J. Austral. Math. Soc. 21 (Series A) (1976), 487–497.

# ON THE PERMANENT OF SCHUR'S MATRIX

**Dedicated to George Szekeres on his 65th birthday**

R. L. GRAHAM and D. H. LEHMER

(Received 22 November 1974; revised 7 March 1975)

Communicated by Jennifer Šeberry Wallis

**Abstract**

*Schur's matrix* $M_n$ is ordinarily defined to be the $n$ by $n$ matrix $(\varepsilon^{jk})$, $0 \leqq j,\ k < n$, where $\varepsilon = \exp(2\pi i/n)$. This matrix occurs in a variety of areas including number theory, statistics, coding theory and combinatorics. In this paper, we investigate $P_n$, the *permanent* of $M_n$, which is defined by

$$P_n = \sum_{\pi} \prod_{j=0}^{n-1} \varepsilon^{j\pi(j)}$$

where $\pi$ ranges over all $n!$ permutations on $\{0, 1, \cdots, n-1\}$.

$P_n$ occurs, for example, in the study of circulants. Specifically, let $X_n$ denote the $n$ by $n$ circulant matrix $(x_{i,j})$ with $x_{i,j} = x_{i-j}$ where the subscript is reduced modulo $n$. The determinant of $X_n$ is a homogeneous polynomial of degree $n$ in the $x_i$ and can be written as

$$\det X_n = \sum_{j_0+\cdots+j_{n-1}=n} A(j_0, \cdots, j_{n-1})\, x_0^{j_0} \cdots x_{n-1}^{j_{n-1}}.$$

Then $P_n = A(1, 1, \cdots, 1)$.

Typical of the results established in this note are:

(i) $P_{2n} = 0$ for all $n$,

(ii) $P_p \equiv p! \pmod{p^3}$ for $p$ a prime $> 3$.

(iii) If $p^\alpha$ divides $n$ then $p^{(p^\alpha - 1)n/(p-1)p^\alpha}$ divides $P_n$.

Also, a table of values of $P_n$ is given for $1 \leqq n \leqq 23$.

## Introduction

Schur's matrix (Schur (1921)) $M_n(t)$ is the $n$ by $n$ matrix defined by

$$M_n(t) = (\alpha_{j,k}^{(t)}) = (\varepsilon^{tjk}), \qquad 0 \leqq j, k < n,$$

where

$$\varepsilon = \exp(2\pi i/n).$$

and $(t, n) = 1$. Ordinarily one takes $t = 1$ in which case we abbreviate $a_{j,k}^{(1)}$ by $\alpha_{j,k}$ and $M_n(1)$ by $M_n$.

$M_n$ occurs in a variety of contexts, e.g., number theory, statistics, coding theory and combinatorics. In this note we investigate $P_n$, the permanent of $M_n$. This is defined by

$$P_n = \sum_{\pi} \alpha_{0,\pi(0)} \alpha_{1,\pi(1)} \cdots \alpha_{n-1,\pi(n-1)}$$

where $\pi$ ranges over all $n!$ permutations on $\{0, 1, \cdots, n-1\} = [0, n-1]$.

One place in which $P_n$ comes up is in the study of circulants. Specifically, let $X_n$ denote the $n$ by $n$ circulant matrix $(x_{i,j})$ with $x_{i,j} = x_{i-j}$ where the subscript is reduced modulo $n$. The determinant of $X_n$ is a homogeneous polynomial of degree $n$ in the $x_i$ and can be written as

$$\det X_n = \sum_{j_0 + \cdots + j_{n-1} = n} A(j_0, \cdots, j_{n-1}) x_0^{j_0} \cdots x_{n-1}^{j_{n-1}}.$$

Then

$$P_n = A(1, 1, \cdots, 1). \tag{1}$$

This follows immediately from the explicit expression (see Muir (1960)) for $\det X_n$, namely,

$$\det X_n = \prod_{j=0}^{n-1} \sum_{k=0}^{n-1} \varepsilon^{jk} x_k.$$

## Elementary facts

Let $S_n$ denote the set of permutations $\pi: [0, n-1] \to [0, n-1]$. We begin by defining the *spread* of a permutation $\pi \in S_n$ to be the inner product

$$\sigma(\pi) = \sum_{k=0}^{n-1} k\pi(k)$$

where the sum is reduced modulo $n$.

FACT 1. *Let* $(a, n) = 1$ *and let* $\pi_1, \pi_2 \varepsilon S_n$ *satisfy*

$$\pi_2(k) \equiv a\pi_1(k) + t \pmod{n}.$$

*Then*

$$\sigma(\pi_2) \equiv \begin{cases} a\sigma(\pi_1) \text{ if } n \text{ is odd or } t \text{ is even,} \\ a\sigma(\pi_1) + n/2 \text{ otherwise.} \end{cases}$$

The proof is immediate from the definition.

Denote by $U_n(r)$ the set $\{\pi \in S_n : \sigma(\pi) = r\}$ and let $u_n(r)$ denote $|U_n(r)|$. Of course,

$$\sum_{r=o}^{n-1} u_n(r) = n! \tag{1}$$

The following table gives some of the small values of $u_n(r)$.

Table 1. $u_n(r)$

| n r | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | | | | | | | | |
| 2 | 1 | 1 | | | | | | | | |
| 3 | 0 | 3 | 3 | | | | | | | |
| 4 | 4 | 8 | 4 | 8 | | | | | | |
| 5 | 20 | 25 | 25 | 25 | 25 | | | | | |
| 6 | 144 | 108 | 108 | 144 | 108 | 108 | | | | |
| 7 | 630 | 735 | 735 | 735 | 735 | 735 | 735 | | | |
| 8 | 5696 | 4608 | 5248 | 4608 | 5696 | 4608 | 5248 | 4608 | | |
| 9 | 39366 | 40824 | 40824 | 39285 | 40824 | 40824 | 39285 | 40824 | 40824 | |
| 10 | 366400 | 362000 | 362000 | 362000 | 362000 | 366400 | 362000 | 362000 | 362000 | 362000 |

FACT 2. *For n even,*

$$u_n(r) = u_n\left(r + \frac{n}{2}\right).$$

PROOF. The map $\alpha : S_n \to S_n$ given by

$$\alpha(\pi)(k) = \pi(k) + 1$$

is a bijection of $U_n(r)$ into $U_n(r + (n/2))$. ■

FACT 3. *Let n, r and s be integers with* $(n, r) = (n, s)$. *Then*

$$u_n(r) = u_n(s).$$

PROOF. By hypothesis, there exists an integer $t$, with $(t, n) = 1$, such that $s \equiv rt \pmod n$. If $\gamma : S_n \to S_n$ by

$$\gamma(\pi)(k) = t\pi(k) \quad \text{then} \quad \gamma : U_n(r) \to U_n(s)$$

is an injection. By symmetry, $u_n(r) = u_n(s)$. ■

Thus, to evaluate $u_n(r)$ for all $r$, it suffices to evaluate $u_n(\delta)$ for all $\delta \mid n$. From the definition of $P_n$ we have

$$P_n = \sum_{r=1}^{n} u_n(r) \exp(2\pi i r/n). \tag{2}$$

Since the sum of the primitive $k$th roots of unity is $\mu(k)$, where $\mu$ denotes the ordinary Möbius function, then by Fact 3 we can write

$$P_n = \sum_{\delta | n} u_n(\delta)\mu(n/\delta). \tag{3}$$

In the case that $n$ is prime we have by (1)

$$P_n = \frac{n}{n-1}(u_n(0) - (n-1)!). \tag{3'}$$

THEOREM 1.

$$P_{2n} = 0. \tag{4}$$

PROOF. By (2)

$$\begin{aligned} P_{2n} &= \sum_{r=1}^{2n} u_{2n}(r) \exp(2\pi ir/2n) \\ &= \sum_{r=1}^{n} u_{2n}(\exp(2\pi ir/2n) + \exp(2\pi i(r+n)/2n)) \text{ by Fact 2} \\ &= 0 \end{aligned}$$

since the right hand factor in the sum vanishes. ■

Note that if $n$ is odd then $\alpha_k : S_n \to S_n$ defined by $\alpha_k(\pi)(i) = \pi(i) + k$ actually satisfies $\alpha_k : U_n(r) \to U_n(r)$ for all $r$, since $\Sigma_{k=0}^{n-1} k \equiv 0 \pmod n$. Thus,

$$u_n(r) \equiv 0 \pmod n,\ n \text{ odd}, \tag{5}$$

and by (3) and (4)

$$P_n \equiv 0 \pmod n. \tag{6}$$

In the next sections, considerably stronger modular results will be established.

## Some modular results for $n$ prime

Let $n$ be a fixed odd prime $p$ and let $U_p$ denote $U_p(0)$. Suppose $G$ is a group of permutations acting on $U_p$. The set $U_p$ is then partitioned into some number, say $m$, disjoint orbits $\pi_i^G$ for suitable $\pi_i \in U_p$, $1 \leqq i \leqq m$.

Since

$$u_p = |U_p| = \sum_{i=1}^{m} |\pi_i^G| \quad \text{and} \quad |\pi_i^G| \;\Big|\; |G| \text{ for all } i \tag{7}$$

then if $G$ is chosen appropriately (for example, so that $|G|$ has a small number of prime factors), it is often possible to determine the structure of some of the smaller orbits of $G$ and, as a consequence, gain information about $u_p$. In this section, we give several illustrations of this technique.

THEOREM 2. *For any prime* $p > 3$,

$$P_p \equiv p!\,(\mathrm{mod}\ p^3) \tag{8}$$

PROOF. Let $G$ be the group generated by the two maps $\alpha, \beta : S_p \to S_p$ defined by:

$$\alpha(\pi)(k) = \pi(k) + 1\,,$$

$$\beta(\pi)(k) = \pi(k+1)\,,$$

where $k \in [0, p-1]$, $\pi \in S_p$ and all addition is taken modulo $p$. Note that for $\pi \in U_p$,

$$\sigma(\alpha(\pi)) = \sum_{k=0}^{p-1} k\alpha(\pi)(k) \equiv \sigma(\pi) + \binom{p}{2} \equiv 0\,(\mathrm{mod}\ p)$$

and

$$\sigma(\beta(\pi)) = \sum_{k=0}^{p-1} k\beta(\pi)(k) \equiv \sigma(\pi) - \binom{p}{2} \equiv 0\,(\mathrm{mod}\ p)$$

so that $\alpha$ and $\beta$ map $U_p$ into $U_p$. Since $\alpha$ and $\beta$ commute and each has order $p$, then $|G| = p^2$. Of course, each orbit $\pi_i^G$ is nontrivial so that (7) implies $|\pi_i^G| = p$ or $|\pi_i^G| = p^2$, $1 \leqq i \leqq m$. We call these *small* and *large* orbits, respectively.

Suppose $\pi^G$ is a small orbit of $G$. Since

$$\pi, \alpha(\pi), \alpha(\alpha(\pi)) = \alpha^{(2)}(\pi), \alpha^{(3)}(\pi), \cdots, \alpha^{(p-1)}(\pi)$$

are all distinct then we must have

$$\beta(\pi) = \alpha^{(t)}(\pi)$$

for some $t \not\equiv 0$ (mod $p$). Thus, for all $k$,

$$\beta(\pi)(k) \equiv \alpha^{(t)}(\pi)(k)\,(\mathrm{mod}\ p),$$

i.e.,

$$\pi(k+1) \equiv \pi(k) + t(\mathrm{mod}\ p)$$

and so

$$\pi(k) \equiv \pi(0) + kt\,(\mathrm{mod}\ p), \qquad 0 \leqq k < p. \tag{9}$$

Hence, we have shown that if $\pi$ belongs to a small orbit of $G$, then $\pi$ satisfies (9).

On the other hand, if $\pi$ is any element of $U_p$ which satisfies (9), then

$$\begin{aligned}\sigma(\pi) &= \sum_{k=0}^{p-1} k\pi(k) = \sum_{k=0}^{p-1} k(\pi(0)+kt)\\ &= \pi(0)\sum_{k=0}^{p-1} k + t\sum_{k=0}^{p-1} k^2\\ &= \pi(0)\binom{p}{2} + t\cdot\frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod{p}\end{aligned}$$

since $p$ is odd and greater than 3. Therefore, *all* $\pi$ which satisfy (9) belong to $U_p$. From this we conclude that exactly $p(p-1)$ elements of $U_p$ (corresponding to the choices of $\pi(0)$ and $t$) belong to small orbits and so we may write

$$u_p = |U_p| = p(p-1)+jp^2$$

for some $j$, i.e.,

(10) $$u_p \equiv -p \pmod{p^2}.$$

Hence,

$$\frac{u_p}{p-1} \equiv p \pmod{p^2}.$$

By (3′) we have for some integer $z$,

$$\begin{aligned}P_p &= p(p+zp^2-(p-2)!)\\ &\equiv p! \pmod{p^3}\end{aligned}$$

and the theorem is proved. ∎

THEOREM 3. *Suppose $p$ and $q$ are odd primes satisfying $p = 2q^\alpha + 1$ for some $\alpha \geqq 1$. Then*

(11) $$P_p \equiv 0 \pmod{q}$$

PROOF. Let $r$ be a fixed primitive root of $p$. Define the maps $\gamma, \delta: S_p \to S_p$ by

$$\left.\begin{aligned}\gamma(\pi)(k) &\equiv r\pi(k),\\ \delta(\pi)(k) &\equiv \pi(rk).\end{aligned}\right\} \pmod{p}$$

It is easy to check that $\gamma$ and $\delta$ map $U_p$ into $U_p$. Since for any $\pi \in U_p$, the $p-1$ permutations

$$\pi, \gamma(\pi), \gamma^{(2)}(\pi), \cdots, \gamma^{(p-2)}(\pi)$$

are distinct, then any orbit $\pi^G$ of $G$ must satisfy

(12) $$|\pi^G| \equiv 0 \pmod{p-1}$$

On the other hand, $\gamma$ and $\delta$ each have order $p-1$, they commute, and all the products $\gamma^i\delta^j$, $0 \leqq i, j < p-1$, are distinct. Therefore,

$$|G| = (p-1)^2 = 4q^{2\alpha}. \tag{13}$$

Let us call an orbit $\pi^G$ small if $|\pi^G| \,\Big|\, 4q^\alpha$. Thus, $\pi^G$ is small if and only if for some $m$, $0 < m < p-1$,

$$\delta^{(2)}(\pi) = \gamma^{(m)}(\pi)$$

iff

$$\pi(r^{2t}k) = r^{mt}\pi(k) \tag{14}$$

for all $k \in [0, p-1]$. Define $a_0$ and $a_1$ by

$$\pi(1) = r^{a_0},\ \pi(r) = r^{a_1},\ 0 \leqq a_0, a_1 < p-1.$$

Note that (14) implies $\pi(0) = 0$. Also, by (14) we have

$$\pi(r^{2t}) = r^{mt+a_0},\ \pi(r^{2t+1}) = r^{mt+a_1}$$

for $t = 0, 1, \cdots, q^\alpha$. Since $\delta^{(2)}$ has order $q^\alpha$ then we must have

$$(m, q) = 1 \qquad \text{and} \qquad m \equiv 0 \pmod 2. \tag{15}$$

Furthermore, it is also necessary that

$$a_0 - a_1 \equiv 1 \pmod 2 \tag{16}$$

since otherwise $\pi$ is not a permutation. Thus, by (14), (15) and (16) we see that there are exactly $q^{\alpha-1}(q-1)$ choices for $m$ and $2q^{2\alpha}$ choices for $(a_0, a_1)$ so that the permutation $\pi = \pi_{m,a_0,a_1}$ determined by $m$, $a_0$ and $a_1$ has a small orbit $\pi^G$.

We must next determine how many of these $\pi$ belong to $U_p$. By definition,

$$\pi \in U_p \qquad \text{iff} \qquad \sigma(\pi) = \sum_{k=0}^{p-1} k\pi(k) \equiv 0 \pmod p.$$

But

$$\sum_{k=0}^{p-1} k\pi(k) \equiv \sum_{k=0}^{q^\alpha-1} (r^{2k}\pi(r^{2k}) + r^{2k+1}\pi(r^{2k+1})) \equiv \sum_{k=0}^{q^\alpha-1} r^{2k+mk+a_0} + r^{2k+mk+a_1+1}$$

$$\equiv (r^{a_0} + r^{a_1+1}) \sum_{k=0}^{q^\alpha-1} r^{(m+2)k} \tag{17}$$

$$\equiv (r^{a_0} + r^{a_1+1}) \begin{cases} \dfrac{r^{(m+2)q^\alpha} - 1}{r^{m+2} - 1} & \text{if} \quad r^{m+2} \not\equiv 1 \pmod p \\ q^\alpha & \text{if} \quad r^{m+2} \equiv 1 \pmod p \end{cases}$$

where all congruences are modulo $p$. However, since $m$ is even by (15) then

$$r^{(m+2)q^\alpha} \equiv 1 \pmod p \quad \text{and so} \quad \sigma(\pi) = 0 \text{ when } r^{m+2} \not\equiv 1 \pmod p.$$

On the other hand, since $a_0$ and $a_1$ have different parity by (16) then $q^\alpha - a_0 - a_1 - 1$ is odd and so

$$2q^\alpha \nmid q^\alpha - a_0 - a_1 - 1.$$

Hence,

$$r^{q^\alpha - a_0 - a_1 - 1} \not\equiv 1 \pmod p,$$

$$r^{a_0 + a_1 + 1} \not\equiv r^{q^\alpha} \equiv -1 \pmod p, \quad r^{a_0} + r^{a_1} + 1 \not\equiv 0 \pmod p.$$

Thus, since $(q^\alpha, p) = 1$ then in the case that $r^{m+2} \equiv 1 \pmod p$ we have $\sigma(\pi) \neq 0$. Therefore, we see that $\pi = \pi_{m,a_0,a_1} \in U_p$ iff $r^{m+2} \equiv 1 \pmod p$, i.e., iff $m = 2q^\alpha - 2$. This implies that of the $q^{\alpha-1}(q-1)\cdot 2q^{2\alpha}$ permutations $\pi_{m,a_0,a_1}$ with small orbits, exactly

$$q^{\alpha-1}(q-1)\cdot 2q^{2\alpha} - 2q^{2\alpha} = (q^\alpha - q^{\alpha-1} - 1)\cdot 2q^{2\alpha}$$

of them belong to $U_p$. Since any $\tau \in U_p$ satisfies

$$|\tau^G| \,\Big|\, |G| = 4q^{2\alpha}$$

then if $\tau^G$ is not small, we have

$$2q^{\alpha+1} \,\Big|\, |\tau^G|.$$

Hence,

$$u_p = |U_p| \equiv (q^\alpha - q^{\alpha-1} - 1)2q^{2\alpha} \pmod{(2q^{\alpha+1})}. \tag{18}$$

Finally, by a straightforward calculation using (3′) we conclude that

$$P_p \equiv 0 \pmod q$$

and the theorem is proved.

## Some modular results for $n$ composite

For an $n$ by $n$ matrix $M = (m_{ij})$, let $m_i$ denote the row vector $(m_{i1}, \cdots, n_{in})$. For $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$, let $xy$ denote $(x_1y_1, \cdots, x_ny_n)$ and let $\bar{x}$ denote $\Sigma_{i=1}^n x_i$. Finally if $\eta$ is a partition of $[1, n]$ with blocks $B_1, \cdots, B_{|\eta|}$, define $c(\eta)$ by

$$c(\eta) = \prod_{i=1}^{|\eta|} (-1)^{|B_i|-1}(|B_i| - 1)!$$

It is known (see Crapo (1968)) that the permanent of $M$ can be expressed in the following form:

$$\operatorname{Per} M = \sum_{\eta} c(\eta) \prod_{B\in\eta} \overline{\left(\prod_{i\in B} m_i\right)}$$

where $\eta$ ranges over all partitions of $[1, n]$.

In the case that $M$ is the Schur matrix $M_n$, Graver (1967) has obtained from (15) the following particularly appealing expression for the permanent of $M_n$:

$$P_n = \sum_{\eta\in Q_n} c(\eta) n^{|\eta|} \tag{19}$$

where $|\eta|$ denotes the number of blocks of $\eta$ and $Q_n$ is the set of all partitions $\eta = (B_1, \cdots, B_{|\eta|})$ of $[1, n-1]$ for which $\Sigma_{b\in B_i} b \equiv 0 \pmod m$ for $1 \leqq i \leqq |\eta|$.

An important aspect of (19) is that if $p \mid n$ then for each $\eta \in Q_n$, either $|\eta|$ is small in which case a large power of $p$ divides $c(\eta)$, or $|\eta|$ is large and therefore a large power of $p$ divides $n^{|\eta|}$. This implies $P_n$ itself is always highly divisible by $p$ since each term in the sum is. A careful analysis of this behavior results in the following theorem.

THEOREM 4. *If $p^\alpha$ divides $n$ then $p^{(p^\alpha-1)n/(p-1)p^\alpha}$ divides $P_n$.* (This result for $\alpha = 1$ was given by Graver (1967)).

## The parity of $P_n$

THEOREM 5.

$$P_n \equiv n \pmod 2 \tag{20}$$

PROOF. For $n$ even, (20) follows from (4). Hence, we may assume $n$ is odd. Let $\Delta_n(1)$ denote the determinant of $M_n = M_n(1)$ so that

$$\begin{aligned}\Delta_n(1) &= \sum_{\pi\in S_n} (-1)^\pi \alpha_{0,\pi(0)} \cdots \alpha_{n-1,\pi(n-1)} \\ &= -\sum_{\pi\in S_n} \alpha_{0,\pi(0)} \cdots \alpha_{n-1,\pi(n-1)} + 2\sum_{\pi\in A_n} \alpha_{0,\pi(0)} \cdots \alpha_{n-1,\pi(n-1)} \\ &= -P_n + 2Q_n(1)\end{aligned}$$

where $A_n$ denotes subgroup of even permutations of $S_n$ and $(-1)^\pi$ is 1 if $\pi \in A_n$ and $-1$ otherwise. That is,

$$\Delta_n(1) + P_n = 2Q_n(1) \tag{21}$$

where

$$Q_n(1) = \sum_{k=0}^{n-1} c_k \varepsilon^k$$

for suitable integers $c_k$, $k \in [0, n-1]$.

Now it is well known (see Schur (1921)) that

$$\Delta_n(1) = i^{\binom{n}{2}} n^{n/2}.$$

For $1 \leqq t < n$ with $(t, n) = 1$, we see that

$$\Delta_n(t) = \det M_n(t) = (-1)^{\rho_t} \Delta_n(t)$$

where $\rho_t : [0, n-1] \to [0, n-1]$ is defined by $\rho_t(k) \equiv tk \pmod{n}$. (In fact, $(-1)^{\rho_t} = (t/n)$, the familiar Jacobi symbol.) Since the permanent of $M_n(t)$ is just $P_n$, independent of $t$, then we have

$$(22) \qquad (-1)^{\rho_t} i^{\binom{n}{2}} n^{n/2} + P_n = 2Q_n(t).$$

Hence,

$$(23) \qquad \prod_{\substack{t=1 \\ (t,n)=1}}^{n} ((-1)^{\rho_t} i^{\binom{n}{2}} n^{n/2} - P_n) = 2^{\varphi(n)} \prod_{\substack{t=1 \\ (t,n)=1}}^{n} Q_n(t).$$

The right hand side of (23) is a symmetric function of the primitive $n^{\text{th}}$ roots of unity and consequently, an even integer. Any irrational and imaginary terms occurring on the left hand side must cancel. The one term in the expansion free of the factor $P_n$ is

$$\left(\prod_t (-1)^{\rho_t}\right) i^{\binom{n}{2}\varphi(n)} n^{n\varphi(n)/2} = \pm n^{n\varphi(n)/2},$$

i.e., an odd rational integer. Thus, if $P_n$ were even then the left hand side would be an odd integer while the right hand side is even. This contradiction completes the proof. ∎

## Concluding remarks

The known values of $P_n$, $n$ odd, are listed below in Table 2.

*Table* 2.

| $n$ | $P_n$ | |
|---|---|---|
| 1 | 1 | |
| 3 | −3 | |
| 5 | −5 | |
| 7 | −105 | $= -3 \cdot 5 \cdot 7$ |
| 9 | 81 | $= 3^4$ |
| 11 | 6765 | $= 3 \cdot 5 \cdot 11 \cdot 41$ |
| 13 | 175747 | $= 11 \cdot 13 \cdot 1229$ |
| 15 | 30375 | $= 3^5 \cdot 5^3$ |
| 17 | 25219857 | $= 3 \cdot 13 \cdot 17 \cdot 38039$ |
| 19 | 142901109 | $= 3^2 \cdot 13 \cdot 19 \cdot 64283$ |
| 21 | 4548104883 | $= 3^8 \cdot 7^3 \cdot 43 \cdot 47$ |
| 23 | −31152650265 | $= -3^2 \cdot 5 \cdot 11 \cdot 23 \cdot 733 \cdot 3733$ |

The last three values were calculated using an efficient algorithm for permanents of Nijenhuis and Wilf (1975).

Note that by Theorem 4,

$$3^4 \mid P_9,\ 3^5 \cdot 5^3 \mid P_{15},\ 3^7 \cdot 7^3 \mid P_{21}$$

and, in fact, we have equality for the first two. Theorem 3 explains why $3 \mid P_7$, $5 \mid P_11$, and $11 \mid P_{23}$. Except for the fact that $n \mid P_n$, most of the other small factors are not yet understood.

It follows from results of Wilf (1968) (also see Ryser (1963)) that

$$P_n = \frac{1}{2^n} \sum_S (-1)^{w(S)} \det C(S) \tag{24}$$

where $C(S)$ denotes the circulant matrix with first row $S = (s_1, \cdots, s_n)$, $w(S)$ denotes $|\{i : s_i = -1\}|$, and $S$ ranges over all $2^n$ sequences of $\pm 1$'s. It then follows from the Hadamard bound on determinants of $\pm 1$'s. that $|P_n| \leqq n^{n/2}$. On the other hand, it is not even known if $P_n > 0$ infinitely often. From the limited data available, it certainly seems as if $\lim |P_n^{1/n}| > 0$.

**Acknowledgements**

The authors wish to acknowledge the valuable suggestions of H. S. Wilf and the aid of N. J. A. Sloane for his assistance in calculating $P_{17}$, $P_{19}$, $P_{21}$ and for pointing out the third reference by means of Sloane (1973).

**References**

Henry H. Crapo (1968), 'Permanents by Möbius Inversion', *J. Comb. Th.* **4**, 198–200.

J. E. Graver (1967), 'Notes on permanents' (unpublished).

D. H. Lehmer (1973), 'Some properties of circulants', *J. Number Theory* **5**, 43–54.

Th. Muir (1960), *The theory of determinants in the historical order of development*, (London (1890), New York, Dover).

A. Nijenhuis and H. S. Wilf (to appear 1975), *Combinatorial Algorithms*, (Acad. Press, New York).

H. J. Ryser (1963), *Combinatorial mathematics*, (Carus Monograph **14**, M.A.A., Wiley, New York).

I. Schur (1921), Über die Gausschen Summen', *Akad. Wiss. Göttingen, Nachrichten, Math-Phys. Klasse*, 147–153.

N. J. A. Sloane (1973), *A handbook of integer sequences*, (Acad. Press, New York).

H. S. Wilf, (1968), 'A mechanical counting method and combinatorial applications', *J. Comb. Th.* **4**, 246–258.

Bell Laboratories
Murray Hill, N. J. 07974
U. S. A.

University of California
Berkeley, California
U. S. A.