GENERALIZATION OF A RESULT OF E. LUCAS

by

R.A. MacLeod

DM-344-IR

JANUARY 1985

GENERALIZATION OF A RESULT OF E. LUCAS

1. Introduction. The following theorem has been known at least since the time of E. Lucas, who gives it in [3], pp. 417-420.

Theorem. Let p be prime, and let

$$M = M_0 + M_1p + M_2p^2 + \dots + M_kp^k, \quad 0 \leq M_r < p, \quad 0 \leq r \leq k$$

$$N = N_0 + N_1p + N_2p^2 + \dots + N_kp^k, \quad 0 \leq N_r < p, \quad 0 \leq r \leq k.$$

Then

$$\begin{pmatrix} M \\ N \end{pmatrix} \equiv \begin{pmatrix} M_0 \\ N_0 \end{pmatrix} \begin{pmatrix} M_1 \\ N_1 \end{pmatrix} \begin{pmatrix} M_2 \\ N_2 \end{pmatrix} \dots \begin{pmatrix} M_k \\ N_k \end{pmatrix} \pmod{p} \quad \blacksquare \quad (1)$$

N.J. Fine [1] gives a short and simple proof of this result. It is our object to see what this result looks like if we replace the modulus p by the modulus p^r for arbitrary positive integer r . With the help of a recent result of P.W. Haggard and J.O. Kiltanen, it has been possible to adapt Fine's method to obtain a result corresponding to (1).

2. Main Results

Lemma 1. For q a prime, m and n positive integers with $n \geq m - 1$, and for $0 \leq k \leq q^n$, we have

$$\begin{pmatrix} q^n \\ k \end{pmatrix} \equiv \begin{cases} 0, & \text{if } q^{n-m+1} \nmid k \\ \begin{pmatrix} q^{m-1} \\ i \end{pmatrix}, & \text{if } k = iq^{n-m+1} \end{cases} \pmod{q^m}.$$

Proof. This is the main result in [2]. ■

Lemma 2. Let r and m be positive integers. Then for prime q we have

$$(1+x)^{q^{mr}} \equiv \left(1+x^{q^{mr-m+1}} \right)^{q^{m-1}} \pmod{q^m}.$$

Proof.
$$(1+x)^{q^{mr}} = \sum_{k=0}^{q^{mr}} \begin{pmatrix} q^{mr} \\ k \end{pmatrix} x^k.$$

Now, by Lemma 1,

$$\begin{pmatrix} q^{mr} \\ k \end{pmatrix} \equiv \begin{cases} 0, & \text{if } q^{mr-m+1} \nmid k \\ \begin{pmatrix} q^{m-1} \\ i \end{pmatrix}, & \text{if } k = iq^{mr-m+1} \end{cases}, \pmod{q^m}.$$

Hence we have

$$\begin{aligned} (1+x)^{q^{mr}} &\equiv \sum_{i=0}^{q^{m-1}} \begin{pmatrix} q^{m-1} \\ i \end{pmatrix} x^{q^{mr-m+1}i} \pmod{q^m} \\ &= \left(1+x^{q^{mr-m+1}} \right)^{q^{m-1}} \pmod{q^m}. \quad \blacksquare \end{aligned}$$

Theorem. Let q be prime, and let r be a positive integer, and let

$$M = M_0 + M_1 q^r + M_2 q^{2r} + \dots + M_k q^{kr}, \quad 0 \leq M_s < q^r, \quad 0 \leq s \leq k.$$

Then

$$\begin{pmatrix} M \\ N \end{pmatrix} \equiv \sum \begin{pmatrix} q^{r-1} M_0 \\ N_0 \end{pmatrix} \begin{pmatrix} q^{r-1} M_1 \\ N_1 \end{pmatrix} \dots \begin{pmatrix} q^{r-1} M_k \\ N_k \end{pmatrix} \pmod{q^r}$$

over all $k+1$ -tuples $(N_0, N_1, \dots, N_k)$ such that

$$q^{r-1} N = N_0 + N_1 q^r + \dots + N_k q^{kr}, \quad 0 \leq N_s < q^{r-1} M_s, \quad 0 \leq s \leq k.$$

Proof. From the binomial theorem and Lemma 2, we have

$$\begin{aligned} \sum_{N=0}^M \begin{pmatrix} M \\ N \end{pmatrix} x^N &= (1+x)^M = \prod_{s=0}^k \left\{ (1+x)^{q^{rs}} \right\}^{M_s} \\ &\equiv (1+x)^{M_0} \prod_{s=1}^k \left\{ 1+x^{q^{rs-r+1}} \right\}^{q^{r-1} M_s} \pmod{q^r} \\ &= (1+x)^{M_0} \prod_{s=1}^k q^{r-1} M_s \sum_{m_s=0}^{q^{r-1} M_s} \begin{pmatrix} q^{r-1} M_s \\ m_s \end{pmatrix} x^{m_s q^{rs-r+1}}. \end{aligned} \quad (2)$$

Define M'_s and ℓ_s by

$$M'_s = \begin{cases} M_0, & s = 0 \\ q^{r-1} M_s, & s \geq 1 \end{cases} \quad \ell_s = \begin{cases} 0, & s = 0 \\ rs-r+1, & s \geq 1 \end{cases}.$$

Then line (1) becomes

$$\sum_{N=0}^M \binom{M}{N} x^N = \prod_{s=0}^k \sum_{m_s=0}^{M'_s} \binom{M'_s}{m_s} x^{m_s q^{\ell_s}}$$

$$= \sum_{N=0}^M \left\{ \sum_{s=0}^k \prod \binom{M'_s}{m_s} \right\} x^N,$$

where the inner sum is over all $k+1$ -tuples $(m_0, m_1, \dots, m_k)$ such that

$$\sum_{s=0}^k m_s q^{\ell_s} = N, \quad 0 \leq m_s \leq M'_s,$$

i.e.
$$m_0 + \sum_{s=1}^k m_s q^{rs-r+1} = N, \quad 0 \leq m_0 \leq M_0 < q^r, \quad 0 \leq m_s \leq q^{r-1} M'_s, \quad 1 \leq s \leq k,$$

i.e.
$$m_0 q^{r-1} + \sum_{s=1}^k m_s q^{rs} = q^{r-1} N. \quad (3)$$

Write $m'_0 = q^{r-1} m_0$, $m'_s = m_s$, $s \geq 1$. Then (3) becomes

$$\sum_{s=0}^k m'_s (q^r)^s = q^{r-1} N.$$

But since
$$\begin{pmatrix} M_0 \\ m_0 \end{pmatrix} \equiv \begin{pmatrix} q^{r-1} M_0 \\ q^{r-1} m_0 \end{pmatrix} \pmod{q^r} \quad (\text{by Lemma 1})$$

$$\equiv \begin{pmatrix} M'_0 \\ m'_0 \end{pmatrix} \pmod{q^r},$$

we find on equating coefficients of x^N

$$\binom{M}{N} = \sum_{s=0}^k \prod \left[\begin{matrix} q^{r-1} M_s \\ m'_s \end{matrix} \right] \pmod{q^r}$$

over all $k+1$ -tuples $(m'_0, m'_1, \dots, m'_k)$ such that

$$\sum_{s=0}^k m'_s (q^r)^s = q^{r-1} N, \quad 0 \leq m'_s \leq q^{r-1} M_s, \quad 0 \leq s \leq k \quad \blacksquare$$

We note that, unlike the case $r = 1$, we need not have a unique $k+1$ -tuple. For example, with $q = r = 2$ and $N = 10$, we have the potential 3-tuples $(0,1,1)$, $(4,0,1)$, $(0,5,0)$, and $(4,4,0)$. If we take $M = 14$, we have $2M_0 = 4$, $2M_1 = 6$, $M_2 = 0$, and the result becomes (using only the 3-tuples $(0,5,0)$ and $(4,4,0)$)

$$\binom{14}{10} \equiv \binom{4}{0} \binom{6}{5} + \binom{4}{4} \binom{6}{4} = 6 + 15 = 21 \equiv 1 \pmod{4}.$$

REFERENCES

1. N.J. Fine, Binomial coefficients modulo a prime. Amer. Math. Monthly 54(1947), 589-592.
2. P.W. Haggard and J.O. Kiltenen, Binomial expansions modulo prime powers. Internat. J. Math. and Math. Sc. 3(1980), 397-400.
3. E. Lucas, Théorie des nombres, Tome I, Librairie Scientifique et Technique Albert Blanchard, Paris (1961) (Original 1891).