MORE BINOMIAL COEFFICIENT CONGRUENCES

D. F. Bailey
Trinity University, San Antonio, TX 78212
(Submitted May 1990)

1. Introduction

In 1878 Edouard Lucas gave the following result for computing binomial coefficients modulo a prime [3], [4].

Theorem 1.1: If p is a prime, n, r, n_0, and r_0 are nonnegative integers, and n_0 and r_0 are both less than p, then

$$\binom{np+n_0}{rp+r_0} \equiv \binom{n}{r}\binom{n_0}{r_0} \pmod{p}.$$

We have recently derived the following variations of Lucas' Theorem (see [1]).

Theorem 1.2: If n and r are nonnegative integers, and p is prime, then

$$\binom{np}{rp} \equiv \binom{n}{r} \pmod{p^2}.$$

Theorem 1.3: If n and r are nonnegative integers, and p is a prime greater than 3, then

$$\binom{np}{rp} \equiv \binom{n}{r} \pmod{p^3}.$$

In [2] we have also obtained the following congruences which bear a strong resemblance to the theorem of Lucas.

Theorem 1.4: If p is prime, n and r are nonnegative integers, and i is an integer strictly between 0 and p, then

$$\binom{np}{rp+i} \equiv (r+1)\binom{n}{r+1}\binom{p}{i} \pmod{p^2}.$$

Theorem 1.5: If $p \geq 5$ is prime, n, m, and k are nonnegative integers, $k < p$, and i is an integer strictly between 0 and p, then

$$\binom{mp^2}{np^2+kp+i} \equiv (n+1)\binom{m}{n+1}\binom{p^2}{kp+i} \pmod{p^3}.$$

In this paper we show that in fact an infinite sequence of results like those above hold. In our proofs we need the following result (see, e.g., [5]).

Theorem 1.6: If p is prime, $n = p^s$, and p^t divides k while p^{t+1} does not divide k, then p^{s-t} divides $\binom{n}{k}$ and p^{s-t+1} does not divide $\binom{n}{k}$.

2. Main Results

Our first result is as follows.

Theorem 2.1: If $p \geq 5$ is prime, n and m are nonnegative integers, s and all the a_k are integers with $s \geq 1$, $0 < a_0 < p$, and $0 \leq a_k < p$ for $k = 1, 2, \ldots, s-1$, then

$$\binom{mp^s}{np^s + a_{s-1}p^{s-1} + \cdots + a_1p + a_0}$$

$$\equiv (n+1)\binom{m}{n+1}\binom{p^s}{a_{s-1}p^{s-1} + \cdots + a_1p + a_0} \pmod{p^{s+1}}.$$

Proof: Theorems 1.4 and 1.5 show that the conclusion of the theorem is valid for $s = 1$ and $s = 2$. We assume therefore that the theorem's conclusion holds for some $s \geq 2$ and consider the assertion

$$\binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv (n+1)\binom{m}{n+1}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

If $m = 0$ the assertion above is merely that $0 \equiv 0$. Likewise, if $m = 1$ one can check that our inductive assertion holds trivially. Therefore, we assume the validity of the inductive assertion for some $m \geq 1$ and consider first the case in which $n = 0$. Then we must treat

$$\binom{(m+1)p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} = \sum_{j=0}^{a_sp^s + \cdots + a_1p + a_0}\binom{mp^{s+1}}{a_sp^s + \cdots + a_0 - j}\binom{p^{s+1}}{j}.$$

We first show that whenever $0 < j < a_sp^s + \cdots + a_1p + a_0$, we have

$$\binom{mp^{s+1}}{a_sp^s + \cdots + a_1p + a_0 - j}\binom{p^{s+1}}{j} \equiv 0 \pmod{p^{s+2}}. \tag{1}$$

To this end, let $j = b_sp^s + \cdots + b_1p + b_0$ and note that, if $b_0 \neq 0$, then Theorem 1.6 shows that

$$\binom{p^{s+1}}{j} \equiv 0 \pmod{p^{s+1}}.$$

Moreover, by Theorem 1.1,

$$\binom{mp^{s+1}}{a_sp^s + \cdots + a_0 - j} = \binom{mp^{s+1}}{c_sp^s + \cdots + c_0}$$

$$\equiv \binom{m}{0}\binom{0}{c_s}\binom{0}{c_{s-1}} \cdots \binom{0}{c_0} \equiv 0 \pmod{p},$$

since not all the c_i are zero. Hence, we have the product in (1) congruent to 0 modulo p^{s+2} as desired. If, on the other hand, $b_0 = 0$, we see that

$$\binom{mp^{s+1}}{a_sp^s + \cdots + a_0 - j} = \binom{mp^{s+1}}{c_sp^s + \cdots + c_1p + a_0}$$

and that this last is congruent to zero modulo p^{s+1} since $a_0 \neq 0$ by hypothesis. Likewise, one can argue that

$$\binom{p^{s+1}}{j} \equiv 0 \pmod{p},$$

and again the product in (1) is congruent to 0 modulo p^{s+2}.

Therefore, we have established that

$$\binom{(m+1)p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \equiv \binom{mp^{s+1}}{a_sp^s + \cdots + a_0} + \binom{p^{s+1}}{a_sp^s + \cdots + a_0} \pmod{p^{s+2}}$$

and by the inductive hypothesis this is congruent modulo p^{s+2} to

$$(m+1)\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0}$$

which is the desired result.

Next we assume $n \neq 0$ and consider

$$\binom{(m+1)p^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_0} = \sum_{j=0}^{p^{s+1}} \binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_0 - j}\binom{p^{s+1}}{j}.$$

As previously, one can show that all terms in the above sum are congruent to 0 modulo p^{s+2} save those where $j = 0$, $j = p^{s+1}$, or $j = a_sp^s + \cdots + a_0$. So, thus far, we have

$$\binom{(m+1)p^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1 + a_0}$$

$$\equiv \binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0} + \binom{mp^{s+1}}{np^{s+1}}\binom{p^{s+1}}{a_sp^s + \cdots + a_0}$$

$$\binom{mp^{s+1}}{(n-1)p^{s+1} + a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

Now consider the terms on the right-hand side of the above congruence. By the inductive assumption

$$\binom{mp^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv (n+1)\binom{m}{n+1}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

Moreover, since

$$\binom{mp^{s+1}}{np^{s+1}} - \binom{m}{n} \equiv 0 \pmod{p} \text{ and } \binom{p^{s+1}}{a_sp^s + \cdots + a_0} \equiv 0 \pmod{p^{s+1}},$$

$$\binom{mp^{s+1}}{np^{s+1}}\binom{p^{s+1}}{a_sp^s + \cdots + a_0} \equiv \binom{m}{n}\binom{p^{s+1}}{a_sp^s + \cdots + a_0} \pmod{p^{s+2}}.$$

And calling on the inductive assumption once again, we see that

$$\binom{mp^{s+1}}{(n-1)p^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv n\binom{m}{n}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0} \pmod{p^{s+2}}.$$

Thus, we conclude that

$$\binom{(m+1)p^{s+1}}{np^{s+1} + a_sp^s + \cdots + a_1p + a_0}$$

$$\equiv \left[(n+1)\binom{m}{n+1} + \binom{m}{n} + n\binom{m}{n}\right]\binom{p^{s+1}}{a_sp^s + \cdots + a_0} \pmod{p^{s+2}}.$$

But this last expression is obviously

$$(n+1)\binom{m+1}{n+1}\binom{p^{s+1}}{a_sp^s + \cdots + a_1p + a_0}.$$

This completes the induction and establishes the theorem.

Our next result generalizes that of Theorem 1.3.

Theorem 2.2: If $p \geq 5$ is prime and k, r, and s are all nonnegative integers, then

$$\binom{kp^{s+1}}{rp^{s+1}} \equiv \binom{kp^s}{rp^s} \pmod{p^{s+3}}.$$

Proof: We proceed by induction. For $s = 0$ the assertion is identical with that of Theorem 1.3. We therefore assume the result for some $s \geq 0$ and consider the assertion

$$(2) \qquad \binom{kp^{s+2}}{rp^{s+2}} \equiv \binom{kp^{s+1}}{rp^{s+1}} \pmod{p^{s+4}}.$$

Obviously assertion (2) holds for $r = 0$. Thus, we fix $r \geq 1$, assume (2) holds for all smaller r, and establish our assertion by induction on k. Assertion (2) clearly holds for $k \leq r$, so we assume its validity for some fixed $k \geq r$ and consider

$$\binom{(k+1)p^{s+2}}{rp^{s+2}} = \sum_{i=0}^{p^{s+2}} \binom{kp^{s+2}}{rp^{s+2} - i}\binom{p^{s+2}}{i} = \sum_{i=0}^{p^{s+1}} \binom{kp^{s+2}}{rp^{s+2} - lp}\binom{p^{s+2}}{lp} + B$$

where B is the sum of those terms of the form

$$\binom{kp^{s+2}}{rp^{s+2} - i}\binom{p^{s+2}}{i} \quad \text{for } i \text{ not a multiple of } p.$$

As in Theorem 2.1, it is easy to show that each summand in B is congruent to 0 modulo p^{s+4}. Therefore, we have

$$(3) \qquad \binom{(k+1)p^{s+2}}{rp^{s+2}} \equiv \sum_{l=0}^{p^{s+1}} \binom{kp^{s+2}}{rp^{s+2} - lp}\binom{p^{s+2}}{lp} \pmod{p^{s+4}}.$$

Now we consider a particular summand in (3) with $0 < l < p^{s+1}$ so that

$$l = a_s p^s + a_{s-1}p^{s-1} + \cdots + a_q p^q \text{ where } a_q \neq 0 \text{ and } 0 \leq q \leq s.$$

Then

$$\binom{p^{s+2}}{lp} = \binom{p^{s+1-q}p^{q+1}}{(a_s p^{s-q} + \cdots + a_q)p^{q+1}}$$

$$\equiv \binom{p^{s+1-q}p^q}{(a_s p^{s-q} + a_{s-1}p^{s-q-1} + \cdots + a_q)p^q} \pmod{p^{q+3}}$$

by inductive assumption. But this simply says

$$\binom{p^{s+2}}{lp} \equiv \binom{p^{s+1}}{l} \pmod{p^{q+3}}.$$

One can also show

$$\binom{p^{s+1}}{l} \equiv 0 \pmod{p^{s+1-q}},$$

$$\binom{kp^{s+2}}{rp^{s+2} - lp} \equiv \binom{kp^{s+1}}{rp^{s+1} - l} \pmod{p^{q+3}},$$

and

$$\binom{kp^{s+2}}{rp^{s+2} - lp} \equiv 0 \pmod{p^{s+1-q}}.$$

Therefore,

$$\binom{p^{s+2}}{lp}\binom{kp^{s+2}}{rp^{s+2}-lp} \equiv \binom{p^{s+1}}{l}\binom{kp^{s+2}}{rp^{s+2}-lp} \pmod{p^{s+4}}$$

and

$$\binom{p^{s+1}}{l}\binom{kp^{s+1}}{rp^{s+2}-lp} \equiv \binom{p^{s+1}}{l}\binom{kp^{s+1}}{rp^{s+1}-l} \pmod{p^{s+4}}.$$

It follows then that

$$\binom{p^{s+2}}{lp}\binom{kp^{s+2}}{rp^{s+2}-lp} \equiv \binom{p^{s+1}}{l}\binom{kp^{s+1}}{rp^{s+1}-l} \pmod{p^{s+4}}.$$

Now if we note finally that the inductive hypotheses on k and r insure that

$$\binom{kp^{s+2}}{rp^{s+2}} \equiv \binom{kp^{s+1}}{rp^{s+1}} \pmod{p^{s+4}}$$

holds, as does a similar statement with r replaced by $r - 1$, we see that

$$\binom{(k+1)p^{s+2}}{rp^{s+2}} \equiv \sum_{l=0}^{p^{s+1}} \binom{kp^{s+1}}{rp^{s+1}-l}\binom{p^{s+1}}{l} \pmod{p^{s+4}}.$$

But this clearly gives

$$\binom{(k+1)p^{s+2}}{rp^{s+2}} \equiv \binom{(k+1)p^{s+1}}{rp^{s+1}} \pmod{p^{s+4}}.$$

This completes the inductive proof of assertion (2) and establishes the theorem.

Remark: Professor Ira Gessel has called the author's attention to a result which implies Theorem 2.2. See Ira Gessel, "Some Congruences for Generalized Euler Numbers," *Can. J. Math.* *35.4* (1983):687-709.

References

1. D. F. Bailey. "Two p^3 Variations of Lucas' Theorem." *J. Number Theory* *35.2* (1990):208-15.
2. D. F. Bailey. "Some Binomial Coefficient Congruences." *Applied Math. Letters* *4.4* (1991):1-5.
3. N. J. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* *54* (1947):589-92.
4. Edouard Lucas. "Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier." *Bull Soc. Math. France* *6* (1878):49-54.
5. David Singmaster. "Divisibility of Binomial and Multinomial Coefficients by Primes and Prime Powers." *A Collection of Manuscripts Related to the Fibonacci Sequence*. Santa Clara, Calif: The Fibonacci Association, 1980, pp. 98-113.

*****