SORTING NUMBERS FOR CYLINDERS AND OTHER CLASSIFICATION NUMBERS

THEODORE S. MOTZKIN[1]

0. **Introduction.** Set partitions (corresponding to equivalence relations) are in the following called sortings. Catalan [**3**, pp. 22–23] expressed in 1865 Stirling numbers of the second kind and their sums (now also called Bell-Stirling numbers) as numbers (i.e., cardinals of sets) of sortings. The umbral generating function of these sums, namely e^{e^z-1}, and its coefficients were mentioned in a different context by Boole [**2**, pp. 27, 245] in 1860. (For further references see [**4**] and [**10**].)

When of all sortings obtained from each other by a permutation of the sorted set S only one is counted then the sorting numbers become (arithmetical) partition numbers. As an intermediate step one can use only those permutations that belong to a given subgroup G of the symmetric group on S. We study the two cases where S is a direct product S_1S_2 and G is induced either by the powers of a cyclic permutation of one factor S_1 or by the symmetric group of S_1. In the first case it is natural to call the structure (S, G) a *cylinder*.

Together with sortings we consider similar structures where the sets are replaced by lists (indexed sets), and other classifications. These are structures—i.e., sets (or lists) of sets (or lists) of sets (or lists) etc. (finitely many times) of elements which *pave* a set S, that is, cover *and* pack S. A structure T *covers* S if every element of S occurs *at least* once in T; while if every element of S occurs *at most* once, and if no element outside S occurs, then T is a *packing* (the lists are nonrepetitive and the lists and sets are disjoint).

For numbers of structures so defined we obtain in §§4–7 recurrences, generating functions, values and congruence properties. Many of these results (even for ordinary sorting numbers) are new. Some proofs are omitted or condensed. §§1–3 help systematize the notation.

1. **Mappings.** Let L, M, N be finite, possibly empty sets, with cardinals $|L|=l$, $|M|=m$, $|N|=n$. Let

MN be the direct product of M and N,
L^N the set of mappings from N into L (N-*lists in* L), including as subsets

[1] This work was supported in part by NSF Grant 14026.

Copyright © 1971, American Mathematical Society

$L^N_<$ (in-valence ≤ 1 on L) the set of injections (*N-ads in L*),
$L^N_>$ the set of surjections (*N-lists on L*),
$L^N_=$ the set of bijections,
$M! = M^M_=$ the set of permutations of M.

In analogy to $|MN| = mn$, $|L^N| = l^n$, $|M!| = m!$ we define

$$l^n_> = |L^N_>|, \qquad l^n_< = |L^N_<| = \binom{l}{n} n!,$$

and similarly in the sequel. Since

$$l^n_> = 0 \quad \text{for } l > n \qquad \text{and} \qquad l^n_< = 0 \quad \text{for } n > l,$$

the sums

$$\sum_l l^n_> \qquad \text{and} \qquad \sum_n l^n_<$$

are finite; such sums will be abbreviated to

$$\Sigma^n_> \qquad \text{and} \qquad l^\Sigma_<,$$

and their largest terms to

$$\max{}^n_> \qquad \text{and} \qquad l^{\max}_< = l!.$$

Deemphasizing the individuality of N, the sets $L^N, L^N_<, L^N_>, L^N_=$ can be regarded as sets of lists of elements of L (*n-lists in L*, *n-ads in L*, etc.) and denoted L^n, $L^n_<$, $L^n_>$, $L^n_=$.

2. **Symmetric merging and subgroupwise merging.** If we merge (identify, collect into equivalence classes) those mappings that are obtained from each other by a permutation of N we replace, in the above notations, N by $!N$ and n by $!n$; similarly for L.

The set $L^{!n}_<$, also denoted $\binom{L}{n}$, is the set of sets of n elements of L (*n-sets in L*), and $L^{!n}$ is the set of *n-tuples in L* (the sum of the "multiplicities" of the elements is n). We have

$$l^{!n} = \binom{l+n-1}{n}, \qquad l^{!n}_< = l^n_</n! = \binom{l}{n},$$

$$l^{!n}_> = \binom{n-1}{l-1}, \qquad l^{!n}_= = \delta_{l,n},$$

and the largest term of $l^{!\Sigma}_< = 2^l$ is $l^{!\max}_< = \binom{l}{[l/2]}$.

If, for merging of mappings, we use a subgroup G of $N!$ we replace, in the notations, $!N$ by ${}^GN$, $!n$ by ${}^Gn$. If G is the group N_{cy} generated by a cyclic permutation of N we write ${}^{cy}N$ for ${}^GN$ and ${}^{cy}n$ for ${}^Gn$.

If only those mappings are admitted that are *invariant* under (every member of) G we write ${}^{\underline{G}}N$ and ${}^{\underline{G}}n$.

3. **Classifications.** Deemphasizing the individuality of L, the set $L^N_>$ becomes $l^N_>$, the set of *listed sortings* of N into l nonempty disjoint classes. While its members are l-ads of sets, those of $!l^N_>$ are l-sets of sets, namely *sortings* of N. We have

$$!l^n_> = l^n_>/l!;$$

$!l^n_>$ is the Stirling number of second kind for n and l.

The members of $!l^{!N}_>$ and $l^{!N}_>$ are respectively sets of cardinals and lists of cardinals, namely *partitions* of n and *listed partitions* (compositions) of n into l nonzero terms, and correspond to the isomorphism classes of sortings and listed sortings. For results on the "cyclic" compositions or partitions ${}^{cy}l^{!N}_>$ and related concepts see [9].

Summing over $\lambda = 0, \ldots, l$ we have

$$!l^{!n} = \sum_{\lambda \leq l} !\lambda^{!n}_>, \qquad !l^n = \sum_{\lambda \leq l} !\lambda^n_>.$$

For $\lambda > n$ the terms are 0; the sums become, for $l \geq n$, independent of l and will be denoted by

$$!^{!n} = !\Sigma^{!n}_> \qquad \text{and} \qquad !^n = !\Sigma^n_>,$$

respectively the partition number and the sorting number (Bell-Stirling number) of n. Their largest terms are

$$!\max{}^{!n}_> \qquad \text{and} \qquad !\max{}^n_>.$$

The set $l^{N+}_>$ of l-ads of nonempty disjoint ads exhausting N and the set $!l^{N+}_>$ of l-sets of such ads cannot be obtained from L^N by subset formation and merging. If we admit empty ads we omit the $>$ sign; again we have

$$!l^{n+} = \sum_{\lambda \leq l} !\lambda^{n+}_>, \qquad l^{n+} = \sum_{\lambda \leq l} \lambda^{n+}_>,$$

and denote $!l^{n+}$, $l \geq n$, and its largest term by

$$!^{n+} = !\Sigma^{n+}_> \qquad \text{and} \qquad !\max{}^{n+}_>.$$

From $l^{n+}_> = l^{!n}_> n!$ follows for $n \geq 1$

$$\Sigma^{n+}_> = \Sigma^{!n}_n \, n! = 2^{n-1} n!,$$

$$\max{}^{n+}_> = \max{}^{!n}_> \, n! = \binom{n-1}{[(n-1)/2]} n!.$$

If every class of a sorting of N is divided into subclasses, we have an example of a *3-level classification* of N (levels 0, 1, 2, 3 are the elements, subclasses, classes and the union or set of the classes). The members of $\Sigma^{N+}_>$, $\Sigma^N_>$, $!^{N+}$, $!^N$ are various kinds of 2-level classifications of N, N itself and its permutations are 1-level classifications. A classification is *setwise* if it is obtained only by set formation, e.g., a sorting.

A classification of N is *proper* if a class with only one subclass can only have one subsubclass, and if, for $n>1$, not every 1-level class has only one element. The number of proper setwise classifications of N is finite and will be denoted by h_n.

4. **Sortings of a product.** Among numbers connected with mappings from a product MN we mention

$$(1)\qquad !\,l^{!m\cdot n},\qquad !\,l^{\mathrm{cy}m\cdot n},\qquad !\,l^{\underline{!}m\cdot n},\qquad !\,l^{\underline{\mathrm{cy}}m\cdot n}.$$

For $l\geq mn$ they are independent of l and can be denoted by

$$!^{!m\cdot n},\qquad !^{\mathrm{cy}m\cdot n},\qquad !^{\underline{!}m\cdot n},\qquad !^{\underline{\mathrm{cy}}m\cdot n}.$$

Some of these latter combinatorial functions arise in the study of the number of identities in semigroups.

For $m=1$ the numbers in (1) become $!\,l^n$. For $m=2$ still $M\,!=M_{\mathrm{cy}}$, and

$$!\,l^{!2\cdot n} = \tfrac{1}{2}(!\,l^{2n}+!\,l^{\underline{!}2\cdot n}).$$

For $m\geq 3$, each class in a member of $!\,l^{\underline{!}M\cdot N}$ is easily seen to be either MN_1, $N_1\subset N$, or $\{\mu\}N_2$, $\mu\in M$, $N_2\subset N$, and in the latter case the N_2 are the same for all $\mu\in M$. Thus the number of sortings does not depend on m, and

$$!\,l_{>}^{\underline{!}m\cdot n}{}_{m\geq 3} = !\,l_{>}^{\underline{!}n} = \sum_{\lambda\leq l;\,\nu\leq n}\binom{n}{\nu}\,!\,\lambda_{>}^{\nu}\ !(l-\lambda)_{>}^{n-\nu}.$$

By summation over l we obtain

$$!^{\underline{!}m\cdot n}{}_{m\geq 3} = !^{\underline{!}\cdot n} = \sum_{\nu\leq n}\binom{n}{\nu}\ !^{\nu}\ !^{n-\nu}.$$

For prime m, each class in a member of $!\,l^{\underline{\mathrm{cy}}M\cdot N}$ is easily seen to be either

$$MN_1,\qquad N_1\subset N,$$

or a member of

$$M^{N_2},\qquad N_2\subset N,$$

and in the latter case its cyclic transforms pave MN_2.

5. **Recurrences.** From the combinatorial definitions one obtains easily

$$(2)\qquad n_{<}^{\Sigma} = n(n-1)_{<}^{\Sigma}+1,\qquad n\geq 1,$$

$$(3)\qquad 2\,\Sigma_{>}^{n} = (1+\Sigma_{>}^{|})^n,\qquad n\geq 1,$$

$$(4)\qquad !^{n+1} = (1\,+\,!^{|})^n,\qquad n\geq 0,$$

$$(5)\qquad !^{\underline{!}\cdot(n+1)} = 2(1+!^{\underline{!}\cdot|})^n,\qquad n\geq 0,$$

$$(6)\qquad !^{\underline{\mathrm{cy}}p\cdot(n+1)} = (1+!^{\underline{\mathrm{cy}}p\cdot|})^n+(p+!^{\underline{\mathrm{cy}}p\cdot|})^n,\qquad n\geq 0,\ p\text{ prime},$$

$$(7)\qquad h_{n+1} = 2\sum_{0}^{n-1}\binom{n}{\nu}h_{n-\nu}h_{\nu+1}-nh_1h_n,\quad n\geq 1,$$

where $^{|}$ is the vicarious exponentiation recipient; e.g., $(1+!^{|})^2=1+2\,!^1+!^2$. (Compare also $b_n=(1+b_{|})^n$, $n\geq 2$, for the Bernoulli numbers.)

From the recurrence

$$!^{(n+1)+} = \sum_{0}^{n}\binom{n}{\nu}(\nu+1)!\ !^{(n-\nu)+}$$

and the same expansion for $!^{n+}$ we deduce

$$!^{(n+1)+}-n\,!^{n+} = !^{n+}+\sum_{1}^{n} n\cdot\cdots\cdot(n-\nu+1)\ !^{(n-\nu)+}$$

and then similarly

$$(!^{(n+1)+}-(n+1)\,!^{n+})-n(!^{n+}-n\,!^{(n-1)+}) = n\,!^{(n-1)+};$$

hence the simpler recurrence

$$(8)\qquad !^{(n+1)+} = (2n+1)\,!^{n+}-(n^2-n)\,!^{(n-1)+},\qquad n\geq 1.$$

6. **Generating functions.** The umbral (exponential) generating functions

$$(2')\qquad w = \sum n_{<}^{\Sigma}z^n/n! = e^z/(1-z),\qquad |z|<1,\qquad (1-z)w' = (2-z)w,$$

$$(3')\qquad w = \sum\Sigma_{>}^{n}\,z^n/n! = 1/(2-e^z),\qquad |z|<\log 2,\qquad w' = 2w^2-w,$$

$$(4')\qquad w = \sum !^n z^n/n! = e^{e^z-1},\qquad |z|<\infty,\qquad w' = e^z w,\ w''w = w'(w'+w),$$

$$(5')\qquad w = \sum !^{\underline{!}\cdot n}z^n/n! = e^{2(e^z-1)},\qquad |z|<\infty,\qquad w' = 2e^z w,\ w''w = w'(w'+w),$$

$$(6')\qquad \begin{aligned} w &= \sum !^{\underline{\mathrm{cy}}p\cdot n}z^n/n! = e^{e^z-1+(e^{pz}-1)/p},\qquad |z|<\infty,\\ w' &= w(e^z+e^{pz}),\quad (w'^2+pw'w-w''w)^p = (p-1)^{p-1}(w''w-w'^2-w'w)w^{2p-2},\\ w'''w^2 &= 3w''w'w+(p+1)w''w^2-2w'^3-(p+1)w'^2w-pw'w^2,\end{aligned}$$

$$(7')\qquad w = \sum h_n z^n/n!,\qquad z = 2w-1-e^{w-1},\ |z|<\log 4-1,\qquad (z+3)w' = 2w'w+1,$$

$$(8')\qquad w = \sum !^{n+}z^n/n! = e^{z/(1-z)},\qquad |z|<1,\qquad (1-z)^2w' = w,$$

are obtained from the corresponding recurrences, via the first-order differential equations with initial value $w(0) = 1$.

Formula (6′) defines w for every complex p. In particular,

$$w = e^{e^z-1+z} = (e^{e^z-1})' = \sum !^{n+1}z^n/n!\quad\text{for } p = 0,$$

$$w\to e^{e^z-1}\quad\text{for } p\to-\infty \text{ and } \operatorname{Re} z\geq 0.$$

The coefficients of w are polynomials in p (see §7) and are, for $n>0$, smaller than $!^{\underline{\mathrm{cy}}p\cdot n}$ when p is composite.

It can be shown that if an umbral series w generates the numbers of classifications of a certain level, then those of the next higher level are generated by e^{w-1} if the new classifications consist of sets of old ones, and by $1/(2-w)$ if they consist of lists (ads).

7. **Values.** The relative size of numbers of lists or sets is apparent from the following table where packing is, but covering is not assumed.

elements	n	0	1	2	3	4	5	For further values or references see
lists	$n^{!\Sigma}_{<}$ (from (2))	1	2	5	16	65	326	[11]
	$n^{!\max}_{<}=n!$	1	1	2	6	24	120	[1, pp. 272–273]; [11]
sets	$n^{!\Sigma}_{<}=2^n$	1	2	4	8	16	32	see below
	$n^{!\max}_{<}=\binom{n}{[n/2]}$	1	1	2	3	6	10	see below

For level 2: numbers of lists (or sets) of lists (or sets or numbers) we reassume covering, and obtain by inspection (i.e., without machines) and use of recurrences

	n	0	1	2	3	4	5	6	7	8	9	For further values or references see
lists of lists	$\Sigma^{n+}=2^{n-1}n!$	1	1	4	24	192	1920	23040	322560	5160960	92897280	
	$\max^{n+}_{>}=\binom{n-1}{[(n-1)/2]}n!$	1	1	2	12	72	720	7200	100800	1411200	24501600	
sets of lists	$!\Sigma^{n+}_{>}=!^{n+}$ (from (8))	1	1	3	13	73	501	4051	37633	394353	4596553	[11]
	$!\max^{n+}_{>}$	1	1	2	6	36	240	1800	15120	141120	1693440	
lists of sets	$\Sigma^{n}_{>}$ (from (3))	1	1	3	13	75	541	4683	47293	595835	7088261	[11]
	$\max^{n}_{>}$	1	1	2	6	36	240	1800	16800	191520	2328480	
sets of sets	$!\Sigma^{n}_{>}=!^n$ (from (4))	1	1	2	5	15	52	203	877	4140	21147	**; [11]
	$!\max^{n}_{>}$	1	1	1	3	7	25	90	350	1701	7770	***; [1, p. 835]
lists of numbers	$\Sigma^{!n}_{>}=2^{n-1}$	1	1	2	4	8	16	32	64	128	256	[1, pp. 24–44]; [11]
	$\max^{!n}_{>}=\binom{n-1}{[(n-1)/2]}$	1	1	1	2	3	6	10	20	35	70	[1, pp. 828–830]; [11, 1 2 6 20]
sets of numbers	$!\Sigma^{!n}=!^{!n}$	1	1	2	3	5	7	11	15	22	30	[1, pp. 836–839]; [11]
	$!\max^{!n}_{>}$	1	1	1	1	2	2	3	4	5	6	*

* continued 9 11 15 18 23 30 37 47 58 71 90.

** The values of $!^n$ for $n \leq 51$ are given in [8]. I have the values for $n \leq 200$, obtained (with help from D. Cantor and A. Fraenkel), in 16 sec., by the IBM 360/91 at the UCLA Computing Facility. We give here 4 values to 8 figures:

$$!^{50} = .18572426\ldots\cdot 10^{48},$$
$$!^{100} = .47585391\ldots\cdot 10^{116},$$
$$!^{150} = .68206412\ldots\cdot 10^{193},$$
$$!^{200} = .62474847\ldots\cdot 10^{276}.$$

By [8], $!^n$ is asymptotic to

$$\exp\left(((\log \nu)^2 - \log \nu + 1)\nu - \tfrac{1}{2}\log\log\nu - 1\right) = \nu^n e^{\nu-n-1}/\sqrt{\log n}$$

where $\nu \log \nu = n$. A better approximation seems to be

$$\mu_n = \nu^n e^{\nu-n-1}\left(\frac{n}{\nu}+1\right)^{-1/2}\left(1-\frac{n(2n^2+7n\nu+10\nu^2)}{24\nu(n+\nu)^3}\right),$$

given in [8] without error term or indication of the way in which it might be superior to other asymptotic expressions. Setting $!^n = \mu_n(1-\lambda_n/n)$ we find

$$\lambda_{50} = .0015\ldots,$$
$$\lambda_{100} = .0008\ldots,$$
$$\lambda_{150} = .0006\ldots,$$
$$\lambda_{200} = .0004\ldots.$$

*** By [7], p. 413 last line (at whose end an exponent 1/2 should be appended) and p. 412, line 17 (both only with hints to proofs), $!\max^{n}_{>}$ is asymptotic to

$$\exp\left(((\log \nu)^2 - \log \nu + 1)\nu - \tfrac{1}{2}\log \nu - 1 - \tfrac{1}{2}\log 2\pi\right) = \nu^{n-1/2}e^{\nu-n-1}/\sqrt{2\pi}.$$

Similarly we obtain these numbers of certain sets of subsets of direct products:

n	0	1	2	3	4	5	6	7	8	9
$!^{!\cdot n}$	1	2	6	22	94	454	2430	14214	89918	
$!\max^{!\cdot n}_{>}$	1	2	4	12	48	200	1040	5600	33600	
$!^{!2\cdot n}$	1	2	7	31	164	999	6841	51790	428131	3929021
$!\max^{!2\cdot n}_{>}$	1	1	3	10	53	265	1700			
$!^{\mathrm{cy}3\cdot n}$	1	2	8	42	268	1994	16852			
$!\max^{\mathrm{cy}3\cdot n}_{>}$	1	2	4	24	128	880	7440			

For prime p, $!^{\mathrm{cy}p\cdot n}_{>}$ is a polynomial in p of degree $n-1$ (for $n>0$). The sequence of these polynomials starts

$$1$$
$$2$$
$$5+p$$
$$15+6p+p^2$$
$$52+30p+11p^2+p^3$$
$$203+150p+80p^2+20p^3+p^4$$
$$877+780p+525p^2+190p^3+37p^4+p^5$$

Finally, for classifications of unbounded level we find

									For further values or references see
h_n	1	1	1	4	26	236	2752	39208	[11]

8. **Congruence properties.** While the linear recurrence (4) for $!^n$ is not of bounded degree, $!^n$ mod a prime p fulfills the linear recurrence

$$!^{n+p} \underset{p}{=} !^n + !^{n+1} \tag{9}$$

of degree p and with constant coefficients [6]. A combinatorial proof of (9) is the, by far simplest, case $t=1$ of the proof of (10).

From (9) follows, first letting $n=0$, then using (4) for $n=p-1$,

$$!^p \underset{p}{=} 2, \qquad \sum_{2}^{p-1} (-1)^k \, !^k \underset{p}{=} 2.$$

The recurrence (9) holds also for α^n if $\alpha^p=\alpha+1$. In the field $\mathrm{GF}(p^p)$, the characteristic polynomial $g(x)=x^p-x-1$ has p roots $\alpha_k=\alpha_p+k$, no proper subset of which has its sum in the prime field $\mathrm{GF}(p)$, over which $g(x)$ is therefore irreducible. The α_k^n are the p fundamental solutions of (9); the linear combination that represents $!^n$ can be shown to be

$$!^n \underset{p}{=} \sum f(\alpha_k)\alpha_k^n, \qquad f(x) = x^p - \sum_{0}^{p} !^j x^j.$$

Since $\alpha_k^{p^j}=\alpha_k+j$ we have $\alpha_k^{p'}=1$ where

$$p' = 1+p+\cdots+p^{p-1} = (p^p-1)/(p-1);$$

hence

$$!^{n+p'} \underset{p}{=} !^n.$$

It is unknown where $!^n$ mod p can have a smaller period. The prime decompositions of the first values of p' are, according to J. L. Selfridge,

2	3
3	13
5	$11\cdot 71$
7	$29\cdot 4733$
11	$15797\cdot 1806113$
13	$53\cdot 264031\cdot 1803647$
17	$10949\cdot 1749233\cdot 2699538733$

For $!^n$ mod p^t, $t\geq 1$, we prove the linear recurrence

$$!^{n+p^t} \underset{p^t}{=} \sum_{0}^{p^{t-1}} s_{p^{t-1}-j}(p)\binom{p^{t-1}}{j} \, !^{n+j}, \tag{10}$$

of degree p^t with constant coefficients; $s_\lambda(x)$ denotes the *sorting polynomial* $\sum !(\lambda-k)^{\lambda}_{>} x^k$. Indeed consider the set $N+P^t$, $|P|=p$ (+ means disjoint union) and a cyclic permutation τ of P^t, acting indirectly on an arbitrary sorting σ of $N+P^t$. The list

$$\sigma, \sigma\tau, \ldots, \sigma\tau^{p^t-1}$$

has no repetitions unless $\sigma\hat{\tau}=\sigma$ where $\hat{\tau}=\tau^{p^{t-1}}$. If $\sigma\hat{\tau}=\sigma$ then, for each element π of P^t, either

$$\pi, \pi\hat{\tau}, \ldots, \pi\hat{\tau}^{p-1} \tag{11}$$

belong to the same class in σ (case I) or they belong to p different classes (case II); the latter contain no element of N nor any case I-element. Finally it is easily seen that the number of sortings of $N+P^t$ for which exactly j of the p-sets (11) belong to case I ($j=0, \ldots, p^{t-1}$) is

$$s_{p^{t-1}-j}(p)\binom{p^{t-1}}{j} \, !^{n+j}.$$

For $j \neq_p 0$ we have $\binom{p^{t-1}}{j} =_{p^{t-1}} 0$, hence $s_{p^{t-1}-j}(p)$ in (10) can then be replaced by its constant coefficient 1. For $j =_p 0$, $\neq_{p^2} 0$ we have $\binom{p^{t-1}}{j} =_{p^{t-2}} 0$, but

$$s_{p^{t-1}-j}(p) \underset{p^2}{=} \binom{p^{t-1}-j}{2}p+1 \underset{p^2}{=} 1+0^{p-2}\cdot 2 \quad (\text{unless } p=t=j=2),$$

where $0^0=1$; thus $s_{p^{t-1}-j}(p)$ in (10) can be replaced by $1+0^{p-2}\cdot 2$. There follows in particular

$$!^{n+p^2} \underset{p^2}{=} \sum_{0}^{p} \binom{p}{j} \, !^{n+j} + 0^{p-2}\cdot 2 \, !^n.$$

For $p>2$ this can be written

$$!^{n+p^2} \underset{p^2}{=} (1+!^{n+1})^p.$$

A more detailed analysis shows that for every $t\geq 1$ and prime $p>2$ we have

$$!^{n+p^t} \underset{p^t}{=} (1+!^{n+1})^{p^{t-1}}. \tag{12}$$

Setting $n=0$ we obtain

$$!^{p^t} \underset{p^t}{=} !^{p^{t-1}+1}.$$

The characteristic polynomial of the recurrence (10) is

$$x^{p^t} - \sum s_{p^{t-1}-j}(p)\binom{p^{t-1}}{j}x^j.$$

For $p\neq 2$ we can replace it by

$$x^{p^t}-(x+1)^{p^{t-1}}.$$

For $t=2$, $p=2$ the characteristic polynomial is x^4-x^2-2x-3.

A similar (and simpler) proof than that of (10) shows that

$$!^{\underline{\mathrm{cy}2}\cdot(n+p)} \underset{p}{=} (2-0^{p-2}) \, !^{\underline{\mathrm{cy}2}\cdot n} + !^{\underline{\mathrm{cy}2}\cdot(n+1)}.$$

For $p>2$ the corresponding polynomial is $x^p-x-2 =_p 2g(x/2)$, and p' is again a period.

It follows from the fact that the highest and lowest coefficients of the recurrence (10) are $\neq_p 0$ that $!^n$ is periodic, without preperiod, for p^t and hence for every modulus m, and that the period is $\leq m^\mu$, where μ is the largest prime power dividing m. The periodicity, with possible preperiods, follows also from (4′) and Fujiwara's theorem [5] on the umbral coefficients (if integer) of solutions $w = \sum a_n z^n/n!$ of algebraic differential equations

$$F(z, w, w', \ldots, w^{(d)}) = 0$$

with integer coefficients for which

$$\frac{\partial F}{\partial w^{(d)}}(0, a_0, a_1, \ldots, a_d) = 1.$$

By the same theorem, modular periodicity holds also for the coefficients

$$n^{\Sigma}_{<}, \quad \textstyle\sum^{n}_{>}, \quad !^{\underline{!}\cdot n}, \quad !^{\underline{\mathrm{cy}}\,p\cdot n}, \quad h_n, \quad !^{n+}$$

in (2′), (3′), (5′), (6′), (7′), (8′).

References

1. M. Abramowitz and I. A. Stegun (Editors), *Handbook of mathematical functions, with formulas, graphs and mathematical tables*, Nat. Bur. Standards Appl. Math. Series, 55, Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964; 3rd printing with corrections, 1965. MR **29** #4914; MR **31** #1400.
2. George Boole, *A treatise on the calculus of differences*, Cambridge, 1860.
3. Eugène Catalan, *Mélanges mathématiques*. I, Mém. Soc. Sci. Liège II **12** (1885).
4. H. C. Finlayson, *Numbers generated by* e^{e^x-1}, Masters Thesis, University of Alberta, 1954.
5. M. Fujiwara, *Periodizität der Entwicklungskoeffizienten einer analytischen Funktion nach dem Modul m*, Tôhoku Math. J. **2** (1912), 57–73.
6. Marshall Hall, *Arithmetic properties of a partition function*, Bull. Amer. Math. Soc. **40** (1934) 387. Abstract #200.
7. L. H. Harper, *Stirling behavior is asymptotically normal*, Ann. Math. Statist. **38** (1967), 410–414. MR **35** #2312.
8. Leo Moser and Max Wyman, *An asymptotic formula for the Bell numbers*, Trans. Roy. Soc. Canada Sect. III (3) **49** (1955), 49–54. MR **17**, 1201.
9. T. S. Motzkin, *Ordered and cyclic partitions*, Riveon leMatematika **1** (1947), 61–67 (Hebrew). MR **8**, 566.
10. Gian-Carlo Rota, *The number of partitions of a set*, Amer. Math. Monthly **71** (1964) 498–504. MR **28** #5009.
11. N. J. A. Sloane, *A catalog of sequences* (unpublished).

UNIVERSITY OF CALIFORNIA, LOS ANGELES

PATHOLOGICAL LATIN SQUARES

E. T. PARKER

1. The central open question in finite projective planes is whether one exists c order *not* a prime-power. They have been known to exist for every prime-powe order since about the turn of the century. Only one theorem, due to Bruck an Ryser [1], shows nonexistence of finite projective planes of infinitely many order *not* prime-powers, of course. Considerable partially expository literature is availabl such as [2], [3], [4], [5].

A latin square of order n is an n by n array of n symbols each present (only onc in each row and each column. A set of latin squares of like order is called *orthogon* if each pair of distinct members of the set includes all ordered pairs of symbols (onl once) among the n^2 positions. A folk theorem of the 1930 decade asserts th existence of a projective plane of order n (n an integer exceeding 1) implies existenc of a *complete set* (for no larger set can exist) of $n-1$ orthogonal latin squares c order n, and conversely.

The lowest order for which existence of a projective plane (and equivalently complete set of orthogonal latin squares) is undecided is ten. The author [6] an quite recently John W. Brown have found by using digital computers that few (an quite possibly none) of the numerous distinct latin squares of order ten are e tendible to complete sets. Unfortunately for order ten, to say nothing of large orders, the number of nonisomorphic latin squares (after identifying equivalenc by permuting rows, columns, and symbols independently) is astronomical. Wh seems needed is theorems rejecting wide classes of latin squares as possibilities fc inclusion in complete sets. The author knows of only two previously know theorems of this nature: Euler [7] proved this and more for *cyclic* latin squares c *even* orders (except for the rather degenerate order two); Mann [8] proved tw further theorems, in spirit almost a generalization of Euler's. The author in th paper generalizes the fundamental theorem of Euler in another direction.

A latin square not extendible to a complete set will be called *pathological*; thu Euler, Mann, and the author have given sufficient conditions for a latin square t be pathological. While the author is designating these latin squares as pathologica experiments indicate that these constitute the majority for any consequenti order. Metaphorically, many more people are ill than sound, and the task is t

Copyright © 1971, American Mathematical Socie