ON SOLUTIONS OF $x^d = 1$ IN SYMMETRIC GROUPS

LEO MOSER AND MAX WYMAN

1. Introduction. Several recent papers have dealt with the number of solutions of $x^d = 1$ in S_n, the symmetric group of degree n. Let us denote this number by $A_{n,d}$ and let $A_{n,2} = T_n$. Chowla, Herstein and Moore **(1)** proved:

1.1 $$T_n = T_{n-1} + (n-1)T_{n-2} \qquad T_0 = T_1 = 1$$

1.2 $$n^{\frac{1}{2}} \leqslant T_n/T_{n-1} \leqslant n^{\frac{1}{2}} + 1$$

1.3 $$T_n = n! \sum_{j=0}^{[\frac{1}{2}n]} 1/\{2^j j!(n-2j)!\}$$

1.4 $$\sum_{n=0}^{\infty} T_n x^n/n! = e^{x+\frac{1}{2}x^2}$$

1.5 $$T_n \sim \frac{(n/e)^{\frac{1}{2}n} e^{n^{\frac{1}{2}}}}{2^{\frac{1}{2}} e^{1/4}}.$$

In §2 we establish a connection between T_n and the Hermite polynomials. This will enable us to refine 1.5 and to prove a conjecture concerning T_n/T_{n-1} made in **(1)**.

Jacobsthal **(3)** showed that for p a prime

1.6 $$\sum_{n=0}^{\infty} A_{n,p}\, x^n/n! = e^{x+x^p/p}.$$

This was generalized by Chowla, Herstein and Scott **(2)** who proved

1.7 $$\sum_{n=0}^{\infty} A_{n,d}\, x^n/n! = \exp \sum_{k \mid d} x^k/k.$$

The problem of finding asymptotic formulae for $A_{n,d}$ was proposed in **(2)**. In §3 we obtain asymptotic formulae for T_n and $A_{n,p}$ by a method which also yields results in the general case.

It was pointed out in **(2)** that Frobenius' theorem implies

1.8 $$A_{n,p} \equiv 0 \pmod{p}$$

and this, together with an explicit expression for $A_{n,p}$ constitutes a generalization of Wilson's theorem. Some other arithmetic properties of T_n were developed in **(1)**. In §4 we obtain still another generalization of Wilson's theorem, and also further arithmetic properties of T_n.

In §5 we show how some corresponding results can be obtained for the number of solutions of $x^d = 1$ in alternating groups.

Received June 16, 1954.

2. T_n and the Hermite Polynomials. The recurrence 1.1 is similar to that satisfied by the Hermite polynomials, namely

2.1 $$H_n(x) = 2x\,H_{n-1}(x) - 2(n-1)\,H_{n-2}(x), \quad H_0(x) = 1, \quad H_1(x) = 2x.$$

In fact, we prove the following theorem:

2.2 $$T_n = \frac{H_n(i/2^{\frac{1}{2}})}{i^n 2^{\frac{1}{4}n}}, \qquad i^2 = -1.$$

Since 2.2 is readily verified for $n = 0$ and $n = 1$ we may proceed by induction. Using the induction hypothesis and 2.1 we obtain,

$$T_{n-1} + (n-1)T_{n-2}$$
$$= \frac{H_{n-1}(i/2^{\frac{1}{2}})}{i^{n-1}2^{\frac{1}{4}(n-1)}} + \frac{(n-1)H_{n-2}(i/2^{\frac{1}{2}})}{i^{n-2}2^{\frac{1}{4}(n-2)}} = \frac{H_n(i/2^{\frac{1}{2}})}{i^n 2^{\frac{1}{4}n}}$$

which completes the proof.

From 2.2 we can obtain the asymptotic expansion of T_n. The asymptotic expansion of $H_n(x)$ is given by Szegö **(4**, p. 194**)** to be

2.3 $$\lambda_n^{-1} e^{-\frac{1}{2}x^2} H_n(x) = \cos(N^{\frac{1}{2}}x - \tfrac{1}{2}n\pi)\sum_{\nu=0}^{p-1} U_\nu(x)\,N^{-\nu}$$
$$+ N^{-\frac{1}{2}}\sin(N^{\frac{1}{2}}x - \tfrac{1}{2}n\pi)\sum_{\nu=0}^{p-1} V_\nu(x)\,N^{-\nu} + \exp\{-N^{\frac{1}{2}}|\mathcal{J}(x)|\}\,O(n^{-p}),$$

where $N = 2n + 1$ and

$$\lambda_n = \frac{\Gamma(n+1)}{\Gamma(\frac{1}{2}n+1)} \text{ or } \lambda_n = \frac{\Gamma(n+2)}{\Gamma(\frac{1}{2}n+3/2)}N^{-\frac{1}{2}}$$

according as n is even or odd. The coefficients $U_\nu(x)$ and $V_\nu(x)$ are polynomials depending on ν; they contain only even and odd powers of x, respectively. The first two terms of this expansion yield

2.4 $$H_n(x) \sim \frac{\Gamma(n+1)}{\Gamma(\frac{1}{2}n+1)}\,e^{\frac{1}{2}x^2}\,(\cos(N^{\frac{1}{2}}x - \tfrac{1}{2}n\pi) + \tfrac{1}{6}x^3N^{-\frac{1}{2}}\sin(N^{\frac{1}{2}}x - \tfrac{1}{2}n\pi)).$$

Using 2.2, 2.4 and the asymptotic expansion of the gamma function we obtain the theorem

2.5 $$T_n \sim \frac{(n/e)^{\frac{1}{2}n}e^{n^{\frac{1}{2}}}}{2^{\frac{1}{4}}e^{1/4}}\left(1 + \frac{7}{24n^{\frac{1}{2}}} + \dots\right).$$

This is a refinement of 1.5. A numerical check of 2.5 and a still more accurate formula for T_n derived in §3 will be given later in the paper.

We next consider $R_n = T_n/T_{n-1}$. By 1.1 we have

2.6 $$R_{n+1} = 1 + n/R_n.$$

Iterating 2.6 gives the continued fraction expansion

2.7 $$R_{n+1} = 1 + \frac{n}{1+}\,\frac{n-1}{1+}\,\frac{n-2}{1+}\cdots\frac{1}{1}.$$

We now use elementary means to sharpen the bounds for R_n given in 1.2. Let α_n be the positive solution of $x^2 - x - n = 0$, i.e.,

2.8 $$\alpha_n = (1 + \tfrac{1}{2}(4n + 1)^{\frac{1}{2}}).$$

We prove

2.9 $$\alpha_{n-1} \leqslant R_n \leqslant \alpha_n.$$

Proof. We proceed by induction over n. The result is trivial for $n = 1$. Assume it true for $n = K$, then

$$R_{K+1} = 1 + K/R_K \geqslant 1 + K/\alpha_K = \alpha_K.$$

Also,

$$R_{K+1} = 1 + K/R_K \leqslant 1 + K/\alpha_{K-1}.$$

It remains to show that

$$1 + K/\alpha_{K-1} \leqslant \alpha_{K+1}$$

and this follows from 2.8 and simple algebraic manipulation. An easy consequence of 2.9 is

2.10 $$\lim_{n\to\infty} (R_n - n^{\frac{1}{2}}) = \tfrac{1}{2}.$$

In **(1)** it was conjectured that

2.11 $$R_n \sim n^{\frac{1}{2}} + A + Bn^{-\frac{1}{2}} + Cn^{-1} + \ldots$$

for appropriate constants A, B, C, ... We shall prove this conjecture and obtain the following theorem

2.12 $$R_n \sim n^{\frac{1}{2}} + \tfrac{1}{2} - \tfrac{1}{8}n^{-\frac{1}{2}} + \ldots.$$

Proof. Let us consider

2.13 $$f_n(x) = xH_n(x)/H_{n-1}(x).$$

From 2.2 and 2.13 we have

2.14 $$R_n = -f_n(i/2^{\frac{1}{2}}).$$

However, it is well known that

2.15 $$H_n'(x) = 2n\,H_{n-1}(x).$$

Hence,

2.16 $$f_n(x) = 2n\,x\frac{H_n(x)}{H_n'(x)} = \frac{2nx}{(\log H_n(x))'}.$$

If we restrict x to be pure imaginary, say $x = it$, $t > 0$, then the expansion 2.3 takes the form

2.17 $$H_n(x) \sim \tfrac{1}{2}\lambda_n e^{\frac{1}{4}x^2} i^n e^{-iN^{\frac{1}{2}}x}\left[\sum_{\nu=0}^{p-1} U_\nu(x)\,N^{-\nu} + \frac{1}{iN^{\frac{1}{2}}}\sum_{\nu=0}^{p-1} V_\nu(x)\,N^{-\nu}\right].$$

From 2.15, $H_n'(x)$ is known to have an asymptotic expansion of the form 2.3. Hence differentiation of 2.3 is justified and leads to

$$2.18 \qquad (\log H_n(x))' \sim x - iN^{\frac{1}{2}} + \sum_{\nu=1}^{p-1} q_\nu(x)\, N^{-\nu} + \frac{1}{iN^{\frac{1}{2}}} \sum_{\nu=0}^{p-1} Q_\nu(x)\, N^{-\nu}$$

where again, $q_\nu(x)$ and $Q_\nu(x)$ are polynomials in x. Since these polynomials contain only even powers of x, and odd powers of x respectively, the coefficients of the various powers of $N^{-\nu}$ will be real in 2.17 and pure imaginary in 2.18. Hence for $x = i/2^{\frac{1}{2}}$,

$$2.19 \qquad f_n(i/2^{\frac{1}{2}}) \sim \frac{2^{\frac{1}{2}} n}{2^{\frac{1}{2}} - N^{\frac{1}{2}} + \beta_1 + \beta_2 N^{-\frac{1}{2}} + \dots}$$

where $\beta_1, \beta_2 \dots$ are constants. Hence,

$$2.20 \qquad R_n \sim \frac{2^{\frac{1}{2}} n}{N^{\frac{1}{2}}} \left(1 + \frac{\gamma_1}{N^{\frac{1}{2}}} + \frac{\gamma_2}{N} + \dots\right)$$

where $\gamma_1, \gamma_2 \dots$ are constants. Since $N = 2n+1$ we may expand in terms of n and find

$$2.21 \qquad R_n \sim n^{\frac{1}{2}} \left(1 + \frac{\delta_1}{n^{\frac{1}{2}}} + \frac{\delta_2}{n} + \dots\right)$$

where $\delta_1, \delta_2 \dots$ are constants. We have calculated the first three terms to be those given in 2.12.

3. Asymptotic Expansions. Previously in this paper we obtained an asymptotic expansion of T_n by recognizing the relationship between T_n and the Hermite polynomials. This method of course does not help us when considering the more general problem involving $A_{n,d}$. In this section we shall obtain an asymptotic expansion for T_n by a different method. This method not only applies to $A_{n,d}$, but also to many other problems, some of which will be discussed in a later paper.

In our method we make use of a result, indicated in the following lemma, which is probably known. Since we have been unable to find a reference we include, for completeness, a proof of the

LEMMA. *Let $f(z)$ be a function of a complex variable z regular in a neighborhood of $z = 0$. If*

(a) $f(0) = 0$,

(b) *the Maclaurin expansions of $f(z)$, $e^{f(z)}$ are*

$$f(z) = \sum_{k=1}^{\infty} a_k z^k, \quad e^{f(z)} = 1 + \sum_{k=1}^{\infty} b_k z^k,$$

(c) $|a_k| \leqslant K\sigma^k$,

where K, σ are positive numbers, then

$$3.1 \qquad |b_k| \leqslant K\,\sigma^k (1 + K)^{k-1}.$$

Proof. By Taylor's Theorem,

$$3.2 \qquad a_k = \frac{1}{k!} \left(\frac{d^k f(z)}{dz^k}\right)_{z=0}$$

$$3.3 \qquad b_k = \frac{1}{k!} \left(\frac{d^k e^{f(z)}}{dz^k}\right)_{z=0}.$$

Since $b_1 = a_1$ the result is trivially true for $k = 1$. From 3.3 we may write

3.4 $$b_{k+1} = \frac{1}{(k+1)!}\frac{d^k}{dz^k}\left[e^{f(z)}\frac{df}{dz}\right]_{z=0}.$$

Expanding the kth derivative of a product we have

3.5 $$b_{k+1} = \frac{1}{(k+1)}\sum_{s=0}^{k} b_s a_{k-s+1}(k-s+1), \qquad b_0 = 1.$$

Hence

3.6 $$|b_{k+1}| \leqslant \sum_{s=0}^{k} |b_s||a_{k-s+1}|.$$

From (c) we obtain

3.7 $$|b_{k+1}| \leqslant K\sigma^{k+1}\left(1 + \sum_{s=1}^{k} |b_s|\,\sigma^{-s}\right).$$

From 3.7 the result follows easily by induction.

We now proceed to outline our method for finding an asymptotic expansion of T_n. By 1.4 and Cauchy's theorem,

3.8 $$T_n = \frac{n!}{2\pi i}\int_C (e^{z+\frac{1}{2}z^2})\, z^{-(n+1)}dz,$$

where C is the circle $z = Re^{i\theta}$. Hence T_n can be expressed as

3.9 $$T_n = H\int_{-\pi}^{\pi} e^{f(\theta)}d\theta,$$

where

3.10 $$H = (n!\, e^{R+\frac{1}{2}R^2})/2\pi R^n$$

and

3.11 $$f(\theta) = R(e^{i\theta} - 1) + \tfrac{1}{2}R^2(e^{2i\theta} - 1) - in\theta.$$

If we let

3.12 $$\epsilon = R^{-3/4}$$

and

3.13 $$I = \int_{\epsilon}^{\pi} e^{f(\theta)}d\theta$$

then a simple calculation shows that $|I| = O(e^{-R^{\frac{1}{2}}})$. Since we shall show that our asymptotic expansion of the integral in 3.9 involves only powers of $1/R$ we may drop 3.13 and write

3.14 $$T_n \sim H\int_{-\epsilon}^{\epsilon} e^{f(\theta)}d\theta.$$

Expanding $f(\theta)$ in a Maclaurin expansion we obtain

3.15 $$f(\theta) = i(R^2 + R - n)\theta - \theta^2(R^2 + \tfrac{1}{2}R) + \sum_{k=3}^{\infty}(R + 2^{k-1}R^2)\frac{(i\theta)^k}{k!}.$$

We now choose R so that

3.16 $$R^2 + R - n = 0$$

and define ϕ by means of

3.17 $$\phi = \theta(R^2 + \tfrac{1}{2}R)^{\frac{1}{2}}.$$

https://doi.org/10.4153/CJM-1955-021-8 Published online by Cambridge University Press

We may then write 3.14 in the form

3.18 $$T_n \sim J \int_{-c}^{c} e^{-\phi^2 + F(z,\phi)} d\phi$$

where

3.19 $$c = \epsilon(R^2 + \tfrac{1}{2}R)^{\frac{1}{2}}$$

3.20 $$z = 1/R$$

3.21 $$J = H/(R^2 + \tfrac{1}{2}R)^{\frac{1}{2}}$$

3.22 $$F(z, \phi) = \sum_{k=3}^{\infty} (z + 2^{k-1})(1 + \tfrac{1}{2}z)^{-\frac{1}{2}k} z^{k-2} \frac{(i\phi)^k}{k!}.$$

Since $\epsilon = R^{-3/4}$, $c = O(R^{1/4})$ and $c \to \infty$ as $R \to \infty$. Further for any fixed ϕ, $F(z, \phi)$ is regular in the neighborhood $|z| < 2$ and $e^{F(z,\phi)}$ will have a Maclaurin expansion of the form

3.23 $$e^F = \sum_{m=0}^{\infty} \psi_m(\phi)\, z^m,$$

where $\psi_m(\phi)$ is a polynomial in ϕ. Hence

3.24 $$T_n \sim J\left[\sum_{m=0}^{s-1} \left(\int_{-c}^{c} e^{-\phi^2} \psi_m(\phi) d\,\phi \right) z^m + R_s \right]$$

where

3.25 $$R_s = \int_{-c}^{c} \left(e^{-\phi^2} \sum_{m=s}^{\infty} \psi_m(\phi) z^m \right) d\phi.$$

Since $\psi_m(\phi)$ is a polynomial in ϕ and $c = O(R^{1/4})$ one can place

3.26 $$\int_{-c}^{c} e^{-\phi^2} \psi_m(\phi)\, d\phi = \int_{-\infty}^{\infty} e^{-\phi^2} \psi_m(\phi)\, d\phi$$

with an error that is of exponential order. Hence we write

3.27 $$T_n \sim J\left[\sum_{m=0}^{s-1} \left(\int_{-\infty}^{\infty} e^{-\phi^2} \psi_m(\phi)\, d\phi \right) z^m + R_s \right].$$

In order to complete our proof we merely have to show that, for fixed s, $|R_s| = 0(|z|^s)$.

If the Maclaurin expansion of $F(z, \phi)$, as a function of z, is written

3.28 $$F(z, \phi) = \sum_{r=1}^{\infty} a_r(\phi)\, z^r,$$

then by 3.22

3.29 $$a_r(\phi) = \frac{1}{r!} \sum_{k=3}^{r+2} \left[\frac{d^r}{dz^r} (z + 2^{k-1})(1 + \tfrac{1}{2}z)^{-\frac{1}{2}k} z^{k-2} \right]_{z=0} \frac{(i\phi)^k}{k!}.$$

By using Cauchy's theorem for derivatives one may easily show, for $|z|<1$, that

3.30 $$\left| \frac{1}{r!} \frac{d^r}{dz^r} (z + 2^{k-1})(1 + \tfrac{1}{2}z)^{-\frac{1}{2}k} z^{k-2} \right|_{z=0} \leqslant 2^{2k}.$$

https://doi.org/10.4153/CJM-1955-021-8 Published online by Cambridge University Press

Hence

3.31 $$|a_r(\phi)| \leqslant \sum_{k=3}^{r+2} \frac{(4|\phi|)^k}{k!}.$$

From 3.31 it is easy to show by induction that

3.32 $$|a_r(\phi)| \leqslant (4|\phi|^2(1 + 4|\phi|)^r.$$

Making use of our lemma with $K = (4|\phi|)^2$, $\sigma = 1 + 4|\phi|$ we have

3.33 $$|\psi_m(\phi)| \leqslant (4|\phi|)^2(1 + 4|\phi|)^m(2 + (4|\phi|)^2)^{m-1}.$$

Hence

3.34 $$\left|\sum_{m=s}^{\infty} \psi_m(\phi)\, z^m\right| \leqslant \frac{(4|\phi|)^2(1 + 4|\phi|)^s(2 + (4|\phi|)^2)^{s-1}|z|^s}{M}$$

where

3.35 $$M = 1 - (1 + 4|\phi|)(2 + (4|\phi|)^2)|z|.$$

Now $z = 1/R$ and in 3.25 $|\phi| \leqslant c = O(R^{1/4})$. Therefore $|z|\,|\phi|^3 = O(R^{-1/4}) \to 0$ as $R \to \infty$. Hence for sufficiently large R, $M \geqslant \frac{1}{2}$. Thus one can say

3.36 $$\left|\sum_{m=s}^{\infty} \psi_m(\phi)\, z^m\right| \leqslant P_s(|\phi|)|z|^s,$$

where $P_s(|\phi|)$ is a polynomial in $|\phi|$. From 3.25

3.37 $$|R_s| \leqslant \left(\int_{-c}^{c} e^{-\phi^2} P_s(|\phi|)\, d\phi\right)|z|^s \leqslant \int_{-\infty}^{\infty} e^{-\phi^2} P_s(|\phi|)\, d\phi\, |z|^s.$$

Since the integral exists for each fixed s we must have

3.38 $$|R_s| = O(|z|^s)$$

for a fixed s. This completes the proof of the theorem. Hence, an asymptotic expansion of T_n is given by

3.39 $$T_n \sim \frac{n!\, e^{R+\frac{1}{2}R^2}}{2\pi R^n (R^2 + \frac{1}{2}R)^{\frac{1}{2}}}\left[\sum_{m=0}^{\infty} \frac{\int_{-\infty}^{\infty} e^{-\phi^2}\psi_m(\phi)\, d\phi}{R^m}\right]$$

where $R^2 + R - n = 0$.

We have used 3.39 to show that up to and including terms of the order $1/n$

3.40 $$T_n \sim \frac{1}{2^{\frac{1}{2}} e^{1/4}}\left(\frac{n}{e}\right)^{\frac{1}{2}n} e^{n^{\frac{1}{2}}}\left(1 + \frac{7}{24\sqrt{n}} - \frac{119}{1152n} + \ldots.\right)$$

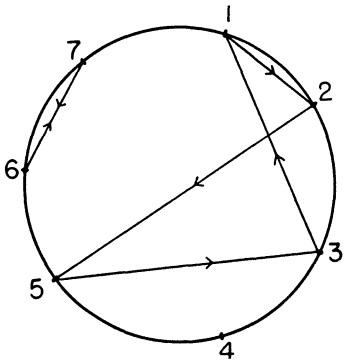
Numerically T_{100} is given by 3.39 to be $2.40537\ldots \times 10^{82}$. Correct to six significant figures $T_{100} = 2.40533\ldots \times 10^{82}$.

The method outlined here can be easily generalized, and can be used to find an asymptotic expansion for $A_{n,d}$. For example, the first term of the asymptotic expansion of $A_{n,p}$ is given by

3.41 $$A_{n,p} \sim p^{-\frac{1}{2}}\left(\frac{n}{e}\right)^{n(1-1/p)} e^{n^{1/p}}, \qquad p > 2.$$

https://doi.org/10.4153/CJM-1955-021-8 Published online by Cambridge University Press

4. Arithmetic properties of $A_{n,d}$. Let a permutation x, on n letters, be represented as a product of disjoint cycles. It will also be convenient to represent x by a diagram in the following way: Let a unit circle have n equi-spaced points on its circumference, labelled $1, 2, \ldots, n$. If x takes i into j, join i and j by a directed line segment. Thus a permutation x will be represented by a circle and a set of directed inscribed polygons. For example, the permutation (1253)(4)(67) corresponds to Figure 1.



A rotation of the circle through $2\pi m/n$ $(m = 1, 2, \ldots n-1)$ leaving the labels fixed will, in general, yield a new permutation having the same order as the old one. If $n = p$, p a prime, the only diagrams left unaltered by a rotation of the form mentioned above will be those corresponding to either the unit permutation I, or the regular directed p-gons, of which there are $p - 1$. We now use these concepts to prove

4.1 $$A_{p,d} \equiv 1 \pmod{p}, d \not\equiv p, \qquad A_{p,p} \equiv 0 \pmod{p}.$$

Since $A_{p,p}$ is easily seen to be $(p-1)! + 1$, the result may be viewed as still another generalization of Wilson's theorem.

Proof. Suppose $x^d = 1$, $d \not\equiv p$. Apart from $x = I$, all solutions (diagrams) must come in sets of p by rotation through $2\pi m/p$, $m = 0, 1, \ldots, p-1$. This proves the first part of 4.1. If $x^p = 1$, then $x = I$ or the diagram for x must consist of a directed p-gon (of which there are $(p-1)!$). If we eliminate the diagram for I, and the $p - 1$ directed regular p-gons, then the remaining $A_{p,p} - p$ diagrams must again come in sets of p, by rotation. Thus the proof is complete.

In **(1)** it was shown that

4.2 $$T_{n+m} \equiv T_n \pmod{m} \qquad m \text{ odd}.$$

We next derive a similar theorem in which m is unrestricted, namely

4.3 $$T_{n+m} \equiv T_n \cdot T_m \pmod{m}.$$

https://doi.org/10.4153/CJM-1955-021-8 Published online by Cambridge University Press

Proof. For $n = 0$ the theorem is trivial and for $n = 1$ it follows immediately from 1.1. Assuming it true for $n < k$ we have

$$T_{k+m} = T_{k+m-1} + (k + m - 1)T_{k+m-2}$$
$$\equiv T_{k-1} \cdot T_m + (k - 1)\, T_{k-2} \cdot T_m = T_k \cdot T_m \pmod{m}.$$

5. The alternating group. Let $B_{n,d}$ denote the number of solutions of $x^d = 1$ in the alternating group on n letters. Further, let $B_{n,2} = U_n$. Define V_n and W_n by

5.1 $$U_n + V_n = T_n, \quad U_n - V_n = W_n.$$

To study U_n it clearly suffices to consider W_n. The analogue of 1.1 is given by

5.2 $$W_n = W_{n-1} - (n - 1)W_{n-2}, \qquad W_0 = W_1 = 1.$$

Proof. The only elements of order two in the alternating group on n letters are those which are the product of an even number of disjoint transpositions and the unit element. Hence the number of even elements of order two which can be obtained from the permutations of the digits $1, 2, \ldots, n - 1$ alone is U_{n-1}. Further, since a single transposition is odd, the only other such elements are obtained by involving the digit n in a transposition with some other digit, and multiplying by any other *odd* permutation of order two, involving the remaining $n - 2$ digits. Their number is clearly $(n - 1)\, V_{n-2}$. Thus

5.3 $$U_n = U_{n-1} + (n - 1)\, V_{n-2}.$$

Similarly we obtain

5.4 $$V_n = V_{n-1} + (n - 1)\, U_{n-2}.$$

Subtracting 5.4 from 5.3 yields 5.2.

Following the lines of the proof of 1.3 given in **(1)** we easily obtain

5.5 $$\sum_{n=0}^{\infty} W_n x^n/n! = e^{x-\frac{1}{2}x^2}.$$

The analogue of 2.2 is given by

5.6 $$W_n = \frac{H_n(1/2^{\frac{1}{2}})}{2^{\frac{1}{2}n}}.$$

Since the proof is essentially the same as that of 2.2 we omit it. The well-known explicit formula for $H_n(x)$ yields the following analogue of 1.4:

5.7 $$W_n = n! \sum_{j=0}^{[\frac{1}{2}n]} (-1)^j/2^j j!(n - 2j)!.$$

Combining 1.3 and 5.7 yields

5.8 $$U_n = n! \sum_{k=0}^{[n/4]} 1/\{4^k(2k)!(n - 4k)!\}.$$

https://doi.org/10.4153/CJM-1955-021-8 Published online by Cambridge University Press

From the asymptotic formula for $H_n(x)$ and 5.6 we obtain

5.9 $$W_n \sim (n/e)^{\frac{1}{2}n}\, 2^{\frac{1}{2}}\, e^{1/4} \cos\{(n+\tfrac{1}{2})^{\frac{1}{2}} - \tfrac{1}{2}n\pi\}.$$

The arithmetic properties of T_n and $A_{n,d}$ also have direct analogues. Thus we obtain without difficulty,

5.10 $$B_{p,d} \equiv 1 \pmod{p},\ d \neq p, \qquad B_{p,p} = A_{p,p}.$$

Finally, the analogue of 4.3 is given by

5.11 $$W_{n+m} \equiv W_n \,.\, W_m \pmod{m}.$$

The following is a short table of T_n, U_n, W_n.

n	T_n	U_n	W_n
0	1	1	1
1	1	1	1
2	2	1	0
3	4	1	−2
4	10	4	−2
5	26	16	6
6	76	46	16
7	232	106	−20
8	764	281	−132
9	2620	1324	28
10	9496	5356	1216

In concluding we wish to thank F. L. Miksa for computing for us the exact values of T_n up to and including T_{152}. These values have been of value to us in checking different forms of our asymptotic formulae.

References

1. S. Chowla, I. N. Herstein, and K. Moore, *On recursions connected with symmetric groups* I, Can. J. Math. *3* (1951), 328–334.
2. S. Chowla, I. N. Herstein, and W. R. Scott, *The solutions of* $x^d = 1$ *in symmetric groups*, Norske Vid. Selsk., *25* (1952), 29–31.
3. E. Jacobsthal, *Sur le nombre d'elements du group symetrique* S_n *dont l'ordre est un nombre premier*, Norske Vid. Selsk., *21* (1949), 49–51.
4. G. Szegö, *Orthogonal Polynomials*, Amer. Math. Soc. Coll. publications (New York, 1939).

Research Institute, Canadian Mathematical Congress
and
University of Alberta