Europ. J. Combinatorics (1980) **1**, 67–76

Congruences Derived from Group Action

GIAN-CARLO ROTA* AND BRUCE SAGAN

Dedicated to G. Polya, in friendship and admiration.

1. INTRODUCTION

Since the beginning of this century the development of group theory has been dominated by the notion of representation, and the seemingly more specialized theory of group actions (permutations) has been given short shrift. To be sure, every action of a group can be considered as a particular representation by matrices, but in this setting some of the finer structure of the original permutations is lost.

There are signs that the tables may be turning. Topology, ergodic theory, combinatorics and sundry other subjects abound with problems that cannot be dismissed by group characters alone. To name but one instance, the Burnside algebra yields more structural information than the Grothendik ring, as Solomon was first to note [11].

An important problem in combinatorics is to enumerate unlabeled objects, i.e. equivalence classes of "labeled" objects under a group of automorphisms. Since Polya's fundamental paper of 1937 [6], it has been wrongly believed that all the necessary information is given by the cycle index of a permutation group. However, in the same year, Witt's enumeration of the dimensions of free Lie algebras [13] displayed the need for more detailed invariants. The same need arose in Rota's generalization of Spitzer's probabalistic formula [8]. In both these instances the problem is that of enumerating aperiodic elements of a group action (definition below) and this lies beyond the scope of the cycle index.

The idea for the solution of this problem bears a resemblance to Galois theory, an approach first fully presented by Rota and Smith [9]. Whenever a group G acts on a set, one can define certain special subgroups associated with this action which we call periodic subgroups (*vide* below). The periodic subgroups form a lattice, in general smaller than the lattice of all subgroups of G, and this lattice is analogous to the lattice of normal subfields of a field extension. Möbius inversion over the lattice of periods gives an explicit expression for the number of aperiodic functions on the underlying set. One obtains, as a special case, proofs of congruences due to Fermat, Lucas and others.

In this paper we show that similar congruences can be derived for any group of permutations whatsoever (Theorem 3.2 below). We are also led to define an analog of the Euler ϕ function for a general group action and to derive corresponding congruences. We surmise that other number theoretic functions can also be so generalized. Thus it is seen that the lattice of periods may be a useful enumerative invariant of a group action.

2. PRELIMINARIES

In this section we present a sketch of some useful results from a theory of enumeration developed by Rota and Smith. The reader is referred to [9] for a more detailed exposition.

Consider the set $[n]=\{1, 2, \ldots, n\}$ and a group G of permutations of $[n]$, i.e. G is a subgroup of the symmetric group $\mathcal{G}_n$. We will use σ to denote an arbitrary element of G, and for $i\varepsilon[n]$ we will write σi for the image of i under σ.

* Partially supported by NSF Contract No. MCS 78-02743.

0195-6698/80/010067+10$01.00/0

Let Π_n be the lattice of all partitions of $[n]$ (ordered by refinement) and let L_G be the lattice of all subgroups of G (ordered by inclusion). Define a mapping $\eta : L_G \to \Pi_n$ as follows: each subgroup $H \subseteq G$ is mapped to the partition $\pi = \eta(H)$ where $i, j \in [n]$ are in the same block of π if and only if $\sigma i = j$ for some $\sigma \in H$. Also consider the map $\theta : \Pi_n \to L_G$ defined by

$$\theta(\pi) = \{\sigma | i \text{ and } \sigma i \text{ are in the same block of } \pi \text{ for all } i \in [n]\}.$$

It is easy to verify that $\theta(\pi)$ is indeed a subgroup of G.

From these definitions we see that for all subgroups H and partitions π:

$$H \subseteq \theta\eta(H)$$

$$\pi \geqslant \eta\theta(\pi).$$

It follows that we have a *coclosure operator* on Π_n given by $\bar{\pi} = \eta\theta(\pi)$, i.e. the mapping $\pi \to \bar{\pi}$ is idempotent, $\bar{\pi} \leqslant \pi$, and $\pi_1 \leqslant \pi_2$ implies $\bar{\pi}_1 \leqslant \bar{\pi}_2$. We can describe $\bar{\pi}$ as the coarsest partition less than π whose blocks are the orbits of some subgroup of G. The coclosed partitions, called *periods*, form a lattice $\mathcal{P}(G, [n])$; in other words the set $\{\pi \in \Pi_n | \pi = \bar{\pi}\}$ forms a lattice when ordered by refinement. This lattice is fundamental in reflecting the interaction of G with $[n]$.

Now consider functions $f : [n] \to X$ where $X = \{x_1, x_2, \ldots, x_a\}$. The group G acts on these functions by defining

$$(\sigma f)(i) = f(\sigma^{-1} i).$$

The *kernal* of f is the partition $\pi_f = \ker f$ where $i, j \in [n]$ are in the same block of π_f if and only if $f(i) = f(j)$. The coclosure of π_f is called the *G-period* of f in $[n]$ and is denoted

$$\operatorname{per} f = \bar{\pi}_f.$$

Thus per f is the coarsest partition of $[n]$ satisfying the two conditions

(i) the blocks of per f are the orbits of some subgroup of G, and

(ii) f is constant on each block of per f.

We will be particularly concerned with functions whose G-period is $\mathbf{0}$, the minimal element of $\mathcal{P}(G, [n])$. Such functions will be called *aperiodic*. In this regard the following result is important.

PROPOSITION 2.1. *The number of aperiodic functions is divisible by $o(G)$, the order of G.*

PROOF. Let f be aperiodic and consider the set $Gf = \{\sigma f | \sigma \in G\}$. We claim that Gf has $o(G)$ distinct elements. To show this it suffices to prove that $\sigma f \neq f$ for any $\sigma \in G$. But if $\sigma f = f$ then we can consider the partition $\pi = \eta(H)$ where H is the subgroup generated by σ. Clearly $\pi \neq \mathbf{0}$ and $\pi \leqslant \ker f$. Hence $\bar{\pi} \leqslant \operatorname{per} f$ and $\bar{\pi} = \pi \neq \mathbf{0}$ which contradicts the fact that f is aperiodic.

Now we can find aperiodic functions $f_1, f_2, \ldots, f_l$ such that the sets $Gf_1, Gf_2, \ldots, Gf_l$ form a partition of the set of all aperiodic functions. Since each of these sets contain $o(G)$ elements, we are done.

3. Generating Functions

It is convenient to consider the elements $x_1, x_2, \ldots, x_a$ of X as independent indeterminates. Thus for each function $f:[n]\to X$ we can form the monomial

$$M(f)=\prod_{i=1}^{n} f(i)=x_1^{r_1}x_2^{r_2}\ldots x_a^{r_a}$$

where r_i is the number of elements of $[n]$ mapped to x_i by f.

More generally, let $\mathcal{F}$ be any family of functions $f:[n]\to X$ which is *proper* in the sense that if $f\in\mathcal{F}$ and $\sigma\in G$ then $\sigma f\in\mathcal{F}$. Examples of proper families include the family of all functions from $[n]$ to X, the family of all onto functions from $[n]$ to X, etc. For each family we have the generating function

$$M(\mathcal{F})=\sum_{f\in\mathcal{F}} M(f).$$

Now let π be a partition in the lattice of periods $\mathcal{P}(G,[n])$, so $\bar{\pi}=\pi$, and let $\mathcal{F}$ be a proper family. Two generating functions that will play an important role in the sequel are defined by

$$A(\pi)=M(\{f\in\mathcal{F}|\text{per } f=\pi\})$$

and

$$B(\pi)=M(\{f\in\mathcal{F}|\text{per } f\geqslant\pi\}).$$

Note that $A(\mathbf{0})$ enumerates aperiodic functions. Also note that

$$B(\mathbf{0})=\sum_{\pi\in\mathcal{P}(G,[n])} A(\pi). \tag{3.1}$$

To isolate $A(\mathbf{0})$ we must invert the sum (3.1). Let μ be the Möbius function of the lattice $\mathcal{P}(G,[n])$ (an exposition of the theory of Möbius inversion can be found in [7]). Then μ is defined inductively on each $\pi\in\mathcal{P}(G,[n])$ by

$$\mu(\mathbf{0})=1$$
$$\mu(\pi)=-\sum_{\substack{\pi_1<\pi\\ \pi_1\in\mathcal{P}(G,[n])}}\mu(\pi_1)\quad\text{for } \pi>\mathbf{0}.$$

It follows that we can rewrite (3.1) as

$$A(\mathbf{0})=\sum_{\pi\in\mathcal{P}(G,[n])}\mu(\pi)B(\pi).$$

We can now strengthen Proposition 2.1 to:

Theorem 3.2. *For any proper family*

$$\sum_{\pi\in\mathcal{P}(G,[n])}\mu(\pi)B(\pi)\equiv 0(\operatorname{mod} o(G)).$$

Proof. We need to show that the coefficient of each term in the generating functions $A(\mathbf{0})$ is divisible by $o(G)$. If $c\cdot x_1^{r_1}x_2^{r_2}\cdots x_a^{r_a}$ is such a term then c is the number of $f\in\mathcal{F}$ which map r_i of the elements of $[n]$ to x_i. Since $\mathcal{F}$ is proper we have $Gf\subseteq\mathcal{F}$ and it follows from the proof of Proposition 2.1 that $|Gf|=o(G)$. Hence we can partition the functions counted by c into equivalence classes each containing $o(G)$ elements.

In order to utilize Theorem 3.2 to derive other congruences it is useful to give an explicit expression for $B(\pi)$. If π has blocks $B_1, B_2, \ldots, B_r$ then per $f\geqslant\pi$ if and only if f is constant on each B_i. Hence

$$B(\pi)=\prod_{i=1}^{r}\left(x_1^{|B_i|}+x_2^{|B_i|}+\cdots+x_a^{|B_i|}\right) \tag{3.3}$$

when $\mathscr{F}$ is the family of all functions from $[n]$ to X. We will now consider some specific examples.

4. Cyclic Groups

Let C_n be the subgroup of $\mathscr{G}_n$ generated by the cycle $(1, 2, \ldots, n)$. Then the lattice of periods $\mathscr{P}(C_n, [n])$ is isomorphic to the lattice of subgroups of C_n, which is in turn isomorphic to the lattice of divisors of n.

In the simplest case we have $n=p^m$, where p is a prime, so that $\mathscr{P}(C_n, [n])$ is merely a chain. Letting π' be the atom of this chain, we see that the Möbius function takes the values

$$\begin{aligned}&\mu(\mathbf{0})=1\\&\mu(\pi')=-1\\&\mu(\pi)=0 \quad \text{if } \pi>\pi'.\end{aligned}$$

Now π' has blocks $B_1, B_2, \ldots, B_{p^{m-1}}$ where $B_i=\{i, i+p^{m-1}, i+2p^{m-1}, \ldots, i+(p-1)p^{m-1}\}$. Hence we obtain from (3.3) the generating function

$$B(\pi')=(x_1^p+x_2^p+\cdots+x_a^p)^{p^{m-1}}$$

for the proper family of all functions from $[p^m]$ to x. Also $B(\mathbf{0})=(x_1+x_2+\cdots+x_a)^{p^m}$ so Theorem 3.2 becomes

$$\sum_{\pi}\mu(\pi)B(\pi)=(x_1+x_2+\cdots+x_a)^{p^m}-(x_1^p+x_2^p+\cdots+x_a^p)^{p^{m-1}}\equiv 0(\operatorname{mod} p^m). \tag{4.1}$$

Equation (4.1) immediately yields certain congruence properties of multinomial coefficients.

Proposition 4.2

$$\binom{p^m}{i_1, i_2, \ldots, i_a}\equiv\binom{p^{m-1}}{i_1/p, i_2/p, \ldots, i_a/p}(\operatorname{mod} p^m)$$

where by convention a multinomial coefficient containing a non-integral fraction has the value zero.

By repeated application of Proposition 4.2 we obtain

Corollary 4.3. *If the greatest common divisor g.c.d.* $(i_1, i_2, \ldots, i_a, p^m)=p^k$ *then*

$$\begin{aligned}\binom{p^m}{i_1, i_2, \ldots, i_a}&\equiv\binom{p^{m-k}}{i_1/p^k, i_2/p^k, \ldots, i_a/p^k}(\operatorname{mod} p^{m-k+1})\\&\equiv 0(\operatorname{mod} p^{m-k}).\end{aligned}$$

In the case of binomial coefficients, i.e. $a=2$, Corollary 4.3 gives the best possible result. In other words if $p^k=g.c.d.\ (i_1, i_2, p^m)$ then

$$p^{m-k}\left|\binom{p^m}{i_1, i_2}\right. \quad\text{and}\quad p^{m-k+1}\nmid\binom{p^m}{i_1, i_2}$$

(see for example Krummer [5]). However, for larger values of 'a' the power of p dividing $\binom{p^m}{i_1, i_2, \ldots, i_a}$ can easily exceed p^m.

If we now set $x_1 = x_2 = \cdots = x_a = 1$ in (4.1) then the congruence reduces to $a^{p^m} - a^{p^{m-1}} \equiv 0 \pmod{p^m}$ or

PROPOSITION 4.4. $a^{p^m} \equiv a^{p^{m-1}} (\operatorname{mod} p^m)$.

For the special case $m = 1$ we have the well-known result

COROLLARY 4.5 (FERMAT'S THEOREM). $a^p \equiv a (\operatorname{mod} p)$.

We can also obtain Euler's generalization of Corollary 4.5:

COROLLARY 4.6 (EULER). *If g.c.d.* $(a, n) = 1$ *and* $\phi(n) = |\{d : 0 < d < n$ *and g.c.d.* $(d, n) = 1\}|$ *then* $a^{\phi(n)} \equiv 1 (\operatorname{mod} n)$.

PROOF. If $n = \prod_i p_i^{m_i}$ then $\phi(n) = \prod_i (p_i^{m_i} - p_i^{m_i - 1})$. Hence

$$a^{\phi(n)} = a^{\prod_i (p_i^{m_i} - p_i^{m_i-1})} = (a^{p_1^{m_1} - p_1^{m_1-1}})^{\prod_{i \neq 1} (p_i^{m_i} - p_i^{m_i-1})}.$$

It follows that $a^{\phi(n)} \equiv 1 \ (\operatorname{mod} p_1^{m_1})$. Similarly $a^{\phi(n)} \equiv 1 \ (\operatorname{mod} p_i^{m_i})$ for any i, so $a^{\phi(n)} \equiv 1 \ (\operatorname{mod} \prod_i p_i^{m_i})$.

By restricting ourselves to the proper family of onto functions we can obtain congruences for the Stirling numbers of the second kind, $S(n, a)$. Equation (4.1) is replaced by

$$a!S(p^m, a) - a!S(p^{m-1}, a) \equiv 0 \ (\operatorname{mod} p^m)$$

where we are taking $x_1 = x_2 = \cdots = x_a = 1$ in $B(\pi)$.

PROPOSITION 4.7. *If* $k = \lfloor a/p \rfloor$, *the greatest integer* $\leq a/p$, *then*

$$S(p^m, a) \equiv S(p^{m-1}, a) (\operatorname{mod} p^{m-k}).$$

Repeated application of Proposition 4.7 yields:

COROLLARY 4.8. *If* $k = \lfloor a/p \rfloor$ *then*
$S(p^m, a) \equiv S(p^{m-r}, a) \ (\operatorname{mod} p^{m-k-r+1})$. *In particular if* $1 < a < p$ *then* $S(p^m, a) \equiv 0 \ (\operatorname{mod} p)$.

Returning to the lattice $\mathcal{P}(C_n, [n])$ where n is an arbitrary integer, we have a period π_d for each divisor d of n. Furthermore π_d has blocks $B_1, B_2, \ldots, B_{n/d}$ where

$$B_i = \left\{ i, i + \frac{n}{d}, i + 2\frac{n}{d}, \ldots, i + (d-1)\frac{n}{d} \right\}.$$

Hence for the proper family of all functions from $[n]$ to X we have

$$B(\pi_d) = (x_1^d + x_2^d + \cdots + x_a^d)^{n/d}. \tag{4.9}$$

It follows that

$$\sum_{\pi_d} \mu(\pi_d) B(\pi_d) = \sum_{d \mid n} \mu(d)(x_1^d + x_2^d + \cdots + x_a^d)^{n/d} \tag{4.10}$$

where $\mu(d)$ is the classical Möbius function of number theory, i.e.

$\mu(d)=0$ if d is not square free

$\mu(d)=(-1)^k$ if d is the product of k distinct primes.

The following propositions and corollaries are derived from equation (4.10) in much the same way as the preceding results for $n=p^m$. In view of this similarity, their proofs have been omitted.

PROPOSITION 4.11

$$\sum_{d|n}\mu(d)\binom{n/d}{i_1/d,\ldots,i_a/d}\equiv 0(\bmod n).$$

COROLLARY 4.12. *If $g=g.c.d.\,(i_1,\ldots,i_a,n)$ then*

$$\binom{n}{i_1,\ldots,i_a}\equiv 0\left(\bmod \frac{n}{g}\right).$$

COROLLARY 4.13. *If $g.c.d.\,(i_1,\ldots,i_a,n)=p^k$ for some prime p then*

$$\binom{n}{i_1,\ldots,i_a}\equiv\binom{n/p^k}{i_1/p^k,\ldots,i_a/p^k}\left(\bmod \frac{n}{p^{k-1}}\right).$$

PROPOSITION 4.14. $\sum_{d|n}\mu(d)a^{n/d}\equiv 0(\bmod n)$.

PROPOSITION 4.15. $\sum_{d|n}\mu(d)\cdot a!S(n/d,a)\equiv 0(\bmod n)$. *In particular if $a<p$ where p is the smallest prime divisor of n then $\sum_{d|n}\mu(d)\cdot S(n/d,a)\equiv 0(\bmod n)$.*

One consequence of the above results is a strengthening of Lucas' congruence for binomial coefficients, which states that $\binom{ap}{p}\equiv a(\bmod p)$.

COROLLARY 4.16 (GENERALIZED LUCAS' THEOREM)

$$\binom{ap}{p}\equiv a(\bmod ap).$$

PROOF. Since $g.c.d.(p,(a-1)p,ap)=p$, Corollary 4.13 yields

$$\binom{ap}{p}\equiv\binom{a}{1}(\bmod ap).$$

5. THE SYMMETRIC GROUP

If $\mathcal{G}_n$ is the full symmetric group then the lattice of periods $\mathcal{P}(\mathcal{G}_n,[n])$ is just the lattice of all partitions of $[n]$. The Möbius function of this lattice is well known (see [7]): if π is a partition of $[n]$ having r_i blocks of size i, $1\leqslant i\leqslant n$, then

$$\mu(\pi)=\prod_{i=1}^{n}[(-1)^{i-1}(i-1)!]^{r_i}. \tag{5.1}$$

Furthermore the generating function (3.3) becomes

$$B(\pi)=\prod_i (x_1^i+x_2^i+\cdots+x_a^i)^{r_i}$$
$$=a^{r_1+r_2+\cdots+r_n} \tag{5.2}$$

when $x_1=x_2=\cdots x_a=1$.

Associated with each partition π of the set $[n]$ we have a corresponding partition λ of the integer n where r_i parts of λ are equal to i. A convenient notation for such partitions of n is $\lambda\vdash n$ where $\lambda=(1^{r_1},2^{r_2},\ldots,n^{r_n})$.

PROPOSITION 5.3

$$\sum_{\lambda\vdash n}\left[\frac{n!}{\prod_i i^{r_i}\cdot r_i!}(-1)^{r_e}a^r\right]\equiv 0(\text{mod } n!)$$

where

$$\lambda=(1^{r_1},2^{r_2},\ldots,n^{r_n}),\qquad r=\sum_j r_j,\quad \textit{and}\quad r_e=\sum_j r_{2j}.$$

PROOF. If we let π_λ be the number of partitions of $[n]$ associated with a given partition λ of n then

$$\pi_\lambda=\frac{n!}{\prod_i (i!)^{r_i}(r_i!)}. \tag{5.4}$$

Using equations (5.1), (5.2) and (5.4) we have

$$\sum_{\pi\in\mathcal{P}(\mathcal{G}_n,[n])}\mu(\pi)B(\pi)=\sum_{\lambda\vdash n}\pi_\lambda\left[\prod_i(-1)^{i-1}(i-1)!\right]^{r_i}a^r$$
$$=\sum_{\lambda\vdash n}\frac{n!}{\prod_i i^{r_i}r_i!}(-1)^{r_e}a^r$$

where $\sum_{\pi\in\mathcal{P}(\mathcal{G}_n,[n])}\mu(\pi)B(\pi)\equiv 0(\text{mod } o(\mathcal{G}_n))$.

Every permutation $\sigma\in\mathcal{G}_n$ has a unique decomposition into disjoint cycles. If this decomposition has r_i cycles of length i $(1\leq i\leq n)$ we say that σ has type $\lambda=(1^{r_i},2^{r_2},\ldots,n^{r_n})$.

COROLLARY 5.5. *Suppose $n\geq 2$ and let σ_e be the number of $\sigma\in\mathcal{G}_n$ whose decomposition contains an even number of cycles of even length. Similarly let σ_0 be the number of $\sigma\in\mathcal{G}_n$ having an odd number of even length cycles, then $\sigma_e=\sigma_0=n!/2$.*

PROOF. The number of $\sigma\in\mathcal{G}_n$ of type λ is

$$\frac{n!}{\prod_i i^{r_i}\cdot r_i!}.$$

Setting $a=1$ in Proposition 5.3 we obtain $\sigma_e-\sigma_0\equiv 0(\text{mod } n!)$, but since $0<\sigma_e,\sigma_0<n!$ we must have $\sigma_e-\sigma_0=0$. Also $\sigma_e+\sigma_0=n!$ and the corollary follows.

If we restrict our attention to functions from $[n]$ onto X then

$$B(\pi)=a!S(n,a)$$

when $x_1=x_2=\cdots=x_a=1$. In this case Proposition 5.3 is replaced by:

PROPOSITION 5.6

$$\sum_{\lambda\vdash n}\left[\frac{n!}{\prod_i i^{r_i}\cdot r_i!}(-1)^{r_e}a!S(n,a)\right]\equiv 0(\mathrm{mod}\ n!).$$

6. THE ϕ FUNCTION

In this section we introduce a generalization of the classical Euler ϕ function used in Corollary 4.6. Given a period $\pi\in\mathcal{P}(G,[n])$ we define

$$\phi(\pi)=|\{g\in G\colon \text{the cycles of } g \text{ are exactly the blocks of } \pi\}|.$$

If $G=C_n$ and $\pi=\pi_d$ then

$$\phi(\pi_d)=\phi(d), \tag{6.1}$$

where the second ϕ is Euler's function.

From the work of Rota and Smith [9] it follows that the equivalence classes of functions under the action of G are enumerated by

$$\frac{1}{o(G)}\sum_{\pi\in\mathcal{P}(G,[n])}\phi(\pi)B(\pi)$$

(cf. Theorem 3.2). Hence:

THEOREM 6.2

$$\sum_{\pi\in\mathcal{P}(G,[n])}\phi(\pi)B(\pi)\equiv 0(\mathrm{mod}\ o(G)).$$

Applying Theorem 6.2 to the case $G=C_n$ we obtain, via equations (4.9) and (6.1),

PROPOSITION 6.3. $\sum_{d|n}\phi(d)(x_1^d+x_2^d+\cdots+x_a^d)^{n/d}\equiv 0(\mathrm{mod}\ n)$ *where* $\phi(n)=|\{d\colon 0<d<n \textit{ and } g.c.d.(d,n)=1\}|$.

COROLLARY 6.4. *For all non-negative integers* $i_1,i_2,\ldots,i_a$ *such that* $i_1+i_2+\cdots+i_a=n$:

$$\sum_{d|n}\phi(d)\binom{n/d}{i_1/d,\,i_2/d,\ldots,i_a/d}\equiv 0(\mathrm{mod}\ n)$$

and

$$\sum_{d|n}\phi(d)a^{n/d}\equiv 0(\mathrm{mod}\ n),$$

and for the proper family of onto functions:

PROPOSITION 6.5. $\sum_{d|n}\phi(d)a!S(n/d,a)\equiv 0(\mathrm{mod}\ n)$.

Considering $G=\mathscr{G}_n$, the symmetric group, we can calculate $\phi(\pi)$ explicitly. If B is a block of π, $|B|=i$, then there are $(i-1)!$ cycles in $\mathscr{G}_n$ that are transitive on B. Thus

$$\phi(\pi)=\prod_i (i-1)!^{r_i} \tag{6.6}$$

where r_i of the blocks of π have size i. Comparing (6.6) with (5.1) we see that $\phi(\pi)=|\mu(\pi)|$. Hence Theorem 6.2 provides the following analogs of Propositions 5.3 and 5.6.

PROPOSITION 6.7

$$\sum_{\lambda\vdash n}\left[\frac{n!}{\prod_i i^{r_i}r_i!}a^r\right]\equiv 0(\text{mod } n!)$$

where $\lambda=(1^{r_1},2^{r_2},\ldots,n^{r_n})$, $r=\sum_j r_j$.

PROPOSITION 6.8

$$\sum_{\lambda\vdash n}\left[\frac{n!}{\prod_i i^{r_i}r_i!}a!S(n,a))\right]\equiv 0(\text{mod } n!).$$

7. FURTHER WORK

(1) The methods of this paper can be extended to arbitrary finite abelian groups by considering them as direct products of cyclic groups. Wreath products also yield interesting results. These considerations will be presented in a future paper [10].

(2) Can congruences be obtained from the alternating group? Here the major obstruction is a precise description of the lattice of periods.

(3) Ira Gessel [2] has considered the action of a group on the vertices of a labeled graph. Among other things, this technique yields congruences for the Stirling numbers of both kinds.

(4) Since every group action gives rise to a representation, we can consider the corresponding character χ. What relationship exists between χ and the Möbius function μ? Specifically, can one express one function in terms of the other?

(5) It would be interesting to examine the action of a group on sets of pairs, triples, or even n-tuples. As a special case one could obtain congruences for di- and multigraphs,

(6) For what groups, G, is the lattice of periods modular? Semi-modular? Supersolvable? (See Stanley [12] for definitions.)

(7) Since μ and ϕ can be interpreted in an arbitrary lattice of periods, one would suspect that other number theoretic functions can be so generalized. In particular, τ and λ are likely candidates.

REFERENCES

1. L. E. Dickson, *History of the theory of numbers. I. Divisibility and primality*, Carnegie Institute of Washington (1919).
2. I. M. Gessel, Combinatorial proofs of congruences, in preparation.
3. S. W. Golomb, A mathematical theory of discrete classification, *Proc. Fourth London Symp. on Information Theory*, 404–425.
4. P. Hall, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* (2), **36** (1934), 29–95.
5. E. E. Kummer, Über die Ergänzungsstätze zu den allgemeinen Reciprocitätsgesetzen, *J. für Math.* **44** (1852), 93–146.

6. G. Polya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen, *Acta Math.*, **68** (1937), 145–254.
7. G.-C. Rota, On the foundations of combinatorial theory, I: Theory of Möbius functions, *Z. Wahrscheinlichkeits theorie* **2** (1964), 340–368.
8. G.-C. Rota, Baxter algebras and combinatorial identities, II, *Bull. Amer. Math. Soc.* **75** (1969), 330–334.
9. G.-C. Rota and D. A. Smith, Enumeration under group action, *Annali Scuola Normale Superiore-Pisa Classe di Scienze* (4), **4** (1977), 637–646.
10. B. E. Sagan, Congruences via Abelian groups, in preparation.
11. L. Solomon, The Burnside algebra of a finite group, *J. Combinatorial Theory* **2** (1967), 603–615.
12. R. P. Stanley, Supersolvable lattices, *Algebra Universalis* (2) **2** (1972), 197–217.
13. E. W. Witt, Treue Darstellung Liescher Ringe, *J. für die Reine und Aug.* **177** (1937), 152–160.

(*Received 7 June 1979*)

G.-C. ROTA
Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, Mass. 02139, U.S.A.
B. SAGAN
Département de Mathématique, Université de Strasbourg,
7, rue René Descartes, 67 Strasbourg, France