Internat. J. Math. & Math. Sci.
VOL. 11 NO. 4 (1988) 743-750

SOME CONGRUENCE PROPERTIES OF BINOMIAL COEFFICIENTS AND LINEAR SECOND ORDER RECURRENCES

NEVILLE ROBBINS

Department of Mathematics
San Francisco State University
San Francisco, CA 94132

(Received May 21, 1987)

ABSTRACT. Using elementary methods, the following results are obtained:(I) If p is prime, $0 \leq m \leq n$, $0 < b < ap^{n-m}$, and $p \nmid ab$, then $\binom{ap^n}{bp^m} \equiv (-1)^{p-1}\binom{ap^{n-m}}{b} \pmod{p^n}$; If r,s are the roots of $x^2 = Ax-B$, where $(A,B) = 1$ and $D = A^2-4B > 0$, if $u_n = \frac{r^n-s^n}{r-s}$, $v_n = r^n+s^n$, and $k > 0$, then (II) $v_{kp^n} \equiv v_{kp^{n-1}} \pmod{p^n}$;

(III) If p is odd and $p \nmid D$, then $u_{kp^n} \equiv (\frac{D}{p})\, u_{kp^{n-1}} \pmod{p^n}$;

(IV) $u_{k2^n} \equiv (-1)^B u_{k2^{n-1}} \pmod{2^n}$.

KEYWORDS AND PHRASES. Binomial coefficient, linear second order recurrence.
1980 AMS SUBJECT CLASSIFICATION CODE: 10A10k 10A35.

1. INTRODUCTION.

Following Lucas [1], let A, B be integers such that $(A,B) = 1$ and $D = A^2-4B > 0$. Let the roots of $x^2 = Ax-B$ be: $r = \frac{1}{2}(A+D^{1/2})$, $s = \frac{1}{2}(A-D^{1/2})$.

Let $n \geq 0$. Let the sequences u_n, v_n be defined by:

$$u_n = \frac{r^n-s^n}{r-s} \tag{1.1}$$

$$v_n = r^n+s^n \tag{1.2}$$

then

$$u_0 = 0,\ u_1 = 1,\ u_n = Au_{n-1} - Bu_{n-2} \text{ for } n \geq 2 \tag{1.3}$$

$$v_0 = 2,\ v_1 = A,\ v_n = Av_{n-1} - Bv_{n-2} \text{ for } n \geq 2 \tag{1.4}$$

$$r + s = A \tag{1.5}$$

$$rs = B \tag{1.6}$$

$$r-s = D^{1/2} \tag{1.7}$$

$$u_{2n} = u_n v_n \tag{1.8}$$

$$v_{2n} = v_n^2 - 2B^n \tag{1.9}$$

$$2u_{m+n} = u_m v_n + u_n v_m \tag{1.10}$$

Let p be prime. Let $O_p(t) = j$ if $p^j \mid t$, $p^{j+1} \nmid t$.

If $0 < k < p$, then $p \mid \binom{p}{k}$. (1.11)

If $0 \leq k \leq n$, then $\binom{n}{n-k} = \binom{n}{k}$ (1.12)

$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}$ (1.13)

If $x \equiv \pm a \pmod{2^n}$, then $x^2 \equiv a^2 \pmod{2^{n+1}}$ (1.14)

If $0 < k < p^e$ and $p \nmid k$, then $O_p(\binom{p^e}{k}) = e$ (1.15)

REMARK. (1.1) through (1.10) appear in Lucas [1]. (1.11) through (1.14) are elementary. (1.15) is theorem 2 in Robbins [2].

2. MAIN RESULTS.

Lemma (2.1), If $0 \leq m \leq n$, $0 < b < ap^{n-m}$, and $p \nmid ab$,

then $\binom{ap^n}{bp^m} \equiv \binom{ap^{n-m}}{b}(-1)^{b(p^m-1)} \pmod{p^n}$.

PROOF. $\binom{ap^n}{bp^m} = \prod_{j=0}^{bp^m-1} \frac{ap^n-j}{bp^m-j} = P_1 P_2$, where P_1 is the product of all such factors where $p^m \mid j$, and P_2 is the product of all such factors where $p^m \nmid j$.

Now $P_1 = \prod_{i=0}^{b-1} \frac{ap^n-ip^m}{bp^m-ip^m} = \prod_{i=0}^{b-1} \frac{ap^{n-m}-i}{b-i} = \binom{ap^{n-m}}{b}$, while

$P_2 = \prod_{\substack{j=1 \\ j \neq ip^m}}^{bp^m-1} \frac{ap^n-j}{j} \equiv (-1)^{bp^m-b} \pmod{p^n}$. Therefore

$\binom{ap^n}{bp^m} \equiv \binom{ap^{n-m}}{b}(-1)^{b(p^m-1)} \pmod{p^n}$.

THEOREM 2.1. If $0 < m < n$, $0 < b < ap^{n-m}$, and $p \nmid ab$, then $\binom{ap^n}{bp^m} \equiv (-1)^{p-1}\binom{ap^{n-m}}{b} \pmod{p^n}$.

PROOF. If p is odd, then $b(p^m-1) \equiv p-1 \equiv 0 \pmod 2$; if $p = 2$, then by hypothesis, b is odd, so $b(2^m-1) \equiv 1 \equiv 2-1 \pmod 2$. In either case, the conclusion now follows from Lemma 2.1.

LEMMA 2.2. $v_{2n+1} = A^{2n+1} - \sum_{k=1}^{n} \binom{2n+1}{k} B^k v_{2n+1-2k}$

PROOF. By (1.2) and the binomial theorem, we have

$$v_{2n+1} = r^{2n+1} + s^{2n+1} = (r+s)^{2n+1} - \sum_{k=1}^{2n} \binom{2n+1}{k} r^{2n+1-k} s^k,$$ so (1.5) implies

$$v_{2n+1} = A^{2n+1} - \{\sum_{k=1}^{n} \binom{2n+1}{k} r^{2n+1-k} s^k + \sum_{k=1}^{n} \binom{2n+1}{2n+1-k} r^k s^{2n+1-k}\}.$$ Now (1.12) implies

$$v_{2n+1} = A^{2n+1} - \sum_{k=1}^{n} \binom{2n+1}{k} (rs)^k (r^{2n+1-2k} + s^{2n+1-2k}),$$ so (1.2) and (1.6) imply

$$v_{2n+1} = A^{2n+1} - \sum_{k=1}^{n} \binom{2n+1}{k} B^k v_{2n+1-2k}.$$

LEMMA 2.3. $v_p \equiv v_1 \pmod p$

PROOF. Lemma 2.2 and (1.11) imply $v_p \equiv A^p \pmod p$; (1.13) implies $A^p \equiv A \pmod P$, so (1.4) implies $v_p \equiv v_1 \pmod p$.

LEMMA 2.4. If $i > j$, then $v_{i+j} = v_i v_j - B^j v_{i-j}$

PROOF. By (1.2) and (1.6),

$$v_i v_j - v_{i+j} = (r^i+s^i)(r^j+s^j)-(r^{i+j}+s^{i+j}) = r^i s^j + r^j s^i = (rs)^j (r^{i-j}+s^{i-j}) = B^j v_{i-j}.$$

LEMMA 2.5. If $0 < m < n$, $y \equiv z \pmod{p^m}$, $w \equiv x \pmod{p^n}$, and $x \equiv 0 \pmod{p^{n-m}}$, then $wy \equiv xz \pmod{p^n}$.

PROOF. Hypothesis implies $y = z+ip^m$, $w = x+jp^n$, so $wy \equiv xz+ip^m x \pmod{p^n}$. Hypothesis also implies $p^{n-m} | x$, so $wy \equiv xz \pmod{p^n}$.

LEMMA 2.6. If $k > 0$, $m > 1$, and $v_{p^m} \equiv v_{p^{m-1}} \pmod{p^m}$, then $v_{kp^m} \equiv v_{kp^{m-1}} \pmod{p^m}$.

PROOF. (Induction on k). Lemma 6 holds trivially for k=0, and by hypothesis for k=1.

$$v_{(k+1)p^m} = v_{kp^m+p^m} = v_{kp^m} v_{p^m} - B^{p^m} v_{kp^m-p^m} = v_{kp^m} v_{p^m} - B^{p^m} v_{(k-1)p^m}$$ by Lemma 2.4.

Now induction hypothesis and (1.13) imply that

$$v_{(k+1)p^m} \equiv v_{kp^{m-1}} v_{p^{m-1}} - B^{p^{m-1}} v_{(k-1)p^{m-1}} \pmod{p^m}.$$ Now Lemma 2.4 implies

$$v_{(k+1)p^m} \equiv v_{(k+1)p^{m-1}} \pmod{p^m}.$$

LEMMA 2.7. If p is odd and $n \geq 1$, then $v_{p^n} \equiv v_{p^{n-1}} \pmod{p^n}$.

PROOF. (Induction on n) Lemma 2.7 holds for $n=1$, by Lemma 2.3. Suppose Lemma 2.7 holds for all $m < n$, where $n \geq 2$. Then Lemma 2.2 implies

$$v_{p^{n-1}} = A^{p^{n-1}} - \sum_{i=0}^{\frac{1}{2}(p^{n-1}-1)} \binom{p^{n-1}}{i} B^i v_{p^{n-1}-2i}, \text{ also}$$

$$v_{p^n} = A^{p^n} - \sum_{j=0}^{\frac{1}{2}(p^n-1)} \binom{p^n}{j} B^j v_{p^n-2j}.$$

If $p \nmid j$, then (1.15) implies $\binom{p^n}{j} \equiv 0 \pmod{p^n}$.

Therefore
$$v_{p^n} \equiv A^{p^n} - \sum_{j=0}^{\frac{1}{2}(p^{n-1}-1)} \binom{p^n}{ip} B^{ip} v_{p^n-2ip}.$$

Let $ip = hp^m$, where $p \nmid h$ and $m < n$. Now

$B^{ip} \equiv B^{hp^m} \equiv B^{hp^{m-1}} \equiv B^i \pmod{p^m}$, by (1.13); also $v_{p^n-2ip} =$

$$v_{p^n-2hp^m} = v_{(p^{n-m}-2h)p^m} \equiv v_{(p^{n-m}-2h)p^{m-1}} \equiv v_{p^{n-1}-2i} \pmod{p^m}$$ by induction hypothesis

and Lemma 2.6. Therefore $B^{ip} v_{p^n-2ip} \equiv B^i v_{p^{n-1}-2i} \pmod{p^m}$. Also

$$\binom{p^n}{ip} \equiv \binom{p^n}{hp^m} \equiv \binom{p^{n-1}}{hp^{m-1}} \equiv \binom{p^{n-1}}{i} \equiv \binom{p^{n-m}}{h} \pmod{p^n}$$ by Theorem 2.1, and (1.15)

implies

$\binom{p^{n-m}}{h} \equiv 0 \pmod{p^{n-m}}$. Therefore Lemma 2.5 implies

$$\binom{p^n}{ip} B^{ip} v_{p^{n-2ip}} \equiv \binom{p^{n-1}}{i} B^i v_{p^{n-1}-2i} \pmod{p^n}.$$ Now (1.13) implies

$$v_{p^n} \equiv A^{p^{n-1}} - \sum_{i=0}^{\frac{1}{2}(p^{n-1}-1)} \binom{p^{n-1}}{i} B^i v_{p^{n-1}-2i} \pmod{p^n}, \text{ that is,}$$

$$v_{p^n} \equiv v_{p^{n-1}} \pmod{p^n}.$$

LEMMA 2.8. If $2 \mid A$, then $v_{2^n} \equiv 2 \pmod{2^{n+1}}$ for $n > 0$.

PROOF. (Induction on n) $v_{2^0} = v_1 = A = 2 \pmod{2}$ by (1.4) and hypothesis. Now induction hypothesis implies $v_{2^{n-1}} \equiv 2 \pmod{2^n}$, so (1.14) implies $v^2_{2^{n-1}} \equiv 4 \pmod{2^{n+1}}$. Hypothesis implies $2 \nmid B$, so $B^{2^{n-1}} \equiv 1 \pmod{2^n}$. Now (1.9) implies $v_{2^n} = v^2_{2^{n-1}} - 2B^{2^{n-1}} \equiv 4-2(1) \equiv 2 \pmod{2^{n+1}}$.

LEMMA 2.9. If $2 \nmid AB$, then $v_{2^n} \equiv -1 \pmod{2^{n+1}}$ for $n > 0$.

PROOF. (Induction on n) $v_{2^0} = v_1 = A \equiv -1 \pmod{2}$ by (1.4) and hypothesis. Now induction hypothesis implies $v_{2^{n-1}} \equiv -1 \pmod{2^n}$, so (1.14) implies

$v^2_{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$. Again, B odd implies $B^{2^{n-1}} \equiv 1 \pmod{2^n}$, so (1.9) implies $v_{2^n} = v^2_{2^{n-1}} - 2B^{2^{n-1}} \equiv 1-2(1) \equiv -1 \pmod{2^{n+1}}$.

LEMMA 2.10. If $2 \mid B$, then $v_{2^n} \equiv 1 \pmod{2^{n+1}}$ for $n > 0$.

PROOF. (Induction on n) Hypothesis implies A is odd, so (1.4) implies

$v_{2^0} = v_1 = A \equiv 1 \pmod{2}$. By hypothesis, $B \equiv 0 \pmod{2}$, so $B^{2^{n-1}} \equiv 0 \pmod{2^{2^{n-1}}}$. Since $2^{n-1} > n$ for $n > 1$, we have $B^{2^{n-1}} \equiv 0 \pmod{2^n}$. By induction hypothesis, $v_{2^{n-1}} \equiv 1 \pmod{2^n}$, so (1.14) implies $v^2_{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$.

Now (1.9) implies $v_{2^n} = v^2_{2^{n-1}} - 2B^{2^{n-1}} \equiv 1-2(0) \equiv 1 \pmod{2^{n+1}}$.

LEMMA 2.11. $v_{2^n} \equiv v_{2^{n-1}} \pmod{2^n}$

PROOF. Lemmas 2.8, 2.9, 2.10 imply $v_{2^{n-1}} \equiv t \pmod{2^n}$, $v_{2^n} \equiv t \pmod{2^{n+1}}$, where $t = 2$ or ± 1. Therefore $v_{2^n} \equiv t \equiv v_{2^{n-1}} \pmod{2^n}$.

THEOREM 2.2. In $n \geq 1$, then $v_{p^n} \equiv v_{p^{n-1}} \pmod{p^n}$.

PROOF. Follows from Lemmas 2.7 and 2.11.

THEOREM 2.3. If $n \geq 1$ and $k > 0$, then $v_{kp^n} \equiv v_{kp^{n-1}} \pmod{p^n}$

PROOF. Follows from Theorem 2.2 and Lemma 2.6.

LEMMA 2.12. $u_{2n+1} = D^n - \sum_{k=1}^{n} \binom{2n+1}{k} (-B)^k u_{2n+1-2k}$

PROOF. (1.1) and (1.7) imply $D^{1/2} u_{2n+1} = r^{2n+1} - s^{2n+1} =$

$(r-s)^{2n+1} - \sum_{k=1}^{2n} (-1)^k \binom{2n+1}{k} r^{2n+1-k} s^k$, so (1.7) implies

$$D^{1/2} u_{2n+1} = D^{n+1/2} - \{\sum_{k=1}^{n} (-1)^k \binom{2n+1}{k} r^{2n+1-k} s^k + \sum_{j=n+1}^{2n} (-1)^j \binom{2n+1}{j} r^{2n+1-j} s^j\}$$

Setting $j = 2n+1-k$ in the second sum, we obtain

$$D^{1/2} u_{2n+1} = D^{n+1/2} - \{\sum_{k=1}^{n} (-1)^k \binom{2n+1}{k} r^{2n+1-k} s^k - \sum_{k=1}^{n} (-1)^{2n-k} \binom{2n+1}{2n+1-k} r^k s^{2n+1-k}\}$$

$$= D^{n+1/2} - \sum_{k=1}^{n} (-1)^k (rs)^k \binom{2n+1}{k} (r^{2n+1-2k} - s^{2n+1-2k}) \quad \text{by (1.12)}$$

$$= D^{n+1/2} - D^{1/2} \sum_{k=1}^{n} \binom{2n+1}{k} (-B)^k u_{2n+1-2k} \quad \text{by (1.6) and (1.7), so}$$

$$u_{2n+1} = D^n - \sum_{k=1}^{n} \binom{2n+1}{k} (-B)^k u_{2n+1-2k} .$$

LEMMA 2.13. If p is odd, then $u_p \equiv (\frac{D}{p}) \pmod{p}$.

PROOF. Follows from Lemma 2.12, (1.11), and Euler's criterion.

LEMMA 2.14. If p is odd, $p \nmid D$, and $n \geq 1$, then $D^{1/2 \phi(p^n)} \equiv (\frac{D}{p}) \pmod{p^n}$.

PROOF. (Induction on n) Lemma 2.14 holds for n=1 by Euler's criterion. Let $(\frac{D}{p}) = t = \pm 1$. Now induction hypothesis implies

$D^{1/2 \phi(p^n)} \equiv t \pmod{p^n}$, so $D^{1/2 \phi(p^n)} = t + ip^n$. $D^{1/2 \phi(p^{n+1})} = (D^{1/2 \phi(p^n)})^p$

$= (t+ip^n)^p = t^p + pt^{p-1}(ip^n) + \sum_{j=2}^{p} \binom{p}{j} t^{p-j} (ip^n)^j$. Now $t^p = t$, and $p^{n+1} \mid p^{nj}$ for $j \geq 2$, so $D^{\frac{1}{2}\phi(p^{n+1})} \equiv t \pmod{p^{n+1}}$.

LEMMA 2.15. If $k \geq 0$, $m \geq 1$, p is odd, $t = (\frac{D}{p})$, and

$u_{p^m} \equiv tu_{p^{m-1}} \pmod{p^m}$, then $u_{kp^m} \equiv tu_{kp^{m-1}} \pmod{p^m}$.

PROOF. (Induction on k) Lemma 2.15 is trivially true for k=0, and is true by hypothesis for k=1. Now (1.10) implies

$2u_{(k+1)p^m} = 2u_{kp^m+p^m} = u_{kp^m}v_{p^m} + u_{p^m}v_{kp^m}$. By induction hypothesis,

$u_{kp^m} \equiv tu_{kp^{m-1}} \pmod{p^m}$, and $u_{p^m} \equiv tu_{p^{m-1}} \pmod{p^m}$;

Theorem 2.2 implies $v_{kp^m} \equiv v_{kp^{m-1}} \pmod{p^m}$ for $k \geq 0$. Therefore

$2u_{(k+1)p^m} \equiv tu_{kp^{m-1}}v_{p^{m-1}} + tu_{p^{m-1}}v_{kp^{m-1}} \equiv 2tu_{kp^m} \pmod{p^m}$. Since

p is odd, we have $u_{(k+1)p^m} \equiv tu_{kp^m} \pmod{p^m}$.

LEMMA 2.16. If p is odd, $p \nmid D$, and $n \geq 1$, then $u_{p^n} \equiv (\frac{D}{p})u_{p^{n-1}} \pmod{p^n}$.

PROOF. (Induction on n) Lemma 2.16 is true for n = 1 by Lemma 2.13.

Lemma 2.12 implies $u_{p^{n-1}} = D^{\frac{1}{2}(p^{n-1}-1)} - \sum_{i=1}^{\frac{1}{2}(p^{n-1}-1)} \binom{p^{n-1}}{i} (-B)^i u_{p^{n-1}-2i}$

also $u_{p^n} = D^{\frac{1}{2}(p^n-1)} - \sum_{j=1}^{\frac{1}{2}(p^n-1)} \binom{p^n}{j} (-B)^j u_{p^n-2j}$. If $p \nmid j$, then (1.15) implies

$\binom{p^n}{j} \equiv 0 \pmod{p^n}$. Therefore

$$u_{p^n} \equiv D^{\frac{1}{2}(p^n-1)} - \sum_{i=1}^{\frac{1}{2}(p^{n-1}-1)} \binom{p^n}{ip} (-B)^{ip} u_{p^n-2ip} \pmod{p^n}.$$

Let $ip = hp^m$ where $p \nmid h$ and $m < n$. Let $t = (\frac{D}{p})$.

Now $(-B)^{ip} \equiv (-B)^{hp^m} \equiv (-B)^{hp^{m-1}} \equiv (-B)^i \pmod{p^m}$ by (1.13). By induction

hypothesis and Lemma 2.15, we have

$$u_{p^n-2ip} \equiv u_{p^n-2hp^m} \equiv u_{(p^{n-m}-2h)p^m} \equiv tu_{(p^{n-m}-2h)p^{m-1}} \equiv tu_{p^{n-1}-2hp^{m-1}} \equiv$$

$tu_{p^{n-1}-2i}$ (mod p^m). Therefore $(-B)^{ip}u_{p^n-2ip} \equiv t(-B)^i u_{p^{n-1}-2i}$ (mod p^m).

As in the proof of Lemma 2.7, we have

$\binom{p^n}{ip}(-B)^{ip}u_{p^n-2ip} \equiv t\binom{p^{n-1}}{i}(-B)^i u_{p^{n-1}-2i}$ (mod p^n). Therefore

$u_{p^n} \equiv D^{1/2(p^n-1)} - t(D^{1/2(p^{n-1}-1)} - u_{p^{n-1}})$ (mod p^n), that is

$u_{p^n} \equiv tu_{p^{n-1}} + D^{1/2(p^{n-1}-1)}(D^{1/2(p^n-p^{n-1})} - t)$ (mod p^n). Since

$\phi(p^n) = p^n - p^{n-1}$, Lemma 2.14 implies $u_{p^n} \equiv (\frac{D}{p})u_{p^{n-1}}$ (mod p^n).

LEMMA 2.17. If $n > 1$ and D is odd, then $u_{2^n} \equiv (-1)^B u_{2^{n-1}}$ (mod 2^n).

PROOF. By hypothesis and by the definitions of A, B, and D, A must be odd. If B is odd, then Lemma 2.9 implies $v_{2^{n-1}} \equiv -1$ (mod 2^n); if B is even then Lemma 2.10 implies $v_{2^{n-1}} \equiv 1$ (mod 2^n). Therefore, in either case, $v_{2^{n-1}} \equiv (-1)^B$ (mod 2^n). Now (1.8) implies $u_{2^n} \equiv (-1)^B u_{2^{n-1}}$ (mod 2^n).

THEOREM 2.4. If $n > 1$ and $p \nmid D$, then $u_{p^n} \equiv tu_{p^{n-1}}$ (mod p^n), where

$$t = \begin{cases} (\frac{D}{p}) & \text{if } p \text{ is odd} \\ (-1)^B & \text{if } p = 2 \end{cases}$$

PROOF. Follows from Lemmas 2.16 and 2.17.

THEOREM 2.5. If $k > 0$, $n > 1$, and $p \nmid D$, then $u_{kp^n} \equiv tu_{kp^{n-1}}$ (mod p^n).

where t is defined as in Theorem 2.4.

PROOF. Follows from Lemma 2.15 and Theorem 2.4.

Concluding Remarks. Let t be defined as in Theorem 2.4 as a result of Theorems 2.3 and 2.5, the sequences v_{kp^n}, $t^n u_{kp^n}$ determine p-adic integers for each $k > 0$.

REFERENCES

1. LUCAS, E. Theorie des fonctions numeriques simplement periodiques, Amer. J. Math. 1 (1877) 184-240; 289-321.

2. ROBBINS, N. On the number of binomial coefficients which are divisible by their row number, Canad. Math. Bull. 25 (3) 1982, 363-365.