JOURNAL OF NUMBER THEORY 35, 208–215 (1990)

Two p^3 Variations of Lucas' Theorem

D. F. BAILEY

Department of Mathematics, Trinity University, San Antonio, Texas 78212

Communicated by R. L. Graham

Received August 28, 1989

In 1878 Lucas established a method of computing binomial coefficients modulo a prime. We establish the following variations of Lucas' Theorem. If n, r, n_0, and r_0 are non-negative integers, $p \geqslant 5$ is prime, and n_0, r_0 are less than p, then

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

and

$$\binom{np^3+n_0}{rp^3+r_0} \equiv \binom{n}{r}\binom{n_0}{r_0} \pmod{p^3}.$$

A theorem of Édouard Lucas [2, 4] tells us how to compute binomial coefficients modulo a prime. One statement of Lucas' Theorem is as follows.

THEOREM 1. *If p is a prime, N, R, n_0, and r_0 are non-negative integers, and n_0 and r_0 are both less than p, then*

$$\binom{Np+n_0}{Rp+r_0} \equiv \binom{N}{R}\binom{n_0}{r_0} \pmod{p}.$$

In [1] we have shown that one may replace p by p^2 at various points in the above congruence, but only at the expense of restricting n_0 and r_0 more so than would be the case in a true generalization of Lucas' result. In particular we have established:

THEOREM 2. *If k and r are non-negative integers and p is prime, then*

$$\binom{kp}{rp} \equiv \binom{k}{r} \pmod{p^2}.$$

0022-314X/90 $3.00

THEOREM 3. *If p is prime, N, R, n_0, and r_0 are non-negative integers, and n_0 and r_0 are both less than p, then*

$$\binom{Np^2+n_0}{Rp^2+r_0} \equiv \binom{N}{R}\binom{n_0}{r_0} \pmod{p^2}.$$

We also show in [1] that one cannot replace p^2 by a higher power of p in either of the above theorems. However, as we now know and will show, p^2 can be replaced by p^3 in Theorems 2 and 3 so long as the prime p is greater than 3. Having missed this p^3 replacement in our earlier paper we emphasize that our proof of Lemma 1 below shows that no further modification along this line is possible. That is, p^2 cannot be replaced by p^4.

LEMMA 1. *If p is a prime and $p \geqslant 5$, then,*

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Proof. Since it is well known that

$$\binom{2p}{p} = \sum_{i=0}^{p} \binom{p}{i}^2$$

and since the first and last terms of this sum are 1, we need only show that

$$\sum_{i=1}^{p-1} \binom{p}{i}^2 \equiv 0 \pmod{p^3}.$$

But it is easy to see that

$$\sum_{i=1}^{p-1} \binom{p}{i}^2 = 2\left[\binom{p}{1}^2 + \binom{p}{2}^2 + \cdots + \binom{p}{(p-1)/2}^2\right]$$

and hence we need only show that

$$\binom{p}{1}^2 + \binom{p}{2}^2 + \cdots + \binom{p}{(p-1)/2}^2 \equiv 0 \pmod{p^3}. \tag{1}$$

Now the left hand side of (1) is equal to

$$p^2\left[\left(\frac{(p-1)!}{(p-1)!\,1!}\right)^2 + \left(\frac{(p-1)!}{(p-2)!\,2!}\right)^2 + \cdots + \left(\frac{(p-1)!}{(p+1)/2)!((p-1)/2)!}\right)^2\right].$$

Therefore we are through if we can show that

$$L=\left(\frac{(p-1)!}{(p-1)!\,1!}\right)^2+\left(\frac{(p-1)!}{(p-2)!\,2!}\right)^2+\cdots$$
$$+\left(\frac{(p-1)!}{((p+1)/2)!((p-1)/2)!}\right)^2\equiv 0 \pmod{p}.$$

At this point we note that

$$\frac{(p-1)!}{(p-k)!\,k!}=\frac{(p-1)(p-2)\cdots(p-k+1)}{k!}$$
$$\equiv\frac{(-1)(-2)\cdots(-(k-1))}{k!} \pmod{p}.$$

Therefore in the field Z_p we have

$$\frac{(p-1)!}{(p-k)!\,k!}=\pm\frac{1}{k}.$$

Moreover $1/k$ is in the set

$$A=\left\{1, 2, ..., \frac{p-1}{2}\right\}$$

or in

$$B=\left\{\frac{p+1}{2}, \frac{p+3}{2}, ..., p-1\right\}.$$

But if $1/k$ is in B then $1/k=p-m$ where $m=1, 2, ..., (p-1)/2$. In this case $-1/k\equiv m \pmod{p}$ where $m\in A$. Hence the elements of

$$\left\{\left(\frac{(p-1)!}{(p-1)!\,1!}\right)^2, \left(\frac{(p-1)!}{(p-2)!\,2!}\right)^2, ..., \left(\frac{(p-1)!}{((p+1)/2)!\,((p-1)/2)!}\right)^2\right\}$$

are congruent in some order to the elements of

$$\left\{1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2\right\}.$$

Thus the sum

$$\begin{aligned} L &\equiv 1^2 + 2^2 + \cdots + \left(\frac{p-1}{2}\right)^2 \\ &= \frac{((p-1)/2)((p+1)/2)\,p}{6} \equiv 0 \pmod{p}. \end{aligned}$$

Of course, this completes the proof.

LEMMA 2. *If p is a prime and $p \geqslant 5$, then*

$$\binom{kp}{p} \equiv k \pmod{p^3}.$$

Proof. First, by comparing the coefficients of x^n in the individual expansions of $(1+x)^{(k+1)p}$ and $(1+x)^{kp}(1+x)^p$, one can see that

$$\binom{(k+1)\,p}{n} = \sum_{i=0}^{n} \binom{kp}{n-i}\binom{p}{i}. \tag{2}$$

Now, we establish the lemma by induction on k. The lemma is trivially true for $k=1$, and by Lemma 1 the lemma is true for $k=2$. Thus we make the inductive assumption that $\binom{mp}{p} \equiv m \pmod{p^3}$ for $m = 1, 2, ..., k+1$ where $k \geqslant 1$. We then consider

$$\begin{aligned} \binom{(k+2)\,p}{p} &= \binom{([k+1]+1)\,p}{p} \\ &= \sum_{i=0}^{p} \binom{(k+1)\,p}{p-i}\binom{p}{i} \\ &= \binom{(k+1)\,p}{p} + \sum_{i=1}^{p-1} \binom{(k+1)\,p}{p-i}\binom{p}{i} + 1. \end{aligned}$$

By the inductive hypothesis and Eq. (2) the last term above is congruent modulo p^3 to

$$k + 2 + \sum_{i=1}^{p-1} \binom{p}{i} \sum_{j=0}^{p-i} \binom{kp}{p-i-j}\binom{p}{j}.$$

Thus, to complete the induction, we need only show that

$$S = \sum_{i=1}^{p-1} \binom{p}{i} \sum_{j=0}^{p-i} \binom{kp}{p-i-j}\binom{p}{j} \equiv 0 \pmod{p^3}.$$

But S can be further expanded to

$$\sum_{i=1}^{p-1}\binom{p}{i}\binom{kp}{p-i}+\sum_{i=1}^{p-1}\sum_{j=1}^{p-i-1}\binom{p}{i}\binom{kp}{p-i-j}\binom{p}{j}+\sum_{i=1}^{p-1}\binom{p}{i}\binom{p}{p-i}. \tag{3}$$

Now by Lucas' Theorem each summand in the middle term in (3) is congruent to 0 modulo p^3. Moreover

$$\begin{aligned}
&\sum_{i=1}^{p-1}\binom{p}{i}\binom{kp}{p-i}+\sum_{i=1}^{p-1}\binom{p}{i}\binom{p}{p-i}\\
&\quad=\sum_{i=0}^{p}\binom{p}{i}\binom{kp}{p-i}-\binom{kp}{p}-1+\sum_{i=0}^{p}\binom{p}{i}\binom{p}{p-i}-2\\
&\quad=\binom{(k+1)p}{p}-\binom{kp}{p}+\binom{2p}{p}-3.
\end{aligned}$$

But by the inductive hypothesis the last expression above is congruent, modulo p^3, to $(k+1)-k+2-3=0$. Thus the proof is complete.

THEOREM 4. *If k and r are non-negative integers, p is a prime, and $p \geqslant 5$, then*

$$\binom{kp}{rp}\equiv\binom{k}{r} \qquad (\mathrm{mod}\ p^3).$$

Proof. Once again the proof is by induction. Observe that the result is trivially true for $r=0$ and the preceding lemma shows it is true for $r=1$. Therefore we fix $r\geqslant 2$ and assume the result for any smaller value. For this fixed r we then induct on k.

Clearly the result will hold for all $k\leqslant r$ and thus we assume the result for some $k\geqslant r$. To complete the proof we then consider $\binom{(k+1)p}{rp}$. Since $k\geqslant 2$ we write $k=m+1$ with $m\geqslant 1$. Thus, using Eq. (2), we have

$$\begin{aligned}
\binom{(k+1)p}{rp}&=\sum_{i=0}^{rp}\binom{kp}{rp-i}\binom{p}{i}=\sum_{i=0}^{p}\binom{kp}{rp-i}\binom{p}{i}\\
&=\sum_{i=0}^{p}\binom{(m+1)}{rp-i}\binom{p}{i}\\
&=\sum_{i=0}^{p}\sum_{j=0}^{rp-i}\binom{mp}{rp-i-j}\binom{p}{j}\binom{p}{i}\\
&=\sum_{i=0}^{p}\sum_{j=0}^{p}\binom{mp}{rp-i-j}\binom{p}{j}\binom{p}{i}
\end{aligned}$$

$$= \sum_{j=0}^{p} \binom{mp}{rp-j}\binom{p}{j} + \sum_{i=1}^{p-1} \sum_{j=0}^{p} \binom{mp}{rp-i-j}\binom{p}{j}\binom{p}{i}$$
$$+ \sum_{j=0}^{p} \binom{mp}{(r-1)p-j}\binom{p}{j}.$$

Now the last term above is clearly

$$\binom{(m+1)p}{rp} + \sum_{i=1}^{p-1} \sum_{j=0}^{p} \binom{mp}{rp-i-j}\binom{p}{j}\binom{p}{i} + \binom{(m+1)p}{(r-1)p}. \tag{4}$$

As in the proof of Lemma 2 one can show that the middle term in (4) is congruent to 0 modulo p^3. Moreover, by the inductive hypothesis we see

$$\binom{(m+1)p}{rp} + \binom{(m+1)p}{(r-1)p} \equiv \binom{m+1}{r} + \binom{m+1}{r-1} \pmod{p^3}$$

and it is clear that

$$\binom{m+1}{r} + \binom{m+1}{r-1} = \binom{m+2}{r} = \binom{k+1}{r}.$$

Thus we have made the inductive step and completed the proof.

It is now an easy corollary that

$$\binom{kp^3}{rp^3} \equiv \binom{k}{r} \pmod{p^3}$$

but we are able to obtain a bit more than this in Theorem 5. Our proof uses the method of Hausner [3].

THEOREM 5. *Let p be a prime greater than 3. If N, R, n_0, and r_0 are non-negative integers with n_0 and r_0 less than p then*

$$\binom{Np^3+n_0}{Rp^3+r_0} \equiv \binom{N}{R}\binom{n_0}{r_0} \pmod{p^3}.$$

Proof. (Note that in this proof we denote the cardinality of a set S by $|S|$.) First define

$$A_i = \{(i, 1), ..., (i, N)\} \qquad \text{for} \quad i = 1, ..., p^3 \ (A_i = \phi \text{ if } N = 0)$$

and

$$B = \{(0, 1), ..., (0, n_0)\} \qquad (B = \phi \text{ if } n_0 = 0).$$

Next set $A = A_1 \cup A_2 \cup \cdots \cup A_{p^3} \cup B$, define $n = Np^3 + n_0$, and note that $|A| = n$. Now define $f: A \to A$ by

$$f(i, x) = (i+1, x) \qquad \text{if} \quad 1 \leqslant i < p^3,$$
$$f(p^3, x) = (1, x) \qquad \text{and} \qquad f(0, x) = (0, x)$$

so that $f(A_i) = A_{i+1}$ for $1 \leqslant i < p^3$, $f(A_{p^3}) = A_1$, and $f(B) = B$. Obviously f^{p^3} is the identity mapping on A.

Define $r = Rp^3 + r_0$ and let X be the collection of all subsets $C \subseteq A$ such that $|C| = r$. Clearly $|f(C)| = |C|$ since f is one-to-one. Thus $f: X \to X$ and f^{p^3} is the identity on X. For any $C \in X$ we define the orbit of C as

$$O(C) = \{C, f(C), f^2(C), ..., f^{p^3-1}(C)\}.$$

Obviously $\{O(C) \mid C \in X\}$ partitions X and each $O(C)$ contains exactly 1, exactly p, exactly p^2, or exactly p^3 elements. If we denote by X_i the collection of elements in X whose orbit contains p^i points we see that $|X| = |X_0| + |X_1| + |X_2| + |X_3|$. Since it is clear that $|X| = \binom{n}{r}$ and $|X_3| \equiv 0 \pmod{p^3}$ the proof will be complete if we can show $|X_0| = \binom{N}{R}\binom{n_0}{r_0}$, and both $|X_1| \equiv 0 \pmod{p^3}$ and $|X_2| \equiv 0 \pmod{p^3}$.

Let us therefore first consider C satisfying $f(C) = C$ and think of C as

$$C = C_1 \cup C_2 \cup \cdots \cup C_{p^3} \cup C_0,$$

where $C_i \subseteq A_i$ and $C_0 \subseteq B$. Since $C_0 \subseteq B$ we must have $f(C_0) = C_0$. Likewise $f(C) = C$ and $f(C_i) \subseteq A_{i+1}$ for $1 \leqslant i < p^3$ implies $f(C_i) = C_{i+1}$ for those values of i. From the fact that f is one-to-one we then deduce that

$$|C| = p^3 |C_1| + |C_0| = r = Rp^3 + r_0.$$

Thus $|C_0| - r_0 = (R - |C_1|) p^3$ which implies that $|C_0| - r_0$ is divisible by p. But since $|C_0| \leqslant n_0 < p$ and $r_0 < p$ this means $|C_0| = r_0$ which in turn implies $|C_1| = R$. It follows then that one may choose C_1 in $\binom{N}{R}$ ways and C_0 in $\binom{n_0}{r_0}$ ways. But once C_0 and C_1 are chosen, C is completely determined. Thus

$$|X_0| = \binom{N}{R}\binom{n_0}{r_0}$$

as desired.

Next consider C satisfying $f^p(C) = C$. Since $f^p(C) = C$ we must have

$$f^p(C_1) = C_{p+1}, f^p(C_2) = C_{p+2}, ..., f^p(C_{p+1}) = C_{2p+1},$$

etc., and

$$f(C_0) = C_0.$$

Therefore C is determined as soon as we determine $C_1, C_2, ..., C_p, C_0$. Moreover

$$|C| = p^2|C_1| + p^2|C_2| + \cdots + p^2|C_p| + |C_0| = r = p^3R + r_0.$$

As before it follows that

$$r_0 = |C_0| \qquad \text{and} \qquad |C_1| + |C_2| + \cdots + |C_p| = pR.$$

Hence there are $\binom{pN}{pR}$ ways to choose $C_1, C_2, ..., C_p$ and $\binom{n_0}{r_0}$ ways to choose C_0. Thus C may be chosen in $\binom{pN}{pR}\binom{n_0}{r_0}$ ways. But this number includes all those C such that $f(C) = C$. Subtracting these out we find that, by Theorem 4,

$$\begin{aligned} |X_1| &= \binom{pN}{pR}\binom{n_0}{r_0} - \binom{N}{R}\binom{n_0}{r_0} \\ &= \binom{n_0}{r_0}\left[\binom{pN}{pR} - \binom{N}{R}\right] \equiv 0 \qquad (\text{mod } p^3). \end{aligned}$$

Finally we consider C such that $f^{p^2}(C) = C$. Reasoning as above one determines that there are $\binom{p^2N}{p^2R}\binom{n_0}{r_0}$ such C. But in this number one has counted all C satisfying $f^p(C) = C$. Subtracting out such elements we have

$$\begin{aligned} |X_2| &= \binom{p^2N}{p^2R}\binom{n_0}{r_0} - \binom{pN}{pR}\binom{n_0}{r_0} \\ &= \binom{n_0}{r_0}\left[\binom{p^2N}{p^2R} - \binom{pN}{pR}\right] \equiv 0 \qquad (\text{mod } p^3). \end{aligned}$$

Thus the proof is complete.

References

1. D. F. Bailey, Some variations of Lucas' theorem, submitted for publication.
2. N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (1947), 589–592.
3. M. Hausner, Applications of a simple counting technique, *Amer. Math. Monthly* **90** (1983), 127–129.
4. Édouard 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.