CONGRUENCE PROPERTIES OF ORDINARY AND q-BINOMIAL COEFFICIENTS

By Robert D. Fray

1. Introduction. The arithmetic properties of the binomial coefficients have been studied extensively; for references see Dickson [3, vol. 1]. Some of these properties, as well as those of other coefficients involving factorials, are easily proved from the following theorem of Legendre [7; 10, vol. 1].

Theorem 1.1. *If p is a prime and μ is the highest power of p dividing $n!$ then*

$$\mu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \frac{n-\alpha}{p-1},$$

where

$$n = a_0 + a_1 p + \cdots + a_m p^m \qquad (0 \le a_i < p)$$

and

$$\alpha = a_0 + a_1 + \cdots + a_m .$$

Here, as usual, $[a/b]$ denotes the greatest integer in a/b.

Using this theorem Kummer [6; 115-6] obtained a formula determining the highest power of a prime p dividing a binomial coefficient. The residue of a binomial coefficient to a prime modulus can readily be obtained by the following theorem, proved by Lucas [8; 52].

Theorem 1.2. *If p is a prime and*

$$n = a_0 + a_1 p + a_2 p^2 + \cdots \qquad (0 \le a_i < p),$$

$$r = b_0 + b_1 p + b_2 p^2 + \cdots \qquad (0 \le b_i < p),$$

then

$$\binom{n}{r} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2} \cdots \pmod{p}.$$

In §3 of this paper these results have been extended to the q-binomial coefficients. In addition, Kummer's result has been extended to the multinomial and q-multinomial coefficients.

For a positive integer n it is of interest to determine the smallest positive integer A such that

$$\binom{n+A}{k} \equiv \binom{n}{k} \qquad (\mathrm{mod}\ p^r)$$

Received July 22, 1966. Supported in part by NSF grant GP-1593.

for all integers r and k, where

$$0 \leq k \leq n, \qquad r = 1, 2, 3, \cdots .$$

Although this result and the corresponding one for fixed k are known, references on them are not readily available. Therefore they are stated in §4 and generalized for the q-binomial coefficient.

2. Preliminaries. The idea of q-numbers originated with F. H. Jackson [5] who published many papers on the subject. Morgan Ward [10] has considered more general binomial and multinomial coefficients.

For a non-negative integer n the q-number $[n]$ is defined by

$$[n] = \frac{q^n - 1}{q - 1},$$

for q an indeterminate. By a q-binomial coefficient we mean

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]_k}{[k]!} = \prod_{j=1}^{k} \frac{q^{n-j+1} - 1}{q^j - 1}, \tag{2.1}$$

where

$$[n]_k = [n][n-1] \cdots [n-k+1], \qquad [k]! = [k]_k, \qquad [0]! = [n]_0 = 1.$$

It is well known that [4; 280]

$$\prod_{k=0}^{n-1} (1 + q^k x) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^{\frac{1}{2}k(k-1)} x^k. \tag{2.2}$$

From this we see that the q-binomial coefficient is a polynomial in q and that for $q = 1$ it reduces to the ordinary binomial coefficient.

The q-binomial coefficient has many properties similar to those of the ordinary binomial coefficient. We shall need the following result which is easily obtained from (2.1):

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]}{[k]} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}. \tag{2.3}$$

A generalization of Vandermonde's theorem for binomial coefficients (see [9; 9]) which we can obtain from (2.2) is the following relation for q-binomial coefficients:

$$\begin{bmatrix} n+m \\ r \end{bmatrix} = \sum_{k=0}^{r} q^{k(n-r+k)} \begin{bmatrix} n \\ r-k \end{bmatrix} \begin{bmatrix} m \\ k \end{bmatrix}. \tag{2.4}$$

See Carlitz [1] for additional arithmetic properties of the q-binomial coefficient.

Throughout this paper the letter p will as usual designate a prime. In the following sections we shall assume that q is a rational number which is p-integral (that is, p does not divide the denominator of q) and is not congruent to zero (mod p). (Two rational numbers a/b and c/d which are p-integral are said to be congruent (mod p^k) if $ad - bc$ is divisible by p^k.) The letter e will designate the exponent to which q belongs (mod p), and the letter h will designate the largest exponent of p such that q^e is congruent to one (mod p^h). Clearly e and h are positive integers.

3. Analogues of the theorems of Legendre, Kummer and Lucas. The analogues of the theorems of Legendre and Kummer will be different for the cases $p^h > 2$ and $p^h = 2$, which is not surprising due to the close connection with primitive roots. We shall first develop the theorems for $p^h > 2$. The development of the results for the case $p^h = 2$ will be similar.

For our discussion we shall need the following preliminary result which is easily proved.

THEOREM 3.1. *Let q belong to the exponent e(mod p), and let h be the highest power of p dividing $q^e - 1$. If $p^h > 2$ and j is a non-negative integer, then q belongs to the exponent ep^j(mod p^{h+j}).*

If $q \equiv 1$ (mod p), we have by Theorem 3.1 that

$$q^s \equiv 1 \qquad (\text{mod } p^{h+j})$$

if and only if p^j divides s. Applying Theorem 1.1 we obtain the following theorem, which is our desired analogue of Legendre's Theorem.

THEOREM 3.2. *Let $q \equiv 1$ (mod p) and h be the highest power of p dividing $q - 1$. If $p^h > 2$, the highest power μ of the prime p dividing $(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$ is determined by*

$$\mu = nh + \frac{n - \alpha}{p - 1},$$

where

$$n = a_0 + a_1 p + \cdots + a_k p^k \qquad (0 \leq a_i < p)$$

and

$$\alpha = a_0 + a_1 + \cdots + a_k .$$

For p a prime and e a positive integer we can write any non-negative integer n in one and only one way in the form

$$n = a_0 + e(a_1 + a_2 p + \cdots + a_k p^{k-1}), \tag{3.1}$$

where

$$0 \leq a_0 < e, \qquad 0 \leq a_j < p \qquad (j = 1, 2, \cdots, k).$$

The integers a_j for $j = 0, 1, \cdots, k$ will be called the digits of n. The non-negative integers r and $n + r$ may be expanded similarly, so let

$$\begin{cases} r = b_0 + e(b_1 + b_2 p + \cdots + b_k p^{k-1}), \\ n + r = c_0 + e(c_1 + c_2 p + \cdots + c_k p^{k-1}), \end{cases} \tag{3.2}$$

where

$$0 \leq b_0 < e, \qquad 0 \leq c_0 < e,$$

and

$$0 \leq b_j < p, \qquad 0 \leq c_j < p \qquad (j = 1, 2, \cdots, k).$$

Now choose ϵ_0 equal to zero or one so that

$$a_0 + b_0 = \epsilon_0 e + c_0 .$$

Also choose ϵ_j equal to zero or one for $j = 1, 2, \cdots, k$ so that

$$(3.3) \qquad \begin{cases} \epsilon_0 + a_1 + b_1 = \epsilon_1 p + c_1 \\ \epsilon_1 + a_2 + b_2 = \epsilon_2 p + c_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \epsilon_{k-2} + a_{k-1} + b_{k-1} = \epsilon_{k-1} p + c_{k-1} \\ \epsilon_{k-1} + a_k + b_k = c_k . \end{cases}$$

Using this notation we state the following theorem, which is an analogue for q-binomial coefficients of Kummer's theorem.

THEOREM 3.3. *Let q belong to the exponent e* (mod p), *and let h be the highest power of p dividing $q^e - 1$. If $p^h > 2$, the highest power N of the prime p dividing the q-binomial coefficient $\begin{bmatrix} n + r \\ r \end{bmatrix}$ is given by*

$$N = \epsilon_0 h + \epsilon_1 + \cdots + \epsilon_{k-1} ,$$

where the ϵ's *are defined by* (3.3).

Proof. Let

$$a = \left[\frac{n}{e}\right], \qquad b = \left[\frac{r}{e}\right], \qquad c = \left[\frac{n + r}{e}\right].$$

If we let $t = q^e$, we then have that N is the highest power of p dividing

$$(3.4) \qquad \frac{(t^c - 1)(t^{c-1} - 1) \cdots (t - 1)}{(t^a - 1)(t^{a-1} - 1) \cdots (t - 1)(t^b - 1)(t^{b-1} - 1) \cdots (t - 1)} .$$

Therefore, applying Theorem 3.2 to (3.4) we have

$$(3.5) \qquad N = \left(ch + \frac{c - \gamma}{p - 1}\right) - \left(ah + \frac{a - \alpha}{p - 1}\right) - \left(bh + \frac{b - \beta}{p - 1}\right) ,$$

where α, β and γ are the sums of the digits of a, b and c respectively.

If in the system of equations (3.3) we multiply the first equation by 1, the second by p, the third by p^2, etc. and add the resulting equations, we have

$$(3.6) \qquad c - a - b = \epsilon_0 .$$

By just adding the equations (3.3) we see that

$$\alpha + \beta - \gamma = (p - 1)(\epsilon_1 + \epsilon_2 + \cdots + \epsilon_{k-1}) - \epsilon_0 \,. \tag{3.7}$$

Substituting (3.6) and (3.7) into (3.5) we see that the theorem is proved.

Before proceeding further let us return to the exceptional case $p^h = 2$, for which the development will be similar to that of the case $p^h > 2$. Note that the condition $p^h = 2$ implies $q \equiv 3 \pmod 4$.

THEOREM 3.4. *Let $q \equiv 3 \pmod 4$ and s be the highest power of 2 dividing $q + 1$. Then the highest power λ of 2 dividing $q^n - 1$ is*

$$\lambda = \begin{cases} 1 & (n \text{ odd}) \\ s + r & (n = 2^r m,\ 2 \nmid m,\ r > 0). \end{cases}$$

The proof is straightforward and is therefore omitted.

THEOREM 3.5. *Let $q \equiv 3 \pmod 4$ and s be the highest power of 2 dividing $q + 1$. Then the highest power λ of 2 dividing $(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$ is*

$$\lambda = \frac{n - a_0}{2}(s + 1) + n + a_0 - \alpha, \tag{3.8}$$

where

$$n = a_0 + a_1 2 + \cdots + a_k 2^k \qquad (0 \le a_i < 2)$$

and

$$\alpha = a_0 + a_1 + \cdots + a_k \,.$$

Proof. Suppose n is even, then $a_0 = 0$. By Theorem 3.4 the highest power of 2 dividing $q^{n-2i} - 1$ is $r_i + s$, where r_i is the highest power of 2 dividing $n - 2i$. By the same theorem the highest power of 2 dividing $q^{n-2i-1} - 1$ is 1. Therefore

$$\lambda = \frac{n}{2} + \frac{n}{2}s + \sum_{i=0}^{n/2-1} r_i = \frac{n - a_0}{2}(s + 1) + \sum_{i=0}^{n/2-1} r_i \,.$$

Moreover, it is clear that $\sum_{i=0}^{n/2-1} r_i$ is the highest power of 2 dividing $n!$ Hence from Theorem 1.1 we obtain (3.8).

The proof for the case n odd is similar.

Using Theorem 3.5 we are able to prove the analogue of Kummer's Theorem for the case $p^h = 2$.

THEOREM 3.6. *Let $q \equiv 3 \pmod 4$ and s be the highest power of 2 dividing $q + 1$. Then the highest power N of 2 dividing $\begin{bmatrix} n + r \\ r \end{bmatrix}$ is*

$$N = \epsilon_0 s + \epsilon_1 + \cdots + \epsilon_{k-1} \,, \tag{3.9}$$

where the ϵ's are defined by (3.11).

Proof. Let

$$n = a_0 + a_1 2 + \cdots + a_k 2^k,$$
$$r = b_0 + b_1 2 + \cdots + b_k 2^k,$$
$$n + r = c_0 + c_1 2 + \cdots + c_k 2^k,$$

where a_i , b_i and c_i are equal to zero or one, and let α, β and γ be the sums of the digits of n, r and $n + r$ respectively. Then by Theorem 3.5

$$(3.10) \qquad N = \frac{a_0 + b_0 - c_0}{2}(s + 1) + c_0 - a_0 - b_0 + \alpha + \beta - \gamma.$$

Now choose ϵ_i equal to zero or one so that

$$(3.11) \qquad \begin{cases} a_0 + b_0 = \epsilon_0 2 + c_0 \\ \epsilon_0 + a_1 + b_1 = \epsilon_1 2 + c_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \epsilon_{k-1} + a_k + b_k = c_k \ . \end{cases}$$

Adding these equations we have

$$\alpha + \beta - \gamma = \epsilon_0 + \epsilon_1 + \cdots + \epsilon_{k-1} \ .$$

Also note that $a_0 + b_0 - c_0 = 2\epsilon_0$. Substituting these values into (3.10) we obtain (3.9).

As a natural extension of the q-binomial coefficient we shall now consider the q-multinomial coefficient

$$(3.12) \qquad \frac{[m]!}{[m_1]!\,[m_2]! \cdots [m_n]!} \qquad (m = m_1 + m_2 + \cdots + m_n);$$

a generalization of this coefficient has been considered by Ward [10; 255]. We shall now determine the highest power of a prime p dividing (3.12); as before we shall state separate theorems for the cases $p^h > 2$ and $p^h = 2$. The ϵ's are chosen as in Theorems 3.3 and 3.6 except that now we choose $\epsilon_i = 0, 1, \cdots$, or $n - 1$.

THEOREM 3.7. *Let q belong to the exponent e* (mod p), *and let h be the highest power of p dividing $q^e - 1$. If $p^h > 2$, the highest power N of the prime p dividing the q-multinomial coefficient* (3.12) *is given by*

$$N = \epsilon_0 h + \epsilon_1 + \cdots + \epsilon_{k-1} \ .$$

THEOREM 3.8. *Let $q \equiv 3$* (mod 4) *and let s be the highest power of 2 dividing $q + 1$. Then the highest power N of 2 dividing the q-multinomial coefficient* (3.12) *is*

$$N = \epsilon_0 s + \epsilon_1 + \cdots + \epsilon_{k-1} \ .$$

The proofs of Theorems 3.7 and 3.8 have been omitted since they are essentially the same as the proofs of Theorems 3.3 and 3.6, respectively.

A direct consequence of Theorems 3.7 and 3.8 is the following theorem which gives necessary and sufficient conditions for the divisibility of the q-multinomial coefficient by a prime p. The proof of the theorem is obvious since h and s are positive.

THEOREM 3.9. *The q-multinomial coefficient* (3.12) *is relatively prime to the prime p if and only if the partition of m into m_1, m_2, $\cdots$, m_n arises by the independent partitions of each digit of m into the corresponding digits of m_1, m_2, $\cdots$, m_n.*

The corresponding theorem for the ordinary multinomial coefficient was proved by Dickson [2; 378-9]. Although his method of proof is similar to that employed in the proof of Theorem 3.7, a similar result is not stated. Therefore we shall now state a theorem determining the highest power of a prime dividing a multinomial coefficient; the ϵ's are chosen as in Theorem 3.7.

THEOREM 3.10. *The highest power N of a prime p dividing the multinomial coefficient $m!/m_1!m_2! \cdots m_n!$, where $m = m_1 + m_2 + \cdots + m_n$, is*

$$N = \epsilon_0 + \epsilon_1 + \cdots + \epsilon_{k-1} .$$

The following theorem is a generalization of the result by Lucas, Theorem 1.2.

THEOREM 3.11. *Let q belong to the exponent e* (mod p), *and let n and r be expanded as in* (3.1) *and* (3.2) *respectively. Then*

$$\begin{bmatrix} n \\ r \end{bmatrix} \equiv \begin{bmatrix} a_0 \\ b_0 \end{bmatrix} \binom{a_1}{b_1} \binom{a_2}{b_2} \cdots \pmod{p}. \tag{3.13}$$

Proof. Let

$$a = a_1 + a_2 p + a_3 p^2 + \cdots ,$$

$$b = b_1 + b_2 p + b_3 p^2 + \cdots .$$

Then

$$n = a_0 + ea,$$

$$r = b_0 + eb.$$

Since

$$\prod_{r=1}^{n} (1 + q^r x) \equiv \prod_{r=1}^{a_0} (1 + q^r x) \prod_{r=1}^{e} (1 + q^r x)^a \pmod{p},$$

we have by (2.2) that

$$\sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix} q^{\frac{1}{2}r(r+1)} x^r \equiv \sum_{k=0}^{a} \sum_{j=0}^{a_0} \begin{bmatrix} a_0 \\ j \end{bmatrix} \binom{a}{k} q^{\frac{1}{2}ke(e+1)+\frac{1}{2}j(j+1)} x^{ke+j} \pmod{p}.$$

For $r > n$ the theorem is obvious; therefore assume $r \leq n$, and hence $b \leq a$. Comparing coefficients of x^r we have for $b_0 \leq a_0$ that

$$\begin{bmatrix} n \\ r \end{bmatrix} \equiv \begin{bmatrix} a_0 \\ b_0 \end{bmatrix} \binom{a}{b} \pmod{p}. \tag{3.14}$$

Now if $b_0 > a_0$, then $\begin{bmatrix} a_0 \\ b_0 \end{bmatrix} = 0$. Comparing coefficients of x^r in this case we see that

$$\begin{bmatrix} n \\ r \end{bmatrix} \equiv 0 \pmod{p}.$$

Therefore

$$\begin{bmatrix} n \\ r \end{bmatrix} \equiv \begin{bmatrix} a_0 \\ b_0 \end{bmatrix} \binom{a}{b} \pmod{p}. \tag{3.15}$$

Applying Theorem 1.2 to (3.14) and (3.15) we obtain (3.13).

The following two theorems are immediate corollaries of Theorem 3.11.

THEOREM 3.12. *Let $N(n)$ be the number of coefficients $\begin{bmatrix} n \\ r \end{bmatrix}$ that are prime to p. Then*

$$N(n) = (a_0 + 1)(a_1 + 1)(a_2 + 1) \cdots,$$

where $a_0, a_1, \cdots$ are the digits of n.

THEOREM 3.13. *Let q belong to the exponent e* (mod p), *and let $k = (p - 1)/e$. Then*

$$\begin{bmatrix} pn \\ pr \end{bmatrix} \equiv \begin{bmatrix} n \\ r \end{bmatrix} \binom{a_0 k}{b_0 k} \pmod{p},$$

where a_0 and b_0 are defined by (3.1) *and* (3.2) *respectively.*

4. Periods of the binomial and q-binomial coefficients. For any non-negative integer n we shall determine the smallest positive integer A such that

$$\begin{bmatrix} n + A \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r} \tag{4.1}$$

for all integers k and r where

$$0 \leq k \leq n, \quad r = 1, 2, 3, \cdots.$$

Similarly for any positive integer k we shall determine the smallest positive integer A such that (4.1) holds for all nonnegative integers n and all positive integers r. As in the previous section we shall have to consider an exceptional case.

The corresponding results for the ordinary binomial coefficients are given at the end of this section. Since the proofs of these results are similar to those in the q case, they will be omitted.

Recall that we have assumed that q is a rational number which is not congruent to zero (mod p), that e is the exponent to which q belongs (mod p), and that h is the highest power of p dividing $q^e - 1$. For a fixed n it will be necessary to consider separately the theorems for $n < e$ and $n \geq e$; a similar situation exists for a fixed k. We shall first consider the case where n is fixed.

THEOREM 4.1. *Let q belong to the exponent e* (mod p), *and let h be the highest power of p dividing $q^e - 1$. Then if $e > 1$ and n is a positive integer less than e, the smallest positive integer A such that*

$$\begin{bmatrix} n + A \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r} \tag{4.2}$$

for all k such that $0 \leq k \leq n$ is

$$A = \begin{cases} ep^{r-h} & (r > h) \\ e & (r \leq h). \end{cases}$$

Proof. Note that $e > 1$ implies $p > 2$. Since $k \leq n < e$, (4.2) is equivalent to

$$\begin{aligned} (q^{n+A} - 1)(q^{n+A-1} - 1) \cdots (q^{n+A-k+1} - 1) \\ \equiv (q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1) \pmod{p^r}. \end{aligned} \tag{4.3}$$

Also since (4.2) must be satisfied for all k such that $0 \leq k \leq n$, it is necessary that it holds for $k = 1$, or

$$q^A \equiv 1 \pmod{p^r} \tag{4.4}$$

since $e > 1$. From (4.3) and (4.4) we see that the smallest positive integer A satisfying (4.2) is the exponent to which q belongs (mod p^r). Hence the theorem follows from Theorem 3.1.

To make our discussion complete we should consider the trivial case $n = 0$; then $A = 1$.

THEOREM 4.2. *Let q belong to the exponent e* (mod p), *and let h be the highest power of p dividing $q^e - 1$. Let $n \geq e$ for $p^h > 2$ and $n \geq 2$ for $p^h = 2$. Then if $ep^s \leq n < ep^{s+1}$ the smallest positive integer A such that*

$$\begin{bmatrix} n + A \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r} \tag{4.5}$$

for all integers k, where $0 \leq k \leq n$, is $A = ep^{r+s}$.

Proof. From (2.4) and (2.3) we see that

$$\begin{bmatrix} n + ep^{r+s} \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r}.$$

Therefore $A \leq ep^{r+s}$.

Now since (4.5) must hold for all $k \leq n$, it must be valid for $k = 1$. Hence it is necessary that

$$\begin{bmatrix} A \\ 1 \end{bmatrix} \equiv 0 \pmod{p^r}. \tag{4.6}$$

From this we see that

$$q^A \equiv 1 \pmod{p^r}, \tag{4.7}$$

which implies that e divides A.

We shall first consider the case $p^h > 2$. Let $A = cep^z$, where $(c, p) = 1$ and $z \geq 0$. Since $n \geq e$ we may choose $k = e$ in (4.5). From (2.4) and (4.7) we have

$$\begin{bmatrix} n + cep^z \\ e \end{bmatrix} \equiv \begin{bmatrix} n \\ e \end{bmatrix} + q^{en} \begin{bmatrix} cep^z \\ e \end{bmatrix} \pmod{p^r}.$$

Then to satisfy (4.5) it is necessary that

$$\begin{bmatrix} cep^z \\ e \end{bmatrix} \equiv 0 \pmod{p^r}.$$

From this and Theorem 3.3 we must have $z \geq r$. Hence if $s = 0$ the theorem is proved for this case.

Now consider the case $p^h = 2$ and $n \geq 2$. From (4.6) we have that

$$q^A \equiv 1 \pmod{4},$$

and hence by Theorem 3.4 it follows that 2 divides A. Let $A = c2^z$, where $(c, 2) = 1$ and $1 \leq z \leq r + s$. Choosing $k = 2$ in (4.5) we see that it is necessary for

$$\begin{bmatrix} A \\ 2 \end{bmatrix} \equiv 0 \pmod{2^r}.$$

Then from Theorem 3.6 we have that 2^{r+1} divides A. Note that the assumption $n \geq 2$ implies that $s > 0$.

In the remainder of the proof we shall assume that $s > 0$; both cases, $p^h > 2$ and $p^h = 2$, will be considered together. Suppose $A < ep^{r+s}$; therefore let $A = cep^{r+z-1}$ where $(c, p) = 1$ and $1 \leq z \leq s$. From (2.4) and (2.3) we have that

$$\begin{bmatrix} n + cep^{r+z-1} \\ ep^z \end{bmatrix} \equiv \begin{bmatrix} n \\ ep^z \end{bmatrix} + q^{nep^z} \begin{bmatrix} cep^{r+z-1} \\ ep^z \end{bmatrix} \pmod{p^r}.$$

Hence if we choose $k = ep^z$ in (4.5), it is necessary that

$$\begin{bmatrix} cep^{r+z-1} \\ ep^z \end{bmatrix} \equiv 0 \pmod{p^r}.$$

But from Theorems 3.3 and 3.6 this cannot be. Therefore we must have $A = ep^{r+s}$.

To complete our study we now consider the case which was excluded above, namely $p^h = 2$ and $n = 1$.

THEOREM 4.3. *Let $q \equiv 3 \pmod{4}$ and s be the highest power of 2 dividing $q + 1$. The smallest positive integer A such that*

$$\begin{bmatrix} 1 + A \\ k \end{bmatrix} \equiv \begin{bmatrix} 1 \\ k \end{bmatrix} \pmod{2^r} \qquad (4.8)$$

for $k = 0$ and 1 and r a positive integer is

$$A = \begin{cases} 2^{r-s+1} & (r > s) \\ 2 & (r \leq s). \end{cases}$$

Proof. Since for $k = 0$ both sides of (4.8) are one, we need only consider the case $k = 1$. Thus it is sufficient to determine the smallest positive integer A such that

$$q^A \equiv 1 \pmod{2^{r+1}}.$$

Since $r \geq 1$, the theorem follows from Theorem 3.4.

THEOREM 4.4. *Let q belong to the exponent e (mod p), and let h be the highest power of p dividing $q^e - 1$. Then if $e > 1$ and k is a positive integer less than e, the smallest positive integer A such that*

$$\begin{bmatrix} n + A \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r} \tag{4.9}$$

for all non-negative integers n is

$$A = \begin{cases} ep^{r-h} & (r > h) \\ e & (r \leq h). \end{cases}$$

Proof. Since $0 < k < e$, (4.9) is equivalent to (4.3). Since (4.9) must be satisfied for all $n \geq 0$, we may let $n = k - 1$ and k, and we have that

$$\begin{bmatrix} A + k - 1 \\ k \end{bmatrix} \equiv 0 \pmod{p^r}$$

and

$$\begin{bmatrix} A + k \\ k \end{bmatrix} \equiv 1 \pmod{p^r}$$

respectively. From these two congruences we have

$$\begin{aligned} q^A - 1 &\equiv (q^A - 1)\begin{bmatrix} A + k \\ k \end{bmatrix} \pmod{p^r} \\ &\equiv (q^{A+k} - 1)\begin{bmatrix} A + k - 1 \\ k \end{bmatrix} \pmod{p^r} \\ &\equiv 0 \pmod{p^r}. \end{aligned} \tag{4.10}$$

Hence from (4.3) and (4.10) we see that A is the exponent to which q belongs (mod p^r), and the theorem follows from Theorem 3.1.

In the trivial case $k = 0$, it is evident that $A = 1$ is the smallest positive integer since both terms are one in this case.

THEOREM 4.5. *Let q belong to the exponent e* (mod p), *and let h be the highest power of p dividing $q^e - 1$. Let $k \geq e$ for $p^h > 2$ and $k \geq 2$ for $p^h = 2$. Then if $ep^s \leq k < ep^{s+1}$ the smallest positive integer A such that*

$$\begin{bmatrix} n + A \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r} \tag{4.11}$$

for every non-negative integer n is $A = ep^{r+s}$.

Proof. As in the proof of Theorem 4.2 we see from (2.4) and (2.3) that $A \leq ep^{r+s}$. Also letting $n = k - 1$ and k successively in (4.11) we have as in (4.10) that

$$q^A \equiv 1 \pmod{p^r},$$

and hence e divides A.

First we consider the case $r = 1$. Let $A = eB$, and let

$$n = a_0 + ea, \qquad k = b_0 + eb,$$

where

$$0 \leq a_0 < e, \qquad 0 \leq b_0 < e.$$

Then we have by Theorem 3.11 that

$$\begin{bmatrix} n + A \\ k \end{bmatrix} \equiv \begin{bmatrix} a_0 \\ b_0 \end{bmatrix} \binom{a + B}{b} \pmod{p}$$

and

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv \begin{bmatrix} a_0 \\ b_0 \end{bmatrix} \binom{a}{b} \pmod{p}.$$

Therefore it will suffice to determine the smallest positive integer B such that

$$\binom{a + B}{b} \equiv \binom{a}{b} \pmod{p}$$

for all non-negative integers a. By Theorem 1.2 it is evident that $B = p^{s+1}$. Hence $A = ep^{s+1}$, and the theorem is proved in this case.

Now assume $r > 1$. Let $A = cep^z$, where $(c, p) = 1$ and $z \geq 0$. Suppose $A < ep^{r+s}$ then $r + s - 1 - z \geq 0$. Let $k = b_0 + e(b_1 + b_2p + \cdots + b_{s+1}p^s)$, where $0 \leq b_0 < e$, $0 \leq b_j < p$ for $j = 1, 2, \cdots, s$ and $0 < b_{s+1} < p$. For any positive integer A satisfying (4.11) we have

$$\begin{bmatrix} n + mA \\ k \end{bmatrix} \equiv \begin{bmatrix} n \\ k \end{bmatrix} \pmod{p^r},$$

where m is a non-negative integer. Therefore

$$\begin{bmatrix} k - eb_{s+1}p^s + cep^{r+s-1} \\ k \end{bmatrix} \equiv \begin{bmatrix} k - eb_{s+1}p^s \\ k \end{bmatrix} \equiv 0 \pmod{p^r}.$$

But by Theorems 3.3 and 3.6 we have that the highest power of p dividing

$$\begin{bmatrix} k - eb_{s+1}p^s + cep^{r+s-1} \\ k \end{bmatrix}$$

is $r - 1$, which gives us a contradiction and proves the theorem.

The next theorem completes our examination by considering the exceptional case $p^h = 2$ and $k = 1$.

THEOREM 4.6. *If* $q \equiv 3 \pmod 4$ *and* s *is the highest power of* 2 *dividing* $q + 1$, *then the smallest positive integer* A *such that*

$$\begin{bmatrix} n + A \\ 1 \end{bmatrix} \equiv \begin{bmatrix} n \\ 1 \end{bmatrix} \pmod{2^r} \tag{4.12}$$

for all non-negative integers n *is*

$$A = \begin{cases} 2^{r-s+1} & (r > s) \\ 2 & (r \leq s). \end{cases}$$

Proof. If $r = 1$, (4.12) reduces to a congruence in binomial coefficients and the theorem is obvious. Now assume $r > 1$. By (2.4) we see that the theorem is equivalent to determining the smallest positive integer A such that

$$\begin{bmatrix} A \\ 1 \end{bmatrix} \equiv 0 \pmod{2^r}.$$

But since $q \equiv 3 \pmod 4$, this integer is the exponent to which q belongs $\pmod{2^{r+1}}$, and this theorem follows from Theorem 3.4.

The next two theorems state the corresponding results for the ordinary binomial coefficients.

THEOREM 4.7. *Let* $p^s \leq n < p^{s+1}$. *Then the smallest positive integer* A *such that*

$$\binom{n + A}{k} \equiv \binom{n}{k} \pmod{p^r}$$

for all integers k, *where* $0 \leq k \leq n$, *is* $A = p^{r+s}$.

THEOREM 4.8. *Let* $p^s \leq k < p^{s+1}$. *Then the smallest positive integer* A *such that*

$$\binom{n + A}{k} \equiv \binom{n}{k} \pmod{p^r}$$

for all non-negative integers n *is* $A = p^{r+s}$.

Since the proofs of these theorems are similar to those of Theorems 4.2 and 4.5 respectively, they have been omitted.

References

1. L. Carlitz, *q-Bernoulli numbers and polynomials*, this Journal, vol. 15(1948), pp. 987–1000.
2. L. E. Dickson, *Theorems on the residues of multinomial coefficients with respect to a prime modulus*, Quart. J. Math., vol. 33(1902), pp. 378–384.
3. L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institution of Washington, Washington, 1919.
4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford, 1960.
5. F. H. Jackson, *q-difference equations*, Amer. J. Math., vol. 32(1910), pp. 305–314.
6. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math., vol. 44(1852), pp. 93–146.
7. A. M. Legendre, *Théorie des Nombres*, third edition, Paris, 1830.
8. E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier*, Bull. Soc. Math. France, vol. 6(1878), pp. 49–54.
9. J. Riordan, *Combinatorial Analysis*, New York, 1958.
10. Morgan Ward, *A calculus of sequences*, Amer. J. Math., vol. 58(1936), pp. 255–266.

Duke University
and
Florida State University