ON BINOMIAL COEFFICIENT RESIDUES

J. B. ROBERTS

The number of binomial coefficients $\binom{u}{v}$, $0 \leqslant v \leqslant u < n$, which are congruent to j, $0 \leqslant j \leqslant p - 1$, modulo the prime number p is denoted by $\theta_j(n)$. In this paper we give systems of simultaneous linear difference equations with constant coefficients whose solutions would yield the quantities $\theta_j(n)$ explicitly. In this direction we compute $\theta_j(n)$ in all cases for $p = 2$ and $\theta_j(p^k)$, $k \geqslant 0$, in all cases for $p = 3$ or 5. The complete explicit determination of $\theta_j(n)$ for arbitrary n is quite tedious for $p > 2$.

We also include various special results in the case $p = 2$ and prove that every prime divides "most" binomial coefficients in the sense that

$$\lim_{\to\infty} \theta(n)/\theta_0(n) = 0$$

where

$$\theta(n) = \sum_{j=1}^{p-1} \theta_j(n).$$

1. Definitions. If c, a, s, k are constants satisfying $0 \leqslant a \leqslant c \leqslant p - 1$, $1 \leqslant s \leqslant p^k$, k > 0, then the collection of all $\binom{u}{v}$ satisfying

$$cp^k \leqslant u < cp^k + s,\ ap^k \leqslant v \leqslant u + (a - c)p^k,$$

will be denoted by $(c, s, a)_k$. When we write $(c, s, a)_k$ we will assume that c, a, s, k satisfy the specified conditions unless stated explicitly to the contrary. For instance if we write $(0, s, a)_k$ this implies $0 \leqslant a \leqslant p - 1$, $1 \leqslant s \leqslant p^k$, $k > 0$. Any collection $(c, s, a)_k$ will be called a *k-triangle*.

The k-triangle $(c, s, a)_k$ can be put into 1–1 correspondence with the k-triangle $(0, s, 0)_k$ by the mapping

$$\binom{u}{v} \leftrightarrow \binom{u - cp^k}{v - ap^k}.$$

Hence any two k-triangles can be put into $1 - 1$ correspondence. Corresponding elements will be called *homologous*.

If K_1 and K_2 are two k-triangles and α is an integer such that $k_1 \equiv \alpha k_2 \pmod p$ whenever $k_1 \in K_1$ and $k_2 \in K_2$ are homologous we will write $K_1 \equiv \alpha K_2 \pmod p$.

Received October 2, 1956

2. A lemma of Lucas and applications. Our first lemma is a result of Lucas (**1**, p. 271). A simple proof may be found in Glaisher (**2**). We use p for a prime throughout.

LEMMA 1. *If in the scale of radix* p,

$$m = b_0 + b_1 p + \ldots + b_k p^k$$
$$n = a_0 + a_1 p + \ldots + a_k p^k;$$

then

$$\binom{n}{m} \equiv \binom{a_0}{b_0} \cdots \binom{a_k}{b_k} \pmod{p}.$$

(The quantity $\binom{r}{s} = 0$ when $s > r$.)

Before making use of this lemma we observe that by repeated use of the identity

$$\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b+1}$$

and the almost obvious fact that

$$\binom{p^k}{m} \equiv 0 \pmod{p} \qquad (1 \leqslant m \leqslant p^k - 1, \quad k > 0)$$

we are able to prove

LEMMA 2. *If* $n - p^k + 1 \leqslant m < p^k \leqslant n < 2p^k - 1$, $k > 0$, *then*

$$\binom{n}{m} \equiv 0 \pmod{p}.$$

We come now to our first application of Lemma 1.

LEMMA 3. *If* $0 \leqslant v \leqslant u$, $cp^k \leqslant u < (c+1)p^k$, $1 \leqslant c \leqslant p-1$ *and if* $\binom{u}{v}$ *is in none of the k-triangles* $(c, p^k, a)_k$, $0 \leqslant a \leqslant c$, *then*

$$\binom{u}{v} \equiv 0 \pmod{p}.$$

Proof. Since $\binom{u}{v}$ is not in $(c, p^k, a)_k$ for each a, $0 \leqslant a \leqslant c$, v must satisfy for some a, $0 \leqslant a \leqslant c-1$, the inequality

$$u + 1 + (a - c)p^k \leqslant v \leqslant (a+1)p^k - 1.$$

Since for each a, $0 \leqslant a \leqslant c - 1$, this inequality is impossible when $u = (c+1)p^k - 1$ we can restrict attention to $u < (c+1)p^k - 1$. Now

$$u = a_0 + a_1 p + \ldots + a_{k-1} p^{k-1} + cp^k$$
$$v = b_0 + b_1 p + \ldots + b_{k-1} p^{k-1} + ap^k$$

https://doi.org/10.4153/CJM-1957-043-6 Published online by Cambridge University Press

and therefore by Lemma 1,

$$\binom{u}{v} \equiv \binom{a_0}{b_0} \cdots \binom{a_{k-1}}{b_{k-1}} \binom{c}{a} \equiv \binom{u - (c-1)p^k}{v - ap^k} \pmod{p}.$$

But since

$$(u - (c-1)p^k) - p^k + 1 = u + 1 - cp^k \leqslant v - ap^k \leqslant p^k - 1 < p^k \leqslant u - (c-1)p^k < 2p^k - 1,$$

we know by Lemma 3 that

$$\binom{u - (c-1)p^k}{v - ap^k} \equiv 0 \pmod{p}.$$

This completes the proof.

By this lemma we see that when $u \not\equiv (c+1)p^k - 1$ there is always a v, $0 \leqslant v \leqslant u$, such that $\binom{u}{v}$ is divisible by p. It is interesting to note that for each u of the form $(c+1)p^k - 1$, $\binom{u}{v}$ is non-divisible by p for $0 \leqslant v \leqslant u$. Thus we state the

COROLLARY. *No* $\binom{u}{v}$, $0 \leqslant v \leqslant u$, *is divisible by* p *if and only if* u *is of the form* $(c+1)p^k - 1$ *where* $0 \leqslant c \leqslant p - 1$.

Proof. The necessity is by the lemma. For the sufficiency we have

$$(c+1)p^k - 1 = (p-1) + (p-1)p + \ldots + (p-1)p^{k-1} + cp^k$$
$$v = b_0 + b_1 p + \ldots + b_{k-1}p^{k-1} + b_k p^k$$

where $b_i \leqslant p - 1$, $1 \leqslant i \leqslant k - 1$ and $b_k \leqslant c$. Hence

$$\binom{(c+1)p^k - 1}{v} \equiv \binom{p-1}{b_0} \cdots \binom{p-1}{b_{k-1}} \binom{c}{b_k} \pmod{p}$$

by Lemma 1. But this right-hand side is not congruent to 0 modulo p. This completes the proof.

Another important application of Lemma 1 is the following

LEMMA 4.

$$(c, s, a)_k \equiv \binom{c}{a} (0, s, 0)_k \pmod{\text{p}}.$$

Proof. Let $\binom{u}{v}$ be in $(c, s, a)_k$. Then $cp^k \leqslant u < cp^k + s$, $ap^k \leqslant v \leqslant u + (a - c)p^k$ and we can write in radix p,

https://doi.org/10.4153/CJM-1957-043-6 Published online by Cambridge University Press

$$u = a_0 + a_1 p + \ldots + a_{k-1} p^{k-1} + cp^k$$
$$v = b_0 + b_1 p + \ldots + b_{k-1} p^{k-1} + ap^k.$$

Hence by Lemma 1,

$$\binom{u}{v} \equiv \binom{u - cp^k}{v - ap^k}\binom{c}{a} \qquad (\text{mod } p).$$

Since $\binom{u-cp^k}{v-ap^k}$ runs over $(0, s, 0)_k$ as $\binom{u}{v}$ runs over $(c, s, a)_k$ the proof is complete.

COROLLARY. *The number of numbers in $(c, s, a)_k$ which are congruent to j (mod p), $1 \leqslant j \leqslant p-1$, is*

$$\theta_{j_a}(s)$$

where j_a is that number satisfying

$$1 \leqslant j_a \leqslant p - 1, j_a\binom{c}{a} \equiv j \qquad (\text{mod } p).$$

Proof. By the lemma a number in $(c, s, a)_k$ is congruent to j modulo p if and only if $\binom{c}{a}$ times its homologous element in $(0, s, 0)_k$ is congruent to j modulo p. Since

$$j_a\binom{c}{a} \equiv j \ (\text{mod p})$$

the number of possibilities is the number of j_a in $(0, s, 0)_k$ and this is just

$$\theta_{j_a}(s).$$

3. The main recursion relation. Utilizing Lemma 3 we see that for $0 \leqslant c \leqslant p-1$, $1 \leqslant s \leqslant p^k$ all of those $\binom{u}{v}$, $0 \leqslant v \leqslant u$, $cp^k \leqslant u < cp^k + s$, which are not congruent to zero modulo p are in one of the $c+1$ k-triangles $(c, s, a)_k$, $0 \leqslant a \leqslant c$. Therefore $\theta_j(cp^k + s) - \theta_j(cp^k)$ is just the number of elements congruent to j modulo p contained in these k-triangles. By Lemma 4 this number is

$$\sum_{a=0}^{c} \theta_{j_a}(s).$$

Defining $e_{qj}(c)$, $1 \leqslant q \leqslant p-1$, to be the number of j_a, $0 \leqslant a \leqslant c$, which are equal to q, the above sum becomes

$$\sum_{q=1}^{p-1} e_{qj}(c)\, \theta_q(s).$$

But $e_{qj}(c)$ is just the number of solutions of the congruence

$$\binom{c}{x} q \equiv j \pmod{p},$$

which number is, by definition,

$$\theta_{j\bar{q}}(c+1) - \theta_{j\bar{q}}(c)$$

where $\bar{q}$ is the reciprocal of q modulo p. Hence we have the following theorem setting forth our main recursion relation.

THEOREM 1. *If* $0 \leqslant c \leqslant p-1$, $1 \leqslant s \leqslant p^k$, $k > 0$, $q\bar{q} \equiv 1 \pmod{p}$ *then*

$$\theta_j(cp^k + s) = \theta_j(cp^k) + \sum_{q=1}^{p-1} (\theta_{j\bar{q}}(c+1) - \theta_{j\bar{q}}(c))\, \theta_q(s).$$

Remembering the definition of $\theta(n)$ we have under the hypotheses of the theorem the following

COROLLARY 1. $\theta(cp^k + s) = \theta(cp^k) + (c+1)\theta(s)$.

Proof. For each q, $1 \leqslant q \leqslant p-1$, the residues modulo p of the numbers $\bar{q}, 2\bar{q}, \ldots, (p-1)\bar{q}$ are the numbers $1,2,\ldots, p-1$ in some order. Using this fact and the theorem we obtain

$$\begin{aligned}\theta(cp^k + s) &= \sum_{j=1}^{p-1} \theta_j(cp^k + s)\\ &= \sum_{j=1}^{p-1} \theta_j(cp^k) + \sum_{q=1}^{p-1} \sum_{j=1}^{p-1} (\theta_{j\bar{q}}(c+1) - \theta_{j\bar{q}}(a))\, \theta_q(s)\\ &= \theta(cp^k) + (\theta(c+1) - \theta(c))\, \theta(s).\end{aligned}$$

Since $\theta(c+1) - \theta(c) = c + 1$, because c is smaller than p, the proof is complete.

COROLLARY 2. *If* $0 \leqslant c \leqslant p$, $k \geqslant 0$ *then*

(a) $$\theta_j(cp^k) = \sum_{q=1}^{p-1} \theta_{j\bar{q}}(c)\, \theta_q(p^k);$$

(b) $$\theta(cp^k) = \tfrac{1}{2}\, c(c+1)\, \theta(p^k).$$

Proof. (a) This is true for $c = 0$ or $k = 0$ so we suppose $c > 0$, $k > 0$. Now taking $s = p^k$ the theorem gives, for $1 \leqslant c \leqslant p$,

$$\begin{aligned}\theta_j(cp^k) &= \sum_{i=1}^{c} (\theta_j(ip^k) - \theta_j((i-1)p^k))\\ &= \sum_{i=1}^{c} \sum_{q=1}^{p-1} (\theta_{j\bar{q}}(i) - \theta_{j\bar{q}}(i-1))\, \theta_q(p^k)\\ &= \sum_{q=1}^{p-1} \sum_{i=1}^{c} (\theta_{j\bar{q}}(i) - \theta_{j\bar{q}}(i-1))\, \theta_q(p^k)\\ &= \sum_{q=1}^{p-1} \theta_{j\bar{q}}(c)\, \theta_q(p^k).\end{aligned}$$

(b) $$\theta(cp^k) = \sum_{j=1}^{p-1} \theta_j(cp^k)$$
$$= \sum_{q=1}^{p-1} \left(\sum_{j=1}^{p-1} \theta_{j\bar{q}}(c)\right) \theta_q(p^k)$$
$$= \theta(c)\,\theta(p^k) = \tfrac{1}{2}\,c(c+1)\,\theta(p^k).$$

COROLLARY 3. (a) *If* $k > 0$, $1 \leqslant j \leqslant p-1$ *then*

$$\theta_j(p^k) = \sum_{q=1}^{p-1} \theta_{j\bar{q}}(p)\,\theta_q(p^{k-1})\;;$$

(b) *If* $k \geqslant 0$ *then*

$$\theta(p^k) = (\tfrac{1}{2}p(p+1))^k.$$

Proof. (a) Taking $c = p$ in Cor. 2 (a) gives

$$\theta_j(p^{k+1}) = \sum_{q=1}^{p-1} \theta_{j\bar{q}}(p)\,\theta_q(p^k),\; k \geqslant 0$$

and this is equivalent with (a).

(b) This is obvious for $k = 0$. If true up to some $k \geqslant 0$ then by Cor. 2(b),

$$\theta(p^{k+1}) = \tfrac{1}{2}\,p(p+1)\,\theta(p^k) = (\tfrac{1}{2}\,p(p+1))^{k+1}.$$

This completes the proof.

By repeated application of these corollaries we are able to give an explicit expression for $\theta(n)$. This we do in the next corollary.

COROLLARY 4. *If* $n = a_0 + a_1p + \ldots + a_kp^k$, $0 \leqslant a_i \leqslant p-1$ *then*

$$\theta(n) = \tfrac{1}{2}\sum_{i=0}^{k} a_i((a_i+1)\ldots(a_k+1))\,(\tfrac{1}{2}\,p(p+1))^i.$$

Theorem 1 and its corollaries determine the $\theta_j(n)$, $1 \leqslant j \leqslant n$, as solutions of a system of linear difference equations with constant coefficients. The quantity

$$\theta_0(n) = \tfrac{1}{2}n(n+1) - \theta(n).$$

In general the calculations needed to compute explicitly the $\theta_j(n)$ are prohibitive. However we perform some calculations in this direction in the next section.

4. $\theta_j(p^k)$ **for** $p = 3, 5$. The simplest case to deal with is $p = 2$. In this case we can compute $\theta_j(n)$ for arbitrary n. The details will be given in the next section where some other aspects of our results for $p = 2$ are discussed.

When $p = 3$, since $(j\bar{q})q \equiv j \pmod 3$, we have

$$1\,\bar{1} \equiv 2\bar{2} \equiv 1,\; 1\bar{2} \equiv 2\bar{1} \equiv 2 \qquad \pmod 3.$$

https://doi.org/10.4153/CJM-1957-043-6 Published online by Cambridge University Press

By direct examination we find $\theta_1(3) = 5$, $\theta_2(3) = 1$. We now obtain from Cor. 3(a) of Theorem 1 the following pair of simultaneous difference equations

$$\theta_1(3^k) - 5\,\theta_1(3^{k-1}) - \theta_2(3^{k-1}) = 0,$$
$$\theta_2(3^k) - \theta_1(3^{k-1}) - 5\theta_2(3^{k-1}) = 0.$$

Solving these equations using the empirical initial conditions

$$\theta_1(1) = \theta_2(3) = 1,\ \theta_1(3) = 5,\ \theta_2(1) = 0$$

we obtain

$$\theta_1(3^k) = \tfrac{1}{2}\,(6^k + 4^k),\ \theta_2(3^k) = \tfrac{1}{2}(6^k - 4^k).$$

From these it follows that

$$\theta_0(3^k) = \tfrac{1}{2}\,3^k(3^k + 1) - 6^k.$$

In a similar way with $p = 5$ we find a system of four linear difference equations in four unknowns. Using the suitable initial conditions we obtain:

$$\begin{aligned}
\theta_1(5^k) &= \tfrac{1}{4}(15^k + 9^k + (8 - i)^k + (8 + i)^k),\\
\theta_2(5^k) &= \tfrac{1}{4}(15^k - 9^k - i(8 - i)^k + i(8 + i)^k),\\
\theta_3(5^k) &= \tfrac{1}{4}(15^k - 9^k + i(8 - i)^k - i(8 + i)^k),\\
\theta_4(5^k) &= \tfrac{1}{4}(15^k + 9^k - (8 - i)^k - (8 + i)^k).
\end{aligned}$$

From these it follows that

$$\theta_0(5^k) = \tfrac{1}{2}\,5^k(5^k + 1) - 15^k.$$

5. The case $p = 2$. In the case $p = 2$, Cor. 4 of Theorem 1 reads as follows:
(1) If $n = 2^{\alpha_1} + \ldots + 2^{\alpha_r}$, $\alpha_1 > \ldots > \alpha_r$, then

$$\theta(n) = \sum_{i=1}^{r} 2^{i-1} \cdot 3^{\alpha_i}.$$

Since every n is of one of the three forms:

(i) $2^{\alpha_1} + \ldots + 2^{\alpha_r}$ with $\alpha_1 > \ldots > \alpha_r > 0$;
(ii) $2^{\alpha_1} + \ldots + 2^{\alpha_r} + 2^s + 2^{s-1} + \ldots + 2 + 1$ with $\alpha_1 > \ldots > \alpha_r > s+1$;
(iii) $2^s + 2^{s-1} + \ldots + 2 + 1$

we can use (1) to compute $\theta(n + 1) - \theta(n)$ finding its values in the three cases to be 2^r, 2^{s+r}, 2^{s+1} respectively. Hence we have the result:

(2) the number of odd $\binom{n}{m}$ for fixed n and $0 \leqslant m \leqslant n$ is equal to 2^s where s is the number of non-zero digits in the binary expansion of n.

This result was proved by Glaisher **(2)** from our Lemma 1. From this we have the special result, which can be proved in a very nice way directly **(3**, p. 15 problem 12 and the solution pp. 97-98**)**, that the nth row of Pascal's triangle consists of odd numbers exclusively if and only if n is a power of 2. This special case is also an immediate consequence of the corollary to Lemma 3.

If we let $\theta_n = \theta_1(n+1) - \theta_1(n)$ and $E_n = \theta_0(n+1) - \theta_0(n)$ we have the result:

(3) $E_n < \theta_n$ if and only if $n + 1 < 2^{1+s}$ where s is the number of non-zero digits in the binary expansion of n. In all other cases $E_n > \theta_n$.

The first statement in (3) follows from (2) since $E_n - \theta_n = n + 1 - 2^s$. In order to prove the second part of (3) suppose the contrary. That is, suppose $E_n = \theta_n$ for some n. Then by (2), $n + 1 = 2^{1+s}$ or $n = 2^s + \ldots + 1$. But then the number of non-zero digits in the binary expansion of n is $s + 1$. This is a contradiction and therefore $E_n \neq \theta_n$ for all n.

We include one other result whose proof we omit.

(4) $\theta_1(n) > \theta_0(n)$ if and only if $1 \leqslant n \leqslant 18$.

6. "Most binomial coefficients are divisible by a given prime".

In this section we prove the

THEOREM 2.

$$\lim_{n\to\infty} \theta(n)/\theta_0(n) = 0.$$

Proof. Clearly $\theta(n)$ and $\theta_0(n)$ are non-decreasing functions of n. Hence if $p^k \leqslant n < p^{k+1}$ then, using Cor. 3(b) of Theorem 1,

$$\theta(n)/\theta_0(n) \leqslant \theta(p^{k+1})/\theta_0(p^k)$$
$$= \binom{p+1}{2}^{k+1}\left\{\binom{p^k+1}{2} - \binom{p+1}{2}^k\right\}^{-1} = p(p+1)\left\{\left(\frac{2p}{p+1}\right)^k + \left(\frac{2}{p+1}\right)^k - 2\right\}^{-1},$$

and this tends to 0 as $n \to \infty$.

REFERENCES

1. L. E. Dickson, *History of the Theory of Numbers*, vol. 1 (Chelsea, New York, 1952).
2. J. W. L. Glaisher, *On the residue of a binomial theorem coeffcient with respect to a prime modulus*, Quart. J. Math., *30* (1899), 150–156.
3. I. M. Vinogradoff, *An Introduction to the Theory of Numbers*, (London and New York, Pergamon Press, 1955).

Wesleyan University,
Middletown, Conn.

and

Reed College
Portland, Oregon.

https://doi.org/10.4153/CJM-1957-043-6 Published online by Cambridge University Press