Combinatorial Proofs of Congruences

Ira M. Gessel[1]

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139

Abstract

Congruences are found for sequences of integers which count labeled objects. A finite group acts on a set of digraphs, and the congruence is found by counting digraphs which lie in orbits of size divisible by the modulus.

1. Introduction

A frequently rediscovered proof in number theory is the combinatorial proof of Fermat's congruence $a^p \equiv a \pmod{p}$ for p prime: We take a wheel with p spokes and color each in one of a colors, so that there are a^p possible colorings of the wheel. We call two colorings equivalent if one can be obtained from the other by spinning the wheel. Then each equivalence class contains p colorings except those which consist of a single monochromatic coloring. There are a of these, and the congruence follows.

According to Dickson's *History of the Theory of Numbers* [31, p.75], this proof was first given by J. Petersen in 1872 in [53]. Petersen also found a similar proof of Wilson's congruence $(p-1)! \equiv -1 \pmod{p}$.

The method of proving congruences through actions of finite groups is a fruitful one which has not been seriously studied until recently. Examples of congruences derived from group actions have been given by Aigner [1], James and Kerber [42, pp. 237-239], Moser and Wyman [51], Radoux [56], Chao [27], and others. Systematic applications of group actions to congruences have been given in the recent work of Rota and Sagan [62], Smith [64], and Sagan [63], who

[1] Partially supported by NSF Grant MCS 3105188

ISBN 0-12-179120-0

studied congruences for binomial coefficients, Stirling numbers, and related numbers. Pleasants [54] has used group actions to derive congruences for Bell numbers.

In the present work we study congruences for sequences of integers (or polynomials with integer coefficients) which arise in counting labeled objects, usually represented as graphs or digraphs. Many of these sequences can be defined by exponential generating functions, such as e^{e^x-1} (Bell numbers), $(2-e^x)^{-1}$, e^{te^x}, and $\exp[\sum_{n=1}^{\infty} t_n \frac{x^n}{n}]$ (cycle indicator polynomials). Related work on congruences of the type we consider here for these and other sequences has been done by Kummer [46], Hurwitz [41], Touchard [70], [71], Carlitz [4]-[23], Stevens [65]-[69], Lunnon, Pleasants, and Stephens [50], and others.

One of the advantages of the combinatorial approach is that an explicit formula or generating function is not needed. Thus we can find congruences for labeled objects such as d-regular graphs, k-line Latin rectangles, and partial orders, where explicit formulas are not known. In addition, we find better congruences than those known in many cases. For example, there are a number of congruences in the literature of the form

$$\sum_{i=0}^{r} \binom{r}{i} u^{r-i} a_{n+pi} \equiv 0 \pmod{p^{\lceil r/2 \rceil}}.$$

In Section 10 we show how the exponent $\lceil r/2 \rceil$ can always be improved for $p > 2$.

We shall assume that the reader is familiar with the combinatorial interpretation of multiplication and composition of exponential generating functions, as described, for example, in Harary and Palmer [39, Chapter 1]. For a more formal development of the theory of exponential generating functions, see Joyal [44] and the references cited there.

2. Notation and Definitions

Let Γ be a digraph (directed graph). The *components* of Γ are the components of its underlying graph. If V is a set of vertices of Γ, $\Gamma(V)$ is the induced subdigraph on V, that is, V together with all arcs joining vertices in V. An arc of Γ with only one end in V is called an *external arc* of $\Gamma(V)$. Two sets of vertices in Γ are *adjacent* if there is an arc from one to the other.

We shall represent an undirected graph by a digraph in which each edge corresponds to a pair of oppositely directed arcs between two points.

If a group G acts on a set S, the *stabilizer* of s in S is $G_s = \{g \in G | gs = s\}$. We write $O(s) = O_G(s)$ for the orbit of s under G. It is well known that $|G| = |G_s| \cdot |O(s)|$. The identity element of G is denoted by e. We write $[n]$ for $\{1,2,\ldots,n\}$ and $m + [n]$ for $\{m + 1, m + 2, \ldots, m + n\}$, with $[0]$ the empty set. We write $\lfloor \alpha \rfloor$ for the greatest integer not greater than α and $\lceil \alpha \rceil$ for the least integer not less than α.

We always use p to denote a prime. A rational number is *p-integral* if its denominator is not divisible by p. A polynomial is p-integral it its coefficients are.

3. Congruences from Group Actions

The basic idea of this paper is the following: Let S be a finite set and let w be a weight on S whose value is always an integer or a polynomial with integer coefficients. Let G be a group which acts on S and preserves weights. Let m be a positive integer and let T be a subset of S on which G acts such that under the action of G, every element of T lies in an orbit of size divisible by m. Then $\sum_{t \in T} w(t) \equiv 0 \pmod{m}$.

For our applications of this very general principle, we shall be much more specific. We start with a finite group G acting on $[m]$. Then G acts in a natural way on labeled objects with label set $[m + n]$, and in particular on digraphs with vertex set $[m + n]$, for any $n \geq 0$.

Now we take a weighted set of digraphs on $[m + n]$ on which G acts, and sum the weights of digraphs in orbits of specified sizes to get congruences.

All the weights we use will be *multiplicative*, that is, the weight of a digraph is the product of the weights of its components.

4. Cyclic Groups

In this section we take G to be the cyclic group C_m on $[m]$ generated by the m-cycle $(1,2,\ldots,m)$. We define the degree of a digraph to be the maximum indegree or outdegree of any vertex, with loops not counted and multiple arcs counted only once.

LEMMA 4.1. Let Γ be a digraph on $[m + n]$ with degree at most d. Let l be the least common multiple of all divisors of m not greater than d. If $[m]$ is adjacent to $m + [n]$ then $|O(\Gamma)|$ is a multiple of m/l.

PROOF. Suppose the arc (i,j) is in Γ with i in $[m]$ and j in $m + [n]$. (The same argument works for (j,i).) Then for any g in G_Γ, the arc (gi,j) is in Γ. Thus $|G_\Gamma| \leq d$, so $|G_\Gamma|$ divides l and the lemma follows.

THEOREM 4.2. Let D be a class of digraphs such that:

(i) Membership in D depends only on isomorphism type.

(ii) A digraph is in D if and only if its components are.

(iii) Every digraph in D has degree at most d.

Suppose that a (multiplicative) weight is defined on D. Let a_n be the sum of the weights of the digraphs on $[n]$ in D. (As usual, $a_0 = 1$.) Then for any $n \geq 0$, $m \geq 1$,

$$a_{m+n} \equiv a_m a_n \pmod{m/l}, \tag{4.1}$$

where l is the least common multiple of all divisors of m not greater than d.

PROOF. The sum of the weights of the digraphs on $[m + n]$ in D with $[m]$ not adjacent to $m + [n]$ is $a_m a_n$, so $a_{m+n} - a_m a_n$ counts a set of digraphs to which Lemma 4.1 applies, and the theorem follows.

Note that if b_n is the sum of the weights of the connected digraphs on $[n]$ in D, then

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \exp\left[\sum_{n=1}^{\infty} b_n \frac{x^n}{n!}\right] \tag{4.2}$$

by the "exponential formula" [39, p.8].

The simplest case of Theorem 4.2 is that in which D is the set of digraphs in which every vertex has indegree 1 and outdegree 1, so that each component is a directed cycle. We call these digraphs *cycle digraphs*. We assign the weight t_i to a cycle of length i, and we write $c_n(\mathbf{t}) = c_n(t_1, t_2, \ldots, t_n)$ for a_n in this case. Since the coefficient of $t_1^{k_1} \cdots t_n^{k_n}$ in $c_n(\mathbf{t})$ is the number of permutations of $[n]$ with k_i cycles of length i, $c_n(\mathbf{t})$ is called the *cycle indicator* of the symmetric group [60, p.68]. A table of $c_n(\mathbf{t})$ can be found in [60, p.69].

Since there are $(n-1)!$ cycles on $[n]$, (4.2) becomes

$$\sum_{n=0}^{\infty} c_n(\mathbf{t}) \frac{x^n}{n!} = \exp\left[\sum_{n=1}^{\infty} t_n \frac{x^n}{n}\right] \tag{4.3}$$

and (4.1) becomes

$$c_{m+n}(\mathbf{t}) \equiv c_m(\mathbf{t}) c_n(\mathbf{t}) \pmod{m}. \tag{4.4}$$

There are several specializations of $c_n(\mathbf{t})$ which are of particular interest. Congruences for some of these, which are all special cases of (4.4), have been given by Riordan [60, pp. 80-89].

If we set each t_i equal to t then (4.3) becomes

$$\sum_{n=0}^{\infty} c_n(\mathbf{t})\frac{x^n}{n!} = \exp\left[t \log\frac{1}{1-x}\right] = (1-x)^{-t},$$

so

$$c_n(\mathbf{t}) = t(t+1)\cdots(t+n-1) = \sum_{k=0}^{n}(-1)^{n-k}\, s(n,k)t^k,$$

where $s(n,k)$ is the Stirling number of the first kind.

If we set $t_1 = 0$ and $t_i = 1$ for $i > 1$, we have the derangement numbers d_n,

$$\sum_{n=0}^{\infty} d_n\frac{x^n}{n!} = \frac{e^{-x}}{1-x}.$$

The polynomials obtained from $c_n(\mathbf{t})$ by setting $t_i = 0$ for $i > 2$ are essentially Hermite polynomials, which may be defined by $H_n(t) = c_n(2t,-2) = c_n(2t,-2,0,0,\ldots)$. Congruences for Hermite polynomials have been studied by Carlitz [8], [15] and Stevens [60]. The special case of (4.4) for $c_n(1,1)$ was found by Chowla, Herstein, and Moore [28], and by Moser and Wyman [51].

Chowla, Herstein, and Scott [29] and Moser and Wyman [51] also studied the numbers $c_n(\mathbf{t})$ where $t_i = 1$ if i divides d and $t_i = 0$ otherwise. These numbers count permutations whose dth power is the identity.

The Laguerre polynomials $L_n^{(\alpha)}(t)$ may be defined by

$$(1-x)^{-\alpha-1}\, e^{tx/(x-1)} = \sum_{n=0}^{\infty} \Lambda_n^{(\alpha)}(t)\frac{x^n}{n!}, \text{ where } \Lambda_n^{(\alpha)}(t) = n!\, L_n^{(\alpha)}(t).$$

It is straightforward to check that

$$\Lambda_n^{(\alpha)}(t) = c_n(\alpha+1-t,\ \alpha+1-2t,\ \ldots,\ \alpha+1-nt).$$

Congruences for the $\Lambda_n^{(\alpha)}(t)$ have been found by Carlitz [8], [15].

Carlitz [7], [16] gave congruences for the numbers $g_n = c_n(0,0,\frac{1}{2},\frac{1}{2},\ldots,)$ which count graphs in which every vertex has degree 2. Since we represent these by digraphs of degree 2, Theorem 4.2 gives Carlitz's congruence [7]

$$g_{m+n} \equiv g_m g_n \pmod{m_0},$$

where $m_0 = m$ if m is odd and $m_0 = m/2$ if m is even.

As another example, consider the polynomials $v_n(t_1,\ldots,t_{k+1})$ defined by

$$\sum_{n=0}^{\infty} v_n(\mathbf{t}) = \exp[\sum_{n=1}^{k+1} t_n \frac{x^n}{n!}]. \tag{4.5}$$

Then $v_n(\mathbf{t})$ counts graphs on $[n]$ in which each component is a complete graph with at most $k+1$ vertices, where a complete graph with i vertices is weighted t_i. By Theorem 4.2,

$$v_{m+n}(\mathbf{t}) \equiv v_m(\mathbf{t})v_n(\mathbf{t}) \pmod{m/l}, \tag{4.6}$$

where l is the least common multiple of the divisors of m not greater than k.

5. Groups of Prime Order

Theorem 4.2 does not apply to digraphs in which the degrees are not bounded. But it is easy to find congruences to a prime modulus without a degree restriction. (We shall consider prime-power moduli later.) Suppose G is a p-group acting on a set. Then since the size of any orbit is a power of p, anything not fixed by G lies in an orbit of size divisible by p. So to obtain a mod p congruence, we need only count fixed points under G. In this section we consider the action of the cyclic group C_p.

We illustrate the situation by a somewhat trivial example, the case of all graphs. The number of graphs on $[n]$ is $2^{\binom{n}{2}}$. A graph Γ on $[p+n]$ is fixed by C_p if and only if:

(i) Each vertex in $[p]$ has the same set of neighbors in $p + [n]$,

and

(ii) $\Gamma([p])$ is fixed by C_p.

To determine such a graph we pick an arbitrary graph Γ' on $[1+n]$ and a graph Γ'' on $[p]$ which is fixed by C_p. (We call such a graph a *p-graph.*) To obtain Γ we first relabel each vertex i in Γ' as $i+p-1$, getting a new graph $\overline{\Gamma}'$ on $\{p, p+1, \ldots, p+n\}$. Then we obtain Γ by removing vertex p from $\overline{\Gamma}'$, and adding Γ'', together with an edge from each vertex of Γ'' to each neighbor of p in $\overline{\Gamma}'$.

It is easy to see that Γ' and Γ'' are uniquely determined by Γ. We call Γ' the *contracted graph* of Γ and Γ'' the *p-graph* of Γ.

Now the contracted graph of Γ can be chosen in $2^{\binom{n+1}{2}}$ ways. If p is odd, a p-graph can be chosen in $2^{(p-1)/2}$ ways, since it is determined by choosing an arbitrary subset of the edges joining 1 to $2, 3, \ldots, (p+1)/2$. (If $p = 2$ there are 2 choices for a p-graph.) Thus

we find the congruences

$$2^{\binom{n+p}{2}} \equiv 2^{(p-1)/2}\, 2^{\binom{n+1}{2}} \pmod{p},\ p \text{ odd}$$

$$2^{\binom{n+2}{2}} \equiv 0 \pmod{2}.$$

A more interesting example is that of connected graphs. For Γ to be connected, the contracted graph must be connected, and the p-graph may be arbitrary, except that if the contracted graph has only one vertex the p-graph must be connected. Thus if s_n is the number of connected graphs on $[n]$, for p odd we have

$$s_{n+p} \equiv 2^{(p-1)/2}\, s_{n+1} \pmod{p},\ n > 0 \tag{5.1}$$

$$s_p \equiv 2^{(p-1)/2} - 1 \pmod{p},$$

and for $p = 2$ we have $s_{n+2} \equiv 0 \pmod{2}$ with $s_2 = 1$.

Another important example is that of the Bell numbers. The Bell number B_n is the number of partitions of $[n]$, or equivalently the number of graphs on $[n]$ in which every component is a complete graph. The Bell numbers have the generating function $\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}$. Congruences for them have been studied by many authors [2], [3], [10], [32], [34], [48], [50], [56], [57], [70], [71], [72].

In a "Bell number graph" on $[p + n]$ fixed by C_p, the p-graph must be either an edgeless graph or a complete graph. If the p-graph is edgeless, then the contracted graph can have no edges from 1 to $1 + [n]$, so these graphs are counted by B_n. If the p-graph is complete, the contracted graph may be any graph counted by B_{n+1}. Thus we recover Touchard's congruence [70]

$$B_{n+p} \equiv B_n + B_{n+1} \pmod{p}. \tag{5.2}$$

More generally, the analysis just given holds if we weight a component of size i by t_i, provided that $t_{i+p} \equiv t_{i+1} \pmod{p}$ for $i \geq 0$. Here the generating function is

$$\sum_{n=0}^{\infty} B_n(\mathbf{t}) \frac{x^n}{n!} = \exp\Big[\sum_{n=1}^{\infty} t_n \frac{x^n}{n!}\Big] \tag{5.3}$$

and the congruence is

$$B_{n+p}(t) \equiv t_1^p B_n(t) + B_{n+1}(t) \pmod{p}. \tag{5.4}$$

If we drop the condition $t_{i+p} = t_i$ we obtain a more complicated congruence: we get a separate term for each possible size of the component of the contracted graph containing 1. The congruence is

$$B_{n+p}(t) \equiv t_1^p B_n(t) + \sum_{i=0}^{n} \binom{n}{i} t_{i+p} B_{n-i}(t) \pmod{p}, \tag{5.5}$$

due to Carlitz [20].

We now give two examples where the objects counted are not digraphs, although they can be represented as digraphs.

First let q_n be defined by $\sum_{n=0}^{\infty} q_n \frac{x^n}{n!} = (2-e^x)^{-1}$. These numbers were apparently first studied by Cayley [26]. They count "ordered partitions" of sets: q_n is the number of sequences $(T_1, \ldots, T_k)$ of nonempty disjoint sets whose union is $[n]$. The action of C_p on $[p]$ extends in a natural way to an action on the ordered partitions of $[p+n]$. The ordered partitions of $[p+n]$ fixed by C_p are those in which $[p]$ is contained in a single block. There are q_{n+1} of these, so $q_{n+p} \equiv q_{n+1} \pmod{p}$.

Congruences for the q_n have been studied by Touchard [70], Gross [38], Kauffman [45], Neumann [52], and Good [36]. Kummer's method [46] applies to them, although he did not consider them explicitly.

Next, for fixed p let e_n be defined by

$$\sum_{n=0}^{\infty} e_n \frac{x^{pn}}{(pn)!} = \left[\sum_{n=0}^{\infty} (-1)^n \frac{x^{pn}}{(pn)!}\right]^{-1}.$$

Carlitz [24] showed that e_n is the number of permutations $a_1 a_2 \cdots a_{pn}$ of $[pn]$ such that $a_i > a_{i+1}$ if and only if p divides i. Let E_n be the set of these permutations.

Now the obvious action of C_p on permutations does not take E_{n+1} to itself, but a modified action does: Given π in E_{n+1} and g in C_p, first replace each element of $[p]$ in π by its image under g. The resulting permutation π' need not be in E_{n+1}. Let us call the segments $a_{pj+1} a_{pj+2} \cdots a_{(p+1)j}$ of a permutation $a_1 a_2 \cdots a_n$ its *blocks*. Then we obtain g by rearranging each block of π' in increasing order. It is easy to check that this defines an action of C_p on E_{n+1}. The fixed permutations are those in which $[p]$ constitutes a block. But if this is the case, $[p]$ must be the last block. Thus these fixed permutations are

equinumerous with E_n and we have the congruence $e_{n+1} \equiv e_n \pmod{p}$, so since $e_0 = e_1 = 1$, $e_n \equiv 1 \pmod{p}$ for all n.

The stronger congruences $e_n \equiv 1 \pmod{p^2}$ for all primes p and $e_n \equiv 1 \pmod{p^3}$ for $p \geq 5$ are proved in Gessel [35]. Other congruences for these numbers have been given by Carlitz [9], Stevens [66], Leeming and MacLeod [47], and Gessel [35].

6. Cyclic p-Groups

We now consider the action of the cyclic group C_{p^k}. Since the size of any orbit under C_{p^k} is either 1 or a multiple of p, we obtain a mod p congruence by counting fixed digraphs, just as in the last section.

If we have a congruence $a_{n+p} \equiv ua_{n+1} \pmod{p}$ or $a_{n+p} \equiv ua_n \pmod{p}$ then the congruence for a_n that we would get from the action of C_{p^k} is more easily obtained directly from the congruence for C_p. The congruences for Bell numbers and Bell polynomials are more interesting; we leave it to the reader to derive Touchard's generalization of (5.2) [70]:

$$B_{n+p^k} \equiv k\,B_n + B_{n+1} \pmod{p} \tag{6.1}$$

and Carlitz's generalization of (5.5) [22]:

$$B_{n+p^k}(\mathbf{t}) \equiv \sum_{i=0}^{k-1} t_{p^i}^{p^{k-i}}\, B_n(\mathbf{t}) + \sum_{i=0}^{n} \binom{n}{i} t_{i+p^k} B_{n-i}(\mathbf{t}) \pmod{p}. \tag{6.2}$$

For an example of a somewhat different nature, let U_n be the set of graphs on $[n]$ in which every component is a rooted tree and every non-root is adjacent to a root. These graphs are equivalent to the "idempotent mappings" considered by Harris and Schoenfeld [40]. Let the coefficient of t^i in $u_n(t)$ be the number of graphs in U_n with i components. Then

$$\sum_{n=0}^{\infty} u_n(T)\frac{x^n}{n!} = e^{txe^x}$$

and

$$u_n(t) = \sum_{i=0}^{n} t^i \binom{n}{i} i^{n-i}.$$

The graphs in U_{n+p} fixed by the action of C_p are of two types:

(i) those in which the elements of $[p]$ are isolated roots, and

(ii) those in which the elements of $[p]$ are not roots, but all lie in the same component.

The fixed graphs of type (i) are counted by $t^p u_n(t)$. Those of type (ii) can be found by taking a graph in U_n, adding p to each label, and joining the elements of $[p]$ to one of the roots. It follows that they are counted by $tu_n'(t)$. Thus we have the congruence

$$u_{n+p}(t) \equiv t^p u_n(t) + tu_n'(t) \pmod{p}, \tag{6.3}$$

as found by Riordan [61]. (A congruence equivalent to the case $t = 1$ was found by Harris and Schoenfeld [40].)

To find a congruence for $u_n(t)$ that does not involve derivatives, we consider the action of C_{p^2} on U_{p^2+n}, and we find as before,

$$u_{n+p^2}(t) \equiv t^{p^2} u_n(t) + t\, u_n'(t) \pmod{p}, \tag{6.4}$$

so from (6.3) we have

$$u_{n+p^2}(t) - u_{n+p}(t) \equiv (t^{p^2} - t^p)u_n(t) \pmod{p}. \tag{6.5}$$

If we set $t = 1$, this reduces to

$$u_{n+p^2}(1) \equiv u_{n+p}(1) \pmod{p}. \tag{6.6}$$

A *cutpoint* of a graph is a vertex whose removal increases the number of components. A *block* is a connected graph with no cutpoints. Let b_n be the number of blocks on $[n]$. (The value of b_n for $n \leq 2$ is not important.) An implicit generating function for b_n can be found in Harary and Palmer [39, p.10].

Suppose p is odd. For a block Γ on $[p + n]$ to be fixed by C_p for $n \geq 2$, the p-graph of Γ may be arbitrary, and the contracted graph of Γ may be any block or any graph on $[1 + n]$ in which 1 is the only cutpoint. Thus if r_n is the number of graphs on $[n]$ with no cutpoints except possibly 1, then

$$b_{n+p} \equiv 2^{(p-1)/2} r_{n+1} \pmod{p}, \quad n \geq 2 \tag{6.7}$$

We find easily that $b_p \equiv b_{p+1} \equiv 2^{(p-1)/2} - 1 \pmod{p}$, since here the p-graph must be a block.

Similarly we find that $b_{n+p^2} \equiv 2^{(p^2-1)/2} r_{n+1} \pmod{p}$, $n \geq 2$. Now $2^{(p^2-1)/2} = (2^{p-1})^{(p+1)/2} \equiv 1 \pmod{p}$, so we obtain

$$b_{n+p^2} \equiv 2^{(p-1)/2} b_{n+p} \pmod{p}, \quad n \geq 2. \tag{6.8}$$

We leave it to the reader to verify that (6.8) holds for all $n \geq 0$, and that b_n is odd for $n \geq 4$.

One can also use the action of C_p^k to find mod p^k congruences, by counting digraphs which are fixed only by the identity. Since C_p^k has a unique minimal nontrivial subgroup generated by g, where $g(i) \equiv i + p^{k-1} \pmod{p^k}$, we need only count digraphs fixed by g. We obtain in this way the congruence $q_{n+p^k} \equiv q_{n+p^{k-1}} \pmod{p^k}$ of Touchard [70] for the number of ordered partitions. However, we shall see in Section 11 a more general method for congruences of this type.

7. A Kummer Congruence

If a group G acts on $[m]$, then the product $G^r = G \times G \times \cdots \times G$ acts on $[rm]$ in natural way: the ith copy of G acts on $(i-1)m + [m]$ as a translation of the action of G on $[m]$.

Let us consider the action of C_p^r on ordered partitions of $[rp + n]$. For $r = 1$ we saw that the ordered partitions of $[p + n]$ in orbits of size p under C_p are the ones in which $[p]$ is not contained in a block, and these are $q_{n+p} - q_{n+1}$ in number. Similarly, the ordered partitions of $[rp + n]$ in orbits of size p^r under C_p^r are those in which no set $(i-1)p + [p]$ is contained in a block for any i in $[r]$. These can be counted by inclusion-exclusion; however, we shall use a different approach which generalizes more easily. For another approach, using Möbius inversion, see Sagan [63].

For any infinite sequence $\{a_n\}$, the shift operator E is defined by $Ea_n = a_{n+1}$. (E will always act on the variable n.) Thus the number of ordered partitions of $[2p + n]$ in which $[p]$ is not contained in a block is $(E^p - E)q_n$. By the same contraction argument we used before, the number of partitions of $[2p+n]$ in which $[p]$ is not contained in a block, but $p+[p]$ is contained in a block, is $(E^p - E)q_{n+1}$. Thus the number of ordered partitions of $[2p + n]$ in which neither $[p]$ nor $p + [p]$ is contained in a block, is

$$(E^p - E)(q_{n+p} - q_{n+1}) = (E^p - E)^2 q_n \equiv 0 \pmod{p^2}.$$

Similarly we find the congruence $(E^p - E)^r q_n \equiv 0 \pmod{p^r}$, or equivalently,

$$\sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} q_{n+i(p-1)} \equiv 0 \pmod{p^r},\ n \geq r. \tag{7.1}$$

If we had weighted a block of size i by t_i, our generating function would have been

$$\sum_{n=0}^{\infty} q_n(\mathbf{t})\frac{x^n}{n!} = [1 - \sum_{n=1}^{\infty} t_n \frac{x^n}{n!}]^{-1}.$$

If $t_{n+p} = at_{n+1}$ for all $n \geq 0$ then the argument given above applies, and we obtain

$$(E^p - aE)^r q_n(\mathbf{t}) \equiv 0 \pmod{p^r}. \tag{7.2}$$

Congruences of this form are often called Kummer congruences, after Kummer's congruences for the Bernoulli and Euler numbers [46]. (Kummer's congruence for Euler numbers is obtained from (7.2) by setting $t_n = -1$ for n even and $t_n = 0$ for n odd, and taking p odd.)

Kummer congruences and their generalizations have been studied by Hurwitz [41], Carlitz [4] - [19], [21], Johnson [43], Stevens [65] - [69], and Gessel [35].

8. Products of Cyclic Groups

There are many congruences in the literature of the form

$$\sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} a_{n+im} a_m^{r-i} \equiv 0 \pmod{m^{\lceil r/2 \rceil}}.$$

See, for example, Carlitz [6] - [8], [15] - [18], [21], Johnson [43], and Stevens [68]. Some of these congruences can easily be explained by the action of C_m^r.

Let G be a group acting on $[m]$. Then G^r acts on $[rm]$. Let us write X_i for the set $(i-1)m + [m]$, where i is in $[r]$, and X_A for $\bigcup_{i \in A} X_i$. We call the sets X_i *sectors*. Let G_i be the copy of G in G^r which acts on X_i. If H is a subgroup of G^r, its *support* is the set $\{i \mid H \text{ acts nontrivially on } X_i\}$. For any subset A of $[r]$, we denote by G_A the subgroup of G^r generated by all G_i for i in A, and for any subgroup H of G^r, we write H_A for $H \cap G_A$. We call a nontrivial subgroup H of G *irreducible* if for any partition $\{A,B\}$ of its support, $H_A \times H_B$ as a subgroup of H is a proper subgroup.

A *component* of a subgroup H of G is an irreducible subgroup H_A of H such that $H = H_A \times H_{[r]-A}$. The components of H must have disjoint support since if H_A and H_B are components of H

$$\begin{aligned} H_B = H \cap H_B &= (H_A \times H_{[r]-A}) \cap H_B \\ &= H_{A \cap B} \times H_{([r]-A) \cap B} \end{aligned}$$

so A and B are either equal or disjoint.

THEOREM 8.1. Let H be any subgroup of G^r. Then H is the product of its components.

PROOF. If H is irreducible, it is a component. Otherwise H can be expressed as a nontrivial product $H_A \times H_B$. By induction, H_A and H_B are products of their components, so H is a product of some of its components. But since the supports of the components of H are disjoint, every component must appear in the product.

We now consider the case where G is C_m.

THEOREM 8.2. Let Γ be a digraph on $[rm + n]$ such that if k is in X_i and $i \neq j$, there are arcs from k to at most d elements of X_j. Let l be the least common multiple of all *proper* divisors of m not greater than d. Then the size of a component of $(C_m^r)_\Gamma$ with support A divides $l^{|A|-1}m$.

PROOF. Let H be a component of $(C_m^r)_\Gamma$ with support of size k. Without loss of generality we may assume that the support of H is $[k]$. Now the group C_m^i acts on $\Gamma(X_{[i]})$. Let H_i be the stablizer of $\Gamma(X_{[i]})$ in C_m^i, so that $H = H_k$.

We claim that, by permuting the X_j if necessary, we may assume that each H_i is irreducible. Clearly H_1 is irreducible. If, for some $i < k$, H_i is irreducible, but there is no j, $i < j \leq k$, such that the stablizer of $\Gamma(X_{[i]} \cup X_j)$ is irreducible, then H_i is a component of H, contradicting the irreducibility of H. Thus we may assume without loss of generality that H_{i+1} is irreducible.

Now H_i acts in a natural way on $X_{[i-1]}$. (Just ignore the action on X_i.) Since H_i must fix $\Gamma(X_{[i-1]})$, we have a homomorphism ϕ_i: $H_i \to H_{i-1}$. Thus $|H_i| = |\ker \phi_i| \cdot |\operatorname{im} \phi_i|$, so $|H_i|$ divides $|\ker \phi_i| \cdot |H_{i-1}|$ for $i > 1$. It will suffice to prove that $|\ker \phi_i|$ is a proper divisor of m and is at most d.

Now $\ker \phi_i$ is the subgroup of C_m acting on X_i which fixes $\Gamma(X_i)$. Since H_i is irreducible, $\ker \phi_i$ must be a proper subgroup of C_m. There must also be some $j < i$, and some a in X_j and b in X_i with an arc from a to b (or b to a). Then there must be an arc from a to every image of b under $\ker \phi_i$, so $|\ker \phi_i| \leq d$.

If Γ is a digraph on $[rm + n]$ and $A \subseteq [r]$ is the support of a component of G_Γ, we call $\Gamma(X_A)$ a *tube* of Γ of *length* $|A|$.

THEOREM 8.3. Suppose $G = C_m^r$ acts on a set D of digraphs satisfying the conditions of Theorem 8.2, such that for Γ in D, every tube of Γ has length at least 2. Then the sum of the weights of the elements of D is divisible by $(m/l)^{\lceil r/2 \rceil}$.

PROOF. By Theorem 8.2, if the tubes of Γ have lengths $a_1, \ldots, a_k$, where $\sum a_i \le r$, then $|G_\Gamma|$ divides $l^{r-k}m^k = l^r(m/l)^k$. Since $a_i \ge 2$, k is at most $\lfloor r/2 \rfloor$ so $|G_\Gamma|$ divides $l^r(m/l)^{\lfloor r/2 \rfloor} = l^{\lceil r/2 \rceil}m^{\lfloor r/2 \rfloor}$. Thus $|O(\Gamma)|$ is divisible by $m^r/l^{\lceil r/2 \rceil}m^{\lfloor r/2 \rfloor} = (m/l)^{\lceil r/2 \rceil}$.

We now apply Theorem 8.3 to the cycle indicator polynomial $c_n(\mathbf{t})$. An argument similar to that of section 7 for q_n shows that $[E^m - c_m(\mathbf{t})]^r c_n(\mathbf{t})$ counts cycle digraphs on $[rm + n]$ in which every $\Gamma(X_i)$ has an external edge in Γ. These digraphs satisfy the conditions of Theorem 8.3 with $l = 1$ and we obtain

$$[E^m - c_m(\mathbf{t})]^r c_n(\mathbf{t}) \equiv 0 \pmod{m^{\lceil r/2 \rceil}}, \tag{8.1}$$

as found by Carlitz [21].

We have the following generalization of Theorem 4.2:

THEOREM 8.4. Under the hypotheses of Theorem 4.2,

$$(E^m - a_m)^r a_n \equiv 0 \pmod{(m/l)^{\lceil r/2 \rceil}}. \tag{8.2}$$

If $m = p^k$, then l in Theorem 8.2 divides p^{k-1} for any d, so Theorem 8.3 gives a mod $p^{\lceil r/2 \rceil}$ congruence. Let us consider first the number s_n of connected graphs on $[n]$, and let p be odd. For $r > 1$, $(E^p - 2^{(p-1)/2}E)^r s_n$ is the number of connected graphs on $[rp + n]$ which are not fixed by any $(C_p)_i$, the copy of C_p acting on X_i. Thus the length of any tube of such a graph is at least 2, so by Theorem 8.3,

$$(E^p - 2^{(p-1)/2}E)^r s_n \equiv 0 \pmod{p^{\lceil r/2 \rceil}}. \tag{8.3}$$

For the Bell numbers B_n, $(E^p - E - 1)^r B_n$ is the number of partitions of $[rp + n]$ in which no sector consists of singletons or is contained in a block, and we have the congruence

$$(E^p - E - 1)^r B_n \equiv 0 \pmod{p^{\lceil r/2 \rceil}}, \tag{8.4}$$

as shown by Lunnon, Pleasants, and Stephens [50].

Similarly, for the number h_n of partial orders of $[n]$ we have the congruence

$$(E^p - E)^r h_n \equiv 0 \pmod{p^{\lceil r/2 \rceil}}. \tag{8.5}$$

The special case $h_p \equiv 1 \pmod{p}$ was found by Radoux [56].

For the polynomials $u_n(t)$ defined in section 6, we have the congruence

$$(E^{p^2} - E^p - t^{p^2} + t^p)^r u_n(t) \equiv 0 \pmod{p^{\lceil r/2 \rceil}}. \tag{8.6}$$

9. More on Tubes

In this section we find mod p^r congruences by counting digraphs which have trivial stabilizers under the action of C_p^r. We consider digraphs which can be decomposed nicely into tubes and digraphs with no tubes. More precisely, we want to work with the identity

$$\sum_{r=0}^{\infty} a_{n,r} \frac{x^r}{r!} = \exp\Big[\sum_{r=1}^{\infty} v_r \frac{x^r}{r!}\Big] \sum_{r=0}^{\infty} b_{n,r} \frac{x^r}{r!}, \tag{9.1}$$

where $a_{n,r}$ counts digraphs of a certain type on $[rp + n]$, $b_{n,r}$ counts digraphs of this type on $[rp + n]$ with no tubes, and v_r counts tubes of this type of length r.

Since $b_{n,r}$ counts digraphs with no tubes, $b_{n,r} \equiv 0 \pmod{p^r}$, and we can easily solve (9.1) for $b_{n,r}$:

$$\sum_{r=0}^{\infty} b_{n,r} \frac{x^r}{r!} = \exp\Big[-\sum_{r=1}^{\infty} v_r \frac{x^r}{r!}\Big] \sum_{r=0}^{\infty} a_{n,r} \frac{x^r}{r!}. \tag{9.2}$$

Thus equating coefficients in (9.1) gives the congruences we want.

Before we explain precisely the conditions under which (9.1) holds, we note that the simplest example is that in which $a_{n,r}$ is the cycle indicator $c_{n+rp}(\mathbf{t})$, v_r counts cycle digraphs of length r which are tubes, and $b_{n,r}$ counts cycle digraphs on $[rp + n]$ with no tubes.

In most applications of exponential generating functions, the coefficient of $\frac{x^m}{m!}$ counts a certain set of objects on the label set $[m]$. However, in (9.1) the coefficient of $\frac{x^r}{r!}$ counts a set of objects on the label set $[rp + n]$. We shall now give an informal and nonrigorous explanation of this more general use of exponential generating functions.

Suppose that $a(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$ and $b(x) = \sum_{n=0}^{\infty} b_n \frac{x^n}{n!}$ are exponential generating functions for classes A and B of labeled objects. Then the coefficient of $\frac{x^n}{n!}$ in $a(x)b(x)$ counts labeled objects γ which may be constructed as follows: Pick some k, with $0 \le k \le n$. Then pick an object α in A with label set $[k]$ and an object β in B with label set $[n - k]$. Pick a subset S of $[n]$ with $|S| = k$. Replace the labels of α in an order-preserving way by the elements of S to obtain $\tilde{\alpha}$ and construct $\tilde{\beta}$ analogously from $[n] - S$. Then γ is the ordered pair $(\tilde{\alpha}, \tilde{\beta})$. A similar construction is associated with exponentiation (or more

generally, composition) of exponential generating functions.

Now we consider a more general kind of labeled object, with two kinds of labels which we call "active labels" and "passive labels." We require that the set of active labels be $[k]$ for some k, but the passive labels may be arbitrary and need not be distinct. (We will want to allow a passive label to have the same "value" as an active label, but we must be able to distinguish between active and passive labels - if necessary we may "color" the passive labels to prevent ambiguity.)

Now we can carry out the same operations as before, corresponding to multiplication and exponentiation of generating functions, but shifting only the active labels.

To interpret (9.1), we take a digraph on $[rp + n]$ and construct a modified digraph with active label set $[r]$ as follows: For each i in $[r]$ we add a new vertex with active label i and add arcs from i to the (passive) vertices in $(i-1)p + [p]$. Then we replace each passive label $(i - 1)p + j$ by the passive label j. It is clear that the original digraph can be recovered from the modified digraph. Now shifting an active label in a modified digraph corresponds to shifting "in parallel" the labels in a sector of the original digraph.

The interpretation of (9.1) is now straightforward. We fix n and for each r let $a_{n,r}$ count a set of modified digraphs with original label set $[rp + n]$. Then (9.1) holds if a modified digraph may be decomposed into a set of modified tubes and a modified digraph without tubes. (For this to be the case tubes must have no external arcs.)

It is now clear that (9.1) holds for cycle digraphs, where $a_{n,r} = c_{n+rp}(\mathbf{t})$. Let us now compute v_r, the sum of the weights of the tubes of length r, for this case. By Theorem 8.2, the stabilizer of a tube has size p, and thus is generated by some $g_1^{k_1} g_2^{k_2} \cdots g_r^{k_r}$, with $1 \le k_i \le p-1$, where g_i is a generator for C_p acting on X_i. Since each possible stabilizer has $p - 1$ generators, there are $(p - 1)^{r-1}$ possibilities for the stabilizer.

Now let us count the tubes of length r with a given stabilizer. If the tube has an arc within X_i, then it must have p such arcs, and this can happen only for $r = 1$. Thus if $r > 1$ there must be an arc from X_i to some X_j, $j \neq i$, and since there must be p such arcs, j is uniquely determined. Thus every sector has a unique "succesor," and similarly, a unique "predecessor," so the sectors form a set of cycles. But since a tube must be connected, there can be only one cycle, which may be chosen in $(r - 1)!$ ways. If we take the cyclic order $(x_1, x_2, \ldots, x_r)$, then we have p choices for the set of arcs from X_i to X_{i+1}, for $i = 1, 2, \ldots, r-1$. The set of arcs from X_r to X_1 may

also be chosen in p ways: one of these choices will create p r-cycles and the other $p-1$ choices will create one rp-cycle. Thus

$$v_r = [p(p-1)]^{r-1}(r-1)![t_r^p + (p-1)t_{rp}] \tag{9.3}$$

for $r > 1$, and this formula clearly holds for $r = 1$ also.

The congruence we obtain may be simplified with the help of the following lemma:

LEMMA 9.1. Suppose $\alpha_n \equiv \beta_n \equiv 0 \pmod{p^n}$, $n \geq 1$. Then $\gamma_n \equiv 0 \pmod{p^n}$, where

$$\sum_{n=0}^{\infty} \gamma_n \frac{x^n}{n!} = [\sum_{n=0}^{\infty} \alpha_n \frac{x^n}{n!}] \exp[\sum_{n=1}^{\infty} \beta_n \frac{x^n}{n!}]. \tag{9.4}$$

PROOF. Let us set $\alpha_n = p^n\alpha_n'$, $\beta_n = p^n\beta_n'$, and $\gamma_n = p^n\gamma_n'$. Then the lemma asserts that if α_n and β_n are p-integral, so is γ_n' where

$$\sum_{n=0}^{\infty} \gamma_n' \frac{x^n}{n!} [\sum_{n=0}^{\infty} \alpha_n' \frac{x^n}{n!}] \exp[\sum_{n=1}^{\infty} \beta_n' \frac{x^n}{n!}],$$

and this is immediate.

By Lemma 9.1 we may reduce $v_r \pmod{p^r}$ before substituting in (9.2). Since $v_r \equiv (-p)^{r-1}(r-1)!\,(t_r^p - t_{rp}) \pmod{p^r}$, we obtain:

THEOREM 9.2

$$b_{n,r} \equiv 0 \pmod{p^r}$$

where

$$\sum_{r=0}^{\infty} b_{n,r} \frac{x^r}{r!} = \exp[\sum_{r=1}^{\infty} (-1)^r p^{r-1}(t_r^p - t_{rp}) \frac{x^r}{r}] \times \sum_{r=0}^{\infty} c_{n+rp}(\mathbf{t}) \frac{x^r}{r!} \tag{9.5}$$

We may write (9.5) in terms of the shift operator as

$$\sum_{r=0}^{\infty} b_{n,r} \frac{x^r}{r!} = \exp[(E^p - t_1^p + t_p)x + \sum_{r=2}^{\infty} (-1)^r p^{r-1}(t_r^p - t_{rp}) \frac{x^r}{r}] c_n(\mathbf{t}) \tag{9.6}$$

or

$$c_r(E^p - t_1^p + t_p,\ p(t_2^p - t_{2p}),\ -p^2(t_3^p - t_{3p}),\ \ldots)c_n(\mathbf{t})$$

$$\equiv 0 \pmod{p^r}. \tag{9.7}$$

If we write F for the operator $E^p - t_1^p + t_p$ and write (9.7) as $h_r(F)c_n(\mathbf{t}) \equiv 0 \pmod{p^r}$, then the first few values of $h_r(F)$ are

$$\begin{aligned} h_1 &= F \\ h_2 &= F^2 + p(t_2^p - t_{2p}) \\ h_3 &= F^3 + 3p(t_2^p - t_{2p})F - 2p^2(t_3^p - t_{3p}). \end{aligned} \tag{9.8}$$

Let us now take $t_n = \alpha+1 - nt$ in Theorem 9.2, with α a p-integral rational, so that $c_n(\mathbf{t})$ is the Laguerre polynomial $\Lambda^{(\alpha)}(t)$. Let us write $\bar{t}$ for $-t$. Then

$$\begin{aligned} t_r^p - t_{rp} &= (\alpha+1+r\bar{t})^p - (\alpha+1+rp\bar{t})^p \\ &\equiv r\bar{t}^p \pmod{p}. \end{aligned}$$

Then

$$\begin{aligned} \exp[\sum_{r=1}^{\infty} (-1)^r p^{r-1} r\bar{t}^p \frac{x^r}{r}] &= \exp[-\frac{\bar{t}^p}{p} \frac{px}{1+px}] \\ &= \sum_{n=0}^{\infty} \Lambda_n^{(-1)}(-\bar{t}^p/p) \frac{(-px)^n}{n!}, \end{aligned}$$

so Theorem 9.2 yields

$$\sum_{i=0}^{r} \binom{r}{i} (-p)^{r-i} \Lambda_{r-i}^{(-1)}(-\bar{t}^p/p) \Lambda_{n+pi}^{(\alpha)}(t) \equiv 0 \pmod{p^r}. \tag{9.9}$$

If $t_r^p - t_{rp} \equiv 0 \pmod{p}$ for $r > 1$, then Theorem 9.2 yields the congruence

$$[E^p - (t_1^p - t_p)]^r c_n(\mathbf{t}) \equiv 0 \pmod{p^r}. \tag{9.10}$$

Thus for the derangement numbers, where $t_1 = 0$ and $t_i = 1$ for $i > 0$, we have

$$(E^p + 1)^r d_n \equiv 0 \pmod{p^r}. \tag{9.11}$$

We now turn to the Bell numbers. We cannot use (9.1) directly, since tubes in Bell number graphs may have external edges. However, it is not difficult to count certain subsets of these graphs in which tubes do not have external edges. If a vertex in a tube of a Bell number graph has an external edge, then the sector containing that vertex must be contained in a component. But by contraction, the number of Bell number graphs on $[rp + n]$ in which no sector is contained in a

component is $(E^p - E)^r B_n$, and (9.1) applies with $a_{n,r} = (E^p - E)^r B_n$. We find that $v_r = [p(p-1)]^{r-1}$, which may be reduced (mod p^r) to $(-p)^{r-1}$. The congruence we obtain can be expressed in several ways, but the simplest is probably the following:

THEOREM 9.3. Let C be the operator $E^p - E - 1$. Define the "associated Stirling numbers" $S_2(n,k)$ by

$$\sum_{j \geq 2k \geq 0} S_2(j,k) u^k \frac{z^j}{j!} = \exp[u(e^z - z - 1)], \tag{9.12}$$

and let

$$g_r(C) = \sum_{j=0}^{r} C^{r-j}(-1)^j \binom{r}{j} \sum_{k=0}^{\lfloor j/2 \rfloor} S_2(j,k) p^{j-k}. \tag{9.13}$$

Then

$$g_r(C) B_n \equiv 0 \pmod{p^r}. \tag{9.14}$$

PROOF. From 9.2 and the remarks above, we have $b_{n,r} \equiv 0$, where

$$\begin{aligned}
\sum_{r=0}^{\infty} b_{n,r} \frac{x^r}{r!} &= \exp[-\sum_{r=1}^{\infty} (-p)^{r-1} \frac{x^r}{r!}] \cdot \sum_{r=0}^{\infty} (E^p - E)^r B_n \frac{x^r}{r!} \\
&= \exp[(e^{-px} - 1)/p] \cdot \exp[(E^p - E)x] B_n \\
&= \exp(Cx) \cdot \exp[(e^{-px} + px - 1)/p] B_n \\
&\sum_{i=0}^{\infty} C^i \frac{x^i}{i!} \sum_{j \geq 2k \geq 0} S_2(j,k) p^{-k} \frac{(-px)^j}{j!} B_n \\
&= \sum_{r=0}^{\infty} \frac{x^r}{r!} \sum_{j=0}^{r} C^{r-j}(-1)^j \binom{r}{j} \sum_{k=0}^{\lfloor j/2 \rfloor} S_2(j,k) p^{j-k} B_n.
\end{aligned}$$

A table of $S_2(n,k)$ can be found in [30, p.222]. The first few values of $g_r(C)$ are

$$\begin{aligned}
g_1 &= C \\
g_2 &= C^2 + p \\
g_3 &= C^3 + 3pC - p^2 \\
g_4 &= C^4 + 6pC^2 - 4p^2C + (3p^2 + p^3).
\end{aligned} \tag{9.15}$$

Congruences equivalent to these have been found by Lunnon, Pleasants, and Stephens [50]; however, the equivalence is not obvious.

A digraph is *d-regular* if every vertex has indegree and outdegree d (with loops and multiple arcs counted in the usual way, not as in

Section 4). Our next theorem gives congruences for these digraphs with various restrictions on loops and multiple arcs.

THEOREM 9.4. Let f_n be the number of d-regular digraphs on $[n]$, as specified below. Then for $p > d \geq 2$ we have

$$(E^p - w)^r f_n \equiv 0 \pmod{p^r}, \tag{9.16}$$

where w is as follows.

(i) No loops or multiple arcs:

$$w = \binom{p-1}{d} \equiv (-1)^d \pmod{p} \tag{9.17}$$

(ii) Loops, but no multiple arcs:

$$w = \binom{p}{d} \equiv 0 \pmod{p} \tag{9.18}$$

(iii) Multiple arcs, but no loops:

$$w = \binom{p+d-2}{d} \equiv 0 \pmod{p} \tag{9.19}$$

(iv) Loops and multiple arcs:

$$w = \binom{p+d-1}{d} \equiv 0 \pmod{p} \tag{9.20}$$

PROOF. We shall prove only (i). The others can be proved similarly. It is clear that (9.1) applies with $a_{n,r} = f_{n+rp}$. We need only show that $v_1 = w = \binom{p-1}{d}$ and $v_r \equiv 0 \pmod{p^r}$ for $r > 1$. Now v_1 is the number of tubes of length 1, that is, the number of digraphs on $[p]$ fixed by C_p. Such a digraph is determined by specifying the d arcs leaving vertex 1, which may be chosen without repetition from the $p-1$ possible arcs from 1 to the other vertices. Thus $v_1 = \binom{p-1}{d}$.

To show that $v_r \equiv 0 \pmod{p^r}$ for $r > 1$, we define a new action of C_p^r on tubes of length r, which does not fix any tubes: if a group element g acting on $[rp]$ takes i to j, then acting on digraphs it takes an arc (i,k) to an arc (j,k) but does not affect arcs entering i (unless g acts on their intitial vertices). This action preserves regularity and for $r > 1$ will not create loops hence $v_r \equiv 0 \pmod{p^r}$. (This argument also shows that $v_1 \equiv 0 \pmod{p}$ in (ii) and (iv), where we are allowed

to create loops.)

The congruences of (ii) and (iv) can be improved by representing a digraph Γ on $[n]$ as a bipartite graph Γ' on $[2n]$: an arc from i to j in Γ corresponds to an edge from i to $n+j$ in Γ'. Then instead of the action of C_p^r on Γ we look at an appropriate action of C_p^{2r} on Γ'.

Formula (9.1) can also be applied to d-regular graphs, but it seems difficult to evaluate v_r in this case. For some recent work on the difficult problem of counting d-regular graphs and digraphs, see Read and Wormald [58] and Goulden, Jackson, and Reilly [37].

We now consider another class of digraphs which are difficult to count. A *k-line Latin rectangle* of length n is a $k \times n$ array a_{ij} of numbers such that each row is a permutation of $[n]$ and each column has distinct entries. A Latin rectangle is *reduced* if its first row is $1\ 2 \cdots n$. We can represent a reduced k-line Latin rectangle of length n as a digraph on $[n]$ in which the arcs are colored in $k-1$ colors: if the Latin rectangle is (a_{ij}), the digraph has an arc of color $i-1$ from j to a_{ij} for $2 \le i \le k$. Thus every vertex has one arc of each color going out and one of each color coming in, and there are no loops or multiple arcs.

The number of tubes of length 1 is

$$(p-1)(p-2)\ldots(p-(k-1)+1)=(k-1)!\binom{p-1}{k-1}\equiv(k-1)!(-1)^{k-1}(\mathrm{mod}\ p),$$

and the same argument as in Theorem 9.4 shows that the number of tubes of length $r > 1$ is divisible by p^r, so we have the congruence

$$[E^p + (-1)^k(k-1)!]^r L_n^{(k)} \equiv 0\ (\mathrm{mod}\ p^r), \tag{9.21}$$

where $L_n^{(k)}$ is the number of reduced k-line Latin rectangles of length n. Note that $k = 2$ reduces to (9.11). The case $k = 3$ was found by Carlitz [5]. (See also Riordan [59].) For recent work on counting Latin rectangles see Pranesachar [55].

10. Wreath Products

Let H act on $[r]$ and G on $[m]$. We define the *wreath product* $H(G)$ (also denoted $G \sim H$ or G wr H) as a group of size $|H| \cdot |G|^r$ acting on $[rm]$. First we define a new action of H on $[rm]$. Let us write $h \cdot i$ for the old action of H and $h(i)$ for the new action. Then $h((i-1)m+j) = ((h \cdot i) - 1)m+j$ for j in $[m]$ and i in $[r]$. In other words, with $X_i = (i-1)m + [m]$, $h(X_i) = X_{h \cdot i}$ and h is order-preserving within each X_i. Then $H(G)$ is generated by H and G^r, where G^r acts in the usual way on $[rm]$.

Wreath products may be used in several ways to obtain congruences. We use them in this section to improve the power of p in congruences like (8.3) and (8.4).

Fix a prime p. For any positive integer l, let $\nu(l)$ be the highest power of p dividing l and let $\mu(l) = \nu(l!)$. It is convenient to write $\mu(\alpha)$ for $\mu(\lfloor\alpha\rfloor)$ if α is not an integer. It is well known that $\mu(\alpha) = \lfloor\frac{\alpha}{p}\rfloor + \lfloor\frac{\alpha}{p^2}\rfloor + \lfloor\frac{\alpha}{p^3}\rfloor + \cdots$. We note also that $\mu(p\alpha) = \lfloor\alpha\rfloor + \mu(\alpha)$ and that $\mu(\alpha+\beta) \geq \mu(\alpha) + \mu(\beta)$. We will also often use the formula $\lfloor\lfloor\alpha\rfloor/n\rfloor = \lfloor\alpha/n\rfloor$.

By Sylow's theorem we know that there is a subgroup of the symmetric group S_r of size $p^{\mu(r)}$. We shall write W_r for this group. We do not need to know anything about the structure of W_r here, but W_r can be constructed from C_p by wreath products and direct products.

Now suppose Γ is a digraph on $[rp+n]$. Then $W_r(C_p)$ acts on $[rp]$, and hence on Γ. Since $W_r(C_p)$ is a p-group containing C_p^r, we may hope to use it to strengthen the congruences obtained from C_p^r. (It may be noted that $W_r(C_p)$ is isomorphic to W_{rp}.)

By Theorem 8.3, if every tube of Γ under C_p^r has length at least 2, then the orbit of Γ under C_p^r has size at least $p^{\lceil r/2\rceil}$. We usually get a larger orbit under $W_r(C_p)$.

THEOREM 10.1. Let Γ be a digraph on $[rp + n]$ and suppose that under C_p^r, Γ has no tubes of length 1. Let Γ lie in an orbit of size p^e under $W_r(C_p)$. Then

(a) If $p \geq 5$, or if $p = 3$ and there are no tubes of length 3, then $e \geq \lceil r/2\rceil + \mu(r) - \mu(r/2)$.

(b) If $p = 3$ then $e \geq \lfloor(2r+1)/3\rfloor$.

Note. If we set $\phi(r) = \lceil r/2\rceil + \mu(r) - \mu(r/2)$ then $\phi(r) = \mu(pr) - \mu(pr/2)$, and for $p \neq 2$,

$$\phi(r) - \phi(r-1) = \begin{cases} 0, & r \text{ even} \\ 1+\nu(r), & r \text{ odd.} \end{cases}$$

Thus if r is odd, $f(r) = (r+1)/2 + \nu(1 \cdot 3 \cdot 5 \cdots r)$. The alternative expression

$$\phi(r) = \lfloor\tfrac{1}{2}(1+r)\rfloor + \lfloor\tfrac{1}{2}(1+r/p)\rfloor + \lfloor\tfrac{1}{2}(1+r/p^2)\rfloor + \cdots$$

follows from the formula $\lfloor\alpha\rfloor - \lfloor\alpha/2\rfloor = \lfloor(\alpha+1)/2\rfloor$ and the formula for $\mu(\alpha)$.

PROOF. We find the smallest possible orbit under $W_r(C_p)$ by finding

the largest possible stabilizer. Now $W_r(C_p)_\Gamma$ is a p-group which is a subgroup of $S_r(C_p)_\Gamma$, where S_r is the symmetric group on $[r]$. Thus $|W_r(C_p)_\Gamma| = p^t$ where $t \le \nu(|S_r(C_p)_\Gamma|)$.

Now suppose that, with respect to C_p^r, Γ has a_i tubes of length i, for $i = 2,3,\ldots,r$, and b sectors not in tubes. We claim that $|S_r(C_p)_\Gamma|$ divides

$$N = 2!^{a_2}3!^{a_3} \cdots r!^{a_r}a_2!a_3! \cdots a_r!b!p^{a_2 + \cdots + a_r}. \quad (10.1)$$

To see this we first observe that the sectors of a tube of length i can be permuted in at most $i!$ ways, giving the factor $2!^{a_2} \cdots r!^{a_r}$. Next the a_i tubes of length i may be permuted among themselves in at most $a_i!$ ways and the b sectors not in tubes may be permuted in at most $b!$ ways, giving the factor $a_2! \cdots a_r!b!$. The stabilizer of Γ under C_p^r has at most one copy of C_p for each tube, giving the factor $p^{a_2 + \cdots + a_r}$.

Our problem now is given r, to find an "optimal" partition of $r-b$, for some b, into a_2 2's, a_3 3's, etc., so that the power of p in (10.1) is as large as possible. Let this largest power of p be l. Then since $p^{\mu(pr)} = |W_r(C_p)| \le p^e \cdot p^l$,

$$e \ge \mu(pr) - l. \quad (10.2)$$

If $p = 2$ we may take $a_2 = \lfloor r/2 \rfloor$ to get $l \ge 2a_2 + \mu(a_2) = a_2 + \mu(2a_2) = \lfloor r/2 \rfloor + \mu(r)$. Thus the best bound we can hope to obtain is $e \ge \mu(2r) - \lfloor r/2 \rfloor - \mu(r) = \lceil r/2 \rceil$, which is no improvement on the results of Section 8.

Now we show that under the conditions of (a), $\nu(N)$ is greatest when $a_2 = \lfloor r/2 \rfloor$ and the other a_i are zero (so that b is 0 or 1).

If we replace the a_i i's in (10.1) by $\lfloor ia_i/2 \rfloor$ 2's for $i \ge 3$ (and ignore the remainder), then N is multiplied by

$$\frac{2^{\lfloor ia/2 \rfloor}(a_2 + \lfloor ia/2 \rfloor)!}{i!^a a_2!a!} p^{\lfloor ia/2 \rfloor - a}, \quad (10.3)$$

where we have written a for a_i. For $p \ne 2$ the power of p in (10.3) is

$$\begin{aligned} &\mu(a_2 + ia/2) - \mu(a_2) + \lfloor ia/2 \rfloor - \mu(a) - a - a\mu(i) \\ &\quad \ge \mu(ia/2) + \lfloor ia/2 \rfloor - \mu(pa) - a\mu(i) \\ &\quad = \mu(pia/2) - \mu(pa) - a\mu(i). \end{aligned} \quad (10.4)$$

We want to show that (10.4) is nonnegative. Since $\mu(i) = \mu(p\lfloor i/p \rfloor)$, (10.4) is the power of p in

$$\lfloor pia/2 \rfloor ! / (pa)! \ ((p \lfloor i/p \rfloor)!^a). \tag{10.5}$$

If $pa + ap\lfloor i/p \rfloor \le pia/2$, then (10.5) is an integer times a multinomial coefficient, and is thus an integer. So (10.4) is nonnegative if

$$i - 2\lfloor i/p \rfloor \ge 2. \tag{10.6}$$

The stronger inequality $i(1-2/p) \ge 2$ holds if $p = 3$ and $i \ge 6$, $p = 5$ and $i \ge 4$, or $p \ge 7$ and $i \ge 3$. The only remaining cases covered by (a) are $p = 3$, $i = 4$ or 5; and $p = 5$, $i = 3$. In these cases (10.6) is easily checked directly.

We have shown that under the conditions of (a) there is an optimal partition in which $a_i = 0$ for $i \ne 2$. We must now show that we may take $b = 0$ or 1 in an optimal partition. If we change a_2 to $a_2 + \lfloor b/2 \rfloor$ and b to $b - 2\lfloor b/2 \rfloor$ in (10.1) then $\nu(N)$ increases by

$$\mu(a_2 + b/2) - \mu(a_2) - \mu(b) + \lfloor b/2 \rfloor \ge \mu(pb/2) - \mu(b) \ge 0.$$

Thus under (a), we have $l = \lfloor r/2 \rfloor + \mu(r/2) = \mu(pr/2)$, so by (10.2), $e \ge \mu(pr) - \mu(pr/2) = \lceil r/2 \rceil + \mu(r) - \mu(r/2)$.

We shall now show that for $p = 3$, there is an optimal partition consisting of $\lfloor r/3 \rfloor$ 3's, together with a single 2 if $r \equiv 2 \pmod 3$.

What we have already done shows that for $p = 3$ there is an optimal partition containing only 2's and 3's, with $b = 0$ or 1. Thus (10.1) becomes

$$N = 2!^{a_2} 3!^{a_3} a_2! a_3! b! 3^{a_2 + a_3}, \tag{10.7}$$

where $b = 0$ or 1.

Suppose that in (10.7) we change the a_2 2's to $\lfloor 2a_2/3 \rfloor$ 3's. If $a_2 \equiv 1 \pmod 3$ we will have a remainder of 2, so we keep one 2. Then the power of 3 in (10.7) increases by

$$\begin{aligned} &\mu(a_3 + 2a_2/3) - \mu(a_3) + 2\lfloor 2a_2/3 \rfloor - \mu(a_2) - a_2 + \epsilon \\ &\quad = \mu(3a_3 + 2a_2) - \mu(3a_3) - \mu(a_2) + \lfloor -a_2/3 \rfloor + \epsilon \\ &\quad \ge \mu(2a_2) - \mu(a_2) + \lfloor -a_2/3 \rfloor + \epsilon, \end{aligned} \tag{10.8}$$

where

$$\epsilon = \begin{cases} 1 & \text{if } a_2 \equiv 1 \pmod 3 \\ 0 & \text{if } a_2 \equiv 0,2 \pmod 3. \end{cases}$$

If $a_2 \equiv 0 \pmod 3$, (10.8) is

$$\mu(2a_2) - \mu(a_2) - a_2/3 \geq \mu(a_2) - a_2/3 \geq 0.$$

If $a_2 \equiv 2 \pmod 3$, (10.8) is

$$\mu(2a_2) - \mu(a_2 - 2) - (a_2 + 1)/3 \geq \mu(a_2 + 2) - (a_2 + 1)/3 \geq 0.$$

If $a_2 \equiv 1 \pmod 3$, (10.8) is

$$\mu(2a_2) - \mu(a_2) - (a_2 + 2)/3 + 1 > \mu(a_2) - a_2/3 \geq 0.$$

Thus there is an optimal partition consisting of only 2's and 3's, with $a_2 = 0$ or 1 and $b = 0$ or 1. It is clear that if $a_2 = 1$ and $b = 1$, we can do better by changing a_2 and b to 0 and increasing a_3 by 1. Thus there is an optimal partition with $a_3 = \lfloor r/3 \rfloor$ and $a_2 = 1$ if $r \equiv 2 \pmod 3$, $a_2 = 0$ otherwise. Then

$$\nu(N) = \mu(r/3) + 2\lfloor r/3 \rfloor + \delta = \mu(r/3) + \lfloor 2r/3 \rfloor,$$

where δ is 1 if $r \equiv 2 \pmod 3$ and 0 otherwise. So by (10.2),

$$e \geq \mu(3r) - \mu(r/3) - \lfloor 2r/3 \rfloor = r + \lfloor r/3 \rfloor - \lfloor 2r/3 \rfloor = \lfloor (2r + 1)/3 \rfloor.$$

This completes the proof of Theorem 10.1.

It is clear that Theorem 10.1 can be extended to cover cases in which tubes of length 2 (or other lengths) cannot occur.

It should be noted that in those cases where (9.1) applies, the congruences obtained from Theorem 10.1 can be derived without the use of wreath products. We write (9.1) as

$$e^{-\nu_1 x} \sum_{r=0}^{\infty} a_{n,r} \frac{x^r}{r!} = \exp\Big[\sum_{r=2}^{\infty} \nu_r \frac{x^r}{r!}\Big] \sum_{r=0}^{\infty} b_{n,r} \frac{x^r}{r!}. \tag{10.9}$$

The left side counts digraphs with no tubes of length 1. We find the smallest power of p dividing a term on the right, using the fact that p^{r-1} divides ν_r and p^r divides $b_{n,r}$. The calculations are the same as in the proof of Theorem 10.1.

If we are careful about when the inequalities in the proof of Theorem 10.1 are strict, we find that for $p \neq 3$ the optimal partition is unique. Thus we can prove in some cases that the congruences obtained from Theorem 10.1 are sharp:

THEOREM 10.2. Suppose $p \neq 3$. Let D be a set of digraphs on $[rp + n]$ with no tubes of length 1 on which $W_r(C_p)$ acts. Let $e = \lceil r/2 \rceil$ if $p = 2$ and $e = \lceil r/2 \rceil + \mu(r) - \mu(r/2)$ if $p \geq 5$. Then the sum of the weights of the digraphs in D is congruent (mod p^{e+1}) to the sum of the weights of those digraphs in D with $\lfloor r/2 \rfloor$ tubes of length 2.

For $p = 3$ the optimal partition need not be unique. However, it

should be possible with a little more work to classify the optimal partitions in this case.

If (9.1) applies, so that D is counted by the coefficient of $\frac{x^r}{r!}$ in (10.9), then we obtain the congruence

$$\sum_{i=0}^{r}\binom{r}{i}a_{n,i}(-v_1)^{r-i} \equiv \begin{cases} \frac{(2s)!}{2^s s!}b_{n,0}v_2^s, & r = 2s \pmod{p^{e+1}} \\ \frac{(2s+1)!}{2^s s!}b_{n,1}v_2^s, & r = 2s+1 \end{cases} \tag{10.10}$$

Moreover, it is not hard to verify that if we reduce $v_i \pmod{p^i}$, and define $b_{n,i}$ in term of the reduced v_i, as we did for the cycle indicator polynomials and Bell numbers, then (10.10) still holds.

For the cycle indicator polynomials, after reducing $v_i \pmod{p^i}$ we have $v_1 = t_1^p - t_p$, $v_2 = -p(t_2^p - t_{2p})$, $b_{n,0} = c_n(\mathbf{t})$, and $b_{n,1} = (E^p - t_1^p + t_p)c_n(\mathbf{t})$. (In general, we have $b_{n,1} = a_{n,1} - v_1 a_{n,0}$ by (9.1).) Thus (10.10) yields

$$(E^p - t_1^p + t_p)^r c_n(\mathbf{t})$$

$$\equiv \begin{cases} (-p)^s \frac{(2s)!}{2^s s!}(t_2^p - t_{2p})^s c_n(\mathbf{t}), & r = 2s \pmod{p^{e+1}} \\ (-p)^s \frac{(2s+1)!}{2^s s!}(t_2^p - t_{2p})^s (E^p - t_1^p + t_p)c_n(\mathbf{t}), & r = 2s+1 \end{cases} \tag{10.11}$$

From (10.11) we may conclude that if $t_2^p - t_{2p} \not\equiv 0 \pmod{p}$, and $c_n(\mathbf{t}) \not\equiv 0 \pmod{p}$ for r even, or $(E^p - t_1^p + t_p)c_n(\mathbf{t}) \not\equiv 0 \pmod{p^2}$ for r odd, then $(E^p - t_1^p + t_p)^r c_n(\mathbf{t}) \not\equiv 0 \pmod{p^{e+1}}$. In particular we have $c_0(\mathbf{t}) = 1 \not\equiv 0 \pmod{p}$. If $(E^p - t_1^p + t_p)c_n(\mathbf{t}) \equiv 0 \pmod{p^2}$ for all n, then $(E^p - t_1^p + t_p)^2 c_n(\mathbf{t}) \equiv 0 \pmod{p^2}$ for all n, so by (9.8), $(t_2^p - t_{2p})c_n(\mathbf{t}) \equiv 0 \pmod{p}$ for all n.

Thus we have proved the following:

THEOREM 10.3. If $p \neq 3$ then

$$(E^p - t_1^p + t_p)^r c_n(\mathbf{t}) \equiv 0 \pmod{p^e}, \tag{10.12}$$

where $e = \lceil r/2 \rceil + \mu(r) - \mu(r/2)$ for $p \geq 5$ and $e = \lceil r/2 \rceil$ for $p = 2$. If $t_2^p \not\equiv t_{2p} \pmod{p}$ then for each r there is an n for which the congruence fails (mod p^{e+1}).

Stevens [69] considered the special case of the Hermite

polynomials $c_n(2t,-2)$. He obtained the exponent $\lceil r/2\rceil + \mu(\lceil r/2\rceil)$ for p odd and proved that it was sharp if $\mu(r) = 2\mu(r/2)$. (In this case it agrees with our exponent.) He conjectured that the congruence might hold mod $p^{\lceil r/2\rceil + \mu(r) - \mu(\lceil r/2\rceil)}$; this is still a little less than the correct exponent.

For Bell numbers the analog of (10.11) is

$$(E^p-E-1)^r B_n \equiv$$

$$\begin{cases} (-p)^s \dfrac{(2s)!}{2^s s!} B_n, & r=2s \pmod{p^{e+1}} \\ (-p)^s \dfrac{(2s+1)!}{2^s s!}(E^p-E-1)B_n, & r=2s+1 \end{cases} \tag{10.13}$$

Thus we find that the congruence $(E^p - E - 1)^r B_n \equiv 0 \pmod{p^e}$ is sharp in the same sense as in Theorem 10.3. This was proved by Lunnon [49] in the cases $r < p^2$ and $p = 2$. His numerical evidence suggests that the congruence $(E^3 - E - 1)^r B_n \equiv 0 \pmod{3^{\lfloor (2r+1)/3\rfloor}}$ is also sharp.

11. Some Algebraic Techniques

There are some generalizations of the congruences obtained from Theorem 10.1 that seem to be more easily derived algebraically then combinatorially.

In this section we assume that $\{a_n\}$ is a sequence which satisfies

$$(E^p - \alpha E - \beta)^r a_n \equiv 0 \pmod{p^{\lambda(r)}} \tag{11.1}$$

for all n and r, where α and β are p-integral, for some function λ.

THEOREM 11.1. Suppose that $\alpha \equiv \alpha'$ and $\beta \equiv \beta' \pmod{p}$ and that λ satisfies

$$\lambda(r) \le \nu\left(\binom{r}{s}\right) + r - s + \lambda(s). \tag{11.2}$$

for $0 \le s \le r$.

Then

$$(E^p - \alpha' E - \beta')^r a_n \equiv 0 \pmod{p^{\lambda(r)}}. \tag{11.3}$$

PROOF. We have

$$(E^p - \alpha' E - \beta')^r a_n = [E^p - \alpha E - \beta + ph(E)]^r a_n$$

$$= \sum_{s=0}^{r} \binom{r}{s} (E^p - \alpha E - \beta)^s p^{r-s} h(E)^{r-s} a_n, \quad (11.4)$$

where $h(E) = \frac{\alpha - \alpha'}{p} E + \frac{\beta - \beta'}{p}$. The power of p dividing a term of (11.4) is at least $\nu\left(\binom{r}{s}\right) + \lambda(s) + r - s \geq \lambda(r)$, so (11.3) holds.

If $\lambda(r) - \lambda(r-1) \leq 1$ for all r, then

$$\lambda(r) - \lambda(s) \leq r - s \leq \nu\left(\binom{r}{s}\right) + r - s$$

so (11.2) is satisfied.

If $\lambda(r) = \lceil r/2 \rceil + \mu(r) - \mu(r/2) = r + \mu(r) - \mu(pr/2)$, then

$$\nu\left(\binom{r}{s}\right) + r - s + \lambda(s) = \mu(r) - \mu(r-s) + r - \mu(ps/2)$$

$$= \lambda(r) + \mu(pr/2) - \mu(r-s) - \mu(ps/2) \geq \lambda(r),$$

since $pr/2 - (r-s) - ps/2 = (r-s)(p/2-1) \geq 0$.

Thus (11.2) is satisfied for all functions $\lambda(r)$ which we have encountered.

THEOREM 11.2

(a) If $\lambda(r + p - 1) > \lambda(r)$ then

$$[E^{p^{k+1}} - (\alpha E + \beta)^{p^k}]^r a_n \equiv 0 \pmod{p^{kr + \lambda(r)}}. \quad (11.5)$$

(Note that this applies to all our examples with $p > 2$, and for $p = 2$, $\lambda(r) = r$.)

(b) If $p = 2$ and $\lambda(r) = \lceil r/2 \rceil$ then

$$[E^{2^{k+1}} - (\alpha E + \beta)^{2^k}]^r a_n \equiv 0 \pmod{2^{kr}}, \quad (11.6)$$

for $k \geq 1$.

PROOF. Let $F = E^p - \alpha E - \beta$ and let $G = \alpha E + \beta$. Then $E^{p^{k+1}} = (F + G)^{p^k}$, so

$$E^{p^{k+1}} - G^{p^k} = \sum_{i=1}^{p^k} \binom{p^k}{i} F^i G^{p^k - i}. \quad (11.7)$$

Now if $i < p^{j+1}$, $\binom{p^k}{i}$ is divisible by p^{k-j}. Thus (11.7) may be written

$$E^{p^{k+1}} - G^{p^k} = \sum_{i=0}^{k} p^{k-i} F^{p^i} h_i,$$

where h_i is a polynomial in E with p-integral coefficients. Therefore

$$(E^{p^{k+1}} - G^{p^k})^r =$$

$$\sum_{0 \le i_1, \ldots, i_r \le k} p^{kr-(i_1+\ldots+i_r)} F^{p^{i_1}+\ldots+p^{i_r}} h_{i_1} \ldots h_{i_r}. \tag{11.8}$$

A term of (11.8) is divisible by p to the power

$$A(i_1, \ldots, i_k) = kr - (i_1 + \ldots + i_r) + \lambda(p^{i_1} + \ldots + p^{i_r}). \tag{11.9}$$

We claim that with condition (a), (11.9) is least for $i_1 = i_2 = \cdots = i_r = 0$, which gives (11.5). To see this, we have

$$\begin{aligned} &A(i_1, \ldots, i_r) - A(0, i_2, \ldots, i_r) \\ &= -i_1 + \lambda(p^{i_1} + \cdots + p^{i_r}) - \lambda(1 + p^{i_2} + \cdots + p^{i_r}) \\ &\ge -i_1 + \frac{p^{i_1}-1}{p-1} = 1 + p + \cdots + p^{i_1 - i_1} \ge 0. \end{aligned}$$

We claim that with condition (b), (11.9) is least for $i_1 = i_2 = \cdots = i_r = 1$, if $k \ge 1$. Here we have

$$A(i_1, \ldots, i_r) - A(1, i_2, \ldots, i_r) \tag{11.10}$$

$$= 1 - i_1 + \lambda(2^{i_1} + \cdots + 2^{i_r}) - \lambda(2 + 2^{i_2} + \cdots + 2^{i_r}).$$

Since $\lambda(r + 2j) = \lambda(r) + j$, for $i_1 \ge 1$ (11.10) is $1 - i_1 + (2^{i_1 - 1} - 1) = 2^{i_1 - 1} - i_1 \ge 0$. For $i_1 = 0$, (11.10) is $1 + \lambda(1 + \cdots + 2^{i_r}) - \lambda(2 + \cdots + 2^{i_r}) = 1$. Now $A(1, \ldots, 1) = kr - r + \lambda(2r) = kr$, which gives (11.6).

As in Section 10, we can sharpen Theorem 11.2 by noting when equalities occur in the proof.

A somewhat stronger result than Theorem 11.2 for the case

$$\phi(0,r,2) = \lceil r/2 \rceil.$$

Applying Theorems 10.1 and 11.2 to the Bell numbers, we have

$$[E^{p^{k+1}} - (E+1)^{p^k}]^r B_n \equiv 0 \pmod{p^{\phi(k,r,p)}}. \tag{11.12}$$

The case $r = 1$, $p \geq 3$ of (11.12) was found by Lunnon, Pleasants, and Stephens [50].

For the cycle indicator polynomials we have

$$[E^{p^{k+1}} - (t_1^p - t_p)^{p^k}]^r c_n(\mathbf{t}) \equiv 0 \pmod{p^{\phi(k,r,p)}}. \tag{11.13}$$

For the number s_n of connected graphs we have (with the help of Theorem 11.1) for p odd,

$$(E^{p^{k+1}} - \epsilon E^{p^k})^r s_n \equiv 0 \pmod{p^{\phi(k,r,p)}}, \tag{11.14}$$

where

$$\epsilon = \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

For the number h_n of partial orders we have

$$(E^{p^{k+1}} - E^{p^k})^r h_n \equiv 0 \pmod{p^{\phi(k,r,p)}}. \tag{11.15}$$

In many cases we will have congruences of the form

$$(E^p - u^p)^r a_n \equiv 0 \pmod{p^{\lambda(r)}} \tag{11.16}$$

for several primes p, where u does not depend on p. In these cases, since $E^{p^k} - u^{p^k}$ divides $E^m - u^m$ whenever p^k divides m, we can get congruences for $(E^m - u^m)^r a_n$.

For example, let f_n be the number of d-regular digraphs on $[n]$ without loops or multiple arcs. If every prime divisor of m is greater than $d \geq 2$, then by (9.17) and Theorems 11.1 and 11.2,

$$[E^m - (-1)^d]^r f_n \equiv 0 \pmod{m^r}. \tag{11.17}$$

For the number $L_n^{(k)}$ of $k \times n$ reduced Latin rectangles we obtain similarly the congruence

$$[E^m + (-1)^{km}(k-1)!^m]^r L_n^{(k)} \equiv 0 \pmod{m^r} \tag{11.18}$$

for all m. The case $k = 3$ of (11.18) is due to Carlitz [5].

We recall the congruence

$$(E^p - t_1^p + t_p)^r \, c_n(\mathbf{t}) \equiv 0 \pmod{p^{\phi(0,r,p)}} \tag{11.19}$$

for cycle indicator polynomials. Suppose now that the t_i are such that for all primes p in some set P of primes, $t_1^p - t_p \equiv u^p \pmod{p}$ for some u independent of p. If $m = p_1^{d_1} \cdots p_l^{d_l}$, where each p_i is in P, then

$$(E^m - u^m)^r \, c_n(\mathbf{t}) \equiv 0 \pmod{p_1^{e_1} \cdots p_l^{e_l}}. \tag{11.20}$$

where $e_i = \phi(d_i - 1, r, p_i)$.

For example, let P be an arbitrary set of primes and take $t_p = 0$ for p in P. Then (11.20) holds with $u = t_1$. In particular, if we set $t_i = 0$ for $i > 2$, we get congruences for Hermite polynomials. (In this case the exponent for $p = 3$ is $(d-1)r + \lceil r/2 \rceil + \mu(r) - \mu(r/2)$, since there are no tubes of length 3.) Similar congruences were obtained by Stevens [69] with the exponent $(d - 1)r + \lceil r/2 \rceil + \mu(r/2)$.

For the Laguerre polynomials

$$\Lambda_n^{(\alpha)}(t) = c_n(\alpha+1-t, \, \alpha+1-2t \, , \ldots , \, \alpha+1-nt),$$

we have $t_1 = \alpha+1-t$ and $t_p = \alpha+1-pt$, so $t_1^p - t_p \equiv (-t)^p \pmod{p}$ if α is rational and p-integral. Thus (11.20) holds here for all primes, with $u = -t$. The weaker congruence

$$[E^m - (-t)^m]^r \, \Lambda_n^{(\alpha)}(t) \equiv 0 \pmod{m^{\lceil r/2 \rceil}}$$

was found by Carlitz [15].

Congruences of the form (11.16) also arise in counting d-regular graphs. Let w_p be the number of d-regular graphs on $[p]$ fixed by C_p. It is not hard to compute w_p for $p > d$, with various restrictions on loops and multiple edges. (We count a loop as contributing 1 to the degree of its vertex.) If we interpret the binomial coefficient $\binom{a}{b}$ as zero if b is not an integer, then the values of w_p may be described as follows.

(i) No loops or multiple edges:

$$w_p = \binom{(p-1)/2}{d/2} \equiv \binom{-1/2}{d/2} \pmod{p} \tag{11.21}$$

(ii) Loops, but no multiple edges:

$$w_p = \binom{(p-1)/2}{\lfloor d/2 \rfloor} \equiv \binom{-1/2}{\lfloor d/2 \rfloor} \pmod{p} \tag{11.22}$$

(iii) Multiple edges, but no loops:

$$w_p = \binom{(p+d-3)/2}{d/2} \equiv (-1)^{d/2}\binom{1/2}{d/2} \pmod{p} \tag{11.23}$$

(iv) Loops and multiple edges:

$$w_p = \binom{\lfloor (p+d-1)/2 \rfloor}{\lfloor d/2 \rfloor} \equiv (-1)^{\lfloor d/2 \rfloor}\binom{-1/2}{\lfloor d/2 \rfloor} \pmod{p} \tag{11.24}$$

In each of these cases we may write $w_p \equiv w \pmod{p}$, where w is independent of p. Thus if g_n is the number of d-regular graphs of one of these types on $[n]$, then for $m = p_1^{d_1} \cdots p_l^{d_l}$, where $p_i > d$, we have

$$(E^m - w^m)^r g_n \equiv 0 \pmod{p_1^{e_1} \cdots p_l^{e_l}}, \tag{11.25}$$

where $e_i = \phi(d_i - 1, r, p_i)$.

Carlitz [16] found the weaker congruence

$$[E^m - (-1/2)^m]^r g_n \equiv 0 \pmod{m^{\lceil r/2 \rceil}}$$

for the special case $d = 2$ of (i).

In those cases where $w_p = 0$, the congruence reduces to

$$g_n \equiv 0 \pmod{p^{\mu(n)-\mu(n/2)}}.$$

12. More on Wreath Products

In this section we give a combinatorial analog of the case $r = 1$, $p > 2$ of Theorem 11.2. It would be interesting to treat the general case by this method; however, the congruences we obtain here are obtained with less work from Theorem 11.2. Here we identify $W_{p^{k+1}}$ with $C_p(W_{p^k})$.

THEOREM 12.1. Suppose $p > 2$ and let Γ be a digraph on $[p^k + n]$. If the size of the orbit of Γ under W_{p^k} is less than p^k, then Γ is fixed by the action of C_p on $(i-1)p + [p]$ for each i in $[p^{k-1}]$.

PROOF. If $k = 1$ the theorem is trivial. Suppose it holds for k. Let $G^{(i)}$ be W_{p^k} acting on $(i-1)p^k + [p^k]$ for i in $[p]$. We write G for $G^{(1)}$ and G^p for $W_{p^k}^p = G^{(1)} \times \cdots \times G^{(p)}$. Let g be the permutation that takes i to $i + p^k \pmod{p^{k+1}}$.

It suffices to show that if a digraph Γ on $[p^{k+1}+n]$ is not fixed by C_p acting on $[p]$ then it lies in an orbit of size at least p^{k+1} under $W_{p^{k+1}}$. By induction, the orbit of Γ under G has size at least p^k, so it is enough to prove that either $|O_G(\Gamma)| > p^k$ or $O_G(\Gamma) \neq O_W(\Gamma)$, where $W = W_{p^{k+1}}$. Assume to the contrary that $|O_G(\Gamma)| = p^k$ and $O_G(\Gamma) = O_W(\Gamma)$.

Let $A_\Gamma = \{A_1, A_2, \ldots, A_l\}$ be the set of supports of the components of G^p_Γ (the stabilizer of Γ in G^p). If Γ' is in $O_G(\Gamma)$ then $A_\Gamma = A_{\Gamma'}$. Thus since by assumption $g\Gamma$ is in $O_G(\Gamma)$, A_Γ is invariant under cyclic permutation of $[p]$, so there are three possibilities for A_Γ: $A_\Gamma = \varnothing$, $A_\Gamma = \{\{1\},\{2\}, \ldots, \{p\}\}$, and $A_\Gamma = \{[p]\}$.

In the first case, the stabilizer of Γ is trivial, so $|O_G(\Gamma)| = |G| > p^k$.

In the second case, let h_2 be any element of $G^{(2)}$. Then $h_2\Gamma = h\Gamma$ for some h in G, so $h^{-1}h_2$ is in G^p_Γ. Since 1 and 2 are in separate blocks of A, h_2 must be in G^p_Γ. Also there is an element h_1 in G such that $g^{-1}\Gamma = h_1\Gamma$.

Now let h be any element of G. Then

$$h\Gamma = hh_1^{-1}h_1\Gamma = hh_1^{-1}g^{-1}\Gamma = g^{-1}ghh_1^{-1}g^{-1}\Gamma.$$

Since $g(hh_1^{-1})g^{-1}$ is in $G^{(2)}$, we have $h\Gamma = g^{-1}\Gamma$. Since this holds for all h in G, $|O_G(\Gamma)| = 1$, a contradiction.

In the third case, if all of $G^{(2)}$ fixes Γ then the argument of the second case applies. Otherwise, there is some h_2 in $G^{(2)}$ and h_1 in G with $h_2\Gamma = h_1\Gamma$ and $h_2, h_1 \neq e$. Then $h_1^{-1}h_2$ is in G^p_Γ, which contradicts the irreducibility of G^p_Γ. (This part of the proof breaks down for $p=2$.)

Let us apply Theorem 12.1 to the cycle indicator polynomials and Bell numbers.

A cycle digraph Γ on $[p^k+n]$ will be fixed by C_p acting on $X_i = (i-1)p + [p]$ only if $\Gamma(X_i)$ is either a p-cycle or p one-cycles. Thus

$$c_{n+p^k}(\mathbf{t}) \equiv [t_1^p + (p-1)t_p]^{p^{k-1}}\, c_n(\mathbf{t}) \pmod{p^k} \qquad (12.1)$$

This is the case $r = 1$, $p > 2$ of (11.13).

A Bell number graph Γ on $[p^k+n]$ will be fixed by C_p acting on X_i if and only if either X_i consists of p isolated vertices or X_i is contained in a block. Thus we obtain

$$B_{n+p^k} \equiv (E+1)^{p^{k-1}} B_n \pmod{p^k}, \tag{12.2}$$

which is the case $r = 1$, $p > 2$ of (11.12).

Other congruences of Section 11 can be obtained similarly.

13. The Symmetric Group

One might expect that the "best" congruences obtainable from a group acting on $[m]$ would come from the symmetric group S_m. This is the case, and these congruences are often fairly easy to prove.

Congruences of this type have been obtained algebraically for Bell numbers by Lunnon, Pleasants, and Stephens [50] and for several other sequences by Gessel [35] and Flajolet [32].

For the Bell numbers, we want to count a set of partitions of $[m+n]$ which are not fixed by the action of any element of S_m. Such a set consists of those partitions satisfying

(i) No two elements of $[m]$ lie in the same block, and

(ii) No element of $[m]$ is a singleton block.

(We could have allowed at most one singleton, but (ii) gives a simpler result.)

Let $B_{n,m}$ be the number of partitions of $[m+n]$ satisfying (i) and (ii). It is clear that $B_{n,m} \equiv 0 \pmod{m!}$. Now any partition of $[l+n]$ can be reduced to a partition counted by $B_{n,m}$ for some $m \le l$ by first removing all blocks containing only elements of $[l]$, then removing from each remaining block all but the least element of $[l]$, and then "shifting" the labels to $[m+n]$. This correspondence leads to the generating function

$$\sum_{l=0}^{\infty} B_{n+l} \frac{x^l}{l!} = e^{e^x-1} \sum_{m=0}^{\infty} B_{n,m} \frac{(e^x-1)^m}{m!}. \tag{13.1}$$

Thus

$$\sum_{m=0}^{\infty} B_{n,m} \frac{x^m}{m!} = e^{-x} \sum_{l=0}^{\infty} B_{n+l} \frac{[\log(1+x)]^l}{l!} \tag{13.2}$$

so if we define $D_{m,l}$ by

$$e^{-x} \frac{[\log(1+x)]^l}{l!} = \sum_{m=l}^{\infty} D_{m,l} \frac{x^l}{l!}, \tag{13.3}$$

then

$$\sum_{l=0}^{m} D_{m,l}B_{n+l} = B_{n,m} \equiv 0 \pmod{m!}. \tag{13.4}$$

The first few instances of (13.4) are

$$B_{n+2} - 3B_{n+1} + B_n \equiv \pmod 2$$

$$B_{n+3} - 6B_{n+2} + 8B_{n+1} - B_n \equiv 0 \pmod 6$$

$$B_{n+4} - 10B_{n+3} + 29B_{n+2} - 24B_{n+1} + B_n \equiv 0 \pmod{24}.$$

These congruences were first found by Lunnon, Pleasants, and Stephens [50]. Further properties of the numbers $D_{m,l}$ can be found in [35].

For the cycle indicator polynomials, we want to count cycle digraphs on $[m+n]$ in which no cycle lies entirely within $[m]$. Let $c_{n,m}(\mathbf{t})$ be the sum of the weights of these digraphs. Then we have

$$\sum_{l=0}^{\infty} c_{n+l}(\mathbf{t})\frac{x^l}{l!} = [\sum_{m=0}^{\infty} c_m(\mathbf{t})\frac{x^m}{m!}][\sum_{m=0}^{\infty} c_{n,m}(\mathbf{t})\frac{x^m}{m!}], \tag{13.5}$$

since any cycle digraph on $[l+n]$ consists of some cycles lying entirely within $[l]$ together with some other cycles, none of which lie entirely within $[l]$.

Thus

$$\sum_{m=0}^{\infty} c_{n,m}(\mathbf{t}) = [\sum_{m=0}^{\infty} c_m(\mathbf{t})\frac{x^m}{m!}]^{-1}[\sum_{l=0}^{\infty} c_{n+l}(\mathbf{t})\frac{x^l}{l!}] \tag{13.6}$$

$$= [\sum_{m=0}^{\infty} c_m(-\mathbf{t})\frac{x^m}{m!}][\sum_{l=0}^{\infty} c_{n+l}(\mathbf{t})\frac{x^l}{l!}],$$

where $c_m(-\mathbf{t}) = c_m(-t_1, -t_2, \ldots, -t_m)$. We obtain the congruence

$$\sum_{l=0}^{m} \binom{m}{l} c_{m-l}(-\mathbf{t})\, c_{n+l}(\mathbf{t}) = c_{n,m} \equiv 0 \pmod{m!}. \tag{13.7}$$

The first few instances of (13.7) are

$$c_{n+2}(\mathbf{t}) - 2t_1c_{n+1}(\mathbf{t}) + (t_1^2 - t_2)c_n(\mathbf{t}) \equiv 0 \pmod 2$$

$$c_{n+3}(\mathbf{t}) - 3t_1c_{n+2}(\mathbf{t}) + 3(t_1^2 - t_2)c_{n+1}(\mathbf{t}) - (t_1^3 - 3t_1t_2 + 2t_3)c_n(\mathbf{t}) \equiv 0 \pmod 6$$

$$c_{n+4}(\mathbf{t}) - 4t_1c_{n+3}(\mathbf{t}) + 6(t_1^2 - t_2)c_{n+2}(\mathbf{t}) - 4(t_1^3 - 3t_1t_2 + 2t_3)c_{n+1}(\mathbf{t}) + (t_1^4 - 6t_1^2t_2 + 3t_2^2 + 8t_1t_3 - 6t_4)c_n(\mathbf{t}) \equiv 0 \pmod{24}.$$

The special case $t_1 = t_2 = 1$, $t_i = 0$ for $i > 2$ of (11.7) was given in

[35]. We note that there is an easy algebraic proof of (13.7), which we leave to the reader.

Now let $q_{n,m}$ be the number of ordered partitions of $[m+n]$ in which the elements of $[m]$ lie in different blocks. Clearly $q_{n,m} \equiv 0 \pmod{m!}$. An easy argument shows that

$$\sum_{l=0}^{\infty} q_{n+l}\frac{x^l}{l!} = \sum_{m=0}^{\infty} q_{n,m}\frac{(e^x-1)^m}{m!}, \tag{13.8}$$

so

$$\sum_{m=0}^{\infty} q_{n,m}\frac{x^m}{m!} = \sum_{l=0}^{\infty} q_{n+l}\frac{[\log(1+x)]^l}{l!} \tag{13.9}$$

Thus

$$q_{n,m} = \sum_{l=0}^{m} s(m,l)q_{n+l} \equiv 0 \pmod{m!}, \tag{13.10}$$

where $s(m,l)$ is the Stirling number of the first kind.

In [35] a better congruence is given:

$$\sum_{l=0}^{m} (-1)^{m-l}s(m,l)q_{n+l} \equiv 0 \pmod{2^{m-1}m!}. \tag{13.11}$$

We now give a combinatorial proof of (13.11), based on the algebraic proof in [35]. The factor 2^{m-1} does not arise from a group action.

Let $\bar{q}_{n,m}$ be the number of ordered partitions of $[m+n]$ in which the elements of $[m]$ in each block are linearly ordered. We claim that

$$\bar{q}_{n,m} = \sum_{l=0}^{m} (-1)^{m-l}s(m,l)q_{n+l}. \tag{13.12}$$

To prove (13.12), first recall that $(-1)^{m-l}s(m,l) = |s(m,l)|$ is the number of permutations of $[m]$ with l cycles. Now take an ordered partition of $[l] \cup (m + [n])$ and a permutation of $[m]$ with l cycles. Replace i in the ordered partition by the ith smallest cycle, where the cycles are ordered by their least elements. Then replace the set of cycles in each block by the corresponding linear arrangement.

Next we show that the ordered partitions counted by $\bar{q}_{n,m}$ are in 1-1 correspondence with ordered partitions $T = (T_1, T_2, \ldots, T_j)$ of $[m+n]$ where each T_i is either

(i) a single element of $[m]$, or

(ii) a nonempty subset of $m + [n]$,

and in the first case, if $i > 1$ a "+" or "-" is affixed to the element. To obtain the ordered partition counted by $\bar{q}_{n,m}$, we move every

element of $[m]$ with a "+" into the previous block, keeping elements of $[m]$ in the same order.

Thus $\bar{q}_{n,m}$ is divisible by $2^{m-1}m!$ since S_m acts without fixed points on the ordered partitions T, and the signs can be chosen in 2^{m-1} (or 2^m) ways for each arrangement of numbers.

14. Other Groups

We mention briefly here two additional kinds of congruences that can be obtained from group actions.

First, if we want a best possible congruence modulo a power of p, we may count digraphs which are fixed only by the identity element of W_m. This will give us a mod $p^{\mu(m)}$ congruence. The power of p will be the same as that obtained from the action of S_m, but in general these congruences will have fewer nonzero coefficients. However, it is harder to give explicit formulas for these congruences. As a simple example, if we apply W_{p^2} to the case of Fermat's theorem, we find

$$[(E^p - E)^p - p^{p-1}(E^p - E)]a^n \equiv 0 \pmod{p^{p+1}}. \qquad (14.1)$$

This congruence is easily proved directly by writing it in the form $[(a^p - a)/p]^p \equiv (a^p - a)/p \pmod{p}$ and using Fermat's theorem twice. Congruences of this type for Bell numbers have been considered by Pleasants [54].

Another type of congruence comes from counting digraphs not fixed by $S_r(C_m)$. We give here the congruence of this type for cycle indicator polynomials.

Let $X_i = (i-1)m + [m]$ for i in $[r]$. Let $c_{n,r}(\mathbf{t})$ be the sum of the weights of the cycle digraphs on $[rm+n]$ such that for every nonempty subset A of $[r]$, $\Gamma(X_A)$ has an external edge. These digraphs are fixed only by the identity element of $S_r(C_m)$, and hence

$$c_{n,r}(\mathbf{t}) \equiv 0 \pmod{r!m^r}. \qquad (14.1)$$

An argument similar to that for (9.1) shows that

$$\sum_{r=0}^{\infty} c_{n+rm}(\mathbf{t})\frac{x^r}{r!} = [\sum_{r=0}^{\infty} c_{rm}(\mathbf{t})\frac{x^r}{r!}][\sum_{r=0}^{\infty} c_{n,r}(\mathbf{t})\frac{x^r}{r!}] \qquad (14.2)$$

from which $c_{n,r}(\mathbf{t})$ can be computed. Unfortunately, it seems that $[\sum_{r=0}^{\infty} c_{rm}(\mathbf{t})\frac{x^r}{r!}]^{-1}$ can be simplified only when $m = 1$, when we obtain (13.6).

Carlitz [14], [23] has found some congruences which suggest the group $S_r(C_m)$. Let $a(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$ be either $\exp(t \arctan x)$

$= \left(\frac{1+ix}{1-ix}\right)^{-it/2}$ or $(1-2x)^{-1}(1+2x)^{-1/2}$. Then

$$\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}a_{n+sm}a_{(r-s)m} = 0 \pmod{r!m^r}. \qquad (14.3)$$

It should be possible to prove these congruences using group actions.

References

[1] A. Aigner, Kombinatorische Deutung und Verallgemeinerung des Fermatschen Satzes, Elem. Math. *21* , (1966), 91.

[2] D. Barsky, Analyse p-adique et nombres de Bell, C.R. Acad. Sci. Paris (A) *282* (1976), 1257-1259.

[3] H.W. Becker and J. Riordan, The arithmetic of Bell and Stirling numbers, Amer. J. Math. *70* (1948), 385-394.

[4] L. Carlitz, Some theorems on Kummer's congruences, Duke Math. J. *20* (1953), 423-431.

[5] L. Carlitz, Congruences connected with three-line Latin rectangles, Proc. Amer. Math. Soc. *4* (1953), 9-11.

[6] L. Carlitz, Congruences for the solutions of certain difference equations of the second order, Duke Math. J. *21*, (1954), 669-679.

[7] L. Carlitz, Congruences for the number of n-gons formed by n lines, Amer. Math. Monthly *61* (1954), 407-411.

[8] L. Carlitz, Congruence properties of the polynomials of Hermite, Laguerre, and Legendre, Math. Z. *59* (1954), 474-483.

[9] L. Carlitz, Some arithmetic properties of the Olivier functions, Math. Annalen *128* (1954-1955), 412-419.

[10] L. Carlitz, Congruences for generalized Bell and Stirling numbers, Duke Math. J. *22* (1955), 193-205.

[11] L. Carlitz, A note on Kummer's congruences, Arch. Math. *7* (1957), 441-445.

[12] L. Carlitz, Composition of sequences satisfying Kummer's congruences, Collect. Math. *11* (1959), 137-152.

[13] L. Carlitz, Kummer's congruences (mod 2^r), Monatshefte für Math. *63* (1959), 394-400.

[14] L. Carlitz, Some arithmetic properties of a special sequence of polynomials, Duke Math. J. *26* (1959), 583-590.

[15] L. Carlitz, Congruence properties of Hermite and Laguerre polynomials, Arch. Math. *10* (1959), 460-465.

[16] L. Carlitz, Congruences for the number of n-gons formed by n lines, Amer. Math. Monthly *67* (1960), 961-966.

[17] L. Carlitz, Congruence properties of certain polynomial sequences, Acta Arith. *6* (1960), 149-158.

[18] L. Carlitz, Arithmetic properties of certain polynomial sequences, Bull. Amer. Math. Soc. *66* (1960), 202-204.

[19] L. Carlitz, Criteria for Kummer's congruences, Acta Arith. *6* (1960/61), 375-391.

[20] L. Carlitz, Some congruences for the Bell polynomials, Pacific J. Math. *11* (1961), 1215-1222.

[21] L. Carlitz, Congruence properties of certain linear homogeneous difference systems, Acta Arith. *7* (1962), 173-186.

[22] L. Carlitz, Arithmetical properties of the Bell polynomials, J. Math. Anal. Appl. *15* (1966), 33-52.

[23] L. Carlitz, Note on some generating functions, Fibonacci Quarterly *13* (1975), 129-133.

[24] L. Carlitz, Permutations with prescribed pattern, Math. Nachr. *58* (1973), 31-53.

[25] L. Carlitz and H. Stevens, Criteria for generalized Kummer's congruences, J. reine angew. Math. *207* (1961), 203-220.

[26] A. Cayley, On the analytical forms called trees. Second part, *Coll. Math. Papers*, Vol. 4, pp. 112-115. Originally published in Philosophical Magazine *18* (1859), 374-378.

[27] C.-Y. Chao, Generalizations of theorems of Wilson, Fermat, and Euler, J. Number Theory *15* (1982), 95-114.

[28] S. Chowla, I.N. Herstein, and W.K. Moore, On recurrences connected with symmetric groups I, Can. J. Math. *3* (1951), 328-334.

[29] 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.

[30] L. Comtet, *Advanced Combinatorics*, Reidel, Dordrecht, 1974.

[31] L.E. Dickson, *History of the Theory of Numbers*, Vol. 1, Carnegie Institution of Washington, 1919.

[32] P. Flajolet, On congruences and continued fractions for some classical combinatorial quantities, Discrete Math. 42 (1982), 145-153..

[33] F.G. Frobenius, Über die Bernoullischen Zahlen und die Eulerschen Polynome, Gesammelte Abhandlungen, Band III, 440-478. Originally published in Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin (1910), 809-847.

[34] I.M. Gessel, Congruences for Bell and tangent numbers, Fibonacci Quarterly *11* (1981), 137-144.

[35] I.M. Gessel, Some congruences for generalized Euler numbers, Can. J. Math., to be published.

[36] I.J. Good, The number of orderings of n candidates when ties are permitted, Fibonacci Quarterly *13* (1975), 11-18.

[37] I.P. Goulden, D.M. Jackson, and J.W. Reilly, The Hammond series of a symmetric function and its application to P-recursiveness, SIAM J. Alg. Disc. Meth. *3* (1982), 359-368.

[38] O.A. Gross, Preferential arrangements, Amer. Math. Monthly *69* (1962), 4-8.

[39] F. Harary and E.M. Palmer, *Graphical Enumeration*, Academic Press, 1973.

[40] B. Harris and L. Schoenfeld, The number of idempotent elements in symmetric semigroups, J. Combin. Theory *3* (1967), 122-135. Erratum J. Combin. Theory *5* (1968), 104.

[41] A. Hurwitz, Ueber die Entwickelungscoefficienten der lemniscatischen Functionen,

Math. Annalen *51* (1899), 196-226.

[42] F. James and A. Kerber, *The Representation Theory of Symmetric Groups*. (Volume 16 of Encyclopedia of Mathematics and its Applications). Addison-Wesley, 1981.

[43] J.R. Johnson, Jr., Congruence properties of the solutions of certain difference equations, Duke Math. J. *25* (1957), 155-170.

[44] A. Joyal, Une théorie combinatoire des séries formelles, Advances in Math. *42* (1981), 1-82.

[45] D.H. Kauffman, Note on preferential arrangements, Amer. Math. Monthly *70* (1963), 62.

[46] E.F. Kummer, Uber eine allgemeine Eigenschaft der rationalen Entwickelungscoëfficienten einer bestimmten Gattung analytischer Function, J. reine angew. Math. *41* (1851), 368-372.

[47] D.J. Leeming and R.A. MacLeod, Some properties of generalized Euler numbers, Can. J. Math. *33* (1981), 606-617.

[48] J. Levine and R.E. Dalton, Minimum periods, modulo p, of first order Bell exponential intergers, Math. Comp. *16* (1962), 416-423.

[49] W.F. Lunnon, Personal communication.

[50] 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.

[51] L. Moser and M. Wyman, On solutions of $x^d = 1$ in symmetric groups, Can. J. Math. *7* (1955), 159-168.

[52] P.G. Neumann, A note on periodicities of preferential arrangement numbers, Amer. Math. Monthly *72* (1965), 157.

[53] J. Petersen, Beviser for Wilsons og Fermats Theoremer, Tidsskift for Mathematic (3) *2* (1872), 64-65.

[54] P. Pleasants, personal communication.

[55] C.R. Pranesachar, Enumeration of Latin rectangles via SDR's in *Combinatorics and Graph Theory*, ed. S.B. Rao, Lecture Notes in Mathematics *885*, Springer-Verlag, 1981, pp. 380-390.

[56] Chr. Radoux, Nouvelles propriétés arithmétiques des nombres de Bell, Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 2, Exp. No. 22. 12 pp. Secrétariat Mathématique, Paris, 1975.

[57] Chr. Radoux, Arithmétique des nombres de Bell et analyse p-adique, Bull. Soc. Math. de Belgique (B) *29* (1977), 13-28.

[58] R.C. Read and N.C. Wormald, Number of labelled 4-regular graphs, J. Graph Theory *4* (1980), 203-212.

[59] J. Riordan, A recurrence relation for three-line Latin rectangles, Amer. Math. Monthly *59* (1952), 159-162.

[60] J. Riordan, *An Introduction to Combinatorial Analysis*, Wiley, 1968.

[61] J. Riordan, Forests of labeled trees, J. Combin. Theory *5* (1968), 90-103.

[62] G.-C. Rota and B. Sagan, Congruences derived from group action, Europ. J. Combinatorics *1* (1980), 67-76.

[63] B. Sagan, Congruences via Abelian groups, to be published.

[64] J.H. Smith, Combinatorial congruences derived from the action of Sylow subgroups of the symmetric group, to be published.

[65] H. Stevens, Generalized Kummer congruences for products of sequences, Duke Math. J. *28* (1961), 25-38.

[66] H. Stevens, Generalized Kummer congruences for the products of sequences. Applications, Duke Math. J. *28* (1961), 261-275.

[67] H. Stevens, Kummer congruences for products of numbers, Math. Nachr. *24* (1962), 219-227.

[68] H. Stevens, Kummer's congruences of a second kind, Math. Z. (1962), 180-191.

[69] H. Stevens, Some congruence properties of the Hermite polynomials, Arch. Math. *14* (1963), 391-398.

[70] J. Touchard, Propriétés arithmétique de certains nombres récurrents, Ann. Soc. Sci Bruxelles (A) *53* (1933), 21-31.

[71] J. Touchard, Nombres exponentiels et nombres de Bernoulli, Can. J. Math. *8* (1956), 305-320.

[72] G.T. Williams, Numbers generated by the function $e^{e^x}-1$, Amer. Math. Monthly *52* (1945), 323-327.