JOURNAL OF NUMBER THEORY 20, 210–237 (1985)

Congruences via Abelian Groups

BRUCE E. SAGAN*

Department of Mathematics, Middlebury College, Middlebury, Vermont 05753

Communicated by D. J. Lewis

Received May 1, 1983

DEDICATED TO GIAN-CARLO ROTA

Given a group G acting on a set S, Möbius inversion over the lattice of subgroups can be used to obtain congruences relating the number of elements of S stabilized by each subgroup. By taking S to be a set of subsets, partitions, or permutations congruences for binomial and multinomial coefficients, Stirling numbers of both kinds, and various other combinatorial sequences are derived. Congruences for different moduli are obtained by varying the order of G. © 1985 Academic Press, Inc.

1. INTRODUCTION

Proving congruences by counting equivalence classes under the action of a finite group is not a new idea. It goes back at least one hundred years to a paper of Peterson [27] who used the action of the cyclic group of order p to prove the congruences of Fermat and Wilson. A glance at Dickson's *History of the Theory of Numbers* [9] shows that this method has been rediscovered many times, but a systematic development of the area was still lacking. This has changed recently: Rota and Sagan [32] investigated congruences derived from groups acting on functions, Smith [38] has considered wreath products, and Gessel [12] has studied congruences for groups acting on graphs.

The purpose of this paper is to obtain congruences by using Mobius inversion over the lattice of subgroups of a given group. Since this lattice is difficult to work with if the group is very complicated, we will concern ourselves only with abelian groups. In spite of this restriction, we will be able to prove a long list of congruences. We will concentrate on congruences for

* Research supported by NSF Grant MCS 80-03027.

0022-314X/85 $3.00

Copyright © 1985 by Academic Press, Inc.
All rights of reproduction in any form reserved.

binomial and multinomial coefficients, Stirling numbers of both kinds, and iterated Stirling numbers. It is, however, a simple matter to apply the same technique and obtain congruences for other sequences enumerating labeled objects. Some further examples are provided in the penultimate section. Finally, we end with some open questions.

2. Preliminaries

Let G be a finite group with identity element e, and let S be a finite set on which G acts. Given $s \in S$, the *stabilizer* of s is $G_s := \{g \in G | gs = s\}$ and the *orbit* of s is $O_s := \{t \in S | t = gs \text{ for some } g \in G\}$. It is well known and easy to prove that

$$|O_s| = |G|/|G_s|, \tag{2.1}$$

where $|\ |$ denotes cardinality.

An element $s \in S$ is said to be *aperiodic* whenever $G_s = e$. In view of (2.1) s is aperiodic if and only if $|O_s| = |G|$ so we immediately have the following result.

Lemma 1. *The number of aperiodic elements in S is divisible by $|G|$.*

Although Lemma 1 is trivial to prove, all the other congruences in this paper are derived from it, making it a powerful tool. The only thing needed now is an expression for the number of aperiodic elements that can be easily computed. We will first try to solve a more general problem and then specialize to the case above.

Consider the lattice $\mathscr{L}(G)$ of all subgroups $H \leqslant G$ ordered by inclusion. For $H \in \mathscr{L}(G)$ define

$$\alpha(H) := |\{s \in S | G_s = H\}|,$$

then Lemma 1 can be restated

$$\alpha(e) \equiv 0 \pmod{|G|}. \tag{2.2}$$

Calculating the values of α directly is difficult, but there is a related function which is less exacting and hence easier to work with. Let

$$\beta(H) := |\{s \in S | G_s \supseteq H\}|$$

then clearly

$$\beta(H) = \sum_{\substack{K \geqslant H \\ K \in \mathscr{L}(G)}} \alpha(K). \tag{2.3}$$

To express the α's in terms of the β's we need the *Mobius Inversion Theorem* (see Rota [31] for details).

THEOREM 2. *Let $\mathscr{L}$ be a lattice with unique minimal element $\hat{0}$ and let R be any ring. Suppose there are two functions $\alpha, \beta: \mathscr{L} \to R$ satisfying $\beta(b) = \sum_{a \geq b} \alpha(a)$ for all $b \in \mathscr{L}$, then*

$$\alpha(\hat{0}) = \sum_{b \in \mathscr{L}} \mu(b)\, \beta(b),$$

where μ is the Mobius function of $\mathscr{L}$ defined recursively by $\mu(\hat{0}) = 1$ and $\mu(a) = -\sum_{b<a} \mu(b)$ for $a \neq \hat{0}$.

Combining Eqs. (2.2) and (2.3) with Theorem 2 we obtain

COROLLARY 3. $\sum_{H \in \mathscr{L}(G)} \mu(H)\, \beta(H) \equiv 0 \pmod{|G|}$.

In order to obtain congruences from Corollary 3 we need only substitute various groups G and sets S on which they can act. For notational convenience we let $[n] := \{1, 2, \ldots, n\}$ and $m + [n] := \{m+1, m+2, \ldots, m+n\}$. We take G to be the abelian subgroup of the symmetric group which is a product of cyclic groups $C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r}$, where C_{m_j} is generated by the cycle $(J+1, J+2, \ldots, J+m_j)$, $J = \sum_{i<j} m_i$. Finally, the letter p will always be used to denote a prime.

The congruences following from Corollary 3 will be numbered consecutively throughout the paper on the left. Auxiliary equations will continue to be labeled by section on the right.

3. THE CASE $G = C_p$

Here the details are particularly simple, as $\mathscr{L}(C_p)$ consists of a two element chain

The Möbius function is trivial to compute from the definition in Theorem 2:

$$\mu(e) = 1 \qquad \text{and} \qquad \mu(C_p) = -1.$$

Hence Corollary 3 becomes $\beta(e) - \beta(C_p) \equiv 0 \pmod{p}$ or

$$\beta(e) \equiv \beta(C_p) \pmod{p}. \tag{3.1}$$

Since all congruences in this section will be mod p, we will sometimes drop the modulus. Now let us consider various sets on which C_p can act.

A. *Binomial and Multinomial Coefficients*

Let S be the set of all k element subsets T of $[n+p]$ and let C_p act on S in the natural way, i.e., if $g \in C_p$ and $T = \{t_1,..., t_k\}$ then $gT = \{gt_1,..., gt_k\}$.

$$(1) \quad \binom{n+p}{k} \equiv \binom{n}{k} + \binom{n}{k-p} \pmod{p}.$$

Proof. Since every k-subset of $[n+p]$ is stabilized by e, we have

$$\beta(e) = \binom{n+p}{k}. \tag{3.2}$$

For the subsets T that C_p stabilizes there are two possibilities. If $1 \in T$ then the repeated action of $(1, 2,..., p)$ forces $[p] \subseteq T$. Now we must choose the remaining $k-p$ elements of T out of the elements of $p+[n]$, giving a contribution of $\binom{n}{k-p}$. If instead $1 \notin T$ then we have $T \subseteq p+[n]$, giving $\binom{n}{k}$ choices for T. Hence $\beta(C_p) = \binom{n}{k} + \binom{n}{k-p}$ and (1) follows using (3.1) and (3.2). ∎

As a corollary we have the well-known congruence of Lucas [24].

(2) If $n = \sum_j n_j p^j$ and $k = \sum_j k_j p^j$ are the p-ary expansions of n and k then

$$\binom{n}{k} \equiv \prod_j \binom{n_j}{k_j} \pmod{p}.$$

Proof. This is an easy induction based on the recurrence relation (1) and is left to the reader. ∎

If we now take S to be all partitions of $[n+p]$ into subsets $T_1, T_2,..., T_a$ with $|T_i| = k_i$ for $i = 1, 2,..., a$ then we have the following analogs of (1) and (2) for multinomial coefficients.

$$(3) \quad \binom{n+p}{k_1, k_2,..., k_a} \equiv \sum_{i=1}^{a} \binom{n}{k_1, k_2,..., k_i - p,..., k_a} \pmod{p}.$$

(4) If $n = \sum_j n_j p^j$ and $k_i = \sum_j k_{ij} p^j$ and the p-ary expansions of n and the k_i then

$$\binom{n}{k_1, k_2,..., k_a} \equiv \prod_j \binom{n_j}{k_{1j}, k_{2j},..., k_{aj}} \pmod{p}.$$

We also obtain Fermat's theorem:

(5) $a^p \equiv a \pmod{p}$.

Proof. $a^p = \sum_{k_1+k_2+\cdots+k_a=p} \binom{p}{k_1, k_2, \ldots, k_a}$ and by (4), the only nonzero terms, mod p, in this sum are those of the form $\binom{p}{0,0,\ldots,p,\ldots,0}$. ∎

B. *Stirling Numbers of the Second Kind.*

Take S to be the set of all partitions π of $[n+p]$ into k subsets (or blocks), which is counted by the Stirling number of the second kind $S(n+p, k)$. The action of C_p on subsets extends naturally to such partitions.

(6) $S(n+p, k) \equiv S(n+1, k) + S(n, k-p) \pmod{p}$.

Proof. As before, $\beta(e) = |S| = S(n+p, k)$. To compute $\beta(C_p)$ there are again two cases. If $\{1\}$ is a singleton block of π then so are $\{2\}, \{3\}, \ldots, \{p\}$. This means there are $S(n, k-p)$ ways to choose the rest of the blocks of π. If 1 is in a block of size at least two then 2, 3,..., p are also in the same block. Thus the set $[p]$ is acting like a single element, which we shall denote by P, so we are really just partitioning the set $\{P, p+1, p+2, \ldots, p+n\}$ into k blocks. This gives a final contribution of $S(n+1, k)$ to $\beta(C_p)$ and hence (6) follows from (3.1). ∎

Define the *falling factorial* polynomial by $(x)_n := x(x-1)(x-2)\cdots(x-n+1)$.

(7) (Lagrange [22]) $(x)_p \equiv x^p - x \pmod{p}$.

Proof. The identity

$$x^m = \sum_{k=0}^{m} S(m, k)\,(x)_k \tag{3.3}$$

can be easily proved by counting the number of functions from a set with m elements to a set with x elements in two different ways (see, e.g., [18]). Setting $n=0$ in (6) gives

$$S(p, k) \equiv S(1, k) + S(0, k-p) = 1 \qquad \text{if } k = 1 \text{ or } p,$$
$$= 0 \qquad \text{otherwise,}$$

and inserting these values in (3.3) with $m=p$ results in (7). ∎

The $S(n, k)$ are periodic functions of n as is shown by the next congruence.

(8) (Becker and Riordan [2]). If j is defined by the equation $p^j \leqslant k < p^{j+1}$ then

$$S(n + p^j(p-1), k) \equiv S(n, k) \pmod{p}.$$

Proof. This can be proved by induction on j through repeated application of (6) and (2). The umbral calculus can also be used to make the proof more elegant and details of this approach can be found in [2].

There is also a way to derive this congruence directly by using group actions. Consider $G = C_{p^{j+1}}$ acting on the set S of partitions of $[n + p^{j+1}]$ into k parts. From (2.1) we see that every element of S lies in an orbit whose size is either divisible by p or equal to 1, hence

$$\beta(e) \equiv \beta(G). \tag{3.4}$$

To compute $\beta(C_{p^{j+1}})$ note that either the set $[p^{j+1}]$ acts as a single element P, yielding $S(n+1, k)$ partitions, or $[p^{j+1}]$ is partitioned into p^i sets of size p^{j+1-i}, viz., $\{r + sp^i | 0 \leqslant s \leqslant p^{j+1-i} - 1\}$ for $1 \leqslant r \leqslant p^i$. Hence (3.4) becomes

$$S(n + p^{j+1}, k) \equiv S(n+1, k) + \sum_{i=1}^{j+1} S(n, k - p^i).$$

But if $k < p^{j+1}$ then $S(n, k - p^{j+1}) = 0$ and so

$$\begin{aligned} S(n + p^{j+1}, k) &\equiv S(n+1, k) + \sum_{i=1}^{j} S(n, k - p^i) \\ &\equiv S(n + p^j, k). \quad \blacksquare \end{aligned}$$

The Bell numbers, $B(n) := \sum_k S(n, k)$, count all partitions of $[n]$.

(9) (Touchard [40]) $B(n+p) \equiv B(n+1) + B(n) \pmod{p}$.

Proof. This congruence can be obtained either by taking S to be all partitions of $[n+p]$ or by summing (6) for all values of k. $\blacksquare$

We can also iterate (9) or use (3.4) with $G = C_p \times C_{p^2} \times \cdots \times C_{p^{p-1}}$ to obtain

(10) (Hall [16]) $B(n + (p^p - 1)/(p-1)) \equiv B(n) \pmod{p}$.

Our methods can also be extended to provide congruences for generating functions. For example, associate with each partition π of $[n]$ a monomial $\pi(\mathbf{x}) = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where i_j is the number of blocks of size j in π. Define the nth Bell polynomial by

$$B_n(\mathbf{x}) := \sum \pi(\mathbf{x}), \qquad \pi \text{ a partition of } [n],$$

then considerations similar to those that led to (6) yield the following formula of Gessel [12]

$$(11)\quad B_{n+p}(\mathbf{x}) \equiv x_1^p B_n(\mathbf{x}) + \sum_i \binom{n}{i} x_{i+p} B_{n-i}(\mathbf{x}) \pmod{p}.$$

C. *Stirling Numbers of the First Kind*

Consider the set of all permutations σ of $[n+p]$ with k cycles as our set S, with C_p acting by conjugation. We define $c(n+p,k) := |S|$ as the corresponding *signless Stirling number of the first kind* [30] (the normal Stirling numbers of the first kind being $s(n,k) = (-1)^{n-k} c(n,k)$). All the congruences below are for the signless numbers, but the identities for the signed ones can be recovered by inserting the appropriate powers of -1.

$$(12)\quad c(n+p,k) \equiv (p-1)\, c(n,k-1) + c(n,k-p) \pmod{p}.$$

Proof. The reader can easily see where the terms $c(n+p,k)$ and $c(n,k-p)$ come from. The remaining summand results from those permutations σ stabilized by C_p, where 1 is in a cycle τ of length at least two. There are $p-1$ choices for τ, i.e., $\tau = (1, 2, \ldots, p)^j$ for some j with $1 \leqslant j < p$, and there are $c(n,k-1)$ ways to construct the rest of σ. ∎

Taking $n=0$, $k=1$ in (12) and recalling that $c(0,k) = \delta_{0k}$ we have Wilson's theorem.

$$(13)\quad (p-1)! \equiv p-1 \pmod{p}.$$

These Stirling numbers behave differently from those of the second kind with respect to periodicity. In fact

$$(14)\quad c(n,k) \equiv 0 \pmod{p} \text{ if } n > kp.$$

Proof. Using the fact that $c(n+1,1) = n! \equiv 0$ for $n \geqslant p$, the result follows from (12) and induction on k. ∎

To find a congruence for arbitrary values of n and k, we can induct on n and obtain the following corollary of (12).

$$(15)\quad c(n, n-k) \equiv (-1)^{k_1} \binom{n_1}{k_1} c(n_0, n_0 - k_0) \pmod{p},$$

where $n = n_1 p + n_0$, $0 \leqslant n_0 < p$, and $k = k_1(p-1) + k_0$, $0 \leqslant k_0 < p-1$. Equation (15), in its turn, yields as a corollary the following result of Gupta [15].

$$(16)\quad c(np,k) \equiv 0, \qquad \text{if } p-1 \nmid np-k \pmod{p},$$

$$\equiv (-1)^m \binom{n}{m}, \quad \text{if } m(p-1) = np-k \pmod{p}.$$

D. *Iterated Stirling Numbers*

The *iterated Stirling numbers* were introduced by Bell [3, 4] and are derived from Stirling's triangle by repeated matrix multiplication. Specifically, for $s \geqslant 0$ we define the numbers $S(n, k, s)$ by

$$S(n, k, 1) := S(n, k)$$

and

$$S(n, k, s) := \sum_{i=0}^{n} S(n, i, 1) \cdot S(i, k, s-1). \tag{3.5}$$

Note that if the index s, called the *stack*, is zero then equation (3.5) forces

$$S(n, k, 0) = \delta_{nk}.$$

The notation used above differs from other papers on the subject [2, 5] in that the first two indices are transposed. We also have the corresponding *iterated Bell numbers*, $B(n, s) := \sum_k S(n, k, s)$.

We shall call the objects counted by $B(n, s)$ *s-fold partitions of* $[n]$. An s-fold partition π_s is obtained by partitioning a set $\{B_1, B_2, \ldots, B_i\}$ whose elements are the blocks of an $(s-1)$-fold partition, e.g., the 1-fold partition $\pi_1 = \{1, 3\}\ \{2, 4\}\ \{5\}$ gives rise to 2-fold partitions such as $\pi_2 = \{\{1, 3\}, \{5\}\}\ \{\{2, 4\}\}$. The elements of $[n]$ are called *blocks of depth* 0, and for $t > 0$ the *blocks of depth t* are those sets whose elements are blocks of depth $t-1$. For example, in π_2 the depth of $\{1, 3\}$ is 1 while the depth of $\{\{1, 3\}, \{5\}\}$ is 2. If we take S to be the set of s-fold partitions of $[n+p]$ into k blocks of depth s then clearly $|S| = S(n+p, k, s)$.

(17) $$S(n+p, k, s) \equiv S(n, k-p, s) + \sum_{t=0}^{s-1} \sum_{i=0}^{n} S(n, i, t) \times S(i+1, k, s-t) \pmod{p}.$$

Proof. To obtain the right-hand side of (17) we must count those $\pi_s \in S$ which are stabilized by C_p. A *singleton block* of π_s is one which contains a single element of $[n]$. Let t be the maximum depth of a singleton block containing 1 so that $0 \leqslant t \leqslant s$. If $t = s$ then 2, 3,..., p are also in singleton blocks of depth s and there are $S(n, k-p, s)$ ways to build the rest of π_s. If $t < s$ then 2, 3,..., p are in singleton blocks of depth t but the block of depth $t+1$ containing 1 also contains 2, 3,..., p. Letting the number of depth t blocks be $i+p$, $0 \leqslant i \leqslant n$, we see that there are $S(n, i, t)$ ways to choose the blocks of depth at most t and $S(i+1, k, s-t)$ ways to choose the blocks of depth greater than t. ∎

Analogous to Eqs. (8), (9), and (10), we have three results first obtained by Becker and Riordan [2]. These congruences follow from (17) in the same way that (8)–(10) follow from (6).

(18) Let $q_m = p^{p^m}$, where m is chosen so that $q_{m-1} < s \leqslant q_m$. If $q_m^{j-1} p^s \leqslant k < q_m^j p^s$ then

$$S(n + q_m^j(q_m - 1), k, s) \equiv S(n, k, s) \pmod{p}.$$

(19) $B(n+p, s) \equiv B(n,s) + \sum_{t=0}^{s-1} \sum_{i=0}^{n} S(n,i,t)\ B(i+1,\ s-t) \pmod{p}$.

(20) If $p^{m-1} \leqslant s < p^m$ and $q_m = p^{p^m}$ then

$$B(n + q_m - 1, s) \equiv B(n, s) \pmod{p}.$$

We can extend the definition of $S(n, k, s)$ to include negative values of s. From Eq. (3.5) we see that

$$S(n, k, -1) = s(n, k).$$

In general, if $s < 0$ the numbers $c(n, k, |s|) = |S(n, k, s)|$ count $|s|$-fold permutations of $[n]$ with k cycles of depth $|s|$. The corresponding "Bell numbers" are $b(n, |s|) := \sum_k c(n, k, |s|)$. For convenience's sake we will henceforth drop the absolute value signs and take s to be positive. The next four congruences are, to my knowledge, new.

(21) $c(n+p,k,s) \equiv c(n,k-p,s) + (p-1) \cdot \sum_{t=1}^{s} \sum_{i=0}^{n} c(n, i, t)$
$\times c(i+1, k, s-t) \pmod{p}$.

Proof. This generalization of (12) is proved in a manner similar to the demonstration of (17). We omit the details. ∎

Using (14) and either (21) or (3.5) we have

(22) $c(n, k, s) \equiv 0 \pmod{p}$ if $n > kp^s$.

Consideration of all s-fold permutations of $[n]$ yields

(23) $b(n+p, s) \equiv b(n, s) + (p-1) \cdot \sum_{t=1}^{s} \sum_{i=0}^{n} c(n, i, t)\ b(i+1, s-t) \pmod{p}$.

Finally we show that these bell numbers have period 1.

(24) $b(n, s) \equiv 0 \pmod{p}$ if $n > p^{s-1}(p-1), s > 0$.

Proof. Induct on s using the fact that $b(n, 1) = n! \equiv 0$ if $n > p - 1$. ∎

The methods of this section can be easily extended to the group C_{p^r},

thereby providing congruences modulo p^r. Since $\mathscr{L}(C_{p^r})$ is a chain with one subgroup H_i of order p^i for $0 \leqslant i \leqslant r$ we have

$$\begin{aligned} \mu(H_i) &= +1, \quad i = 0, \\ &= -1, \quad i = 1, \\ &= \ 0, \quad i \geqslant 2. \end{aligned}$$

Hence Corollary 3 becomes

$$\beta(e) = \beta(H_0) \equiv \beta(H_1) \pmod{p^r}. \tag{3.6}$$

This approach has been used in conjunction with Polya actions in Rota and Sagan [32], however, the congruences obtained are not always the best possible. It turns out to be more efficient to use products of cyclic groups as will be shown in the next two sections. By way of illustration, in Section 4 we work out some example for $r = 2$ in detail. Finally the general case is treated in Section 5.

4. The Case $G = C_p \times C_p$

For notational convenience let $\sigma = (1, 2, \ldots, p)$, $\tau = (p+1, p+2, \ldots, 2p)$, and for $A \subseteq G$ let $\langle A \rangle$ denote the subgroup generated by A. The lattice $\mathscr{L}(C_p \times C_p)$ is pictured in Fig. 1; note that there are $p+1$ subgroups of order p.

The Möbius function for each $H \leqslant G$ is easily seen to be

$$\begin{aligned} \mu(H) &= \ \ 1 \quad \text{if } |H| = 1, \\ &= -1 \quad \text{if } |H| = p, \\ &= \ \ p \quad \text{if } |H| = p^2. \end{aligned} \tag{4.1}$$

Hence we need only compute $\beta(H)$ to obtain congruences modulo p^2.

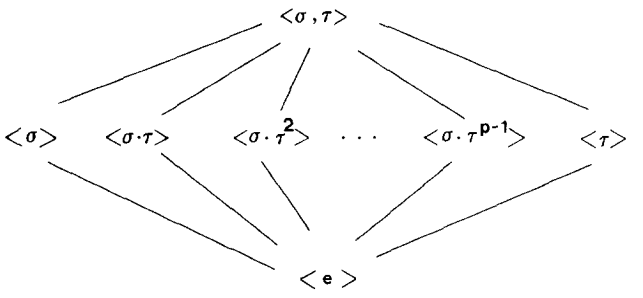

Figure 1

A. *Binomial and Multinomial Coefficients*

$$(25)\quad \binom{n+2p}{k}-2\left[\binom{n+p}{k}+\binom{n+p}{k-p}\right]+\left[\binom{n}{k}+2\binom{n}{k-p}+\binom{n}{k-2p}\right]\equiv 0 \pmod{p^2}.$$

Proof. Let $S=\{T \mid T\subseteq [n+2p]\}$ and let $G=C_p\times C_p$ act on S. As before $\beta(e)=\binom{n+2p}{k}$ and $\beta(\langle\sigma\rangle)=\beta(\langle\tau\rangle)=\binom{n+p}{k}+\binom{n+p}{k-p}$ accounting for the first three terms of (25). For the group $\langle\sigma\cdot\tau\rangle$ we have four cases depending on which of the two elements 1, $p+1$ are in T, hence

$$\mu(\langle\sigma\cdot\tau\rangle)\,\beta(\langle\sigma\cdot\tau\rangle)=-\left[\binom{n}{k}+2\binom{n}{k-p}+\binom{n}{k-2p}\right].$$

Since all $p-1$ of the subgroups $\langle\sigma\cdot\tau^i\rangle$, $1\leqslant i\leqslant p-1$, as well as the full group stabilize the same sets and $\mu(G)=p$ we obtain a final contribution of

$$-(p-1)\left[\binom{n}{k}+2\binom{n}{k-p}+\binom{n}{k-2p}\right]+p\left[\binom{n}{k}+2\binom{n}{k-p}+\binom{n}{k-2p}\right]. \quad \blacksquare$$

Using the recursion relation (25) and induction on n we can prove the following strengthening of Lucas' congruence for the case when the size of the set is dividible by p.

(26) If $k=k_1p+k_0$, $0\leqslant k_0<p$, then

$$\binom{np}{k}\equiv\binom{n}{k_1} \pmod{p^2} \qquad \text{if } k_0=0,$$

$$\equiv n\binom{n-1}{k_1}\binom{p}{k_0} \pmod{p^2} \qquad \text{if } k_0\neq 0.$$

Kazandzidis [19, 20] has investigated extensions of Lucas' results for odd primes. If we adopt the usual conventions

$$\binom{n}{k}:=0 \qquad \text{if } k<0,$$

$$:=(-1)^k\binom{k-n-1}{k} \qquad \text{if } n<0,$$

then a double induction and (25) yields

(27) For $p \geqslant 3$ and $n = n_1 p + n_0$, $k = k_1 p + k_0$ with $0 \leqslant n_0, k_0 < p$, we have

$$\binom{n}{k} \equiv \binom{n_1}{k_1}\left[(n_1+1)\binom{n_0}{k_0} - (n_1+k_1)\binom{n_0-p}{k_0} - k_1\binom{n_0-p}{k_0+p}\right] \pmod{p^2}.$$

Taking specific values for n_0 and/or k_0 in (27) results in various simple formulas, e.g.,

(28) (Kazandzidis [19]) If $p \geqslant 3$ then

$$\binom{np-1}{kp-1} \equiv \binom{n-1}{k-1} \pmod{p^2}.$$

Analogs of these congruences can be proved for multinomial coefficients. Two examples are

$$(29)\quad \binom{n+2p}{k_1, k_2, \ldots, k_a} - 2\sum_i \binom{n+p}{k_1, \ldots, k_i - p, \ldots, k_a} + \sum_{i,j} \binom{n}{k_1, \ldots, k_i - p, \ldots, k_j - p, \ldots} \equiv 0 \pmod{p^2}.$$

(30) If $k_i = k_{i1}p + k_{i0}$ with $0 \leqslant k_{i0} < p$ for $1 \leqslant i \leqslant a$ then

$$\binom{np}{k_1, k_2, \ldots, k_a} \equiv \binom{n}{k_{11}, \ldots, k_{a1}} \pmod{p^2} \qquad \text{if } k_{i0} = 0 \ \forall i.$$

$$\equiv n\binom{n-1}{k_{11}, \ldots, k_{a1}}\binom{p}{k_{10}, \ldots, k_{a0}} \pmod{p^2} \qquad \text{if } \sum_i k_{i0} = p.$$

$$\equiv 0 \pmod{p^2} \qquad \text{if } \sum_i k_{i0} \geqslant 2p.$$

The third part of Eq. (30) illustrates the more general result of Singmaster [34, 35] that the highest power of p dividing $\binom{n}{k_1, k_2, \ldots, k_a}$ is equal to the number of carries in the addition $\sum_i k_i$ in p-ary arithmetic.

B. *Stirling Numbers of the Second Kind*

Take $S = \{\pi | \pi \text{ a partition of } [n+2p] \text{ into } k \text{ blocks}\}$.

$$(31)\quad S(n+2p, k) - 2\sum_{i=0}^{1} S(n+p+i, k+(i-1)p) + \sum_{i=0}^{2}\binom{2}{i} S(n+i, k+(i-2)p) - p(p-1)\,S(n, k-p) \equiv 0 \pmod{p^2}.$$

Proof. The first half of (31) comes from the action of the subgroups $\langle e\rangle$, $\langle\sigma\rangle$, and $\langle\tau\rangle$. The second summation is the contribution from $\langle\sigma\cdot\tau^i\rangle$, $1\leqslant i\leqslant p-1$, and $\langle\sigma,\tau\rangle$ acting on partitions, where the sets $[p]$ and $p+[p]$ are either divided into singletons or are contained wholly in one block. Finally, there are partitions stabilized by $\langle\sigma\cdot\tau\rangle$ consisting of p doubletons of the form $\{1,t\}$, $\{2,\tau(t)\},\ldots,\{p,\tau^{p-1}(t)\}$, $t\in p+[p]$, and a partition of $2p+[n]$ into $k-p$ parts, for which there are $p\cdot S(n,k-p)$ possibilities. Since the same count holds for all $p-1$ of the subgroups $\langle\sigma\cdot\tau^i\rangle$, $1\leqslant i\leqslant p-1$, each having Mobius function -1, we get a total contribution of $-(p-1)\cdot pS(n,k-p)$. ∎

Enlarging the set S to all partitions of $[n+2p]$ we obtain

$$B(n+2p)-2\sum_{i=0}^{1}B(n+p+i)+\sum_{i=0}^{2}\binom{2}{i}B(n+i)-p(p-1)\,B(n)\equiv 0\ (\mathrm{mod}\ p^2). \tag{32}$$

It is useful to express complicated congruences like (31) and (32) in umbral form. If we define the *shift operator* E acting on a function $f(n)$ by $Ef(n):=f(n+1)$ then (32) becomes

$$[E^{2p}-2(E^{p+1}+E^p)+(E^2+2E+1)-p(p-1)]\,B(n)\equiv 0\ (\mathrm{mod}\ p^2).$$

Hence we have

$$[(E^p-E-1)^2-p(p-1)]\,B(n)\equiv 0\ (\mathrm{mod}\ p^2) \tag{4.2}$$

which also appears in Lunnon, Pleasants, and Stephens [25], and Gessel [12].

Following Becker and Riordan [2], we extend the shift operator to iterated Bell and Stirling numbers. The operators E_t are defined by the equations

$$E_tB(n,s):=\sum_i B(i+1,t)\,S(n,i,s-t),$$

$$E_tS(n,k,s):=\sum_i S(i+1,k,t)\,S(n,i,s-t).$$

In particular,

$$\begin{aligned}E_sB(n,s)&=\sum_i B(i+1,s)\,S(n,i,0)\\&=B(n+1,s),\end{aligned}$$

since $S(n, i, 0) = \delta_{ni}$. Also

$$E_0 S(n, k, s) = \sum_i S(i+1, k, 0)\, S(n, i, s)$$
$$= S(n, k-1, s)$$

so we can rewrite (31) as

$$[(E_1^p - E_1 - E_0^p)^2 - p(p-1)\, E_0^p]\, S(n, k) \equiv 0 \pmod{p^2}. \tag{4.3}$$

We should note that with the help of (26), Eqs. (4.2) and (4.3) can now be used to derive the periods of the Bell and Stirling numbers mod p^2. However, these derivations offer no new concepts so we will defer them until we deal with congruences modulo an arbitrary prime power in the next section.

Umbral notation is also extremely useful in simplifying congruences for s-fold partitions and permutations $s \geqslant 2$. For example, if we replace t by $s-t$ in Eq. (17) we get

$$E_s^p\, S(n, k, s) \equiv \left(E_0^p + \sum_{t=1}^{s} E_t\right) S(n, k, s) \pmod{p}.$$

Finally, it is most convenient to write the congruences for multinomial coefficients in terms of the *reverse shift operators* F_i defined by

$$F_i \binom{n}{k_1, k_2, \ldots, k_a} := \binom{n-1}{k_1, \ldots, k_i - 1, \ldots, k_a}.$$

Hence we can simplify (29) to

$$\left[1 - \sum_{i=1}^{a} F_i^p\right]^2 \binom{n+2p}{k_1, k_2, \ldots, k_a} \equiv 0 \pmod{p^2}.$$

5. The Case $G = C_p^r$

The group C_p^r (written additively) is an r-dimensional vector space over the Galois field $GF(p)$ and so the number of subgroups of order p^d is just the number of subspaces of dimension d. A well-known result (see, e.g., Andrews [1, Theorem 13.1]) states that this number is the Gaussian or p-binomial coefficient

$$\begin{bmatrix} r \\ d \end{bmatrix}_p = \frac{(p^r-1)(p^{r-1}-1)\cdots(p^{r-d+1}-1)}{(p^d-1)(p^{d-1}-1)\cdots(p-1)}. \tag{5.1}$$

All subgroups $H \leqslant C_p^r$ of order p^i are isomorphic to C_p^i so we need only calculate the Möbius function of the whole group. This is also well known (see [31]) but we include this calculation out of interest.

LEMMA 4. $\mu(C_p^r) = (-1)^r p^{\binom{r}{2}}$.

Proof. Induct on r. We have already seen that the lemma holds for $r \leqslant 2$ (Eq. (4.1)). For the induction step

$$\begin{aligned}
\mu(C_p^r) &= -\sum_{H < C_p^r} \mu(H) \\
&= -\sum_{d<r} \sum_{\substack{H \\ |H| = p^d}} (-1)^d p^{\binom{d}{2}} \qquad \text{by induction,} \\
&= -\sum_{d<r} \begin{bmatrix} r \\ d \end{bmatrix}_p (-1)^d p^{\binom{d}{2}} \qquad \text{by (5.1),} \\
&= (-1)^r p^{\binom{r}{2}}
\end{aligned}$$

where the last equality is the p-analog of the alternating sum of binomial coefficients [1, Theorem 3.3].

A. *Binomial and Multinomial Coefficients*

$$(33) \quad \sum_{i=0}^{r} (-1)^i \binom{r}{i} \sum_{j=0}^{i} \binom{i}{j} \binom{n-ip}{k-jp} \equiv 0 \pmod{p^r},$$

or in umbral form

$$(1 - F_1^p - F_2^p)^r \binom{n+rp}{k} \equiv 0 \pmod{p^r}.$$

Proof. Consider the cycles $\sigma_j = (jp+1, jp+2, \ldots, jp+p)$, $0 \leqslant j < r$. Given $g \in C_p^r$, $g = \prod_{j=0}^{r-1} \sigma_j^{n_j}$, then σ_j is a *factor* of g if $p \nmid n_j$. We say that a subgroup $H \leqslant C_p^r$ is associated with i *cycles* if the set of all factors of elements of H contains exactly i of the cycles σ_j. Equivalently H is associated with i cycles if and only if the smallest subgroup of the form $\bar{H} = \langle \sigma_{j_1}, \sigma_{j_2}, \ldots \rangle$ containing H has i generators.

If H is associated with i cycles and stabilizes a subset $T \subseteq [n+rp]$, then each of the i cycles is either completely contained in or completely disjoint from T. Choosing j of the cycles to be in T can be done in $\binom{i}{j}$ ways and the rest of T can be completed in $\binom{n-ip}{k-jp}$ ways thus

$$\beta(H) = \sum_{j=0}^{i} \binom{i}{j} \binom{n-ip}{k-jp}.$$

Since there are $\binom{r}{i}$ subgroups of the form $\bar{H}$, to complete the proof we need only show that for each choice of $\bar{H}$ we have

$$\sum_{H} \mu(H) = (-1)^i,$$

where the sum is over all $H \leqslant \bar{H}$ such that H is associated with i cycles. By the principle of inclusion and exclusion [33, Theorem 1.1] the number of subgroups of $\bar{H}$ having order p^d and associated with i cycles is

$$\sum_{j} (-1)^{i-j} \binom{i}{j} \begin{bmatrix} j \\ d \end{bmatrix}_p.$$

Since each of these subgroups has Möbius function $(-1)^d p^{\binom{d}{2}}$, we have

$$\begin{aligned} \sum_{H} \mu(H) &= \sum_{d} (-1)^d p^{\binom{d}{2}} \sum_{j} (-1)^{i-j} \binom{i}{j} \begin{bmatrix} j \\ d \end{bmatrix}_p \\ &= \sum_{j} (-1)^{i-j} \binom{i}{j} \sum_{d} (-1)^d p^{\binom{d}{2}} \begin{bmatrix} j \\ d \end{bmatrix}_p \\ &= \sum_{j} (-1)^{i-j} \binom{i}{j} \delta_{j0} \\ &= (-1)^i. \quad \blacksquare \end{aligned}$$

The corresponding result for multinomial coefficients is

$$\left(1 - \sum_{i=1}^{a} F_i^p\right)^r \binom{n+rp}{k_1, k_2, \ldots, k_a} \equiv 0 \pmod{p^r}. \tag{34}$$

Equation (34) may be used inductively to prove various congruences for specific values of the upper index. By way of example, we give the following result which has been observed by Kazandzidis [19], Rota and Sagan [32], and Smith [38].

$$\binom{np^r}{k_1, \ldots, k_a} \equiv \binom{np^{r-1}}{k_1/p, \ldots, k_a/p} \pmod{p^r}, \tag{35}$$

where by convention a multinomial coefficient containing a nonintegral fraction is zero.

B. *Stirling Numbers of the Second Kind*

It will be convenient to express the congruences in this subsection in terms of a new umbral operator $(\ )_S^r$ defined by

$$(U+V)_S^r := \sum_{i=0}^{r} S(r,i)\, U^i V^{r-i},$$

where U and V can be either numbers or other operators. In words, the operator $(\ )_S^r$ replaces the binomial coefficients in the normal expansion of the rth power with Stirling numbers of the second kind. Note that since Stirling's triangle is not symmetric, elements inside the operator do not commute, i.e., in general $(U+V)_S^r \neq (V+U)_S^r$.

$$(36)\quad \sum_{i=0}^{r} (-1)^i \binom{r}{i} \sum_{j=0}^{i} S(i,j)[-p(p-1)]^{i-j} \cdot \sum_{l=0}^{j} \binom{j-1+\delta_{ij}}{l} S(n+(r-i)\,p+l,\, k-(j-l)\,p) \equiv 0 \pmod{p^r}.$$

Equivalently,

$$(E_1^p - F_2^\varepsilon[(E_1+E_0^p)-p(p-1)]_S)^r\, S(n,k) \equiv 0 \pmod{p^r},$$

where $(F_2^\varepsilon)^i \binom{j}{l} := \binom{j-1+\delta_{ij}}{l}$.

Proof. If a subgroup H stabilizes a partition π of $[n+rp]$, then π induces a partition $\bar{\pi}$ of the cycles associated with H. Specifically, σ_a and σ_b are in the same block of $\bar{\pi}$ if and only if some element of σ_a appears in the same block with some element of σ_b in π (hence every element of σ_a appears in a block with some element of σ_b in π). This accounts for the $S(i,j)$ term in (36), the rest of the proof being similar to that of (33). ∎

The periods of these Stirling numbers modulo p^r can be derived from the recursion above.

(37) (Carlitz [5]) If $p^j \leqslant k < p^{j+1}$ then

$$S(n+p^{r+j}(p-1),\, k) \equiv S(n,k) \pmod{p^r}.$$

We also have the corresponding results for the Bell numbers

$$(38)\quad \sum_{i=0}^{r} (-1)^i \binom{r}{i} \sum_{j=0}^{i} S(i,j)[-p(p-1)]^{i-j} \times \sum_{l=0}^{j} \binom{j-1+\delta_{ij}}{l} B(n+(r-i)p+l) \equiv 0 \pmod{p^r}$$

or $(E_1^p - F_2^\varepsilon[(E_1+1)-p(p-1)]_S)^r\, B(n) \equiv 0 \pmod{p^r}$.

(39) (Lunnon, Pleasants, and Stephens [25])

$$B\left(n+p^r\left(\frac{p^p-1}{p-1}\right)\right)\equiv B(n) \pmod{p^r}.$$

C. *Stirling Numbers of the First Kind*

We define the operator $(\ )_c^r$ by

$$(U+V)_c^r := \sum_{i=0}^{r} c(r,i)\, U^i V^{r-i}$$

and proceed as in the last subsection. The reader can fill in the details of the proofs.

(40) $$\sum_{i=0}^{r}(-1)^i\binom{r}{i}\sum_{j=0}^{i}c(i,j)[-p(p-1)]^{i-j},$$

$$\sum_{l=0}^{j}\binom{j-1+\delta_{ij}}{l}(p-1)^l\, c(n+(r-i)\,p,\ k-(j-l)\,p-l)\equiv 0 \pmod{p^r},$$

or in umbral notation,

$$(E_1^p - F_2^{\varepsilon}[(p-1)\,E_0+E_0^p)-p(p-1)]_c)^r\, c(n,k)\equiv 0 \pmod{p^r}.$$

(41) If $n>krp$ then

$$c(n,k)\equiv 0 \pmod{p^r}.$$

D. *Iterated Stirling Numbers*

The only new observation here is that when an s-fold partition π_s is stabilized by a subgroup H then there is an induced partition $\bar{\pi}_s$ on the cycles associated with H which is also s-fold. Some of the congruences obtained are complicated enough that we will only state them in their umbral forms

(42) $$\left(E_s^p-\sum_{t=1}^{s-1}F_2^{\varepsilon}[E_t^p-p(p-1)]_S-F_2^{\varepsilon}[(E_1+E_0^p)-p(p-1]_S\right)^r S(n,k,s)\equiv 0 \pmod{p^r}.$$

(43) (Carlitz [5]) If $q_m=p^{p^m}$, where $q_{m-1}<s\leqslant q_m$ and $q_m^{j-1}p^s\leqslant k<q_m^j p^s$ then

$$S(n+p^r\cdot q_m^j(q_m-1),k,s)\equiv S(n,k,s)\ (\mathrm{mod}\ p^r).$$

(44) $$\left(E_s^p-\sum_{t=1}^{s-1}F_2^e[E_t^p-p(p-1)]_S-F_2^e[(E_1+1)-p(p-1)]_S\right)^r B(n,s)\equiv 0\ (\mathrm{mod}\ p^r).$$

(45) (Carlitz [5]) If $q_m=p^{p^m}$, where $q_{m-1}<s\leqslant q_m$ then

$$B(n+p^{r-1}(q_m-1),s)\equiv B(n)\ (\mathrm{mod}\ p^r).$$

(46) $$\left(E_s^p-\sum_{t=0}^{s-2}F_2^e[(p-1)E_t-p(p-1)]_c-F_2^e[((p-1)E_0+E_0^p)-p(p-1)]_c\right)^r c(n,k,s)\equiv 0\ (\mathrm{mod}\ p^r).$$

(47) If $n>krp^s$ then

$$c(n,k,s)\equiv 0\ (\mathrm{mod}\ p^r).$$

(48) $$\left(E_s^p-\sum_{t=0}^{s-2}F_2^e[(p-1)E_t-p(p-1)]_c-F_2^e[((p-1)E_0+E_0^p)-p(p-1)]_c\right)^r b(n,s)\equiv 0\ (\mathrm{mod}\ p^r).$$

(49) If $n>rp^{s-1}(p-1)$ and $s>0$ then

$$b(n,s)\equiv 0\ (\mathrm{mod}\ p^r).$$

6. Congruences Modulo m

Let m be an arbitrary positive integer. There are several ways to derive congruences modulo m. The first is to factor m, $m=\prod_i p_i^{\alpha_i}$, and use the results of previous sections.

For example, if $m=\prod_i p_i$ is a product of distinct primes then for each prime p_i we have

$$(E^{p_i}-E-1)B(n)\equiv 0\ (\mathrm{mod}\ p_i)$$

by Touchard's congruence (9). Hence

(50) If $m=\prod_{i=1}^r p_i$ then

$$\left[\prod_{i=1}^r (E^{p_i}-E-1)\right]B(n)\equiv 0\ (\mathrm{mod}\ m).$$

It follows that the period of $B(n)$ mod m is just the least common multiple of the periods mod p_i, in this case

$$\text{LCM } [(p_i^{p_i}-1)/(p_i-1)].$$

A second way to obtain results modulo $m=\prod_i p_i^{\alpha_i}$ is to use group actions directly. The abelian group yielding the best congruences is $\prod_i (C_{p_i}^{\alpha_i})$, where

$$\mathscr{L}\left(\prod_i (C_{p_i}^{\alpha_i})\right)=\prod_i \mathscr{L}(C_{p_i}^{\alpha_i})$$

as lattices since the orders of the groups $C_{p_i}^{\alpha_i}$ are relatively prime.

To see how this method applies to (50), consider the group $G=C_{p_1}\times C_{p_2}\times\cdots\times C_{p_r}$. Now $\mathscr{L}(G)$ is isomorphic to the Bollean Algebra of rank r since each subset $T\subseteq[r]$ corresponds to the subgroup $H_T=\prod_{t\in T} C_{p_t}$, thus $\mu(H_T)=(-1)^{|T|}$. Also H_T stabilizes all partitions of $[n+\sum_i p_i]$, where the elements of each C_{p_t} are singletons or act as if coalesced into one element. If we let j denote the number of C_{p_t} which coalesce and set $p_{TC}=\sum_{t\notin T} p_t$ then

$$\beta(H_T)=\sum_j \binom{|T|}{j} B(n+p_{TC}+j).$$

Hence

$$\sum_{T\subseteq[r]} \mu(H_T)\,\beta(H_T)=\left[\sum_{T\subseteq[r]} (-1)^{|T|}\sum_j \binom{|T|}{j} E^{p_{TC}+j}\right] B(n)$$
$$\equiv 0 \pmod m$$

which is precisely (50) expressed as a sum.

Since it is a straightforward matter to extend these methods to products of prime powers, we suppress the details. The analogs for multinomial coefficients and iterated Stirling numbers of both kinds are also easily derived.

More interesting congruences can be obtained from the action of C_m itself. In this case $\mathscr{L}(C_m)$ is isomorphic to the lattice of divisors of m. In fact each d where $d|m$ corresponds to the subgroup H_d generated by the product

$$\prod_{i=1}^{m/d}\left(i, i+\frac{m}{d}, i+2\frac{m}{d},\ldots, i+m-\frac{m}{d}\right).$$

Hence Corollary 3 becomes

$$\sum_{H_d \in \mathscr{L}(C_m)} \mu(H_d)\,\beta(H_d) = \sum_{d|m} \mu(d)\,\beta(H_d) \equiv 0 \pmod{m}, \tag{6.1}$$

where $\mu(d)$ is the classical Möbius function. Applying (6.1) to various sets, S, allows us to obtain congruences involving this number theoretic function. Since the details are similar to those of the last section, we omit them. All congruences will be stated in both the explicit and umbral forms.

A. *Binomial and Multinomial Coefficients*

$$\text{(51A)}\quad \sum_{d|m} \mu(d) \sum_{i=0}^{m/d} \binom{m/d}{i} \binom{n}{k-id} \equiv 0 \pmod{m}.$$

$$\text{(51B)}\quad \sum_{d|m} \mu(d)\,(F_1^d + F_2^d)^{m/d} \binom{n+m}{k} \equiv 0 \pmod{m}.$$

$$\text{(52A)}\quad \sum_{d|m} \mu(d) \sum_{i_1 + \cdots + i_a = m/d} \binom{m/d}{i_1, \ldots, i_a} \times \binom{n}{k_1 - i_1 d, \ldots, k_a - i_a d} \equiv 0 \pmod{m}.$$

$$\text{(52B)}\quad \sum_{d|m} \mu(d)(F_1^d + F_2^d + \cdots + F_a^d)^{m/d} \binom{n+m}{k_1, \ldots, k_a} \equiv 0 \pmod{m}.$$

B. *Stirling Numbers of the Second Kind*

$$\text{(53A)}\quad \sum_{d|m} \mu(d) \sum_{i=0}^{m/d} \binom{m/d}{i} \sum_{j=0}^{i} S(i,j)\,d^{i-j} \times \mathrm{S}(n + (m/d) - i,\ k - dj) \equiv 0 \pmod{m}.$$

$$\text{(53B)}\quad \sum_{d|m} \mu(d)[E_1 + (E_0^d + d)_S]^{m/d} S(n,k) \equiv 0 \pmod{m}.$$

$$\text{(54A)}\quad \sum_{d|m} \mu(d) \sum_{i=0}^{m/d} \binom{m/d}{i} \sum_{j=0}^{i} S(i,j)\,d^{i-j}\,B(n + (m/d) - i) \equiv 0 \pmod{m}.$$

$$\text{(54B)}\quad \sum_{d|m} \mu(d)[E_1 + (1+d)_S]^{m/d}\,B(n) \equiv 0 \pmod{m}.$$

C. *Stirling Numbers of the First Kind*

$$(55A)\quad \sum_{d|m} \mu(d) \sum_{i=0}^{m/d} \binom{m/d}{i} (d-1)^{m/d-i} \times \sum_{j=0}^{i} c(i,j)\, d^{i-j}\, c(n, k-dj-(m/d)+i) \equiv 0 \pmod{m}.$$

$$(55B)\quad \sum_{d|m} \mu(d)[(d-1)\, E_0 + (E_0^d + d)_c]^{m/d}\, c(n,k) \equiv 0 \pmod{m}.$$

D. *Iterated Stirling Numbers*

The formulas here are sufficiently complicated that we will only present them in the umbral form.

$$(56)\quad \sum_{d|m} \mu(d) \left[E_s + \sum_{t=1}^{s-1} (E_t + d)_S + (E_0^d + d)_S \right]^{m/d} \times S(n,k,s) \equiv 0 \pmod{m}.$$

$$(57)\quad \sum_{d|m} \mu(d) \left[E_s + \sum_{t=1}^{s-1} (E_t + d)_S + (1+d)_S \right]^{m/d} B(n,s) \equiv 0 \pmod{m}.$$

$$(58)\quad \sum_{d|m} \mu(d) \left\{ (d-1)\, E_{s-1} + \sum_{t=0}^{s-2} [(d-1)\, E_t + d]_c + (E_0^d + d)_c \right\}^{m/d} \times c(n,k,s) \equiv 0 \pmod{m}.$$

$$(59)\quad \sum_{d|m} \mu(d) \left\{ (d-1)\, E_{s-1} + \sum_{t=0}^{s-2} [(d-1)\, E_t + d]_c + (1+d)_c \right\}^{m/d} \times b(n,s) \equiv 0 \pmod{m}.$$

7. Further Examples

We have far from exhausted the possible sets upon which our groups can act. In this section we will mention some other examples which have appeared in various areas of combinatorics and group theory.

A. *Preferential Arrangements*

A *preferential arrangement* of the set $[n]$ consists of a partition π of $[n]$ together with a linear order on the blocks of π, e.g., the preferential arrangement $\{1,3\}, \{2\}$ is different from the arrangement $\{2\}, \{1,3\}$. Physically preferential arrangements can be thought of as describing the

possible outcomes of a race where ties are permitted. Preferential arrangements were first studied by Touchard [40], rediscovered by Gross [14], and then re-rediscovered by Good [13].

Let $A(n, k)$ be the number of preferential arrangements of $[n]$ with k blocks and let $P(n) = \sum_k A(n, k)$. Clearly $A(n, k)$ is just the number of surjections $f: [n] \twoheadrightarrow [k]$ so $A(n, k) = k!\, S(n, k)$. Thus we would expect the numbers $A(n, k)$ to have arithmetic properties similar to the Stirling numbers of the second kind but simpler (because of the factorial). This is borne out by applying group actions.

First let C_p act in the natural way on preferential arrangements of $[n+p]$ with k blocks and use (3.1). Clearly partitions where $1, 2, \ldots, p$ are singletons are no longer stable because of the order on the blocks thus $\beta(C_p) = A(n+1, k)$, and so $A(n+p, k) \equiv A(n+1, k)$. Hence $A(n, k)$ has period $p-1$ modulo p for all k, and for $k \geqslant p$ we have $A(n, k) \equiv 0 \pmod p$. Acting with the group C_{p^r} and using (3.6) we find, that $A(n, k)$ has period $p^{r-1}(p-1)$ for $n \geqslant p^{r-1}$ and is congruent to 0 for sufficiently large k. Now applying the methods of Section 6 we can obtain a result of Touchard [40],

(60) Let $m = \prod_i p_i^{\alpha_i}$ and let ϕ be Euler's function, then for $n \geqslant \max_i \{p_i^{\alpha_i - 1}\}$ we have

$$A(n + \phi(m), k) \equiv A(n, k) \pmod m,$$

$$P(n + \phi(m), k) \equiv P(n, k) \pmod m.$$

One could now consider s-fold preferential arrangments modelling, say, the results of s races where the people who tie in each category of race i compete only among themselves in race $i+1$. We leave this as an exercise.

B. *Involutions*

Let $v(n)$ be the number of involutions in the symmetric group $\sum_n$, i.e., the number of permutations of $[n]$ such that $\sigma^2 = e$. Equivalently $v(n)$ counts the number of $\sigma \in \sum_n$ whose canonical decomposition contains only one-cycles and two-cycles. Since conjugation preserves cycle structure, we have a well-defined action of C_n on involutions. This permits us to derive three congruences due to Chowla, Herstein, and Moore [7].

(61) For $p \geqslant 3$ we have

$$v(n + p^r) \equiv v(n) \pmod{p^r}.$$

Proof. We will actually prove the finer result that if $w(n, k)$ is the number of involutions in $\sum_n$ with k two cycles then

$$w(n + p^r, k) \equiv w(n, k) \pmod{p^r}. \tag{7.1}$$

Note that (7.1) implies by an easy induction that

$$w(np^r, k) \equiv 0 \pmod{p^r} \tag{7.2}$$

for $k \geqslant 1$.

When $r = 1$, the action of C_p stabilizes only involutions of the form (1)(2)$\cdots$(p)τ, where τ is an involution of $p + [n]$ (since $p \geqslant 3$, the cycle $(1, 2, \ldots, p)^j$, $1 < j < p$, is not an involution). Hence $w(n+p, k) \equiv w(n, k) \pmod{p}$.

Considering the action of $G = C_{p^r}$ on $\sum_{n+p^r}$ we see that G's subgroup H_1 of order p stabilizes involutions of the form $\sigma \cdot \tau$, where σ is an involution of $[p^r]$ and τ is an involution of $p^r + [n]$. Since H_1 stabilizes σ, σ itself induces an involution $\bar{\sigma}$ on the p^{r-1} cycles of H_1. If $\bar{\sigma}$ has i cycles of length two then there are p^i different involutions of $[p^r]$ that induce $\bar{\sigma}$, giving $w(p^{r-1}, i) \cdot p^i$ choices for σ. Since σ must have $p \cdot i$ two-cycles there are $w(n, k - pi)$ choices for τ and so (3.6) yields

$$w(n + p^r, k) \equiv \sum_i w(n, k - pi) \cdot w(p^{r-1}, i) \cdot p^i \pmod{p^r}.$$

However by induction on r and Eq. (7.2), we have $p^{r-1+i} | w(p^{r-1}, i)\, p^i$ for $i \geqslant 1$ so this term is zero mod p^r if $i \neq 0$. Hence (7.1) follows. ∎

As an immediate corollary we have

(62) If m is odd, then

$$v(n + m) \equiv v(n) \pmod{m}.$$

Applying the action of C_2^r and arguments similar to those in the proof of (61) we obtain

(63) If $n \geqslant 4r - 2$ then

$$v(n) \equiv 0 \pmod{2^r}.$$

In a like manner, results can be derived for the number of permutations in $\sum_n$ whose dth power is the identity. These congruences have been derived using different techniques by Chowla, Herstein, and Scott [8] and Moser and Wyman [26].

C. *Derangements and the Cycle Indicator*

Another subset of Σ_n that is often studied is the set of derangements [30, 33]. A *derangement* is a permutation of $[n]$ having no fixed points. Hence conjugation also leaves the set of derangements invariant.

Let $d(n)$ be the number of derangements of $[n]$ and consider the action of C_p. Since $1, 2, \ldots, p$ can no longer be fixed points (cf. Eq. (12)) we have

$$d(n+p) \equiv (p-1)\, d(n) \pmod{p}$$
$$\equiv -d(n) \pmod{p}.$$

As in the case of involutions, similar considerations with products of the C_{p^r} for different prime powers lead to

$$(64) \quad d(n+m) \equiv (-1)^m\, d(n) \pmod{m}.$$

One can obviously use these methods to obtain congruences for any set of permutations having the same cycle structure. In terms of generating functions, associate with each $\sigma \in \Sigma_n$ the monomial

$$\sigma(\mathbf{x}) = \sigma(x_1, x_2, \ldots, x_n) := x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

where i_j is the number of cycles of length j in σ. Define the nth *cycle indicator polynomial* by $c_n(\mathbf{x}) := \sum_{\sigma \in \Sigma_n} \sigma(\mathbf{x})$. In this notation we have $v(n) = c_n(1, 1, 0, \ldots, 0)$ and $d(n) = c_n(0, 1, 1, \ldots, 1)$. It has been noted by Riordan [30] that

$$c_{n+m}(\mathbf{x}) \equiv c_n(\mathbf{x}) \cdot c_m(\mathbf{x}) \pmod{m}$$

and Gessel [12] has given a proof using group actions on graphs. It is also possible to prove this using our techniques, but we leave the details to the reader.

8. Comments and Questions

Several observations and queries about the methods we have introduced are in order.

(A) It should now be apparent that a large number of congruences follow from Corollary 3. Are there other results from the literature that can be obtained in this way? It seems likely that many of the sequences in Sloane's handbook [37] could be so analyzed.

(B) The use of group actions helps to explain why binomial coefficients and Stirling numbers of both kinds satisfy similar recurrence relations modulo p (compare Eqs. (1), (6), and (12)). Instead of applying ad hoc techniques in each case, we are able to give a unified treatment to several seemingly unrelated congruences.

(C) One of the problems that can arise is finding the appropriate

action. Two important examples are generalized Euler permutations and integer partitions.

A *generalized Euler permutation* of $[pn]$ is a sequence $a_1, a_2, \ldots, a_{pn}$ such that $a_i > a_{i+1}$ precisely when p divides i. Congruences for the number of generalized Euler permutations have been proved by Gessel [11], Leeming and MacLeod [23], and Stevens [39]. Gessel [12] has found an action for C_p on these permutations but it does not extend immediately to other abelian groups.

The number of ways of writing n as a sum of positive integers denoted $p(n)$ is called the number of integer partitions of n. The function $p(n)$ has many interesting arithmetic properties which have been studied by Ramanujan [29, Paper 25], Knopp [21] and others. In contrast to set partitions, however, it is not even obvious how to let the group C_p act on integer partitions.

(D) In order to obtain better congruences it is often necessary to employ more complicated groups. Unfortunately this makes it harder to compute with the full lattice of subgroups. One can instead use the period sublattice described by Rota and Sagan [32], but this is only possible when counting functions under the usual Polya action [28]. Are there other sublattices which yield interesting results?

(E) In Section 6 we were able to give congruences for the classical Möbius function by picking the appropriate group. Specialization to the period lattice also gives congruences for Euler's phi-function. Perhaps one can also investigate the arithmetic properties of other number theoretic functions, e.g., τ and λ, in this setting.

References

1. G. E. Andrews, "The Theory of Partitions," Vol. 2, Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, Mass., 1976.
2. H. W. Becker and J. Riordan, The arithmetic of Bell and Stirling numbers, *Amer. J. Math.* **70** (1948), 385–394.
3. E. T. Bell, The iterated exponential integers, *Ann. of Math.* **39** (1938), 539–557.
4. E. T. Bell, Generalized Stirling transforms of sequences, *Amer. J. Math.* **61** (1939), 89–101.
5. L. Carlitz, Congruences for generalized Bell and Stirling numbers, *Duke Math. J.* **22** (1955), 193–205.
6. L. Carlitz, Some congruences for the Bell polynomials, *Pacific J. Math.* **11** (1961), 1215–1222.
7. S. Chowla, I. N. Herstein, and W. K. Moore, On recurrences connected with symmetric groups I, *Canad. J. Math.* **3** (1951), 328–334.
8. S. Chowla, I. N. Herstein, and W. R. Scott, The solution of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk.* **25** (1952), 29–31.

9. L. E. DICKSON, "History of the Theory of Numbers," Vol. 1, Carnegie Inst. Washington, D.C., 1919.
10. I. M. GESSEL, Congruences for Bell and tangent numbers, *Fibonacci Quart.* **11** (1981), 137–144.
11. I. M. GESSEL, Some congruences for generalized Euler numbers, preprint.
12. I. M. GESSEL, Combinatorial proofs of congruences, preprint.
13. I. J. GOOD, The number of orderings of n candidates when ties are permitted, *Fibonacci Quart.* **13** (1975), 11–18.
14. O. A. GROSS, Preferential arrangements, *Amer. Math. Monthly* **69** (1962), 4–8.
15. H. GUPTA, "Symmetric Functions in the Theory of Integral numbers," Lucknow Univ. Stud., Lucknow, 1940.
16. M. HALL, Arithmetic properties of a partition function, *Bull. Amer. Math. Soc.* **40** (1934), Abstract 200.
17. G. H. HARDY AND E. M. WRIGHT, "An Introduction to the Theory of Numbers," Oxford Univ. Press, Oxford, 1938.
18. S. A. JONI, G.-C. ROTA, AND B. SAGAN, From sets to functions: Three elementary examples, *Discrete Math.* **37** (1981), 193–202.
19. G. S. KAZANDZIDIS, Congruences on the binomial coefficients, *Bull. Soc. Math. Grèce* **9** (1968), 1–12.
20. G. S. KAZANDZIDIS, On congruences in number theory, *Bull. Soc. Math. Grèce* **10** (1969), 35–40.
21. M. I. KNOPP, "Modular Functions in Analytic Number Theory," Markham, Chicago, 1970.
22. J. L. LAGRANGE, Œuvres iii. 425, *Nouveaux mémoires de l'Académie royale de Berlin* **2** (1773), 125.
23. D. J. LEEMING AND R. A. MACLEOD, Some properties of generalized Euler numbers, *Canad. J. Math.* **33** (1981), 606–617.
24. E. LUCAS, Sur les congruences des nombres euleriens et des coefficients différentiels des fonctions trigonométriques suivant un module premier, *Bull. Soc. Math. France* **6** (1877–8), 49–54.
25. W. F. LUNNON, P. A. B. PLEASANTS, AND N. M. STEPHENS, Arithmetic properties of Bell numbers to a composite modulus I, *Acta Arith.* **35** (1979), 1–16.
26. L. MOSER AND M. WYMAN, On solutions to $x^d = 1$ in symmetric groups, *Canad. J. Math.* **7** (1955), 159–168.
27. J. PETERSON, Beviser for Wilsons og Fermats Theoremer, *Tidsskrift for Mathematik* **2** (1872), 64–65.
28. G. POLYA, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen, *Acta Math.* **68** (1937), 145–254.
29. S. RAMANUJAN, "Collected Papers of S. Ramanujan," Cambridge Univ. Press, London/New York, 1927.
30. J. RIORDAN, "An introduction to Combinatorial Analysis," Wiley, New York, 1968.
31. G.-C. ROTA, On the foundations of combinatorial theory. I. Theory of Möbius functions, *Z. Wahrsch. Theorie* **2** (1964), 340–368.
32. G.-C. ROTA AND B. E. SAGAN, Congruences derived from group action, *European J. Combin.* **1** (1980), 67–76.
33. H. J. RYSER, "Combinatorial Mathematics," Carus Mathematical Monograph No. 14, Math. Ass. of America, Washington, D.C., 1973.
34. D. SINGMASTER, Notes on binomial coefficients I—A generalization of Lucas' congruence, *J. London Math. Soc.* (*2*) **8** (1974), 545–548.
35. D. SINGMASTER, Notes on binomial coefficients II—The least n such that p^e divides an r-nomial coefficient of rank n, *J. London Math. Soc.* (*2*) **8** (1974), 549–554.

36. D. SINGMASTER, Notes on binomial coefficients III—Any integer divides almost all binomial coefficients, *J. London Math. Soc.* (*2*) **8** (1974), 555–560.
37. N. J. A. SLOANE, "A Handbook of Integer Sequences," Academic Press, New York, 1973.
38. J. H. SMITH, Combinatorial congruences derived from the action of Sylow subgroups of the symmetric group, preprint.
39. H. STEVENS, Generalized Kummer congruences for the products of sequences and applications, *Duke Math. J.* **28** (1961), 261–275.
40. J. TOUCHARD, Propriétés arithmétiques de certains nombres recurrent, *Ann. Soc. Sci. Bruxelles* **53** (1933), 21–31.
41. J. TOUCHARD, Nombres exponentials et nombres de Bernoulli, *Canad. J. Math.* **8** (1956), 305–320.