

# binomial series and its Applications in congruences

By Shazly Abdullah

**ABSTRACT.** In this study we used an algebraic method that uses elementary algebra and binomial theorem. To create binomial series  $L_n(k, g, u) = V_n^q(k, g, u)S_n(k, g)$ . This is a type of series that has several properties in variables such as if  $u = 1$  then  $L_n(k, g, 1) = S_n(k, g)$  where  $V_n^q(k, g, 1) = 0$ . We used these series to prove results in congruences for example, we proved If  $g^m = yx^n - 1$  where  $\varphi(g^m)$  Euler function  $m, n \neq 0$  and  $\frac{\varphi(g^m)}{n}$  then  $y^{\frac{\varphi(g^m)}{n}} \equiv 1 \pmod{g^m}$ . We also obtained several results in finite series.

**Key words:** binomial theorem, binomial series, primitive roots, congruences

## 1. INTRODUCTION

Gauss foot concept congruences in number theory, where it facilitates operations and study in division, is one of the most important theorems in congruence, Euler theorem, which is considered one of the most important theorems in number theory because it is related to many theorems and definitions in number theory, for example, [see James J Tattersall 162] Primitive roots can be defined

In this paper, elementary algebra and binomial theorem, and difference of tow nth power are used to created finite series in an algebraic method, then we used series to create congruence with specific properties. Through this process, we reached the theorem. 1 theorem.2 and several results in finite series.

The goal of this paper is to construct a kind of finite binomial series it is a binomial and its application in the study of congruences, it was used to prove the theorem.1. and theorem.2. according binomial theorem and difference of tow nth power theorem if  $n$  a positive integer and  $x$   $y$  real numbers then [see K.H 22]

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

And

$$x^n - y^n = (x - y) \sum_{j=1}^n x^{n-j} y^{j-1}$$

## 2. basic series

**Theorem.1** let  $a, d$  real numbers where  $n$  a positive integer then

$$a^{n-1}(d^n - 1) = \frac{d-1}{a-1}(a^n - 1) + (d-1) \sum_{j=1}^{n-1} \frac{(ad-1)^j}{(a-1)^{j+1}} \left( a^n - \binom{n}{0} - \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right)$$

**Theorem.2** let  $y, x, m$  a positive integers and  $n = yx^m - 1$  and  $\varphi(n)$  Euler function where  $\frac{\varphi(n)}{k}$   $1 \leq k \leq m$  then

$$(yx^{m-k})^{\frac{\varphi(n)}{k}} \equiv 1 \pmod{n}$$

In this section first we will create the basic binomial series Then we use the series to prove the first theorem and the other results

**Basic binomial series.** let  $k, g, u$ , real numbers and  $m$  constant then

$$L_n(k, g, u) = V_n^n(k, g, u) + S_n(k, g)$$

Where

$$L_n(k, g, u) = (u - k + g)^n - m(1 + g)^n$$

And

$$V_n^n(k, g, u) = \sum_{j=0}^n (-1)^j \binom{n}{j} (u^{n-j} - m)(k - g)^j$$

And

$$S_n(k, g) = mk \sum_{j=0}^{n-1} (-1)^{j+1} \frac{(k - g)^j}{g^{j+1}} \left( (1 + g)^n - \left( \binom{n}{0} + \binom{n}{1}g + \binom{n}{2}g^2 \dots \dots \dots \binom{n}{j}g^j \right) \right)$$

**Proof.** let  $g, k, u$ , real numbers then according to difference of tow nth power theorem we have that

$$(k - g)^n - (-g)^n = k \sum_{j=1}^n (k - g)^{j-1} (-g)^{n-j}$$

Then

$$-(-g)^n = -(k - g)^n + k \sum_{j=1}^n f^{j-1}(k, h)g^{n-j}(-h)$$

let  $q \in R, n \in N$  where  $m$  constant then by multiplying  $m$  and adding  $u^q(k - g)^n$  from both sides

$$u^q(k - g)^n - m(-g)^n = u^q(k - g)^n - m(k - g)^n + m k \sum_{j=1}^n (k - g)^{j-1} (-g)^{n-j}$$

Then

$$(1) \quad u^q(k - g)^n - m(-g)^n = (u^q - m)(k - g)^n + m k \sum_{j=1}^n (k - g)^{j-1} (-g)^{n-j}$$

According binomial theorem

$$(u - k + g)^n = u^n - \binom{n}{1} u^{n-1}(k - g) + \binom{n}{2} u^{n-2}(k - g)^2 - \binom{n}{3} u^{n-3}(k - g)^3 \dots \dots \dots (k - g)^n$$

And

$$m(1 + g)^n = m + m \binom{n}{1} g + m \binom{n}{2} g^2 + m \binom{n}{3} g^3 \dots \dots \dots mg^n$$

By subtracting  $m(1 + g)^n$  from  $(u - k + g)^n$  then

$$\begin{aligned}
& (u - k + g)^n - m(1 + g)^n \\
&= u^n - m - \binom{n}{1} u^{n-1}(k - g) - m \binom{n}{1} g + \binom{n}{2} u^{n-2}(k - g)^2 - m \binom{n}{2} g^2 \\
&\quad - \binom{n}{3} u^{n-3}(k - g)^3 - m \binom{n}{3} g^3 \dots \dots \dots (k - g)^n - mg^n
\end{aligned}$$

By extracting the common factor  $\binom{n}{j}$  between the terms

$$\begin{aligned}
(2) \quad & (u - k + g)^n - m(1 + g)^n \\
&= u^n - m - \binom{n}{1} (u^{n-1}(k - g) + mg) + \binom{n}{2} (u^{n-2}(k - g)^2 - mg^2) \\
&\quad - \binom{n}{3} (u^{n-3}(k - g)^3 + mg^3) \dots \dots \dots ((k - g)^n - mg^n)
\end{aligned}$$

According equation (1)

$$u^q(k - g)^n - m(-g)^n = (u^q - m)(k - g)^n + m k \sum_{j=1}^n (k - g)^{j-1} (-g)^{n-j}$$

So we note in (2) limit (1) equal  $u^n - m$  and limit (2) equal  $\binom{n}{1} (u^{n-1}(k - g) + mg)$  and limit 2 equal  $\binom{n}{2} (u^{n-2}(k - g)^2 - mg^2)$  and 3 equal  $\binom{n}{3} (u^{n-3}(k - g)^3 + mg^3) (k - g)^n - mg^n$  then

Let

$$(3) \quad W_n^q(k, g, u) = u^q(k - g)^n - m(-g)^n$$

And

$$Z_n^q(k, g, u) = (u^q - m)(k - g)^n$$

and

$$C_n(k, g) = m k \sum_{j=1}^n (k - g)^{j-1} (-g)^{n-j}$$

So

$$(4) \quad W_n^q(k, g, u) = Z_n^q(k, g, u) + C_n(k, g)$$

From (3) and limit (1) in (2)

$$\binom{n}{0} (u^n - m) = \binom{n}{0} W_0^{n-0}(k, g, u)$$

From equation (3) and Limit (2) in equation (2)

$$\binom{n}{1} (u^{n-1}(k - g) + mg) = \binom{n}{1} W_1^{n-1}(k, g, u)$$

Limit (3)

$$\binom{n}{2} (u^{n-2}(k - g)^2 - mg^2) = \binom{n}{2} W_2^{n-2}(k, g, u)$$

Limit (4) in equation (2)

$$\binom{n}{3} (u^{n-3}(k - g)^3 + mg^3) = \binom{n}{3} W_3^{n-3}(k, g, u)$$

And

4

Last limit

$$\binom{n}{n} ((k-g)^n - mg^n) = \binom{n}{n} W_n^{n-n}(k, g, u)$$

so

$$(u - k + g)^n - m(1 + g)^n = \sum_{j=0}^n (-1)^j \binom{n}{j} w^{n-j}(k, g, u)$$

And

$$L_n(k, g, u) = (u - k + g)^n - m(1 + g)^n$$

Then

$$L_n(k, g, u) = \sum_{j=0}^n (-1)^j \binom{n}{j} w^{n-j}(k, g, u)$$

From equation(4)  $w_n^q(k, g, u) = z_n^q(k, g, u) + c_n(k, g)$  then we have that

$$(5) \quad L_n(k, g, u) = \sum_{j=0}^n (-1)^j \binom{n}{j} z_j^{n-j}(k, g, u) + \sum_{j=0}^n (-1)^j \binom{n}{j} c_j(k, g)$$

We note from the equation (4)

$$Z_n^q(k, g, u) = (u^q - m)(k - g)^n$$

And

$$C_n(k, g) = m k \sum_{j=1}^n (k - g)^{j-1} (-g)^{n-j}$$

Then

$$L_n(k, g, u) = \sum_{j=0}^n (-1)^j \binom{n}{j} (u^{n-j} - m)(k - g)^j + mk \sum_{j=1}^n \sum_{r=1}^j (-1)^j \binom{n}{j} (k - g)^{r-1} (-g)^{j-r}$$

Let

$$V_n^n(k, g, u) = \sum_{j=0}^n (-1)^j \binom{n}{j} (u^{n-j} - m)(k - g)^j$$

And

$$S_n(k, g) = mk \sum_{j=1}^n \sum_{r=1}^j (-1)^j \binom{n}{j} (k - g)^{r-1} (-g)^{j-r}$$

Then we have

$$(6) \quad L_n(k, g, u) = V_n^n(k, g, u) + S_n(k, g)$$

we find in  $S_n(k, g)$  tow signs  $(-1)^j(-1)^{j-r} = (-1)^r$  if r j even or odd so they can by combined in  $(-1)^r$  then we find that

$$S_n(k, g) = mk \sum_{j=1}^n \sum_{r=1}^j (-1)^r \binom{n}{j} (k - g)^{r-1} g^{j-r}$$

where

$$s_n(k, g) = mk \left( \sum_{r=1}^1 (-1)^r \binom{n}{1} (k-g)^{r-1} g^{1-r} + \sum_{r=1}^2 (-1)^r \binom{n}{2} (k-g)^{r-1} g^{2-r} \right. \\ \left. + \sum_{r=1}^3 (-1)^r \binom{n}{3} (k-g)^{r-1} g^{3-r} \dots \dots \dots \sum_{r=1}^n (-1)^r \binom{n}{n} (k-g)^{r-1} g^{n-r} \right)$$

In  $S_n(k, g)$  all compound terms have been dismantled note if we add for every first term in the complex term we find that  $-\left(\binom{n}{1} + \binom{n}{2}g \dots \dots \binom{n}{n}g^{n-1}\right)$  then we adding the terms to include that  $(k-g)$  finding that  $(k-g)\left(\binom{n}{2} + \binom{n}{3}g \dots \dots \binom{n}{n}g^{n-2}\right)$  then the term that include  $(k-g)^2$  we find that  $(k-g)^2\left(-\left(\binom{n}{3} + \binom{n}{4}g \dots \dots \binom{n}{n}g^{n-3}\right)\right)$  if the method is equal all the terms can be added  $1 \leq j \leq n-1$  until we reach the last terms  $(k-g)^{n-1}$  then

$$S_n(k, g) = mk \left( -\left(\binom{n}{1} + \binom{n}{2}g + \binom{n}{3}g^2 \dots \dots \binom{n}{n}g^{n-1}\right) \right. \\ \left. + (k-g)\left(\binom{n}{2} + \binom{n}{3}g + \binom{n}{4}g^2 + \binom{n}{5}g^3 \dots \dots \binom{n}{n}g^{n-2}\right) \right. \\ \left. - (k-g)^2\left(\binom{n}{3} + \binom{n}{5}g + \binom{n}{6}g^2 + \binom{n}{7}g^3 \dots \dots \binom{n}{n}g^{n-3}\right) \dots \dots \binom{n}{n}g^{n-n} \right)$$

Using the binomial theorem it is possible to abbreviate all the terms that include,  $(k-g)$  and  $(k-g)^2$  and  $(k-g)^3$  until we reach the last term  $(k-g)^{n-1}$ , we notice that

$$-\left(\binom{n}{1} + \binom{n}{2}g + \binom{n}{3}g^2 \dots \dots \binom{n}{n}g^{n-1}\right) = -\frac{(1+g)^n - \binom{n}{0}}{g}$$

$$\left(\binom{n}{2} + \binom{n}{3}g \dots \dots \binom{n}{n}g^{n-2}\right) = \frac{(1+g)^n - \binom{n}{0} - \binom{n}{1}g}{g^2}$$

$$-\left(\binom{n}{3} + \binom{n}{4}g \dots \dots \binom{n}{n}g^{n-3}\right) = -\frac{(1+g)^n - \binom{n}{0} - \binom{n}{1}g - \binom{n}{2}g^2}{g^3}$$

Then

$$S_n(k, g) = mk \sum_{j=0}^{n-1} (-1)^{j+1} \frac{(k-g)^j}{g^{j+1}} \left( (1+g)^n - \left(\binom{n}{0} + \binom{n}{1}g + \binom{n}{2}g^2 \dots \dots \binom{n}{j}g^j\right) \right)$$

Let

$$(7) \quad L_n(k, g, u) = (u - k + g)^n - m(1+g)^n$$

$$(8) \quad V_n^n(k, g, u) = \sum_{j=0}^n (-1)^j \binom{n}{j} (u^{n-j} - m)(k-g)^j$$

$$(9) \quad S_n(k, g)$$

$$= mk \sum_{j=0}^{n-1} (-1)^{j+1} \frac{(k-g)^j}{g^{j+1}} \left( (1+g)^n - \left( \binom{n}{0} + \binom{n}{1}g + \binom{n}{2}g^2 \dots \dots \dots \binom{n}{j}g^j \right) \right)$$

### 3.proof theorem.1

In this section we will use the basic series  $L_n(k, g, u) = V_n^n(k, g, u) + S_n(k, g)$  in prove the theorem.1 then according basic infinite series if  $u = 1$  in  $V_n^n(k, g, u)$  we have that

$$V_n^n(k, g, 1) = \sum_{j=1}^n (-1)^j \binom{n}{j} ((1)^{n-j} - 1)(k-g)^j = 0$$

Then according equations

$$L_n(k, g, 1) = V_n^n(k, g, 1) + S_n(k, g)$$

Then

$$L_n(k, g, 1) = S_n(k, g)$$

Then according to the equations, (7, 8,9) we find that

$$L_n(k, g, 1) = S_n(k, g)$$

Then

$$(1-k+g)^n - (1+g)^n = k \sum_{j=0}^{n-1} (-1)^{j+1} \frac{(k-g)^j}{g^{j+1}} \left( (1+g)^n - \left( \binom{n}{0} + \binom{n}{1}g \dots \dots \binom{n}{j}g^j \right) \right)$$

Let a d a positive integers where

$$\begin{aligned} g &= a - 1 \\ k &= -ad + a \end{aligned}$$

Then

$$\begin{aligned} & (1 + ad - a + a - 1)^n - (1 + a - 1)^n \\ = & (-ad + a) \sum_{j=0}^{n-1} (-1)^{j+1} \frac{(-ad + a - a + 1)^j}{(a-1)^{j+1}} \left( (1 + a - 1)^n - \left( \binom{n}{0} + \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right) \right) \end{aligned}$$

We have that

$$= (-ad + a) \sum_{j=0}^{n-1} (-1)^{j+1+j} \frac{(ad-a)^j}{(a-1)^{j+1}} \left( a^n - \left( \binom{n}{0} + \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right) \right)$$

Then

$$\begin{aligned} a^{n-1}(d^n - 1) &= \frac{-d+1}{a-1} (a^n - 1) \\ + (d-1) \sum_{j=1}^{n-1} \frac{(-1)^{2j+2}(ad-1)^j}{(a-1)^{j+1}} &\left( a^n - \left( \binom{n}{0} + \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right) \right) \end{aligned}$$

so we have that

$$a^{n-1}(d^n - 1) = \frac{d-1}{a-1} (a^n - 1)$$

$$+(d-1) \sum_{j=1}^{n-1} \frac{(ad-1)^j}{(a-1)^{j+1}} \left( a^n - \left( \binom{n}{0} + \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right) \right)$$

Note the negative sign in the equation

$$(10) \quad \begin{aligned} & a^{n-1}(d^n - 1) \\ &= \frac{d-1}{a-1} (a^n - 1) \end{aligned}$$

$$+(d-1) \sum_{j=1}^{n-1} \frac{(ad-1)^j}{(a-1)^{j+1}} \left( a^n - \left( \binom{n}{0} + \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right) \right)$$

Then

$$\begin{aligned} & a^{n-1}(d^n - 1) = \frac{d-1}{a-1} (a^n - 1) \\ & +(ad-1) \left( (d-1) \sum_{j=1}^{n-1} \frac{(ad-1)^{j-1}}{(a-1)^{j+1}} \left( a^n - \binom{n}{0} + \binom{n}{1}(a-1) \dots \dots \binom{n}{j}(a-1)^j \right) \right) \end{aligned}$$

Then we note  $(d-1, ad-1) = (a^{n-1}, ad-1) = 1$  then we find that if  $a^n \equiv 1 \pmod{m}$  where  $m = ad - 1$  then  $d^n \equiv 1 \pmod{m}$

**Lemma.1** if  $2^n \equiv 1 \pmod{m}$  and  $m = 2x - 1$  where  $n, x$  a positive integers then

$$x^n \equiv 1 \pmod{m}$$

**Proof** let in theorem.1  $a = 2$  and  $d = x$

### 3. proof theorem.2

In this section we will prove theorem.2 using theorem.1 but before that we mention according to Euler's theorem  $a^{\varphi(n)} \equiv 1 \pmod{n}$  where  $(a, n) = 1$  and  $\varphi(n)$  is Euler function see proof Euler theorem in [K.M. 244]

**Proof theorem.2** according Euler theorem if  $(a, n) = 1$  then  $a^{\varphi(n)} \equiv 1 \pmod{n}$  and according theorem.1 if  $a^n \equiv 1 \pmod{m}$  where  $m = ad - 1$  then  $d^n \equiv 1 \pmod{m}$

Then let in theorem.1  $n = yx^m - 1$  and  $a = x^k$  then  $d = \frac{n+1}{a} = yx^{m-k}$  so we find according Euler's theorem

$$(x^k)^{\frac{\varphi(n)}{k}} \equiv 1 \pmod{n}$$

Then according theorem.1

$$(yx^{m-k})^{\frac{\varphi(n)}{k}} \equiv 1 \pmod{n}$$

**Lemma.2** let  $x, y, k \in \mathbb{N}$  where  $n = yx^m - 1$  and  $\varphi(n)$  Euler function where  $m \setminus \varphi(n)$  then

$$y^{\frac{\varphi(n)}{m}} \equiv 1 \pmod{n}$$

**Proof** let in theorem.2  $m = k$  then  $(yx^{m-m})^{\frac{\varphi(n)}{m}} \equiv 1 \pmod{n}$  then we have that  $y^{\frac{\varphi(n)}{m}} \equiv 1 \pmod{n}$

**Theorem.3** if  $g^m = yx^n - 1$  and  $\varphi(g^m)$  Euler function where  $n \setminus \varphi(g^m)$  then

$$y^{\frac{\varphi(g^m)}{n}} \equiv 1 \pmod{g^m}$$

**Proof.** let in theorem.2  $n = g^m$  and  $a = x^n$  and  $d = y$  where  $k = n$

8

**Lemma.3** let  $p$  prime number and  $x$   $m$  a positive integer and if  $p = dx^m - 1$  and  $\frac{p-1}{m}$  then

$$d^{\frac{p-1}{m}} \equiv 1 \pmod{p}$$

**Proof** let  $n = p$  and  $y = d$  in lemma.2

## References

1. H. S. Rose . A Course in Number Theory " Oxford Science publications (1988).
2. K. M. Rose, Elementary Number Theory" 4<sup>th</sup> Edition Addison- Wesley (2000).
3. James J. Tattersall Elementary Number Theory in Nine Chapters Cambridge University Press 2005

Student :Shazly Abdullah Fdl

Faculty of mathematics sciences & statistics

Aleenlain University Sudan

Shazlyabdullah3@gmail.com