n = \begin{cases} \text{per}(\theta^{ij}) & \text{if } n \text{ odd,} \\ -\text{per}(\theta^{ij}) & \text{if } n \text{ even,} \end{cases} \]

where \( (\theta^{ij}) \) is a Vandermonde matrix.

In another equivalent form \( A_n \) is a circulant. If \( (\theta^{ij}) \) denotes the matrix with general \( ij \)th entry \( \theta^{ij} \), then \( (\theta^{ij}) \) is a circulant and is easily shown to be equivalent to \( A_n \), with \( \text{per} A_n = \text{per}(\theta^{ij}) \).

The determinants of all the matrices mentioned above are readily found but almost nothing can be said about the permanent of any of them.
(c) The Permanent of $A_n$.

Per($A_n$) can be computed by hand without too much difficulty for $n = 2, 3, 4, 5$ to give;

\[
\begin{align*}
\text{per}(A_2) &= 0, \\
\text{per}(A_3) &= -3, \\
\text{per}(A_4) &= 0, \\
\text{per}(A_5) &= -5.
\end{align*}
\]

One would perhaps conjecture from these values that per($A_n$) equals 0 for $n$ even and equals $-n$ for $n$ odd. The former proves to be correct. The latter is destroyed by the result for $n = 7$:

\[
\text{per}(A_7) = -3 \cdot 5 \cdot 7 = -105.
\]

This result and those for $n = 9, 11, 13$ were obtained by use of the University of British Columbia's IBM 7040 computer.

\[
\begin{align*}
\text{per}(A_9) &= +3^4 = +81, \\
\text{per}(A_{11}) &= 3 \cdot 5 \cdot 11 \cdot 41 = 6765, \\
\text{per}(A_{13}) &= 11 \cdot 13 \cdot 1229 = 175747.
\end{align*}
\]

These results which were also communicated by Professor D.H. Lehmer of the Department of Mathematics, University of Santa Barbara, California, do not appear to present any simple pattern.

As we shall subsequently see, the permanent of $A_n$ is always an integer and is always divisible by $n$. In particular if $n=p^2$, where $p$ is a prime, then per($A_n$) is divisible by $p^4$. By using any of a variety of permanent
inequalities [7] we can show \(-\sqrt{n^n} \leq \text{per}(A_n) \leq \sqrt{n^n}\) or equivalently that \(-|\det(A_n)| \leq \text{per}(A_n) \leq |\det(A_n)|\) (since \((\det(A_n))^2 = n^2\)). For \(n\) even, \(\text{per}(A_n)\) is determined (=0) but for \(n\) odd the problem remains generally unresolved. In Section IV of this thesis we investigate the case of \(n\) prime, \(n > 3\); the best result obtained, is that the permanent of \(A_n\) can be narrowed down to be one of a restricted set of integers.

Since \(\text{per}(A_n) = \sum_{\sigma \in S_n} \theta^{i(\sigma)}\)

\[= \sum_{k=0}^{n-1} a_k \theta^k.\]

where \(a_k\) denotes the number of permutations \(\sigma \in S_n\) s.t. \(\sum_{i=1}^{n} i \sigma(i) \equiv k \pmod{n}\), we can attempt to find \(\text{per}(A_n)\) by resolving the alternate number theory problem, of finding the number of permutations \(\sigma\) in the symmetric group \(S_n\), such that \(\sum_{i=1}^{n} i \sigma(i) \equiv k \pmod{n}\), for \(k=0,1,2,...,n-1\).

It is easily seen that if \(n\) is a prime these two problems are equivalent. In the proof of the results that follow, almost no linear algebra is used; the approach generally being to find the permanent of \(A_n\) by solving this second problem. This involves for the most part a study of the symmetric group \(S_n\).
II PRELIMINARY THEOREMS

The following lemma shows that $\text{per } A_n$ is independent of the choice of the primitive $n^{th}$ root of unity.

**Lemma 2.1.** If $A_n = (\theta_{ij})$ is $n \times n$, where $\theta$ is a primitive $n^{th}$ root of unity, and $k$ is a positive integer such that $(k,n) = 1$, then

$$\text{per}(\theta_{ij}) = \text{per}(\theta_{kij}).$$

**Proof:** Since $(k,n) = 1$, $kj \text{ (mod } n) = \sigma(j)$ where $\sigma$ is a permutation in $S_n$. Thus

$$\text{per}(\theta_{kij}) = \text{per}(\theta_{i\sigma(j)}).$$

The matrix $(\theta_{i\sigma(j)})$, however, is just the matrix $(\theta_{ij})$ with its columns permuted according to the permutation $\sigma$. Since the permanent of a matrix is invariant under permutations of rows or columns,

$$\text{per}(\theta_{kij}) = \text{per}(\theta_{ij}).$$

Q.E.D.

The permanent of $A_n$ is obviously a polynomial in $\theta$:

$$\text{per } A_n = \text{per}(\theta_{ij})$$

$$= \sum_{\sigma \in S_n} \theta_{1\sigma(1)}$$

$$= \sum_{\sigma \in S_n} \theta_i \theta_j \sigma(1).$$
Hence
\[
\text{per}(\theta^{ij}) = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}, \quad (1)
\]
where \(a_j\) is the number of permutations \(\sigma \in S_n\) such that
\[
\sum_{i=1}^{n} i\sigma(i) \equiv j (\text{mod } n). \quad (2)
\]
We are thus presented with an interesting problem in number theory, which to the best of our knowledge, has not been solved.

Not all of the coefficients in (1) can be distinct. More precisely, we have

**Theorem 2.2.** If \((k,n) = 1\), then in the representation
\[
\text{per} A_n = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1},
\]
\[
a_i = a_{ki}\text{(mod } n)\] for \(i = 1, \ldots, n-1\).

**Proof:**
\[
\text{per}(\theta^{kij}) = \text{per}((\theta^k)^{ij})
\]
\[
= a_0 + a_1\theta^k + \ldots + \theta^{k(n-1)}.
\]
By Lemma 2.1, \(\text{per}(\theta^{kij}) = \text{per}(\theta^{ij})\),
therefore
\[
\sum_{i=1}^{n-1} a_i\theta^{ki} = \sum_{i=1}^{n-1} a_1\theta^i.
\]
Since \(\theta, \theta^2, \ldots, \theta^{n-1}\) are linearly independent over the real numbers,
\[
a_i = a_{ki}\text{(mod } n)\] for \(i = 1, \ldots, n-1\).

Q.E.D.
Corollary 2.3. If \( n \) is a prime, \( n > 2 \), then in the representation

\[
\text{per } A_n = a_0 + a_1 \theta + \cdots + a_{n-1} \theta^{n-1}, \quad (1)
\]

\[a_1 = a_2 = \cdots = a_{n-1}.
\]

Proof: If \( n \) is prime, \( (k,n) = 1 \) for all \( 1 \leq k \leq n-1 \). Thus by Theorem 2.2,

\[a_k = a_1, \quad \text{for } 1 \leq k \leq n-1.
\]

Q.E.D.

In Theorem 2.2 we showed a relationship between the \( a_i \) for \( 1 \leq i \leq n-1 \). The question whether \( a_0 \) can be related to any of the other \( a_i \), is answered if \( n \) is even in the next Theorem. We first require the following lemma.

Lemma 2.4. If \( \sigma \) is any permutation \( \in S_n \) where \( n \) is even, and \( \rho \) is the full cycle permutation; \( \rho = (1, 2, 3, \ldots, n) \), then

\[
\sum_{i=1}^{n} i(\sigma \rho)(i) \equiv \sum_{i=1}^{n} i\sigma(i) + n/2 \pmod{n}.
\]

Proof: \[
\sum_{i=1}^{n} i(\sigma \rho)(i) = \sum_{i=1}^{n} i[(\sigma(i) + 1)(\mod{n})],
\]

since \( (\sigma \rho)(i) = (\sigma(i) + 1)(\mod{n}) \).

\[
\sum_{i=1}^{n} i(\sigma \rho)(i) \equiv \sum_{i=1}^{n} i\sigma(i) + \sum_{i=1}^{n} 1 \pmod{n}
\]

\[
= \sum_{i=1}^{n} i\sigma(i) + (n+1)n/2 \pmod{n}
\]

\[
= \sum_{i=1}^{n} i\sigma(i) + n/2 \pmod{n}, \quad \text{since } n \text{ is even.}
\]

Q.E.D.
Theorem 2.5. If $n$ is even, $a_i = a_{(i+n/2)\mod n}$ for $i = 0, 1, \ldots, n-1$.

Proof: Let $k$ be any natural number from 1 to $n$.

Consider the set

$$X_k = \{ \sigma \in S_n \mid \sum_{\sigma(i)} i \equiv k \pmod{n} \}; \ k = 0, \ldots, n-1.$$ 

If $\rho = (1, 2, 3, \ldots, n)$ we have by the previous lemma

$$\sum_{i=1}^{n} i(\sigma \rho)(i) \equiv \sum_{i=1}^{n} i\sigma(1) + n/2 \pmod{n} \ \forall \sigma \in X_k$$

$$= k + n/2 \pmod{n}.$$ 

Since for $\sigma, \tau \in S_n$ with $\sigma \neq \tau$, $\sigma \rho \neq \tau \rho$

Therefore $|X_{(k+n/2)\mod n}| \geq |X_k|$ where $|X_k|$ denotes the number of elements in $X_k$.

Similarly if we consider $\sigma \in X_{(k+n/2)\mod n}$

we obtain

$$|X_{((k+n/2)+n/2)\mod n}| \geq |X_{(k+n/2)\mod n}|.$$

i.e., $|X_k| \geq |X_{(k+n/2)\mod n}|$.

Therefore we have that the number of permutations $\sigma \in S_n$ that give $\sum_{i=1}^{n} i\sigma(1) \equiv k \pmod{n}$ is equal to the number that give $\sum_{i=1}^{n} i \tau(1) \equiv k + n/2 \pmod{n}$.

i.e., $a_i = a_{(i+n/2)\mod n}$ for $i = 0, \ldots, n-1$.

Q.E.D.

Observe that $S_n = \bigcup_{k=0}^{n-1} X_k$. 

Theorem 2.2 gives the relation $|X_j| = |X_j k \text{mod } n|$ where $(k,n) = 1$. We would now like to look at the parity of the permutations in $X_j$.

Let $X_j^+$ and $X_j^-$ denote the sets of even and odd permutations in $X_j$ respectively, with $|X_j^+| = a_j^+$, $|X_j^-| = a_j^-$ where $a_j^+ + a_j^- = a_j$.

The analogy to Theorem 2.2 with $X_j^+$ or $X_j^-$ replacing $X_j$ is not generally true. For the case $k = n-1$ we can state the following.

Theorem 2.6. (a) If $n$ is odd, $(n-1)/2$ even, or if $n$ and $(n-2)/2$ are both even, then

$$a_j^+ = a_j^{(n-1) \text{mod } n}, \text{ and } a_j^- = a_j^{(n-1) \text{mod } n}, \quad j = 0, 1, \ldots, n.$$  

(b) If $n$ is even, $(n-2)/2$ odd, or if $n$ and $(n-1)/2$ are both odd, then

$$a_j^+ = a_j^{(n-1) \text{mod } n} \quad \text{for } j = 0, 1, \ldots, n-1.$$  

Proof: Let $\sigma \in S_n$ be an arbitrary permutation and let

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & \cdots & (n-1) & n \\ (n-1) & (n-2) & \cdots & 1 & n \end{pmatrix}$$

$$\sigma \gamma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ (n-1) & (n-2) & \cdots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \cdots & n \\ n-\sigma(1) & n-\sigma(2) & \cdots & n-\sigma(n) \end{pmatrix}$$

i.e., $(\sigma \gamma)(1) = n - \sigma(1)$.

Thus

$$\sum_{i=1}^n i(\sigma \gamma)(i) = \sum_{i=1}^n i(n - \sigma(1))$$

$$= (n-1) \sum_{i=1}^n i\sigma(1) \text{(mod n)},$$
i.e., If \( \sigma \in X_j \) then \( \sigma \gamma \in X_j^{(n-1) \text{mod } n} \). This gives a one-to-one mapping of \( X_j \) onto \( X_j^{(n-1) \text{mod } n} \). (Since if \( \sigma \gamma = \tau \gamma \) then \( \sigma = \tau \).) It is readily checked that \( \gamma \) is an even permutation if \( n \) is odd, \((n-1)/2 \) even, or if \( n \), \((n-2)/2 \) are both even. Similarly \( \gamma \) is an odd permutation if \( n \) is even, \((n-2)/2 \) odd, or if \( n \) and \((n-1)/2 \) are both odd.

Finally since the product of two even permutations is even, the product of an odd and an even is an odd permutation, etc., the result is proved.

Q.E.D.

**Theorem 2.7.** If \( n \) is even, \((n-2)/2 \) odd, or if \( n \) and \((n-1)/2 \) are both odd, then \( X_o \) has an equal number of even and odd permutations.

**Proof:** Consider any \( \sigma \in X_o \) with \( \sigma \) even. As in the previous theorem, if

\[
\gamma = \begin{pmatrix}
1, & 2, & 3, & \ldots, & i, & \ldots & n
\end{pmatrix},
\]

then

\[
\sum_{i=1}^{n} i(\sigma \gamma)(i) \equiv (n-1) \sum_{i=1}^{n} i^1(1) \pmod{n}
\]

\[
= 0, \text{ since } \sum_{i=1}^{n} i^1(1) \pmod{n} \equiv 0.
\]

\( \therefore \quad (\sigma \gamma) \in X_o. \)

Since \( \gamma \) under the conditions of this theorem is an odd permutation, there is thus a one-to-one mapping of the even permutations of \( X_o \) onto the odd permutations of \( X_o \).

Q.E.D.
Theorem 2.8. If \( r \mid n \), say \( r \cdot n_1 = n \) and if \( R = \{ x \mid x \equiv kr \pmod{n} \, (k,n)=1, \, 1 \leq k \leq n \} \), then \( S = \sum_{x \in R} \theta^x \) is an integer.

Proof:

(a) Let \( r_1, r_2, \ldots, r_m = 1 \) be an ordered listing of all the divisors of \( n \), with \( r_i > r_{i+1} \), \( i = 1, \ldots, m-1 \).

Let

\[
R' = \{ \, 1r_1, 2r_1, \ldots, (n_1-1)r_1 \, \} \quad \text{where} \quad n_1 \cdot r_1 = n,
\]

\[
R'_2 = \{ \, 1r_2, 2r_2, \ldots, (n_2-1)r_2 \, \} \quad \text{where} \quad n_2 \cdot r_2 = n,
\]

\[
\vdots
\]

\[
R'_m = \{ \, 1, 2, \ldots, n-1 \, \} \quad \text{where} \quad n \cdot 1 = n,
\]

and define

\[
R_1 = R'
\]

\[
R_2 = R'_2 - (R'_2 \cap R_1)
\]

\[
\vdots
\]

\[
R_m = R_m - \bigcup_{i=1}^{m-1} (R'_i \cap R_1).
\]

It is easily seen that all \( R_j \) are disjoint, and that

\[
R_j = \{ x \mid x \equiv kr \pmod{n} \, (k,n)=1, \, 1 \leq k \leq n \} \quad j = 1, 2, \ldots, m.
\]

(b) To show \( S_j = \sum_{x \in R_j} \theta^x \) is an integer \( \forall j = 1, \ldots, m \) we proceed by induction as follows.
(1) \( S_1 = \sum_{i=1}^{n-1} \theta^i = -1, \) an integer

(2) Assume that all \( S_i \) are integers for \( i = 1, \ldots, k-1 \)

(3) To show \( S_k \) is an integer, consider

\[
S'_k = \sum_{i \in R'_k} \theta^x = \sum_{i \in R'_k} \theta^{r_i} = -1.
\]

By definition \( R_k = R'_k \setminus \bigcup_{i=1}^{k-1} (R_k' \cap R_i) \).

If \( r_k / r_1 \) then \( R_k' \cap R_1 = R_1 \) by construction of \( R_1 \) and \( R_k' \).

If \( r_k / r_1 \) then \( R_k' \cap R_1 = 0 \),

since say \( x \in R_k' \cap R_1 \).

Let \( r_{ki} \) be the L.C.M. of \( r_k \) and \( r_1 \).

\( \therefore r_{ki} / x \) and also \( r_{ki} / n \)

Since \( r_{ki} \) is higher in the list \( r_1, r_2, \ldots, r_n \)

than \( r_1 \), this implies \( x \in R_{ki} \), which gives a contradiction,

since \( R_j \) are disjoint.

We can now write \( S_k \) as follows.

\[
S_k = \sum_{x \in R'_k} \theta^x - \sum_{i} \left[ \sum_{x \in R'_k} \theta^x \right] \quad \text{where the summation over } i,
\]

\[
= S'_k - \sum_{i} S_i \quad \text{is for all } i,
\]

\( \text{s.t. } R_1 \cap R_k' \neq \emptyset. \)

\( \therefore S_k = (-1) - \sum_{i} (\text{integer}), \) since the \( S_i \) are integers by the induction hypothesis.

Q.E.D.
III SOME GENERAL RESULTS ON PER $A_n$.

Theorem 3.1. If $n$ is even, $\text{per } A_n = 0$.

Proof: 

$$\text{Per}(A_n) = a_0 \theta^0 + a_1 \theta^1 + \ldots + a_{n-1} \theta^{n-1}$$

$$= (a_0 \theta^0 + a_{n/2} \theta^{n/2}) + (a_1 \theta^1 + a_{(n/2+1)} \theta^{(n/2+1)}) + \ldots + (a_{(n/2-1)} \theta^{(n/2-1)} + a_{n-1} \theta^{n-1}).$$

By Theorem 2.5

$$a_i = a_{(i+n/2)}, \text{ for } i = 0, \ldots, n-1.$$

Therefore 

$$\text{Per}(A_n) = a_0 (\theta^0 + \theta^{n/2}) + a_1 (\theta^1 + \theta^{(n/2+1)}) + \ldots + a_{(n/2-1)} (\theta^{(n/2-1)} + \theta^{n-1}).$$

But 

$$\theta^k + \theta^{(n/2+k)} = \theta^k + \theta^{n/2} \cdot \theta^k = \theta^k + (-1) \theta^k$$

$$= 0 \text{ for any } k.$$

Thus the result is proved.

Q.E.D.
Theorem 3.2. Per $A_n$ is an integer.

Proof: It is easily seen that we can write

$$\text{per } A_n = a_o \theta^0 + \sum \left[ \sum_{x \in R_i} a_x \theta^x \right]$$

where $R_i = \{ x | x \equiv kr_i \pmod{n} \} \quad (k,n)=1, \quad 1 \leq k \leq n$

and the summation $\sum_{i}$ is over all $i$, such that $r_i \mid n$.

(Note that $R_1$ does not contain $n$; hence $a_0 \theta^0$ term in (3).)

Since by Theorem 2.2, $a_i = a_{ik(n \cdot m \pmod{n})}$ for all $i = 1, \ldots, n$
and for $1 \leq k \leq n, \quad (k,n)=1$,

therefore

$$\text{per } A_n = a_o + \sum_{i} [a_{1i} \sum_{x \in R_i} \theta^x] \quad (4)$$

But by Theorem 2.8 $\sum_{x \in R_i} \theta^x$ is an integer.

Therefore per $A_n$ is an integer.

Q.E.D.

Theorem 3.3. Per $A_n = 0 \pmod{n}$

Proof: If $n$ is even the theorem is obviously true since

per $A_n = 0$.

The theorem is also true if $n$ is odd, but we are not yet
in the position to prove this. It will follow from

Theorem 4.2 that $n/a_i$ for $i = 0, 1, 2, \ldots, n-1$.

This fact together with Theorem 2.8 gives the result.

Q.E.D.
**Theorem 3.4.** Let \( \text{per } A_n = a_0 + a_1 \theta^1 + \ldots + a_{n-1} \theta^{n-1} \),

If \( n \) is an odd prime, then

\[ \text{per } A_n = a_0 - a_1. \]

**Proof:** By Corollary 2.3

\[ a_1 = a_2 = \ldots = a_{n-1}. \]

Therefore

\[ \text{per } A_n = a_0 + a_1 (\theta^1 + \theta^2 + \ldots + \theta^{n-1}) = a_0 + a_1 (-1) = a_0 - a_1. \]

Q.E.D.

**Theorem 3.5.** Let \( \text{per } A_n = a_0 + a_1 \theta^1 + \ldots + a_{n-1} \theta^{n-1} \),

where \( n \) is the square of a prime \( p \). Then

\[ \text{per } A_n = a_0 - a_p. \]

**Proof:** Let \( Y_n \) be the set of residues mod \( n \) which are relatively prime to \( n \). Then by Theorem 2.2

\[ a_1 = a_{1k} \pmod{n}, \quad \text{for } k \in Y_n. \]

For \( n = p^2 \), the only numbers less than \( n \) not relatively prime to \( n \) are \( p, 2p, \ldots, (p-1)p \).

It follows that

\[ \text{per } A_n = a_0 + a_1 \sum_{k \in Y_n} \theta^k + a_p \sum_{j=1}^{p-1} \theta^{jp}. \]

Now

\[ \sum_{k \in Y_n} \theta^1 = -1, \]

and

\[ \sum_{j=1}^{p-1} \theta^{jp} = -1. \]

Subtracting,

\[ \sum_{k \in Y_n} \theta^k = 0. \]

Thus

\[ \text{per } A_n = a_0 + a_1 (0) + a_p (-1) = a_0 - a_p. \]

Q.E.D.
IV PER $A_n$ IF $n$ IS A PRIME $> 3$.

The aim in this section is to show that if $n$ prime, $n > 3$, then the permanent of $A_n$ is limited to be one of a restricted class of odd integers. Most of the preliminary Theorems used here are stated and proved in greater generality than is needed for the above result.

Let $\sigma$ denote an arbitrary permutation in $S_n$, and $\rho$ the full cycle permutation $(1, 2, 3, \ldots, n)$

i.e. $\rho = \begin{pmatrix} 1, 2, 3, \ldots, n \\ 2, 3, 4, \ldots, 1 \end{pmatrix}$.

It is easy to check that

$$\rho^2 = \begin{pmatrix} 1, 2, 3, \ldots, n \\ 2, 3, 4, \ldots, 1 \end{pmatrix} \begin{pmatrix} 1, 2, 3, \ldots, n \\ 2, 3, 4, \ldots, 1 \end{pmatrix} = \begin{pmatrix} 1, 2, 3, \ldots, n \\ 3, 4, 5, \ldots, 2 \end{pmatrix},$$

and in general that

$$\rho^k = \begin{pmatrix} 1, 2, 3, \ldots, n \\ \rho_{(1)}^k, \rho_{(2)}^k, \rho_{(3)}^k, \ldots, \rho_{(n)}^k \end{pmatrix},$$

where $\rho_{(i)}^k = (k+1) \text{mod } n$. If

$$\sigma^- = \begin{pmatrix} 1, 2, 3, \ldots, n \\ \sigma_{(1)}, \sigma_{(2)}, \sigma_{(3)}, \ldots, \sigma_{(n)} \end{pmatrix},$$
when
\[ \rho \sigma = \begin{pmatrix} 1, 2, 3, \ldots, n \\ 2, 3, \ldots, 1 \end{pmatrix} \begin{pmatrix} 1, 2, 3, \ldots, n \\ \sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n) \end{pmatrix} \]
\[ = \begin{pmatrix} 1, 2, 3, \ldots, n \\ \sigma(2), \sigma(3), \ldots, \sigma(n) \end{pmatrix}. \]
and in general
\[ \rho^k \sigma \begin{pmatrix} 1, 2, 3, \ldots, n \\ \rho^k \sigma(1), \rho^k \sigma(2), \rho^k \sigma(3), \ldots, \rho^k \sigma(n) \end{pmatrix} \]
where \( \rho^k \sigma(1) \equiv \sigma((1+k)(\text{mod} n)) \).

By giving \( k \), values from 1 to \( n \), we obtain the set of \( n \) permutations;
\[ \rho \sigma, \rho^2 \sigma, \ldots, \rho^n \sigma \quad \text{(with} \quad \rho^n \sigma = \sigma), \quad (5) \]
which are all obviously distinct (just looking at the image of 1 under each permutation shows them all to be different).

Similarly the permutations obtained by multiplying on the right by powers of \( \rho \), are of the general form
\[ \sigma \rho^k = \begin{pmatrix} 1, 2, 3, \ldots, n \\ \rho^k \sigma(1), \rho^k \sigma(2), \rho^k \sigma(3), \ldots, \rho^k \sigma(n) \end{pmatrix}, \]
where \( \sigma \rho^k(1) \equiv [\sigma(1) + k] \mod n \).

This again gives us \( n \) distinct permutations
\[ \sigma \rho, \sigma \rho^2, \ldots, \sigma \rho^n \quad \text{(with} \quad \sigma \rho^n = \sigma \quad \text{since} \quad \rho^n = 1) \quad (6) \]
which are not necessarily all equal to those in the first set.

The fact that \( \sum_{i=1}^{n} i(\rho^i \sigma)(1) = [\sum_{i=1}^{n} i \sigma(1)] \mod n \) for \( n \) odd and for all \( k \) and \( \ell \), is proved in the following two theorems.

All this leads to the fact, that with any \( \sigma \in S_n \)
but \( \sigma \notin G_n \), where \( G_n \) is a certain subgroup of \( S_n \),
we can associate a block of \( n^2 \) distinct permutations (viz. the permutations \( \rho^k \sigma^l \) where \( k, l = 1, 2, \ldots, n \)) such that if \( \sigma \) and \( \tau \) belong to such a block, then \( \sum_{i=1}^{n} i \sigma(1) \equiv \sum_{i=1}^{n} i \tau(1) \pmod{n} \).

**Theorem 4.1.** If \( \sigma \in S_n \) and \( \rho = (1, 2, \ldots, n) \) a full cycle permutation, then

\[
\sum_{i=1}^{n} i(\sigma \rho^k)(1) \equiv \left[ \sum_{i=1}^{n} i(\rho^k \sigma)(1) \right] \pmod{n}, \quad k = 1, 2, \ldots, n.
\]

**Proof:**

\[
\sum_{i=1}^{n} i(\sigma \rho^k)(1) - \sum_{i=1}^{n} i(\rho^k \sigma)(1) = \sum_{i=1}^{n} i(\sigma(1) + k \pmod{n}) - \sum_{i=1}^{n} i \sigma(1 + k \pmod{n}) = \sum_{i=1}^{n} i \sigma(1) + k \sum_{i=1}^{n} i - \sum_{i=1}^{n} i \sigma(1) - k \sum_{i=1}^{n} i \pmod{n} = 2k \sum_{i=1}^{n} i \pmod{n} = 2k(n+1)n/2 \pmod{n} = 0 \pmod{n}.
\]

Therefore \( \sum_{i=1}^{n} i(\sigma \rho^k)(1) \equiv \left[ \sum_{i=1}^{n} i(\rho^k \sigma)(1) \right] \pmod{n} \).

Q.E.D.
Theorem 4.2. If \( \sigma \in S_n \) and \( \rho = (1,2,\ldots,n) \) a full cycle permutation in \( S_n \) then

(a) if \( n \) odd \( \sum_{i=1}^{n} i(\sigma \rho^k)(i) \equiv \sum_{i=1}^{n} i\sigma(i) \pmod{n} \) for any \( k \),

(b) if \( n \) even \( \sum_{i=1}^{n} i(\sigma \rho^k)(i) \equiv \sum_{i=1}^{n} i\sigma(i) \pmod{n} \) for \( k \) even,

\[ \sum_{i=1}^{n} i(\sigma \rho^k)(i) \equiv \sum_{i=1}^{n} i\sigma(i)^+ \frac{n}{2} \pmod{n} \] for \( k \) odd.

Proof:

\[ \sum_{i=1}^{n} i(\sigma \rho^k)(i) = \sum_{i=1}^{n} \left[ (\sigma(i) + k) \pmod{n} \right] \pmod{n} \]
\[ = \sum_{i=1}^{n} i\sigma(i) \pmod{n} + k \sum_{i=1}^{n} i \pmod{n} \]
\[ = \sum_{i=1}^{n} i\sigma(i) \pmod{n} + k(n+1)n/2 \pmod{n}. \]

(a) If \( n \) is odd, \( k(n+1)/2 \) is an integer.

Therefore \( \sum_{i=1}^{n} i(\sigma \rho^k)(i) \equiv \sum_{i=1}^{n} i\sigma(i) \pmod{n} \) for all \( k \).

(b) If \( n \) is even, \( k(n+1)n/2 \) is an integer,

\[ \sum_{i=1}^{n} i(\sigma \rho^k)(i) \equiv \sum_{i=1}^{n} i\sigma(i) \pmod{n}, \] if \( k \) even,

and \( \sum_{i=1}^{n} i\sigma(i)^+ \frac{n}{2} \pmod{n} \) if \( k \) odd.

Q.E.D.

Corollary 4.3. If \( n \) odd, then

\[ \sum_{i=1}^{n} i(\rho^k \rho^l)(i) \equiv \sum_{i=1}^{n} i\sigma(i) \pmod{n} \] for all \( k, l \).

Proof: (From previous two theorems),
For any $b$, $0 \leq b \leq n-1$, and $m \in \mathbb{Z}_n$, we can now define a function $\tau$:

$$\tau(i) \equiv b + (i-1)m \pmod{n}, \quad i = 1, 2, \ldots, n. \quad (a)$$

where $1 \leq \tau(i) \leq n$ is a permutation of $\{1, 2, \ldots, n\}$. Since $\tau(i) = \tau(j)$ implies $im \equiv jm \pmod{n}$, which in turn implies $i \equiv j \pmod{n}$ since $m \in \mathbb{Z}_n$.

Moreover, distinct values of $b$ and $m$ give rise to distinct permutations. For, suppose

$$\tau(1) \equiv b_1 + (i-1)m_1 \pmod{n} \quad \text{and} \quad \sigma(1) \equiv b_2 + (i-1)m_2 \pmod{n}.$$ 

Then $\tau = \sigma$ implies that $b_1 = \tau(1) = \sigma(1) = b_2$ and $b_1 + m_1 = \tau(2) = (b_2 + m_2)$ since $\tau(2) = \sigma(2)$.

We define $G_n$ to be the set of all permutations $\tau$ that are of the form (a).

**Theorem 4.4.** $G_n$ is a subgroup of $S_n$ containing $n \cdot \phi(n)$ elements, where $\phi(n)$ is the Euler Function.

**Proof:** From the above discussion the permutation $\tau$ in (a) can be specified in $n \cdot \phi(n)$ ways, corresponding to $n$ choices for $b$ and $\phi(n)$ choices for $m$.

To show that $G_n$ is a group it is necessary only to show that $\sigma, \tau \in G_n$ implies $\sigma \tau \in G_n$. Suppose

$$\tau(1) \equiv b_1 + (i-1)m_1 \pmod{n} \quad \text{and} \quad \tau(1) \equiv b_2 + (i-1)m_2 \pmod{n}.$$ 

Since $(m_2, n) = 1$, there exists $m_3$ such that $m_2 m_3 \equiv 1 \pmod{n}$. 
It is readily checked that
\[ \tau'(i) \equiv (b_3 + (i-1)m_3)(\text{mod } n), \]
where \( b_3 \equiv m_3(1-b) + 1 \) (mod n).
Then \( (\sigma \tau')(i) \equiv \tau'(\sigma(i)) \)
\[ \equiv b_3 + [b_1 + (i-1)m_1 - 1]m_3 \]
\[ \equiv (b_3 + b_1m_3 - m_3) + (i-1)m_1m_3 \) (mod n).
Thus \( \sigma \tau' \in G_n \).

Q.E.D.

**Theorem 4.5.** If \( n \) is odd and \( (n, 3) = 1 \), then
\[ \sum_{i=1}^{n} i\tau(i) \equiv 0 \) (mod n) for all \( \sigma \in G_n \).

**Proof:** Let \( \tau(i) \equiv (b + (i-1)m) \) (mod n).
Then \( \sum_{i=1}^{n} i\tau(i) \equiv b\sum_{i=1}^{n} i + m\sum_{i=1}^{n} i^2 - m\sum_{i=1}^{n} i \)
\[ \equiv b\frac{n(n+1)}{2} + m\frac{n(n+1)(2n+1)}{6} - m\frac{n(n+1)}{2} \]
\[ \equiv 0 \) (mod n).
Q.E.D.

**Corollary 4.6.** If \( n \) is an odd prime, \( n \neq 3 \), then
\[ \sum_{i=1}^{n} i\tau(i) \equiv 0 \) (mod n) for all \( \sigma \in G_n \).
Thus in case \( n \) is a prime, \( n > 3 \) we have obtained a
subgroup of \( S_n \) each element \( \sigma \) of which has the property
\[ \sum_{i=1}^{n} i\tau(i) \equiv 0 \) (mod n).
There may however be other \( \sigma \in S_n \) with this property.
We now proceed to show that the remaining portion of $S_n$ consists of disjoint sets $K_j$ each containing $n^2$ elements, each of which give rise to the same residue class.

**Theorem 4.7.** Let $n$ be a prime $> 3$; and let $H_n = S_n - G_n$.

Then $H_n$ is the union of disjoint complexes $K_j$, $j = 1, \ldots, r$ such that

(I) each $K_j$ contains $n^2$ elements, which all have the same parity, and

(II) for each $j$ there exists $c_j$ such that

$$\sum_{i=1}^{n^2} \sigma(i) \equiv c_j \pmod{n} \quad \text{for all } \sigma \in K_j.$$

**Proof:** Let $\sigma \in H_n$; and let $\mathcal{P} = (1, 2, 3, \ldots, n)$

Define $K_{\sigma} = \{\rho^\sigma \mathcal{P}^m; \, l, m = 1, 2, \ldots, n\}$.

The $n^2$ permutations $\rho^\sigma \mathcal{P}^m$ are distinct, for suppose $\rho^\sigma \mathcal{P}^m = \rho^{\sigma'} \mathcal{P}^{m'}$; then, $\sigma(1) = \rho^{l_2 - l_1}(\mathcal{P}^m(i))$ for $i = 1, 2, \ldots, n$.

Specifically, for each $i$,

$$\sigma(1) \equiv \sigma(1 + l_2 - l_1) + m_2 - m_1 \pmod{n} \text{ or}$$

$$\sigma(1 + l_2 - l_1) \equiv \sigma(1) + m_1 - m_2 \pmod{n}. \quad (7)$$

Since $n$ is prime, if $l_2 - l_1 \neq 0$, there exists $k$ such that $(l_2 - l_1) k \equiv 1 \pmod{n}$.

Then $\sigma(i+1) \equiv \sigma(1 + k(l_2 - l_1))$

$$\equiv \sigma(1) + k(m_2 - m_1) \pmod{n}.$$ 

This means that $\sigma \in G_n$, contradicting our assumption that $\sigma \in H_n$. Therefore $l_2 - l_1 = 0$; it follows from (7)
that \( m_1 - m_2 = 0 \) also. Thus \( K_\sigma \) has \( n^2 \) distinct elements. By Corollary 4.3 we have

\[
\sum_{i=1}^{n} (\rho^l \tau \rho^m)(i) \equiv \sum_{i=1}^{n} i \sigma(i) \pmod{n}
\]

for all \( k, l = 1, 2, \ldots, n \). Thus for any particular complex \( K_\tau \),

\[
\sum_{i=1}^{n} i \sigma(i) \pmod{n}
\]

gives the same residue for all permutations \( \sigma \in K_\tau \).

We have

\[
S_n = G_n \cup \bigcup_{\sigma \in \mathbb{S}_n} K_\sigma.
\]

We now show that for two complexes \( K_\sigma, K_\tau \), either

\[
K_\sigma \cap K_\tau = \emptyset \quad \text{or} \quad K_\sigma = K_\tau.
\]

If \( K_\sigma \cap K_\tau \neq \emptyset \), then \( \rho^l \sigma \rho^m = \rho^{l_{1}, \gamma} \rho^{m_{1}} \)

for some \( l_{1}, m_{1}, l_{2}, m_{2} \). It follows that

\[
\sigma = \rho^{l_{2}-l_{1}} \tau \rho^{m_{2}-m_{1}} = \rho^{l_{3}} \rho^{m_{3}}, \quad \text{where}
\]

\[
l_{3} = l_{2} - l_{1} \pmod{n}, \quad m_{3} = m_{2} - m_{1} \pmod{n}, \quad \text{and}
\]

\[1 \leq l_{3}, m_{3} \leq n. \quad \text{Thus } \sigma \in K_\tau, \quad \text{and } \rho^{l} \sigma \rho^{m} \in K_\tau \]

for all \( l, m, \ 1 \leq l, m \leq n \). Therefore \( K_\sigma \subseteq K_\tau \).

Since \( K_\sigma \) and \( K_\tau \) each have \( n^2 \) elements,

\[
K_\sigma = K_\tau.
\]

Therefore complexes are either disjoint or equal.
To show all permutations in a complex $K_\tau$ have the same parity; we note that for $n$ odd,

$$P = (1, 2, \ldots, n) = (1,2)(1,3)\ldots,(1,n)$$

is a product of an even number of transpositions. Also, since a product of even permutations is even and the product of an even and an odd permutation is odd, therefore $\sigma \in K_\tau$ is even or odd according if $\tau$ is even or odd.

Thus the $n^2$ elements in the complex have the same parity.

Q.E.D.

Note: If $r$ is the number of disjoint $K_{\sigma}$s,

$$S_n = G_n \cup K_1 \cup \ldots \cup K_r,$$

Considering the number of elements in each of these sets, we get

$$n! = n(n-1) + r \cdot n^2 \quad (n \text{ prime}).$$

Thus $(n-1)! = n - 1 + rm$,

or $(n-1)! = -1 (\text{mod } n)$.

This is just Wilson's Theorem!

**Theorem 4.8.** If $n$ is a prime, $n > 3$, and if $a_k$ is the number of permutations in $S_n$ such that

$$\sum_{i=1}^{n} i\sigma(i) \equiv k (\text{mod } n),$$

then

(I) $n(n-1)$ divides $a_0$,

and (II) $n^2$ divides $a_k$ if $k = 1, 2, \ldots, n-1$. 
Proof: By Theorem 4.7,
\[ S_n = G_n \cup K_1, \ldots \cup K_s; \]  \hspace{1cm} (8)
and if
\[ \sum_{i=1}^{n} i \sigma(i) \equiv k \neq 0, \text{ then } \sigma \in \text{ some } K; \]
It follows that those \( \sigma \) such that \( \sum_{i=1}^{n} i \sigma(i) \equiv k \text{ (mod n)} \)
completely occupy a certain number, \( r_k \), of \( K_j \)'s. Since
each \( K_j \) has \( n^2 \) elements, \( a_k = r_k \cdot n^2 \); this proves (II).
By Corollary 3, \( a_1 = a_2 = \ldots = a_{n-1} \).
Hence, all \( r_k \) are equal, \( 1 \leq k \leq n-1 \); say \( r_k = r \).
Then \( a_k = r n^2 \).
Now \( a_0 + a_1 + \ldots + a_{n-1} = n! \).
Therefore \( a_0 + (n-1) r n^2 = n! \),
\[ a_0 = n(n-1) [(n-2)! - r n]; \]
and (I) is proved.

Q.E.D.

Theorem 4.9. For \( n \) a prime, \( n > 3 \), there exists non-negative
integers \( y \) and \( z \) such that
\[ \per A_n = n [(n-1) + y(n-1)n - zn]. \]

Proof: From Theorem 3.4,
\[ \per A_n = a_0 - a_1. \]
Now \( a_0 \) is the number of \( \sigma \in S_n \) such that \( \sum_{i=1}^{n} i \sigma(i) \equiv 0. \)
Such \( \sigma \) occupy \( G_n \) and a certain number of the \( K_j \)'s in the
decomposition (8).
Thus \( a_0 = n(n-1) + wn^2 \).

Since \( n-1 \) divides \( a_0 \), it also divides \( w \).

Therefore \( a_0 = n(n-1) + y(n-1)n^2 \), for some non-negative integer \( y \).

Since \( n^2 \) divides \( a_1 \),
therefore \( a_1 = zn^2 \)
for some non-negative integer \( z \).

Therefore \( \text{per } A = n(n-1) + y(n-1)n^2 - zn^2 \)
\( \quad = n[(n-1) + y(n-1) - z] \).

Q.E.D.

**Theorem 4.10.** For \( n \) a prime > 3, there exists a non-negative integer \( y \) such that
\[
\text{per } A_n = n^2 - n(n-2)! + n^3y.
\]

**Proof:** From the discussion in Theorem 4.9,
\[ a_0 = n(n-1) + yn^2(n-1), \]
and \[ a_k = zn^2, \quad k = 1, 2, \ldots, n-1. \]

Since \( n! = \sum_{i=0}^{n-1} a_i \),
\[ n! = n(n-1) + yn^2(n-1) + (n-1)zn^2, \]
Hence \[ zn = (n-2)! - 1 - yn, \]

\[ \therefore \text{per } A_n = a_0 - a_1 \]
\[ = n(n-1) + yn^2(n-1) + (yn + 1 - (n-2)!)n \]
\[ = n^2 + n^3y - n(n-2)! \],

Q.E.D.

**Remark:** Computed values for the \( x \) and \( y \) above will be indicated in Section VI.
This result does not answer the question as to the value of $A_n^\sqrt{n}$, even for $n$ a prime, but it does restrict considerably the possible values.

We note that $A_n^\sqrt{n}$ is a unitary matrix. By a result of Marcus and Newman \[7\]

$$\left| \text{per } A_n^\sqrt{n} \right| \leq 1,$$

which implies

$$\left| \text{per } A_n \right| \leq n^n.$$

Thus if $n$ is a prime, then $\text{per } A_n$ is restricted to the values of $n^2 + n^3y - n(n-2)!$ that lie between $-n^n$ and $+n^n$, where $y$ is a positive integer.
V THE CASE OF \( n = p^2 \), WHERE \( p \) IS A PRIME

In this section we shall obtain some results for the square of a prime somewhat similar to those obtained in Section IV for a prime. Let \( n = p^2 \), where \( p \) is a prime. The group \( G_n \), which was useful in Section IV is not large enough for our purposes here. We shall form a larger group \( F_n \) consisting of permutations of the following type.

Let \( \sigma \) be a permutation of \( \{1,2,\ldots,p\} \). Define:

\[
\sigma(i + cp) \equiv \sigma(i) + (a_1 + cs)p \pmod{p^2}
\]

for \( i = 1, 2, \ldots, p \) and \( c = 0, 1, \ldots, p-1; \)

where \( \{a_1\} \) and \( s \) are constants such that \( 0 \leq a_1 \leq p-1; \)
\( 1 \leq s \leq p-1 \). We show that each such function \( \sigma \) is indeed a permutation of \( \{1,2,\ldots,p^2\} \). Suppose \( \sigma(j) = \sigma(k) \), where, say, \( j = i_1 + c_1 p \) and \( k = i_2 + c_2 p \). Then

\[
\sigma(i_1) + (a_1 + c_1 s)p \equiv \sigma(i_2) + (a_2 + c_2 s)p \pmod{p^2},
\]

and

\[
\sigma(i_1) \equiv \sigma(i_2) \pmod{p}.
\]

By the definition of \( \sigma \), it follows that \( i_1 = i_2 \), \( a_1 = a_2 \), and, from (21), \( c_1 s \equiv c_2 s \pmod{p} \).

Hence \( c_1 = c_2 \), and finally \( j = k \). Thus \( \sigma(j) = \sigma(k) \) implies that \( j = k \), so that \( \sigma \) is a permutation.
Theorem 5.1. The set $F_n$ of permutations in $S_n$ of the form (20) form a subgroup of $S_n$ of order $p^p \cdot p! \cdot (p-1)$. Every permutation $\tau$ in $S_n$ with the property $\tau(i+p) \equiv \tau(i) + kp \pmod{p^2}$, for a fixed $k$, $1 \leq k \leq p-1$, is a member of $F_n$.

Proof: Suppose
\[ \sigma(i+cp) \equiv \sigma(1) + (a_1+cs)p \pmod{p^2}. \] (20)

Then $\sigma^{-1}$ is given by
\[ \sigma^{-1}(i+cp) \equiv \sigma^{-1}(1) + (b_1+ct)p \pmod{p^2}, \]
where $0 \leq b_1 \leq p-1$, $t$ is such that $1 \leq t \leq p-1$,
st $\equiv 1 \pmod{p}$, and $1 \leq b_1 \leq p-1$, $b_1 \equiv -a_1 t \pmod{p}$. For,
\[ \sigma \sigma^{-1}(i+cp) \equiv \sigma^{-1}[\sigma(1) + (a_1+cs)p] \pmod{n} \]
\[ \equiv \sigma \sigma^{-1}(1) + [b_1 + (a_1+cs)t]p \pmod{n} \]
\[ \equiv i + [-a_1 t + a_1 t + c]p \pmod{n} \]
\[ \equiv i + cp \pmod{n}. \]
Thus if $\sigma \in F_n$, $\sigma^{-1} \in F_n$.

Similarly, if $\mu$ is defined by
\[ \mu(i+cp) \equiv \mu(1) + (\alpha_1+cu)p \pmod{n}. \]
then $\sigma \mu(i+cp) \equiv \mu[\sigma(1) + (a_1+cs)p] \pmod{n}$
\[ \equiv \sigma \mu(1) + [\alpha_1 + (a_1+cs)u]p \pmod{n} \]
\[ \equiv \sigma \mu(1) + [\alpha_1 + a_1 u + csu]p \pmod{n} \]
\[ \equiv i + [\alpha_1 + cw]p \pmod{n}, \]
where $0 \leq \gamma_i \leq p-1$, and $1 \leq w \leq p-1$. Hence $\sigma \tau \in F_n$, and $F_n$ is a group.
To obtain the number of elements in $F_n$, we note that there are $p!$ ways of choosing $\sigma$; $p$ ways of choosing each $a_i$, $i=1,2,\ldots,p$; and $p-1$ ways of choosing $s$; yielding $p! \cdot p^p \cdot (p-1)$ ways of choosing $\sigma$. These choices are distinct; for, suppose

$$\sigma(i+cp) \equiv \sigma(1) + (a_i+cs)p \pmod{p^2}$$
and

$$\mu(i+cp) \equiv \mu(1) + (b_i+ct)p \pmod{p^2}$$

define two members $\sigma$ and $\mu$ of $F_n$. If $\sigma \neq \mu$, there exists $j$, $1 \leq j \leq p$, such that $\sigma(j) \neq \mu(j)$; then $\sigma(j) \neq \mu(j)$. If $\sigma = \mu$, $a_i \neq b_i$ for some $i$, then $\sigma(1) \neq \mu(1)$. If $\sigma = \mu$, all $a_i = b_i$, and $s \neq t$, then $\sigma(i+p) \neq \mu(i+p)$. Thus there are $p! \cdot p^p \cdot (p-1)$ distinct elements in $F_n$.

Now suppose that $\tau$ is a member of $S_n$ such that

$$\tau(i+p) \equiv \tau(i) + kp \pmod{p^2}, \quad 1 \leq k \leq p-1,$$
for all $i=1,\ldots,n$. Then $\tau(i)$ can be written

$$\tau(i) = d_i + a_ip, \quad i=1,2,\ldots,p,$$
where $1 \leq d_i \leq p$, and $0 \leq a_i \leq p-1$. We show first that

$\{d_i\}$ is a permutation of $\{1,2,\ldots,p\}$.

Choose $r$ such that $rk \equiv 1(\mod p)$. If

$d_i = d_j$ for $1 \leq j \leq p$, then

$$\tau[i + (a_j-a_i)rp] \equiv \tau(i) + (a_j-a_i)kp \pmod{n}$$
\begin{align*}
\equiv d_i + a_ip + (a_j-a_i)p \pmod{n} \\
\equiv d_j + a_jp \pmod{n} \\
\equiv \tau(j) \pmod{n}.
\end{align*}
Since \( \tau \) is a permutation, \( i + (a_j - a_1)p \equiv j \pmod{n} \), which implies \( i \equiv j \pmod{p} \), and finally that \( i = j \).

We can now write \( d_1 = \overline{\tau}(i) \), where \( \overline{\tau} \in S_p \); and

\[
\tau(1) = \overline{\tau}(1) + a_1 p.
\]

Since \( \tau(i + p) = \tau(1) + kp \),

we have \( \tau(i + cp) = \overline{\tau}(1) + (a_1 + ck)p \).

\( \tau \) is therefore a member of \( F_n \). This completes the proof of Theorem 5.1.

Q.E.D.

We next examine the residue class of

\[
\sum_{i=1}^{n} i \overline{\sigma}(i) \quad \text{for } \sigma \in F_n.
\]

**Theorem 5.2.** If \( \sigma \in F_n \), then

\[
\sum_{i=1}^{n} i \overline{\sigma}(1) \equiv p \sum_{i=1}^{p} i \overline{\sigma}(1) \pmod{n},
\]

where \( \overline{\sigma} \) is the permutation of \( 1, 2, \ldots, p \), given in (2c).

The number of permutations \( \sigma \) in \( F_n \) such that

\[
\sum_{i=1}^{n} i \overline{\sigma}(1) \equiv j p \pmod{n}, \quad 0 \leq j \leq p - 1,
\]

is equal to \( p^p \cdot (p-1) \) times the number of permutations \( \overline{\sigma} \in S_p \) such that

\[
\sum_{i=1}^{p} i \overline{\sigma}(1) \equiv j \pmod{p}.
\]

**Proof:**

\[
\sum_{i=1}^{n} i \overline{\sigma}(1) = \sum_{i=1}^{p} [i \overline{\sigma}(1) + a_1 p] + \sum_{i=1}^{p} (1 + p) [i \overline{\sigma}(1) + (a_1 + s)p] + \sum_{i=1}^{p} (1 + 2p) [i \overline{\sigma}(1) + (a_1 + 2s)p] + \cdots + \sum_{i=1}^{p} [1 + (p-1)p] [i \overline{\sigma}(1) + (a_1 + (p-1)s)p]
\]
\[\equiv p \sum_{i=1}^{p} i \bar{T}(i) + p \sum_{i=1}^{p} a_{i} \bar{p} + \sum_{i=1}^{r} \left[s + 2s + \ldots + (p-1)s\right] p + \sum_{i=1}^{r} i \bar{T}(i) \left[p + 2p + \ldots + (p-1)p\right]
\equiv p \sum_{i=1}^{p} i \bar{T}(i) + p(p+1)/2 \left[s + 2s + \ldots + (p-1)s\right] p + p(p+1)/2 \left[p + 2p + \ldots + (p-1)p\right]
\equiv p \sum_{i=1}^{p} i \bar{T}(i) \pmod{n}.
\]

The latter statement in the theorem follows immediately from Theorem 5.1.

Q.E.D.

As in the previous section, we now consider for each \(\bar{T} \in S_{n} - F_{n}\), the set
\[K_{\bar{T}} = \{P^{\bar{T}} \bar{Q}^{\bar{m}} \mid \bar{l}, \bar{m} = 0,1,\ldots,n-1\}.\]
(see page 27).

**Theorem 5.3.** If \(\bar{T} \in S_{n} - F_{n}\), then \(|K_{\bar{T}}| = n^{2}\).

For all elements \(\bar{T} \in K_{\bar{T}}\),
\[\sum_{i=1}^{n} i \bar{\tau}(i) \equiv \sum_{i=1}^{n} i \bar{T}(i) \pmod{n}.
\]

**Proof:** As \(\bar{l}, \bar{n}\) run through 0,1,\ldots,n-1, \(n^{2}\) permutations \(P^{\bar{l}} \bar{Q}^{\bar{m}}\) are produced. It is required to show that they are different. It is sufficient to show that \(P^{\bar{l}} \bar{Q}^{\bar{m}} = \bar{T}\) implies \(\bar{l} = \bar{m} = 0\). If \(P^{\bar{l}} \bar{Q}^{\bar{m}} = \bar{T}\),
then \(\bar{T}(i+\bar{l}) + \bar{m} \equiv \bar{T}(1) \pmod{n}\).

First, \(\bar{l} = 0\) implies \(\bar{m} = 0\). If \((\bar{l}, \bar{n}) = 1\), choose \(r\) so that \(r\bar{l} \equiv 1 \pmod{n}\). Then
\( \sigma(i + r) \equiv \sigma(i) - r \equiv (\text{mod } n) \),
or
\( \sigma(i + 1) \equiv \sigma(i) - r \equiv (\text{mod } n) \).

Then \( r \equiv 0 \equiv (\text{mod } n) \), and

\( \sigma(i + p) \equiv \sigma(i) - r \equiv (\text{mod } n) \).

By Theorem 5.1, \( \sigma \in F_n \), a contradiction. The remaining alternative for \( \ell \) is \( \ell = cp \), \( 1 \leq c \leq p-1 \). In this event

\( \sigma(i + p) = \sigma(i + cp) \equiv \sigma(i) \equiv (\text{mod } n) \),
and hence \( \sigma(i) \equiv \sigma(i) - pm \equiv (\text{mod } n) \).

It follows that \( m = 0 \equiv (\text{mod } p) \). Moreover \( m \equiv 0 \equiv (\text{mod } n) \),
since, in that case,

\( \sigma(i + cp) \equiv \sigma(i) \equiv (\text{mod } n) \),
which is impossible. Thus \( m = kp \), \( 1 \leq k \leq p-1 \).

By Theorem 5.1, \( \sigma \in F_n \), a contradiction.

Thus \( |K_{\sigma}| = n^2 \).

Let \( \tau = \rho^\ell \sigma^m \); \( 0 \leq \ell, m \leq n-1 \).

Then

\[
\sum \sigma(i) = \sum_{i=1}^{n} \rho^\ell \sigma^m(i) \\
= \sum_{i=1}^{n} [\sigma(i + \ell) + m] \\
= \sum_{i=1}^{n} \sigma(i + \ell) \sigma(i + \ell) - \sum_{i=1}^{n} \sigma(i + \ell) + \sum_{i=1}^{n} \sigma(i + \ell) \\
= \sum_{i=1}^{n} i \sigma(i) - \ell n(n+1)/2 + m n(n+1)/2 \\
= \sum_{i=1}^{n} i \sigma(i) \equiv (\text{mod } n). 
\]

Q.E.D.

**Theorem 5.4.** For \( \sigma, \tau \notin F_n \), either \( K_{\sigma} = K_{\tau} \), or \( K_{\sigma} \cap K_{\tau} = \emptyset \).
Proof: If \( \mu \in K_\sigma \cap K_\tau \), then \( \mu = \rho^{\ell_1} \tau \rho^{m_1} = \rho^{\ell_2} \tau \rho^{m_2} \),
which implies \( \tau = \rho^{\ell_1 - \ell_2} \tau \rho^{m_1 - m_2} \), and hence \( \tau \in K_\sigma \).
It follows that \( K_\tau \subseteq K_\sigma \).
Since \( |K_\sigma| = |K_\tau| \), \( K_\sigma = K_\tau \).

Thus \( S_n \) is partitioned as follows:

\[
\begin{array}{c}
F_n \\
(p^p, p^p (p-1)) \\
K_\sigma \quad (m_1) \\
K_{\sigma_1} \quad (n_1) \\
K_{\sigma_2} \quad (m_2) \\
K_{\sigma_3} \quad (n_2) \\
K_{\sigma_4} \quad (m_3) \\
K_{\sigma_5} \quad (n_3) \\
K_{\sigma_6} \quad (m_4) \\
K_{\sigma_7} \quad (n_4) \\
\end{array}
\]

where the number of elements in the various subsets are shown in brackets.

We are now in a position to get some information on \( \text{per} A_n \). Recall that

\[
\text{per} A_n = a_0 + a_1 \theta + \ldots + a_{n-1} \theta^{n-1},
\]

where \( a_j \) is the number of \( \sigma \in S_n \) such that

\[
\sum_{i=1}^{n} i \sigma(i) = j \pmod{n}. \]

In fact, for \( n=p^2 \), by Theorem 3.5,

\[
\text{per} A_n = a_0 - a_p.
\]

By Theorem 5.2, the number of \( \sigma \)'s in \( F_n \) for which

\[
\sum_{i=1}^{n} i \sigma(i) \equiv 0 \pmod{n}
\]

is \( p^p \cdot (p-1) \) times the number
of \( \sigma \in S_p \) such that \( \sum_{i=1}^{n} i\sigma(i) \equiv 0 \pmod{p} \). By Theorem 4.8 the latter is \( p(p-1) + k_1 p^2 \) for some integer \( k_1 \).

There may, in addition be \( \sigma \notin F_n \) such that \( \sum_{i=1}^{n} i\sigma(i) \equiv 0 \pmod{p} \).

The number of these will be a multiple \( k_2 \) of \( n^2 = p^4 \), by Theorems 5.3 and 5.4. Thus

\[
a_o = p^{p+1}(p-1)^2 + k_1 p^{p+2}(p-1) + k_2 p^4.
\]

Similarly, each \( \sigma \in F_n \) such that \( \sum_{i=1}^{n} i\sigma(i) \equiv p \pmod{p} \) corresponds to a \( \sigma \in S_p \) such that \( \sum_{i=1}^{n} i\sigma(i) \equiv 1 \pmod{p} \).

The number of the latter is \( k_3 p^2 \), by Theorem 4.8.

Thus the number of \( \sigma \in F_n \) such that \( \sum_{i=1}^{n} i\sigma(i) \equiv p \pmod{n} \) is \( k_3 p^{p+2}(p-1) \). Outside \( F_n \) there will be a multiple \( k_4 \) of \( p^4 \) further permutations of this type. We have then

\[
a_p = k_3 p^{p+2}(p-1) = k_4 p^4;
\]

and as a result

\[
\text{per } A_n = p^{p+1}(p-1)^2 + (k_1-k_3) p^{p+2}(p-1) + (k_2-k_4) p^4.
\]

Setting \( k_1 + k_3 + 1 = k \), and \( k_2 + k_4 = \ell \), we have

**Theorem 5.5.** For \( n=p^2 \), \( p \neq 3 \),

\[
\text{per } A_n = p^{p+1}(p-1)(kp-1) + \ell p^4
\]

where \( k, \ell \) are positive integers. In particular

\[
\text{per } A_n \equiv 0 \pmod{p^4}.
\]
VI COMPUTER RESULTS

(a) **Computer Programme.**

Per $A_n$ was calculated for the odd primes, $n = 5, 7, 11, 13$, on an IBM 7040 computer. This was done using the following well known formula due to Ryser [5].

Let $B$ be a $n$-square matrix and let $B_r$ denote a matrix obtained from $B$ by replacing some $r$ columns of $B$ by zeros. Let $S(X)$ be the product of the row sums of the matrix $X$. Then

$$\text{per } B = S(B) - \sum S(B_1) + \sum S(B_2) - \ldots - (-1)^{n-1}\sum S(B_{n-1})$$

where $\sum S(B_r)$ denotes the sum over all $(n\choose r)$ replacements of the $r$ columns by columns of zeros.

If $B = A_n$, where $n$ is odd, and if $A_{n(r)}$ denotes the matrix obtained by replacing $r$ columns of $A_n$ by columns of zeros, then it is easily checked that

$$(1/r)S(A_{n(r)}) = (1/(n-r))S(A_{n(n-r)})$$

If $S'(A_{n(r)})$ denotes the product of the first $n-1$ row sums of $A_{n(r)}$, then since the $n$th row of $A_n$ consists of 1's only, we have

$$S(A_{n(r)}) = r \cdot S'(A_{n(r)})$$
Thus we can rewrite (9) as
\[
\text{per } A_n = -1 \sum S'(A_{n(1)}) + 2 \sum S'(A_{n(2)}) - 3 \sum S'(A_{n(3)}) \\
\ldots + (-1)^{n-1}(n-1) \sum S(A_{n(n-1)}).
\]

Therefore
\[
\text{per } A_n = (n - 2) \sum S'(A_{n(1)}) - (n - 4) \sum S'A_{n(2)} + \\
+ (n - 6) \sum S'A_{n(3)} + \ldots + (-1)^{n-1} \sum S'A_{n(n-1)/2}.
\]

Thus to evaluate \(\text{per } A_n\) if \(n\) is odd, it is only necessary to compute the product of the first \(n-1\) row sums of all possible matrices \(A_n(r)\) for \(r = 1, \ldots, (n-1)/2\). That is for
\[
\binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{(n-1)/2}
\]
matrices in all.

The programme used to obtain values for \(\text{per } A_n\), for \(n = 5, 7, 11, \text{ and } 13\), was based on the equation (10) in the above paragraph.

It consisted essentially of a combination generator, which generated all possible combinations of \(n\) things \(r\) at a time, for \(r = 1, 2, \ldots, (k-1)/2\). From these the matrices \(A_n(r)\) were formed for each value of \(r\), and \(\sum S'A_{n(r)}\) evaluated. By equation (10), \(\text{per } A_n\) was thus obtained.

This programme was originally designed to compute and print out \(S'A_{n(r)}\) for all \(r\), in a particular order; with the hope of observing patterns which would allow a conjecture for \(\text{per } A_n\) to be obtained from equation (10).
Due to the excessive checking involved in the ordering of the combinations, this programme proved to be very inefficient if used to calculate \( \text{per } A_n \) for \( n > 13 \).

For \( n = 17 \), no result could be obtained in two hours computing time. Whereas, for \( n = 5, 7, 11, 13 \), \( \text{per } A_n \) was computed in less than five minutes. With an efficient combination generator, \( A_{17} \) and \( A_{19} \) should be readily obtained by the IBM 7040.

(b) Results.

For \( n \) an odd prime, \( n > 3 \) we have the following computer results.

\[
\begin{align*}
\text{per } A_5 &= -5 \\
\text{per } A_7 &= -3 \cdot 5 \cdot 7 \\
\text{per } A_{11} &= 3 \cdot 5 \cdot 11 \cdot 41 \\
\text{per } A_{13} &= 11 \cdot 13 \cdot 1229.
\end{align*}
\]

Theorem 4.9 gives \( \text{Per } A_n = n \left( (n-1) + y(n-1)n - zn \right) \), or (Theorem 4.10) \( \text{Per } A_n = n^2 - n(n-2)! + n^3y \).

Thus for \( n = 5, 7, 11, \) and \( 13 \), we can list the values of \( y \) and \( z \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( y )</th>
<th>( z )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>3004</td>
<td>29985</td>
</tr>
<tr>
<td>13</td>
<td>36274</td>
<td>2834249</td>
</tr>
</tbody>
</table>
COMPUTING PERMANENT OF A(N) BY RYSERS METHOD.

COMPLEX XI, TH(17), PROD, RSUM, THETA(17, 17), FN
INTEGER SP(17), PER
DIMENSION KOL(1431, 8)
DIMENSION MOT(17)
PRINT 1
1 FORMAT(34H_COLUMNS PRODUCT OF ROWSUMS)
GO TO 112
79 PER=0
SP(1)=1
SP(2) = (N-1)/2
DO 113 I=1, MO
113 PER=PER+(N-2*I)*N*SP(I)*(-1)**I
WRITE(6, 111) PER
112 READ(5, 2) N
2 FORMAT(I2)
19 PRINT 19+N
19 FORMAT(IX, I2)
61 MO=(N-1)/2
M=3
GO TO 51
38 M=M+1
51 M1=M-1
M2=M-2
IF(M GT MO) GO TO 79
T=N
XI=CMPLX(0., 2.*3.1415927/T)
N1=N-1
DO 40 I=1, N1
EN=FLOAT(I)
40 TH(I)=CEXP(EN*X1)
TH(N)=(1., 0., 0., 0.)
DO 10 I=1, N
DO 43 JA=1, N
10 KA=I*JA
44 IF(KA LE N) GO TO 43
KA=KA-N
GO TO 44
43 THETA(I, JA)=TH(KA)
10 CONTINUE
SP(M)=0
NZERO=0
K=1
NO=1
NI=1
DO 3,1=1, M1
NO=NO*(N-1)
3 NI=NI*(I+1)
NO=NO/NI
18 DO 5 I=1, M1
5 KOL(1,I)=1
KOL(1,M)=N+1-M
DO 31 I=1, M
31 MOL(I)=KOL(1,I)
DO 13 I=1, M
13 M0(I)=1
GO TO 55
11 K=K+1
K1=K-1
6 DO 7 I=1, M
7 KOL(K,I)=M0(I)
KOL(K,M1)=M0(M1)-1
KOL(K,M)=M0(M)+1
C
DO 53 I=1, M
53 M0(I)=KOL(K, I)
C
L=1
37 MP=0
J=1
C
62 DO 8 I=1, M
8 IF(K0L(K,I) .NE. K0L(J,I)) GO TO 20
11 GO TO 300
20 IF(J.EQ.K1) GO TO 34
33 J=J+1
8 GO TO 62
34 MP=MP+1
6 J=1
5 KM=KOL(K, I)
4 DO 36 I=1, M1
36
I1=I+1

36 KOL(K,I)=KOL(K,I1)
   KOL(K,M)=KM
   IF(MP.EQ.M) GO TO 200
   GO TO 62
300 IF(MOL(M).LE.1) GO TO 24
   GO TO 6
C

200 MOT(1)=1
   DO 93 I=2,M
93 MOT(I)=MOT(I-1)+MOL(I-1)
55 PROD=(1.0*0.0)/FLOAT(M)
   DO 16 I=1,N
      RSUM=(0.0*0.0)
      DO 17 LA=1,M
         JA=MOT(LA)
17 RSUM=RSUM+THETA(I,JA)
16 PROD=PROD*RSUM
   SP(M)=SP(M)+INT(.5+REAL(PROD))
   WRITE(6,52) PROD, (MOT(LA),LA=1,M)
52 FORMAT (2F10.2,4X,20I3)
   IF(K.EQ.1) GO TO 11

201 K=K+1
   K1=K-1
   IF(K.GT.NO) GO TO 39
   GO TO 300
39 WRITE(6,111) SP(M)
111 FORMAT (60X,110)
   GO TO 38

24 L=L+1
   ML=M-L+1
   ML=M-L
   DO 25 I=1,M
25 KOL(K,I)=MOL(I)
   KOL(K,ML)=MOL(ML)+1
   IF(L.EQ.2) GO TO 41
   DO 26 I=ML,2
26 KOL(K,I)=1
   41 KOL(K,M)=1
   KOL(K,M)=0
   DO 30 I=M1
30 KOL(K,M)=KOL(K,M)+KOL(K,I)
KOL(K,M) = N - KOL(K,1)
GO TO 14
C
14 IF(KOL(K,M).LT.1) GO TO 24
DO 42 I = 1, M
42 MOL(I) = KOL(K,I)
GO TO 37
21 CALL EXIT
END
SENTRY
BIBLIOGRAPHY


