ON PASCAL'S TRIANGLE MODULO $p^2$

BY

JAMES G. HUARD (BUFFALO, N.Y.),
BLAIR K. SPEARMAN (KELOWNA, B.C.),
AND KENNETH S. WILLIAMS (OTTAWA, ONT.)

1. Introduction. Let $n$ be a nonnegative integer. The $n$th row of Pascal's triangle consists of the $n + 1$ binomial coefficients

$$\binom{n}{0} \binom{n}{1} \binom{n}{2} \cdots \binom{n}{n}.$$ 

We denote by $N_n(t,m)$ the number of these binomial coefficients which are congruent to $t$ modulo $m$, where $t$ and $m$ ($\geq 1$) are integers.

If $p$ is a prime we write the $p$-ary representation of the positive integer $n$ as

$$n = a_0 + a_1p + a_2p^2 + \ldots + a_kp^k,$$

where $k \geq 0$, each $a_i = 0, 1, \ldots, p - 1$ and $a_k \neq 0$. We denote the number of $r$'s occurring among $a_0, a_1, \ldots, a_k$ by $n_r$ ($r = 0, 1, \ldots, p - 1$). We set $\omega = e^{2\pi i/(p-1)}$ and let $g$ denote a primitive root (mod $p$). We denote the index of the integer $t \equiv 0$ (mod $p$) with respect to $g$ by \(\text{ind}_g t\); that is, \(\text{ind}_g t\) is the unique integer $j$ such that $t \equiv g^j$ (mod $p$). Hexel and Sachs [2, Theorem 3] have shown in a different form that for $t = 1, 2, \ldots, p - 1$,

$$N_n(t,p) = \frac{1}{p - 1} \sum_{s=0}^{p-2} \omega^{-s \text{ind}_g t} \prod_{r=1}^{p-1} B(r, s)^{n_r},$$

where for any integer $r$ not exceeding $p - 1$ and any integer $s$,

$$B(r, s) = \sum_{c=0}^{r} \omega^{s \text{ind}_g (c)}. $$

In this paper we make use of the Hexel–Sachs formula (1.1) to determine the analogous formula for $N_n(tp,p^2)$ for $t = 1, 2, \ldots, p - 1$. We prove
THEOREM 1.1. For \( t = 1, 2, \ldots, p - 1 \),

\[
N_n(tp, p^2) = \frac{1}{p - 1} \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} n_{ij} \sum_{s=0}^{p-2} \omega^{-s(\text{ind}_p t + \text{ind}_p (i+1) - \text{ind}_p j)} \\
\times B(p - 2 - i, -s)B(j - 1, s) \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r-i) - \delta(r-j)},
\]

where

\[
\delta(x) = \begin{cases} 
1 & \text{if } x = 0, \\
0 & \text{if } x \neq 0,
\end{cases}
\]

and \( n_{ij} \) denotes the number of occurrences of the pair \( ., \) in the string \( a_0 a_1 \ldots a_k \).

The proof of this theorem is given in §3 after a preliminary result is proved in §2. We consider the special cases \( p = 2 \) and \( p = 3 \) of the theorem in §4 and §5 respectively.

The proof of (1.1) given by Hexel and Sachs [2] is quite long so we conclude this introduction by giving a short proof of their result.

Proof of (1.1). For \( t = 1, 2, \ldots, p - 1 \) we have

\[
N_n(t, p) = \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv t \pmod{p}} = \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv t \pmod{p}} = \sum_{r=0}^{p-1} \frac{1}{\binom{n}{r} \equiv t \pmod{p}} \\
= \frac{1}{p - 1} \sum_{r=0}^{n} \sum_{s=0}^{p-2} \omega^{s(\text{ind}_p (\binom{n}{r}) - \text{ind}_p t)} \\
= \frac{1}{p - 1} \sum_{s=0}^{p-2} \omega^{-s \text{ind}_p t} \sum_{r=0}^{n} \omega^{s \text{ind}_p (\binom{n}{r})}. 
\]

It remains to show that

\[
\sum_{r=0}^{n} \omega^{s \text{ind}_p (\binom{n}{r})} = \prod_{r=1}^{p-1} B(r, s)^{n_r}. 
\]

We express \( r \) \((0 \leq r \leq n)\) in base \( p \) as

\[ r = b_0 + b_1 p + \ldots + b_k p^k, \]

where each \( b_i = 0, 1, \ldots, p - 1 \). By Lucas' theorem [5, p. 52], we have

\[
\binom{n}{r} \equiv \binom{a_0}{b_0} \binom{a_1}{b_1} \ldots \binom{a_k}{b_k} \pmod{p}. 
\]
If \( p \mid \binom{n}{r} \), we have \( p \mid \binom{a_i}{b_i} \) (\( i = 0, 1, \ldots, k \)) so that \( b_i \leq a_i \) (\( i = 0, 1, \ldots, k \)). Conversely, if \( b_i \leq a_i \) (\( i = 0, 1, \ldots, k \)) then \( p \mid \binom{a_i}{b_i} \) (\( i = 0, 1, \ldots, k \)) so that \( p \mid \binom{n}{r} \). Hence

\[
\sum_{r=0}^{n} \omega \cdot \text{ind}_p \left( \binom{n}{r} \right) = \sum_{b_0, \ldots, b_k = 0}^{a_0, \ldots, a_k} \omega \cdot \sum_{i=0}^{k} \text{ind}_p \left( \binom{a_i}{b_i} \right)
\]

\[
= \prod_{i=0}^{k} \left\{ \sum_{b_i = 0}^{a_i} \omega \cdot \text{ind}_p \left( \binom{a_i}{b_i} \right) \right\} = \prod_{i=0}^{k} \prod_{r=0}^{p-1} \left\{ \sum_{b_i = 0}^{a_i} \omega \cdot \text{ind}_p \left( \binom{r}{b_i} \right) \right\}
\]

\[
= \prod_{r=0}^{p-1} \left\{ \sum_{b_i = 0}^{r} \omega \cdot \text{ind}_p \left( \binom{r}{b_i} \right) \right\}^{n_r} = \prod_{r=0}^{p-1} B(r, s)^{n_r}.
\]

As \( B(0, s) = 1 \) the term \( r = 0 \) contributes 1 to the product.

### 2. A preliminary result.

We begin by recalling Wilson’s theorem in the form

\[
h!(p - h - 1)! \equiv (-1)^{h+1} \pmod{p} \quad (h = 0, 1, \ldots, p - 1).
\]

We make use of (2.1) in the proof of the following result.

**Lemma 2.1.** Let \( p \) be a prime and let \( g \) be a primitive root of \( p \). Set \( \omega = e^{2\pi i/(p-1)} \). Let \( s \) be an integer. Then

(i) \[
\sum_{b=0}^{a-1} \omega \cdot \text{ind}_p \left( bl(a-1-b)!/a! \right) = \omega^{-s} \cdot \text{ind}_p a \cdot B(a - 1, -s)
\]

for \( a = 1, 2, \ldots, p - 1 \), and

(ii) \[
\sum_{b=0}^{p-1} \omega \cdot \text{ind}_p \left( bl(a+p-b)!/a! \right) = \omega^s \cdot \text{ind}_p (-1) \omega^s \cdot \text{ind}_p (a+1) \cdot B(p - a - 2, s)
\]

for \( a = 0, 1, 2, \ldots, p - 2 \).

**Proof.** (i) We have

\[
\sum_{b=0}^{a-1} \omega \cdot \text{ind}_p \left( bl(a-1-b)!/a! \right) = \omega^{-s} \cdot \text{ind}_p a \sum_{b=0}^{a-1} \omega^s \cdot \text{ind}_p \left( bl(a-1-b)!/(a-1)! \right)
\]

\[
= \omega^{-s} \cdot \text{ind}_p a \sum_{b=0}^{a-1} \omega^{-s} \cdot \text{ind}_p \left( ((a-1)!/(bl(a-1-b)!)) \right)
\]

\[
= \omega^{-s} \cdot \text{ind}_p a \sum_{b=0}^{a-1} \omega^{-s} \cdot \text{ind}_p \left( \frac{a-1}{b-1} \right)
\]

\[
= \omega^{-s} \cdot \text{ind}_p a \cdot B(a - 1, -s).
\]
(ii) By Wilson's theorem (2.1), we have for \( b = a + 1, \ldots, p - 1 \),
\[
\frac{b!(a + p - b)!}{a!} \equiv \frac{(-1)^{b+1}}{(p - b - 1)!} \cdot \frac{(-1)^{a+p-b+1}}{(b - a - 1)!} \cdot \frac{(p - a - 1)!}{(-1)^{a+1}}
\equiv (p - a - 1) \left(\frac{p - a - 2}{b - a - 1}\right) \pmod{p},
\]
as \( 1 \equiv (-1)^{p+1} \pmod{p} \). Thus we have

\[
\sum_{b=a+1}^{p-1} \omega_s \text{ind}_g(b!(a + p - b)!/a!) = \sum_{b=a+1}^{p-1} \omega_s \text{ind}_g((p - a - 1)(p - a - 2))
= \sum_{l=0}^{p-a-2} \omega_s \text{ind}_g((p - a - 1)(p - a - 2))
= \omega_s \text{ind}_g(p - a - 1) \sum_{l=0}^{p-a-2} \omega_s \text{ind}_g(p - a - 2)
= \omega_s \text{ind}_g(-a - 1) B(p - a - 2, s).
\]
The asserted result now follows as

\[
\omega_s \text{ind}_g(-a - 1) = \omega_s \text{ind}_g(-1) + s \text{ind}_g(a + 1).
\]

Remark. We adopt the convention that (i) holds when \( a = 0 \) and (ii) holds when \( a = p - 1 \) as \( B(-1, \pm s) = 0 \).

3. Proof of the theorem. Let \( n \) be a fixed positive integer. Let

\[
n = \sum_{j=0}^{k} a_j p^j
\]
be the \( p \)-ary representation of \( n \) so that \( k, a_0, \ldots, a_k \) are fixed integers satisfying

\[
k \geq 0, \quad 0 \leq a_j \leq p - 1 \quad (j = 0, 1, \ldots, k), \quad a_k \neq 0.
\]

Let \( r \) denote an arbitrary integer between 0 and \( n \). We express \( r \) and \( n - r \) in base \( p \) as follows:

\[
r = \sum_{j=0}^{k} b_j p^j, \quad n - r = \sum_{j=0}^{k} c_j p^j,
\]
where each \( b_j \) and \( c_j \) is one of the integers \( 0, 1, \ldots, p - 1 \). Let \( c(n, r) \) denote the number of carries when \( r \) is added to \( n - r \) in base \( p \). Kazandzidis
[4, pp. 3-4] (see also Singmaster [6]) has shown that

\begin{equation}
\binom{n}{r} \equiv (-p)^{c(n,r)} \prod_{j=0}^{k} \frac{a_j!}{b_j!c_j!} \pmod{p^{c(n,r)+1}}.
\end{equation}

If \(c(n,r) = 0\) then \(b_j + c_j = a_j\) for \(j = 0, 1, \ldots, k\). Conversely, if \(b_j + c_j = a_j\) for \(j = 0, 1, \ldots, k\), then \(c(n,r) = 0\). Hence, for \(t = 1, 2, \ldots, p-1\), we have

\begin{equation}
\binom{n}{r} \equiv t \pmod{p}
\end{equation}

\(\Leftrightarrow b_j + c_j = a_j\) (\(j = 0, 1, \ldots, k\)) and \(\prod_{j=0}^{k} \frac{a_j!}{b_j!c_j!} \equiv t \pmod{p}\).

Thus

\begin{equation}
N_n(t, p) = \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv t \pmod{p}}
= \sum_{r=0}^{p-1} 1.
\end{equation}

Suppose now that \(c(n,r) = 1\). If the unique carry occurs in the \(j\)th place \((0 \leq j \leq k - 1)\), then, for \(i = 0, 1, \ldots, k\), the pair \((b_i, c_i)\) satisfies

\begin{equation}
b_i + c_i = \begin{cases} a_i & \text{if } i \neq j, j + 1, \\ a_j + p & \text{if } i = j, \\ a_{j+1} - 1 & \text{if } i = j + 1. \end{cases}
\end{equation}

Conversely, if each pair \((b_i, c_i)\) satisfies (3.7) then \(c(n,r) = 1\), and the carry occurs in the \(j\)th place. By Kazandzidis' theorem (3.4) we have

\begin{equation}
\binom{n}{r} \equiv tp \pmod{p^2} \Leftrightarrow c(n,r) = 1 \text{ and } \prod_{t=0}^{k} \frac{a_t!}{b_t!c_t!} \equiv -t \pmod{p}.
\end{equation}

As

\begin{equation}
N_n(tp, p^2) = \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{p-1} \frac{1}{\prod_{t=0}^{k} \frac{a_t!}{b_t!c_t!} \equiv -t \pmod{p}}
= \sum_{r=0}^{p-1} \frac{1}{\prod_{t=0}^{k} \frac{a_t!}{b_t!c_t!} \equiv -t \pmod{p}}
= \sum_{r=0}^{p-1} \frac{1}{\prod_{t=0}^{k} \frac{a_t!}{b_t!c_t!} \equiv -t \pmod{p}}
= \sum_{r=0}^{p-1} \frac{1}{\prod_{t=0}^{k} \frac{a_t!}{b_t!c_t!} \equiv -t \pmod{p}}
\end{equation}

appealing to (3.8), we obtain

\begin{equation}
N_n(tp, p^2) = \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{k-1} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
= \sum_{r=0}^{n} \frac{1}{\binom{n}{r} \equiv tp \pmod{p^2}}
\end{equation}

Appealing to (3.1), (3.3) and (3.7), we deduce that
\[ N_n(tp, p^2) = \sum_{j=0}^{k-1} \sum_{l=0}^{p-1} \frac{b_j + c_j}{b_j + c_j = a_j + p} \frac{b_{j+1} + c_{j+1}}{b_{j+1} + c_{j+1} = a_{j+1} - 1} 1, \]

where the product is over \( l = 0, \ldots, j - 1, j + 2, \ldots, k. \) Next, appealing to (3.6), we see that the inner sum is

\[ N_{n-a_jp^j-a_{j+1}p^{j+1}} \left( \frac{-tb_j!c_j!b_{j+1}!c_{j+1}!}{a_j!a_{j+1}!}, p \right), \]

where the quotient is taken as an integer modulo \( p. \) Then

\[ N_n(tp, p^2) = \sum_{j=0}^{k-1} \sum_{l=0}^{p-1} N_{n-a_jp^j-a_{j+1}p^{j+1}} \left( \frac{-tb_j!c_j!b_{j+1}!c_{j+1}!}{a_j!a_{j+1}!}, p \right) \]

where

\[ K_j = N_{n-a_jp^j-a_{j+1}p^{j+1}} \left( \frac{-tb_j!(a_j + p - b_j)!b_{j+1}!(a_{j+1} - 1 - b_{j+1})!}{a_j!a_{j+1}!}, p \right). \]

The next step is to apply Hexel and Sachs' theorem (see (1.1)) to \( n - a_jp^j - a_{j+1}p^{j+1}. \) The number of \( r \)'s in the \( p \)-ary representation of \( n - a_jp^j - a_{j+1}p^{j+1} \) is \( n_r - \delta(r - a_j) - \delta(r - a_{j+1}). \) Hence

\[ K_j = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^s \text{ind}_g(-tb_j!(a_j + p - b_j)!b_{j+1}!(a_{j+1} - 1 - b_{j+1})!/(a_j!a_{j+1}!)) \]

\[ \times \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r - a_j) - \delta(r - a_{j+1})}. \]

Thus

\[ N_n(tp, p^2) = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^s \text{ind}_g(-t) \sum_{j=0}^{k-1} \left\{ \sum_{b_j = a_j + 1}^{a_{j+1} - 1} \omega^s \text{ind}_g(b_j!(a_j + p - b_j)!/a_j!) \right\} \]

\[ \times \left\{ \sum_{b_{j+1} = 0}^{a_{j+1} - 1} \omega^s \text{ind}_g(b_{j+1}!(a_{j+1} - 1 - b_{j+1})!/a_{j+1}!) \right\} \]

\[ \times \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r - a_j) - \delta(r - a_{j+1})}. \]
Appealing to Lemma 2.1, we obtain

\[ N_n(tp, p^2) = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^{-s \text{ind}_p(-1)} \omega^{-s \text{ind}_p t} \times \sum_{j=0}^{k-1} \{ \omega^{-s \text{ind}_p(-1)} \omega^{-s \text{ind}_p(a_j+1)} B(p - a_j - 2, -s) \} \]

\[ \times \{ \omega^{s \text{ind}_p(a_j+1)} B(a_j+1 - 1, s) \} \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r-a_j - \delta(r-a_{j+1})} \]

\[ = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^{-s \text{ind}_p t} \sum_{j=0}^{k-1} \omega^{s(\text{ind}_p a_j+1 - \text{ind}_p(a_j+1))} \]

\[ \times B(p - a_j - 2, -s) B(a_j+1 - 1, s) \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r-a_j - \delta(r-a_{j+1})} \]

\[ = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^{-s \text{ind}_p t} \sum_{u=0}^{p-2} \sum_{v=1}^{p-1} \sum_{j=0}^{k-1} \omega^{s(\text{ind}_p v - \text{ind}_p(u+1))} \]

\[ \times B(p - u - 2, -s) B(v - 1, s) \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r-u) - \delta(r-v)} \]

\[ = \frac{1}{p-1} \sum_{u=0}^{p-2} \sum_{v=1}^{p-1} n_{uv} \sum_{s=0}^{p-2} \omega^{-s(\text{ind}_p t + \text{ind}_p(u+1) - \text{ind}_p v)} \]

\[ \times B(p - 2 - u, -s) B(v - 1, s) \prod_{r=1}^{p-1} B(r, s)^{n_r - \delta(r-u) - \delta(r-v)} . \]

4. **Case** \( p = 2 \). Here \( \omega = 1 \) and \( g = 1 \). From (1.2) we obtain

\[ B(0, s) = 1, \quad B(1, s) = 2. \]

Taking \( p = 2 \) and \( t = 1 \) in the theorem, we deduce that

\[ N_n(2, 4) = n_{01} B(0, 0)^2 B(1, 0)^{n_1 - 1} = n_{01} 2^{n_1 - 1}. \]

This result is due to Davis and Webb [1, Theorem 7].
5. Case $p = 3$. Here $\omega = -1$ and $g = 2$. From (1.2) we have

$$B(0, s) = 1, \quad B(1, s) = 2, \quad B(2, s) = 2 + (-1)^s.$$ 

Taking $p = 3$ and $t = 1, 2$ in the theorem, we obtain

$$N_n(3t, 9) = n_{01}(2^{n_1-1}3^{n_2} - (-1)^t2^{n_1-1}) + n_{02}(2^{n_1+1}3^{n_2-1} + (-1)^t2^{n_1+1}) + n_{11}(2^{n_1-3}3^{n_2} + (-1)^t2^{n_1-3}) + n_{12}(2^{n_1-1}3^{n_2-1} - (-1)^t2^{n_1-1}).$$

This result is due to Huard, Spearman and Williams [3].

6. Concluding remarks. As

$$\sum_{t=1}^{p-1} \omega^{-s \text{ind}_t} = \begin{cases} p - 1 & \text{if } s = 0, \\ 0 & \text{if } s \neq 0, \end{cases}$$

and

$$B(r, 0) = r + 1,$$

summing (1.1) and (1.3) over $t = 1, 2, \ldots, p - 1$, we obtain

$$n + 1 - N_n(0, p) = \sum_{t=1}^{p-1} N_n(t, p) = \prod_{r=1}^{p-1} (r + 1)^{n_r},$$

and

$$N_n(0, p) - N_n(0, p^2) = \sum_{i=1}^{p-1} N_n(tp, p^2)$$

$$= \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} n_{ij}(p - 1 - i) j \prod_{r=1}^{p-1} (r + 1)^{n_r-\delta(r-i)-\delta(r-j)},$$

so that

$$(6.1) \quad N_n(0, p^2) = n + 1 - \prod_{r=1}^{p-1} (r + 1)^{n_r} - \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} n_{ij}(p - 1 - i) j \prod_{r=1}^{p-1} (r + 1)^{n_r-\delta(r-i)-\delta(r-j)}.$$

We conclude this paper by observing that our theorem shows that $N_n(tp, p^2)$ ($p \uparrow t$) depends only on $t$, $n_i$ ($i = 1, 2, \ldots, p - 1$) and $n_{ij}$ ($i = 0, 1, \ldots, p - 2; j = 1, 2, \ldots, p - 1$). This result should be compared to that of Webb [7, Theorem 3] for $N_n(t, p^2)$ ($p \uparrow t$).
REFERENCES


Department of Mathematics
Canisius College
Buffalo, New York 14208
U.S.A.
E-mail: huard@canisius.edu

Department of Mathematics and Statistics
Okanagan University College
Kelowna, British Columbia
Canada V1V 1V7
E-mail: bkspearm@okanagan.bc.ca

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
E-mail: williams@math.carleton.ca

Received 27 June 1996;
revised 2 January 1997