ELEMENTARY PROOF OF CONGRUENCES INVOLVING SUM OF BINOMIAL COEFFICIENTS

MOA APAGODU

To Olyad Apagodu

ABSTRACT. We provide elementary proof of several congruences involving single sum and multisums of binomial coefficients.

INTRODUCTION: We consider congruence of the form:

\[ \left( \sum_{k=0}^{r^{p^a}-1} b(n + d) \right) \mod p, \]

where \( b(n) \) is a combinatorial sequence, mainly binomial coefficients, \( d \in \{0, 1, 2, 3, \ldots, p^a\} \), \( a \in \{0, 1, 2, 3, \ldots\} \), \( r \) is a specific positive integer, and \( p \) is an arbitrary prime. The case \( a = 1 \) and single sum and single variable is covered in [3] and later extended to multisums and multivariables in [1]. This article generalizes the results in [1, 3] where the upper limit of summation is replaced by \( r p^a - 1 \).

The main “trick” in [1, 3] is The Freshman’s Dream Identity: \( (x + y)^p = x^p + y^p \). In this article we use the same trick in the form \( (x + y)^{p^a} = x^{p^a} + y^{p^a} \). The proof follows from induction on \( a \) and the case \( a = 1 \). The second ingredient is Sum of a Geometric Series: \[ \sum_{i=0}^{n-1} z^i = \frac{z^n - 1}{z - 1}. \]

NOTATION: Let \( x \equiv y \mod p \) mean \( x \equiv y \) (mod \( p \)), in other words, that \( x - y \) is divisible by \( p \).

The constant term of a Laurent polynomial \( P(x_1, x_2, \ldots, x_n) \), alias the coefficient of \( x_1^0 x_2^0 \ldots x_n^0 \), is denoted by \( CT[P(x_1, x_2, \ldots, x_n)] \). The general coefficient of \( x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} \) in \( P(x_1, x_2, \ldots, x_n) \) is denoted by

\[ [x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}] P(x_1, x_2, \ldots, x_n). \]

Example 1.

\[ CT \left[ \frac{1}{xy} + 3 + 5xy - x^3 + 6y^2 \right] = 3, \quad [xy] \left[ \frac{1}{xy} + 3 + 5xy + x^3 + 6y^2 \right] = 5. \]

We use the symmetric representation of integers in \( \left( -\frac{p}{2}, \frac{p}{2} \right] \) when reducing modulo a prime \( p \).

Example 2. 6 (mod 5) = 1 and 4 (mod 5) = -1.
We start by providing an elementary proof of, as advertised in the title, a result in [7], where a complicated method is used to prove.

**Proposition 1** [7, Remark 1.2] For any prime \( p \) and \( d \in \{0, 1, 2, 3, \ldots, p^a\} \), we have

\[
\sum_{n=0}^{p^a-1} \binom{2n}{n + d} \equiv_p \begin{cases} 
1, & \text{if } (p \equiv_3 2, d \equiv_3 1, a \text{ is odd}) \lor (p \equiv_3 1 \text{ and } d \equiv_3 0) \lor (p \equiv_3 2, d \equiv_3 0, a \text{ is odd}) \\
-1, & \text{if } (p \equiv_3 2, d \equiv_3 0, a \text{ is odd}) \lor (p \equiv_3 1 \text{ and } d \equiv_3 2) \lor (p \equiv_3 2, d \equiv_3 2, a \text{ is even}) \\
0, & \text{otherwise.}
\end{cases}
\]

**Proof.**

\[
\sum_{n=0}^{p^a-1} \binom{2n}{n + d} = \sum_{n=0}^{p^a-1} CT \left[ \frac{(1+x)^{2n}}{x^{n+d}} \right] = \sum_{n=0}^{p^a-1} CT \left[ \frac{(2+x+\frac{1}{x})^n}{x^n} \right] = \sum_{n=0}^{p^a-1} CT \left[ \frac{2^n + x^n + \frac{1}{x^n} - 1}{1+x+\frac{1}{x}} \times \frac{1}{x^d} \right]
\]

\[
\equiv_p CT \left[ \frac{2^n + x^n + \frac{1}{x^n} - 1}{1+x+\frac{1}{x}} \times \frac{1}{x^d} \right]
\]

\[
= CT \left[ \frac{1+1}{x} + \frac{1}{x^d} \right]
\]

\[
= \binom{2^a+d}{1} \left[ \sum_{i=0}^{\infty} x^{3i+1} + \sum_{i=0}^{\infty} (-1) \cdot x^{3i+2} \right] + [x^d] \left[ \sum_{i=0}^{\infty} x^{3i+1} + \sum_{i=0}^{\infty} (-1) \cdot x^{3i+2} \right].
\]

The result follows from extracting the coefficients of \( x^{p^a+d} \) and \( x^d \) in the above geometric series.

For example, when \( p \equiv 2(\text{mod } 3) \), \( d \equiv 2(\text{mod } 3) \) \text{ and } a \text{ is even}, then \( \equiv_3 2 \equiv_3 0 \text{ (mod } 3) \) and the contribution from the first sum is zero. The only contribution is from the second sum, which is \(-1\).

\[ \square \]

Now we state and proof some of the results in [8] when the upper limit of summation is \( rp^a - 1 \).

**Proposition 1’.** For any prime \( p \) and \( d \in \{0, 1, 2, 3, 4, 5, \ldots, p^a\} \), we have

\[
\sum_{n=0}^{2p^a-1} \binom{2n}{n + d} \equiv_p \begin{cases} 
1, & \text{if } p \equiv_3 1 \text{ and } d \equiv_3 1 \\
-4, & \text{if } p \equiv_3 1 \text{ and } d \equiv_3 2 \\
4, & \text{if } p \equiv_3 2 \text{ and } d \equiv_3 1 \\
-1, & \text{if } p \equiv_3 2 \text{ and } d \equiv_3 2 \\
3, & \text{if } p \equiv_3 1 \text{ and } d \equiv_3 0 \\
-3, & \text{if } p \equiv_3 2 \text{ and } d \equiv_3 0
\end{cases}
\]

**Proof.**

\[
\sum_{n=0}^{2p^a-1} \binom{2n}{n} = \sum_{n=0}^{2p^a-1} CT \left[ \frac{(2+x+\frac{1}{x})^n}{x^n} \right] = \sum_{n=0}^{2p^a-1} CT \left[ \frac{(2+x+\frac{1}{x})^{p^a-1}}{x^{p^a}} \right]
\]

\[
\equiv_p CT \left[ \frac{(6+4x+\frac{1}{x}+x^2+\frac{1}{x^2})^{p^a-1}}{2+x+\frac{1}{x}} \times \frac{1}{x^d} \right]
\]
The same method can be used to find the “mod” result follows from extracting the coefficients of other ones, and simplifying, we get that this equals

\[
\begin{align*}
\left[ x^{2p^n} + d - 1 \right] & \left[ \frac{1 + 4x^{p^n} + 5x^{2p^n}}{1 + x + x^2} \right] = \left[ x^{2p^n} + d - 1 \right] \left[ \frac{1}{1 + x + x^2} \right] + 4 \cdot \left[ x^{p^n} + d - 1 \right] \left[ \frac{1}{1 + x + x^2} \right] \\
& + 4 \cdot \left[ x^{2p^n} + d - 1 \right] \left[ \frac{1}{1 + x + x^2} \right] \\
& = \left[ x^{2p^n} + d \right] \left[ \sum_{i=0}^{\infty} x^{3i+1} \right] + \left[ x^{2p^n} + d \right] \left[ \sum_{i=0}^{\infty} (-1) \cdot x^{3i+2} \right] + 4 \cdot \left[ x^{p^n} + d \right] \left[ \sum_{i=0}^{\infty} x^{3i+1} \right] + \\
& 4 \cdot \left[ x^{p^n} + d \right] \left[ \sum_{i=0}^{\infty} (-1) \cdot x^{3i+2} \right] + 5 \left[ x^d \right] \left[ \sum_{i=0}^{\infty} x^{3i+1} \right] + 5 \left[ x^d \right] \left[ \sum_{i=0}^{\infty} (-1) \cdot x^{3i+2} \right].
\end{align*}
\]

The result follows from extracting the coefficients of \( x^{p^n + d} \) and \( x^d \) as in Proposition 2. \( \square \)

The same method can be used to find the “mod” \( p \) of \( \sum_{n=0}^{p^n-1} \binom{2n}{n+d} \) for any specific \( r \).

Next we consider the Catalan numbers, \( C_n = \frac{1}{n+1} \binom{2n}{n} \).

**Proposition 2.** Let \( C_n \) denote the \( n \)th Catalan number. Then, for any \( p > 3 \), we have

\[
\sum_{n=0}^{p^n-1} C_n \equiv_p \begin{cases} 
1, & \text{if } p \equiv 1 \pmod{3} \text{ or } p \equiv 2 \pmod{3} \text{ and } a \text{ is even} \\
-2, & \text{if } p \equiv 2 \pmod{3} \text{ and } a \text{ is odd}
\end{cases}
\]

**Proof.** Since \( C_n = \binom{2n}{n} - \binom{2n}{n-1} \), it is readily seen that

\[
C_n = CT \left[ (1 - x) \left( 2 + x + \frac{1}{x} \right)^n \right].
\]

We have

\[
\sum_{n=0}^{p^n-1} C_n = \sum_{n=0}^{p^n-1} CT \left[ (1 - x) \left( 2 + x + \frac{1}{x} \right)^n \right] = CT \left[ (1 - x) \left( \frac{(2 + x + \frac{1}{x})^n - 1}{2 + x + \frac{1}{x} - 1} \right) \right] \\
\equiv_p CT \left[ \frac{(1 - x) \left( (2 + x^{p^n} + \frac{1}{x}) - 1 \right)}{2 + x + \frac{1}{x} - 1} \right] \text{ (By freshman’s dream).}
\]

Since only the term \( \frac{1}{x} \) in the numerator contributes to the constant term, this equals

\[
\left[ x^{p^n-1} \right] \left[ \frac{1 - x}{1 + x + x^2} \right] = \left[ x^{p^n-1} \right] \left[ \frac{(1 - x)^2}{1 - x^3} \right]
\]
Proof. Since Proposition \(2\) and the result follows from extracting the coefficients of \(x\), we have

\[
[x^n] \frac{x}{1 - x^3} + [x^n] \frac{-2x^2}{1 - x^3} + [x^n] \frac{x^3}{1 - x^3}
\]

\[
= [x^n] \left[ \sum_{i=0}^{\infty} 1 \cdot x^{3i+1} \right] + [x^n] \left[ \sum_{i=0}^{\infty} (-2) \cdot x^{3i+2} \right] + [x^n] \left[ \sum_{i=0}^{\infty} 1 \cdot x^{3i+3} \right],
\]

and the result follows from extracting the coefficient of \(x^n\) from the first or second geometric series above. (Note that we would never have to use the third geometric series, since \(p > 3\).) \(\square\)

Proposition 2'. Let \(C_n\) denote the \(n\)th Catalan number. Then, for every prime \(p\),

\[
\sum_{n=0}^{2p-1} C_n 
\]

\[
\equiv_p \begin{cases} 
-7, & \text{if } p \equiv 2(\text{mod } 3) \text{ and } a \text{ is even} \\
2, & \text{if } p \equiv 1(\text{mod } 3) \text{ or } p \equiv 2(\text{mod } 3) \text{ and } a \text{ is odd}.
\end{cases}
\]

Proof. Since \(C_n = \binom{2n}{n} - \binom{2n}{n-1}\), it is readily seen that

\[
C_n = CT \left(1 - x \right) \left(2 + x + \frac{1}{x}\right)^n.
\]

We have

\[
\sum_{n=0}^{2p-1} C_n = \sum_{n=0}^{2p-1} CT \left[1 - x \right] \left(2 + x + \frac{1}{x}\right) = CT \left[ \frac{(1 - x) \left( \left(2 + x + \frac{1}{x}\right)^{2p} - 1 \right)}{2 + x + \frac{1}{x} - 1} \right]
\]

\[
= CT \left[ \frac{\left(1 - x \right) \left( \left(6 + 4x + \frac{4}{x} + x^2 + \frac{x^2}{x}\right)^{2p} - 1 \right)}{2 + x + \frac{1}{x} - 1} \right]
\]

\[
\equiv_p CT \left[ \frac{(1 - x) \left( \left(6 + 4x^{2p} \left(\left(\frac{4}{x}\right)^p \right) + x^{2p} \left(\frac{1}{x^p}\right)\right) - 1 \right)}{2 + x + \frac{1}{x} - 1} \right].
\]

Since only the terms \(\frac{1}{x^p}\) and \(\frac{1}{x}\) in the numerator contribute to the constant term, this equals

\[
[x^{2p-1}] \left[ \frac{(1 - x) \left(1 + 4x^{2p}\right)}{1 + x + x^2} \right] = [x^{2p-1}] \left[ \frac{(1 - x)^2 \left(1 + 4x^{2p}\right)}{1 - x^3} \right]
\]

\[
= [x^{2p}] \left[ \frac{x}{1 - x^3} \right] + [x^{2p}] \left[ \frac{-2x^2}{1 - x^3} \right] + [x^{2p}] \left[ \frac{x^3}{1 - x^3} \right]
\]

\[
+ [x^{2p}] \left[ \frac{4x}{1 - x^3} \right] + [x^{2p}] \left[ \frac{-8x^2}{1 - x^3} \right] + [x^{2p}] \left[ \frac{4x^3}{1 - x^3} \right]
\]

\[
= [x^{2p}] \left[ \sum_{i=0}^{\infty} 1 \cdot x^{3i+1} \right] + [x^{2p}] \left[ \sum_{i=0}^{\infty} (-2) \cdot x^{3i+2} \right] + [x^{2p}] \left[ \sum_{i=0}^{\infty} 1 \cdot x^{3i+3} \right],
\]

\[
+ [x^{2p}] \left[ \sum_{i=0}^{\infty} 4 \cdot x^{3i+1} \right] + [x^{2p}] \left[ \sum_{i=0}^{\infty} (-8) \cdot x^{3i+2} \right] + [x^{2p}] \left[ \sum_{i=0}^{\infty} 4 \cdot x^{3i+3} \right],
\]

and the result follows from extracting the coefficients of \(x^{2p}\) and \(x^{p}\). \(\square\)
The same method can be used to find the “mod $p$” of $\sum_{n=0}^{rp^a-1} C_n$ for any specific $r$.

The same method applied to the Motzkin numbers, $M_n$, that may be defined by the constant term formula

$$M_n = CT \left[ (1 - x^2) \left( 1 + x + \frac{1}{x} \right)^n \right],$$

leads to the following:

**Proposition 3.** Let $M_n$ denote the $n$th Motzkin number. Then, for any prime $p \geq 3$, we have

$$\sum_{n=0}^{p^a-1} M_n \equiv_p \begin{cases} -2, & \text{if } p \equiv 1 \pmod{4} \text{ or } p \equiv 3 \pmod{4} \text{ and } a \text{ is even} \\ 2, & \text{if } p \equiv 3 \pmod{4} \text{ and } a \text{ is odd} \end{cases}$$

**Proof.**

$$\sum_{n=0}^{p^a-1} M_n = \sum_{n=0}^{p^a-1} CT \left[ (1 - x^2) \left( 1 + x + \frac{1}{x} \right)^n \right] = CT \left[ \frac{(1 - x^2) \left( (1 + x + \frac{1}{x})^{p^a-1} - 1 \right)}{1 + x + \frac{1}{x} - 1} \right]$$

$$\equiv_p CT \left[ \frac{(1 - x^2) \left( 1 + x^{p^a} + \frac{1}{p^a x} - 1 \right)}{1 + x + \frac{1}{x} - 1} \right] = CT \left[ \frac{(1 - x^2) \left( x^{p^a} + \frac{1}{p^a x} \right)}{x + \frac{1}{x}} \right] = CT \left[ \frac{x(1 - x^2) \left( x^{p^a} + \frac{1}{p^a x} \right)}{1 + x^2} \right]$$

$$= [x^{p^a}] \left[ \frac{1 - x^2}{1 + x^2} \right] = [x^{p^a}] \left[ \frac{x}{1 + x^2} \right] - [x^{p^a}] \left[ \frac{x^3}{1 + x^2} \right]$$

$$= [x^{p^a}] \left[ \sum_{i=0}^{\infty} (-1)^i x^{2i+1} \right] + [x^{p^a}] \left[ \sum_{i=0}^{\infty} (-1)^{i+1} x^{2i+3} \right],$$

and the result follows from extracting the coefficient of $x^{p^a}$ from the first and second geometric series above, by noting that when $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$ and $a$ is even, then $p^{a+1} \equiv 1 \pmod{4}$ and in this case, $i$ is even in the first series, and odd in the second one, and vice-versa when $p \equiv 3 \pmod{4}$ and $a$ is odd.

The same method can be used to find the “mod $p$” of $\sum_{n=0}^{rp^a-1} M_n$ for any specific $r$.

Next we consider the Apagodu-Zeilberger extension of Chen-Hou-Zeilberger method for discovery and proof of congruence theorems to multisums and multivariables [1] when the upper summation is replaced by $p^a - 1$.

**Proposition 4.** For any prime $p$ and $a \in \{0, 1, 2, 3, \ldots\}$, we have

$$\sum_{n=0}^{p^a-1} \sum_{m=0}^{p^a-1} \left( \frac{n+m}{m} \right)^2 \equiv_p \begin{cases} 1, & \text{if } p \equiv 1 \pmod{3} \text{ or } p \equiv 2 \pmod{3} \text{ and } a \text{ is odd} \\ -1, & \text{if } p \equiv 2 \pmod{3} \text{ and } a \text{ is even} \\ 0 & \text{if } p \equiv 0 \pmod{3} \end{cases}$$
Proof. Let \( P(x, y) = (1 + y)(1 + \frac{1}{x}) \) and \( Q(x, y) = (1 + x)(1 + \frac{1}{y}) \). Then

\[
\left( \frac{n + m}{m} \right)^2 = \left( \frac{n + m}{m} \right) \left( \frac{n + m}{n} \right) = CT \left[ P(x, y)^n Q(x, y)^m \right].
\]

We have

\[
\sum_{m=0}^{p^n-1} \sum_{n=0}^{p^n-1} \left( \frac{m + n}{m} \right)^2 = \sum_{m=0}^{p^n-1} \sum_{n=0}^{p^n-1} CT \left[ P(x, y)^n Q(x, y)^m \right]
\]

\[
= \sum_{m=0}^{p^n-1} \sum_{n=0}^{p^n-1} \left[ \frac{(P(x, y)^{p^n} - 1)Q(x, y)^m}{P(x, y) - 1} \right]
\]

\[
= \left[ \frac{(P(x, y)^{p^n} - 1)(Q(x, y)^{p^n} - 1)}{P(x, y) - 1} \right].
\]

We can pass to mod \( p \) as above, and get

\[
\sum_{m=0}^{p^n-1} \sum_{n=0}^{p^n-1} \left( \frac{m + n}{m} \right)^2 \equiv_p \left[ \frac{(P(x, y)^{p^n} - 1)(Q(x, y)^{p^n} - 1)}{P(x, y) - 1} \right]
\]

It is possible to show that the coefficient of \( x^n y^n \) in the Maclaurin expansion of the rational function \( \frac{1}{(1+y+y)\left(1+x+x+y\right)} \) is 1 when \( n \equiv 0 \) (mod 3), -1 when \( n \equiv 1 \) (mod 3), and 0 when \( n \equiv 2 \) (mod 3).

One way is to do a partial fraction decomposition, and extract the coefficient of \( x^n \), getting a certain expression in \( y \) and \( n \), and then extract the coefficient of \( y^n \). Another way is by using the Apagodu–Zeilberger algorithm (\[2\]), that outputs that the sequence of diagonal coefficients, let’s call them \( a(n) \), satisfy the recurrence equation \( a(n+2) + a(n+1) + a(n) = 0 \), with initial conditions \( a(0) = 1, a(1) = -1 \).

We finally consider partial sums of trinomial coefficients.

**Proposition 5.** Let \( p > 2 \) be prime; then we have

\[
\sum_{m_1=0}^{p^n-1} \sum_{m_2=0}^{p^n-1} \sum_{m_3=0}^{p^n-1} \left( \frac{m_1 + m_2 + m_3}{m_1, m_2, m_3} \right) \equiv_p 1.
\]

**Proof.** First observe that \( \left( \frac{m_1 + m_2 + m_3}{m_1, m_2, m_3} \right) = CT \left[ \frac{(x+y+z)^{m_1+m_2+m_3}}{x^{m_1}y^{m_2}z^{m_3}} \right]. \)
So far this is true for all \( i \) and \( j \).

Finally, if we set \( i = j = k \), the desired coefficient of \( x^p - y^p z^p - z^p y^p \) is

\[
\sum_{i=0}^{p-1} (-1)^i (y^i + z^{p-1-i}) = \sum_{i=0}^{p-1} (-1)^i (1 - 1) + \ldots + 1 - 1 + 1 = 1.
\]

The same method of proof used in Proposition 5 yields (with a little more effort) a multinomial generalization.

**Proposition 7.** Let \( p \geq 3 \) be prime, then

\[
\sum_{m_1=0}^{p^n-1} \cdots \sum_{m_n=0}^{p^n-1} (m_1 + \ldots + m_n) \equiv_p 1.
\]
\[
\sum_{n=0}^{p-1} (3n+1) \binom{2n}{n} \equiv_p \begin{cases} 
-1, & \text{if } p \equiv 2 \pmod{3} \\
1, & \text{if } p \equiv 1 \pmod{3} 
\end{cases}.
\]

Motivated by this, we state two conjectures where the current method results in a rational function of higher degree that does not result the desired form.

**Conjecture 1:** For any prime \( p \geq 3 \), we have
\[
\sum_{n=0}^{p-1} (5n+1) \binom{4n}{2n} \equiv_p \begin{cases} 
1, & \text{if } p \equiv 2 \pmod{3} \\
-1, & \text{if } p \equiv 1 \pmod{3} 
\end{cases}.
\]

The super Catalan numbers, first introduced by Ira Gessel [4], also admits the following simple formulas.

**Conjecture 2:** For any prime \( p \), the supper Catalan number satisfies,
\[
\sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \binom{2m}{m} \binom{2n}{n} \binom{m+n}{n} \equiv_p \begin{cases} 
1, & \text{if } p \equiv 1 \pmod{3} \\
-1, & \text{if } p \equiv 2 \pmod{3} 
\end{cases},
\]

and
\[
\sum_{m=0}^{p-1} \sum_{n=0}^{p-1} (3m+3n+1) \binom{2m}{m} \binom{2n}{n} \binom{m+n}{n} \equiv_p \begin{cases} 
-7, & \text{if } p \equiv 1 \pmod{3} \\
7, & \text{if } p \equiv 2 \pmod{3} 
\end{cases}.
\]

**Acknowledgements** We are grateful to Tewodros Amdeberhan and Doron Zeilberger for their valuable comments on an earlier version.

**References**

[1] M. Apagodu and D. Zeilberger, *Using the "Freshman’s Dream" to Prove Combinatorial Congruences*, American Mathematical Monthly, v. 124 No. 7 (Aug.-Sept. 2017), 597-608.

[2] M. Apagodu and D. Zeilberger, Multi-Variable Zeilberger and Almkvist-Zeilberger Algorithms and the Sharpening of Wilf-Zeilberger Theory, *Adv. Appl. Math.* 37 (2006), 139-152, http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/multiZ.html.

[3] William Y.C. Chen, Qing-Hu Hou, and Doron Zeilberger, Automated Discovery and Proof of Congruence Theorems for Partial Sums of Combinatorial Sequences, *J. of Difference Equations and Applications* 22 (2016), 780-788.

[4] I. Gessel, Super ballot numbers, *J. Symb. Comput.* 14 (1992), 179-194

[5] S. W. Golomb, *Combinatorial proof of Fermat’s “Little” Theorem*, American Mathematical Monthly, 63(1956), 718.

[6] H. Pan and Z. Sun, A combinatorial Identity with Applications to Catalan numbers, *Discrete Math.* 306(2006), 16, 2011-2040.

[7] Z. Sun and R. Tauraso, *On some congruences for Binomial coefficients*, *In. J. Number Theory*(2011), 3(645-662).

[8] Wikipedia contributors, Freshman Dream, *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Freshman’s_dream.
