Europ. J. Combinatorics (1990) **11**, 229–233

Lucas' Theorem for Prime Powers

KENNETH S. DAVIS AND WILLIAM A. WEBB

Lucas' theorem on binomial coefficients states that $\binom{A}{B} \equiv \binom{a_r}{b_r} \cdots \binom{a_1}{b_1}\binom{a_0}{b_0} \pmod p$ where p is a prime and $A = a_r p^r + \cdots + a_1 p + a_0$, $B = b_r p^r + \cdots + b_1 p + b_0$ are the p-adic expansions of A and B. If $s \geqslant 2$, it is shown that a similar formula holds modulo p^s where the product involves a slightly modified binomial coefficient evaluated on blocks of s digits.

INTRODUCTION

One of the most beautiful results concerning binomial coefficients is Lucas' Theorem [1, 2]. If $0 \leqslant B \leqslant A$ are integers and p is a prime, write A and B in p-adic notation $A = a_r p^r + \cdots + a_1 p + a_0$, $B = b_r p^r + \cdots + b_1 p + b_0$, where $0 \leqslant a_i$, $b_i < p$ and $a_r \neq 0$. Then

$$\binom{A}{B} \equiv \binom{a_r}{b_r}\binom{a_{r-1}}{b_{r-1}} \cdots \binom{a_1}{b_1}\binom{a_0}{b_0} \pmod p. \tag{1}$$

If $A - B = c_r p^r + \cdots + c_1 p + c_0$ and $p^t \mid \binom{A}{B}$ then Kazandzidis [3] proved that

$$\binom{A}{B} \equiv (-p^t) \prod_{i=0}^{r} \frac{a_i!}{b_i!\, c_i!} \pmod{p^{t+1}}.$$

This result is applicable for only one power of p for each $\binom{A}{B}$, and in particular does not apply for $t \geqslant 1$ if $(\binom{A}{B}, p) = 1$. Singmaster [5] also obtained similar results.

For integers A and B as above, define the string $A_{ij} = a_i a_{i-1} \cdots a_j$ for $0 \leqslant j \leqslant i \leqslant r$, with B_{ij} defined similarly. Corresponding to a string A_{ij} is the integer $\mathscr{A}_{ij} = a_i p^{i-j} + \cdots + a_{j+1} p + a_j$. Let $\leqslant$ be the lexical order on strings, so that $A_{ij} \leqslant B_{ij}$ iff $\mathscr{A}_{ij} \leqslant \mathscr{B}_{ij}$, with O_i denoting the string of $i + 1$ zeros.

We also define a modified binomial coefficient on such strings as follows. In the following assume j is fixed and write $A_i = A_{ij}$, etc. Also p^s is a fixed power of p.

If $B_i \leqslant A_i$ then $\left\langle {A_i \atop B_i} \right\rangle = \binom{\mathscr{A}_i}{\mathscr{B}_i}$.

If $A_0 < B_0$ then $\left\langle {A_0 \atop B_0} \right\rangle = p$, and recursively if $A_i < B_i$, $i \geqslant 1$, then $\left\langle {A_i \atop B_i} \right\rangle = p \left\langle {A_{i-1} \atop B_{i-1}} \right\rangle$.

In general $\left\langle {A_i \atop B_i} \right\rangle = p^t \alpha$, where $t \geqslant 0$ and $p \nmid \alpha$.

Formally, $\left\langle {A_i \atop B_i} \right\rangle^{-1} = p^{-t} \alpha^{-1}$, where α^{-1} is such that $\alpha\alpha^{-1} \equiv 1 \pmod{p^s}$ and $0 < \alpha^{-1} < p^s$. The following properties are clear:

(1) $\left\langle {A_i \atop B_i} \right\rangle \left\langle {A_i \atop B_i} \right\rangle^{-1} \equiv 1 \pmod{p^s}$.

(2) If $A_k \geqslant B_k$ and $A_{k+l} < B_{k+l}$ for $1 \leqslant l \leqslant i - k$ then $\left\langle {A_i \atop B_i} \right\rangle = p^{i-k} \left\langle {A_k \atop B_k} \right\rangle$.

(3) Suppose $p^t \parallel \left\langle {A_i \atop B_i} \right\rangle$. If $A_i \geqslant B_i$ then it is well known that t is the number of borrows necessary in the subtraction $\mathscr{A}_i - \mathscr{B}_i$. [4] If $A_i < B_i$ then t is the number of borrows in the subtraction $(p^{i+1} + \mathscr{A}_i) - \mathscr{B}_i$. Thus if $\left\langle {A_{i+1} \atop B_{i+1}} \right\rangle \left\langle {A_i \atop B_i} \right\rangle^{-1} = p^t \alpha$, where $p \nmid \alpha$, then $t \geqslant 0$.

Our goal is to prove the following generalization of Lucas' Theorem which completely determines the value of any binomial coefficient modulo any prime power.

THEOREM 1. *For any integers $0 \leqslant B \leqslant A$ and any prime power p^s, $2 \leqslant s \leqslant r + 1$,*

$$\begin{aligned}\binom{A}{B} &\equiv \left\langle {a_{s-1} \cdots a_0 \atop b_{s-1} \cdots b_0} \right\rangle \prod_{j=1}^{r-s+1} \left\langle {a_{j+s-1} \cdots a_j \atop b_{j+s-1} \cdots b_j} \right\rangle \left\langle {a_{j+s-2} \cdots a_j \atop b_{j+s-2} \cdots b_j} \right\rangle^{-1} \\ &\equiv \left\langle {A_{s-1} \atop B_{s-1}} \right\rangle \prod_{j=1}^{r-s+1} \left\langle {A_{j+s-1,j} \atop B_{j+s-1,j}} \right\rangle \left\langle {A_{j+s-2,j} \atop B_{j+s-2}} \right\rangle^{-1} \pmod{p^s}.\end{aligned} \tag{2}$$

0195-6698/90/030229 + 05 $02.00/0

The modified binomial coefficients are needed only in evaluating $\binom{A_j}{B_j}$, where $B_j > A_j$, so we have as an immediate corollary.

COROLLARY. *If $b_i \leq a_i$ for $0 \leq i \leq r$ then*

$$\binom{A}{B} \equiv \binom{\mathscr{A}_{s-1}}{\mathscr{B}_{s-1}} \prod_{j=1}^{r-s+1} \binom{\mathscr{A}_{j+s-1,j}}{\mathscr{B}_{j+s-1,j}} \binom{\mathscr{A}_{j+s-2,j}}{\mathscr{B}_{j+s-2,j}}^{-1} \pmod{p^s}.$$

The following example illustrates how this theorem can be used in a specific case. Note that we can always reduce the calculation to ordinary binomial coefficients.

Let $p = 7$ and $s = 3$, and suppose that the base 7 representations of A and B are $A = 2413605$ and $B = 1261632$.

$$\begin{aligned}\binom{2413605}{1201632} &\equiv \left\langle {241 \atop 120} \right\rangle \left\langle {41 \atop 20} \right\rangle^{-1} \left\langle {413 \atop 201} \right\rangle \left\langle {13 \atop 01} \right\rangle^{-1} \left\langle {136 \atop 016} \right\rangle \left\langle {36 \atop 16} \right\rangle^{-1} \left\langle {360 \atop 163} \right\rangle \left\langle {60 \atop 63} \right\rangle^{-1} \left\langle {605 \atop 632} \right\rangle \\ &\equiv \binom{241}{120}\binom{41}{20}^{-1}\binom{413}{201}\binom{13}{1}^{-1}\binom{136}{16}\binom{36}{16}^{-1}\binom{360}{163}7^{-2}7^{2}\binom{5}{2} \\ &\equiv (33)(286)^{-1}(116)(10)^{-1}(10)(3)^{-1}(98)(10) \\ &\equiv (33)(6)(116)(229)(98)(10) \equiv 98 \pmod{343}.\end{aligned}$$

PROOF OF THEOREM 1

The following lemma will be useful.

LEMMA:

$$\binom{pA}{pB} = \binom{A}{B} \prod_{j=1}^{p-1} \prod_{k=1}^{B} \frac{p(k+A-B)-j}{pk-j}$$

for integer $0 \leq B \leq A$.

PROOF:

$$\begin{aligned}\binom{pA}{pB} &\equiv \frac{(pA)(pA-1)\cdots(p(A-B)+1)}{(pB)(pB-1)\cdots 1} \\ &\equiv \frac{(pA)(p(A-1))\cdots p(A-B)}{(pB)(p(B-1))\cdots p} \times \prod_{j=1}^{p-1} \prod_{k=1}^{B} \frac{p(k+A-B)-j}{pk-j}\end{aligned}$$

and the result follows by cancelling p^B in the first factor. □

Our proof of Theorem 1 uses induction on A. It is trivial for $A < p$. From now on let $A_i = A_{io}$ etc. Let $\prod \langle A_r, B_r \rangle = \prod \langle A, B \rangle$ denote a product of the type on the right side of (2), and

$$\prod{}^{*} \langle A, B \rangle = \prod \langle A, B \rangle \left\langle {A_{s-1} \atop B_{s-1}} \right\rangle^{-1}.$$

The result is also clear for $r = s-1$ since $\binom{A}{B} = \left\langle {A_r \atop B_r} \right\rangle$, so we may assume $r \geq s$.

Assume that (2) holds for all integers A' less than A and all $B \leq A'$ and suppose that $A = a_r p^r + \cdots + a_0$, $a_r \neq 0$.

We consider several cases, depending on the values of a_0 and b_0.

Case 1: $a_0=0$ and $b_0=0$. Let $\alpha_k = a_k p^{k-1} + \cdots + a_1$ and $\beta_k = b_k p^{k-1} + \cdots + b_1$, so $A = \mathscr{A}_{r,0} = p\alpha_r$ and $B = \mathscr{B}_{r,0} = p\beta_r$. Hence,

$$\binom{A}{B} = \binom{p\alpha_r}{p\beta_r} = \binom{\alpha_r}{\beta_r} \prod_{j=1}^{p-1} \prod_{k=1}^{\beta_r} \frac{p(k+\alpha_r-\beta_r)-j}{pk-j} \tag{3}$$

by the lemma.

Since $0 \leqslant \beta_r \leqslant \alpha_r < A$, we may apply the induction hypothesis to $\binom{\alpha_r}{\beta_r}$. We also note that formally, the expressions for $\prod \langle A, B\rangle$ and $\prod \langle \alpha_r, \beta_r\rangle$ are identical except for two factors. Hence,

$$\begin{aligned} \prod \langle A_r, B_r\rangle &= \prod \langle \alpha_r, \beta_r\rangle \left\langle {a_{s-1} \cdots a_1 0 \atop b_{s-1} \cdots b_1 0} \right\rangle \left\langle {a_{s-1} \cdots a_1 \atop b_{s-1} \cdots b_1} \right\rangle^{-1} \\ &= \binom{\alpha_r}{\beta_r} \left\langle {A_{s-1} \atop B_{s-1}} \right\rangle \left\langle {A_{s-1,1} \atop B_{s-1,1}} \right\rangle^{-1}. \end{aligned} \tag{4}$$

If $p^s \mid \binom{\alpha_r}{\beta_r}$ then both sides of (2) are zero and case 1 is settled. Otherwise, let $p^\lambda \,\|\, \binom{\alpha_r}{\beta_r}$ where $\lambda < s$. Then comparing (3) and (4), equation (2) holds iff

$$\prod_{j=1}^{p-1} \prod_{k=1}^{\beta_r} \frac{p(k+\alpha_r-\beta_r)-j}{pk-j} \equiv \left\langle {A_{s-1} \atop B_{s-1}} \right\rangle \left\langle {A_{s-1,1} \atop B_{s-1,1}} \right\rangle^{-1} \pmod{p^{s-\lambda}}. \tag{5}$$

By earlier remarks,

$$\left\langle {A_{s-1} \atop B_{s-1}} \right\rangle = p^t \left\langle {A_u \atop B_u} \right\rangle,$$

where $A_u \geqslant B_u$ for some $u \geqslant 0$, $0 \leqslant t < s$. If $u=0$,

$$\left\langle {A_{s-1} \atop B_{s-1}} \right\rangle = p^{s-1} = \left\langle {A_{s-1,1} \atop B_{s-1,1}} \right\rangle$$

and the right hand side of (5) is 1. For $u > 0$, we also have

$$\left\langle {A_{s-1,1} \atop B_{s-1,1}} \right\rangle = p^t \left\langle {A_{u,1} \atop B_{u,1}} \right\rangle$$

and so the right side of (5) becomes

$$\begin{aligned} p^t \left\langle {A_t \atop B_u} \right\rangle p^{-t} \left\langle {A_{u,1} \atop B_{u,1}} \right\rangle^{-1} &\equiv \binom{\mathscr{A}_u}{\mathscr{B}_u} \binom{\alpha_u}{\beta_u}^{-1} \\ &\equiv \binom{p\alpha_u}{p\beta_u} \binom{\alpha_u}{\beta_u}^{-1} \equiv \binom{\alpha_u}{\beta_u} \prod_{j=1}^{p-1} \prod_{k=1}^{\beta_u} \frac{p(k+\alpha_u-\beta_u)-j}{pk-j} \binom{\alpha_u}{\beta_u}^{-1} \\ &\equiv \prod_{j=1}^{p-1} \prod_{k=1}^{\beta_u} \frac{p(k+\alpha_u-\beta_u)-j}{pk-j} \pmod{p^s}. \end{aligned}$$

Thus it now suffices to show

$$\prod_{j=1}^{p-1} \prod_{k=1}^{\beta_r} \frac{p(k+\alpha_r-\beta_r)-j}{pk-j} \equiv \prod_{j=1}^{p-1} \prod_{k=1}^{\beta_u} \frac{p(k+\alpha_r-\beta_r)-j}{pk-j} \pmod{p^{s-\lambda}}. \tag{6}$$

Also, since $t \leqslant \lambda$ it suffices to prove (6) modulo $p^{s-t} = p^{u+1}$. Finally, since $p(\alpha_r - \beta_r) \equiv p(\alpha_u - \beta_u) \pmod{p^{u+1}}$, it suffices to show

$$\prod_{j=1}^{p-1} \prod_{k=\beta_u+1}^{\beta_r} \frac{p(k+\alpha_r-\beta_r)-j}{pk-j} \equiv 1 \pmod{p^{s-\lambda}}. \tag{7}$$

We observe that $px-j$ runs over a reduced residue system modulo p^{u+1} as $1\leqslant j\leqslant p-1$ and x runs over any p^u consecutive integers. In (7), k runs over $\beta_r-\beta_u=b_rp^r+\cdots+b_{u+1}p^u$ consecutive integers. This in (7), both $p(k+\alpha_r-\beta_r)-j$ and $pk-j$ runs over a reduced residue system modulo p^{u+1}, exactly $b_rp^{r-u}+\cdots+b_{u+1}$ times, which proves (7).

Case 2: $a_0\neq 0$ and $b_0\neq 0$. The result is trivial if $A=B$. If $A\geqslant B+1$ then (3) follows immediately from applying the induction hypothesis to $\binom{A-1}{B}$ and $\binom{A-1}{B-1}$ and noting that

$$\left\langle\begin{matrix}a_{s-1}\cdots a_1a_0-1\\ b_{s-1}\cdots b_1b_0\end{matrix}\right\rangle+\left\langle\begin{matrix}a_{s-1}\cdots a_1a_0-1\\ b_{s-1}\cdots b_1b_0-1\end{matrix}\right\rangle=\left\langle\begin{matrix}a_{s-1}\cdots a_1a_0\\ b_{s-1}\cdots b_1b_0\end{matrix}\right\rangle.$$

Case 3: $a_0\neq 0$ and $b_0=0$. We note that $p\nmid B+1$ and $p\mid A-B$ and, furthermore,

$$\binom{A}{B}=\binom{A}{B+1}\frac{B+1}{A-B}.$$

By Case 2, equation (3) holds for $\binom{A}{B+1}$ and so it suffices to show that

$$p^s\left|\prod{}^*\left\langle\begin{matrix}A_{s-1}\\ B_{s-1}\end{matrix}\right\rangle-\prod{}^*\left\langle\begin{matrix}A_{s-1}\\ B_{s-1}+1\end{matrix}\right\rangle\frac{B+1}{A-B},\right.$$

where $\prod^*=\prod^*\langle A,B\rangle=\prod^*\langle A,B+1\rangle$. Since $A\equiv\mathscr{A}_{s-1}$ and $B\equiv\mathscr{B}_{s-1}(\bmod p^s)$ we must show that

$$p^s\left|\prod{}^*\left(\left\langle\begin{matrix}A_{s-1}\\ B_{s-1}\end{matrix}\right\rangle(\mathscr{A}_{s-1}-\mathscr{B}_{s-1})-\left\langle\begin{matrix}A_{s-1}\\ B_{s-1}+1\end{matrix}\right\rangle(\mathscr{B}_{s-1}+1)\right).\right.$$

Now,

$$\left\langle\begin{matrix}A_{s-1}\\ B_{s-1}\end{matrix}\right\rangle=p^t\left\langle\begin{matrix}A_u\\ B_u\end{matrix}\right\rangle,$$

where $A_u>B_u$ for some $u=s-t-1>0$, and also

$$\left\langle\begin{matrix}A_{s-1}\\ B_{s-1}+1\end{matrix}\right\rangle=p^t\left\langle\begin{matrix}A_u\\ B_u+1\end{matrix}\right\rangle,$$

where $A_u\geqslant B_u+1$. By earlier remarks $\prod^*$ is divisible by a non-negative power of p and so it suffices to show that

$$p^{s-t}\left|\left(\left\langle\begin{matrix}A_u\\ B_u\end{matrix}\right\rangle(\mathscr{A}_{s-1}-\mathscr{B}_{s-1})-\left\langle\begin{matrix}A_u\\ B_u+1\end{matrix}\right\rangle(\mathscr{B}_{s-1}+1)\right).\right. \tag{8}$$

But $p^{s-t}=p^{u+1}$ and $\mathscr{A}_{s-1}\equiv\mathscr{A}_u$, $\mathscr{B}_{s-1}\equiv\mathscr{B}_u$ modulo p^{u+1}, and

$$\left\langle\begin{matrix}A_u\\ B_u\end{matrix}\right\rangle(\mathscr{A}_u-\mathscr{B}_u)-\left\langle\begin{matrix}A_u\\ B_u+1\end{matrix}\right\rangle(\mathscr{B}_{s-1}+1)=\binom{\mathscr{A}_u}{\mathscr{B}_u}(\mathscr{A}_u-\mathscr{B}_u)-\binom{\mathscr{A}_u}{\mathscr{B}_u+1}(\mathscr{B}_u+1)=0,$$

so equation (8) holds.

Case 4: $a_0=0$ and $b_0\neq 0$. This is similar to Case 3. By Case 1, the theorem holds for $\binom{A}{B}$, where $b_0=0$ and $a_0=0$. For A fixed, $a_0=0$, assume true for $\binom{A}{B}$, where $0\leqslant b_0\leqslant p-2$, and note that

$$\binom{A}{B+1}=\binom{A}{B}\frac{A-B}{B+1}$$

where $p \nmid A - B$ and $p \nmid B + 1$. As before, it suffices to show that

$$p^s \,\Big|\, \prod{}^* \left(\left\langle {A_{s-1} \atop B_{s-1}+1} \right\rangle (\mathscr{B}_{s-1}+1) - \left\langle {A_{s-1} \atop B_{s-1}} \right\rangle (\mathscr{A}_{s-1} - \mathscr{B}_{s-1}) \right). \tag{9}$$

It may happen that

$$\left\langle {A_{s-1} \atop B_{s-1}+1} \right\rangle = p^s = \left\langle {A_{s-1} \atop B_{s-1}} \right\rangle,$$

in which case (9) is immediate. Otherwise,

$$\binom{A_{s-1}}{B_{s-1}+1} = p^t \binom{A_u}{B_u+1},$$

where $A_u \geqslant B_u + 1$ and the rest is the same as Case 3.

REFERENCES

1. L. E. Dickson, *History of the theory of numbers, Vol. 1,* Chelsea, New York, 1952.
2. N. J. Fine, Binomial coefficients modulo a prime, *Am. Math. Monthly,* **54** (1947), 589–592.
3. G. S. Kazandzidis, Congruences on binomial coefficients, *Bull. Soc. Math. Grèce* (*NS*), **9** (1968), 1–12.
4. D. Singmaster, Divisibility of binomial and multinomial coefficients by primes and prime powers, From a collection of manuscripts related to the Fibonacci Sequence.
5. D. Singmaster, Notes on binomial coefficients I—a generalization of Lucas' congruence, *J. Lond. Math. Soc.* (2), **8** (1974), 545–548.

Received 16 May 1989 and accepted 15 January 1990

KENNETH S. DAVIS
Albion College,
Department of Mathematics,
Albion, Michigan 49224, U.S.A.

WILLIAM A. WEBB
Washington State University,
Department of Pure and Applied Mathematics,
Pullman, Washington 99164-2930, U.S.A.