CONGRUENCE PROBLEMS INVOLVING STIRLING NUMBERS OF THE FIRST KIND

Rhodes Peele
Auburn University at Montgomery, Montgomery, AL 36117-3596

A. J. Radcliffe
University of Pennsylvania, Philadelphia, PA 19104-6395

Herbert S. Wilf*
University of Pennsylvania, Philadelphia, PA 19104-6395
(Submitted April 1991)

1. INTRODUCTION AND SUMMARY OF RESULTS

It is by now well known that the parities of the binomial coefficients show a fractal-like appearance when plotted in the x-y plane. Similarly, if $f(n,k)$ is some counting sequence and p is a prime, we can plot an asterisk at (n,k) if $f(n,k)\not\equiv 0 \pmod p$, and a blank otherwise, to get other complex, and often interesting, patterns.

For the ordinary and Gaussian binomial coefficients and for the Stirling numbers of the second kind, formulas for the number of asterisks in each column are known ([12], [2], [4], [1]). Moreover, in each row the pattern is periodic, and formulas for the minimum period have been bound ([2], [3], [6], [7], [12], [13], [9], [15]) in all three cases.

If $\left[{n \atop k}\right]$, the signless Stirling number of the first kind, denotes, as usual, the number of permutations of n letters that have k cycles, then for fixed k and p we will show that there are only finitely many n for which $\left[{n \atop k}\right]\not\equiv 0 \pmod p$, i.e., there are only finitely many asterisks in each row of the pattern. Let $v(n,k)$ be the number of these.

To describe the generating function of the $v(n,k)$ we first need to define a *special integer modulo p*. We say that a nonnegative integer n is special modulo p if

$$n \bmod p+\left\lfloor \frac{n}{p}\right\rfloor \le p-1.$$

This means that n is a 1- or 2-digit p-ary integer and, in the addition of n to its digit reversal, there is no carry out of the units place. We denote by N_p the (finite) set of all special integers modulo p, and we write $N_p(x)$ for the polynomial $\sum_{n\in N_p} x^n$; e.g., $N_3(x)=1+x+x^2+x^3+x^4+x^6$.

Finally, we denote by c_p the finite sequence that is defined by $c_p(0)=1$ and

$$c_p(i)=\left|\left\{n\le p-1:\left[{n \atop i}\right]\not\equiv 0 \pmod p\right\}\right| \quad (1\le i\le p-1).$$

We write $C_p(x)$ for the polynomial $\sum_{0\le i\le p-1} c_p(i)x^i$; e.g., $C_3(x)=1+2x+x^2$.

* Supported in part by the United States Office of Naval Research.

Theorem A: The number $v(k,p)$ of $n \geq 0$ such that $\left[{n \atop k}\right] \not\equiv 0 \pmod{p}$ is given by

$$\sum_{k\geq 0} v(k,p)x^k = C_p(x)\prod_{j\geq 0} N_p(x^{p^j})$$

As an illustration of Theorem A, take $p = 3$. Then $C_3(x) = 1+2x+x^2$, and so

$$\begin{aligned}\sum_{k\geq 0} v(k,3)x^k &= (1+2x+x^2)\prod_{j\geq 0} N_3(x^{3^j}) \\ &= 1+3x+4x^2+5x^3+7x^4+7x^5+7x^6+9x^7+8x^8+12x^{10} \\ &\quad +12x^{11}+12x^{12}+16x^{13}+15x^{14}+13x^{15}+15x^{16}+12x^{17}+\cdots.\end{aligned}$$

Thus there are, for example, 12 values of n for which $\left[{n \atop 17}\right]$ is not a multiple of 3. In Corollary 2.2 below we will see that the largest of these is $\left[{kp \atop k}\right] = \left[{51 \atop 17}\right]$ (which has 59 decimal digits).

Along the way to proving Theorem A we will find the following result, which seems to be of independent interest.

Theorem B: Let $k \geq 0$ and p be a fixed integer and prime, respectively. Then the following two sets are equinumerous:

- The set of all $j \leq k/(p-1)$ for which the binomial coefficient $\binom{k-(p-1)j}{j} \not\equiv 0 \pmod{p}$, and
- The set of all partitions of the integer k into parts that are powers of p, and in which the multiplicity of each part is special modulo p.

Although we find Theorem B by means of generating functions, the form of the result suggests that there may be a natural bijection between the two sets. We will give such a bijection also.

Our results dualize, in an interesting way, results of Carlitz [1]. He studied similar questions for the Stirling numbers of the second kind. More precisely, he studied the number of k for which $\left\{{n \atop k}\right\}$ is not divisible by p and deduced infinite product-generating functions for these numbers that are quite similar to ours. His results are complete if p = 2, 3, 5, but only partial for other values of p. The duality of the questions and the similarity of the answers are arresting.

2. AN ANALOG OF LUCAS'S CONGRUENCE

Lucas's congruence ([2], [8]) for binomial coefficients asserts that

$$\binom{n'p+n_0}{k'p+k_0} \equiv \binom{n'}{k'}\binom{n_0}{k_0} \pmod{p}$$

if n', k', n_0, and k_0 are nonnegative integers with n_0 and k_0 less than p. It is easily proved by viewing $(x+1)^{n'p+n_0} = (x+1)^{n'p}(x+1)^{n_0}$ as an identity over $GF(p)[x]$ and using the "freshman" $\left((x+1)^p \equiv x^p+1\right)$ and binomial theorems. By imitating this proof we can get a somewhat similar congruence for the residue modulo p of $\left[{n \atop k}\right]$.

Recall that

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \text{ for } n, k > 0,$$

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = 0 \text{ for } n > 0, \ \begin{bmatrix} 0 \\ k \end{bmatrix} = 0 \text{ for } k > 0, \text{ and } \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1.$$

Further recall that the ordinary generating function for $\left\{\begin{bmatrix} n \\ \cdot \end{bmatrix}\right\}$ is

$$s_n(x) = x(x+1)(x+2)\cdots(x+n-1).$$

For the remainder of this section, all of our computations will take place in the polynomial ring $GF(p)[x]$. To begin with, note that $s_0(x) = 1$ is the only $s_n(x)$ with a constant term, and that

(1) $$s_p(x) = x^p - x$$

in $GF(p)[x]$ since both sides of (1) are polynomials of degree p with simple roots $r = 0, 1, \ldots, p-1$ and leading coefficient 1.

Lemma 1: For all n,

(2) $$s_n(x) \equiv x^{n'}(x^{p-1}-1)^{n'} s_{n_0}(x) \pmod p$$

where $n' = \lfloor n/p \rfloor$, $n_0 = n \bmod p$.

Proof: We have $n = n'p + n_0$ with $0 \le n_0 < p$. Then

$$\begin{aligned} s_n(x) &= \prod_{t=0}^{n'-1}(x+tp)(x+tp+1)\cdots(x+tp+p-1)\cdot\prod_{u=0}^{n_0-1}(x+n'p+u) \\ &= \prod_{t=0}^{n'-1} x(x+1)\cdots(x+p-1)\cdot\prod_{u=0}^{n_0-1}(x+u) = s_p(x)^{n'} s_{n_0}(x) \\ &= (x^p - x)^{n'}\cdot s_{n_0}(x) \end{aligned}$$

where empty products are interpreted as 1. □

If we simply equate coefficients of like powers of x on both sides of (2), we obtain the known

Proposition 2.1: Let p be prime and let n and k be integers with $1 \le k \le n$. Let $n' = \lfloor n/p \rfloor$, $n_0 = n \bmod p$. Define integers i and j as follows:

(3) $$k - n' = j(p-1) + i \quad \begin{array}{l}(0 \le i < p-1 \ \text{ if } n_0 = 0; \\ \ 0 < i \le p-1 \ \text{ if } n_0 > 0).\end{array}$$

Then

(4) $$\begin{bmatrix} n \\ k \end{bmatrix} = (-1)^{n'-j}\binom{n'}{j}\begin{bmatrix} n_0 \\ i \end{bmatrix} \pmod p.$$

Corollary 2.2: For a fixed k, the set $\left\{n : \begin{bmatrix} n \\ k \end{bmatrix} \not\equiv 0 \pmod p\right\}$ is finite. Its largest element is pk and its smallest is k.

Proof: If $n > pk$, then in (3) above $j < 0$ and so $\left[{n \atop k}\right] = 0 \pmod p$. If $n = pk$, then $n' = n_0 = i = j = 0$ and $\left[{pk \atop k}\right] = (-1)^k \pmod p$. If $n = k$ then $n' = j$, $n_0 = i$, and $\left[{k \atop k}\right] = 1 \pmod p$. If $n < k$, then either $n' < j$ or $n_0 < i$. In either case, $\left[{n \atop k}\right] = 0 \pmod p$. □

Comments: There are other approaches to Proposition 2.1. One [5] uses a double induction, first on k with $\lfloor n/p \rfloor = 1$, and then on $\lfloor n/p \rfloor$. Another [11] uses abelian group actions to prove an additive congruence for $\left[{n+p \atop k}\right]$, and then induction on n.

To obtain a more explicit form of the congruence (4) for $k \le n \le pk$, we can use the following iterated form of Lucas's congruence: If $(n'_s, n'_{s-1}, \dots, n'_0)_p$ and $(j_s, j_{s-1}, \dots, j_0)_p$ are the p-ary representations of the nonnegative integers n' and j, then

$$\binom{n'}{j} = \binom{n'_s}{j_s}\binom{n'_{s-1}}{j_{s-1}}\cdots\binom{n'_0}{j_0} \pmod p.$$

Therefore,

$$\left[{n \atop k}\right] \equiv (-1)^{n'-j}\binom{n'_s}{j_s}\binom{n'_{s-1}}{j_{s-1}}\cdots\binom{n'_0}{j_0}\left[{n_0 \atop i}\right] \pmod p \tag{5}$$

where $k = ej + i$, $0 \le i < e$; $n = en' + n_0 < e$, and $(n'_s, n'_{s-1}, \dots, n'_0)_p$ and $(j_s, j_{s-1}, \dots, j_0)_p$ are the p-ary expansions of n' and j as before.

3. EVALUATION OF $\left|\left\{k : \left[{n \atop k}\right] \not\equiv 0 \pmod p\right\}\right|$

For completeness, and since its proof is now quite simple, we recall the following result [10].

Theorem 3.1: For n fixed, the number $h(n,p)$ of Stirling numbers of the first kind that are not multiples of the prime p is given by

$$h(n,p) = (n_s+1)(n_{s-1}+1)\cdots(n_1+1)h(n_0,p)$$

where $(n_s, n_{s-1}, \dots, n_0)_p$ is the p-ary representation of n.

Proof: We count the nonzero terms of the polynomial $s_n(x) \in GF(p)[x]$, making use of (2). The number of nonzero terms in $s_{n_0}(x) \in GF(p)[x]$ is by definition $h(n_0,p)$, and the degrees of any two of its nonzero terms differ by less than $p-1$. To count the nonzero terms in $(x^{p-1}-1)^{n'}$ $GF(p)[x]$, we make use of the following well-known [2] corollary of Lucas's congruence (in iterated form): If $(m_s, m_{s-1}, \dots, m_0)_p$ is the p-ary representation of m, then the number of nonzero terms of $(a+b)^m \in GF(p)[a,b]$ is $\prod_{j=0}^{s}(m_j+1)$. Since $(n_s, n_{s-1}, \dots, n_1)_p$ is the p-ary representation of n', it follows that $(x^{p-1}-1)^{n'} \in GF(p)[x]$ has $(n_s+1)(n_{s-1}+1)\cdots(n_1+1)$ nonzero terms, the degrees of any two of which differ by at least $p-1$. Therefore, $s_n(x) \in GF(p)[x]$ has $(n_s+1)(n_{s-1}+1)\cdots(n_1+1)h(n_0,p)$ nonzero terms.

4. EVALUATION OF $\left|\left\{n: \left[{n \atop k}\right] \not\equiv 0 \pmod p\right\}\right|$

We now consider the more difficult problem of determining for fixed k the number of n such that $\left[{n \atop k}\right]$ is a nonmultiple of p. In this section we will reduce this to a problem concerning binomial coefficients, and in the next section we will solve the latter problem. For p prime and $k \geq 0$ define

$$v(k,p) = \left|\left\{n : \left[{n \atop k}\right] \not\equiv 0 \pmod p\right\}\right|;$$

$$b(k,p) = \left|\left\{j : k-(p-1)j \geq 0 \text{ and } \binom{k-(p-1)j}{j} \not\equiv 0 \mod p\right\}\right|.$$

Theorem 4.1 Let $c_p(0) = 1$ and

$$c_p(i) = \left|\left\{n \leq p-1 : \left[{n \atop i}\right] \not\equiv 0 \pmod p\right\}\right| \quad (1 \leq i \leq p-1).$$

Then for all $k \geq 0$,

$$v(k,p) = c_p(0)b(k,p) + c_p(1)b(k-1,p) + \cdots + c_p(p-1)b(k-p+1,p). \tag{6}$$

Proof: For k and p fixed, let each n such that $k \leq n \leq pk$ determine n_0, n', i and j as in Proposition 2.1. Then

$$\begin{aligned} v(k,p) &= \left|\left\{n : k \leq n \leq kp \text{ and } \binom{k-i-(p-1)j}{j}\left[{n_0 \atop i}\right] \not\equiv 0 \pmod p\right\}\right| \\ &= \sum_{i=0}^{p-1}\sum_{n_0=i}^{p-1}\left|\left\{j : k-i-(p-1)j \geq 0 \text{ and } \binom{k-i-(p-1)j}{j}\left[{n_0 \atop i}\right] \not\equiv 0 \pmod p\right\}\right| \\ &= \sum_{i=0}^{p-1} c_p(i)\left|\left\{j : k-i-(p-1)j \geq 0 \text{ and } \binom{k-i-(p-1)j}{j} \not\equiv 0 \pmod p\right\}\right| \\ &= \sum_{i=0}^{p-1} c_p(i) b(k-i,p). \quad \square \end{aligned}$$

Comment: The first few coefficient sequences c_p are:

$c_2 : (1,1)$; $c_3 : (1,2,1)$; $c_5 : (1,4,3,2,1)$; $c_7 : (1,6,5,3,3,2,1)$;
$c_{11} : (1,10,7,8,7,6,5,4,3,2,1)$.

5. DETERMINATION OF THE $b(k,p)$

Theorem 5.1: Let $k = pm + r$ with $0 \leq r < p$ and $m \geq 0$. Then

$$b(k,p) = b(mp+r,p) = b(m,p) + b(m-1,p) + \cdots + b(m-p+r+1,p). \tag{7}$$

Proof: In the following computation, all binomial coefficients $\binom{a}{b}$ mentioned are implicitly assumed to be "classical" (i.e., a and b are nonnegative integers), and since the argument hinges on Lucas's congruence, one of the details that should be checked is that if they start out as such, then they remain so throughout the computation.

$$\begin{aligned} b(pm+r,p) &= \left|\left\{t : \binom{pm+r-(p-1)t}{t} \not\equiv 0 \pmod p\right\}\right| \\ &= \sum_{j=0}^{p-1}\left|\left\{s : \binom{pm+r-(p-1)(ps+j)}{ps+j} \not\equiv 0 \pmod p\right\}\right| \\ &= \sum_{j=0}^{p-r-1}\left|\left\{s : \binom{p(m-(p-1)s-j)+r+j}{ps+j} \not\equiv 0 \pmod p\right\}\right| \\ &\qquad + \sum_{j=p-r}^{p-1}\left|\left\{s : \binom{p(m-(p-1)s-j+1)+r+j-p}{ps+j} \not\equiv 0 \pmod p\right\}\right| \end{aligned}$$

where the last sum is the empty sum if $r=0$. Applying Lucas's congruence to the last two sums, we get

$$\begin{aligned} b(pm+r,p) &= \sum_{j=0}^{p-r-1}\left|\left\{s : \binom{m-(p-1)s-j}{s}\binom{r+j}{j} \not\equiv 0 \pmod p\right\}\right| \\ &\qquad + \sum_{j=p-r}^{p-1}\left|\left\{s : \binom{m-(p-1)s-j+1}{s}\binom{r+j-p}{j} \not\equiv 0 \pmod p\right\}\right| \\ &= \sum_{j=0}^{p-r-1}\left|\left\{s : \binom{m-j-(p-1)s}{s} \not\equiv 0 \pmod p\right\}\right| = \sum_{j=0}^{p-r-1} b(m-j,p). \end{aligned}$$

□

6. PROOFS OF THEOREMS A AND B

From the recurrence relation of Theorem 5.1 it is easy to obtain the generating function of the $\{b(\cdot,p)\}$, as follows. Define $B_p(x)=\sum_{k\ge0} b(k,p)x^k$. Then multiply both sides of (7) by x^{mp+r} and sum over $m\ge0$, $0\le r\le p-1$. There results

$$\begin{aligned} B_p(x) &= \sum_{m\ge0}\sum_{r=0}^{p-1} x^{mp+r}\sum_{j=0}^{p-r-1} b(m-j,p) \\ &= \sum_{r=0}^{p-1} x^r \sum_{j=0}^{p-r-1} x^{jp}\sum_{m\ge0} b(m-j,p)x^{p(m-j)} = B_p(x^p)\left\{\sum_{r=0}^{p-1} x^r \sum_{j=0}^{p-r-1} x^{jp}\right\}. \end{aligned}$$

The quantity in curly braces in the rightmost member is exactly the generating function $N_p(x)$ that was defined in section 1 above. Hence, $B_p(x)=N_p(x)B_p(x^p)$ and, therefore, by iteration, the generating function of the $b(\cdot,p)$ is

$$B_p(x)=\prod_{j\ge0} N_p(x^{p^j})=\sum_{k\ge0} b(k,p)x^k. \tag{8}$$

The infinite product that occurs in (8) is well known (e.g., [14, Eq. (3.16.4)]) to generate the number of partitions of the integer k into powers of p, each taken with a multiplicity that is special modulo p, as defined in section 1 above, and the proof of Theorem B is complete.

Theorem A now follows from this result and Theorem 4.1. Indeed, equation (6) above, when translated into generating function terms, states that the generating function of the $\{\nu(k,p)\}$ is $C_p(x)B_p(x)$, as claimed. □

7. BIJECTIVE PROOF OF THEOREM B

As promised in the introduction, we will give here a bijective proof of Theorem B. We let $\Pi(n, \mathcal{P}, \mathcal{M})$ denote the set of all partitions of the integer n into parts that all belong to $\mathcal{P}$, each having a multiplicity that belongs to $\mathcal{M}$. Set $\mathcal{P}_p = \{p^i : i \geq 0\}$ and $\mathcal{M}_p \{a : a \text{ is special for } p\}$.

We will exhibit an explicit bijection between the sets

$$A_{n,p} = \left\{ j \in \{0, 1, \ldots, \lfloor n/p \rfloor\} : \binom{n-(p-1)j}{j} \not\equiv 0 \pmod p \right\}$$

$$B_{n,p} = \Pi(n, \mathcal{P}_p, \mathcal{M}_p).$$

To do this, note first that Lucas's theorem gives a simple criterion for deciding whether a given j belongs to $A_{n,p}$; it says that

$$\binom{n-(p-1)j}{j} \equiv \binom{b_k}{a_k}\binom{b_{k-1}}{a_{k-1}} \cdots \binom{b_0}{a_0} \pmod p,$$

where the b's and the a's are the p-ary digits of $n-(p-1)j$ and of j, respectively. In particular, the left side is not congruent to 0 provided that $a_i \leq b_i$ for all i.

We will now define a mapping $\phi : \{0, 1, \ldots, \lfloor n/p \rfloor\} \to \Pi(n, \mathcal{P}_p, \mathbf{N})$ as follows: $\phi(j)$ is that partition of the integer n in which, for all i, the part p^i occurs with multiplicity $b_i + (p-1)a_i$, and no other parts occur. Since $\Sigma a_i p^i$ and $n-(p-1)j = \Sigma b_i p^i$, it is clear that $\phi(j)$ is indeed a partition of n into powers of p.

To show that ϕ restricts to a bijection between $A_{n,p}$ and $B_{n,p}$, it is necessary to check that for $j \in A_{n,p}$ the image $\phi(j)$ is in $B_{n,p}$, and that the restriction is invertible. Consider then a $j \in A_{n,p}$, i.e., a j for which $a_i \leq b_i$ for all i. Now the number of parts of size p^i in $\phi(j)$ is

$$b_i + (p-1)a_i = pa_i + (b_i - a_i).$$

Since $0 \leq a_i \leq b_i \leq p-1$, the multiplicity of p^i is $(a_i(b_i - a_i))_p$ in p-ary notation, and thus belongs to $\mathcal{M}_p$. We have shown that $\phi(A_{n,p}) \subset B_{n,p}$.

Finally, if $\pi \in B_{n,p}$ is given, define $\psi(\pi) \in A_{n,p}$ by its p-ary expansion—the i^{th} digit of $\psi(\pi)$ is a_i, where $m_i = (a_i, c_i)_p$ is the multiplicity of p^i in π. So

$$\psi(\pi) = (a_k, a_{k-1}, \ldots, a_0)_p \quad \text{and} \quad n - p\psi(\pi) = (c_k, c_{k-1}, \ldots, c_0)_p.$$

Further, $n-(p-1)\psi(\pi) = ((a_k + c_k), (a_{k-1} + c_{k-1}), \ldots, (a_0 + c_o))_p$. The last expression is a legitimate p-ary expansion because each m_i is special for p, and moreover it shows that

$$\binom{n-(p-1)\psi(\pi)}{\psi(\pi)} \not\equiv 0 \pmod p.$$

It is clear that ψ and ϕ are inverses.

REFERENCES

1. L. Carlitz. "Some Partition Problems Related to the Stirling Numbers of the Second Kind." *Acta. Arith.* **10** (1965):409-22.
2. N. J. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* **54** (1947):589-92.
3. R. Fray. "Congruence Properties of Ordinary and q-Binomial Coefficients." *Duke Math. J.* **34** (1967):467-80.
4. F. T. Howard. "Prime Divisors of q-Binomial Coefficients." *Rend. Sem. Mat. Univ. Padova* **48** (1972):181-88.
5. F. T. Howard. "Congruences for the Stirling and Associated Stirling Numbers." *Acta. Arith.* **55** (1990):29-41.
6. Y. H. H. Kwong. "Minimum Periods of $\left[{n \atop k}\right]$ Modulo M." *Fibonacci Quarterly* **27.3** (1989): 217-21.
7. Y. H. H. Kwong. "Minimum Periods of Binomial Coefficients Modulo M." *Fibonacci Quarterly* **27.4** (1989):348-51.
8. E. Lucas. "Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier." *Bull. Soc. Math. France* **6** (1877-1878):49-54.
9. A. Nijenhuis & H. S. Wilf. "Periodicities of Partition Functions and Stirling Numbers Modulo p." *J. Number Theory* **25** (1987):308-12.
10. R. Peele. "Divisibility Patterns for Some Combinatorial Sequences." (To appear.)
11. B. Sagan. "Congruences via Abelian Groups." *J. Number Theory* **20** (1985):210-37.
12. D. Singmaster. "Divisibility of Binomial and Multinomial Coefficients by Primes and Prime Powers." In *A Collection of Manuscripts Related to the Fibonacci Sequence: 18th Anniversary Volume of the Fibonacci Association*, ed. V. E. Hoggatt, Jr., & M. Bicknell-Johnson, pp. 98-113. Santa Clara, Calif: The Fibonacci Association, 1980.
13. W. F. Trench. "On Periodicities of Certain Sequences of Residues." *Amer. Math. Monthly* **67** (1960):652-56.
14. H. Wilf. *generatingfunctionology*. Boston: Academic Press, 1990.
15. S. Zabek. "Sur la périodicité modulo m des suites des nombres $\binom{n}{k}$." *Ann. Univ. Mariæ Curie-Sklodowska*, Sect. A **10** (1956):37-47.

AMS Classification Numbers: 05A15, 11B73

❖❖❖

(continued from page 81-referees)