ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 25, Number 3, Summer 1995

SOME CONGRUENCES FOR GENERALIZED BINOMIAL COEFFICIENTS

WILLIAM A. KIMBALL AND WILLIAM A. WEBB

For an arbitrary sequence of integers $\{u_n\}_{n=1}^{\infty}$, the generalized binomial coefficients are defined by

$$\begin{bmatrix} n \\ k \end{bmatrix}_j = \frac{u_{nj}u_{(n-1)j}\cdots u_j}{(u_{kj}u_{(k-1)j}\cdots u_j)(u_{(n-k)j}\cdots u_j)}$$

and $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix}_1$. In order to guarantee that these expressions are integers, it is usually required that the sequence $\{u_n\}$ be regularly divisible, that is, $p^i|u_j$ if and only if $r(p^i)|j$ for all $i \geq 1$, $j \geq 1$, and all primes p. Here $r(p^i)$ denotes the *rank of apparition* of p^i, that is, the index of the first element of $\{u_n\}$ divisible by p^i.

Such generalized binomial coefficients have many properties in common with the usual binomial coefficients $\binom{n}{k}$. Analogs of results such as Kummer's theorem, Lucas's theorem, the Star of David property, etc., have all been studied [**3, 4, 7, 10**].

The principal class of sequences which are known to be regularly divisible are the second order recurrence sequences $u_n = au_{n-1} + bu_{n-2}$ with $(a, b) = 1$ and initial conditions $u_0 = 0$ and $u_1 = 1$ [**5**]. We will deal with such sequences and introduce the following additional notation. Let $D = a^2 + 4b \neq 0$, $\alpha = (a + \sqrt{D})/2$, $\beta = (a - \sqrt{D})/2$, so that $\alpha + \beta = a$ and $\alpha\beta = -b$. Then $u_n = (\alpha^n - \beta^n)/\sqrt{D}$ and we also define the companion integer sequence $v_n = \alpha^n + \beta^n$. The following identities are easily established

(1) $2u_{n+k} = u_n v_k + u_k v_n$

(2) $2v_{n+k} = v_n v_k + D u_n u_k$

(3) $v_{n+k} = v_n v_k - (-b)^k v_{n-k}$

(4) $v_n = u_{n+1} + bu_{n-1}$.

Received by the editors on May 19, 1993.

Finally, p will always denote an odd prime, τ the period and $r = r(p)$ the *rank of apparition* of $\{u_n\}$ modulo p, and $t = \tau/r$ which will be an integer. We also assume that $p \nmid b$ and $p \nmid D$.

It is readily apparent that

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p},$$

and it has at various times been noted that

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^2}$$

for $p \geq 3$ and mod p^3 for $p \geq 5$ [**1, 2, 8**]. Another special case when u_n is the nth Fibonacci number also produces a congruence which holds modp^2 [**6**]. We will examine what happens when u_n is an arbitrary second order recurrence, subject only to the conditions noted previously. Simple numerical examples show that we cannot expect a congruence of such a simple form to hold. We will also note how these general theorems apply to another widely studied type of expression, namely the q-binomial coefficients.

Theorem 1. *For* $n \geq m \geq 0$,

$$\begin{bmatrix} nr \\ mr \end{bmatrix} \equiv \left(\frac{v_r}{2}\right)^{(n-m)mr} \binom{n}{m} \pmod{p^2}.$$

Proof. Separating the factors divisible by p from those relatively prime to p, we have

$$(5) \quad \begin{bmatrix} nr \\ mr \end{bmatrix} = \left(\frac{u_{nr}}{u_{mr}} \frac{u_{(n-1)r}}{u_{(m-1)r}} \cdots \frac{u_{(n-m+1)r}}{u_r}\right)\left(\frac{\prod_{k=(n-1)r+1}^{nr-1} u_k \cdots \prod_{k=(n-m)r+1}^{(n-m+1)r-1} u_k}{\prod_{k=(m-1)r+1}^{mr-1} u_k \cdots \prod_{k=1}^{r-1} u_k}\right) = \begin{bmatrix} n \\ m \end{bmatrix}_r \Pi_1,$$

respectively.

We first note that

$$v_{kr} \equiv 2\left(\frac{v_r}{2}\right)^k \pmod{p^2} \quad \text{for } k \geq 0. \tag{6}$$

This can be proved using induction on k and noting that, by (2) and the induction hypothesis,

$$\begin{aligned} v_{(k+1)r} &\equiv \frac{1}{2}(v_{kr}v_r + Du_{kr}u_r) \equiv 2\left(\frac{v_r}{2}\right)^k \left(\frac{v_r}{2}\right) \\ &\equiv 2\left(\frac{v_r}{2}\right)^{k+1} \pmod{p^2}. \end{aligned}$$

Another induction argument shows that if $p^s|k$,

$$\frac{u_{kr}}{u_{p^s r}} \equiv \left(\frac{k}{p^s}\right)\left(\frac{v_r}{2}\right)^{k-p^s} \pmod{p^2}. \tag{7}$$

We can pair off the factors in $\begin{bmatrix} n \\ m \end{bmatrix}_r$ to be of the form u_{kr}/u_{jr} such that k/j is a p-integer, and apply (7) to obtain

$$\begin{bmatrix} n \\ m \end{bmatrix}_r \equiv \binom{n}{m}\left(\frac{v_r}{2}\right)^{(n-m)m} \pmod{p^2}. \tag{8}$$

From (1) and (6) we have

$$u_{mr+k} \equiv \left(\frac{v_r}{2}\right)^m u_k + \frac{1}{2}v_k u_{mr} \pmod{p^2}$$

and so

$$\begin{aligned} \prod_{k=nr+1}^{(n+1)r-1} u_{mr+k} &\equiv \left(\frac{v_r}{2}\right)^{mr-m} \prod_{k=nr+1}^{(n+1)r-1} u_k + \frac{1}{2}\left(\frac{v_r}{2}\right)^{mr-2m} u_{mr} \\ &\quad \prod_{k=nr+1}^{(n+1)r-1} u_k \sum_{k=nr+1}^{(n+1)r-1} \frac{v_k}{u_k} \pmod{p^2}. \end{aligned} \tag{9}$$

However,

$$\sum_{k=nr+1}^{(n+1)r-1} \frac{v_k}{u_k} \equiv 0 \pmod p$$

since

$$\frac{v_{nr+i}}{u_{nr+i}} + \frac{v_{(n+1)r-i}}{u_{(n+1)r-i}} = \frac{2u_{(2n+1)r}}{u_{nr+i}u_{(n+1)r-i}}$$

and if r is even, $v_{nr+r/2} \equiv 0 \pmod p$ by (1). Hence, the second term on the right side of (9) is $0 \pmod{p^2}$, and we have

$$\Pi_1 \equiv \left(\frac{v_r}{2}\right)^{(n-m)m(r-1)} \pmod{p^2}, \tag{10}$$

and Theorem 1 follows from (5), (8) and (10). □

Corollary 2.

$$\begin{bmatrix} n\tau \\ m\tau \end{bmatrix} \equiv \left(1 + \tau(n-m)m\left(\left(\frac{v_r}{2}\right)^t - 1\right)\right)\binom{nt}{mt} \pmod{p^2}. \tag{11}$$

Proof. Replacing n and m by nt and mt, respectively, in Theorem 1, we obtain

$$\begin{bmatrix} n\tau \\ m\tau \end{bmatrix} \equiv \left(\frac{v_r}{2}\right)^{t\tau(n-m)m}\binom{nt}{mt} \pmod{p^2}. \tag{12}$$

Since τ is the period, $u_{\tau-1} \equiv b^{-1} \pmod p$ and $u_{\tau+1} \equiv 1 \pmod p$ so, by (4), $v_\tau \equiv 2 \pmod p$. By (6), $v_\tau \equiv 2(v_r/2)^t \pmod{p^2}$, and so $(v_r/2)^t \equiv 1 \pmod{p^2}$. Hence,

$$\begin{aligned} \left(\frac{v_r}{2}\right)^{tk} &= \left(1 + \left(\left(\frac{v_r}{2}\right)^t - 1\right)\right)^k \\ &\equiv 1 + k\left(\left(\frac{v_r}{2}\right)^t - 1\right) \pmod{p^2}. \end{aligned} \tag{13}$$

Taking $k = \tau(n-m)m$ and substituting in (12) completes the proof. □

The congruence in Corollary 1 still involves the factor v_r as well as the parameters n, m and τ. We can, however, eliminate v_r as follows.

By (3) and (2), respectively,

$$v_{2r} = v_r^2 - 2(-b)^r \quad \text{and} \quad 2v_{2r} \equiv v_r^2 \pmod{p^2}$$

and so $(v_r/2)^2 \equiv (-b)^r \pmod{p}^2$. Since, by (3),

$$\left(\frac{v_r}{2}\right)^{2t} - 2\left(\frac{v_r}{2}\right)^t + 1 \equiv 0 \pmod{p^2}$$

we have

$$\begin{aligned}\left(\frac{v_r}{2}\right)^t &\equiv \frac{1}{2}\left(1 + \left(\frac{v_r}{2}\right)^{2t}\right) \\ &\equiv \frac{1}{2}(1 + (-b)^{rt}) \pmod{p^2}. \qquad \square\end{aligned}$$

Substituting this expression in (12) yields

Theorem 3.

$$\begin{bmatrix} n\tau \\ m\tau \end{bmatrix} \equiv \left(1 + \frac{1}{2}\tau(n-m)m((-b)^\tau - 1)\right)\binom{nt}{mt} \pmod{p^2}.$$

Since τ must be even when $b = -1$ [**9**], we also have

Corollary 4. *If* $b = \pm 1$, *then*

$$\begin{bmatrix} n\tau \\ m\tau \end{bmatrix} \equiv \binom{nt}{mt} \pmod{p^2}.$$

Although we assumed a and b were integers, the extension to any p-integral rational numbers is immediate.

An important special case which has been widely studied are the q-binomial coefficients or Gaussian polynomials.

$$\binom{\mathbf{n}}{\mathbf{k}} = \frac{1(1+q)(1+q+q^2)\cdots(1+q+\cdots+q^{n-1})}{1(1+q)\cdots(1+\cdots+q^{k-1})1(1+q)\cdots(1+\cdots+q^{n-k-1})}$$

which can be considered as generalized binomial coefficients with respect to the sequence $\{u_n\}_{n=0}^{\infty}$ where $u_0 = 0$, $u_1 = 1$, $u_{n+2} = (q+1)u_{n+1} - qu_n$ for $n \geq 0$. Thus, $D = (q-1)^2$, $\alpha = q$, $\beta = 1$, $u_n = (q^n - 1)/(q-1)$ for $n > 0$ and $v_n = q^n + 1$. Clearly r is the smallest $n > 0$ such that $q^n \equiv 1 \pmod p$ and $\tau = r$ so $t = 1$.

We can take q to be any p-integral rational such that $p \nmid q^2 - q$. Applying the various theorems above to the q-binomials, we obtain

Theorem 5.

$$\begin{aligned}\binom{\mathbf{nr}}{\mathbf{mr}} &\equiv \left(\frac{q^r+1}{2}\right)^{(n-m)mr}\binom{n}{m} \pmod{p^2}\\ &\equiv \left(1 + \frac{1}{2}r(n-m)m(q^r-1)\right)\binom{n}{m} \pmod{p^2}.\end{aligned}$$

REFERENCES

1. D.F. Bailey, *Two p^3 variations of Lucas' theorem*, J. Number Theory **35** (1990), 208–215.

2. K. Davis and W. Webb, *A binomial coefficient congruence modulo prime powers*, J. Number Theory **43** (1993), 20–23.

3. R.D. Fray, *Congruence properties of ordinary and q-binomial coefficients*, Duke Math. J. **34** (1967), 467–480.

4. H.W. Bould, *Equal products of generalized binomial coefficients*, Fibonacci Quart. **9** (1971), 337–346.

5. P. Horak and L. Skula, *A characterization of the second-order strong divisibility sequences*, Fibonacci Quart. **23** (1985), 126–132.

6. W.A. Kimball and W.A. Webb, *Congruence properties of Fibonacci numbers and Fibonacci coefficients*, Proceeding of the Fifth International Conference on Fibonacci Numbers and their Applications, Kluwer, Dordrecht, 1993.

7. D.E. Knuth and H.S. Wilf, *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math. **396** (1989), 212–219.

8. R.P. Stanley, *Enumerative combinatorics*, Wadsworth & Brooks/Cole, Monterey, 1986.

9. J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, Fibonacci Quart. **1** (1963), 37–45.

10. D. Wells, *Lucas' theorem for generalized binomial coefficients*, Ph.D. thesis, Washington State University, 1992.

Department of Pure and Applied Mathematics, Washington State University, Pullman, WA 99164-3113