ON RECURSIONS CONNECTED WITH SYMMETRIC GROUPS I

S. CHOWLA, I. N. HERSTEIN AND W. K. MOORE

ALTHOUGH the title of the paper suggests that the nature of the problem considered is group theoretic, our methods are almost completely combinatorial and number theoretic in nature, the group theory entering only insofar as it leads us to various recursions that we study. Let T_n denote the number of solutions of $x^2 = 1$ in S_n, the symmetric group of degree n. We proceed to find a recursion for T_n from which we obtain an explicit solution. From this we obtain an asymptotic value for T_n. We also exhibit some congruence and divisibility properties of the T_n. In a later paper we shall consider the problem of the number of solutions of $x^k = 1$ in S_n for k an arbitrary positive integer.

We begin with finding a recursion formula for the T_n, the number of solutions of $x^2 = 1$ in S_n. Although the derivation of this recursion is very simple, we give two proofs of it which, in a sense, are of a different mood. We assume $T_0 = T_1 = 1$.

LEMMA 1. $T_n = T_{n-1} + (n-1)T_{n-2}$.

First Proof. The only elements of order two in S_n are those which are the product of disjoint transpositions, and the unit element. The number of elements of order two which can be obtained from the permutations of the digits $1, 2, \ldots, n-1$, alone are T_{n-1}. The only other such elements are obtained from involving the digit n in a transposition with some other digit and multiplying by any other permutation of order two involving the remaining $n - 2$ digits. Their number is clearly $(n-1)T_{n-2}$. Thus we obtain

$$T_n = T_{n-1} + (n-1)T_{n-2}. \tag{1}$$

Second Proof. It is well known that S_n is isomophic to the set of $n \times n$ matrices which have precisely one 1 in each row and column and zeros elsewhere. By direct checking it can be readily noted that the inverse of any such matrix is its transpose. So the question of the number of elements of order 2 in S_n becomes the question of finding how many self-adjoint matrices there are of the form described above. If the one in the top row occurs in the first column we are left an $(n-1) \times (n-1)$ matrix to consider, so the number of self-adjoint ones is T_{n-1}. If the one of the top row occurs in any other column, by the symmetry of the matrix, two rows and columns are used up, so we have an $(n-2) \times (n-2)$ matrix to consider, and we obtain T_{n-2}. Since the one in the top row could be put in $n - 1$ such columns, the total number of this form is $(n-1)T_{n-2}$ and so again we obtain our recursion.

Received June 8, 1950; in revised form February 20, 1951.

From the recursion we obtain the following

LEMMA 2. $n^{\frac{1}{2}} \leqslant \frac{T_n}{T_{n-1}} \leqslant n^{\frac{1}{2}} + 1.$

Proof. The proof is by induction over n.

1. If $n = 1$, $T_1/T_0 = 1$, and the result is correct.

2. Suppose the result is correct for $n = r$. Consider T_{r+1}/T_r. Since

$$T_{r+1} = T_r + rT_{r-1},$$
$$T_{r+1}/T_r = 1 + r/(T_r/T_{r-1}) \leqslant 1 + r/r^{\frac{1}{2}} \leqslant 1 + (r+1)^{\frac{1}{2}}.$$

Also,

$$T_{r+1}/T_r = 1 + rT_{r-1}/T_r \geqslant 1 + r/(1 + r^{\frac{1}{2}}) \geqslant (r+1)^{\frac{1}{2}},$$

since

$$n = \left\{(n+1)^{\frac{1}{2}} - 1\right\}\left\{(n+1)^{\frac{1}{2}} + 1\right\} > \left\{(n+1)^{\frac{1}{2}} - 1\right\}(n^{\frac{1}{2}} + 1).$$

So the lemma follows from the induction.

From the lemma it follows trivially that:

THEOREM 3. *T_n/T_{n-1} is asymptotic to $n^{\frac{1}{2}}$.*

We again return to the recursion (1). Let $T_n = n!\,a_n$. Substituting in (1) we immediately obtain

(2) $$na_n = a_{n-1} + a_{n-2}; \quad a_0 = a_1 = 1.$$

Consider the function $y = \sum_{i=0}^{\infty} a_i x^i$. We ask ourselves, what differential equation should y satisfy if the a_n satisfy the recursion in (2)? The differential equation suggested can be seen to be

$$x\,dy/dx = xy + x^2 y.$$

Solving this by separating variables we see that

$$y = A \exp\left(x + \tfrac{1}{2}x^2\right).$$

Since $a_0 = 1$, $A = 1$. Thus we have:

THEOREM 4. *a_n is the coefficient of x^n in the power series expansion of* $\exp(x + \frac{1}{2}x^2)$.

Using the fact that

$$\exp(x + \tfrac{1}{2}x^2) = (\exp x)(\exp \tfrac{1}{2}x^2) = \sum_{i=0}^{\infty} \frac{x^i}{i!} \cdot \sum_{j=0}^{\infty} \frac{x^{2j}}{2^j j!} = \sum_{2j+i=n} \frac{x^n}{2^j j!\,i!},$$

we obtain

(3) $$a_n = \sum_{2j+i=n} \frac{1}{2^j j!\,i!}$$

(4) $$T_n = n! \sum_{2j+i=n} \frac{1}{2^j j!\,i!}.$$

On the other hand,

$$\exp(x + \tfrac{1}{2}x^2) = e^{-\frac{1}{2}} \exp\left(\frac{1+x}{2}\right)^2 = e^{-\frac{1}{2}} \sum_{n=0}^{\infty} \frac{(1+x)^{2n}}{2^n n!}.$$

whence,

$$a_{2m} = e^{-\frac{1}{2}} \frac{1}{2^m m!}\left(1 + \frac{2m+1}{2} + \frac{(2m+1)(2m+3)}{4} + \dots\right)$$

$$= e^{-\frac{1}{2}} \frac{1}{2^m m!} W_m = e^{-\frac{1}{2}} \frac{1}{2^m m!} (1 + \sum_{s=1}^{\infty} V_s),$$

where

$$V_s = \frac{(2m+1)(2m+3)(2m+5)\dots(2m+2s-1)}{(2s)!}.$$

Our first goal is an estimate of the size of W_m. This is given by

THEOREM 5. $W_m \sim \frac{1}{2} e^{\frac{1}{4} + (2m)^{\frac{1}{2}}}$.

To prove[1] Theorem 5, we need:

LEMMA 6 (Stirling's formula). *If x is a positive integer,*

$$\log x! = (x + \tfrac{1}{2}) \log x - x + \tfrac{1}{2} \log (2\pi) + O(x^{-1}).$$

LEMMA 7. *Suppose $b > a$ and that the interval (a, b) is divided into n equal parts of length h; let $f(x)$ be differentiable in (a, b) and $|f'(x)| \leqslant M$ in the interval. Then*

$$\left|\sum_{h=0}^{n-1} h f(a + rh) - \int_a^b f(x)dx\right| \leqslant h(b-a) M.$$

This lemma is an immediate consequence of the theory of Riemann integration and the first mean-value theorem of the differential calculus.

Consider V_s for

(5) $$s = xm^{\frac{1}{2}}$$

and

(6) $$\tfrac{1}{2} < x < 1 \qquad (m > m_0).$$

Now, using Lemma 6,

$$\log V_s = \sum_{t=1}^{s} \log(2m + 2t - 1) - \log(2s)!$$

$$= \sum_{t=1}^{s} \left\{\log 2m + \frac{2t-1}{2m} + O\left(\frac{t^2}{m^2}\right)\right\} - \{(2s + \tfrac{1}{2}) \log(2s) - 2s + \tfrac{1}{2}\log(2\pi) + O(s^{-1})\}$$

$$= s \log(2m) + \frac{s^2}{2m} + O\left(\frac{s^3}{m^2}\right) - \{(2s + \tfrac{1}{2}) \log(2s) - 2s + \tfrac{1}{2}\log(2\pi) + O(m^{-\frac{1}{2}})\}$$

[1]We should like to thank Dr. W. R. Scott who carefully checked the proof of Theorem 5.

(7) $$= - xm^{\frac{1}{2}} \log(2x^2) + 2xm^{\frac{1}{2}} - \tfrac{1}{2}\log(2xm^{\frac{1}{2}}) - \tfrac{1}{2}\log(2\pi) + \tfrac{1}{2}x^2 + O(m^{-\frac{1}{2}}).$$

In (5), put

(8) $$x = 2^{-\frac{1}{2}} + y$$

and restrict the limits of s by the inequality

(9) $$|y| \leqslant \epsilon = m^{-5/24}.$$

Since

(10) $$\log(1 + t) = t - \tfrac{1}{2}t^2 + O(t^3),$$

for small t we obtain:

$$\log V_s = (2m)^{\frac{1}{2}} + 2m^{\frac{1}{2}}y - m^{\frac{1}{2}}(2^{-\frac{1}{2}} + y)\log(1 + 2^{3/2}y + 2y^2)$$
$$- \tfrac{1}{2}\log\{(2m)^{\frac{1}{2}} + 2m^{\frac{1}{2}}y\} - \tfrac{1}{2}\log(2\pi) + \tfrac{1}{4} + O(m^{-1/8})$$
$$= \tfrac{1}{4} - \tfrac{1}{2}\log(2\pi) + (2m)^{\frac{1}{2}} - \tfrac{1}{4}\log(2m) - (2m)^{\frac{1}{2}}y^2 + O(m^{\frac{1}{2}}y^3) + O(m^{-1/8})$$

(11) $$= \tfrac{1}{4} - \tfrac{1}{2}\log(2\pi) + (2m)^{\frac{1}{2}} - \tfrac{1}{4}\log(2m) - (2m)^{\frac{1}{2}}y^2 + O(m^{-1/8}),$$

(12) $$V_s = \frac{e^{\frac{1}{4}}}{(2\pi)^{\frac{1}{2}}}\frac{e^{(2m)^{\frac{1}{2}}}}{(2m)^{\frac{1}{4}}}\, e^{-(2m)^{\frac{1}{2}}y^2}\{1 + O(m^{-1/8})\}.$$

Hence

$$\sum_{\epsilon \leqslant y \leqslant \epsilon} V_s = \frac{e^{\frac{1}{4}}}{(2\pi)^{\frac{1}{2}}}\, e^{(2m)^{\frac{1}{2}}} \sum_s \frac{e^{-(2m)^{\frac{1}{2}}y^2}}{(2m)^{\frac{1}{4}}}\{1 + O(m^{-1/8})\}$$

(13) $$= \frac{e^{\frac{1}{4}}}{(4\pi)^{\frac{1}{2}}}\, e^{(2m)^{\frac{1}{2}}} \sum_s \left[\frac{2}{m}\right]^{\frac{1}{4}} e^{-(2m)^{\frac{1}{2}}y^2}\{1 + O(m^{-1/8})\},$$

where the summation is for all positive integers satisfying

$$|y| \leqslant \epsilon = m^{-5/24};$$

also $O(m^{-1/8})$ stands for $K_s m^{-1/8}$, where $|K_s| \leqslant |K$ an absolute constant for all s.

We proceed to show that

(14) $$\sum_s \left(\frac{2}{m}\right)^{\frac{1}{4}} e^{-(2m)^{\frac{1}{2}}y^2} \sim \int_{-\infty}^{\infty} e^{-w^2}\, dw = \pi^{\frac{1}{2}}.$$

From (13) and (14) we finally obtain

(15) $$\sum_{|y| \leqslant \epsilon} V_s \sim \tfrac{1}{2}\, e^{\frac{1}{4}}\, e^{(2m)^{\frac{1}{2}}},$$

a result to which we shall return later.

To prove (14) we set

(16) $$y = \frac{w}{(2m)^{\frac{1}{4}}}$$

https://doi.org/10.4153/CJM-1951-038-3 Published online by Cambridge University Press

and observe that as s increases by (1), x increases by $m^{-\frac{1}{2}}$, y increases by the same amount, and w increases by $\left(\frac{2}{m}\right)^{\frac{1}{2}}$. Since $w = w(s)$ is a function of s we can write

$$w(s+1) - w(s) = \left(\frac{2}{m}\right)^{\frac{1}{2}}, \tag{17}$$

the sum (14) becomes

$$\sum_{s_1 \leqslant s \leqslant s_2} e^{-w^2(s)}\{w(s+1) - w(s)\}, \tag{18}$$

where s_1 and s_2 are the smallest and largest positive integers s in the range $|y| \leqslant \epsilon$, i.e.

$$|w| \leqslant 2^{\frac{1}{2}}\, m^{1/24}. \tag{19}$$

From (17) and (19),

$$0 \leqslant w(s_1) + 2^{\frac{1}{2}} m^{1/24} \leqslant \left(\frac{2}{m}\right)^{\frac{1}{2}}, \tag{20}$$

and

$$0 \leqslant 2^{\frac{1}{2}} m^{1/24} - w(s_2) \leqslant \left(\frac{2}{m}\right)^{\frac{1}{2}}. \tag{21}$$

Clearly the sum in (18) is (by a crude estimate) equal to

$$\sum_{s_1 \leqslant s \leqslant s_2 - 1} e^{-w^2(s)}\{w(s+1) - w(s)\} + O(m^{-1/8}). \tag{22}$$

Now from Lemma 7,

$$\left| \sum_{s_1 \leqslant s \leqslant s_2 - 1} e^{-w^2} \left(\frac{2}{m}\right)^{\frac{1}{2}} - \int_{w_1}^{w_2} e^{-w^2}\, dw \right| = O\left(\frac{m^{1/24}}{m^{\frac{1}{4}}}\right) = O(m^{-5/24}), \tag{23}$$

where $w_1 = w(s_1)$, $w_2 = w(s_2)$. Clearly, $-w_1, w_2 \to \infty$. Also (14) follows from (17), (18), (19), (20), (21), (22), and (23). Hence we have established (15).

We next proceed to prove

$$\sum_{|y| > \epsilon} V_s = O\left(\frac{e^{(2m)^{\frac{1}{2}}}}{m^{1/24}}\right). \tag{24}$$

For $s \geqslant [(\frac{1}{2}m)^{\frac{1}{2}} + m^{\frac{1}{2}}\epsilon] = s_2$, $m > m_0$, we have

$$\begin{aligned} \frac{V_{s+1}}{V_s} = \frac{2m + 2s + 1}{(2s+1)(2s+2)} &\leqslant \frac{m}{2s^2} + O(m^{-\frac{1}{2}}) \\ &\leqslant \frac{1}{2(2^{-\frac{1}{2}} + \epsilon)^2} + O(m^{-\frac{1}{2}}) \\ &\leqslant 1 - 2^{\frac{1}{2}}\epsilon + O(\epsilon^2) + O(m^{-\frac{1}{2}}) \\ &\leqslant 1 - \epsilon, \end{aligned} \tag{25}$$

https://doi.org/10.4153/CJM-1951-038-3 Published online by Cambridge University Press

since $\epsilon = m^{-5/24}$. From (12),

$$V_{s_2} = O\left(\frac{e^{(2m)^{\frac{1}{2}}}}{m^{\frac{1}{4}}}\right). \tag{26}$$

So,

$$\sum_{s \geq s_2} V_s = O\left(\frac{e^{(2m)^{\frac{1}{2}}}}{m^{\frac{1}{4}}\epsilon}\right) = O\left(\frac{e^{(2m)^{\frac{1}{2}}}}{m^{1/24}}\right). \tag{27}$$

Similarly,

$$\sum_{s \leqslant s_1} V_s = O\left(\frac{e^{(2m)^{\frac{1}{2}}}}{m^{1/24}}\right). \tag{28}$$

From (15), (27), and (28),

$$W_m = 1 + \sum_{s=1}^{\infty} V_s \sim \tfrac{1}{2} e^{\frac{1}{4}+(2m)^{\frac{1}{2}}}, \tag{29}$$

establishing Theorem 5.

Now for $n = 2m$,

$$T_n = n! \, \frac{e^{-\frac{1}{2}}}{2^m m!} W_m \sim \left(\frac{n}{e}\right)^{\frac{1}{2}n} \frac{e^{n^{\frac{1}{2}}}}{2^{\frac{1}{2}} e^{\frac{1}{4}}}. \tag{30}$$

For odd n, $n = 2m + 1$,

$$T_{2m+1} \sim T_{2m}(2m)^{\frac{1}{2}},$$

from Theorem 3. Thus

$$T_{2m+1} \sim 2^{-\frac{1}{2}} e^{-\frac{1}{4}} \left(\frac{2m}{e}\right)^m e^{(2m)^{\frac{1}{2}}} (2m)^{\frac{1}{2}}. \tag{31}$$

But

$$\frac{\left(\frac{2m+1}{e}\right)^m \left(\frac{2m+1}{e}\right)^{\frac{1}{2}}}{(2m)^{\frac{1}{2}} \left(\frac{2m}{e}\right)^m} \; \frac{e^{(2m+1)^{\frac{1}{2}}}}{e^{(2m)^{\frac{1}{2}}}} \to 1 \tag{32}$$

as $m \to \infty$. So

$$T_{2m+1} \sim \frac{1}{2^{\frac{1}{2}}} \frac{1}{e^{\frac{1}{4}}} \left(\frac{2m+1}{e}\right)^{\frac{1}{2}(2m+1)} e^{(2m+1)^{\frac{1}{2}}}, \tag{33}$$

and (30) and (33) together prove

THEOREM 8.
$$T_n \sim \frac{(n/e)^{\frac{1}{2}n} e^{n^{\frac{1}{2}}}}{2^{\frac{1}{2}} e^{\frac{1}{4}}}.$$

We now turn to some other properties of the T_n's. These results on divisibility and congruences of the T_n's, while they are very easy to prove, are of some interest.

We first prove

THEOREM 9. *If m is an odd integer, then $T_{n+m} \equiv T_n \pmod{m}$.*

Proof. It is clear that it is sufficient to prove the theorem for prime powers. The proof for these is exactly the same as the proof for odd primes. So we prove the theorem for odd primes. The proof is by induction over n, where $m = p$, a prime.

(i) If $n = 0$, then $T_p = p! \sum_{2i+j=n} \frac{1}{2^i i! j!}$ and this is clearly congruent to $1 = T_0$ modulo p, if p is an odd prime.

(ii) If $n = 1$, $T_{p+1} = T_p + (p + 1 - 1)T_{p-1}$ and this is congruent to T_p modulo p, hence to 1; that is $T_{p+1} \equiv T_1 \pmod{p}$.

(iii) Suppose that $T_{r+p} \equiv T_r \pmod{p}$. Now

$$T_{r+1+p} = T_{r+p} + (r + p)T_{r+p-1} \equiv T_r + rT_{r-1} \pmod{p},$$

by our induction. Since $T_{r+1} = T_r + rT_{r-1}$, our result follows.

The other number theoretic property of T_n that we prove is that it is highly divisible by powers of 2. In fact, we prove

THEOREM 10. *If $n \geqslant 4s - 2$, then 2^s divides T_n.*

Proof. By induction over s.

(i) If $s = 1$, since all the T_n's for $n \geqslant 2$ are even (as can be easily seen from the recursion), the result is correct.

(ii) Suppose that if $n \geqslant 4r - 2$, $2^r | T_n$. Let $n \geqslant 4(r + 1) - 2 = 4r + 2$.

$$\begin{aligned} T_n &= T_{n-1} + (n - 1)T_{n-2} = nT_{n-2} + (n - 2)T_{n-3} \\ &= (2n - 2)T_{n-3} + n(n - 3)T_{n-2}. \end{aligned}$$

Since $n - 4 \geqslant 4r - 2$, then $2^r | T_{n-3}$ and $2^r | T_{n-4}$. Since the coefficients of each of these in the expression for T_n is even, $2^{r+1} | T_n$. This concludes the induction and proves the theorem.

We should like to make one remark. In Theorem 3 we proved that $T_n/T_{n-1} \sim n^{\frac{1}{2}}$. We feel that much more is true, namely that $T_n/T_{n-1} = n^{\frac{1}{2}} + A + Bn^{-\frac{1}{2}} + Cn^{-1} + Dn^{-3/2} + \ldots$, for appropriate constants $A, B, C, D, \ldots$.

University of Kansas