Canad. Math. Bull. Vol. **31** (1), 1988

GENERALIZATION OF A RESULT OF E. LUCAS

BY

R. A. MACLEOD

ABSTRACT. A well-known result of E. Lucas enables one to obtain the residue modulo p of $\binom{M}{N}$ in terms of the base-p digits of M and N. Using a recent result of P. W. Haggard and J. O. Kiltenen, a proof of N. J. Fine has been adapted to yield the corresponding residue modulo p^r.

The following theorem has been known at least since the time of E. Lucas, who gives it in [4], pp. 417-420.

THEOREM 1. *Let p be prime, and let*

$$M = M_0 + M_1 p + M_2 p^2 + \ldots + M_k p^k, \qquad 0 \leqq M_r < p, 0 \leqq r \leqq k$$

$$N = N_0 + N_1 p + N_2 p^2 + \ldots + N_k p^k, \qquad 0 \leqq N_r < p, 0 \leqq r \leqq k.$$

Then

$$\binom{M}{N} \equiv \binom{M_0}{N_0}\binom{M_1}{N_1}\binom{M_2}{N_2} \cdots \binom{M_k}{N_k} \pmod{p} \tag{1}$$

N. J. Fine [2] 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. Kiltenen, it has been possible to adapt Fine's method to obtain a result corresponding to (1), as follows.

THEOREM 2. *Let p be prime, let r be a positive integer, and let*

$$M = M_0 + M_1 p^r + M_2 p^{2r} + \ldots + M_k p^{kr}, \qquad 0 \leqq M_s < p^r, 0 \leqq s \leqq k.$$

Then

$$\binom{M}{N} \equiv \sum \binom{p^{r-1}M_0}{N_0}\binom{p^{r-1}M_1}{N_1} \cdots \binom{p^{r-1}M_k}{N_k} \pmod{p^r}$$

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

$$p^{r-1}N = N_0 + N_1 p^r + \ldots + N_k p^{kr}, \qquad 0 \leqq N_s < p^{r-1}M_s, 0 \leqq s \leqq k.$$

Received by the editors May 29, 1986, and, in revised form November 25, 1986.
AMS Subject Classification (1980): 11B48, 11B64.

EXAMPLE. We note that, unlike the case $r = 1$, we need not have a unique $k + 1$-tuple. For example, with $p = r = 2$ 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))

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

LEMMA 1. *For p a prime, m and n positive integers with $n \geqq m - 1$, and for $0 \leqq k \leqq p^n$, we have*

$$\binom{p^n}{k} \equiv \begin{cases} 0, \text{ if } p^{n-m+1} \nmid k \\ \binom{p^{m-1}}{i}, \text{ if } k = ip^{n-m+1} \end{cases} \pmod{p^m}.$$

PROOF. This is the main result in [3]. □

LEMMA 2. *Let r and m be positive integers. Then for prime p we have*

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

PROOF.

$$(1 + x)^{p^{mr}} = \sum_{k=0}^{p^{mr}} \binom{p^{mr}}{k} x^k.$$

Now, by Lemma 1,

$$\binom{p^{mr}}{k} \equiv \begin{cases} 0, \text{ if } p^{mr-m+1} \nmid k \\ \binom{p^{m-1}}{i}, \text{ if } k = ip^{mr-m+1} \end{cases}, \pmod{p^m}.$$

Hence we have

$$(1 + x)^{p^{mr}} \equiv \sum_{i=0}^{p^{m-1}} \binom{p^{m-1}}{i} x^{p^{mr-m+1}i} \pmod{p^m}$$

$$= (1 + x^{p^{mr-m+1}})^{p^{m-1}} \pmod{p^m}.$$ □

PROOF OF THEOREM 2. From the binomial theorem and Lemma 2, we have

$$\text{(2)} \qquad \sum_{N=0}^{M} \binom{M}{N} x^N = (1 + x)^M = \prod_{s=0}^{k} \{ (1 + x)^{p^{rs}} \}^{M_s}$$

https://doi.org/10.4153/CMB-1988-014-5 Published online by Cambridge University Press

$$\equiv (1 + x)^{M_0} \prod_{s=1}^{k} (1 + x^{p^{rs-r+1}})^{p^{r-1}M_s} \pmod{p^r}$$

$$= (1 + x)^{M_0} \prod_{s=1}^{k} \sum_{m_s=0}^{p^{r-1}M_r} \binom{p^{r-1}M_s}{m_s} x^{m_s p^{rs-r+1}}.$$

Define M_s' and l_s by

$$M_s' = \begin{cases} M_0, \; s = 0 \\ p^{r-1}M_s, \; s \geqq 1 \end{cases} \qquad l_s = \begin{cases} 0, \; s = 0 \\ rs - r + 1, \; s \geqq 1. \end{cases}$$

Then line (1) becomes

$$\sum_{N=0}^{M} \binom{M}{N} x^N = \prod_{s=0}^{k} \sum_{m_s=0}^{M_s'} \binom{M_s'}{m_s} x^{m_s p^{l_s}} = \sum_{N=0}^{M} \left\{ \Sigma \prod_{s=0}^{k} \binom{M_s'}{m_s} \right\} x^N,$$

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

(3) $$\sum_{s=0}^{k} m_s p^{l_s} = N, \qquad 0 \leqq m_s \leqq M_s',$$

i.e. $$m_0 + \sum_{s=1}^{k} m_s p^{rs-r+1} = N,$$

$$0 \leqq m_0 \leqq M_0 < p^r, \; 0 \leqq m_s \leqq p^{r-1}M_s, \; 1 \leqq s \leqq k,$$

i.e. $$m_0 p^{r-1} + \sum_{s=1}^{k} m_s p^{rs} = p^{r-1}N.$$

Write $m_0' = p^{r-1}m_0$, $m_s' = m_s$, $s \geqq 1$. Then (3) becomes

$$\sum_{s=0}^{k} m_s'(p^r)^s = p^{r-1}N.$$

But since $\binom{M_0}{m_0} \equiv \binom{p^{r-1}M_0}{p^{r-1}m_0} \pmod{p^r}$ (by Lemma 1) $\equiv \binom{M_0'}{m_0'} \pmod{p^r}$,

we find on equating coefficients of x^N

$$\binom{M}{N} = \Sigma \prod_{s=0}^{k} \binom{p^{r-1}M_s}{m_s'} \pmod{p^r}$$

over all $k + 1$-tuples $(m_0', m_1', \ldots, m_k')$ such that

$$\sum_{s=0}^{k} m_s'(p^r)^s = p^{r-1}N, \; 0 \leqq m_s' \leqq p^{r-1}M_s, \; 0 \leqq s \leqq k \qquad \square$$

https://doi.org/10.4153/CMB-1988-014-5 Published online by Cambridge University Press

NOTE. A referee has drawn the author's attention to some related results which appear in a paper of B. Dwork [1], one of which is as follows.

Let p be a fixed prime number; let θ be a p-adic integer which is neither zero nor a negative rational integer; let θ' be that unique rational number, integral at p, such that $p\theta' - \theta$ is an ordinary integer; let $C_\theta(n)$ denote 1 if $n = 0$ and $\prod_{\nu=0}^{n-1}(\theta + \nu)$ if $n > 0$; let $A_\theta(n)$ be $C_\theta(n)/n!$; and if $\theta_1, \ldots, \theta_r$ are rational p-adic integers, none of which are zero or ordinary negative integers, then for $n > 0$ write

$$A(n) = \prod_{t=1}^{r} A_{\theta_t}(n), \qquad B(n) = \prod_{t=1}^{r} A_{\theta'_t}(n).$$

Then

(i) $A(n)/B\left(\left[\frac{n}{p}\right]\right)$ is a p-adic integer

(ii) $A(n + mp^{s+1})/B\left(\left[\frac{n}{p}\right] + mp^s\right) \equiv A(n)/B\left(\left[\frac{n}{p}\right]\right) \bmod p^{s+1}$.

REFERENCES

1. B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math. No. 37 (1969), pp. 27-115.

2. N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), pp. 589-592.

3. P. W. Haggard and J. O. Kiltenen, *Binomial expansions modulo prime powers*, Internat. J. Math. and Math. Sc. **3** (1980), pp. 397-400.

4. E. Lucas, *Théorie des nombres, Tome I*, Librairie Scientifique et Technique Albert Blanchard, Paris (1961) (Original 1891).

UNIVERSITY OF VICTORIA
VICTORIA, BRITISH COLUMBIA V8W 2Y2